

SECURE USE OF THE INTERNET BY BUSINESS

Rana Tassabehji

**Information Systems Institute
University of Salford, Salford, UK**

**Submitted in Partial Fulfilment of the Requirements
of the Degree of Doctor of Philosophy, January 2000**

CONTENTS

1. INTRODUCTION	1
1.1 Background to the Research Topic	2
1.1.1 The Importance of Technology	2
1.1.2 The Importance of the Internet	3
1.1.3 The Importance of Internet Security	4
1.1.4 The Importance of Small and Medium-sized Enterprises	6
1.2 Aims & Objectives	7
1.3 Assumptions and Limitations	9
1.4 Organisation of the Remainder of this Study	10
2. LITERATURE REVIEW - THE MACRO-ENVIRONMENT	13
2.1 The Role of Government	14
2.2 The Developing Legal Infrastructure	17
2.2.1 Internet Law	18
2.3 The Technology and its Application	21
2.3.1 The Internet	21
2.3.1.1 Attitudes and Usage	23
2.3.2 Electronic Mail	28
2.3.2.1 Attitudes and Usage	29
2.3.3 Security	32
2.3.3.1 Physical Security	32
2.3.3.2 Systems and Network Security	33
2.3.3.3 Security of Electronic Data	40
2.4 Summary and Conclusions	41
3. METHODOLOGY	44
3.1 Research Strategy	47
3.2 Research Methodology	48
3.2.1 Design and Development of the Security Solution	48
3.2.1.1 The Methodology	49
3.2.2 Implementation and Usage	49
3.3 The Process of Organic Methodology Development	53
3.3.1 Qualitative Methodology	54
3.3.2 Quantitative Methodology	54
3.4 Conclusions	55
4. DESIGNING A SECURITY SOLUTION - SECONDARY RESEARCH	56
4.1 Cryptography	58
4.1.1 Symmetric Key Cryptography	59
4.1.1.1 Attacks on Symmetric Encryption Algorithms	61
4.1.2 Public Key Cryptography (Asymmetric Cryptography)	62
4.1.2.1 Attacks on Asymmetric/Public Key Encryption Algorithms	64
4.2 Digital Signatures	66

4.3 Digital Certificates	67
4.3.1 Certificate Repositories	68
4.3.2 Certificate Policy	69
4.4 Authentication, Key Management and Trusted Services	70
4.4.1 Certification Authority and Trusted Third Parties	71
4.5 Trusted Service Providers	73
4.5.1 Users of a Trusted Service	73
4.5.2 Trusted Services Organisations 1996/7	74
4.5.2.1 The Main Commercial Providers of Trusted Services	75
4.5.2.2 Trusted Services	78
4.6 Certification Authority (CA) Infrastructures	80
4.6.1 The Hierarchical Certification Authority Structure	81
4.6.2 Cross Certification Authority Structure	83
4.7 Policies Governing Cryptography and TTPs	84
4.8 Conclusions	88
5. DESIGNING A SECURITY SOLUTION - PRIMARY RESEARCH	90
5.1 Authentication Infrastructure Lifecycle	90
5.2 The Analysis Stage	91
5.2.1 Primary Research	91
5.3 The Design Phase	93
5.3.1 Software Evaluation	94
5.3.1.1 Broad Screening	95
5.3.1.1.1 Broad Screening Findings	96
5.3.1.2 Narrow Screening	98
5.3.1.2.1 Narrow Screening Findings	99
5.3.1.2.1.1 Evaluation of PGP	99
5.3.1.2.1.2 Evaluation of Entrust Client 3 for Windows 95	102
5.3.1.3 Conclusions	105
5.3.2 Controls, Procedures and Policy	106
5.3.2.1 The Certification Practice Statement	106
5.3.3 User Training and Support	113
5.3.4 Corporate Associations and Endorsements	113
5.4 Conclusion - The Authentication infrastructure Trust Model	114
6. IMPLEMENTATION OF THE SECURITY SERVICE - CASE STUDIES	115
6.1 Case Study I - Company D	119
6.1.1 Methodology	119
6.1.1.1 Unstructured Observation	119
6.1.1.2 Semi-Structured Depth Interviews	120
6.1.1.3 Documentation	120
6.1.1.4 Observer Participation	121
6.1.2 Findings	121
6.1.2.1 The Organisation and Its Background	122
6.1.2.2 The Current Processes	126
6.1.2.3 Implementing the Security & Authentication infrastructure	131
6.1.3.4 Outcome of the Implementation Process	136
6.1.4 Conclusions	136
6.2 Case Study II - Company T	138
6.2.1 Methodology	138
6.2.1.1 Structured Observation	138

6.2.1.1	Structured Observation	138
6.2.1.2	Time Series Structured Questionnaires	139
6.2.1.3	Depth Interviews	139
6.2.2	Findings	139
6.2.2.1	The Organisation and Its Background	139
6.2.2.2	The Current Business Processes	140
6.2.2.3	Implementing the Authentication infrastructure	142
6.2.2.4	Outcome of the Implementation	143
6.2.4	Conclusion	143
6.3	CASE STUDY III - UNIVERSITY X	144
6.3.1	The Organisation and Its Background	145
6.3.2	Methodology	146
6.3.3	Findings	154
1.	Department Y Sample Group	155
2.	Department Z Sample Group	169
6.3.4	Summary	178
6.4	Case Studies Conclusions	182
7. FURTHER RESEARCH (I)		185
7.1	DEPTH INTERVIEWS	186
7.1.1	Methodology	186
7.1.2	Findings	187
7.1.2.1.	Organisational Infrastructure	187
7.1.2.2	E-mail Usage and Uptake	188
7.1.2.3	Future Strategies	189
7.1.2.4	Trusted Third Party	190
7.1.3	Conclusions	190
7.2	TELEPHONE INTERVIEWS	191
7.2.1	The Telephone Sample	192
7.2.2	Survey Findings	193
7.2.2.1	The Service Sector	194
7.2.2.2	The Manufacturing Sector	199
7.2.2.3	The Trade Sector	202
7.2.3	Summary and Conclusions	203
8. FURTHER RESEARCH (II) - ADDITIONAL FINDINGS		207
8.1	NETWORK INFRASTRUCTURES IN SMES	207
8.2	CONCLUSIONS	209
9. DISCUSSION OF FINDINGS (I)		210
9.1	FRAMEWORK FOR ANALYSIS	210
9.1.1	Commitment to IT Project	211
9.1.2	Planning & Co-ordinating IT Infrastructure in Organisations	213
a)	Analysis and Re-engineering of Current Business Processes	214
b)	The Users	214
c)	The Technology	215
9.2	APPLYING THE MATRIX TO THE CASE STUDIES	216
9.3	CONCLUSIONS	220

10. DISCUSSION OF FINDINGS (II)	222
<hr/>	
10.1 Organisational Lifecycles and Network Infrastructures	222
I. The Entrepreneurial Stage	224
II. The Collectivity Stage	226
III. Formalisation Stage	228
IV. Elaboration Stage	230
10.2 Application of the Framework	231
10.3 Conclusions	233
11. THE BEST PRACTICE GUIDE FOR SMEs	234
<hr/>	
12. CONCLUSIONS	236
<hr/>	
12.1 The Research Study	237
12.2 Limitations of the Study	244
12.3 Implications of the Study	246
12.4 Recommendations	247
12.5 Future areas of study	248
13. EPILOGUE	248
<hr/>	
13.1 The Role of Government	249
13.2 The Growth in Certification Authorities and Trusted Third Parties	253
13.3 Continued Internet Growth	255
13.3.1 Proliferation of E-mail	256
13.3.2 Security	258
13.4 The Application of Internet Technology	260
13.5 The Impact of Technology on Management Thinking	265
13.6 Future Technology and Trends	269
13.6.1 Smart Card	269
13.6.2 Biometrics	270
13.6.3 Internet II	271
13.7 Conclusions	271
APPENDICES	273
<hr/>	
REFERENCES	392
<hr/>	

List of Appendices

Appendix 1 - Economic Regeneration Using IT	273
APPENDIX 2 - HISTORY OF EU FRAMEWORK FUNDING FOR IT	282
APPENDIX 3 - DEFINITION OF ERDF OBJECTIVE AREAS	283
APPENDIX 4 - FIREWALLS	286
APPENDIX 5 - EDI OVER THE INTERNET	288
APPENDIX 6 - SME PERCEPTION OF THE INTERNET - A REGIONAL STUDY	298
APPENDIX 7 - TELEPHONE INTERVIEW QUESTIONS	318
APPENDIX 8 - CERTIFICATION PRACTICE STATEMENT	319
APPENDIX 9 - TECHNOPHOBIA MEASUREMENT INSTRUMENTS INFORMATION	320
APPENDIX 10 - CA VALIDATION FORMS	322
APPENDIX 11 - TRAINING PROCEDURES	349
APPENDIX 12 - TRAINING SESSION HANDOUTS	353
APPENDIX 13 - ENTRUST SOFTWARE USER GUIDE	358
APPENDIX 14 - HELP DESK ENQUIRY FORM	362
APPENDIX 15 - QUESTIONNAIRES FOR COMPANY T	363
APPENDIX 16 - UNIVERSITY X - PRE-IMPLEMENTATION QUESTIONNAIRE	369
APPENDIX 17 - UNIVERSITY X - POST IMPLEMENTATION QUESTIONNAIRE	380
APPENDIX 18 - DISCUSSION GUIDE FOR DEPTH INTERVIEWS	385
APPENDIX 19 - INTERNET AND E-MAIL POLICIES AND GUIDELINES	387
APPENDIX 20 - INTERNATIONAL CERTIFICATION AUTHORITIES	388
Appendix 21 - Methodology Definitions	391

List of Tables

TABLE 1. THE NUMBER OF SMALL BUSINESSES IN THE UK	6
TABLE 2. PROJECT AIMS & OBJECTIVES FORMULATED INTO RESEARCH QUESTIONS	8
TABLE 3. NEW RESEARCH QUESTIONS	8
TABLE 4 . POTENTIAL IMPROVEMENT TO THE INTERNET	26
TABLE 5. ADVANTAGES AND DISADVANTAGES OF E-MAIL	29
TABLE 6. SECURITY THREATS AND PREVENTION MEASURES	34
TABLE 7. SUMMARY OF INTERNET RESEARCH DATA	41
TABLE 8. SUMMARY OF INTERNET SECURITY RESEARCH DATA	42
TABLE 9. FEATURES OF SYMMETRIC AND PUBLIC KEY CRYPTOSYSTEMS	65
TABLE 10. COMMERCIALY AVAILABLE CA CERTIFICATES AND SERVICES	80
TABLE 11 .BROAD SCREENING OF SECURITY SOFTWARE	97
TABLE 12 . MEASURES FOR EVALUATING SECURITY SOFTWARE	98
TABLE 13 . EVALUATION METRICS OF PGP AND ENTRUST	105
TABLE 14 . AREAS OF QUESTIONING FOR INTERNAL STAKEHOLDERS	120
TABLE 15 . CLASSIFICATION OF THE POPULATION SAMPLE ATTRIBUTES	147
TABLE 16 . POPULATION SAMPLE SCREENING CRITERIA	148
TABLE 17 . CATEGORISATION OF DEPARTMENT Z EXAMINATION PAPERS	149
TABLE 18 . CATEGORISATION OF IT INSTITUTE EXAMINATION PAPERS	150
TABLE 19 . CRITERIA FOR MEASURING TIME AND COST OF THE EXAMINATION PROCESS	153
TABLE 20 . DEPARTMENT Y TOTAL SAMPLE GROUP ATTRIBUTES	155
TABLE 21 . TIME AND COST OF TRADITIONAL TRANSMISSION (PAPER I)	161
TABLE 22 . TIME AND COST OF TRADITIONAL TRANSMISSION (PAPER II)	161
TABLE 23 . TIME AND COST OF SECURE TRANSMISSION I (EXAMINER A)	163
TABLE 24 . TIME AND COST OF SECURE TRANSMISSION II (EXAMINER A)	163
TABLE 25 . TIME AND COST OF SECURE TRANSMISSION (EXAMINER B)	164
TABLE 26 . COMPARATIVE TIMES AND COSTS OF TRADITIONAL AND SECURE ELECTRONIC PROCESSES	165
TABLE 27 . DEPARTMENT Z SAMPLE GROUP ATTRIBUTES	169
TABLE 28 PROFILE OF DEPTH INTERVIEW RESPONDENTS	186
TABLE 29 . BREAKDOWN OF RESPONDENTS COMPANY SIZE & INDUSTRY SECTOR (1999)	193
TABLE 30 . PERCENTAGE OF COMPANIES CONNECTED TO THE INTERNET BY SIZE	193
TABLE 31 A. SUMMARY OF THE RESEARCH PROJECT'S AIMS, QUESTIONS & CONCLUSIONS	238
TABLE 31 B. SUMMARY OF THE RESEARCH PROJECT'S AIMS, QUESTIONS & CONCLUSIONS	239

List of Figures

FIGURE 1. THE ENABLERS OF THE INFORMATION SOCIETY	16
FIGURE 2 . HOWARD'S TAXONOMY OF COMPLETE COMPUTER & NETWORK ATTACK	37
FIGURE 3. THE WHEEL OF SCIENCE THEORY OF RESEARCH	44
FIGURE 4. THE CONTINUUM OF RESEARCH METHODOLOGY THEORY	45
FIGURE 5. THE BIPARTITE RESEARCH STRATEGY	47
FIGURE 6. ORGANIC RESEARCH METHODOLOGY DEVELOPMENT	53
FIGURE 7. SYMMETRIC KEY CRYPTOGRAPHY	59
FIGURE 8. PUBLIC KEY CRYPTOGRAPHY	62
FIGURE 9. THE PROCESS OF PRODUCING A DIGITAL SIGNATURE	66
FIGURE 10. THE PROCESS OF VERIFYING A DIGITAL SIGNATURE	67
FIGURE 11. THE MAIN COMMERCIAL PROVIDERS OF TRUSTED SERVICES	78
FIGURE 12. THE HIERARCHICAL CERTIFICATION AUTHORITY STRUCTURE	82
FIGURE 13. THE CROSS CERTIFICATION CA STRUCTURE	83
FIGURE 14. STAGES IN THE RESEARCH PROJECT LIFECYCLE	90
FIGURE 15. COMPONENTS OF A SECURITY AND AUTHENTICATION INFRASTRUCTURE	94
FIGURE 16. DIGITAL CERTIFICATE LIFECYCLE	106
FIGURE 17. CERTIFICATION AUTHORITY COMMUNITY OF SUBSCRIBERS	107
FIGURE 18. GEMISIS CERTIFICATION AUTHORITY INFRASTRUCTURE	108
FIGURE 19 . CASE STUDY DATA GATHERING PROCESS	117
FIGURE 20 COMPANY D ORGANISATIONAL STRUCTURE	125
FIGURE 21 . COMPANY D'S IT DECISION MAKING HIERARCHY	126
FIGURE 22. COMPANY D'S CURRENT SALES PROCESSES	129
FIGURE 23. COMPANY D'S AUTOMATED SALES PROCESS	130
FIGURE 24. COMPANY D'S NETWORK SECURITY INFRASTRUCTURE	135
FIGURE 25 . COMPANY T'S CURRENT BUSINESS PROCESSES	140
FIGURE 26 . COMPANY T'S NETWORK AND SECURITY INFRASTRUCTURE	141
FIGURE 27 . COMPANY T'S MODIFIED BUSINESS PROCESSES	142
FIGURE 28 . UNIVERSITY X ORGANISATIONAL CHART	145
FIGURE 29 . CATEGORISATION OF DEPARTMENT Y SAMPLE	156
FIGURE 30 . DEMOGRAPHICS OF DEPARTMENT Y PARTICIPANTS	156
FIGURE 31 . ATTITUDES TO TECHNOLOGY OF DEPARTMENT Y PARTICIPANTS	157
FIGURE 32. THOUGHTS ON COMPUTERS AND TECHNOLOGY OF DEPT Y PARTICIPANTS	156
FIGURE 33. DEPARTMENT Y EXAMINATION PAPER PRODUCTION PROCESS	160
FIGURE 34 . CATEGORISATION OF DEPARTMENT Z SAMPLES	170
FIGURE 35 . DEMOGRAPHICS OF DEPARTMENT Z PARTICIPANTS	171

FIGURE 36 . ATTITUDES TO TECHNOLOGY OF DEPARTMENT Z PARTICIPANTS	172
FIGURE 37 . DEPARTMENT Z EXAMINATION PAPER PRODUCTION PROCESS	174
FIGURE 38 . LEVELS OF SATISFACTION OF DEPARTMENT Z PARTICIPANTS	175
FIGURE 39 . THE 1999 TELEPHONE SURVEY SAMPLE	193
FIGURE 40 . INTERNET UPTAKE IN THE SERVICE SECTOR	195
FIGURE 41 . INTERNET UPTAKE IN THE MANUFACTURING SECTOR	199
FIGURE 42 . INTERNET UPTAKE IN THE TRADE SECTOR	202
FIGURE 43A. USAGE PATTERNS OF THE INTERNET IN MANUFACTURING & SERVICE COMPANIES (1996/1997)	205
FIGURE 43B . USAGE PATTERNS OF THE INTERNET IN MANUFACTURING & SERVICE COMPANIES (1999)	205
FIGURE 44 . FACTORS FOR IMPLEMENTING NEW TECHNOLOGY	210
FIGURE 45 . THE PROCESS OF DEVELOPING CORPORATE COMMITMENT	211
FIGURE 46 . FACTORS FOR IMPLEMENTING NEW TECHNOLOGY	216
FIGURE 47 . NETWORK INFRASTRUCTURE AND ORGANISATIONAL LIFECYCLE	223
FIGURE 48 A. NETWORK INFRASTRUCTURE AT THE ENTREPRENEURIAL STAGE	224
FIGURE 48 B. NETWORK INFRASTRUCTURE AT THE ENTREPRENEURIAL /COLLECTIVITY STAGE	226
FIGURE 48 C. NETWORK INFRASTRUCTURE AT THE COLLECTIVITY STAGE	227
FIGURE 48 D. NETWORK INFRASTRUCTURE AT THE COLLECTIVITY/FORMALISATION STAGE	228
FIGURE 48 E. NETWORK INFRASTRUCTURE AT THE FORMALISATION/ELABORATION STAGE	230
FIGURE 49. ANATOMY OF THE DIGITAL NERVOUS SYSTEM	267

Acknowledgements

I would like to thank Entrust Technologies, the Co-operative Bank and The Manchester Metropolitan Police both of whom were kind sponsors during the course of this study.

I would also like to thank Marian for her support and time. And finally I would like to thank each and every member of my family for their support and encouragement without whom this study could never have been completed.

Declaration

I declare that no portion of the work referred to in this thesis has been submitted in support of an application for another degree or qualification at this or any other university or institute of learning.

This thesis contains material that has been accepted for publication.

1999 - Computers in Education - Computerisation of the Examination Process - A Case Study (accepted for publication) D.W.Chadwick, R.Tassabehji, A.Young

Declaration on Referencing Secondary Sources

In this PhD study when a reference is given, the text surrounding the reference is often a paraphrase of the reference and is not original material or text.

List of Abbreviations & Definitions

Authority Revocation List (ARL)	List of revoked CA certificates
Back-up keys	Copies of users' private decryption keys held securely in encrypted format by the Issuing CA for the purpose of recovery of the user's data after a disaster
CA certificate	A certificate where the certificate subject is a CA
Certificate Policy	A stated purpose of applicability of a certificate
Certificate Revocation List (CRL)	List of revoked user certificates
Certificate	Digital information securely binding an entity's name to its public key (and implicitly to the private key that matches the public key)
Certification Authority (CA)	A trusted third party that verifies its members and issues certificates to them according to the criteria laid down in its Certification Practice Statement
Certification Practice Statement (CPS)	The rules, guidelines and practices by which the issuing CA and its authorized entities will operate
Client Company	An organisation applying to the CA for membership
Company RA	A registration authority appointed by a company for its own end-users
Customer	The client company
EDI	Electronic data interchange - the transfer of structured information from one computer system to another
Encrypting key pair	The decryption private key and the encryption public key
Entrust	This refers to Entrust Technologies an entrepreneurial spin off of the Canadian corporation Northern Telecom Ltd (NORTEL), incorporated in the province of Ontario on December 20, 1996. Entrust are the developers of the software used in this study
Entrust administrator	The role required by Entrust to create, revoke and otherwise administer end-user certificates
Entrust Client	Part of Entrust software to be installed and used by end users
Entrust Manager	One part of the Entrust software used to operate the certification authority (the other parts are Entrust Server and Entrust Directory)
GEMISIS	Government Education Medical Industry Society Information Superhighway (GEMISIS) a project in association with the public and private sector as well as the University of Salford. For more detail see http://www.gemisis.co.uk
GEMISIS CA	In this project it is the issuing CA
ICE-TEL	EC IV framework research project establishing a certification hierarchy throughout Europe
ICE-TEL RA	A member of the ICE-TEL project authorised by the issuing CA to act as a registration authority
ISP	Internet Service Provider
Issuing CA	The top level CA applying and administering this CPS to itself, its subject CA's, RA's and its customers
Key	A set of 1 or more large random numbers
Master key	The key used by Entrust to encrypt CA data held on computer media
Peer Issuing CA	A top level issuing certification authority whose CPS has been approved by this issuing certification authority
Personal Security Environment (PSE)	The area where Entrust client stores all the security information. This is also known as the User's Profile
PGP	Pretty Good Privacy
Private key	A key known only to the owner
PSTN	Public Switched Telephone Network
Registration Authority (RA)	An entity authorised by the Certification Authority to perform the authentication procedures laid out in the CA's Certification Practice Statement
Revoked User	An end-user who has had his/her certificate withdrawn

Signing key pair / Signing keys	This consists of the signing private key and the verification public key
Signing private key	An entity's private key used to create a digital signature
SME	Small and Medium Sized enterprise. Companies with fewer than 250 employees and a turnover of less than £20 million (p9). This is based on the European Union definition of an SME
Subordinate CA/ Subject CA	A certification authority authorized and appointed by the issuing CA to administer and apply this CPS on its behalf
Super-user	A UNIX system administrator
TCP/IP	Transmission Control Protocol /Internet Protocol
TrueTrust Ltd.	A commercial Certification Authority contributing its time and expertise to the GEMISIS research project
UNCITRAL	United Nations Congress International Trade Regulations and Law
User certificate	A certificate where the certificate subject is a user
Verification public key	An entity's public key, made widely available as a certificate, to allow the certificate user to verify the digital signature of the entity
X.500 directory	An internationally standardised repository used to store information about users

Abstract

This study focuses on electronic data security issues and their applicability to SMEs. Prior to this project, no frame of reference had been identified or defined for:

- The electronic data and Internet security needs of SMEs
- The critical success factors for implementing and using a secure electronic data and authentication solution

Using a source of both primary and secondary research data, firstly, a trusted third party infrastructure based on public key encryption and digital certificate technology was designed and developed. This provided trust, integrity, confidentiality and non-repudiation, all of which are essential components for secure static storage or Internet transmission of electronic data.

The second stage was the implementation of this infrastructure in SMEs. The case studies revealed a reluctance to implement and use the designed infrastructure both during and after the pilot implementation period. Further primary research was undertaken to identify and explain the reluctance of SMEs to participate in piloting this Internet based technology.

As a result of this research project, there are four major contributions to knowledge.

These are,

- A time series survey of SME Internet usage and attitudes in the Greater Manchester region. The initial stage of the research found that at the start of this project (1996/7), only one in three SMEs were using the Internet and the stage of usage was extremely basic (chapter 5.2.1). Towards the end of the project (1998/9), Internet usage by SMEs had doubled and had become more sophisticated (chapter 7.2). Awareness of security needs had also risen, but was still not a part of the overall network infrastructure of the majority of small and medium sized organisations.
- A framework for the analysis of the potential success or failure of the implementation of a security solution in particular and new technology project more generally (chapter 9).

- A framework that can act as broad guide for SMEs in the development of their security network infrastructures.
- The use of organic methodology (chapter 3.3) to deal with the fast moving and changing environment of IT related research projects.

A "Best Practice" guide has been developed based on these two models to help SMEs in the implementation of a data security solution in their own organisations.

As well as raised awareness of the issues, the success factors also include re-engineering existing business processes, changing traditional business thinking and creating a level of commitment to the implementation of technology that will enable SMEs to thrive in the new markets of the 21st century.

Chapter One

Introduction

1. Introduction

" The Internet by its very nature is not a good place to conduct business or send sensitive confidential information ... there is no reasonable expectation of privacy. The environment is not composed of one connection from source to destination" I. Meyer¹

"The panic about network security isn't because the networks are more dangerous than the rest of the world but because most business people don't understand what constitutes good security" W.Rash Jnr.²

These statements encompass the premise on which this research study is based. At the time this study began, the Internet* was seen as a phenomenon, which was being well publicised but not so widely implemented by business.

The research carried out during this study focuses on this new communications and information technology phenomenon and its implementation by small and medium sized businesses. This whole subject area is governed by speed - not only speed of receiving and transmitting information, but also rapidly changing environments, further development and application of innovative technology. Product lifecycles in the IT sector are becoming shorter as competition develops faster ways of introducing new products and component costs fall. Product lifecycles now typically range from 3 to 18 months, by which time they are at least modified and at most obsolete[†].

During the course of this study, the focus has had to adapt to this changing environment and has involved an organic learning process where issues and ideas have been developed, restructured, reorganised and built upon using a variety of methodologies and materials.

* See Chapter 2 Section 3 for a full definition

† For example, since 1996 Microsoft have introduced around four versions of their Windows operating system, where each version integrates Internet facilities and handles information more effectively, than the previous version. Similarly, Intel the computer component manufacturer, has introduced 14 versions of their Pentium III processor in the 8 months since February 1999, each version more powerful than the previous one.

This chapter will lay the foundations of the study. It will introduce the main topic area, focus on the relevant issues, pose the research questions, identify the study's assumptions and limitations and finally outline the structure of the remainder of the thesis.

1.1 Background to the Research Topic

The research study is made up of several areas, which include the Internet, electronic mail, authentication, data security, small and medium sized businesses, implementation of new technology and organisational network infrastructures. The following section will briefly discuss the importance of the general topic area of communications and information technology and the research area of the Internet and, more specifically security.

1.1.1 The Importance of Technology

The importance of technological innovation as the catalyst to economic re-generation and growth has been recognised by many academics, economists and business writers, ranging from Kondratieff to Michael Porter[‡]. Major innovations in technology and its application to industry, have been the instigators of re-generation through the stages from recovery, growth, recession, and depression of economic cycles over the centuries. An empirical base of innovation theory has been set in the context of historical ages, where clusters of basic innovations took place and generated completely new sectors across the last century. The most prominent technological innovations for the end of the 20th century and the beginning of the 21st century relate to telecommunications and information technology in general and the Internet in particular. For many industries, information technology (IT) is now becoming inextricably linked into elements of the value chain³, competitive strategy⁴ and a means of developing longer-term competitive advantage⁵. A survey of over 200 US businesses⁶ in 1996, found that a direct relationship exists between companies that are technologically based and invest in IT and a company's size and market position.

[‡] See Appendix I for paper presented at Business and Economics Society International Rome 7/98 - Using the Information Superhighway to Drive Economic Regeneration

Thus, the more willing a company is to increase IT investment, the more likely it is to be larger and have the infrastructure to be able to invest to sustain a competitive advantage in the long run. It is this innovation in technology, which is driving socio-economic growth and development into the 21st century and it is for this reason that it is crucial that technology, the Internet and its applications are explored and understood.

1.1.2 The Importance of the Internet

The Internet is a cost effective medium for transmitting electronic data globally. In 1996, the Internet was a relatively new phenomenon little known in the UK, with little proliferation in the commercial sector - particularly for the small and medium sized enterprise (SME). Many commentators predicted the Internet would increasingly become the most dominant medium of future business.

"Open networking seems as fundamental to civilisation's needs in the first half to the 21st century as open roads did in the first half of the 20th." ⁷

"It will take 2 years for the Internet to become stable so there will be an evolution from virtual private networks to linked intranets then to the Internet. Today only 2% use electronic transactions, but this will grow to 80%. The web will challenge who we are and what we do, forcing us to adopt new business models." ⁸

Thus, there is a great need for understanding the Internet and the issues surrounding it, ranging from its technical infrastructure through to the facilities and services that are enabled by the Internet. The importance of the Internet and its impact socially, economically and commercially has also been recognised by the international community.

Research about the Internet and how it is adapted to benefit a myriad of users, has commanded large research grants from the European Union⁹ in their series of technology framework funding programmes which first started in 1984 and is now in

its fifth cycle spanning the period 1998-2002. A whole suite of research projects on the topic of the Internet and related issues, of which this research study is a part, is the multi-million pound GEMISIS[‡] project.

1.1.3 The Importance of Internet Security

Commercial transactions carried out over the Internet (Electronic commerce or e-commerce) are increasing at a very rapid rate. By the turn of the century, commercial transactions on the Internet are expected to total hundreds of billions of dollars a year¹⁰. This level of activity could not be supported without a security infrastructure. These levels of security, though not widely used in 1996, give the means to strengthen the foundation with which electronic commerce can grow.

Not only this, but electronic mail** (e-mail) is also increasingly being used to conduct personal and business matters on a daily basis. E-mail has no physical form and may exist electronically in more than one place at a time. This poses a potential problem as it increases the opportunity for an eavesdropper to access the transmission. Thus security is needed to protect e-mail by rendering it difficult to read by any unauthorised individual. Unauthorised intrusions and tampering of electronic data and networks is increasing as the Internet's usage proliferates. In a survey of 2,200 Internet hosts¹¹ in 1996, Farmer found that over 65% were vulnerable to the kind of remote attacks that are widely known to unauthorised intruders. The sites targeted in the survey were mainly credit unions, banks, government sites and other servers that should have unbreachable security. The value of this survey is that it tested the networks directly and did not involve the questioning of people who (with an interest to protect) often withhold information in order to maintain confidence in their organisations.

[‡] Government Education Medical Industry Society Information Superhighway (GEMISIS) a project in association with the public and private sector as well as the University of Salford. For more detail see <http://www.gemisis.co.uk> and appendix II

** See Chapter 2 section 3

Another survey¹², where intrusions were actually reported, found that in 1997, 48% of respondents admitted a security breach had occurred. In 1998, this had risen to 64% indicating the increasing rise in security breaches. Of all respondents, 54% percent indicated that the Internet was the point of entry for the intruders. Once intruders have gained access to the electronic data stored, they either tamper with it, or "steal it". A number of well-publicised credit card data security breaches have been reported¹³. Despite assurance that credit card details and personal data is safe, in fact this highly valuable data is often stored on databases that can be accessed by the Internet. An example of this is the 1997 StarWave case¹⁴. This company hosts many commercial sites and is responsible for protecting the credit card data of their customers. Crackers^{††} captured and distributed credit card numbers of users with an added message stating that StarWave had the worst security they had come across. In a similar case, Salgado¹⁵ installed a program that captured over 100,000 users' names, passwords and credit card details. Many other publicised attacks have also occurred in the case of Levi-Strauss and VISA themselves. An anonymous hacker^{‡‡} admits that any site can be cracked and that:

*"As we move near the 21st century, new and more effective cracking methods will surface. These will be used by hostile foreign nations seeking to destroy our national information infrastructure"*¹⁶

In the recent Nato war with the Yugoslav Republic in Kosovo, this is exactly what happened. Serbian supporters hacked into some UK, NATO and US government sites¹⁷. There was also a flood of e-mails to government and military Internet addresses, which clogged up the bandwidth of the networks causing serious disruption and delays in the sending and receiving of important messages.

^{††} A cracker is one who breaks-and-enters a computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Hackers generally deplore cracking. www.whatis.com

^{‡‡} Hacker is a term used by some to mean "a clever programmer" and by others, especially journalists or their editors, to mean "someone who tries to break into computer systems." www.whatis.com

"some hackers in Belgrade who have hacked into our website and caused line saturation of the server by using 'ping' bombardment strategy, ... stifling Nato's propaganda efforts, Net users opposed to the bombing have also been infiltrating and clogging the defence alliance's computer system."

"It has also been saturated by one individual who is currently sending... 2,000 e-mails a day and we are dealing with macro viruses from Yugoslavia into our e-mail system"¹⁷

1.1.4 The Importance of Small and Medium-sized Enterprises

Over 90% of business entities in the UK's economy are made up of SMEs. The North West has the third highest proportion of SMEs of any region in the UK¹⁸.

SMALL BUSINESSES PER MILLION PEOPLE BY UK REGION	
REGION	SMEs Per million people
ENGLAND & WALES	3,129
London	4,852
South East	3,414
North West	3,242
Eastern	3,144
West Midlands	3,141
East Midlands	3,024
Yorkshire	2,854
Merseyside	2,590
South West	2,484
Wales	1,990
North East	1,390
<i>Trends Business Research © Last Updated on 28/01/99</i>	

Table 1. The Number of Small Businesses in the UK

SMEs do not have the financial or human resources to research or develop technological solutions, which requires a high degree of specialist knowledge and corporate commitment. However, Keegan¹⁹ sees the Internet as a means of shifting the balance of economic power back from multi-national corporations to "everybody". He feels the Internet has a "socialist egalitarian quality" developing its own economy. He cites Microsoft being forced by Netscape to give away free products, as an example of the way in which the economic environment of the 1990's is changing.

Thus, information gathered from this research project can be formulated into implementable and cost-effective solutions for SMEs directly or indirectly. This will encourage SME use of the Internet, helping them to grow and develop their businesses and equalise the balance between the larger and multi-national corporations who have the competitive advantage because of their size.

In this new and innovative environment, successful companies wanting to maintain a competitive advantage must find a completely new business model to incorporate the new technology, not merely to extend their current business onto the Web. It is this implementation and integration process that is the focus of this study.

1.2 Aims & Objectives

The overall objective of this study is to develop a security solution that will facilitate increased competitiveness and confident and trusted participation in global trade for SMEs, by exploiting the opportunities offered by the Internet. If the Internet is to be used by businesses as an alternative medium to paper, the issues of trust, integrity, confidentiality and non-repudiation of the originator's electronic data, both in static and transmitted formats, have to be addressed and are addressed in this study.

From these broad objectives, the more specific aims and objectives of this research, initially were to provide a solution for small and medium sized enterprises (SMEs), to use the Internet for secure and authenticated electronic communications. The technological means of providing the security and authentication - namely digital signatures and encryption based infrastructures - were already available. What was required was to develop a whole security solution based on the existing technology for implementation in small and medium sized businesses. At the outset, the project criteria were pre-set according to the assumptions and limitations laid out in the next section. The initial research questions are summarised in table 2.

AIMS & OBJECTIVES	INITIAL RESEARCH QUESTIONS
Contribute to the development of a secure and authenticated infrastructure for the exchange of information over the Internet for the benefit of SMEs.	<p>Can a security and authentication infrastructure be developed to provide SMEs with trust, integrity, confidentiality and non-repudiation when using the Internet for transmitting electronic data?</p> <p>Does the security solution developed actually work when used by SMEs?</p>
Identify whether the implementation of this security solution enables small and medium-sized enterprises to carry out their business operations/management more effectively and more profitably.	What benefits are achieved for SMEs by secure use of the Internet?
Study how the security solution is implemented by SMEs and how the new infrastructure is integrated into current business practices, processes and procedures.	What is the process of implementation of the security solution by SMEs?
Based on the observations made, produce a "Best Practice" guide for SMEs.	What is the contribution to knowledge of this research project?

Table 2. Project Aims & Objectives Formulated into Research Questions

This is an area of research that was very new and little empirical work had been carried out with SME's in the UK in 1996. Early on in the project, new research questions emerged (summarised in Table 3) as it became apparent that SMEs were reluctant to take part in the research project piloting the security solution.

NEW AIMS AND OBJECTIVES	NEW RESEARCH QUESTIONS
Understand and clarify the reluctance of SMEs to join the research project.	What is the pattern and level of Internet usage by SMEs?
	What are the attitudes to and how are the Internet and security issues perceived by SMEs?
	Was the security solution designed a viable service for use by business?

Table 3. New Research Questions

1.3 Assumptions and Limitations

The development of new technology in the form of software or hardware is beyond the financial and academic scope of this project. Instead commercially available technology will be used, to develop an authentication and security infrastructure for SME use of the Internet. Although based on technology, this project is concerned with identifying the process of implementation, integration into existing business processes and benefits to SMEs of a secure authentication infrastructure.

The assumptions of this research project are that SMEs are not using the Internet to its full potential and are thus not benefiting from it. There is also an assumption that SMEs want to implement and use new technology in their organisations and would be willing to participate in such a research project. These assumptions had to be revised when it was found that few companies were prepared to participate in the project. This led to new research questions being posed and a modification of the methodology, which underlines the organic learning process during the course of this study. Other assumptions are that SMEs are relatively homogenous in behaviour and thus observations made from a selection of case studies, would be representative to the extent that producing a good practice guide could benefit the majority of SMEs.

There are a number of limitations, which must be taken into account relating both to the research methodology and the environment of new technology. Firstly, the criteria for selection of organisations as case study candidates are that they would be:

- Small/Medium sized companies with fewer than 250 employees and a turnover of less than £20 million
- In the objective II areas drawn up the European Union. The objective II areas are designated areas in the respective European Union member states, which need regeneration and qualify for ERDF funding. Such areas in the North West of the UK, include Manchester, Salford and Liverpool. (appendix 3)
- Set up for Internet access and e-mail facilities

Not only this, but there was limited funding which impacts on the accessibility of technology and the degree of support to organisations.

A number of factors confined the impact of these limitations. The structure of the GEMISIS project included partners such as the Manchester Chamber of Commerce and Manchester TEC, providing support for the recruitment of and co-ordination with SMEs. The criteria limiting the selection of project participants was not particularly negative, since:

- SMEs make up a high proportion of the UK economy as already discussed
- EU designated Objective II Areas are mainly urban industrial areas with a high proportion of business
- Funding is a criterion, which is faced by many commercial and social organisations. It represents real life situations - no academic research or business project is ever conducted without this funding limitation.

However, one of the greatest limitations of the study mainly relates to the fast changing nature of the IT environment, where trends and technological developments and social/business applications of it can affect the relevance of findings. Thus, this research can only be said to be true for the point in time at which the research was undertaken.

1.4 Organisation of the Remainder of this Study

This study spans three years of an environment in which there are large changes in technological innovation and trends. This study is organised in a way that incorporates these changes, ensuring that the primary research carried out is always placed in the context of this changing environment.

In chapter 2, the initial literature review surveys the types of research studies that had been carried out by other groups and describes the project's macro-environment as it stood at the beginning of this study in the period 1996-1997. At this stage it is important to place the study in its historical context since the technology, usage of and

attitudes to the Internet, e-mail and security at that time had an impact on the design and development of the security solution and its implementation by SMEs in this study.

Chapter 3 identifies and explains the types of methodology used, including advantages and disadvantages, in each stage of answering the research questions posed.

The stages in the development of the security solution are covered in Chapters 4 and 5. A literature review of the theories and practices of data security and authentication, security services and technology available in 1996-97, yields the conclusion that the solution being designed and developed should be based on public key encryption and digital certification technology provided by a trusted third party certification authority. Chapter 5 describes the process of evaluating commercially available security software, identification and evaluation of practices and procedures of existing security service providers. Finally, a trusted third party certification authority service is developed, incorporating the technology to deliver public key encryption and digital certification; an administrative infrastructure to support all stages of the public key lifecycle and its management; development of a user training framework; production and publication of the operational and management processes, procedures and practice by which the service is governed.

Case studies tracking the implementation and usage of the security solution in SMEs are documented in Chapter 6. This chapter documents the methodology and findings and briefly discusses the outcome. A fuller discussion of these results is included in the final chapters of this study where a thesis is synthesised drawing on all the strands of research carried out.

Chapters 7 and 8 report the findings of the further research undertaken to clarify the results of the case studies and understand the IT infrastructures Internet usage patterns and attitudes to security in SMEs.

The primary and secondary research findings are analysed and synthesised in chapters 9 and 10. A theoretical framework based on the various findings in this research project are developed and presented. A best practice guide for SMEs is summarised in Chapter 11.

The research project is concluded in Chapter 12 by summarising the findings, discussing the limitations, making recommendations and suggesting areas for further research.

Finally, Chapter 13 is an epilogue placing the findings of the research project in the macro-environment context of the commercial, legal, technological, government and social infrastructure in 1999. This chapter confirms the use of the Internet is still growing in both the commercial and social sectors, that the technology is still developing and that governments are developing a legal and socio-economic infrastructure to support the use of the Internet by all types of users.

Chapter Two

Literature Review - The Macro-environment

2. Literature Review - The Macro-environment

Information technology is of prime importance to the future socio-economic development and growth of a nation. However, the technology is not the only factor in the development of an information infrastructure founded on innovative new technology and its application in commerce and society. The macro-environment in which this research project is set, is extremely broad and has been divided into three main areas which have a direct or indirect impact on this research topic area. These are:

- The role of government
- The developing legal infrastructure
- The technology and its application

This chapter surveys the research studies, methodologies, technology and patterns of implementation as they stood in 1996-1997 and is the foundation for the initial design and development of this research project.

The role of government and the developing legal infrastructure was crucial both to this research project itself and as the context in which the research project is set. Had government introduced legislation to outlaw the use of encryption in the UK, or if certification authorities required government issued licenses then this research project would have been terminated or been seriously delayed. Similarly if digital signatures and electronic documentation are not and do not intend to be recognised in law and commerce in the future, then the business application of the security solution being produced would have a limited impact.

The following sections will discuss each of the main areas identifying the core research areas already undertaken by 1997 and conclude with a brief description of how these areas impact on the requirements of this study.

2.1 The Role of Government

In a report by the Information Society²⁰ they site the government as having a crucial role in the development of the Information Society. Government's basic role is identified as protecting the economy by ensuring the development of an appropriate information infrastructure to support future economic growth and national competitive advantage. Government also has a role both as a user as well as a promoter.

The report identifies the government²⁰ is the single largest user of information and a major purchaser of Information Society equipment software and services. As such they use IT to promote efficiency and effectiveness of government processes and services thus developing a best practice model and exemplar to business. As a promoter, the report²⁰ indicates that government is also a:

- Role model and exemplar to businesses
- Regulator of key Information and Communication Technology industries to promote competition
- Facilitator for specific initiatives - stimulating the uptake of information technology
- Creator of the appropriate legislative and administrative environments to facilitate the development of the appropriate environments

All of this involvement by government will support and stimulate the evolution of the Information Society. The European Commission (EC) has adopted the term Information Society to emphasise the fact that the applications and development of an information infrastructure will have a significant social and economic impact. The information society is identified in the report²⁰ as being made up of 3 often converging and integrated areas,

- **The Telecommunications Industry - Public Switch Telephone Network (PSTN), Cable Networks, Satellite Networks, Broadcasting, Mobile Networks, Online Multimedia, Interactive Multimedia and Multimedia Network Equipment**

- **The IT Industry** - computers, software, interfaces, services, interactive multimedia, multimedia network equipment and offline multimedia
- **Information/Content Industry** - databases, information services, audio-visual products, films, music, photos, offline multimedia, online multimedia and interactive multimedia

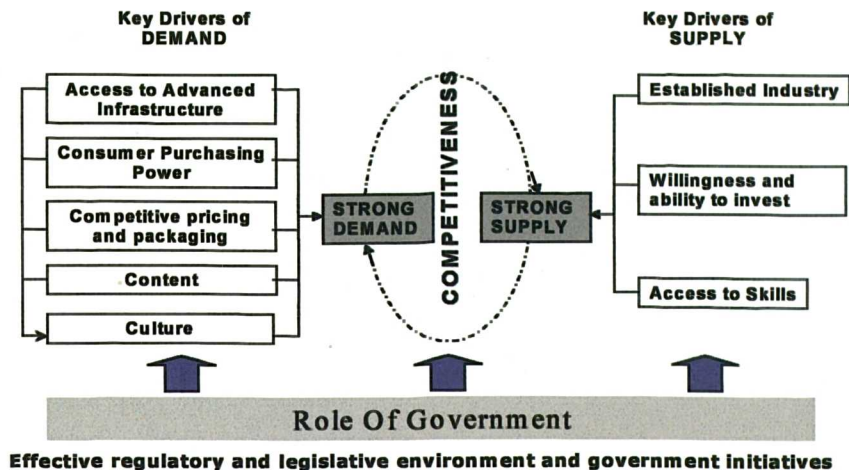
The impact of the integration of these three areas implies availability to access immense quantities of information and entertainment on demand, to interact with and manipulate large quantities of data, to transact and communicate from any location. This ultimately is believed in the report²⁰ to have an impact on a nation's competitiveness which it lists as:

- The effective use of the products and services of the Information Society improving and changing business processes, increasing productivity and efficiency. This also has an impact on the role of government
- The adoption of the tools of the Information Society by the consumer market, which will eventually stimulate uptake in the business market.
- The Information Society becoming one of the fastest growth areas in the developed world over the next 5 years, potentially stimulating the growth of indigenous industries.

The most important demand drivers to the uptake of the Information Society are illustrated in Figure 1 and are listed in the report²⁰ as being:

- Sufficient income among consumers and businesses to purchase the goods and services of the Information Society
- Access to appropriate information and content. The presence of local content can play a major role in stimulating uptake of certain services.
- Access to an infrastructure and other technology
- Competitive Pricing and packaging will affect the speed of adoption and the uptake of new services
- A Culture which supports the various components of the Information society, namely a willingness and tradition of investment in innovation, a strong culture of education and learning, collaboration with academia and business

Enablers of the Information Society



Source: The Information Society Report²⁰

Figure 1. Enablers of the Information Society²⁰

The process for enabling an Information Society is to ensure that a commercial and industrial infrastructure that can support the new technology and the presence of the appropriate skills in society are in place. The impact of government can be seen in figure 1 as underpinning the major drivers of the Information Society. It underlines the importance of government's role in the IT environment in general and in this research project in particular. The fact that this research is part of the European Union sponsored GEMISIS project exploring the applications and development of new information technology for the exploitation by business, illustrates that Government is already beginning to play a role. The macro-economic factors identified in figure 1, together will create a stimulus for the development of an IT based micro-environment at the firm level, which will ultimately drive competitive advantage and economic regeneration and growth. Adversely had government legislation prevented the use of the technology in this project, this would have limited the exploration in and use of IT infrastructures for the development of an Information Society.

The next section will look at the impact of government in terms of the legislation and initiatives introduced to support or hinder the growth of electronic commerce and the use of the Internet for commercial benefit to organisations. This project concentrates on the micro-environment, where the application of information technology at the level of the firm is examined in detail.

2.2 The Developing Legal Infrastructure

The legal issues inherent in the use of the new media at the beginning of this research project were still not fully understood and were far from being adopted and implemented into statutes and policies. The role of national governments in the digital era had yet to be determined. In 1997, the environment of the Internet was one where electronic crime was untraceable, market regulation was inconsequential, intellectual property rights were abused and consumers had no protection or redress. With the increase of global electronic commerce, traditional tax revenues could be eroded. Guarantees of financial payments could be worthless. Societies could become dangerously unbalanced. Unskilled workers and poorer nations could become isolated. Governments believed that traditional instruments and measures of control and regulation - such as tariffs, taxation, consumer protection, guarantees of monetary payment, commercial safeguards - were relevant in the electronic arena of the Internet. As has already been identified, the role of government in developing a macro-environment for the successful creation of an Information Society is crucial. Thus government intervention and regulation is necessary and must focus on three major areas listed by Doyle²¹ as being,

- Networks - the Internet was actually born from government agencies, there is a need for governments to become more involved in developing the network infrastructure either by subsidies and/or socio-economic policy.
- Electronic money - Governments currently play a large part in monetary control, regulation and developing national and international financial infrastructures. Governments must also take a similar role in regulating the issuing, security and control of digital money rather than relying on market mechanisms.
- People - ensuring the security of citizens and their property. There is a particular need for this in the lawless environment of the Internet to protect against fraud and other attacks.

2.2.1 Internet Law

In 1997, law relating to the Internet was still in the embryonic stages of development. In order to protect the future development of the Internet as a medium fit for socio-economic use, there was a need to look at the regulation of cyberspace. There was a common belief amongst users that the Internet is a law-free zone or at most subject to a vague ill-defined global or international law of cyberspace developed from common practice and "netiquette" (acceptable standards of behaviour by Internet users). No such international law had yet emerged, nor was there any body or court which had the authority or jurisdiction to create, interpret or implement Internet law. The Internet was a trans-national phenomenon, which was not contained by any national political or jurisdictional boundaries.

There were three main areas Edwards and Waelde²² believed to be particularly pertinent to developing Internet law.

- **Intellectual property and the Internet** - the problems of whether establishing a hyper-link to another web page constituted an infringement of copyright; or whether merely reading a web page involved illegal copying; or whether ISPs could be held responsible for unknowingly hosting pirated materials; or the issue of "cyber-squatters" who obtained domain names holding them to ransom from the legitimate trademark holders.
- **Electronic commerce** - If goods or services were bought and sold across national boundaries via the Internet how could they be taxed? Which laws were applicable in contracts exchanged between 2 countries over the Internet. Some projects had already been set up to address these problems. One such example was the Bolero System²³, showing that electronic messages can replicate the functions of existing international trade documentation establishing a multilateral contract based on a strong legal framework.
- **Liability for content made available via the Internet** - this included defamation, libel and data protection issues. One problem was the concept of "cookies". These pieces of computer code were generated by a web server and stored on the user's computer for future access. They collected user-specific information and re-transmitted it to the web server for later access. Legally,

this was in breach of the EU data protection directive, since neither consent or knowledge of the transfer of user information is sought or given²⁴. There was also a series of issues surrounding e-mail, ranging from defamation to harassment²⁵.

The implications of electronic evidence and procedure in each area also had to be addressed. Increasingly as test cases build up, so the rules and regulations, which govern the information travelling across the Internet, will also be built up. Many acknowledge that although at the moment the law is difficult to apply, the awareness of users on the various issues from personal privacy to copyright issues must be raised. In order to raise awareness and alleviate the immediate problem of lack of Internet regulation and law, companies can contribute by developing their own Internet and e-mail policies and guidelines (Appendix 19).

Government bodies and International organisations were attempting to develop an infrastructure to bring the Internet under the jurisdiction of International and national trade law and practice. For example, the rules for taxing transactions based on the Internet are nearing agreement by the OECD, but establishing the detail and enforcing them are going to be difficult²⁶. The OECD agreed (1998) a draft policy on the taxation of electronic commerce. They ruled out a flat-rate "bit-tax" on all Internet deals, supporting the continuation of traditional tax principles of indirect taxes being levied on the basis of where the goods or services are consumed, not where they are produced - a definition of this has yet to be established. On data protection, the EU is at loggerheads with the US view that there should be minimal controls on transmittal of personal information. The EU directive currently bans the export of personal data from the EU to any other country that does not have similar data protection laws. The US believes that the Internet should rely on voluntary codes of conduct and self-regulation rather than new laws imposed by governments, and is in direct opposition to the EU's statutory approach. A pledge at the meeting to review the subject within 2 years was given by both parties.

The United Nations Congress International Trade Regulations And Law (UNCITRAL), produced a Model Law on Electronic Commerce²⁷ in 1996 modified in 1998. This was based on the realisation that there was a need to recognise in law, computer records, electronic data transactions, EDI and other means of

communication, which involved the use of alternatives to paper based methods of communication and storage of information. This Model Law was intended to be used by governments as a blue print for facilitating and unifying, the use of electronic commerce between nations with different legal, social and economic systems. UNCITRAL suggested that this law needed to be implemented by governments in order²⁷:

- (1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves;
- (2) to help the parties be aware of the consequences of their entering into a contract;
- (3) to provide that a document would be legible by all;
- (4) to provide that a document would remain unaltered over time and provide a permanent record of a transaction;
- (5) to allow for the reproduction of a document so that each party would hold a copy of the same data;
- (6) to allow for the authentication of data by means of a signature;
- (7) to provide that a document would be in a form acceptable to public authorities and courts;
- (8) to finalise the intent of the author of the "writing" and provide a record of that intent;
- (9) to allow for the easy storage of data in a tangible form;
- (10) to facilitate control and subsequent audit for accounting, tax or regulatory purposes; and
- (11) to bring legal rights and obligations into existence in those cases where a "writing" was required for validity purposes.

In 1997, no government policy had been drafted incorporating any of these issues, which meant that potentially any legislation introduced might have an impact on the implementation of the security technology in SMEs, the legality of this research and the way it was conducted. For instance, the use of high strength encryption software could have been outlawed, which would have ended the project. If certification authorities had to be licensed by government, it would have taken time and money to obtain a licence, which again would have either ended the project or delayed it beyond the funding period.

2.3 The Technology and its Application

This section is divided into three main areas covering:

- The Internet
- E-mail
- Security

For each of these, a definition of the technology is made followed by a survey of the different studies, identifying the core research areas already undertaken, concluding with a brief description of how these areas impact on the requirements of this study.

2.3.1 The Internet

The Internet sometimes called "**the Net**" or "**Information Superhighway**" is a worldwide network of computer networks. The Internet grew out of the conception of the US military's **ARPANET*** developed to help counter the Soviet launch of the Sputnik satellite space initiative in the late 1950's. The early **ARPANET** consisted primarily of research universities and military contractors with computers linked by telephone lines leased from **AT&T**†. Thereafter, the growth of this infrastructure into the Internet was through a myriad of government-sponsored initiatives and projects²⁸. Today, the Internet is a public, co-operative, and self-sustaining facility accessible to hundreds of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, the Internet uses a set of protocols called **TCP/IP** (Transmission Control Protocol/Internet Protocol). **TCP/IP** is the basic two-layered program communication language or protocol of the Internet. The higher layer, **Transmission Control Protocol**, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a **TCP** layer that reassembles the packets into the original message. The lower layer, **Internet Protocol**, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network

* Advanced Research Projects Agency Network of the US Department of Defence in the 1960's

† An American telecommunications company

checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they will finally be reassembled at the destination. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. Even higher layer application protocols that use TCP/IP to get to the Internet include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP).

The most widely used part of the Internet is the World Wide Web ("WWW" or "the Web"). Its outstanding feature is hypertext, a method of instant cross-referencing of information. A Web browser is used to access pages of information, the most popular of which are Netscape Navigator and Microsoft Internet Explorer.

Two adaptations of Internet technology, the intranet and the extranet, also make use of the TCP/IP protocol. An extranet is a private network that uses the Internet protocols and the public telecommunication system to share securely part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet requires security and privacy such as firewall[§] server management, the issuance and use of digital certificates or similar means of user authentication and encryption of messages. An intranet is a network of networks that is contained within an enterprise. It may consist of many inter-linked local area networks and also use leased lines in the wide area network. The main purpose of an intranet is to share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and for tele-conferences. An intranet uses TCP/IP, HTTP, and other Internet protocols and in general looks like a private version of the Internet. An intranet may also include connections through one or more gateway computer to the outside Internet. Typically, larger enterprises allow users within their intranet to access the public Internet through protected firewalled servers that have the ability to screen messages in both directions so that company security is maintained.

[§] See Chapter 2.3 and Appendix 4 for more details.

2.3.1.1 Attitudes and Usage

In July 1995, the predictions about the growth of the Internet were expressed as a phenomenon, which was likely to become so ubiquitous that it is woven into every day life. The Internet would transport not only data, but telephone calls, television and "everything else" merely by plugging in.

At this stage, only around 100,000 businesses around the globe were connected to the Internet. By 1996, the rate of growth of the Internet was exponential, with the Internet having more than 19.5 million hosts (server computers) and growing by 52% per annum²⁹. In November 1996, the predictions that the Internet would grow so big and become such an integral part of everyday life that nobody would notice it any longer, continued. By the end of 1996, the Internet was:

" in the early stages of segmentation where ... 70% are using the net for business and personal use combined [they] see the Internet as a productivity tool to find out information about their customers, competitors and for talking to others and to do their business better"³⁰

It was estimated that British firms were joining the Internet at a rate of 20 a day, but the trend was that senior managers were monopolising the training that came with the installation of the Internet at the expense of workers lower down the hierarchy³¹. At this time, it was mainly the larger corporations who were taking advantage of the Internet. In an EU report³², it was recognised that within the European Union itself, there were more than 16 million SMEs representing 99.8% of all companies, providing 65% of business turnover, 40% of exports and 66% of total employment. According to the Department of Trade and Industry³³ in the UK, small companies with less than 100 employees provide over 50% of all the UK's non-government employment and contribute nearly 50% of output. But in 1996, only 4% of SMEs (companies with fewer than 250 employees) in Europe had Internet access and they were consequently losing out on opportunities and competitiveness to companies around the world, mainly in the US and Japan. Overall, the attitude towards the Internet was more positive in the US than the UK. This was mainly because the UK and the rest of Western Europe lagged behind the US in the physical proliferation of

computers and a prevalent IT culture. The European average per capita IT spend³⁴, was \$276 compared to \$542 in the US. The European average number of PCs per white-collar worker was 76 per 100 compared to 104 per 100 in the US. There was also a negative portrayal of the Internet in the UK media, where the popular press had tended to concentrate on the seamier side of the Internet - the ease of finding and downloading pornographic material³⁵.

The advantages of the Internet were seen largely in marketing terms³⁶. The Internet was the great leveller, "*where nobody knows how big or small you are*"³⁷. Once a company is on the Internet it becomes a multi-national organisation with access to global markets and direct contact with customers worldwide. Early involvement in the Internet was seen as a low cost, low risk strategy, which could give many organisations an edge over their competitors who lacked the foresight or curiosity to use the Internet to their advantage. The world's first Internet bank, Security First National Bank reported overhead costs of less than 1% compared to 3.5% for traditional banks. Similarly, the processing cost of a traditional airline ticket was £5 compared to £0.62p when customers booked their airline ticket over the Internet³⁸.

As Dellecave in the Sloane Management Review observed, "*It is not too difficult for smaller businesses to outperform larger ones*"³⁷. This also applied to start up businesses. Another advantage of connectivity was seen to be in times of recession, the technologically enabled would already have processes in place, making them better able to deal with recession without too much financial outlay to the organisation³⁹.

With the Internet also came the means of overcoming incompatibilities between legacy systems⁴⁰, which could be combined and re-used to provide a new level of customer value and service. Processing engines such as integration hubs^{**}, which could be located anywhere, were developed and would process and distribute information from and to anywhere. Organisations would be able to link incompatible systems together and provide a consistent processing environment and way of

^{**} A collection of one or more application servers that can process information from many disparate data sources and present it in web form to a client/server application or as a fax or e-mail or letter

distributing the consolidated information. This web technology in the form of the integration hub enabled those organisations to exploit their existing investment in IT systems and offer new business functionality with minimum investment.

Other advantages of the Internet were that it provided global reach, another feature allowing head-to-head competition with larger firms. By removing the obstacles of time zones, geography and location, this removes barriers to communication with customers and employees, creating a “*frictionless business environment*”⁴¹. Thus, value was gained from the Internet, providing a means for people to interact with each other instantaneously and at their convenience.

Despite these benefits, Spar and Bussgang⁴² among others, identified a number of drawbacks which they felt would hinder the development and growth of the Internet as an integrated business tool unless they were addressed. They included,

- physical limitations of cable bandwidth for transferring data
- trade regulations
- the role of government in overcoming export controls, copyright laws and industry standard regulations
- a clear definition of property rights
- safe and useful means of exchange
- a way to locate and punish violators of on-line rules

Not only this, but also human resource issues linked with the Internet would also have to be resolved for example those listed by Sunoo⁴³ :

- establishing fair guidelines
- finding new ways of measuring work processes.
- setting up policies and procedures for outlining terms and definitions to prevent lawsuits (for example through downloading illegal material, or sexual harassment by e-mail)

There were also grave social implications being voiced. Although the Internet facilitated high speed processing, disseminated information to a wide audience and allowed a large number of people to interact instantly in different geographical locations, there was also a risk of "*distortion, manipulation and misinformation*",⁴⁴ which had to be weighed against these benefits. There was also the fear of IT knowledge being a socially dividing factor. A MORI survey of over 1,000 people, commissioned by Motorola⁴⁵, revealed that nearly half of adults felt they were being left behind on IT skills as the nation divides into "haves" and "have nots". Just over one in five adults said they had used the Internet but half of them were not doing so regularly.

Of those that were using the Internet in the UK⁴⁶ in 1996, the most common complaints were the slow speed of access and information download and also the difficulty of finding relevant information. Improving security was only mentioned by 9% of respondents indicating the lack of awareness and perception of security needs.

Respondents Views of Potential Improvements to the Internet	%*
Speed up access and downloading information	47
Make it easier to find information	28
Improve ease and success of accessing	12
Improve security of transmitting information	9
Make it more user-friendly	9
More censorship (e.g pornographic material)	8
Make it cheaper	8
Improve visual display	7
Exclude and reduce junk mail	4
Increase Bandwidth	4
Keep it free from control and censorship	2
No improvements necessary	7
*Base 100. Respondents were asked what improvements they would like to see	
Source: Continental Research⁴⁷	

Table 4 . Potential Improvement to the Internet

Business use of the Internet in 1996⁴⁸, focused mainly on e-mail, with over 85% using it for that purpose. About 80% were using the Internet to access online information sources, while 65% were using it as a means of providing customer and technical support and file transfer services.

By 1997, the idea of using the Internet as a means of buying goods was beginning to emerge. However, for the Internet to become a truly useful tool for businesses, many felt that it needed to be controlled, secure and restricted. Whereas the majority of companies were using Web sites primarily for marketing (especially in the US), in 1997, net-based purchasing was still a tiny proportion of world trade, but it was becoming more prominent in the IT plans of major corporations. There were some dissenting voices such as Citicorp who denounce Internet trading as unsafe after its rival Citibank lost millions of dollars to a Russian hacker⁴⁹. The Internet was becoming a substitute for a range of communications, one of which was Electronic Data Interchange (EDI)^{††}. Whereas bespoke EDI systems were a luxury enjoyed by the largest trading partners, only 17,000 out of the 20 million businesses in the UK used it. By 1997, the Internet had facilitated the instant access to automated ordering and payment systems by smaller suppliers with limited IT use. The supermarket chains, such as Tesco and Asda, began piloting a more informal type of EDI over the Internet for their smaller suppliers to increase efficiency and speed of the whole supply chain processes⁵⁰. Total revenues from on-line sales in Europe in 1997, were around \$1.2 billion estimated to rise to \$64.4 billion by 2001⁵¹ by when the majority of revenue was expected to be driven by business-to-business commerce, with Germany and the UK alone generating nearly half of all the on-line revenue in Western Europe.

^{††} EDI (Electronic Data Interchange) is a standard format for exchanging business data. More detail is given in Appendix 5.

2.3.2 Electronic Mail

Electronic mail (e-mail)⁵² was one of the first uses of the Internet and is still one of its most heavily used features, constituting a large proportion of total Internet traffic. E-mail is the exchange of electronic messages by telecommunications, from and to any party who is connected to the Internet or connected to a public or private computer network that has a connection to the Internet. E-mail messages are usually encoded in ASCII[‡] text. Non-text files, such as graphics, video, executable and sound files, can be sent as attachments. These attachments are sent in binary format[§] by being encoded into one of a variety of encoding schemes - of the most popular ones are MIME^{***} and uuencode. The recipient decodes the file with the same scheme that was used to encode the file. This encoding and decoding scheme is usually embedded in the e-mail software with the whole process being done automatically. E-mail uses one of the protocols included with the TCP/IP suite of protocols. A popular protocol for sending e-mail is SMTP^{††} and a popular protocol for receiving it is POP3^{‡‡}. Both Netscape and Microsoft include an e-mail utility with their Web browsers. E-mail can be distributed to lists of people as well as to individuals.

‡ ASCII (American Standard Code for Information Interchange) is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number (a string of seven 0s or 1s). 128 possible characters are defined. www.whatis.com/ASCII

§ Binary is the base two number system that computers use to represent data www.whatis.com/binary

*** Multipurpose Internet Mail Extensions

†† SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used for transferring e-mail across the Internet. E-mail is sent with SMTP and a mail handler either POP3 or IMAP receives it on your recipient's behalf (i.e.local server).. The mail is read using POP or IMAP protocols. Most mail programs specify both an SMTP server and a POP server. On UNIX-based systems, [sendmail](#) is the most widely-used SMTP server for e-mail. The details of SMTP are in RFC 821 of the Internet Engineering Task Force (IETF). An alternative to SMTP that is widely used in Europe is X.400. www.whatis.com/SMTP

‡‡ POP3 (Post Office Protocol 3) is a client/server protocol in which e-mail is received and held on the Internet server until the mail is downloaded. POP3 is built into the Netscape and Microsoft Internet Explorer browsers. POP can be thought of as a "store-and-forward" service.

An alternative protocol is IMAP (Interactive Mail Access Protocol). With IMAP, e-mail is viewed at the server and can be kept on and searched at the server. IMAP can be thought of as a remote file server. POP and IMAP deal with the receiving of e-mail

2.3.2.1 Attitudes and Usage

A survey of 485 organisations conducted by Reed Personnel Services in 1996⁵³, found that 76% believed that new technology increased the effectiveness of communication in the workplace. E-mail was thought to be a useful tool by 44% and the most sociable form of communication compared to voice mail and video conferencing which were seen as *"robotic and impersonal"*. Despite this, it was still not widely implemented or used by businesses in 1996, but was rather an *"executive toy"* reserved for use mainly by top levels of management.

Some of the benefits and drawbacks of electronic mail are wide and varied, a selection of these has been summarised in the following table.

ADVANTAGES	DISADVANTAGES
Instantaneous and fast access - messages can be received within minutes of being sent	The recipient controls their e-mail access and might access it once a week E-mails may get "lost" and never arrive at their destination It may take anything from minutes to days for e-mails to arrive
Worldwide geographic reach. Computer to computer delivery	The recipient must have access to the Internet, e-mail software, and an e-mail address and software
Relatively easy and inexpensive to set up	Computer hardware and software must be available
Inexpensive to use - e-mails can be sent over the Internet at local telephone call rates	The majority of users must be connected to an Internet service provider (ISP) which provides access to the Internet
Reduce paperwork and increase automation of processes	Dependent on the user's practices and the degree of integration of e-mail into business processes
Sound, video and graphics files can be sent by e-mail	E-mail software must be compatible with the senders' in order to decode the files
Other services can be incorporated into this e.g. fax to e-mail and e-mail to fax ⁵⁴	This is dependant on the technological set up of the fax machines
Value added facilities can be combined with the basic e-mail service- for example security, virus checking, conversion to/from fax	Currently e-mail is untrustworthy because there are no security or authentication standards which allows the possibility of: <ul style="list-style-type: none"> ▪ Repudiation (denying that a message was sent or received) ▪ No confidentiality- anyone who has access to the user's e-mail box may read the message ▪ No integrity checks - the message received may have been intercepted, changed and forwarded without detection ▪ No authentication - where a user can masquerade as and send e-mail purporting to be another person without detection
Can be used as a medium of business and commerce	There is currently no legal or commercial support infrastructure for e-mail communications and document transfer.

Table 5. Advantages and Disadvantages of E-mail

The benefits of e-mail to business were measured in practical terms of time and cost saved, by Professor Palme of Stockholme University⁵⁵ who found that the average business letter takes 30 minutes to produce and the average business telephone call lasts 20 minutes, ignoring unsuccessful attempts to reach the intended person. In comparison, the average e-mail takes just under 5 minutes to prepare and send and is much less costly.

With the benefits of e-mail come the problems of a new technology in the early stages of implementation and use. In practice, e-mail was being used as a private form of communication by employees who believed that their e-mails were immune from invasion by others. Companies found that there were often exchanges of disparaging comments about management or their competitors. In the well-publicised case of Norwich Union, their staff had spread rumours about another health insurance company⁵⁶. The company was ordered to pay nearly half a million pounds in damages and costs, after it was found guilty of committing libel by e-mail for the first time in legal history.

"People regard e-mail as a transient medium in that the message disappears into the ether. The reality is that everything you type and send is recorded almost for all time and is available to be reassembled at a later date. " ⁵⁶

With this confusion about e-mail privacy amongst company employees, it was advised that an e-mail policy was needed to avoid disputes. Some of the guidelines suggested by Stobie⁵⁷, included advising users to:

- Avoid ambiguous symbols
- Assume all e-mails can be read by a third party
- Not use e-mail for harassment or abuse of any kind
- Not send multiple copies
- Be security-conscious about attached files, which might be confidential or contain viruses.

Not only this, but a whole programme for educating staff about the risks was also being stressed as necessary because, apart from libel, there were other issues which include copyright infringement, the giving out of negligent advice and unauthorised employees entering into a binding contract on behalf of their company. As well as having an e-mail and Internet policy, many employers were advised to reference these policies and include them in employees' contracts⁵⁸.

Unsolicited junk e-mails and information overload was also increasingly becoming a prominent negative factor of the new technology, as reports of managers being unable to read all the content of their electronic in-boxes⁵⁹ intensifying with wider e-mail usage. There were also problems of reliability and security, where e-mails sent were never received or received days later and e-mails purporting to be from the originator in fact being sent by impostors masquerading as the originators.

Despite this, in 1997 governments were promoting e-mail and the Internet as an indispensable business tool. The European Commission was promoting public procurement efficiencies by introducing electronic tendering, invoicing and payments. It voiced its concerns about the potential problems.

"If a bid for a contract is sent by e-mail over the Internet, the sender has no way of knowing that the bid was successfully delivered and before deadline. The Internet is also inherently insecure and few businesses are prepared to send bids or other confidential information via the system"⁶⁸

"Sending e-mail over the Internet is like sending a postcard - anyone can read them".⁶⁹

But governments and other organisations were working to develop technological and socio-economic frameworks to make e-mail usable by business.

2.3.3 Security

Spar & Bussgang⁴² stressed that until the potential problems with the Internet are dealt with, then growth and development of the Internet for business communications and transactions will be limited. Among the problems they identified are security concerns.

However, there are many issues surrounding security and the Internet, which can be broadly divided into three major levels:

- Physical Security
- Systems/Network Security
- Security of data and electronic transmissions

2.3.3.1 Physical Security

One aspect of security is the prevention of unauthorised access to any computer hardware. This includes the installation of security equipment in buildings and on equipment. For example:

- The use of CCTV to detect and record illegal intrusion.
- Access control such as smart cards and locking mechanisms. Access control is increasingly becoming more sophisticated and some systems even have incorporated bio-technological methods of verification such as fingerprint and iris matching.
- Heat and movement detection intruder systems to prevent unauthorised physical intrusion and theft or damage to equipment.
- Bolting of computing equipment to desks and floors.
- Unique identification of microprocessor chips.

Physical security also incorporates damage control such as, fireproofing of buildings and secure boxes for storing data backups.

2.3.3.2 Systems and Network Security

This involves the prevention of unauthorised access to systems and networks. Some of the threats inherent in connecting to the Internet include:

- Weak or no authentication required. For example, rlogin, requires no password for logging in; Anonymous FTP^{§§§} and WWW provide information with little or no authentication; TCP^{****} and UDP^{††††} trust the IP address of the remote station; NFS^{††††} grants access to anyone from a particular remote host. Other services are similarly insecure as they require passwords to be transmitted over the network in the clear, which makes them vulnerable to capture and replay.
- Sniffer and Cracker programs. Sniffer programs monitor network traffic for user names and passwords. Cracker programs, run in background mode on a machine, encrypting thousands of different words comparing them to encrypted passwords stored on the machine also known as dictionary attacks. This allows systems to be easily compromised by a hacker.
- Insecure software. This is particularly true of shareware or free/low cost software which often has bugs or design flaws in it. Because of their low cost, many people are prepared to use them despite the risks. In the past, a freeware FTP product contained a “Trojan Horse”^{§§§§} that allowed privilege access to the server.

^{§§§} File Transfer Protocol

^{****} Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and in interconnected systems of such networks.

^{††††} User Datagram Protocol (UDP) provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed.

^{††††} Network File System is file system that will mount remote file systems across homogenous and heterogenous systems. NFS consists of client and server systems. An NFS server can export local directories for remote NFS clients to use. NFS runs over IP using UDP (commonly). There are NFS implementations that will work using TCP as the network transport service. NFS was originally developed by Sun Microsystems Computer Corp. (SMCC) and is now part of their Open Network Computing (ONC) initiative. NFS has been accepted by the IETF in certain RFC's as a standard for file services on TCP/IP networks on the Internet.

^{§§§§} A program that masquerades as another common program in an attempt to receive information. For example, a program that masquerades as a system logon to retrieve user names and password information which allows the authors to later break the system.

- **Masquerading (Spoofing).** This is where a hacker falsifies the origin and/or destination of a packet. For example, SMTP protocol uses ASCII messages to transfer messages, so a hacker can TELNET into an SMTP port and simply type in a bogus e-mail message. Also IP source routing allows a caller to falsify its IP address and provide the recipient with a return path directly to itself.

Dr Cavalli⁶¹ introduces the concept of control points. A control point is a tool or process designed to meet a specific threat and acts as a countermeasure against that threat. For example, a physical security system is made up a number of distinct control points - the issuance of passes, guards, CCTV, revocation of passes, security codes, door locks etc. Security is compromised if any one of the control points is absent or not working. Similarly network security consists of a set of control points working together to form an integrated security package, where each control point is designed to meet a particular threat. According to Cavalli, security problems arise not because of poor technology but because of lack of completeness or failure to maintain the proper procedures for the control points. Cavalli matches the possible threats to a network with the control points that can be used to counter them. These are summarised in table 6.

THREAT	CONTROL POINT
Unauthorised users might intercept, read, alter original messages and forward them to the intended recipient	Encryption - Encodes electronic data
Unauthorised users on one network might contact computers on another network	Firewall ^{*****} - Evaluates traffic passing between networks rejecting suspicious traffic and notifying system administrators of possible attempts at penetration while allowing desirable traffic to pass
A hacker might use holes in current operating systems to penetrate corporate computers and steal important information or engage in espionage	Host Security - Runs every computer that is accessible to outsiders with a tightly controlled, auditable and constantly monitored operating system
Masquerading - where a party at either end of the connection might misrepresent their identity to perpetrate a fraud	Mutual Authentication - Uses highly secure cryptography, hardware tokens or other techniques to verify the identities of the parties at both ends of the connection.
A valid identification (certificate) might be issued to an impostor	Certification authority - a trusted and highly secure entity which validates users before issuing them with certificates.
A user who has been removed from the system might still retain a valid certificate	Certification authority - maintains a list of revoked certificates available to members of the system
A valid user with a valid certificate might access information or capabilities they are not authorised to have	Access Control - assigns and manages a user's network privileges and access to areas on the network.

Source: Dr.A.Cavalli⁶¹

Table 6. Security Threats and Prevention Measures

***** A full description a firewall is included in Appendix 4

One of the easiest and most common breaches of security is through the intentional or careless action of people. By following common sense guidelines and procedures, security breaches can be kept to a minimum. This is introduced through a security policy, which lays down best working practices, incorporating all levels of security. The three main areas which need to be addressed in any IT security policy are:

- Keeping data confidential and safe from external threats such as hackers
- Ensuring data is available only to those authorised to see it
- Ensuring data is not corrupted by viruses and that it is correctly updated across the organisation.

These can be covered for example, by ensuring:

- All users understand the importance of keeping their passwords confidential to themselves both for access to the network but also access to buildings and rooms.
- That access given to staff whose employment period is terminated is removed immediately and other non-individual access codes are changed.
- The potential introduction and spread of viruses is minimised by restricting the use of external floppy disks and of downloading material from unauthorised web sites and using and by updating virus checking software regularly.
- Firewall technology is implemented.

These must be in accordance with the BS7799⁶² code of practice that recommends implementation of:

- An information security policy document
- Virus Controls
- Business continuity planning
- Safeguards for organisational records.
- Allocation of information security responsibilities
- Information security and training

- Reporting procedures for security incidents
- Control of proprietary software copying
- Data protection policy and control

2.3.3.2.1 Attitudes and Usage

In 1996/97, there was very little academic or empirical work done on Internet security in the UK. In the US however, a report by John Howard⁶³, analysed trends in Internet security by investigating 4,299 security-related incidents reported to the CERT[®] Coordination Center (CERT[®]/CC) from 1989 to 1995. These findings are based on a period of time where there was no real wide spread use of the Internet by business. Prior to this research, knowledge of security problems on the Internet was limited and largely anecdotal. With the exception of denial-of-service attacks, security incidents were generally found to be decreasing relative to the size of the Internet. These findings must be used with caution, since they are reported breaches of security. A large number security breaches go unreported to prevent the bad publicity associated with the corporate name.

Estimates based on this research indicated that a typical Internet domain was involved in no more than around one incident per year, and a typical Internet host in around one incident every 45 years. It was also found that the majority of identified attackers were former employees. Most of the attacks (89%) were unauthorised access incidents, which included root break-in, account break-in and access attempts. The other types of attacks were denial of service (2%), corruption of information (3%) and disclosure of information (5%). The process of the attacks was to gain access to the target system; to exploit vulnerabilities and gain privileged (root) access; then to attack other systems across the network. The most common type of tool used was scripts and programs namely Trojan horses and sniffers. The most repeated vulnerabilities were found to be password related (22%). That is, password files which indicated that a password file had been copied, password cracking indicating that passwords had been determined by a password cracking tool and weak passwords which had been easily guessed. Two predominant trends were observed over the period of time. Firstly, the sophistication of intruder techniques progressed from

simple user commands, scripts and password cracking, to the use of tools such as sniffers (1993), toolkits (1994) and intricate techniques that deceived the operation of the Internet protocol (1995). The second trend was that initially intruders tended to be confined to a few individuals in specific locations. With time, as tools have become more sophisticated and the Internet has grown globally, it is becoming almost impossible to locate and identify attackers. The findings from research into security, led to estimates that a typical Internet domain is involved in no more than one security breach incident per year. However, it should be noted that the more attractive the sites to attack, the more likely they are to be involved in many incidents each year. Overall though, the research found that the growth in unauthorised use incidents was higher than the rate of growth in Internet hosts.

Howard developed a framework or "taxonomy" which identified the path an attacker takes in order to accomplish his/her objectives (Figure 2). Since computer security can be defined as preventing attackers from achieving their objectives, by looking at the steps in the process, industry and technology specialists can develop a security policy which blocks these steps.

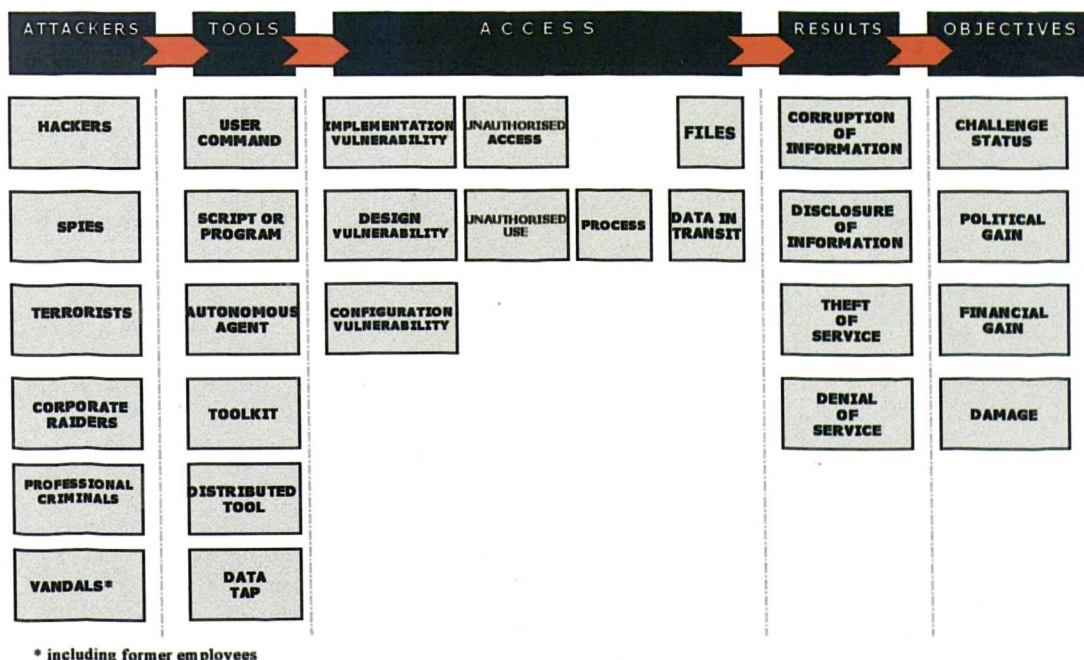


Figure 2 . Howard's Taxonomy of Complete Computer & Network Attack

Level 1 - Attackers - determine who the attackers are and where they are located. Other efforts can be made to prevent attackers from using computer and network resources, such as through closing of accounts or preventing access to network connections.

Level 2 - Tools - When *tools* are found in use they can be removed. For example, users and system administrators are encouraged to use *virus-checking* software to detect and eliminate autonomous agents. Systems can be monitored closely to detect the presence of Trojan horses, or other unauthorised files. Processing can be monitored for unauthorised operation of software, such as password crackers or sniffers. User commands can be monitored and logged. Such monitoring could be used to warn of attack, and logging could be used to investigate after an attack. Systems can also be monitored and filtered for the use of specific forms of attack. Examples of these are IP spoofing packets, mail spam, and attack tools found in common toolkits.

Level 3 - Access to systems can be prevented in two ways: (a) by a vigorous program to discover and eliminate design, implementation and configuration vulnerabilities. Systems administrators are key to this effort. They must keep current on the latest problems that are discovered. They must ensure the system and all its files are configured correctly, that software bugs are patched, and insecure software is eliminated or restricted, (b) to prevent access is to ensure access controls on files and processes are properly implemented. This includes a wide range of controls, from strong passwords and secure password files, to correct default permissions on files. Unauthorised access can also be reduced by narrowing the number of processes that do not have access controls, and by monitoring how processes are being used.

Level 4 - Results - The results of a successful attack can be blocked by limiting the impact of the attack. For example, sensitive files could be encrypted so that even if an attacker succeeds in accessing files, information will not be disclosed. Files can be backed up to limit the damage caused by corruption of information, and systems can be carefully monitored for any signs of theft or denial-of-service.

A subsequent worldwide survey⁶⁴ of international companies in 1996, found that even though 68% of companies were concerned about security threats posed by Internet access, only 54% of over 1,300 respondents had a security policy. Around 60% of European companies viewed computer viruses as a primary security threat. The main preventative measures were data encryption at 15% and firewalls at 28% but even these were rarely used, with companies taking a reactive rather than a proactive approach to security. A Computacentre survey⁶⁵ of hackers in 1997, found that hacking was on the increase because it is facilitated by easy passwords, lack of encryption and firewalls and out of date security systems. Over a third of hackers felt that legislation was not a deterrent since hackers were seldom caught and rarely prosecuted. Mark Rasch, a leading security expert warned in 1997:

"The bad news is that nobody will get serious about cyber crime until there is a serious global catastrophe. The good news is that there will be a serious global catastrophe".²

This trend of inactivity when it came to security was repeated. Security holes were found⁶⁶ at many sites including Zenith Data Systems, Price Waterhouse, Marriott, Fidelity Investments and Corel. Although the security holes had been documented months ago, and easy fixes were available, the companies had not updated their software. Having said this however, it was found that only few sites, stored important data in unsecured locations and no proprietary or valuable information was found on most compromised web sites. Although an intruder might have been able to delete files or crash the server, it would have been more an act of electronic vandalism. The recommendations for introducing security were:

- Educate employees about security and its implications
- Remove sample files and disable unwanted services such as FTP.
- Analyse server logs - a search utility to look for suspicious CGI program use, such as out-of-range values or small numbers of accesses to files that don't currently exist on your server.
- Keep file permissions restrictive - where access to individual directories allow only reading and updating files. Web server accounts should not have permissions to delete or write files.

- Implement digital signatures and encryption - however, digital signatures must be integrated into an infrastructure where programs such as e-mail can use digital signatures seamlessly into their interfaces, there must be agreement on the dissemination of their public keys to ensure authenticity, users must be educated about digital signatures and how to use them.
- Virus checking software for all data.

By 1997, the same observations were being repeated, that hackers account for about 20% of attacks, but the main problems and the source of security breaches were internal personnel - either malicious activity by disgruntled employees or just mistakes, errors or carelessness. This was found to be largely due to the lack of educating users and employees about security and security issues. Although there are means to protect the network by using access controls, firewalls, strong authentication, encryption and digital signatures, these don't provide complete protection because of mis-configuration or malicious misuse by employees⁶⁷.

2.3.3.3 Security of Electronic Data

One of the recurrent recommendations for implementing a total security infrastructure is the use of authentication, encryption and digital signatures. This is the third major barrier to securing electronic data, both when static and in transit after securing the physical and network environments. Confidence in electronic transactions and the validity of documents and archives depends on trusting the authenticity, integrity and source of the data. Traditionally, the commercial infrastructure is paper and ink based, where documents are valid only when they are physically signed. Without this trust, the potential for exploitation of the opportunities provided by electronic commerce, would be severely limited. Within this electronic infrastructure there is a need for encryption technology, digital signatures, Trusted Third Parties and certification. This provides:

- Integrity - which ensures the message has not been tampered with or altered during storage

- Non-repudiation - where unique digital signatures and authenticated acknowledgements provide proof of delivery and receipt -
- Confidentiality - where the message is readable only by those for whom it is intended
- Authentication - proof that the message originated from the sender

This is the core of the authentication infrastructure being designed and developed in this study and is discussed fully in Chapter 4.

2.4 Summary and Conclusions

The importance of the role of government on the Information Society and the legal infrastructure governing the new media, were well recognised but still highly underdeveloped. Despite this, research and innovative business were continuing in the use of this new technology. The information reviewed for each of the identified areas of technology (Internet, e-mail and security) and its impact on the design of this research project are summarised in tables 7 and 8.

a) The majority of information available about the Internet centred on post implementation issues. The types of research carried out are mainly quantitative, largely anecdotal or based on studies of large US corporations.

Type of Research	Aims & Objectives	Summary of Information
Quantitative Connectivity Surveys	To establish numbers of users - both consumers and businesses To determine future projections of users	Use of the Internet has grown and continues to grow world wide. Future projections predict even faster and widespread growth. This indicates that the Internet is a long term medium for communication both for society and business.
Quantitative Usage Surveys	To establish patterns of usage, demographics of users, user perception of the Internet and important issues to the user.	Usage is on the increase, where the Internet is being used largely for e-mail or information. Users want an improved service delivery quality and ease of use of Internet facilities. User need for improved Internet security is very low.
Qualitative Benefit Analysis and Best Practice Guidelines	To determine the kind of benefits to business. To develop a best practice guideline for use of the Internet at work.	Based mainly on benefits to large and US corporations financial benefits have been identified. Best practice is still in the early stages of development and will be based on future usage and legal/regulatory policy.

Table 7 . Summary of Internet Research Data

b) The secondary sources of information about e-mail in the UK, centre largely on best practice guidelines and usage issues. Because it is still a new area in the embryonic stages of development and usage, availability of empirical data is still limited. Best practice frameworks for e-mail usage in business are still being developed based on government proposals, legal precedence and experience from working practice.

c) Internet related security is one of the most researched areas in terms of having identified potential security breaches and developed technological solutions. As with the information gathered for the Internet, the focus of the studies and the evidence gathered is mainly based on large US and European corporations.

Type of Research	Aims & Objectives	Summary of Information
Quantitative Usage Surveys	To establish patterns of usage, demographics of users, awareness of and attitudes to security and IT issues.	Mainly large international companies. Although there are security concerns in organisations, Viruses were seen as the greatest threat. Organisations are aware of security measures, but few used them. The majority of business users have a reactive rather than proactive attitude to security breaches.
Quantitative Security Breach Surveys	To determine the actual numbers of security breaches on the Internet and identify the type of security breaches.	Based on evidence from US corporations, security breaches are increasing with the growth of the Internet. There was found to be problems of apathy and non-awareness confirming the reactive attitude to security.
Qualitative Security Framework Analysis	To develop a framework identifying the type of security breaches to establish means of prevention.	Largely academic frameworks, for example, development of a taxonomy of different types of security breach and their impact and how they can be prevented. One of the most common causes of security breaches is people.
Developing Security Solutions	Developing security solutions to counter security breaches.	Employee training & education, firewalls, encryption, digital signatures and authentication as well as a host of other hardware and software solutions.

Table 8. Summary of Internet Security Research Data

This literature review confirms a number of issues which underlines the importance of the Internet and security as an area of research. These are:

- **The significance of the Internet and the facilities it enables, for business and society both now and in the future**
- **That corporate security breaches are happening and will continue to grow with the growth of the Internet**
- **General awareness and concerns about security is low and that companies are more likely to be reactive than proactive in their approach to security.**
- **Technological solutions are available for the detection and prevention of security breaches.**

The survey of available research also shows that:

- **Very little research has been done with or for SMEs**
- **A large proportion of research has been carried out in the US**
- **There is no frame of reference for electronic data security needs of SMEs**
- **There is no real body of work dealing with issues prior to and during implementation of security solutions**

Therefore, while drawing on the secondary research data already available, the findings of this project will produce a frame of reference for the electronic data and Internet security needs of SMEs in the UK. It will also introduce a framework for identifying the factors of success for implementing and using a secure electronic data and authentication solution.

The following chapter will discuss in detail the design of the research methodology used for this study.

Chapter Three

Methodology

3. Methodology

This chapter will firstly place the research strategy and methodology selected in its overall theoretical context. It will then explain and describe the methodologies used in this project to answer the broad research questions posed. These are:

- Can a security and authentication infrastructure be developed to provide SMEs with trust, integrity, confidentiality and non-repudiation when using the Internet for transmitting electronic data?
- Does the security solution work when used by SMEs?
- What is the process of implementation of the security solution by SMEs?
- What benefits are achieved for SMEs by secure use of the Internet?

The research design process follows a basic logic of enquiry. This was first identified by Wallace (1971)⁶⁹ in his Wheel of Science theory (Figure 3).

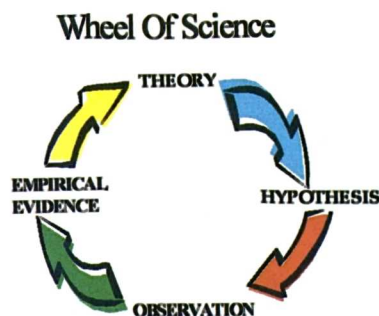


Figure 3. The Wheel of Science Theory of Research

In this context, the first stage is the development of a theory based on the identification and explanation of certain regularities, defined in the project's aims and objectives. The second stage is the derivation of hypotheses from the theory, stating where and when regularities should be found, which is the basis of the development of the "security and authentication solution". The third stage is testing the theories through observation, by implementing the security solution in case study SMEs. These observations inform the generalisations found. This then feeds back into the volumes of theory developing about the subject and should be the basis for further research.

The observation stage is crucial to any research design process, since hypotheses are tested and generalisations made based on the data gathered. It is therefore important to select appropriate methodologies to ensure that the hypotheses are tested as rigorously as possible.

Much has been written about methodological procedures and there are many schools of thought, which dominate methodological choices, ranging from the extremes of nomothetic to the ideographic as identified by Burrell and Morgan⁷⁰. Different methods adopt a position on the continuum, relative to the characteristics of the extremes described (Figure 4).

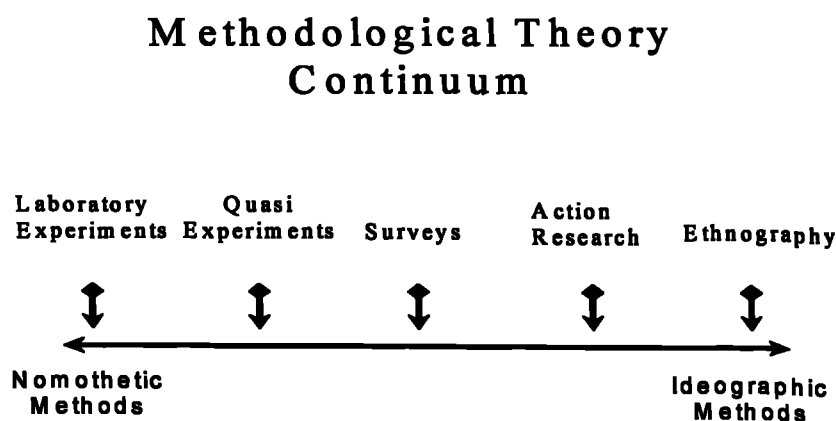


Figure 4 .The Continuum of Research Methodology Theory

The nomothetic approach, underlines the importance of basing research on systematic protocol and techniques. Emphasis is on deduction and explanation by analysis of causal relationships and laws. Quantitative data is used with various physical and statistical controls to test hypotheses. Highly structured research methodology is used to ensure replicability of research methods, allowing for quantitative analysis and thus the creation of mathematically valid results. The other extreme of the research strategy continuum is ideographic methodologies, which emphasise the analysis of subjective accounts that are generated by becoming a part of and being involved in the situations under investigation. Emphasis is upon induction, where subjective meaning and interpretations are explained by understanding. Qualitative data is used and

generated from the research being applied in everyday settings, to allow access to and minimise reactivity among subjects. Research methodology with minimal structure is needed to ensure empirical observations can take account of the subject's meaning and interpretational systems in order to gain explanation by understanding.

The difficulties of selecting the most appropriate methodological approach are well documented. It is described as a process of "muddling through incrementalism and political process" by Pettigrew⁷¹. Martin⁷² likens the research process to the "*garbage can model*" of organisational choice. Kulka⁷³, also suggests that the actual research process, far from being theoretical, is more frequently related to the availability and ease of access.

However, Gill and Johnson⁷⁴ conclude by stating that all research approaches have something to offer and that there are no real independent forms of evaluating different research strategies in any absolute terms.

*"broadly the consensus seems to be in favour of multi-method strategies . . . [i.e.] a strategy that requires not only a convergence of substantive findings from a diversity of methods . . . but also debate about the contribution of each method used"*⁷⁵

This "triangulation" research methodology, where a combination of methodologies is used in the study of the same phenomenon, is seen by Denzin⁷⁶ to have greater reliability than a single methodology approach. Campbell and Fiske⁷⁷ are also advocates of qualitative and quantitative methodologies being complementary and adding convergent validation. Jick⁷⁸ raises the question of whether all components of a multi-method approach should be weighted equally. He argues that there are no formal tests to discriminate methods or judge their applicability and, based on the findings of his own research, he concludes that all methods should be weighted equally since where discrepancies occurred, this was seen to enrich explanations and not weaken the validity of findings.

3.1 Research Strategy

The nature of this research project is bipartite as illustrated in Figure 5. One part involves the creation of a service based on a technological product. The second part is the implementation and testing of this service in a commercial environment.

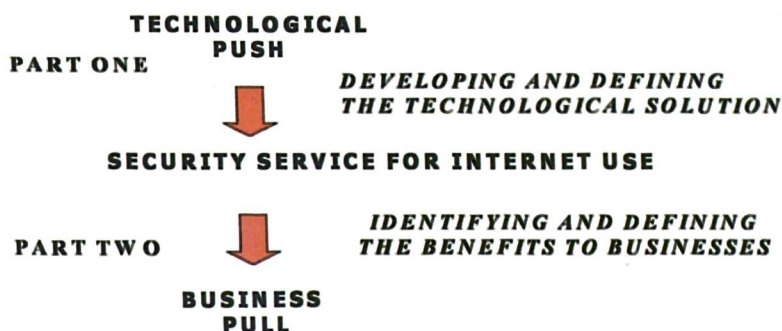


Figure 5 . The Bipartite Research Strategy

A multi-method or triangulation strategy has been used over the course of this three year research project. While all methods have something to offer, by using methodological pluralism, the collated findings will have more empirical validity as the weaknesses of each method are cancelled out.

Initially, the research strategy was designed to be largely deductive with data collection based on measurable and objective criteria. However, the results at certain stages and the nature of the hi-tech environment, where life-cycles are falling and innovation is ever-present, made it necessary to develop a research strategy with an underlying organic structure, allowing modification and flexibility to ensure that a meaningful study is produced.

3.2 Research Methodology

The theory of the research project by deductive analysis based on literary and technological sources is that, the Internet is a medium fast becoming the medium of business, but the current status of the Internet is not secure. From this, two hypotheses have been developed.

- *H₁ - The most appropriate authentication infrastructure for SMEs is Public Key Infrastructure (PKI) and Trusted Third Party supplied Certification Authorities (CA)*
- *H₂ - When the security service is adopted and used by SMEs this would be commercially beneficial to them and provide a means of maintaining a competitive edge*

The research involved testing these hypotheses using a range of methodologies.

3.2.1 Design and Development of the Security Solution

Both deductive and inductive research methods were used in part I to design and develop a security and authentication infrastructure. Deductive methods were used for the evaluation of the technology. The methodology used in the process of the software evaluation was based on a list of measurable, objective criteria under "experimental conditions in a laboratory". This means that the test could be repeated under identical conditions. Full details are given in Chapter 5. Measurements were given for a range of factor attributes important to the provision of a security and authentication service, hereafter also referred to as the **security service or security solution**.

Inductive methods such as quantitative (surveys) and qualitative (focus groups) techniques were used to build the layers of the security service around the technological core.

3.2.1.1 The Methodology

A telephone survey of 145 SMEs in the Greater Manchester area was used to explore the attitude to and the understanding of the Internet and electronic data security in regional SMEs. The size of the telephone sample, gives a 95% confidence level that the findings are within a plus or minus 4% range of error⁷⁹.

A semi-structured, open-ended format of questions was used in the interviews (Appendix 6). The main reason for this is that the subject matter relates to a technical concept which respondents may never have encountered or feel constrained or intimidated by the nature of the subject or their own lack of knowledge. The semi-structured format allowed the respondents to articulate ways in which they understood the matter being discussed. This information would be used to develop the layers of service provision around the technological core of the security software.

Qualitative focus groups (Appendix 6) were used to obtain a wider range of information, insight and ideas about the Internet and security. Information gathered from these sessions was used in conjunction with the information gathered from the telephone surveys. The two methods together give a mix of statistical confidence (telephone survey) and wide-ranging, in-depth insight (groups). More details of this research is given in chapter 5.

3.2.2 Implementation and Usage

The next part was to analyse and document the process of implementation, usage and benefits of the security and authentication infrastructure, to the organisations selected as case studies. Case study is the most appropriate method for this part of the research project, since:

- "How" and "why" questions are being posed and the focus is on a contemporary phenomenon within a real-life context⁸⁰ over which the researcher has little or no control. Namely - the processes for implementing and using an Internet based security and authentication infrastructure by an SME.

- The whole process is based on human action where there is a need to understand it

Yin⁸⁰, argues that for case studies, the use of multiple sources of information - documentation, admin and archive records, interviews, direct observation and participation - is essential because it allows the development of a more complete and reliable account of the issues and processes being studied.

Structured observation methods of data collection were used, post implementation of the security service in case study organisations. This was to determine the technology's functionality, the cost benefits to the organisation and the extent and frequency of its usability. Thus the conclusions of this study would show the effects of implementing the security service in an organisation in real terms. That is, whether:

- The technology worked as expected - encrypting and digitally signing electronic data.
- There were cost benefits to the organisation - in terms of lower operational costs, less time used by employees for various business processes. Comparative measurements of time and costs using the "new" compared to the traditional business process.
- There were other benefits such as:
 - increased sales through faster communication and wider geographical accessibility. Measuring the number of sales and geographical source through the use of the Internet and e-mail.
 - reduced costs through more competitive purchasing opportunities.
 - improved products/services through wider availability of information.
 - marketing benefits in terms of companies being able to convince their clients that their information and communications would be secure.

The techniques of data gathering in this case, would include:

- **Structured observation** by the researcher - where the criteria being observed and measured, are clearly pre-defined.
- **Logs of "help" calls** made to technical support staff to determine the types and frequency of usability issues.
- **Time Series structured questionnaires** (taking profiles of user attitudes, usage and opinions, before during and after the project).

The data gathered from this type of structured methodology would build up an empirical base on which best practice could be developed and replicated in other organisations. However, this type of methodology does not take into account the different settings and social contexts of organisations. Thus other methods of data collection were used to supplement and strengthen the validity of the data gathered.

These were:

- **Documentation** - information obtained from corporate literature; agendas and minutes of meetings; organisational archives - such as hierarchy diagrams, departmental structures.
- **Unstructured observation** - where the researcher would observe all aspects of the organisation relevant to the implementation of the security authentication infrastructure. This form of observation would allow the researcher to formulate the precise problem and be flexible enough to identify the key components of the problem and to develop a hypothesis. Because there is a potential for observer bias and the potential for the "client" to limit access to certain areas of the organisation, the findings here would have to be used in conjunction with other data gathered.
- **Semi-structured Depth Interviews** - Relatively open ended interviews with key personnel, would allow a free exchange of information where the researcher might confirm issues that had been previously raised or identify new areas and issues.

- **Observer-Participation** - here the role of the researcher would be to act as a consultant providing information. While this would offer the researcher the opportunity to gain access to events or groups that would be otherwise inaccessible in research study, there would also be problems such as:
 - the potential of the researcher to manipulate events
 - the researcher having less ability to work as an external observer because too much attention is taken through participation
 - the researcher might become a supporter of the group and thus introduce bias to the observation

Again the different number of data collection methodologies being used would limit the impact of any potential bias.

Although a number of different methodologies were used in the case studies, the findings would have to be analysed carefully before making generalisations, particularly in the case of SMEs. Small and medium sized enterprises are less homogenous in their behaviour than large and multi-national corporations. They are more entrepreneurial and informal in the nature of their business processes, procedures and approaches to innovation. Furthermore, the fact that case study organisations would be volunteers, lowers the validity of the results representing a larger population. The extent to which it would be possible to generalise from the sample of people involved in the research would have to be based on the results. The total sample of case studies would have to be segmented, where each case would have to be analysed and the variables identified for each organisation with clear statements on how representative the phenomenon observed are for the larger population of SMEs. Examples of the variables would be how dependent the business is on written information, what stage they are in their lifecycle, the kinds of customers or suppliers they have. The similarities and differences could then be categorised and used as the basis for further research.

3.3 The Process of Organic Methodology Development

Initially, the research had been designed with a clear definition of which functions had to be observed and measured. However, once the research had begun, in reality it was difficult to recruit volunteer companies to implement the security service. Thus, it was necessary to introduce further research in order to make their action intelligible, to generate an understanding of both the lack of success in recruiting organisations to implement the security service and also incorporate attitudes to security, e-mail and certification authorities in particular. This can be seen as another revolution in the "Wheel of Science" research design process illustrated in Figure 3.

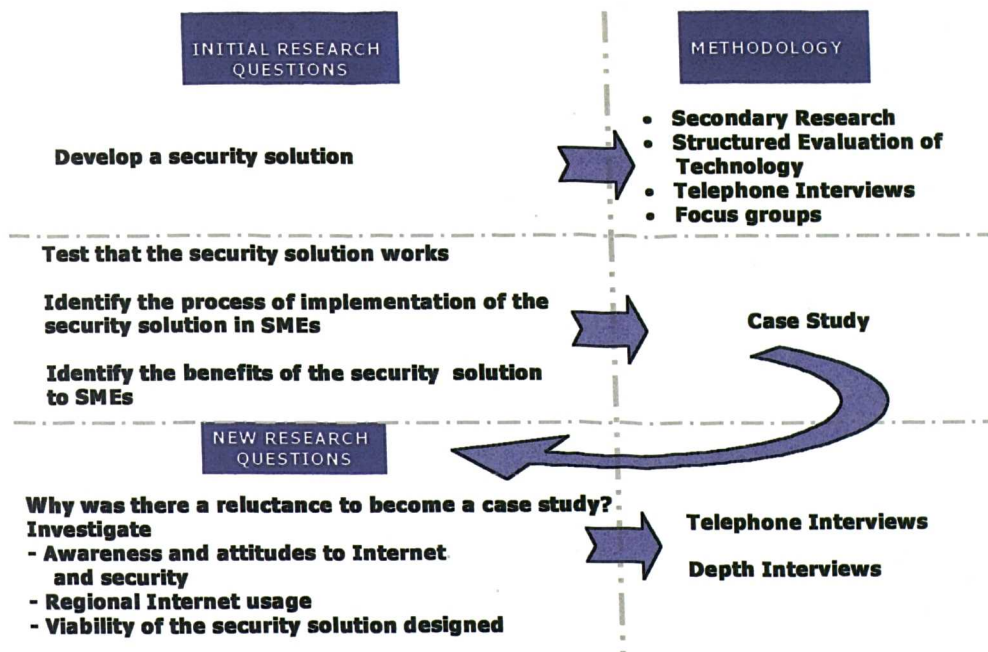


Figure 6 . Organic Research Methodology Development

The basis of the theory in the second revolution is grounded on the findings of the original research design process, that SMEs are unwilling to implement and use the designed authentication infrastructure. The process was then to identify the cause of this reluctance. In order to proceed with this second stage, the observation methodology would involve a combination of the qualitative and quantitative. These are outlined below, but are described in more detail in chapter 7.

3.3.1 Qualitative Methodology

A series of structured depth interviews were conducted with upper managerial decision makers across different industry sectors, to gain an understanding and insight into their attitudes to, knowledge and usage of e-mail, security and certification authorities. The information collated would be used to gauge the reaction of the respective sectors and assess which would be most amenable to a Trusted Third Party security and authentication infrastructure. This information would be used in conjunction with data from the previous methodologies. This is discussed in more detail in Appendix 21.

3.3.2 Quantitative Methodology

Taking the 1996/97 telephone survey sample as a base, the same respondent organisations would be surveyed in 1999. The aims of this interrupted time series survey, were to allow an exploration into the phenomena of the development, usage and adoption of the Internet and data security in regional SMEs. The advantage of this method would be that a pattern of change in the respondent organisations could be seen over time. The disadvantage would be that the absolute validity of comparison, is limited by the different perspective of different individual respondents. This is discussed in more detail in Appendix 21.

3.4 Conclusions

This research project has involved an organic process of methodology development. The limited empirical data available coupled with a new and changing environment has meant the need for two revolutions of Wallace's **Wheel of Science Theory**. The research design from the first revolution did not yield a source of data by which all the research questions could be answered. Initially, case studies were to be used as a source of information for the implementation of the security solution. However, the difficulty in recruiting case study subjects led to further research questions, namely why SMEs were reluctant to participate. This led to the design of further research methodology to gain an understanding of SME attitudes to the Internet and security.

A multi-method or triangulation strategy has been used at all stages to collect data for the design, development, implementation and analysis of this research project. By using a number of sources of information, these can be reviewed and analysed together so that the findings are based on the convergence of information from different sources and not a single source alone. While there are strengths and weaknesses of each method used, the impact of the weaknesses on the validity of the results have been reduced by using a myriad of methodologies and data collection techniques, which allows the evidence collected by different sources to corroborate each other. Fuller details of each methodology are included in the relevant chapter.

Chapter Four

Designing a Security Solution - Secondary Research

4. Designing a Security Solution - Secondary Research

This chapter surveys the different types of data security and authentication infrastructures that were available at the beginning of this research project in 1996. It briefly explains the need for security and the kind of security technology that provides authentication, certification and encryption. It goes on to identify the elements of an authentication and certification infrastructure, reviews the security services currently available and the potential impact of any legislation on this kind of technology. The chapter concludes with the selection of the technological infrastructure most suited to the requirements of this project.

The future potential and impact of the Internet on business and society has already been identified earlier in this study. The Organisation for Economic Co-operation and Development (OECD) in 1997 was one of the many organisations to identify barriers to the full development of the Internet. They list these barriers to include⁸¹:

- Building user and consumer trust in information systems and electronic transactions
- Minimising regulatory uncertainty in information systems
- Ensuring Access to the information infrastructure
- Easing logistical problems for payment and delivery

Many observers saw trust as the biggest impediment to the growth of electronic commerce and this is one of the issues being addressed in this study. Over the centuries, a whole legal, social and business framework and working practices have developed from paper-based transactions that have engendered a real and illusory sense of trust in the infrastructure. Not only this, but paper-based transactions also have a unique set of forensic attributes, such as:

- The chemical bonding of ink/lead and paper
- Biometric properties of handwriting and signatures
- Unique chemical and physical characteristics of paper, printing machines, seals etc.

These can be physically analysed in a laboratory and presented in a court of law to uphold and enhance that trust. The framework of trust on which the concept of paper-based transactions is currently founded, must be duplicated for electronic transactions, in order for paper to be totally superseded by electronic documents. Thus, any trust model for electronic commerce must include a macro-environment with:

- Legally and personally recognised signatures binding parties to agreements and contracts which cannot be repudiated
- Electronic practices, documents, seals and signatures recognised and accepted commercially, socially and legally.
- Recognition by and verification of official and regulatory bodies

On a micro scale, the elements of any security solution must include a mechanism whereby:

- Integrity of the original data and protection from tampering and forgery.
- Assurance that data sent is received in its original format.
- Authentication of parties to a transaction and the verification that a signature belongs to the signatory
- Confidentiality of information, that data being exchanged remains private and confidential between the sender and receiver
- Availability of information and services on demand
- Non-repudiation or denial of sending or receiving data

One of the requirements of this project, was to design a security solution that will provide trust, integrity, non-repudiation and confidentiality of electronic data both in transmission and in a static state. The actual development of security technology is beyond the scope of this research. The security and authentication infrastructure being developed here is based on building a trust model around existing proprietary security technology, in order to provide a solution that can be implemented and used by SMEs.

The following sections will survey the technology and review crypto-systems, digital signatures, key management, authentication and trust, elements of a security and authentication solution. These elements will be analysed to find the best fit for the requirements of this project.

4.1 Cryptography

Cryptography is technology that transforms electronic data into an altered form making it either:

- unintelligible-when-intercepted because the plain text will be transformed into non-readable ciphertext
- detectable-when-modified because the hash algorithm will produce a different value at the decryption stage than that produced at the encryption stage if the message has been modified

Modern cryptographic systems consist of two complementary processes:

Encryption - a process by which a readable message (plaintext) is transformed into a second non-readable message (ciphertext) using a complex mathematical function (encryption algorithm) and a special encryption key [independent data value made up of a random string of binary digits]⁸²

Decryption - reverses the process, where the ciphertext is transformed back into the original plaintext using a second complex mathematical function and a decryption key⁸²

The aim of cryptography is to make it impossible to take a ciphertext and reproduce the original plaintext without the corresponding key. It also aims to ensure that attempts to guess the corresponding key are too costly in terms of time and resources to make them viable. There are two basic types of encryption algorithms in use, known as:

- symmetric key cryptography
- public key cryptography or asymmetric key cryptography.

4.1.1 Symmetric Key Cryptography

The ECC white papers⁸³ describe a symmetric key cryptography system as one where the same key is used to both encrypt and decrypt a message illustrated in Figure 7.

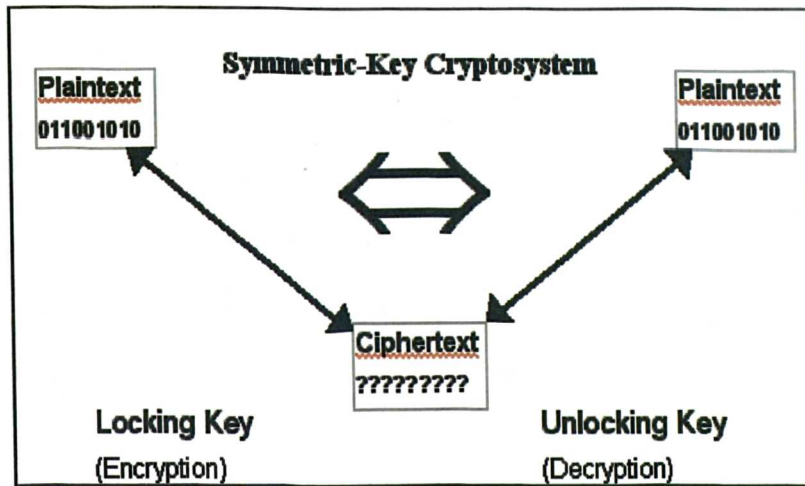


Figure 7. Symmetric Key Cryptography

These algorithms are very fast and extremely secure because once data is encrypted with a given key, it cannot be decrypted without the same key. Symmetric key algorithms consist of **block algorithms**, which encrypt data one block at a time and **stream algorithms**, which encrypt data byte by byte. This system is ideal in situations with a limited number of users in a close and trusted environment. However, Garfinkel & Spafford,⁸⁴ point out limitations to its usage in the real world:

- To securely exchange information between parties, those parties must first securely exchange a common encryption key. Not only must there be mutual trust and confidence in each respective party but also in each one's procedures for maintaining the key's security.
- With a larger number of users who are more geographically dispersed, there is a problem of key distribution and maintenance of security procedures and trust.

There are many symmetric key algorithms in use today and one of the leading authorities on cryptography, Bruce Schneier⁸⁵ has listed these with their source code. Some common symmetric algorithms include:

- **DES - The Data Encryption Standard** adopted as a US government standard in 1977. DES is a block cipher which uses a 56 bit key which means there are 2^{56} or nearly 72 trillion* different keys. It is possible that a machine capable of breaking a DES encrypted message in 3.5 hours can be built for under \$1 million⁸⁶.
- **Triple-DES** - the use of DES encryption algorithm three times with two or three different keys making it even more secure than the original DES algorithm. This though has a comparatively higher processor resource usage requirement.
- **IDEA - International Data Encryption Algorithm** published in 1990. This uses a 128 bit key and is used in the freely available Pretty Good Privacy (PGP) software to encrypt files and electronic mail. In this case, there are 2^{128} possible keys. Garfinkel and Spafford⁸⁴ note that if a computer existed that could try a billion different keys in a second and there were a billion computers, it would still take 10^{13} years to try every possible key. This is approximately a thousand times longer than the estimated current age of the universe.

There are numerous other proprietary algorithms available and being used in commercial products such as the CAST algorithm. One of the most prolific cryptographers is Ron Rivest, the creator of RC2, RC4 and RC5 algorithms, all of which allow keys between 1-2048 bits⁸⁷ and are being used in commercial products.

* 72,057,594,037,900,000

4.1.1.1 Attacks on Symmetric Encryption Algorithms

In order to understand any security issues, it is also important to understand how security can be breached. The methods of breaches on the system that might occur are highlighted by Garfinkel & Spafford⁸⁴ and are outlined below.

a) Search Key or Brute Force attacks - This method of cracking a code, is by trying every possible key one after another. Often these attacks are not very efficient or successful. However, as processors become more powerful, search attacks will become easier especially with smaller bit keys. In 1997 a 40-bit code was cracked in 3.5 hours. Thus the 40-bit key is subject to a search key attack.

b) Cryptanalysis - Breaking codes, is not purely based on key length of a cipher. Encryption algorithms can be deciphered by a combination of sophisticated mathematics and computer processing power for example, when the algorithm is known, the following methods are possible:

- **Known plaintext attack** - where both the plaintext and ciphertext are available and can be analysed simultaneously
- **Chosen plaintext attack** - where chosen blocks of data are encrypted by the subject of the attack and the results are then analysed
- **Differential cryptanalysis** - similar to chosen plaintext attacks, the process involves encrypting many texts that are only slightly different from one another and comparing the results.
- **Differential fault analysis** - where the attack is against the cryptographic system built in the hardware. The hardware is subjected to environmental factors (heat, stress, radiation), where occurring decryption/encryption faults are analysed from them the device's internal state including the encryption key or algorithm can possibly be learned.

c) Algorithmic Attacks - where attackers find a fundamental flaw or weakness in the mathematical problem on which the encryption system is based.

d) System-Based Attacks - where the code breaking attack is to attack the system that uses the cryptographic algorithm without attacking the algorithm itself. For example, the ability to monitor a random number generator, predict the starting configuration and determine the randomly chosen key, or bypass the random number generator part of the program itself, that allowed direct input of the number by the attacker. Another example⁸⁸ is the sale of pirated video decoder boxes, which could intercept the transmission of keys and use them to decrypt the broadcasts.

4.1.2 Public Key Cryptography (Asymmetric Cryptography)

The technology of the public key cryptography was first introduced by Whitfield Diffie and Martin Hellman⁸⁹, who presupposed the existence of an encryption technique where information encrypted with one key could be decrypted by a second unrelated key.

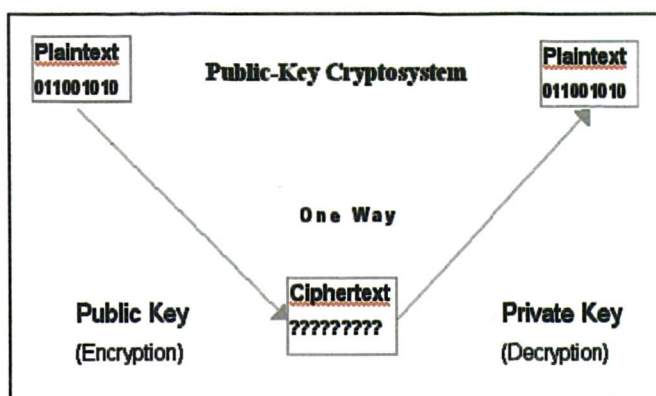


Figure 8. Public Key Cryptography

One key (the private key) is kept secret within the system while the other key (the public key) can be made publicly known. Knowledge of the public key allows encryption of plaintext, but does not allow decryption of the ciphertext. If a person published her public key, then everyone can use that public key to encrypt messages for that person. The private key is kept secret so that only the intended individual can decrypt the ciphertext. The cryptography system became reality a year later with the invention of the RSA algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Netscape

and Microsoft. It is also part of Lotus Notes, Intuit's Quicken and many other products. The RSA algorithm can be used for encrypting information and as the basis of a digital signature system that can be used to prove the authorship and authenticity of digital information. The key may be of any length (generally greater than 512 bits) depending on the particular implementation used.

Asymmetric encryption algorithms are based on number theory and as such it is more difficult to create a good algorithm since it requires identifying new mathematical problems with particular properties. The exploration of the mathematical formulae is beyond the scope of this research project.

The three main systems that are used are briefly summarised from the ECC White paper⁸³. These are classified according to the mathematical problem on which they are based:

- ***Integer Factorisation System*** e.g. RSA - the security of RSA depends on the fact that, while finding large prime numbers is relatively easy, factoring the product of 2 such numbers is difficult. If the numbers are sufficiently large, factoring requires enormous processing resources which makes it computationally unfeasible. Rivest estimates that a 1024-bit modulus part of the public key is likely to be sufficiently strong for several more years.
- ***Discrete Logarithm System*** e.g. ElGamal - named after its creator based on the Diffie-Hellman key exchange protocol and Digital Signature Algorithm from the US government - where the mathematical problem⁸³ is the difficulty of inverting a mathematical exponential operation in a finite field .
- ***Elliptic Curve Cryptosystem***⁹⁰ - the above is not the only mathematical structure over which the discrete logarithm problem can be defined. In 1985, Neil Koblitz⁹¹ and Victor Miller⁹² independently proposed the Elliptic Curve Cryptosystem (ECC), whose security rests on the discrete logarithm problem over the points on an elliptic curve. ECC can be used to provide both a digital signature scheme and an encryption scheme. Elliptic curve-based digital signature systems can perform the same functions as RSA and DSA but with more efficient implementations.

This system depends on the discrete logarithm problem, where elliptic curves are used as the basis for generating multiplicative groups on which the algorithm is based. With elliptic curves, the logarithm problem is more difficult. Thus it is thought to be possible to devise a stronger cryptosystem with a shorter key size than DSA. Using elliptic curves, digital signatures can be verified and generated more quickly and be more readily deployed in small, limited resource devices such as smart cards. More testing needs to be done on this before it is more widely used.

4.1.2.1 Attacks on Asymmetric/Public Key Encryption Algorithms

Public Key algorithms are theoretically more vulnerable to attack because the attacker has access to the public key used to encrypt the message. Attacks fall into two categories:

- ***Factoring attacks*** - where attackers attempt to derive a secret key from its corresponding public key. RSA Data Security publish a list of factoring challenges, with cash rewards for anyone who can factor certain published numbers[†]
- ***Algorithmic attacks*** - where attackers find a fundamental flaw or weakness in the mathematical problem on which the encryption system is based.

[†] A list of challenge numbers can be obtained from challenge-rsa-list@rsa.com

4.1.3 Analysis of Cryptosystems

The advantages and disadvantages of both systems are summarised in Table 9 and relate to the criteria of this project's requirements.

PROJECT REQUIREMENTS	SYMMETRIC KEY ENCRYPTION	PUBLIC KEY ENCRYPTION
EXCHANGE OF ENCRYPTION KEYS	Firstly, the users must exchange these keys securely. They must create their own environment of trust. This is good for a few users but impractical for large numbers.	The public key is published and can be accessed by anybody to encrypt a message. Public keys can also be used to encrypt a symmetric key
MAINTENANCE OF KEYS	Identical keys must be managed by all the users - which is impractical for large numbers of users	The private key is kept and managed by the individual - it is never transmitted or shared The public key is in the public domain and published in a directory
SPEED OF ENCRYPTION	Faster than public key algorithms easier to implement technologically	Very slow between 10 to 100 times slower than equivalent symmetric key encryption algorithm
EASE OF ATTACK	More difficult to attack because only the key owners have a copy of the key.	Easier to attack than symmetric because the attacker has a copy of the public key that was used to encrypt the message
USE FOR AUTHENTICATION	Produces a message authentication code (MAC) that checks the integrity of the message	Produces a digital signature
USE FOR NON-REPUDIATION	Cannot be used because a common secret key is shared	Can be used because only the sender has the private key

Table 9 . Features of Symmetric and Public Key Cryptosystems

The slower public key cryptography is used to exchange a random session key, which is then used as the basis of private symmetric key algorithm. A session key is used only for a single encryption session and is then discarded. This serves the requirements of the project and is the most commonly used technology in commercially available packages.

4. 2. Digital Signatures

Another element of security, which provides integrity of messages is a digital signature.

A digital signature is a data item which accompanies a digitally encoded message and which can be used to ascertain both the originator of the message and the fact that the message has not been modified since it left the originator. ⁹³

Figure 9, illustrates the process of producing a digital signature.

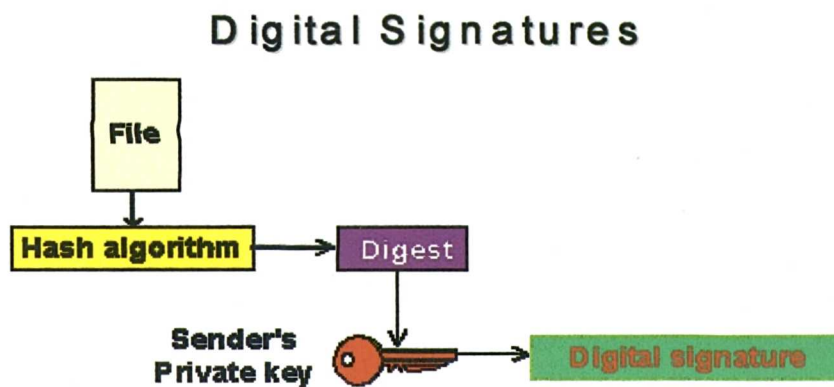


Figure 9 . The Process of Producing a Digital Signature

A digital signature scheme consists of a signature algorithm and a verification algorithm. The digital signature is generated by the originator's private key and is verified by the recipient using the originator's public key.

Usually, a hash function is used within the signature. The hash function is a mathematical formula that reduces values from a large into a relatively small range. A hash function can reduce a message of millions of bits in length to a fixed length data output value (message digest) of about 128 bits. Because there is an infinite number of messages and a finite number of hash values, there is a possibility of the same hash number matching two different messages by chance. Having said this however, the properties of a mathematically "good" hash function are that a) there is very low probability that 2 messages will produce the same hash value b) it is computationally unfeasible to generate a message with a particular hash value.

The hash function has the property that if the original message is changed even minutely, an entirely different digest will be produced. Thus if any part of the originator's message is corrupted or modified, or if the signature was not created by the originator's public key, then the verification will fail illustrated in Figure 10.

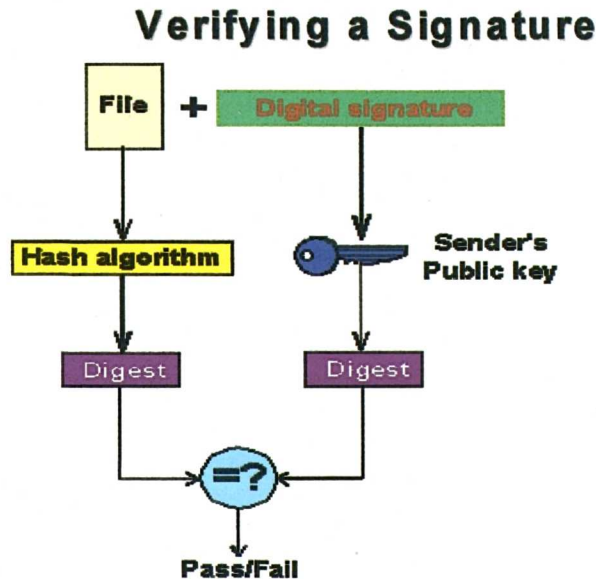


Figure 10 .. The Process of Verifying a Digital Signature

Digital signatures support non-repudiation and although similar to public key cryptography are in fact different. Public key cryptography protects the confidentiality of a message and is reversible, but the digital signature provides data origin authentication and non-repudiation cannot be reversed without corrupting the integrity of the original data.

4.3 Digital Certificates

Digital certificates offer proof of identity. They establish who owns a particular key, providing an electronic means of verifying that the individual or organisation is who they claim to be. A certificate is a digital document that binds an identity or other attribute of its principal to an electronic key that can be used to encrypt and/or verify digitally signed information. Principals can be people, application code or any other uniquely identified entity. From a technological point of view it is possible to include extra identifying information stored on each public key, such as address, e-mail

address, contact details, or any other information. These are digital certificates, attesting that a particular public key belongs to a particular individual or organisation. There are a number proposals specifying the precise format of a certificate, most notable the certificates used in the X.509 Directory Framework. These formats differ to some extent in the fields they include and in the length of individual fields and there have been a number of versions (1,2,3) of the X.509 certificate to date. The latest version 3, is no longer restricted to the X.500 naming system, but recognises entities e.g. certificate subjects. Public key cryptography and digital signatures both rely on certificates.

4.3.1 Certificate Repositories

In order for the message originator to send a message to the recipient using a certificate easily, a public directory service that can distribute certificates is needed. There are a number of standards for storing and retrieving public key certificates. A comprehensive on-line directory service has been developed through the standardisation of processes of the International Standards Organisation (ISO). These directory standards commonly known as X.500 provide the basis for the construction of a multi-purpose distributed directory service.

The X.500 directory service is a highly distributed way of storing and retrieving information and is designed primarily to support querying by human users. It allows users to find information such as telephone numbers, addresses, and other details of users and organisations. It is also intended to support electronic communications in the form of message handling and file transfer. For message handling, there is support for user-friendly naming, distribution lists, and security. There is also name-to-address mapping which provides support for features such as OSI[‡] presentation address look-ups. Each local directory is called a Directory System Agent (DSA). A

[‡] OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. The main idea in OSI is that the process of communication between two end users in a telecommunication network can be divided into layers (usually 7), with each layer adding its own set of special, related functions. So, in a given message between users, there will be a flow of data through each layer at one end down through the layers in that computer and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user. www.whatis.com

DSA can represent one organisation or a group of organisations. The DSAs are interconnected from the Directory Information Tree (DIT). The user interface program for access to one or more DSAs is a Directory User Agent (DUA). In essence the directory is a database with certain key characteristics:

- It can be very large and highly distributed on an organisational basis in most cases.
- It is hierarchically structured, the entries being arranged in the form of a directory information tree (DIT).
- The number of read and search operations, vastly exceed the number of modification operations.
- Temporary inconsistencies in the data are deemed acceptable. This greatly facilitates the replication of data in the directory by nullifying concerns about record locking and atomic operations.

LDAP (Lightweight Directory Access Protocol) is another directory access protocol which is compatible with the X.500 directory model. It is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol) which originated at the University of Michigan and is used for example by Netscape in its latest Communicator suite of products and a number of Microsoft Active Directory products including Outlook Express.

4.3.2 Certificate Policy

The most widely recognised standard public-key certificate format, defined by the International Standards Organisation (ISO) and others is X.509, which defines a certificate policy as,

"a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements"[ISO1]⁶¹

An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

4.4 Authentication, Key Management and Trusted Services

A certificate is used by a "certificate user" or "relying party", that needs to use and rely upon the accuracy of the public key distributed via that certificate. A certificate user is typically an entity that is verifying a digital signature from the certificate's subject or an entity sending encrypted data to the subject. *The degree to which a certificate user can trust the binding embodied in a certificate is limited by the ability of the users to ensure the authenticity of the key used to verify the signature.* In order to rely on the authenticity of that public key, it is necessary to develop the infrastructure of a trusted service. In order to remove the barriers and threats to electronic commerce, this trusted service must provide:

- **Registration**
 - Validity check of organisation or individual
 - Co-operation with other trusted services
 - Training and support for users
- **Key generation and management**
 - Public Key generation
 - Key distribution
 - Key back-up; Key recovery and Key escrow[§]
- **Certificate Management**
 - Certificate generation
 - Certificate distribution
 - Certificate revocation
 - Certificate Revocation List Management
 - Directory management
- **Other additional services which engender trust, could also include:**
 - Time stamping - where messages received and sent have an indelible digital imprint of the date and time of sending or receipt
 - Policy management
 - Network security analysis and consultancy

[§] A way to perform key recovery, is to split a decryption key (typically a secret key or an RSA private key) into several parts and distribute these parts to "trustees". When required, the trustees use their part of the keys either to reconstruct the missing key or simply to decrypt encrypted communications directly. Key escrow is where a copy of the decryption key is filed with an appropriate "escrow agent" with access by law enforcement agents.

For the trusted services to be effective, these depend on several factors, which include:

- The practices followed by the body providing the trusted services in authenticating and verifying users.
- The operating policy, procedures, practices and security controls followed in issuing and otherwise managing certificates, described in detail in a Certification Practice Statement (CPS) published or referenced by the organisation.
- The subject's obligations (for example, in using and protecting the private key)
- The stated undertakings and legal obligations of the organisation providing the trusted services (for example, warranties and limitations on liability)
- Publication of the certificates and certificate revocation list (CRL) for easy access by all relying parties

Trusted services can be provided by a Trusted Third Party (TTP) or a Certification Authority (CA).

4. 4.1 Certification Authority and Trusted Third Parties

A Certification Authority (CA) issues public key certificates and affirms an individual or organisation has the right to use that public key. The certificates are signed by the CA's own private keys after verifying the user's identifying information contained in the certificates. The Certification Authority will digitally sign each certificate and make the user's public key certificate available through an accessible directory available to all certified users. A definition of a Certification Authority is that it:

"might be an external company such as VeriSign that offers digital certificate services or they might be an internal organisation such as a corporate IT department. The Certificate Authority's chief function is to verify the identity of entities and issue digital certificates attesting to that identity " 94

There are many ways that a certification authority (CA) can operate including:

- **Internal Certification Authority** - An organisation can operate its own CA to certify its own employees, their positions and their levels of authority, as well as external stakeholders such as suppliers and customers.
- **Outsourced employee Certification Authority** - A company might contract with an outside firm to provide a certification service for its own employees.
- **Outsourced customer CA** - A company might contract with an outside firm to provide a certification and verification service for its customers and other outside parties with which it has communications and relations
- **Trusted Third Party (TTP)** - This is an independent third party organisation that operates as a CA and offers the security and authentication services already defined.

In 1993, the European Commission gave the following definition of a Trusted Third Party (TTP) as :

*"A trusted third party is an impartial organisation delivering confidence in electronic transactions, through commercial and technical security features. A TTP supplies technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means"*⁹⁵

A Trusted Third Party can act as a Certification Authority. The main difference between a TTP and a CA, according to the European Commission, within a planned Public Key Infrastructure is that, a TTP will become registered and recognised by government legislation. A TTP has the authority to keep private keys stored and to supply these keys when necessary for key escrow. The UK's Department of Trade and Industry (DTI) in 1997, saw the CA as "*a body which mainly issue certificates for electronic signatures*"⁹⁶, the Trusted Third Party as "*the generic term for bodies that provide one or a variety of cryptography services to their clients*"⁹⁷. The DTI also saw a third body involved in the process, Key Recovery Agents who would be

*"responsible for facilitating the "recovery" of encrypted data"*⁶. National and international government legislation and standards have and are still being developed since 1997, and there is still much work to be done before a definitive policy to support PKI is developed. The advances and developments in legislation and policies are detailed in chapter 13.

4.5 Trusted Service Providers

In order to develop a practical trusted authentication service, it is necessary to understand not only the technological and theoretical aspects discussed above, but also to look at the total service provided commercially. That is, to identify and analyse the requirements from a trusted service provider, the Trusted Service/authentication Provider market, the services they provide and the practices and standards they follow as they stood in 1997.

4.5.1 Users of a Trusted Service

Availability of PKI security services, were still in the embryonic stages of its development life cycle in 1997. There were three main market segments for providing a trusted service:

- **Business-to-business** - the characteristics of this segment are lower volume higher value service (in terms of charges for the service). The services required by this sector are tailored to the organisation's needs and the verification procedures and sources of information are centred around the company and its performance in the business community, certified companies are able to communicate with each other securely and in confidence. It is also expected that other added value services such as consultancy and training would be required by this sector.

- **Business-to-individuals** - the characteristics of this segment are higher volume and lower value where the verification procedures and sources of information are centred around the individual. In this sector, the banks and

credit card companies are particularly active in the development of a means of securely buying and paying for goods over the Internet.

- **Individual-to-individual** - the characteristics of this segment are very high volume lower value, where the verification procedures depend on the degree of trust. This sector is envisaged to be controlled by large semi-governmental institutions such as the Post Office.

4.5.2 Trusted Services Organisations 1996/7

This section will outline the main players in the CA market, the services they offer and their strengths. As of 1996/1997, competition was not well developed and it was still unclear how the market will develop. Potentially, any number of bodies and organisations could emerge as authentication and security providers as an extension of their existing service or as a separate start-up. For example,

- **Internet Service Provider** - who would offer authentication services with Internet connectivity
- **Security Software Developer** - providing the software and the supporting authentication service
- **Semi-official Organisations** – such as local government, chambers of commerce
- **Independent Certification Authorities or Trusted Third Parties** - using commercially available software, but providing an independent verification, authentication and administration service

In 1997, the trend was that certification authorities were being set up either in association with trade organisations such as Chambers of Commerce, public bodies such as the Post Office or European Union and security software developers.

4.5.2.1 The Main Commercial Providers of Trusted Services

In 1996/7 there was very little published information about the certification authority market. By looking at the players operating in 1997, we can divide CAs into two main categories,

- a) **CA DEVELOPED AUTHENTICATION SOFTWARE** - which provide the authentication infrastructure service, design and develop their own authentication software.
- b) **CA LICENSED AUTHENTICATION SOFTWARE** - which develop an authentication infrastructure based on commercially available software.

There were relatively few players in each of the categories and these were mainly American companies who had taken the lead. The leading players are identified in the following section by category and geographical origin.

a) CA DEVELOPED AUTHENTICATION SOFTWARE

One of the main players in the overall CA market in 1997, Verisign, was in this category. This began when Netscape contacted RSA Data Security (the encryption software producers) to run a CA on its behalf called the RSA Certification Services, issuing certificates for Netscape servers. In 1995, RSA created Verisign as a spin off of its certificate services division funded by strategic partners which included AT&T, Microsoft, First Data, Reuters, Schlumberger and Softbank among a long list published by Verisign themselves. Verisign, the largest CA and industry leaders, by 1997 had a customer base of 400,000 individuals and 14,000 web sites globally. Verisign estimated that they issue 15,000 new certificates a day, the majority of these were issued to individuals in the USA based on their having an e-mail address. As recognised market leaders, Verisign⁹⁸ were setting industry standards, the main features included:

- physically secure premises with guards, CCTV, tamper-proof enclosures and biometric access controls
- secure networks with a firewall, auditable video-taped key generation, and storage of keys separate from the network.

- Interoperability and compatibility with 50 different programmes
- 24 hour a day, 7 day a week personal customer service by a “live” representative
- the development of digital ID’s on smart cards
- SET** compliant VISA branded digital certificates
- the sole provider of digital certificates to NOVUS a US financial institution with 40 million members and 2 million merchants in the US.
- developing their own security software
- a “Premier Business Partners Program” - where authorised ISP’s act as distributors offering Verisign Digital ID’s to their customers
- a “Technology Partner Program” - where Independent Software Vendors build and promote commercial products which use Verisign’s Digital Authentication Services
- aims to install electronic commerce authentication system “in several international locations this year [1997]”

Other players in the US include:

- **GTE’s CyberTrust** - the certification authority for American Express and Mastercard. They also outsource security services and sell the technology for CA’s.
- **CertCo** - a subsidiary of Banker’s Trust. It was being consulted by the SET committee to recommend software, hardware and the business procedures for managing the digital certificates of the different credit card and bank brands. CertCo have recently become the Root CA (i.e. certifying card brands) for Visa and Mastercard.

The market however was not totally dominated by American players, although they were in the majority. Other European players in this category included:

- **BelSign** - claimed to be Europe’s first CA offering on-line certificate management services both issuing and managing the digital certificates. In

** Secure Electronic Transmission

1997, the service was available only to Belgian users but it was planning to expand its services to Luxembourg. The company was founded in 1996 by the National Federation of Belgian Chambers of Commerce and Industry leading and/or participating in national and European Trusted Third Party projects, based on industry-standard public key management technology and NetVision, one of Belgium's leading providers of commercial enterprise-wide Internet security solutions. In 1997, they were joined as shareholders by three Belgian investment companies - GIMV, Bruficom and Technicom. The Certification Practice Statement is based on that set up by Verisign adapted to Belgian Law. Belsign are also in partnership with Dunn and Bradstreet providers of information on companies world-wide.

- **UNISA (UNINETT)** - is a certification authority based in Norway, there is little information available of this company but initially is developing as part of the ICE-TEL project (a research project involving educational institutions around Europe).

b) CA LICENSED AUTHENTICATION SOFTWARE

Again, for this category, the US were the main leaders in this market. They include,

- **Trade Wave** - a trade authority on-line CA based on Entrust Technologies security software, the leading commercial software provider at the time.
- **Bell Global Solutions** - also based on Entrust Technologies software. There is little information available about this company.
- **TriNet Services** - an Internet presence provider and certification authority also based on Entrust Technologies software. Again there is little information available about this company.

In the UK at this time, the only known commercial Certification Authority was **Card Clear**. They were a digital certification service provider currently recognised by the banking industry as a “trusted third party” issuing digital certificates to retailers, merchants and individuals for credit card transactions over the Internet according to SET specifications. University College London had also set up a non-commercial country level CA for academic and research organisations.

Figure 11 illustrates the state of the CA market in 1997 according to the information available and its relevance to the UK environment.

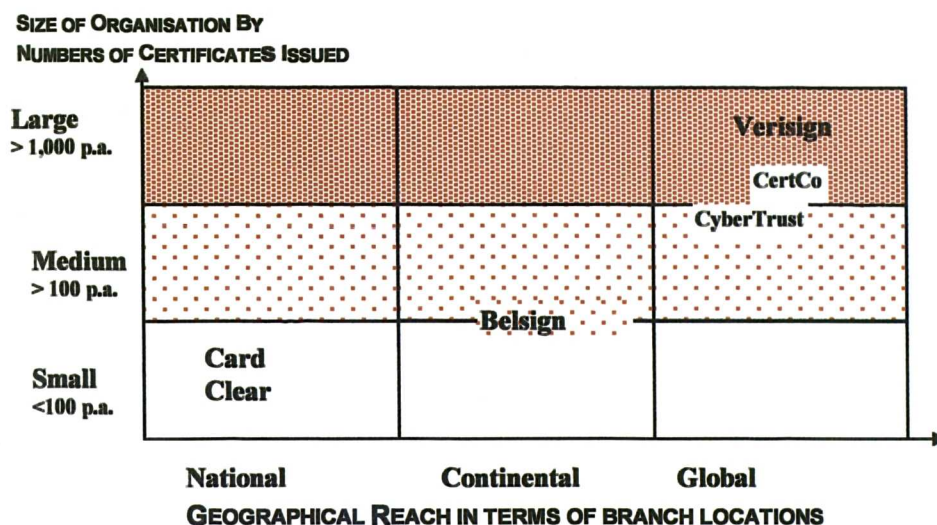


Figure 11 . The Main Commercial Providers of Trusted Services

It shows that Verisign, CertCo and CyberTrust are in a strong position in the market at that time and since they are either subsidiaries of, or are receiving backing from global brands (such as Master Card, Visa, American Express, GTE) they are or can relatively easily develop an international presence. They already have the technology, the infrastructure, the strategic partnerships and the practice statements in place and because the Internet opens up the global market, there are no real geographical barriers preventing any of the players operating in the UK.

4.5.2.2 Trusted Services

The kinds of services available for the client-side digital certificates (a certificate that identifies an individual to a particular key) by the market leaders Verisign, are supported by Microsoft Internet Explorer 3.0 and Netscape Navigator 3.0 and other SSL^{††} and S/MIME^{‡‡} based applications. The service consists of 6 main elements⁹⁸:

^{††} Secure Sockets Layer - a general purpose protocol for sending encrypted information over the Internet

^{‡‡} Secure Multipurpose Internet Mail Extensions - a standard for sending encrypted e-mail with attachments over the Internet

1. **Registration** - for class 1 certificates, all that is needed is the name and e-mail address, so only the fact that the e-mail address exists is validated. For class 2 certificates, full personal details are required including full name, address, e-mail address, date of birth, social security number, driving licence number, contact numbers, employer details and previous address. The user must also confirm they have read and agree to the CA's Certification Practice Statement.
2. **Authentication** - the CA authenticates the user's details according to their CPS. Once this is done, a unique Personal Identification Number is given to the user.
3. **Key creation** - The browser/MIME supporting application creates a public/private key pair. The user's public part of the key is signed by the CA and stored in the CA's public directory.
4. **Certificate acquisition** - Certificates are downloaded from the certification authority via HTTP. The browser/MIME supporting application can then use the certificate.
5. **Secure Storage** - the browser provides a place to store the private key that is secure usually as an encrypted file. Future versions of these will allow keys to be stored on floppy disks or smart cards.
6. **Revocation** - Keys are revoked when a compromise occurs and usually requires the certificate's serial number, class and Personal Identification Number for revocation.

In the first half of 1997, only Verisign offered a comprehensive series of certificates and services, which seemed to be setting the standard for the industry at large. The kinds of certificates and services, which were available commercially at the time, are summarised in Table 10.

CLASS OF CERTIFICATE AND DESCRIPTION OF CHECKING PROCEDURES	VERISIGN	BELSIGN	CARD CLEAR
Class 1 - verifies unique name and accurate e-mail address . This is usually for casual WWW browsing and e-mail	\$6 p.a.	Free	
Class 2 - third party verification of name address and other information using a consumer/business database ^{§§} . This is used for intra company e-mail, on-line subscriptions or on-line purchasing.	\$12 p.a.		£10 p.a. ^c
Class 3 - Class 2 plus personal presence before a local registration body. This is used for inter company e-mail, electronic banking, high value purchases and information services.	\$24 p.a. ^a \$290 p.a. ^b		
a. for individual use b. for companies or web servers with a \$75 annual renewal fee thereafter c. an initial fee of £10 is required for applications to be notarised by a solicitor.			

Table 10 . Commercially Available CA Certificates and Services

These services were largely in the experimental and development phase, where the majority of certificates that were issued were in the Class 1 category, offering minimum security and authentication, only that the e-mail address existed.

4.6 Certification Authority (CA) Infrastructures

This is an area that was also still in the early stages of development. As of 1997, there was no definite certification authority structure that had emerged in practice. However, a number of models describing the process of verifying and authenticating a Certification Authority⁹⁹ had been suggested, based on two main structures, the hierarchical and the cross certification structure.

^{§§} Dunn & Brad Street, Inter NIC and other commercial authorities also commercial credit databases.

4.6.1 The Hierarchical Certification Authority Structure

The Hierarchical Certification Authority structure includes a top level body that certifies lower level bodies and so on until it reaches the end user level.

One of the first infrastructures suggested was that of the PEM (Privacy Enhanced Mail) in 1993. This was based on a top down hierarchical structure, where the top level CA is a non-profit making international Internet-related organisation certifying policy CAs and distributing a root public key for widespread use. At the second level are Policy CAs certified by the root CA. These would register with the root CA and publish a statement of their policy regarding certifying users or subordinate CAs. Lower level CAs would represent particular organisations, organisational units or geographical areas. The PEM⁹² structure specified three types of policy that may be associated with lower level CAs,

- the organisational CA, issuing certificates to individuals affiliated with an organisations e.g. students of an educational institute
- the residential CA, issuing certificates to individuals based on a geographic location
- the personal CA, where the certification does not claim to associate the name in the certificate with a particular persona or entity.

The PEM protocol also had a name subordination rule, where no lower level CA could ever certify entities whose names were not subordinate (according the X.500 naming specifications) to the CA itself.

For example a company CA could only issue certificates for its own employees. This was very restrictive since within PEM infrastructures, organisations would not be able to incorporate a number of their subsidiaries or International branches within their CA. Also the fact that the root CA at the top of the hierarchy was needed to verify certificate chains was felt to be too restrictive. Especially since it was impossible to verify root CAs starting from the user's own domain, which would likely be more secure and the initialisation and key pair update would probably be more efficiently managed.

Another example of hierarchical CA structures, is the global hierarchy model. This involves international and national government bodies in the process of authenticating certification authorities. The diagram in Figure 12, illustrates the structure.

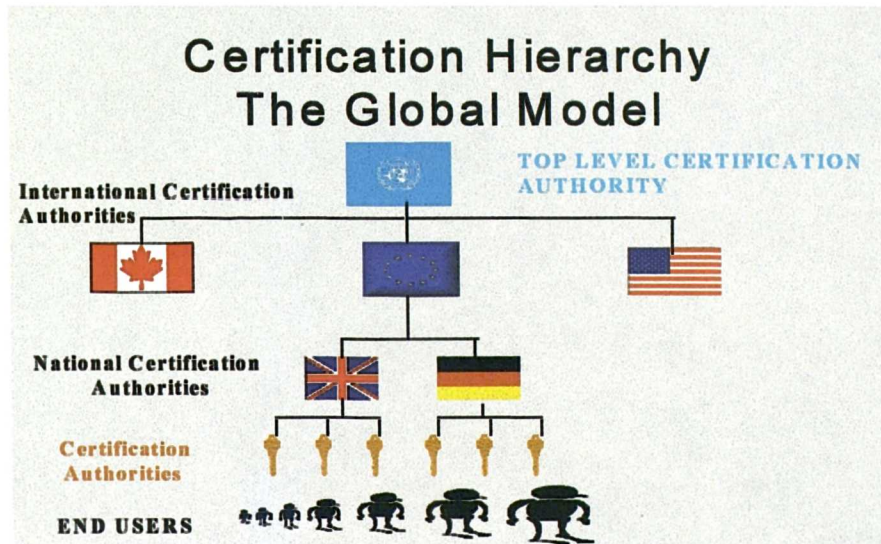


Figure 12 . The Hierarchical Certification Authority Structure

In this model, the Global Certification Authority would be administered by the United Nations which would sign the keys of the National Certification Authorities who in turn would certify the keys of the lower level Certification Authorities. Below this level, are both the corporate key hierarchies and encryption services provided to private individuals.

With this model, a universal standard would have to be developed, which would create an environment of trust for global commercial electronic interaction and document exchange and would help in establishing electronic communication as the socio-economic norm. Much co-ordination and co-operation among world governments would be needed. It is hard to envisage that a level of co-operation and agreement could ever be achieved between the different nations in the world.

Alternatives to this global model, is an industry hierarchy. Where an international industrial body would certify national industrial bodies, which in turn would certify its corporate members who in turn would certify individual end users. These could be Chambers of Commerce, International Car Manufacturers etc. The advantage of this

is that these bodies are already set up as trusted entities and could introduce authentication as an added service. However, one of the major problems would be that there would be a series of industry sector CAs that were relatively isolated unless a standard of certification across industry sectors could be established.

4.6.2 Cross Certification Authority Structure

In this model, the Certification Authorities cross certify each other's keys which enables users authenticated by a Certification Authority in one area or country to be trusted by users authenticated by another Certification Authority. This totally eliminates the hierarchical structure as can be seen in the Figure 13.



Figure 13 . The Cross Certification CA Structure

The main disadvantage of this model, is that in practice cross-certification is not effective for establishing trust among a large number of CAs. The main reasons being the problem of CAs as commercial competitors and so there is little motivation to comply with and promote each other's business plus compatibility and co-operation issues such as:

- Legal indemnities and liabilities
- Certification standards
- The documentation of procedures and agreement of the Certification Practice Statement
- Loyalty and service towards their own certificate holders and cross certified holders

4.7 Policies Governing Cryptography and TTPs

This section will look briefly at the policies and regulations on cryptography and regulation of trusted third parties. It is particularly important in this project to include this information, since the export and use of encryption software over a certain key length (over 40 bit) might be illegal without permission from the government in certain countries. Similarly, certain procedures and regulations governing trusted third parties (for example key escrow^{***}) might be introduced. All these factors could potentially jeopardise the whole project and a summary is included here.

In 1996 and 1997, international organisations were beginning to try and work together to develop common policies and regulations with regards to the use, export and control of cryptography and its supporting services. These organisations included the Organisation for Economic Co-operation and Development, the European Union, the G-7/G-8, the Council of Europe, and the Wassenaar Arrangement. In all of these, the U.S., with the support of the UK Government, led efforts to gain international support for restrictions. Opposition to these efforts, was led by Germany and the Scandinavian countries. The following section will summarise the positions of the respective bodies on the issues of cryptography.

In 1996, the U.S. government approached the OECD^{†††} recommending that it adopt key escrow as an international standard. The OECD was severely divided by the proposals with France and the United Kingdom supporting the US position, but the Japanese and Scandinavian countries against. In March 1997, the OECD issued its Guidelines on Cryptography Policy¹⁰⁰ emphasising "voluntary, market-driven development" of cryptography and included a strong principle in support of privacy protection. The OECD recommendation was a non-legal, non-binding agreement that identified the basic issues that countries should consider in establishing cryptography policies at the national and international level. The OECD felt that these guidelines played an important part in the development of the Global Information Infrastructure

^{***} Key escrow/recovery was a concept promoted by the United States government, whereby the use of strong encryption would involve a third party such as a government agency or a licensed company to hold the keys and provide them to a government agency when requested. Escrow was first introduced in the U.S. in the Clipper Chip in 1993.

^{†††} The Organization for Economic Cooperation and Development (OECD) a Paris-based international body of 29 countries.

(GII) and Global Information Society (GIS) where national policies could be harmonised at the international level to meet the needs of global technologies and applications. They felt that international consultation and co-operation was necessary since failure to co-ordinate national policies at the international level could introduce obstacles to the evolution of national and global information and communications networks and could impede international trade. The guidelines, which governments would adopt and businesses, individuals and law enforcement officials would apply in safeguarding electronic transactions, communications and data storage, are summarised as eight basic principles for cryptography policy:

- i. Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.
- ii. Users should have a right to choose any cryptographic method, subject to applicable law.
- iii. Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.
- iv. Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.
- v. The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.
- vi. National cryptography policies may allow lawful access to plain text, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.
- vii. Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.
- viii. Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

In October 1997, a European Union (EU) report took issue with the US's policy of encouraging key escrow and recovery schemes. The report stated that *"restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks,"*¹⁰¹ adding that key escrow^{‡‡} systems *"would not . . . totally prevent criminals from using these technologies."*¹⁰² On the issue of "back door" mechanisms giving law enforcement and intelligence agencies the right to read the plain text of encrypted messages, the report said that if such systems are required, they *"should be limited to what is absolutely necessary."*

The G8^{§§§} was active in discussing encryption policy again at the urging of the United States and in 1996 agreed to:

*"accelerate consultations, in appropriate bilateral or multilateral fora, on the use of encryption that allows, when necessary, lawful government access to data and communications in order to, inter alia, prevent or investigate acts of terrorism, while protecting the privacy of legitimate communications"*¹⁰³.

In June 1997, the G8 agreed to support the adoption of the OECD guidelines and recommended that all states

*"develop national policies on encryption, including key, management, ... consistent with these guidelines [allowing] lawful government access to prevent and investigate acts of terrorism and to find a mechanism to co-operate internationally in implementing such policies"*¹⁰⁴.

The Council of Europe^{****} approved a recommendation to limit strong cryptography in their member states on September 8, 1995,

*"Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary."*¹⁰³

^{‡‡} Key escrow/recovery was a concept promoted by the United States government, whereby the use of strong encryption would involve a third party such as a government agency or a licensed company to hold the keys and provide them to a government agency when requested. Escrow was first introduced in the U.S. in the Clipper Chip in 1993.

^{§§§} The Group of 8 (G-8) is made up of the heads of state of the top eight industrialised countries in the world.

^{****} an inter-governmental organisation of 40 West European member countries

The US also tried to influence members^{†††} of the Wassenaar Arrangement¹⁰⁵ (WA)^{†††} to restrict the export of conventional weapons and "dual use" technology^{§§§§} including security software to certain other excluded countries. The Wassenaar Arrangement attempted to impose and regulate international export controls by limiting the key lengths of encryption products that can be exported without approval licenses. However, the WA was designed to exchange views and information on international trade in conventional arms and dual-use goods and technologies where members commit to adjust their national export control policies to adhere to the WA Control Lists, but this commitment is discretionary and not mandatory. Thus, the list of excluded countries covered by each participating state's own national sanctions varied widely and so it was in the case of encryption software.

Thus, the legal situation as it stood in 1996/7 was extremely uncertain. In the US, key escrow was to be made mandatory, use of encryption of key length over 40 bits was trying to be restricted and the export of cryptography software was illegal without a special export licence. France restricted the use of encryption with use of 128 bit encryption (such as PGP) requiring government permission and the law made key escrow mandatory. In Taiwan, the government had stated in 1997 that it was planning a key escrow system.

In Germany, free export and use of cryptography was encouraged with the German cabinet extending the data protection law¹⁰⁶ to include the use of digital signatures and computer networks. In December 1997, Belgium amended its 1994 law to eliminate its provision restricting cryptography.

In the UK although it had been the strongest supporter of the US's efforts to promote key escrow and limitations on encryption, no government policy had yet been issued on the subject. The Conservative Government began a Public Consultation on the

^{†††} 33 industrialised countries - Argentina Australia Austria Belgium Bulgaria Canada Czech Republic Denmark Finland France Germany Greece Hungary Ireland Italy Japan Luxembourg Netherlands New Zealand Norway Poland Portugal Republic of Korea Romania Russian Federation Slovak Republic Spain Sweden Switzerland Turkey Ukraine United Kingdom United States

^{†††} The WA replaces the former Cold War-era Coordinating Committee on Multilateral Export Controls (COCOM), a group of 17 countries that placed restrictions on the export of certain technology to countries of the former Warsaw Pact and other communist states.

^{§§§§} "Dual use" technologies are those that can be used for both commercial and military purposes, such as supercomputers and high-level computer security access software.

regulation of Trusted Third Parties (TTPs) for the provision of encryption services in 1996. In 1997, the Science and Technology minister announced that in Britain, like the US, it would be compulsory for anyone providing cryptography services to give keys to a government-run central repository. At the beginning of this project, all the indicators were that legislative restrictions would be introduced governing the setting up and operation of trusted third party services. Thus, potentially, the security service being introduced would have to be licensed by government approved agencies and that its procedures would have to include key escrow made available to government agencies.

4.8 Conclusions

Having reviewed the technology and elements of a security and authentication infrastructure, the components finally selected are based on their ability to fulfil the project's requirements of providing trust, integrity, non-repudiation and confidentiality of electronic data both in transmission and in a static state. The technological elements of the service identified in this review are encryption, digital signatures, digital certificates, authentication and key management. Since the design and development of the security technology is beyond the scope of this project, elements identified as components of a security solution will be used as technological selection criteria for commercially available software in the next chapter.

Looking in more detail at encryption, the service being offered by existing security and authentication providers is founded on public key cryptography technology - either their own or that of a third party commercial software provider (the leaders are Entrust Technologies). Since the focus of this project is not technological and although there are other systems and infrastructures available (for example Kerberos^{****}), it is beyond the remit of this project to test and evaluate them all. A public key based infrastructure was suitable for the requirements of this project and is a criterion for evaluation of the software in the next chapter.

^{****} A system developed at MIT which authenticates users to services in a distributed system. Users are authenticated by user name and password and are issued with "tickets" which are valid for one login session.

By 1997, no model for an authentication infrastructure had clearly emerged. This review of existing security and authentication providers, indicated that apart from the technology, value needed to be added to the service in the form of trust. Despite the uncertainties regarding government regulation and policy about cryptography and Trusted Third Parties, it was decided that the advantages gained from the total security solution, far outweighed the potential disadvantages which might be occur with an introduction of government legislation regulation.

Drawing on these findings, the next chapter will define the elements used to build an environment of trust for the security and authentication service most suitable for SMEs. It will also finalise the stages of development of a security and authentication solution to provide SMEs with physical electronic data security and a supporting infrastructure for the distribution, use, establishment and independent verification of a wide number of users and holders of public keys.

Chapter Five

Designing a Security Solution - Primary Research

5. Designing a Security Solution - Primary Research

This research project involves two stages - the design and implementation of a security and authentication infrastructure. This chapter deals with the design of the infrastructure and is based on a process of formative evaluations made from secondary data gathered in the previous chapters and primary data collated in this chapter.

It is important to note here that the following information was collected between September 1996 - January 1997 and in some instances does not accurately reflect the current situation, especially the growth of commercial organisations and the security software available. The model developed in this study is based on these findings.

5.1 Authentication Infrastructure Lifecycle

The stages of development of any product or service, consists of a series of iterative processes, illustrated in Figure 14.

Research Project Lifecycle Stages



Figure 14. Stages in the Research Project Lifecycle

The processes relevant to the design and development of the authentication infrastructure are Analysis, Design and Development.

5.2 The Analysis Stage

Analysis in this case, included both primary and secondary data sources. The secondary data sources have been discussed in chapters 2 and 4. The secondary data, indicated that public key encryption was the most reliable, effective and transportable method of securing electronic data. Not only this, but at the time this project was underway, it was also believed that a whole economic, political, legal and commercial infrastructure would be built around this technology. Thus, the service being designed here is based on public key encryption technology. The most important criteria for the design and development of an authentication infrastructure, is to create an environment of trust in which potential users have total confidence and understanding of:

- Security and integrity of the technology they are using
- Verification procedures being used
- Integrity of the organisation providing and administering the security

5.2.1 Primary Research

The aims and objectives of this study are centred around the impact of electronic data security on Small and Medium-sized Enterprises (SMEs) in the Greater Manchester region. Thus a series of primary research studies were undertaken to elicit business opinions about the Internet and security. The qualitative research included a series of focus groups, and the quantitative research included semi-structured telephone interviews with 145 local businesses. Full details of this research are included in Appendix 6.

The results of the primary research showed that in December 1996/January 1997, there was not much Internet uptake by SMEs (around one in three) in the region. This figure was consistent with other national surveys¹⁰⁷. The primary research identified SME non-adopters of the Internet to be mainly concentrated in the traditional sectors of manufacturing, such as textiles, chemicals, toys and machinery. These were the laggards and there was a serious danger that these industries might disappear or be forced to change their processes by their trading partners, suppliers, or customers.

The main reason being that as the new technology filters down into the technologies of products and business processes, if they do not implement changes the knowledge they have will become obsolete in the new techno-environment.

SME early adopters of the Internet were found to be in the higher tech industries. In the service sector - training and recruitment, advertising and promotion, transport areas in which the UK economy is relatively strong. The modern manufacturing sector, were mainly electronics and software developers.

Attitudes towards technology and the Internet were largely that technology is making work easier, and increasing efficiency in sales and marketing tasks but that for smaller non-technology oriented companies, there is little training and a sense that staff must "muddle along". The results of this research, revealed that a large gap in knowledge, training and technical support exists between SMEs and the IT industry.

The main priorities for the majority of SME non-users and first time users is:

- obtaining basic information about the Internet and what it can do for a business
- the costs and potential savings involved
- practical training on how to use the Internet

Very few respondents were aware of data security and, for the majority, it was not a priority in their business strategy and growth plans. When questioned about security and whether they felt that security over the Internet was an issue, 90% of Internet users felt it was not an issue, since they believed none of the information they were sending over the Internet was so confidential that extra security measures needed to be introduced. When discussing e-mail security, few participants from both the telephone interviews and focus groups outside the IT industry were aware of potential security breaches.

Some users when told of the potential security pitfalls of the Internet, felt that measures would be taken only when they had experienced a security problem. Inexperienced users felt that security was not a priority, but rather that learning how to use the new technology to its full potential and “properly” was more important. Of the 10% who were aware of security, half were using the Intranet for security purposes, one was using Lotus Notes and one company had a firewall installed.

This information was extremely useful in the development of the security and authentication infrastructure. It indicated the lack of awareness of electronic data security issues among the potential users of the service. This underlined the need for creating a service which not only engendered trust in its users, but one that is simple to use and had an infrastructure for educating and supporting potential users in electronic data security issues.

5.3 The Design Phase

From the analysis stage, the criteria necessary for creating a data authentication infrastructure were identified. The design phase involved the planning of the security service to be offered. A whole security authentication infrastructure had to be built, not only providing a technological solution, but also to create an environment of trust and integrity which included the operating procedures and policies of the service provider, education and training of the users, and a corporate identity of trust, honesty and virtue. This would allow users to gain confidence and trust in the service and the security provided. Figure 15, illustrates the layers needed to create that environment.

The Security Authentication Infrastructure
Creating an Environment of Trust and Corporate Integrity

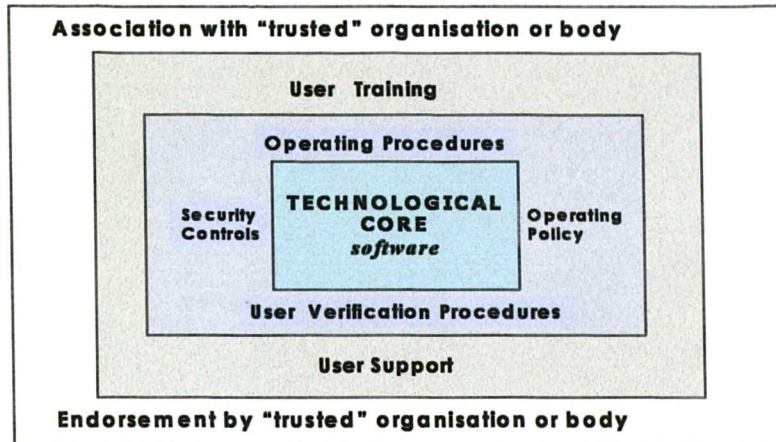


Figure 15 . Components of a Security and Authentication Infrastructure

The stages of setting up this trusted service provider (Trusted Third Party) infrastructure, to support secure transfer and storage of electronic data were:

- (i) Evaluation of technology/software available
- (ii) Developing working practices, policies and procedures based on the examination of existing trusted third parties or Certification Authorities.
- (iii) Developing a programme for user support and training
- (iv) An endorsement by or association with a "trusted" body

The following sections will deal with each of these stages in detail.

5.3.1 Software Evaluation

The design and development of software is not within the remit of this project. However, since encryption technology is at the core of the service being developed, it is necessary to select a software package that fulfils the objectives and goals of the project. The kind of evaluation that took place was inductive not deductive¹⁰⁸. That is, each software package available was tested on the basis that instances of program execution were observed time and again and, from this observation, conclusions about the software's suitability were drawn. There were two stages in the evaluation process, broad screening and narrow screening, the methodology and findings of each stage are detailed in the following section.

5.3.1.1 Broad Screening

There were two main stages in the evaluation of encryption software. The first stage, was a broad screening process, based largely on non-academic and purely practical criteria. However, these limiting factors mirror any commercial environment and could not be seen as having a significant impact on the results of this project.

Using Basili & Rombach's¹⁰⁹ GQM (Goal/Question/Metric) paradigm, this provides an informal mechanism for identifying and measuring attributes as they related to a specific goal. In this case, the goal (G) was defined in the following terms¹¹⁰:

- **Purpose** - To identify encryption software for evaluation in order to incorporate it into the security and authentication infrastructure
- **Perspective** - Examine the product from the viewpoint of the project manager (researcher)
- **Environment** - An academic project with limited financial, hardware and human resources. No funding is available for purchasing software licenses, new hardware or support staff.

The criteria were seen as relating to three particular areas where questions (Q) had been posed:

- **Product** - Does the software exist, which would be of a standard able to support a whole public key infrastructure
- **Process** - Can the software be imported into and used in the UK with or without a licence.
 - If necessary is it possible to obtain a special export licence to import and use the software in the UK*.
 - Do the manufacturers of the software agree to have their software used in such a project including publication of detailed performance assessments.

* If originating in the USA or connected to the USA, a special munitions export licence is needed. No such licence is needed for import from other EU or commonwealth countries.

- **Resources - Are extra resources needed in terms of:**
 - Cash funding for software/licences
 - Personnel to run the software
 - Equipment/Hardware to run the software

If any of the above questions relating to Product and Process returned one or more "no" replies, or any of the questions relating to Resources returned one or more "yes" replies, then the software had failed to comply with the project goal and was thus rejected. This was the **metric (M)** by which the criteria were screened.

5.3.1.1.1 Broad Screening Findings

As with the Internet and the Certification Authority sectors, the encryption software sector was also in the very early stages of its lifecycle at the beginning of the project. The software packages available, were evaluated based on the broad screening criteria and metrics defined in section 5.3.1.1. The results of the evaluation are summarised in Table 11. The ticks and crosses in the table, indicate whether the overall metric of each criterion is positive (tick) or negative (cross).

SECURITY SOFTWARE		BROAD SCREENING CRITERIA	
		ACCEPTED	
Baltimore Technologies - Ireland	Product - Yes		X
	Process - No - Although no licence was necessary, the organisation refused access to the software for an initial evaluation as a comparator to Entrust software on the basis that it would not be favourable. They also did not want detailed performance assessments to be published.		
	Resource - N/A		
Demming Internet Security	Product - Yes		X
	Process - Yes		
	Resource - Yes - Payment for licences at \$872 for 10 users \$20,435 for 250 users		
Entrust software - from Canada's Northern Telecom V3	Product - Yes		✓
	Process - Yes		
	Resource - No - The organisation is willing to allow us the use of the software with 250 licences for a period of one year		
Pretty Good Privacy - Phil Zimmerman USA V2.6.2.i	Product - Yes		✓
	Process - Yes		
	Resource - No - this software is universally available free of charge		
SecureAttache - Australia Beta version	Product - Yes - although the stage of production was at the beta version stage		X
	Process - No - Although the software can be imported and used in the UK, the CA was based in Australia and thus not practical to be used		
	Resource - Yes - Australian CA		
SECUDE - Software from the ICE-TEL project	Product - Yes		X
	Process - Yes		
	Resource ¹¹¹ - Yes - this was too complex to run with current resources. Expert personnel were needed to run the software.		
KEY: X negative metric - this was a negative criteria for the project ✓ positive metric - this was a positive criteria for the project			

Table 11 .Broad Screening of Security Software

From the broad analysis stage, the main types of software carried forward to the next stage for more detailed evaluation were **Pretty Good Privacy (PGP)** and **Entrust Technologies**. The results of this evaluation allow the security and authentication infrastructure being developed here, to implement the most effective and user friendly software according to the evaluation criteria described. This evaluation concentrated on the end-user layers of the certification authority structure and technical features. To evaluate the technological operation of the software from the CA administration perspective was beyond the scope of this project. Some work has already been done on the evaluation of the selected software *"from a security and administrator point of view"¹¹²*, the conclusions of this study have been included in the software evaluation process described in Table 11.

5.3.1.2 Narrow Screening

The second stage was a narrow software evaluation screening process, based more specifically on academic research related criteria. The software evaluation methods used were based on Boehm's quality model¹¹³ and the approach proposed in an IEEE computer society report¹¹⁴, influenced by software metricist, JA McCall¹¹⁰. A number of high level factors were identified for measurement. Factors such as usability, trust management, key management and functionality were seen as being central to the requirements of the software under evaluation. These factors were determined by lower level, dependent criteria, which were easier to measure. These criteria were broken down into metrics - measurable components or simple attributes which could be numerically characterised (such as size, time, cost) and were based on an intuitive understanding of the attribute. Other attributes were slightly less simple and more heavily dependent on subjective assessments, such as attractiveness, ease of understanding, comprehensiveness of the interface. Table 12 summarises the factors, their related criteria and the metrics of the attributes.

SECURITY AND TRUST SOFTWARE EVALUATION		
FACTORS	CRITERIA	METRICS
1. OPERABILITY	Set-up and Installation	Medium of software - Ease of installation - Procedures for installation
	Compatibility	Hardware requirements and optimal configuration
	Integration	Integration with other applications
2. KEY MANAGEMENT	Key Generation	Procedures for key generation
	Key Distribution	Procedures for key distribution, means of distribution
	Key Storage	Location of key storage and accessibility
	Revocation	Availability of Certificate Revocation list and maintenance
3. TRUST MANAGEMENT	Confidentiality	Encryption - key length, algorithms used
	Non- Repudiation	Digital Signature, Time stamping features
	Integrity	Detection of tampering - hash algorithm
	Authentication	Procedures for verification of keys
4. USABILITY	Operability	Ease of Use - Navigation around the screen - Numbers and complexity of key strokes used
	Training/Support	Support literature, On-line help
	Communicativeness	Interface - layout of screen, ease of understanding instructions/functions and key strokes

Table 12 . Measures for Evaluating Security Software

The information obtained from this second stage of software evaluation, was largely objective and based on measured facts. It was also highly structured and thus the "experiment" could be replicated relatively easily for evaluation of any number of software packages. With each criteria, the metric would be described and where it was positive (for example, it was easy to use, or it could be integrated into other applications) then it would score a positive metric indicated by a tick. Similarly, if it was a negative metric it would score a cross. The overall score would include the total metrics for each criterion. This is discussed in more detail in the next section.

5.3.1.2.1 Narrow Screening Findings

The evaluation at this stage took place at the University and was carried out by the author in accordance with the stated criteria. The computer system used was a Pentium 133MHz with a one gigabyte hard drive and 32Mb of memory. The connection was to the University network running on Ethernet at 10Mb with TCP/IP protocol. The results of the PGP and Entrust software evaluations are tabulated in the following sections. The ticks indicate a positive metric, the crosses a negative metric. These metric measures for the attributes, in some instances, are based on the subjective judgement of the researcher and in others, are based on the actual existence of technological features. The different criteria are not weighted in any way, as it was considered that all the criteria listed are equally as important in providing a technologically sound service and usable infrastructure of security and authentication. Having said this however, since this project is centred around creating trust and providing an easy to use service, two of the overall factors which must score highly to warrant selection are Usability and Trust Management.

5.3.1.2.1.1 Evaluation of PGP

The PGP software that was available for evaluation at the beginning of this project, was the PGPV2.6.2i. It operated on a single user MSDOS machine where the user had control. PGP was known as "guerrilla software", the main reason being that it has been promoted and used to circumvent the US government's attempts to suppress its publication and mass use since with this software, electronic data could be secured even from the US government's attempts at interception. The way the software was used supported an organic, decentralised and non-institutional security infrastructure.

Evaluation of Pretty Good Privacy (PGP)

1. OPERABILITY	
INTEGRATION	
▪ PGP is a stand-alone program that does not integrate itself into or with any other application	X
COMPATIBILITY	
▪ PGP only requires MSDOS and a low specification computer with a small amount of memory and minimum processor power. Although with higher specification hardware, there will be an improvement in software performance	✓
SET-UP AND INSTALLATION	
▪ The PGP software is freeware and can be downloaded from a number of Internet sites. It does not originate from any discs and thus there is a risk that the software is corrupt or virus infested which itself compromises security and the environment of trust	X
▪ There is no installation shield or manual to follow installation instructions.	X
▪ The PGP program files are manually copied onto the hard drive and run from within DOS	X
OTHER FEATURES	
▪ It automatically compresses data before encrypting, which saves time in transmitting a document or space and storing it electronically.	✓
▪ Secure delete facilities ensure that deleted data cannot be reconstituted into its original form by re-writing encrypted data onto the original data and deleting.	✓
2. KEY MANAGEMENT	
KEY REVOCATION	
▪ The whole PGP system is based on self-management. The user herself locates, adds, removes, copies and views other correspondent's public keys. This key management system potentially can compromise the whole system since revocation or withdrawal of compromised keys is dependent on the user checking for key compromise, if necessary issuing a "key compromise certificate" and distributing it to other users. Because of the informality of the system, the user has to either contact other users personally to inform them of the breach thus launching a chain, or through the use of an "Electronic Bulletin Board" which is based on random or opportune access by other users.	X
KEY GENERATION	
▪ Once the software is installed on the computer, then the public and private keys are easily generated and protected by a pass phrase created by the user. There is no restriction on the length or characters in the pass phrase.	✓
▪ PGP allows users not to have a pass phrase for creating and subsequently accessing the private key, which compromises the whole system.	X
▪ Users can create as many key pairs as they desire	X
KEY DISTRIBUTION	
▪ The user must maintain and manage their own personal public and private keys. That is, make the public key available to other users by their own means (personal, postal, mail exchange or uploading keys to public bulletin boards or directories)	X
▪ Users must personally exchange keys either by e-mail, post or face-to-face.	✓
KEY STORAGE	
▪ There is no permanent and central repository for storing public keys.	X
▪ Where Electronic Bulletin Boards are used, access is random and maintenance of these bulletin boards is also random and not rigorous.	X
▪ The user must maintain public keys in their own public key ring which resides on their machine.	
▪ PGP is not designed to support a large number of public keys. The maximum manageable number is about 100 keys	X
▪ The user must check regularly for revocation of compromised keys as this could have a knock on effect for keys signed by a compromised key stored on the user's key ring.	X
▪ There are no formal means of checking the validity of other public keys over a period of time.	X
KEY: X negative metric - this was a negative criteria for the project ✓ positive metric - this was a positive criteria for the project	

3. TRUST MANAGEMENT	
NON REPUDIATION - Digital signature Time Stamp	
<ul style="list-style-type: none"> ▪ A digital signature is created and includes a time-stamp within the signature. This however can be circumvented by the user since the time stamp is set to the computer's own clock time which can be altered by the user. 	✗
<ul style="list-style-type: none"> ▪ Messages can be sent as clear text with a digital signature. 	✓
<ul style="list-style-type: none"> ▪ Digital signatures can be nested within a document, which allows the same document to be passed around many users who can subsequently digitally sign the document and forward it. 	✓
<ul style="list-style-type: none"> ▪ Signatures are automatically verified when a signed message is received. PGP verifies the attached signature with the signatures held on the user's own public key ring. 	✓
<ul style="list-style-type: none"> ▪ Any document can be digitally signed if the user's private key is available to the machine being used 	✓
CONFIDENTIALITY - Encryption	
<ul style="list-style-type: none"> ▪ The technological specification of the software is a combination of RSA/conventional hybrid encryption. Because RSA is too slow to be used on large amounts of data, RSA is used to encrypt random session keys. It uses a conventional single key encryption algorithm by using a public key algorithm to encipher the conventional session key, then it switches to fast conventional cryptography. It uses IDEA a single-key block encryption algorithm with a key size of 128 bits which is equal to 3100-bit RSA key. This is nearly 4000 times faster than 1024-bit RSA algorithms. As already discussed, 128-bit encryption will take millions of pounds of resources to break the code. 	✓
<ul style="list-style-type: none"> ▪ PGP allows the deletion of the plain text data when it is decrypted to ensure that confidential data remains confidential to authorised people. 	✓
<ul style="list-style-type: none"> ▪ Encryption facilities are in-built in the PGP software. There is no selection of encryption algorithms. The IDEA algorithm is mandatory. 	✓
INTEGRITY	
<ul style="list-style-type: none"> ▪ Message digests (hash algorithm) is included within the digital signature to ensure that the integrity of the message is detected. When a message is received PGP automatically checks the digest to ensure that it tallies with the digest of the message when it was sent. If not then the software indicates that the message was either tampered with, intercepted or altered in some way. 	✓
AUTHENTICATION	
<ul style="list-style-type: none"> ▪ Authentication is an informal process based on self-authentication of/by other users. There are no criteria or procedures for verifying or authenticating key owners. The onus is on the user to verify other public keys. This is done either by personal knowledge and personal exchange of public keys between parties, or PGP allows other "trusted" users to sign correspondent's public keys to provide a degree of authentication. Once trusted people are identified in PGP, then all keys signed by the trusted people will be verified as being valid. But this process is arbitrary and unique to each user 	✗
<ul style="list-style-type: none"> ▪ PGP keys do not have expiry dates, and are valid indefinitely and any number of keys can be generated for any one person. This causes problems in verification and authentication of key users and holders. 	✗
4. USABILITY	
OPERABILITY	
<ul style="list-style-type: none"> ▪ Instructions and options difficult to understand 	✗
<ul style="list-style-type: none"> ▪ The instructions are largely based on MSDOS code which makes it eminently impossible to use by users with little or no computer knowledge. 	✗
TRAINING AND SUPPORT	
<ul style="list-style-type: none"> ▪ Documentation is unsophisticated, difficult to read from a presentation point of view, but the content is informative although aimed more at the knowledgeable user. 	✗
<ul style="list-style-type: none"> ▪ No on-line help features or third party support line. 	✗
COMMUNICATIVENESS	
<ul style="list-style-type: none"> ▪ Visually unattractive with a plain black DOS background and coloured text. 	✗
<ul style="list-style-type: none"> ▪ Design is unsophisticated and basic where screens are plain text this makes it hard to navigate 	✗
<ul style="list-style-type: none"> ▪ Input into the options is manual typing and it is difficult to understand the correct syntax for inexperienced users. 	✗
<ul style="list-style-type: none"> ▪ Overall impossible for non-experienced users to use 	✗
<p>KEY: ✗ negative metric - this was a negative criteria for the project ✓ positive metric - this was a positive criteria for the project</p>	

PGP is particularly weak on usability, key management and authentication. Despite the fact that it is stronger on technologically centred criteria of integrity, confidentiality and non-repudiation, overall PGP proved unsuitable for this research project.

5.3.1.2.1.2 Evaluation of Entrust software Client 3 for Windows 95

The available Entrust software evaluated was version 3 for Windows 95. The software company was founded in January 1994, as a business unit within Northern Telecom (Nortel), the Canadian telecommunications giant. In December 1996, Entrust Technologies was formed as an entrepreneurial spin off of Nortel and was incorporated in the state of Maryland. Entrust Technologies Limited, the Canadian subsidiary was incorporated in the province of Ontario on December 20, 1996¹¹⁵. The software runs on the Windows 95 operating system. The system is based on a Certification Authority controlling the generation, verification, authentication and management of keys. The software is commercially available and is licensed to the users. As previously, the tick indicates a positive metric and the crosses a negative metric.

Evaluation of Entrust software Client 3 for Windows 95

1. OPERABILITY	
INTEGRATION	
▪ Entrust software can become integrated into any other Microsoft Office '95 application	✓
COMPATIBILITY	
▪ Entrust software requires a windows operating system. Each version of the windows operating system e.g. 3.1, Win 95, requires a specific version of the Entrust software.	✗
▪ Hardware requirements are standard computer with a standard amount of memory (32Mb) and a 486 processor. Although with higher specification hardware, the software is more likely to run faster.	✓
▪ A user's profile can be transferred to a UNIX, Windows 3.x or Macintosh so long as the appropriate Entrust software is installed.	✓
SET-UP AND INSTALLATION	
▪ The Entrust software is available from the manufacturer and comes on a variety of media which are virus checked and approved by the manufacturer.	✓
▪ An installation shield and manual, include installation instructions - which are comprehensive	✓
OTHER FEATURES	
▪ It automatically compresses data before encrypting, which saves time in transmitting a document or space in storing electronic data.	✓
▪ Secure delete facilities ensure that deleted data cannot be reconstituted into the original form by re-writing encrypted data on top of the original data and deleting.	✓
▪ The password that is generated is hashed to protect easy discovery of the password	✓
▪ The Entrust programme automatically logs the user off within 1-60 mins (the user may select the option) of inactivity. This provides added security for when the user is temporarily away from the machine, since the user must log in again.	✓

2. KEY MANAGEMENT	
KEY REVOCATION	
<ul style="list-style-type: none"> ▪ The CA revokes keys in the event of : <ul style="list-style-type: none"> - a compromise in security (the keys have or are suspected to have been used by unauthorised persons) - change of the user's personal details - if the keys have been superseded by a new pair e.g. if a password has been forgotten ▪ The CA issues and publishes Certificate Revocation Lists (CRLs) which is regularly updated and automatically referred to every time the user logs onto Entrust software. ▪ The user can work offline and use the keys already stored in their own personal address book. Entrust software ensures that the user understands that the keys have not been checked and might have been revoked since they were last used. ▪ The user is confident that all the public key certificates stored and signed by their CA have undergone the procedures set out in the CA documentation. 	<p>✓</p> <p>✓</p> <p>✓</p> <p>✓</p>
KEY GENERATION	
<ul style="list-style-type: none"> ▪ The Entrust software is commercial and a fee is required to obtain a user license. Once the software is installed on the computer, including the Entrust.ini file, then the Administrator CA must provide the verified user with a reference number, and authorisation code before the user can be registered and keys generated. 	✓
<ul style="list-style-type: none"> ▪ Entrust software has restrictions on passwords which state that it must have at least - 8 characters, one upper case character or number, one lower case character, no repeat of the character, not the same characters or substring as in the user's profile name. 	✓
<ul style="list-style-type: none"> ▪ Users can only create key pairs if authorised by the Administrator 	✓
KEY DISTRIBUTION	
<ul style="list-style-type: none"> ▪ The user must refer to the administrator in the event that their password is forgotten or their profile is lost. The administrator issues the user with new reference and authorisation codes 	✗
<ul style="list-style-type: none"> ▪ The CA makes the public key available to other users by access to an authorised directory 	✓
<ul style="list-style-type: none"> ▪ Users cannot import a certificate signed by another CA with the same name 	✓
<ul style="list-style-type: none"> ▪ User's public key certificates are automatically updated from time to time. 	✓
KEY STORAGE	
<ul style="list-style-type: none"> ▪ There is a permanent and central repository for storing other CA verified users' public keys. 	✓
<ul style="list-style-type: none"> ▪ Users may import non-verified but Entrust software created keys by personally exchanging keys either by e-mail, post or face-to-face. It is made clear that these keys are not certified by the CA. 	✓
<ul style="list-style-type: none"> ▪ The CA maintains public key certificates in a publicly accessible directory 	✓
<ul style="list-style-type: none"> ▪ The CA certificate directory can store and manage a large number of keys 	✓
<ul style="list-style-type: none"> ▪ The user is confident that all the public key certificates stored and signed by their CA have undergone the procedures set out by the CA documentation. 	✓
3. TRUST MANAGEMENT	
NON REPUDIATION - Digital signature Time Stamp	
<ul style="list-style-type: none"> ▪ A digital signature is created 	✓
<ul style="list-style-type: none"> ▪ Messages can be sent in clear text with a digital signature. 	✓
<ul style="list-style-type: none"> ▪ Signatures are automatically verified when a signed message is received. 	✓
<ul style="list-style-type: none"> ▪ Of the two pairs of keys created, one pair is for signing. The private key is for signing and the public key is used for verification of the signature. 	✓
<ul style="list-style-type: none"> ▪ Any document can be digitally signed with the user's private key stored on the machine being used 	✓
CONFIDENTIALITY - Encryption	
<ul style="list-style-type: none"> ▪ The technological specification of the software is a combination of RSA/conventional hybrid encryption. The symmetric algorithms available for encrypting files are CAST-128 (which is the default), CAST-80, CAST-64, Triple-DES, DES, RC2-128 Compatible, and RC2-40 Compatible. 	✓
<ul style="list-style-type: none"> ▪ The RSA key pair used for transferring keys are 1024-bit modulus 	✓
<ul style="list-style-type: none"> ▪ The user determines the mode of output of decrypted and/or signed documents 	✓
<ul style="list-style-type: none"> ▪ There are two pairs of keys created - the encryption keys are made up of a private decryption key and the public encryption key. 	✓

▪ Encryption facilities are in-built in the Entrust software. There are 7 available algorithms from which to select	✓
▪ Entrust software allows the deletion of the plain text data when it is decrypted to ensure that confidential data remains confidential to authorised people.	✓
INTEGRITY	
▪ A hash algorithm is included within the digital signature to ensure that the integrity of the message is detected. When a message is received Entrust software automatically checks the hash to ensure that it tallies with the hash of the signature when it was sent. If not then the software indicates that the message was trustworthy and had not been tampered with, intercepted or altered in some way.	✓
AUTHENTICATION	
▪ The Entrust system is based on a third party CA, controlling management and verification procedures. The user can add, remove, copy and view other correspondent's public keys which have been downloaded from the CA's directory. The onus is on the CA to verify the other public keys. This is done by a series of procedures set out in the CA's policy and Practice Statement.	✓
▪ The user can import Entrust software generated keys which might not have been cross certified by the user's CA. These keys can be imported by the user and the trust is the user's responsibility. The certificate and validation string (which are generated by Entrust software) are required for the imported keys to be useable. For added security, it is recommended that the key certificate is sent by e-mail and the validation string sent separately (either by telephone or in writing). Even if these keys are compromised in any way, the incident would be isolated to that specific key since it is independently verified and not cross-verified by other users.	✓
▪ The user can manage their own list of CA verified recipients in an address book type of process, where users are added or deleted. But ultimately the authentication can be used by the user at any time.	✓
▪ The information on the certificate gives the name, the distinguishing name (i.e. unique identifier of the user such as e-mail address), the CA name and the certificates validity dates from when it was first activated to when it expires.	✓
▪ The certificates issued by the CA have expiry dates, which ensures that the certificate holder is constantly verified.	✓

4. USABILITY	
OPERABILITY	
▪ Instructions and options relatively easy to understand	✓
▪ Selecting options is mainly by pointing and clicking on icons and text.	✓
TRAINING AND SUPPORT	
▪ Documentation is sophisticated, easy to read from a presentation point of view	✓
▪ For any problems with either the user's own certificate or other certificates, then the user must contact the administrator.	✓
▪ Detailed On-line help facilities	✓
▪ Software manufacturers' technical help line	✓
COMMUNICATIVENESS	
▪ Highly dependent on administrators	✓
▪ Visually attractive, clear icons and well presented layout of user interface.	✓
▪ Sophisticated design	✓
▪ Consistent with other point and click applications	✓
▪ Overall relatively easy for non-experienced users to use	✓
KEY: X negative metric - this was a negative criteria for the project ✓ positive metric - this was a positive criteria for the project	

Entrust software is particularly strong on all factors which are necessary for security software on which a Trusted Third Party Service can be built and is particularly useful for this project.

5.3.1.3 Conclusions

The overall metrics of the software evaluation criteria, are summarised in Table 13. Because there are no mathematical weightings, the results from the previous sections are added up and the predominant measures (positive (tick) or negative (cross)) noted.

	PGP	ENTRUST
OPERABILITY		
INTEGRATION	X	✓
COMPATIBILITY	✓	✓
SET-UP AND INSTALLATION	X	✓
OTHER FEATURES	✓	✓
KEY MANAGEMENT		
KEY REVOCATION	X	✓
KEY GENERATION	X	✓
KEY DISTRIBUTION	X	✓
KEY STORAGE	X	✓
TRUST MANAGEMENT		
NON REPUDIATION	✓	✓
CONFIDENTIALITY	✓	✓
INTEGRITY	✓	✓
AUTHENTICATION	X	✓
USABILITY		
OPERABILITY	X	✓
TRAINING AND SUPPORT	X	✓
COMMUNICATIVENESS	X	✓
KEY: X negative metric - this was a negative criteria for the project		
✓ positive metric - this was a positive criteria for the project		

Table 13 . Evaluation Metrics of PGP and Entrust software

Although technologically both pieces of software provide security, the PGP software was too difficult to use by the non-experienced and non-technical user. Using PGP software would support a public key infrastructure within a small community of users where trust already existed among the users, but many sessions to train users would be crucial and users would find the interface unattractive and difficult to understand. Furthermore, a whole support and trust infrastructure would have to be created to use PGP effectively in the context of providing a trusted service to users. Entrust software was by far the more superior in presentation and usability and was selected as the best software to support PKI and the authentication infrastructure in this project.

5.3.2 Controls, Procedures and Policy

The next layer in the design and development of a data security and authentication infrastructure consists of security controls, operating procedures, operating policy and verification procedures. In order to engender trust in the organisation as well as confidence in the security being provided, the Certification Practice Statement (CPS) is made available to all members of the service. The CPS describes the practices and procedures used by the Certification Authority or Trusted Third Party when generating, storing and using its private keys, and issuing, distributing and publishing certificates and certificate revocation lists. It indicates the level of security applied by the CA/TTP to the protection of its keys, certificates, computer systems, and operating environment. It also describes the responsibilities of its customers and end users when generating, storing and using their private keys and the certificates. The CPS can be used to assess the environment of trust and security provided by the Trusted Third Party security service provider.

5.3.2.1 The Certification Practice Statement

The Certification Practice Statement (CPS) is a document that lays out the procedures and processes, which the Trusted Third Party (TTP) will follow in the execution of its service throughout the lifecycle of a digital certificate illustrated in Figure 16.

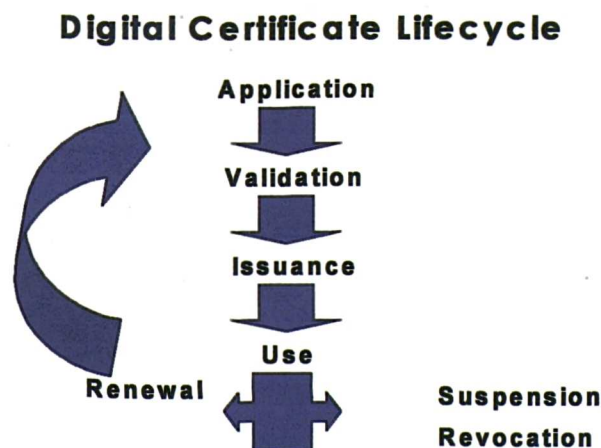


Figure 16 . Digital Certificate Lifecycle

The structure of a CPS had not been standardised at the start of the project, but the IETF[†] is currently working to develop a standard. Some key CPS issues have been documented by experts in the field¹¹⁶ and leaders in the market, such as Verisign. The CPS is part of the trusted third party security service thus, all members should read the CPS in order to understand the level of security being offered. By making the document publicly available, this will allow members to build a relationship of trust with the TTP. The CPS created for this service is attached in Appendix 8 and is based on the work of Chokhani & Ford¹¹⁶. The main areas covered in the CPS are outlined below, but do not reflect the exact numbering system of the sections in the original CPS document.

1. The Community of the Trusted Third Party

This section identifies the infrastructure and stakeholders of the Trusted Third Party. In this case, the TTP organisation was known as the GEMISIS CA and will be referred to as such in this chapter and also in the CPS.

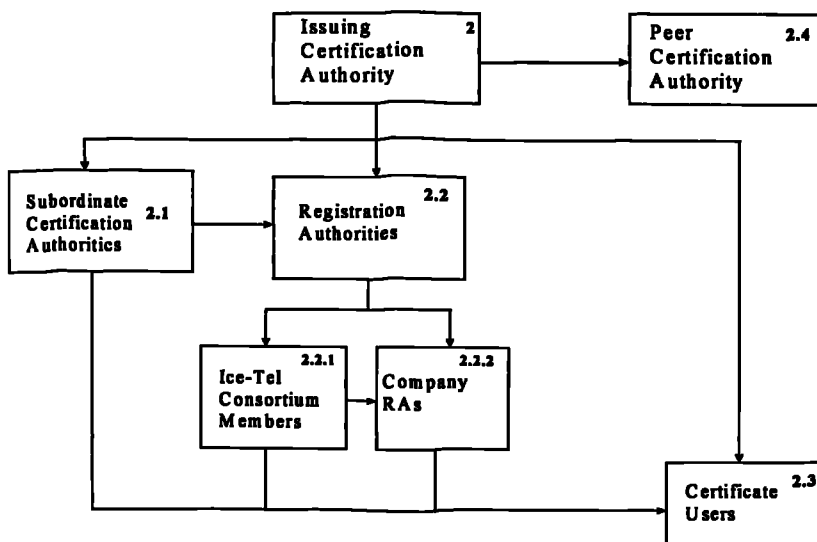


Figure 17 . Certification Authority Community of Subscribers

Here, no top level peer certification authorities have been approved by the GEMISIS CA. A peer CA is one whose CPS for a specific certificate policy has been approved by another top level CA and is willing to have a cross certificate issued by that same top level CA. Neither are there any subordinate CAs - certification authorities which

[†] Internet Engineering Task Force

have been approved to issue certificates by the GEMISIS CA. However, there are registration authorities, which have been authenticated by the GEMISIS CA. In this case, the ICE-TEL[‡] consortium members were personally known to those involved in this project. ICE-TEL¹¹⁷ will have the choice of either allowing the CA to verify the users within the organisation or appoint an internal registration authority (RA) who will verify their own personnel and contact the CA authorising them to issue the new and self-verified users with certificates.



Figure 18 . GEMISIS Certification Authority Infrastructure

2. Applicability of Issued Certificates

This section outlines applicability of the certificates to any document format including text, audio, graphics and video files and also as e-mail attachments. Non-applicability of the certificates includes EDI and electronic funds transfers. This section underlines the technical standards of encryption, digital signatures, hash functions, key management and API (application program interface)[§].

[‡] The aim of the ICE-TEL project is to offer solutions to the problem of security on the Internet as used by industrial and academic research. This will be achieved by support for the usage of secured applications where users need to be certified, by providing a large scale public key certification infrastructure in a number of European countries and by providing all the necessary technology components which allow the deployment.

[§] API is the specific method prescribed by which a programmer writing an application program can make requests of the operating system or another application www.whatis.com

3. Identification and Authentication Policy

This section describes the processes for identification and authentication of the stakeholders, including the registration authorities and end users by the GEMISIS CA. This also included the processes for identification and authentication of end users by the registration authorities. All stakeholders are governed by the ethical policy. The ICE-TEL RAs are authorised and verified by the personal knowledge and relationship of those involved in the GEMISIS CA. All corporate members must have their organisation verified and authenticated. The validation procedures used in this case are based on a generic service being offered on a business-to-business basis. Validation centres on four major areas:

- **Trading references (2)** – this offers information about the trading status of the organisation building confidence that the business exists and the period of time it has existed
- **Banking Reference** – this offers information about the status of the company and its legitimate existence
- **Legal Status** – for registered limited companies, the credentials will be checked with Companies House again building a profile of the organisations legitimacy as a business entity.
- **Site visit** - once the above checks have been completed, then a personal visit to the organisation will take place. This includes personal validation of the organisations' premises and authorising signatory by a member of the CA.

The documentation for the verification of users is included in Appendix 10. Once an organisation has been validated by the Certification Authority, it will have the choice of either allowing the CA to verify the users within the organisation or appoint an internal Registration Authority (RA).

The internal RA will verify their own personnel and contact the CA authorising them to issue the new and self-verified users with certificates. Selection of the Registration

Authority is based on a number of criteria and includes close consultation with the end-user organisation. The criteria include that the RA has,

- a blemish-free record,
- been at the organisation more than 18 months
- full understanding of digital certification
- access to personnel records

All this, will ensure that the RA is trustworthy and follows the procedures laid out by the GEMISIS CA. Once the RA is selected, then he/she must administer a set of procedures to validate the end users such as checking personnel records, physical identification of proposed certificate users, keeping up to date records of users situation.

The GEMISIS CA also audits the RAs and end-users within 6-12 months of their membership to ensure that they are following the correct procedures and upholding the infrastructure of security and trust.

Revocation conditions for certificates issued to both RAs and end-users include if - the company has ceased to exist; there is an un-notified change of address; passwords have been compromised, lost, forgotten; the user has left the company; the RA issues a revocation notice to the GEMISIS CA.

Updated lists of revoked certificates will be published by the GEMISIS CA daily at 8pm in a Certificate Revocation List (CRL), which automatically removes revoked users from the directory of authorised users. All members are advised to connect to the CA directory regularly to ensure their records of authorised users are up to date and correct.

4. Key Management Policy

This section defines the security measures taken by the GEMISIS CA to protect its keys and passwords. This includes Key generation and validity period, storage, usage, archiving and destruction procedures for both the CA and the users.

5. Security Policy

This section outlines non-technical and technical security controls. The non-technical controls for the CA include:

- Physical security - buildings, access points, window and equipment security (bars and chains).
- Software security - password creation and usage procedures.
- Procedures - the roles and responsibilities of the personnel in the CA.
- Personnel Control - the training and recruitment methods and programmes.

The technical controls include:

- Computer controls - login procedures, access controls, back-up procedures
- Network controls - audit tools, network monitoring tools (Securities Administration Tool Analysing Networks), existence of firewalls, no FTP/remote login or access or rhost files, limited TCP access.

Security controls for the RA include the non-technical software and personnel controls and, for end-users, the software controls.

6. Operations Policy

This section describes the operating procedures for the certification keys. This includes:

- Revocation - the CA will act one hour after notification , where CRLs are issued daily at 8pm, and are valid until midnight the following day. The RA and end user must notify the CA immediately of any key compromise or loss. Client software is configured to download CRL's from the GEMISIS CA directory the first time each day that the client PC attaches to the Internet.
- Key compromise - for the CA, compromise will have been deemed to have occurred if there was unauthorised entry to the building or equipment, theft of equipment, or some other security breach. For the RA and end users, compromise occurs when there has been unauthorised access to the user's profile (EPF/PFE) or the password has been made available to anyone other than the user. In these cases, all breaches will be noted and logged.

- **Audit Logs - of CA network, Unix and Entrust software server usage and access. User organisations must keep a log of authorised users for 3 years.**
- **Archives - CA Audit logs, back-up keys, CRLs and certificates issued will be kept for 5 years.**
- **Disaster Recovery - procedures to be carried out in the event that keys are compromised.**
- **Compliance Audit - the CA will undergo a procedure compliance audit, by an independent and internationally recognised expert at least once a year. A report of the findings, will be submitted by the auditor and recommendations and commendations will be noted and acted upon where necessary.**
- **Confidentiality Procedures -at no time will back-up user decryption keys, super-user and Entrust software passwords or the CA's private keys be made available to anybody except a law enforcement officer with a relevant court order from the law enforcement authorities. In this case, the user will be informed as soon as possible.**

7. Legal Provisions

This section describes the CA's liabilities, warranties, limitations and arbitration procedures.

The CPS includes more detail of each of the areas discussed above. It also includes the documentation, which must be completed by the community of users. Each member of the CA must have read the CPS before using the digital certificates. In reality though, the CPS is a large document with highly technical and legal language, which most readers will not read. Thus it is important that training, information and support is provided to potential users at the outset to ensure, at least, a basic understanding of the concepts and infrastructure they are using.

5.3.3 User Training and Support

The third layer in the process for creating an environment of trust and corporate integrity is user training and support. The findings from the primary research at the analysis stage, showed that there is a predominant lack of knowledge, awareness and understanding about security issues amongst Internet users and non-users. This has had a negative impact on the implementation of this new technology by SMEs.

Part of the process of creating a secure and trustworthy environment, is to impart knowledge and raise awareness among users. If the users do not understand the system or the framework of what they are doing, then security will be open to compromise and the whole system will fail. Thus, training procedures have been devised and are fully documented in Appendix 11. These include training for the engineers responsible for installing the software and the users on-site, the administrators of the authentication infrastructure and the technical support. The training procedures for end-users includes a training session explaining security and electronic data security as well as a demonstration of the software (Appendix 12).

The next stage is a one-to-one training session with each user at the computer terminal showing the software in operation. A manual is also available for reference by the users (Appendix 13), and support is either by e-mail or telephone.

5.3.4 Corporate Associations and Endorsements

The final layer in the creation of the data authentication infrastructure is the association with or endorsement by a "trusted" organisation or body. Looking at the CAs currently in existence, they are in some way endorsed by or associated with organisations. For example, Verisign and Microsoft/ Schlumberger/ Softbank/ Reuters; Belsign and the Association of Belgian Chambers of Commerce. The CA in this case, was associated with and funded by the multi-million pound European Union Regional Development Fund supported GEMISIS project¹¹⁸. This project is also endorsed by the Manchester Chamber of Commerce and is an optional service available to customers of The Virtual Chamber¹¹⁹ (TVC).

5.4 Conclusion - The Authentication infrastructure Trust Model

Unbreachable security is the core of building trust for any Trusted Third Party authentication infrastructure. All the procedures and the technology used by the TTP must be fully functional, totally secure and auditable in order to establish confidence in the service. This, however, is not the only component in building an environment of trust. Potential users must be confident in the organisation that is providing the authentication infrastructure as well as the actual service they receive. In order to build trust, the security service being offered must be unquestionable in terms of procedures, operating policy, security controls, CA policy**, technology and personnel.

While it can be argued, that the detailed information contained in the CPS might compromise the CA's security, *this information is necessary to build up an environment of trust and confidence in the authentication service being provided.* Not only this, but the information in the CPS is presented in basic detail. The bulk of the information is already available in the Entrust software manuals, which accompany the software and the CPS will be available to subscribed members and must be kept confidential by them. The security model, which has been developed here, will be tested in the next chapter.

** A named set of rules that indicates the applicability of a certificate to a particular class of application.

Chapter Six

Implementation of the Security Service - Case Studies

6. Implementation of the Security Service - Case Studies

This chapter is divided into three parts, each of which describes a case study. The case studies are a source of data for identifying and developing a framework and best practice guide for the implementation and usage of the security solution designed. The case studies will provide information to answer the following research questions:

- Does the security solution developed actually work when used by SMEs?
- What benefits are achieved for SMEs by secure use of the Internet?
- What is the process of implementation of the security solution by SMEs?

The criteria for the selection of commercial organisations as case study candidates for this project are:

- Small/Medium sized companies with fewer than 250 employees and a turnover of less than £20 million per annum.
- The company has to be in a European Union (EU) designated objective II area. Objective II areas are designated areas in the respective EU member states, which need regeneration and qualify for ERDF* funding. Such areas in the North West of the UK, include Manchester, Salford and Liverpool (Appendix 3).
- The company has to be connected to the Internet with e-mail facilities.

Contact was made with potential companies through the Chamber of Commerce, as part of The Virtual Chamber of commerce project (TVC¹²⁰). In order to maintain the confidentiality of each participant, the actual company names are altered.

* European Regional Development Fund - See appendix 3 for more details

Only two companies volunteered to take part in the pilot and both fulfilled the pre-requisite criteria. These were:

- I. **Company D** - an adhesives manufacturer
- II. **Company T** - a chemical analysis company

Because of the limited number of companies agreeing to take part, no additional criteria were needed to select the required 10-12 individuals from a larger pool of potential companies.

A third organisation which volunteered to implement the pilot, is included in the total number of case studies although it does not fulfil all the project criteria.

III. **University X** - Department Y and Department Z

University X is a large organisation with over 500 employees and is partly government funded. It is a large bureaucracy and, although it does not fit the criterion of size, it does fulfil the criteria of being in an objective II area and has Internet and e-mail facilities. The impact on the overall research findings of including University X is twofold. Firstly on the level of use of the security solution, University X users are equally valid subjects as SME users, since there will be a random mixture of abilities, experiences, skills and opinions from a potential population of all employees regardless of size. On the implementation level, the findings must be used with caution because the decision making and implementation processes are more influenced by the size and structure of an organisation.

A similar structure for each case study has been used to ensure a continuity in methodology and to enable direct comparisons to be made. The data gathering process for each case study is arranged in two distinct parts and are summarised in Figure 19.

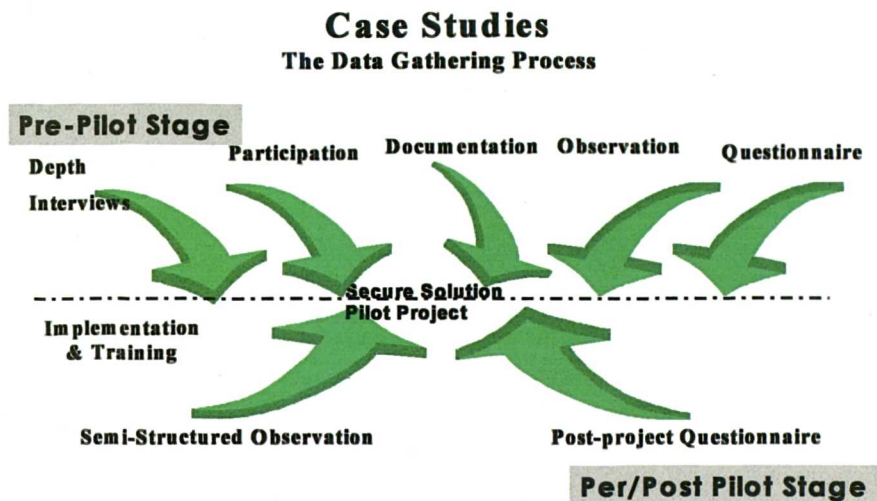


Figure 19 . Case Study Data Gathering Process

- 1) **The Pre Pilot Stage** - data is gathered before implementation of the pilot and includes background information about the organisation, its decision-making process, its current systems and processes, and the stages involved in the decision to implement the pilot authentication infrastructure.

- 2) **The Per and Post Pilot Stage** - data is gathered during and after implementation of the pilot. It includes a description and analysis of the actual stages in the implementation and usage of the pilot authentication infrastructure. This will cover four main areas:
 - (a) **User Profiling** - the participants in the pilot will be profiled, with a description of the relevant user attributes including age, experience and computer usage. This provides valuable information in determining the different types and categories of user and whether these factors have an impact on the system's success or failure.

 - (b) **User Attitudes to Technology** - Drs. Larry Rosen and Michelle Weil¹²¹ identified three measures - computer anxiety, computer thoughts and computer attitudes - as contributing to technological discomfort and technophobia. Their research found that this is a large contributing factor

in the success or failure of implementing technology projects. User attitudes, thoughts and anxiety to technology are gathered in this project, based on questionnaires psychometrically tested by Rosen and Weil (Appendix 9).

(c) Task Performance Measurement – measurement of time, cost and labour efficiencies for the transfer of documents by the traditional process compared with the transfer of the same documents using the security solution. Analysis of these measurements will indicate the benefits or drawbacks of the security solution. If participants return to the traditional method during the pilot, this will be judged a sign of failure of the security solution.

(d) Usability Statements – to determine the degree of usability of the new system, recommendations for usage and possible future improvements.

(e) Future Implementation - to assess the overall success or failure of the project and the potential for improvement and implementation.

The three case studies are described in detail in the subsequent sections. A full analysis and synthesis of these findings into a theoretical framework is developed in Chapters 9 and 10.

6.1 Case Study I - Company D

Company D was selected for participation in this research project having fulfilled the ERDF criteria; that it was an SME and that it was geographically located in the European Union Objective II area. Most importantly, the organisation's participation was voluntary, which was a rare response amongst SMEs. As we shall see, this outlook stemmed from the fact that the company had decided to embrace interactive technology shared between manufacturers and customers and recognised the security issues this raised. Few other SMEs were foresighted enough to embrace technological data interchange in that way.

This case study involved tracking and evaluating the process of implementation and usage of the Trusted Third Party security service developed in the first stage of this project.

6.1.1 Methodology

The aims of this study were to gain an understanding of the ethos of the organisation; its people; their attitudes towards technology, the introduction of new technology; an analysis of existing business processes and the stages of implementing new technology. Because the study involved a large cross section of the organisation, it was necessary to use a variety of methods to gather data and information to ensure that the limitations of one method had less of an impact on the overall validity of the findings. Since the organisation's participation was voluntary and very co-operative, it was possible to use a number of data gathering methods.

6.1.1.1 Unstructured Observation

The researcher was invited to attend a series of decision-making meetings over a period of 6 months. During these meetings, the researcher recorded the relevant information from the meetings as they related to the implementation process within the organisation and project under research.

6.1.1.2 Semi-Structured Depth Interviews

The researcher was allowed access to a number of key personnel in the organisation who were internal stakeholders. Semi-structured face-to-face interviews were conducted on the premises and were largely informal, lasting between 10-30 minutes. Open-ended questions were used to encourage a free flow of information both to gather facts, as well as opinions and attitudes of respondents on issues that might not have been considered by the researcher. These are summarised in Table 14.

INTERNAL STAKEHOLDERS			
	USERS	TECHNICAL ADMINISTRATORS	CORPORATE STRATEGIC DECISION MAKERS
SOURCE:	Sales Staff Administration Staff Product Development Staff Others	IT Director IT Personnel	Sales manager IT Director Customer Services Manager Product Development Manager
AREAS OF QUESTIONING:	How the current system operates Attitudes towards the current system (including any problems or benefits of using the current system) Attitudes to change Training issues and other IT related issues.	Technical specification of the current system Attitudes towards the current system (including any recurrent technical problems or benefits) Plans for future IT development IT training and user support	Corporate aims and objectives Plans for growth and development Training

Table 14 . Areas of Questioning for Internal Stakeholders

6.1.1.3 Documentation

Documentation was used as a source of factual information to support the data gathered from the respondents directly and in meetings. The researcher was allowed access to:

- Minutes of meetings relating to the implementation of a new IT system prior to the company's involvement in this project.
- Agendas and minutes of all IT strategy meetings

- IT systems documentation and manuals
- Corporate brochures and other published promotional literature
- Organisational archives such as hierarchy diagrams and departmental structures

6.1.1.4 Observer Participation

Because of the open and co-operative nature of the organisation, a relationship of trust developed, where the researcher was at times appointed the role of consultant. On the positive side, this offered the researcher the opportunity to gain a high level of access to the internal stakeholders as well as the IT systems of the organisation. On the negative side, as discussed in chapter 3, observer participation has a downside in the potential for the researcher to manipulate events and the reduced ability of the researcher to observe and record the information, due to the time taken in participation. These potential disadvantages were overcome by giving impartial information based on technological facts; and by limiting researcher participation by awaiting the hosts' invitation to participate and contribute.

6.1.2 Findings

In order to assess the process involved in the planning and implementation of the authentication infrastructure in an organisation, it is necessary to understand the framework in which the organisation operates, formulates strategies and makes decisions. The findings reported in the following section, are structured in a way that will firstly describe the business ethos of the organisation including its corporate strategy, its IT strategy and decision making process and its current IT systems. A brief analysis will be made of each area in practice. Then, the planning and implementation of the secure electronic data solution will be described and analysed.

6.1.2.1 The Organisation and Its Background

The host company is a water based adhesives and glue manufacturer founded in 1974. Its growth has been rapid, averaging a rate of about 20% per annum with a turnover of £24 million in 1997. Today (February 1998), the company employs just over 100 people ranging from sales and administrative staff to scientists, manufacturing and customer service staff. Its growth is customer service driven, built around product quality and serving the customer's needs and requirements. The company develops a relationship with its customers as business partners, which contributes to the strategic long term growth of the organisation. The company's strength is in its product range, the application and specification of which is tailor-made to the customer.

The company's strategy is to continue and grow its success into European markets and improve customer services. It is aiming to build stronger relationships with customers, by becoming an integral part of its customers' value chains - notably via automatic ordering facilities between the customer's stocks of adhesive and its factory production. It wants more efficiency in the administration of the organisation, allowing salesmen to input orders directly and give customers what they want, when they want. It also wants to ensure that while this open integration of systems adds value to customer services, the confidentiality and security of the company's data, such as the price lists, customer accounts and product formulae, is not compromised.

6.1.2.1.1 The Business Philosophy

Company D has a business ethos in the organisation which, it believes, puts it ahead of the competition and is a source of their success. It encompasses six major areas:

- **People** – the aim is to encourage an enthusiastic and committed workforce, which will reduce staff turnover and enhance a sense of responsibility to the company.

- **Market** – company D do not deal with solvent-based adhesives and so have a strong hold in water-based adhesives, especially for cigarettes and packaging. Its strength is offering tailor made solutions not just products to customers. For instance, one customer requires four different types of adhesive for one envelope and company D provides all of these as an integral package instead of, for example, offering 3 and expecting the customer to source the other elsewhere.
- **Investment** – the company’s policy is to invest in product quality, good customer service and technology.
- **Innovation** in the development of new products and manufacturing techniques to improve the quality and reduce costs. It currently has over 400 products ranging from water based adhesives to veneers and decorative surfaces.
- **Independence** – the company has built flexibility into its organisation, to respond to customer needs independently of suppliers and other parties in the value chain.
- **Results** – the company is results orientated, ensuring customer satisfaction for building relationships and getting a partner for life.

The competition is mainly dominated by subsidiaries of multi-national corporations such as Unilever, and ICI. Company D feels it has achieved competitive advantage through technological innovation in products and services and also because it is easier for them to react since they are smaller and their market is concentrated mainly in the UK.

6.1.2.1.2 The Business Philosophy in Practice

The above strategy is borne out in fact, where innovation and investment in technology has driven financial growth. The aims and objectives of the organisation are encompassed in the business processes that have been developed.

For example:

- **Customer Service and Relationship building** - Company D has its own fleet of vehicles which ensures reliable deliveries. It operates a Just-In-Time system, which is integrated into the customer's stock control system. This allows the company to control its own stocks of raw materials as well as its customers' stocks. This also allows them much flexibility and independence from third parties. A large number of its customers have been customers for over 5 years.
- **People** - all new employees, no matter what their job description, undertake the same induction training to make sure they experience every department and understand the organisation fully. The company has a relatively low turnover of staff: the majority of core staff have been in the organisation for over 5 years. Company D offers training and support to its network of agents in Ireland, Germany and Holland.
- **Investment** – the company has recently invested in an emulsion plant for raw materials. This is intended to minimise reliance on external companies in the value chain, in order to enhance efficiency, quality control and speed of delivery. The company also has a policy of investing in technology.
- **Product Quality** - the company operates a quality control system - with a process monitoring computer and audited processes complying to ISO 9002 standards.

Not only has this organisation got a corporate strategy, but it has developed a functional business strategy which has assimilated the aims and objectives, goals and ethos of the organisation into everyday working practices. If we look at the organisational structure, we can better understand how corporate strategy is formulated and translated into operational procedures throughout the organisation.

6.1.2.1.3 Organisational Structure

The organisational structure of the company is a mixture of the typically hierarchical and the divisional¹²² as illustrated in the Figure 20. The company owners still play a major part in running the company. They have appointed directors who are also shareholders.

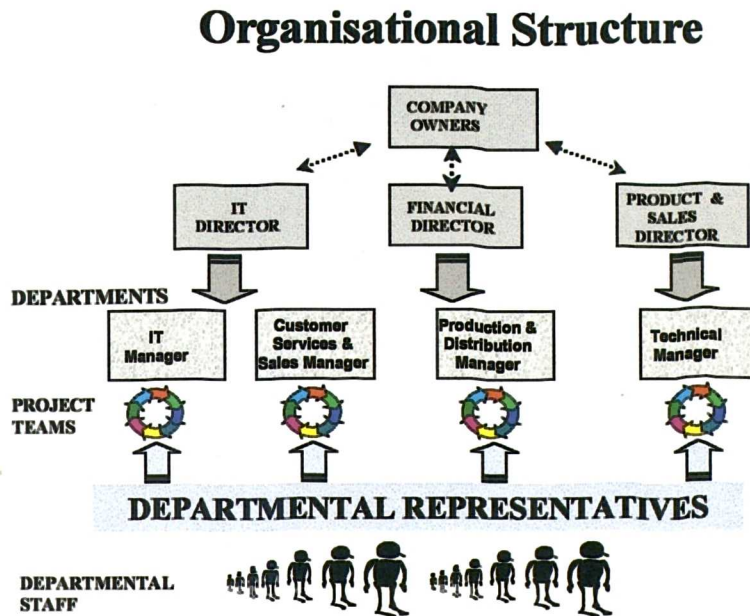


Figure 20 . Company D Organisational Structure

As a group, these stakeholders devise corporate policy and business plans. The directors who also act as departmental heads/managers, have a "hands on" role in the organisation and thus have an awareness of operational and functional issues in different areas of the organisation. Below this level, the organisation is run almost as special business units (SBUs), which is a flat team based structure, with no real hierarchy. The project teams are often inter-departmental and include employees dependent on their knowledge and expertise rather than their position in the organisation. The degree of control and authority is maintained by the inclusion of directors/managers. This kind of structure seems to have developed from the organisation's custom of nurturing employees and promoting a sense that they have a stake in the company. This has reduced staff turnover, increased loyalty and productivity as can be seen from the number of employee turnover which is less than 5% per annum and growth in sales has risen by an average 20% per annum.

6.1.2.2 The Current Processes

As we have seen, this organisation is Porterian¹²³ in its ethos, which sees competitive advantage through technology and innovation. Once the corporate and business strategy of the organisation is discussed and determined by the directors of the company, it is filtered down to the respective departments for implementation. This next section will analyse how operational strategy is formulated within the organisation. The focus here will be on the development and implementation of IT related plans in general and security of electronic data in particular.

6.1.2.2.1 The Decision Making Process

The overall decision making process within the organisation mirrors its organisational structure illustrated in Figure 21. On a monthly basis there is a meeting of directors to determine and review corporate and business strategy. The respective directors then take their allotted projects or feedback to their respective teams for development into a specific departmental strategy.

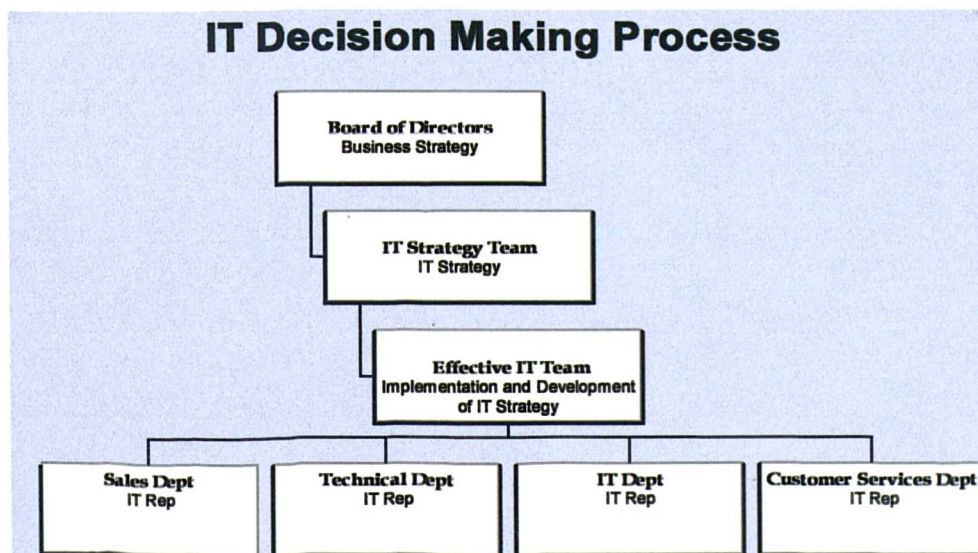


Figure 21 . Company D's IT Decision Making Hierarchy

Looking specifically at the IT decision making process, the IT director holds a monthly meeting with the IT team who translate business decisions and strategies into IT decisions and strategies. They make decisions on the types of IT resources required such as a computer system, database function, automated sales documentation system. From here implementation plans are developed by the team. The IT team consists of personnel from each of the departments usually in senior positions, with a knowledge of or interest in IT. This combined with the experience and knowledge of their own departments ensures that each department's requirements and opinions are taken into account at the planning stage. Specifically:

- The TQM manager makes sure any new system takes into account ISO 9000 procedures and requirements.
- The sales department ensures their need for automated sales documentation, origination and processing is met.
- The technical department ensures their need for keeping secure electronic versions of sensitive product formulae is met.
- Customer services ensure their need for processing and delivery of customer requirements and needs
- The IT department design and implement an integrated system with the minimum use of resources and maximum utility throughout the organisation.

Once the IT decision has been made, then it moves down to the Effective IT Team, where again there is a representative member from each department. This team makes a decision on the actual implementation of the above plans and decisions, testing and piloting the systems, problem solving and other IT related issues. They report and provide feedback, on behalf of the whole department, on how to improve operations and other user related issues.

The participants in the IT strategy and effective IT teams are often the same and include in both cases, the director responsible for IT. In this way there is continuity in the means of communication and ideas from inception to birth. There is an inherent understanding of the aims and objectives of the system being

designed and implemented. The management style in the teams is a mixture of the directive ¹²² and the conceptual. That is, the team leader who is also the IT director, is oriented towards technical matters; requires a structure in which to work and plan; is autocratic, responds to the oral delivery of detailed information, is effective at getting results and has a low tolerance for ambiguity. He also adopts a conceptual style of leadership in that he is achievement oriented, he is open with his team and has trust in his subordinates and other team members. He is open to team opinions and participation and encourages the team to contribute to decision making and goal setting.

6.1.2.2.2 The Current Systems Processes

The organisation is currently in the process of automating its existing systems further, to allow remote access to corporate databases for updating and retrieval of corporate information by off-site personnel. The company's existing and new systems are briefly described, to give an insight into the organisation's attitudes and success in implementing new technology. It is also necessary to understand the processes since the authentication infrastructure from this research project will be integrated into this system.

a) The Manual Sales Process

Travelling salesmen complete order forms manually by either faxing them back to the office when they find a fax machine (usually from the hotel room in the evening) or by presenting the orders manually on their return to the office. The information and sales orders are processed by the customer services/sales department, who input these orders into the system manually, update the records and issue confirmation documents to customers.

Current Company Sales Processes

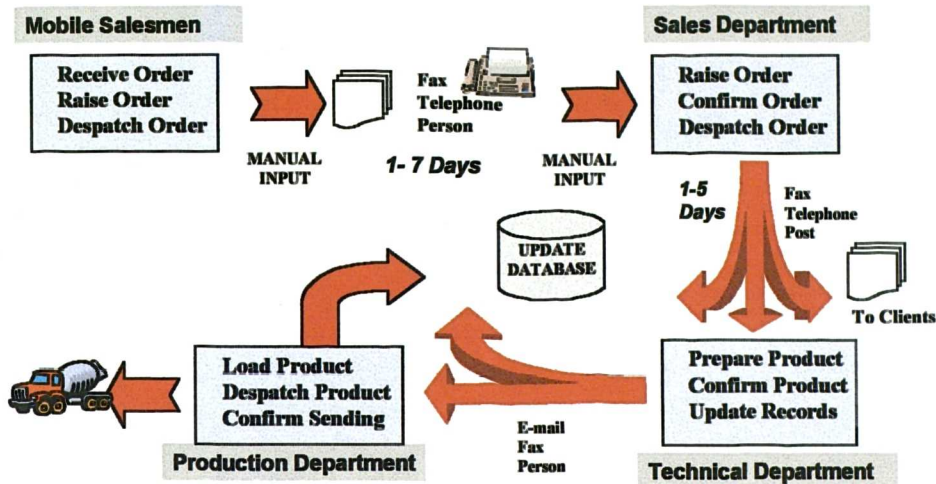


Figure 22 . Company D's Current Sales Processes

There are 5 salesmen who make about 3-4 orders per day. By the end of the week, a large amount of data has been accumulated for input into the system. The sales staff are currently a few months behind and temporary clerical staff have to be hired at 3 monthly intervals to control the accumulated backlog of data. The permanent staff dealing with inputting this information, are customer services staff who also take orders over the telephone or by fax, deal with customer complaints and requests. If not inputting information they would be dealing with some other customer service or be involved in other value creating tasks.

b) The Automated Sales Process

The new system that is being piloted by the salesmen eliminates time consuming duplication by creating orders and documents at source, within the Territorial Management System (TMS) from a laptop computer pre-installed and configured with a modem, log-in procedures and Lotus Notes software. Salesmen connect to the corporate Intranet via a direct dial number, where access is only allowed by a password. Via the TM System, they can directly access areas of the corporate database, which they are authorised to view or update. Once they have updated the database, they send e-mails to the technical and sales staff with template letters of confirmation to clients for printing, posting or faxing.

Automated Sales Processes

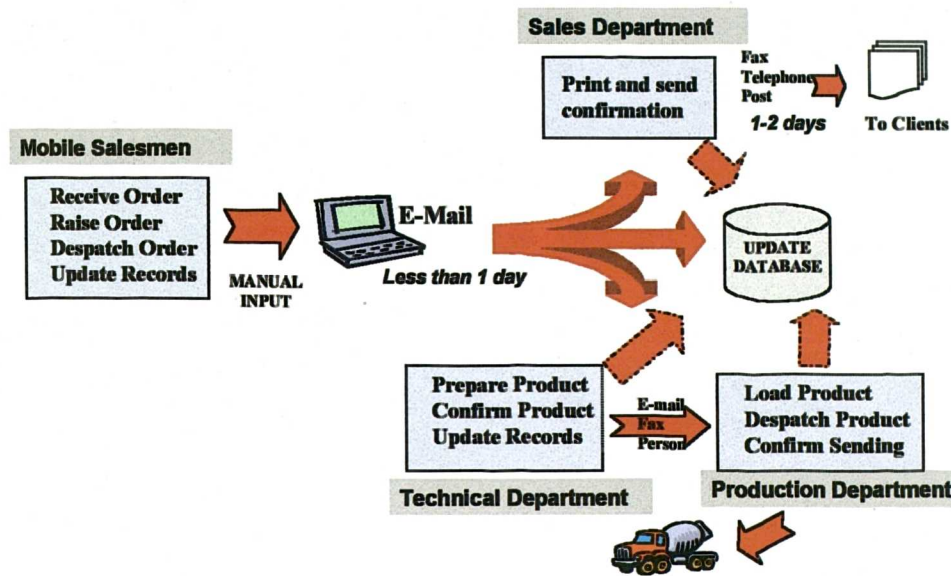


Figure 23 . Company D's Automated Sales Process

Initially, participants in the pilot were 2 salesmen and 2 members of staff in customer services, with the intention of extending the project after 8 weeks to the remaining 3 salesmen. The two salesmen selected are highly IT literate and very enthusiastic about the project. After the initial trial period, the training of the remaining salesmen was in-house by the more experienced participants. For the first 3 months, both the new and the existing processes were being run in parallel to ensure that the quality of service to clients was not compromised by any unexpected errors in the new system.

The results of the pilot showed that there is user uncertainty because the interface is "visually daunting" to administrative and customer service staff in particular. One of the reasons for the uncertainty, is the problem of familiarity with the old system and fear of the new system. It was a common opinion amongst the participants in the Effective IT meeting, that there is a need for more time for the administration and customer services staff to get used to the system and that the training should be out-sourced to a third party. At the same time, help groups within the organisation, should be set up, where employees help each other. It

was also found that employees do not open their e-mails and that staff have an overwhelming feeling of "information overload", so education and information about the new communication medium and its management was also felt to be necessary.

6.1.2.3 Implementing the Security and Authentication infrastructure

Having observed and analysed the organisations' corporate strategy and its processes for implementation of new technology, this section will review the stages in the planning and implementation of the authentication infrastructure developed in the first part of this research project.

Firstly, the business objectives formulated by the directors were communicated to the IT strategy team by the IT director. These were to develop:

- *an interactive system for all members of the organisation*
- a paperless office to cut down on costs and improve efficiency
- easy and immediate communications
- immediate access to information by authorised stakeholders to increase efficiency and improve productiveness

After a series of meetings by the team, a statement of intent was finalised.

"To provide secure access to relevant information to those authorised to use the system, ensure that this information is not available to other parties who are not authorised and to provide secure Electronic Commerce for incoming and outgoing business"

A list of the aims and objectives for the IT system was produced, incorporating the business objectives outlined to the IT strategy team. Some of the issues raised were:

- **Increased functionality of the system:**
 - For salesmen to improve their productivity by having instant access and the ability to update information by secure automation of the sales documentation process. This also extends to agents based outside the UK.
 - To monitor the level of adhesive in the customers' tanks and raise the order automatically under a secure means of communication.
 - To implement a security system, which will allow universal access to the Internet and allow salesmen to reduce costs by dialling a local rather than a national number.
 - To support future development to include ordering on-line, improved communications and increased information on-line for customers.
 - To support Internal and external e-mail communications with attachments
- While providing access to a wider range of stakeholders, a strong security infrastructure needs to be in place, to ensure that only authorised personnel can access key information.
- Security needs to be in place to protect prices from being revealed to competitors and technical information becoming public.
- The system must be able to prevent the altering, saving and printing of key information and to maintain an audit trail of those accessing and changing the database.
- Training is needed to ensure regular and effective use of information and systems by personnel.
- Currently only an informal, verbal security policy covering computer procedures relating to the main AS400 systems existed. This needed to be formalised and cover a wider range of topics and issues including e-mail and network usage.
- The security policy and the IT infrastructure must be incorporated into the ISO 9000 regulations and be documented accordingly.

From these meetings, a plan for implementing a secure environment for the access and transmission of information by authorised personnel was produced. This was to:

1. Define the stages of implementation required for the above mission statement
 - Stage One – To develop a security infrastructure for the remote access of information by authorised personnel.
 - Stage Two – To develop a security infrastructure for the remote access of information by authorised agents not based in the UK.
 - Stage Three – To develop a security infrastructure for the access of customers to their own accounts and for on-line ordering.
2. Identify the tools required at each stage of the implementation - physical hardware, specifications (connection to Internet), detailed specifications and set up of machines.
3. Define training and/or external resource requirements for each stage.
4. Define the use of tools and resources at each stage.
5. Implement a pilot scheme incorporating the enhancements made at each stage of implementation.
6. Evaluate and review pilot scheme at each stage.
7. Define security policy. The Security Policy was devised in a later meeting. The TQM Manager wanted these to be noted circulated and documented in detail. The security policy consisted of the following:
 - Procedures for diskette usage and distribution - no employee could import any unauthorised diskettes - formal complaints would be made in the event that this happened.
 - Notebook back-up procedures
 - Virus checking of attachments - only authorised personnel are allowed to receive attachments

6.1.2.3.1 Current Systems Security

This research project in which Company D had volunteered to take part, centred around the development of a Public Key Infrastructure (PKI) with encryption and digital signatures as a means of providing the security facilities they required. The plan was to introduce Entrust software to the organisation, and train selected users in its use as part of the pilot project. However, issues of compatibility were raised and it was necessary for the researcher to assess the current security measures that had already been implemented by the organisation. The researcher was requested by the host organisation to act as an external consultant in undertaking a technical compatibility analysis.

6.1.2.3.2 The Current Security Infrastructure

Sensitive information, such as product formulae, is stored on a separate AS400 server, which runs in parallel with the Lotus Domino Server. There is an AS400 firewall with strict specification of user permissions and roles in the system. Existing security processes are password protection at each stage of the log-in process and also authorisation for dial-in to the central database.

Currently, a maximum of five passwords which are encrypted are required to access the organisation's intranet. These are, power on/dial-in/DOS LAN services/ AS400 network/Lotus Notes Network. The organisation has an internal network (Local Area Network) based on an Ethernet and switch network, they only have internal e-mail (Figure 24). They use Lotus notes GroupWare and Lotus Territory Management System (TMS), which is used for a number of sales related departments namely:

- Customer Service
- Sales
- Technical Department

There is no universal corporate access to the Internet and no web-site. ISDN dial-back access from home is currently being trialed as an alternative to ISP and mobile phone dial-in is available for employees who need to access the database off site.

Company D's Network Infrastructure

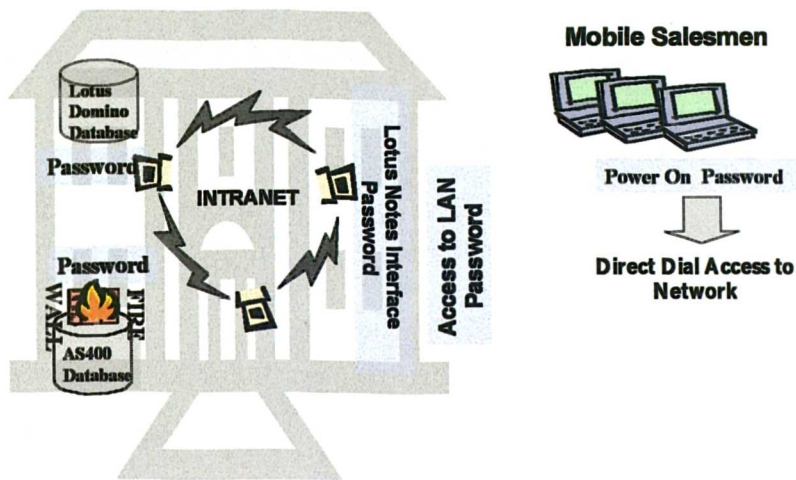


Figure 24 . Company D's Network Security Infrastructure

It was found that the Lotus system already has a PKI infrastructure, which had not been activated. The PKI system allowed an authorised administrator to act as a internal corporate registration authority - verifying, authorising, issuing and revoking digital signature and certificates to personnel in the organisation. The digital signatures issued to personnel could automatically be used with any of the Lotus suite of software installed and used within the organisation. This would include e-mails, automated documents, access and changes to the databases. The system, if activated would fulfil a large number of the aims and objectives stated in the IT strategy. When questioned, the IT personnel including the director, was unaware of the PKI facility and wanted advice on how to activate it, what it could do for the organisation, all the security implications and training in the administration and use of the system.

6.1.3.4 Outcome of the Implementation Process

Once the preliminary research was complete, the next steps were to work with the company to implement a security solution. The company decided to obtain third party consultancy to train its employees in the set up and use of the Lotus PKI infrastructure already integrated into its computing systems. Thus the research project's objectives to implement the security solution, identify the benefits and define the implementation process could not be seen through.

In March 1999, the same company was contacted again. It had been taken over by a multi-national corporation with 94 sales offices world-wide. It still used the Lotus System but had not implemented the Lotus PKI security facility. It was currently trying to integrate all the systems of the 94 sales offices world-wide which it envisaged would take a long time. All E-mail received and sent is routed through the multi-national HQ gateway in Houston. There are no plans to get on the Internet, the company has a global internal WAN by direct dial to the US, where there is a firewall and security infrastructure. The parent company had its own ideas on electronic systems, so no plans could be implemented without prior approval by HQ.

6.1.4 Conclusions

The findings from this case study begin to define a framework for understanding the security needs and implementation processes of SMEs.

The Pre-implementation Stage - this organisation had a highly functional and successful organisational decision-making process. Corporate decisions made at the top level of the organisation were translated into practical actions resulting in the design and implementation of systems that would be used to effect corporate strategy and grow the organisation. The level of communication and the involvement of directors in all stages of the design and implementation of projects, contributed greatly to the company's success. As did the channels developed for communication and feedback from users back to the systems designers. The high degree of commitment to innovation, technology and customers was integrated into all aspects and levels of the organisation's culture

and were also key factors of its success. In terms of security, the organisation developed their own security infrastructure focusing on the protection of access to data stored in the corporate database.

The Implementation Stage - the implementation of the security solution to allow the secure transmission of electronic data across an open network between sales agents, was not effected. The main reasons were:

- No real commitment to implementing a security system which focused on data transmission across public networks. The company's current security needs focused on securing static data and preventing unauthorised access to that data. It was felt that the current infrastructure provided enough security for the organisation's current purposes.
- No full understanding of the existing system and its facilities. The organisation had focused its attention on developing a system that automated the sales process, speeded up order processing and delivery to customers. There had been no proper assessment of existing resources. The organisation also had employees with limited expertise in and knowledge of implemented systems, thus more training was needed.
- Limited financial and human resources. The policy of this company was to take advantage of any government grants (funding ISDN lines) or local TEC/Chamber of Commerce schemes available for funding hardware or software. While this gave it access to hardware, software and expertise, which it would not ordinarily have, in the longer term this might be detrimental since it might not be able to capitalise on the equipment and knowledge to which it had access.

6.2 Case Study II - Company T

Company T was selected for participation in this research study having fulfilled the ERDF criteria that it was an SME with 8 employees and was geographically located in the EU objective II area. The organisation's participation was voluntary and they had been introduced to the project through the Manchester Chamber of Commerce's involvement with the GEMISIS project.

This case study involved tracking and evaluating the process of implementation and the actual usage of the Trusted Third Party service developed in the first stage of this project.

6.2.1 Methodology

The aims of this study were to gain an understanding of the ethos of the organisation; its people; their attitudes towards technology, the introduction of new technology; an analysis of existing business processes and the stages of implementing new technology.

6.2.1.1 Structured Observation

The usage of the software by the operator was observed and noted by the researcher - including overall confidence with software and technology, keyboard skills, competence during and after training. This information would be supported by the data gathered from questionnaires to ensure that a fair assessment of the user could be made.

The time and cost differentials of business processes before and after using the security service would be measured. This would show any concrete benefits or disadvantages, in commercial terms, to the organisation.

Logs of "help" calls or requests made to technical support staff verbally or in writing were also kept. The nature of the problem, recommended solutions and any other follow-up would be recorded (appendix 14). This would support the observations and data collected from other sources. Other sources of information included published corporate brochures.

6.2.1.2 Time Series Structured Questionnaires

A structured questionnaire (appendix 15) was designed to be completed by the relevant participants before and after their participation to gain a profile of the users, their attitudes towards and experience of technology, the software and security. This data would support that collected by structured observation.

6.2.1.3 Depth Interviews

Depth interviews lasting between 10-30 minutes, were conducted with the directors of the organisation, one of whom was also a participant in the pilot.

6.2.2 Findings

In order to assess the processes and forces involved in the implementation and use of the authentication infrastructure in an organisation, it is necessary to understand the framework in which the organisation operates, formulates strategies and makes decisions. The findings are reported in the following section in a way that will firstly describe the general business ethos of the organisation including its corporate strategy, its IT strategy and decision making process and its current IT systems. Then the organisation's implementation and usage of the authentication infrastructure will be assessed.

6.2.2.1 The Organisation and Its Background

This is a small company with eight employees set up in 1992. This company is part of a group of independently management-owned laboratories, which provide chemical analyses of materials to a variety of industries. It has an ethical policy, which prevents them associating with any organisations involved with the manufacture, sale or use of weapons and armaments, animal testing or pornography. Its mission statement is:

"To become the leading organisation in the world providing analytical chemistry services. To achieve this goal, ... we must excel in our relationships with our clients, employees and investors while establishing leadership in technology and operations management"

The company's corporate strategy is to provide a high quality report to customers in a reasonable time, in an accessible format and at a competitive price. The data and its presentation in the final report is extremely important to customers, who use it for crucial business decisions. Report contents are also highly sensitive and must be kept confidential for the recipient only.

The culture and environment of the organisation is technology oriented. There is no formal organisational hierarchy or processes for decision making. The company is a typical entrepreneurial organisation with a flat structure where the owners/directors are the sole decision makers, driving the company by their energy, ideas and physical involvement in all areas of business.

6.2.2.2 The Current Business Processes

The close involvement of management ensured an initial commitment to the project, with innovative and practical ideas for integrating the security and authentication infrastructure into the organisation's business processes illustrated in Figure 25.

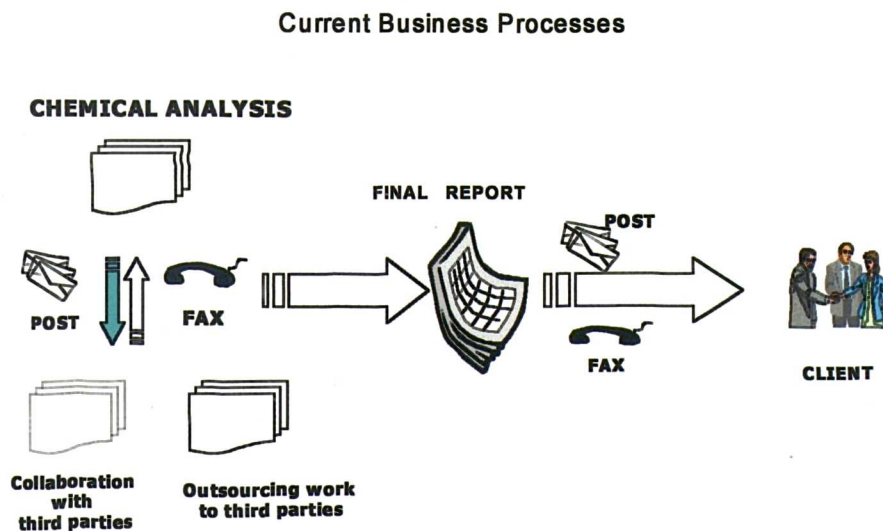


Figure 25 . Company T's Current Business Processes

Although technologically oriented, Company T was not particularly knowledgeable about the Internet. The organisation had an intranet infrastructure with no e-mail facilities, illustrated in Figure 26.

One of the directors was connected from home and was using his personal e-mail address for the business. Although it had no corporate web presence, through the Virtual Chamber of Commerce¹²⁴ pilot project, the company had been given a free single cable modem from Cable and Wireless for connection to the Internet. It was using a Netscape web browser and connection to the Internet was from a standalone machine. The company had three computers on which they had installed Word MS Office, other technical and industry specific applications. They also had a VAX and a PC.

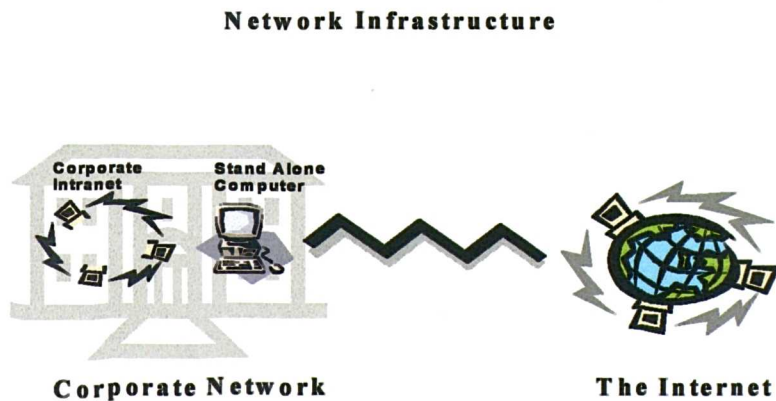


Figure 26 . Company T's Network and Security Infrastructure

6.2.3.3 Implementing the Authentication infrastructure

The management saw the security project as an opportunity to improve customer services by allowing immediate and secure delivery of electronic data that was being produced. Secure transmission of electronic data was seen as the means of achieving the business objectives of speed, confidentiality and cost-effectiveness of the delivery of reports to clients.

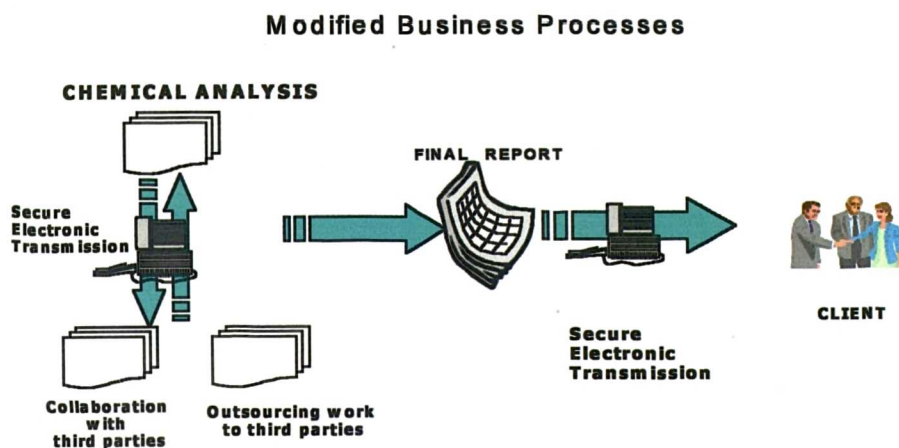


Figure 27 . Company T's Modified Business Processes

Firstly, the verification procedures laid out in section 5.3.2 and the Certification Practice Statement were followed and the necessary documentation was completed. Initially it was agreed that two people from the company would trial the authentication infrastructure. Only the managing director participated and these findings are based on his experience. The fact that this sole participant is also the chief decision-maker in the organisation, gives the data more weight.

Training was given in a one-to-one session, on-site after installation of the software lasting about 30-40 minutes. A user's guideline for using the Entrust software was also given to the participant as a reference. The user was highly technologically literate. He had a basic knowledge of data encryption and was an enthusiastic and fast learner. He was confident using the computer and navigating the software.

6.2.3.4 Outcome of the Implementation

The security facility was used only with the researcher in the test phase and was thereafter abandoned. The main reason the project was abandoned was due to the fact that no business partners were prepared to participate with company T. The observations and comments made by the user on the use of the software were:

- There is a problem with the Entrust screens, which were felt to be too small.
- The user had a problem creating and remembering the password format – which was to include at least a number, capital and small alphabet character and alphanumeric of 8 characters or more.
- It was also felt to be not easy enough to use, that it was too complicated to change directories and select documents for encrypting or signing. The user felt that it should be accessible by a single keystroke.
- The user also felt that it should be integrated into and accessible by existing programs such as through browsers and e-mail.
- The user also wanted added features to the software. For example, where a document could be circulated and digital signatures attached repeatedly so that there is an audit trail of the people who had received the document.
- The kind of security that the respondent found to be particularly important to the organisation included the prevention of junk e-mails and viruses.

6.2.4 Conclusion

Although the concept was totally agreed to, in practice it was not deemed to be usable or suitable for integration into the organisation. The software was not used because there was nobody to use it with. No other external stakeholders agreed to take part in the project. The MD attempted to recruit the association of engineers to use the security solution, however there was apathy and no real interest. Similarly a "friendly" business associate was invited to join the project, but again there was no active response. So there was a total abandonment of the project because of lack of commitment from the various stakeholders.

6.3 Case Study III - University X

University X was selected for participation in this research project to test the process of implementing and using the authentication infrastructure designed in the first part of this study. Although the University is in the EU Objective II area, it is not an SME. However, it does have a real need to improve processes because of limited resources; shortening time scales due to semesterisation; broadening the number of degree courses to widen their appeal; and the increase in student numbers. One such time critical and resource intensive area in need of process times, costs and efficiency improvements, is the collation, preparation and distribution of examination papers.

The aims were to implement and test the designed authentication infrastructure by integrating it into the process of electronic preparation, validation and transmission of examination papers. The benefits of implementing the authentication infrastructure, are envisaged to be:

- Reduced costs by maximising the use of existing resources
- Improved efficiency and lead times by facilitating the management and delivery of electronic documents and reducing paperwork handling
- Reduced possibility of data loss and compromise by introducing security and validation measures.

In order to assess the process involved in the planning and implementation of the security and authentication infrastructure in an organisation, it is necessary to understand the framework in which the organisation operates, formulates strategies and makes decisions. The findings reported in the following section, will firstly give a brief overview of the organisation, its structure and the decision making process. Then, the planning and implementation of the secure electronic data solution will be described and analysed.

6.3.1 The Organisation and its Background

The University is structured into Departments that are responsible for undergraduate teaching. These are grouped into eight Faculties: Art and Design Technology; Business, Management and Consumer Studies; Engineering; Environment; Health Care and Social Work Studies; Media, Music and Performance; Science and Social Sciences, Languages and Humanities. The research and postgraduate activities of the University are co-ordinated by the Research and Graduate College, which comprises six Research Institutes and a Graduate School.

The organisation is hierarchical and highly bureaucratic, with multi-layered procedures and paperwork chains in place for almost every process - ranging from the purely administrative to the policy change.

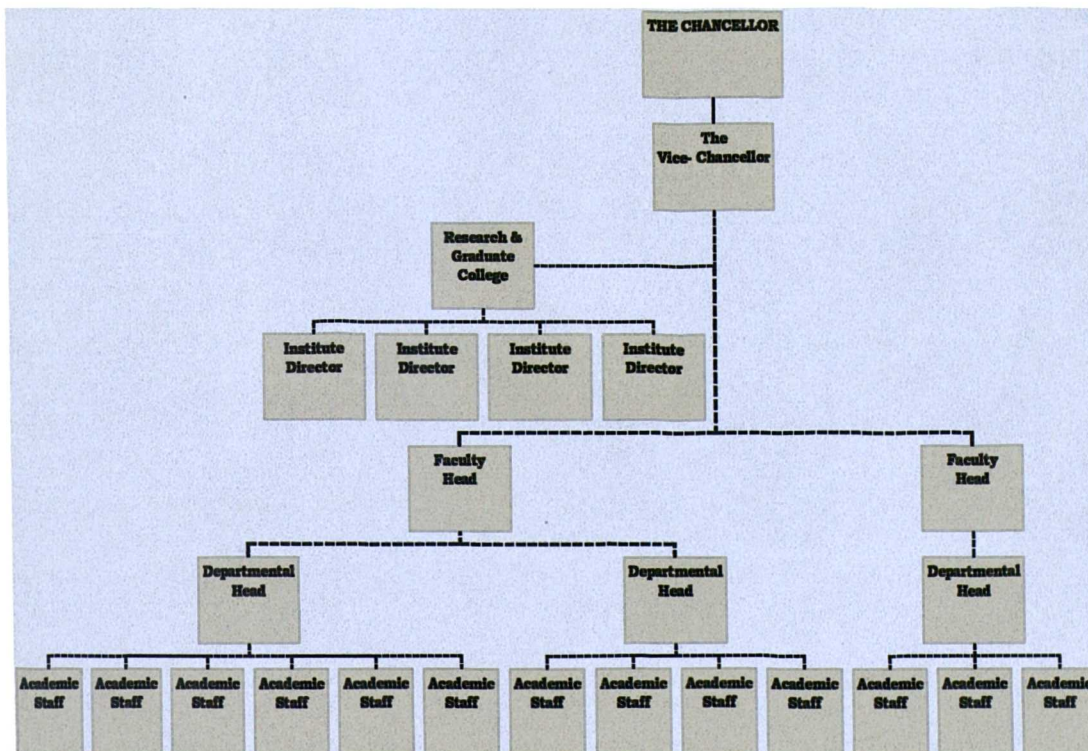


Figure 28 . University X Organisational Chart

The next section will look at decision-making processes within the organisation and also focus on the processes that have been targeted for piloting the authentication infrastructure.

6.3.1.1 Decision Making Processes

The decision making process is complex and hierarchical. It involves a number of committees and decision-makers and must be approved at all levels of the organisation including the finance, policy and other non-academic departments. Any decisions made must not only conform to the university's own policies and working practices, but also the criteria laid down by government. Thus for any changes to take place, the process is slow, bureaucratic with many factors and conditions to be fulfilled. In this case, the pilot for implementing the authentication infrastructure was approved by a top-level committee and implemented at departmental level on a voluntary basis.

6.3.2 Methodology

The pilot took place between the Examination Office, Department Y and Department Z at University X. Department Z and Department Y were selected based on the fact that the former is one of the oldest established departments in the University and is consistently late in the submission of examination papers to the examination office. Department Y was selected because it is one of the newest departments in the University, it is technology oriented and organises its own printing and distribution of examination papers and thus has no problems with late submission and production of examination papers. It was expected that by taking the two most extreme cases, participant attributes (according to the project criteria) would be more prominent.

Overall, the project involved the participation of 12 academic staff, 4 administration staff whom co-ordinate the production of the examination scripts and 4 external examiners who review the scripts.

6.3.2.2 Sample Selection

Within these departments, the population from which the sample selection process took place, was examination papers set for Semester One in January 1999. The examination papers were classified in order to:

- Ensure that the random sample selected is representative of the population
- Identify the range of situational factors likely to affect the successful deployment of an electronically based examination procedure.

Information used to gather the data for categorisation was obtained directly from conversations with heads of departments, past examination papers and solutions, and current examination schedules.

6.3.2.2.1 Exam Paper Classification

Table15, describes the classification criteria for the population of examination papers.

Classification Attribute	Description & Rationale
Subject	A breakdown of the subject categories e.g. IT/Business/Mathematics/Software Development
No. of people involved with setting questions	This will give an indication of the level of co-operation/standardisation necessary to implement a system
How long has the course been running	This will give an indication of the relative “newness” of the course and the exam preparation techniques
Name of Internal Quality Assessor	To ensure participants are not duplicated
Name of External Examiner	To include her/him in the pilot
Name of Examination author	To ensure participants are not duplicated
How long has the current lecturer been running the course	This will give an indication of the propensity for the lecturer to change exam preparation techniques
Length of exam	In terms of duration and also in terms of numbers of questions/numbers of pages
Content of the exam and type	To assess the format of the examination paper e.g. Text/Text & graphics/graphics Problem solving/essay/multi-choice
Format received (questions and answers)	Hand-written/electronic (Q&A) MS Word or WordPerfect only are acceptable
Date of the examination	For administrative purposes

Table 15 . Classification of the Population Sample Attributes

This was a live pilot project in a critical area with tight deadlines and as such certain criteria for the inclusion of population members in the sample selection stage had to be pre-determined. The criteria for including and excluding examination papers from the overall sample selected are summarised and explained in Table 16.

Inclusion Criteria	Exclusion Criteria
<p>(a) Examination papers and solutions in electronic format <i>Encryption software can only be used on electronic documents either text or graphics</i></p>	<p>(a) Handwritten or partially hand written examination papers or solutions</p>
<p>(b) Content of examination papers is text, graphics <i>In cases where mathematical examination papers and solutions are prepared electronically, the software used is a specialist mathematical software. For the purpose of this pilot, all the parties involved - the administrator, the external examiner, the Quality Assessors (QA) and the examination officer would all have to have a copy of this software and know how to use it. This was not expedient for this pilot and thus these papers had to be excluded from the sample.</i></p>	<p>(b) Content of the examination paper is mathematical symbols, equations and formulae</p>
<p>(c) External Examiner is willing to participate <i>If the external examiner is not willing to participate, then this will exclude the papers from the pilot, since the external examiner is a crucial link in improving the speed and reducing the cost of document transmission</i></p>	<p>(c) External examiner is unwilling to participate</p>

Table 16. Population Sample Screening Criteria

The excluded papers were reviewed in the context of the overall population, to assess the impact of their exclusion on the overall sample and ultimately the results. The implications of these are discussed in the conclusion section.

6.3.2.2.2 The Population

In order to understand the degree to which the sample is representative of the overall population of examination papers in the respective departments and the probability of success in implementing the pilot department-wide, it is necessary to analyse the population from which the sample is drawn.

i) Department Z's population of examination papers for Semester One (January 1999), consisted of a total of 54 papers across 5 subject areas ranging from the purely mathematical to the Information Technology and Systems oriented. Over 50% of Department Z's examination papers had to be excluded from the sample because some or all of the questions and solutions for the respective modules, were prepared by hand or were not in an electronic format. Looking at the overall population, 75% of all courses had been running for more than five years, with only 8% of courses having been in existence for one year or less. Within the modules, for the maths courses, all had been running for more than 5 years and over a half of the lecturers had been running the courses for more than 3 years.

With the technology oriented modules the courses had been running for relatively less time a higher proportion had been running for 3 years or less. Similarly, the lecturers tend to have been running the courses for a shorter period of time three years or less.

Department Z						
Subject Category	No. of Papers	Length in Years (of Courses)		Length in Years (of Lecturer running the courses)		Comments
Computer Science	12 (22%)	83%	>5 years 3 years 2 years	58%	> 5 years 3 years 2 years New	
Information Systems	11 (20½ %)	27%	> 5 years 3 years 2 years New	27%	> 5 years 3 years 2 years New	
Maths (I)	11(20½ %)	100%	> 5 years	57%	>3 years 2 years 1 year New	Graphics, text, formulae also solutions are hand written*
Maths (II)	14 (26%)	100%	>5 years	100%	> 3 years	Graphics, text and formulae also solutions are hand written*
OR & Statistics	6 (11%)	63%	>5 years New	63%	>5 years New	Graphics, text and formulae also solutions are hand written*
Total Population	54	78%	>5years 3 years 2 years 1 year New	28%	>5 years 3 years 2 years 1 year New	

*These papers were excluded from the sample

Table 17 . Categorisation of Department Z Examination Papers

ii) Department Y's population of examination papers, consisted of a total of 17 papers with all of them being Information Technology oriented. Nearly all the courses in Department Y had been running for more than five years. However, the majority of lecturers (64%) had been running the course for two years or less.

Department Y					
Subject Category	Number of Papers	Length in Years (of Courses)		Length in Years (of Lecturer running the courses)	
Information Technology	17	94%	>5 years	12%	>5 years
		6%	New	24%	4 years
				23%	2 years
				41%	New

Table 18 . Categorisation of Department Y Examination Papers

6.3.2.3 Data Gathering Process

A variety of methodologies were used for data collection in order to capture relevant information at different stages in the pilot. At the pre-pilot stage, depth interviews and questionnaires were used to gather data. After implementation of the security solution and training, data was gathered by observation, questionnaire, and comments/problems registered by the technical support facility.

6.3.2.3.1 Depth Interviews

Since this was a live project, depth interviews were carried out with the department heads and administration staff to determine,

- authorisation and procedures for carrying out the pilot
- the nature of the current examination preparation and administration process
- population attributes and sample selection criteria
- current security procedures and practices

6.3.2.3.2 Questionnaires

Data was collected from pilot participants at different stages in the project.

Initially, participants were asked to complete a pre-project questionnaire (Appendix 16 a-c) before installation of the software and training was given. Slightly modified questionnaires were given to each of the participant groups – namely examination paper originators, administrators and externals. At this stage a range of information was obtained in order to build up a profile of pilot participants and users. Data included:

- demographics such as age, profession, education
- patterns of computer usage and IT experience
- attitudes to technology in general
- attitudes to the secure electronic transmission of examination papers in particular
- attitudes and opinions on the current process of examination paper production and administration

Finally, participants were asked to complete a post-project questionnaire (Appendix 17) to assess the feelings and attitudes of the project participants to the software they were using and the needs or requirements to improve or alter the process under assessment.

6.3.2.3.3 Semi-Structured Observation

The researcher observed the users during the training sessions, taking particular note of their behaviour, actions and comments in major areas:

- The participant's approach to the training – e.g. whether they were in a hurry, whether they paid attention
- Their use of the computer and software – e.g. level of confidence and competence
- Any relevant comments and questions about the software, computer usage, training, the examination process or any other relevant topic.

- **Measuring the time taken for each stage in the pilot examination process and the actual process**

Data gathered from the semi-structured observation, was used to build up the profile of the user.

6.3.2.3.4 Technical Support

A user help facility was set up for pilot participants with technical or other problems. Data collected from the types of technical problems encountered and user queries or problems are also included in the findings.

6.3.2.4 Installation and Training

Part of the pilot project is the installation of the security software on the participant's machine and training the participants in the usage of the software.

6.3.2.4.1 Internal Participants

The security software was installed by the researcher on the participant's machines for on-site staff of Department Y and Department Z respectively.

Training for on-site participants took the form of a one-to-one session between each participant and the researcher, where the researcher explained the software features by allowing the participant to take control of the keyboard and "walk through" the software. This session lasted between 15-30 minutes depending on the questions asked. A user's guide (Appendix 13) was prepared for the participants.

Once the participant had been registered and trained, the researcher then sent two messages to each participant. One was encrypted for the participant only; the other was encrypted to the exclusion of the participant. This was to ensure that the participants could access encrypted files before the pilot took place in "real life".

6.3.2.4.2 External Participants

The researcher visited one external participant personally. The software was incompatible with the operating system, so no installation took place. However, the researcher explained the software features on a portable machine and also explained the procedures for installation. The external participant later forwarded the correct version of the security software for self-installation.

The external participant was sent a copy of the software for self-installation and training in installation and use of the software was carried out over the telephone.

6.3.2.5 Task Performance Measurement

A measure of success of the secure electronic transmission system being piloted is whether cost, time and efficiency improvements are made using the system. Thus, the time taken and additional costs for the transmission of a document from each process stakeholder in the outlined stages, was measured. Two other examination papers, not involved in the pilot, were selected at random to measure the time and cost of transmission by the traditional method. This was taken as a measure of control against which to gauge the electronic process.

STAGE	MEASUREMENT
1. ORIGINATOR TO ADMINISTRATOR	Time taken from when the originator completes the document to when the administrator receives it. Cost of sending the document from the originator to the administrator.
2. ADMINISTRATOR TO EXTERNAL EXAMINER	Time taken from when the administrator collates the documents to when the external receives it. Cost of sending the document from the administrator to the external examiner.
3. EXTERNAL TO ADMINISTRATOR	Time taken from when the external examiner sends the document to when the administrator receives it. Cost is not incurred by the University.
4. ADMINISTRATOR TO ORIGINATOR	Time taken from when the administrator sends the edited documents back to the originator. Cost of sending the documents from the administrator to the originator.
5. ORIGINATOR TO ADMINISTRATOR	Time taken from when the originator completes the document to when the administrator receives it. Cost of sending the document from the originator to the administrator.

Table 19 . Criteria for Measuring Time and Cost of the Examination Process

Only the time and cost of transmission were measured and not the process time, since the change is the means of transmission not the process and different individuals have different working practices. In this case, individual working practices are not under examination (although it is expected to have an impact on processes).

For the traditional process, the costs of sending documents were noted and the date and time documents were received and sent by the administrator and originators were recorded where possible. The means of measurement for the electronic process was the e-mail acknowledgement of receipt (an option which participants were requested not to deselect) and recording e-mails sent from and received by the administrator. Any additional costs were also recorded.

An indicator of failure of the secure electronic transmission pilot is any user reverting to paper transmission at any stage.

6.3.3 Findings

In order to assess the process involved in the planning and implementation of the security and authentication infrastructure in an organisation, it is necessary to understand the framework in which the organisation operates, formulates strategies and makes decisions. The following section will describe and analyse the planning and implementation of the secure electronic data solution and present the findings for the 2 groups of users and their stakeholders at the Department Y and Department Z separately. These findings are presented as two sections under a new numbering system 1 and 2 with their respective subsections.

1. The Department Y Sample Group

The findings from the pilot are summarised and discussed in this section. The results from each department are presented separately, and any similarities or distinctions will be drawn in the summary section.

1.1 The Sample

The total sample of papers for the courses selected randomly from the IT Institute had been running for more than 5 years. Two of the lecturers had been running the courses for 5 years or more, 2 had been running the course for 2 years and 2 lecturers were new to the courses. All examination papers were prepared electronically. The non-confidential attributes are summarised below.

Subject	Length the course has been running	Length the current lecturer has been running the course	No. of people involved in setting questions	Length of exam In hours	Content Of exam
Information Technology	> 5 years	0 yrs	1	1.5 hrs	text & graphics
Information Technology	> 5 years	0 yrs	1	1.5hrs	text
Information Technology	> 5 years	2 yrs	1	1.5 hrs	text
Information Technology	> 5 years	2 yrs	1	3 hrs	text & diagrams
Information Technology	> 5 years	4/5 yrs	1	1.5 hrs	text & graphics
Information Technology	> 5 years	5/6 yrs	1	1.5 hrs	text

Table 20 . Department Y Total Sample Group Attributes

Figure 29 illustrates the type of examination paper selected randomly within the Department Y sample. This indicates that 100% of the sample papers were associated with courses that had been running over 5 years, while 67% of the papers were run by lecturers who were relatively new to the course i.e. two years or less.

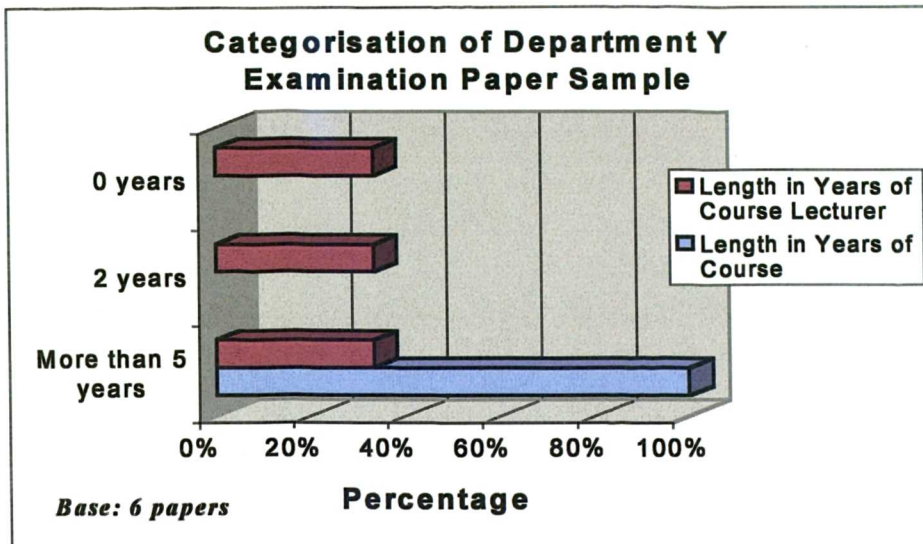


Figure 29 . Categorisation of Department Y Sample

User Profile - Demographics of Department Y Participants

All the participants were lecturers in Department Y with postgraduate qualifications. The main age group of participants were between 35-44. Only one third of respondents were not connected to the Internet at home. The group A and group B distinctions were for the researchers use only to identify participants.

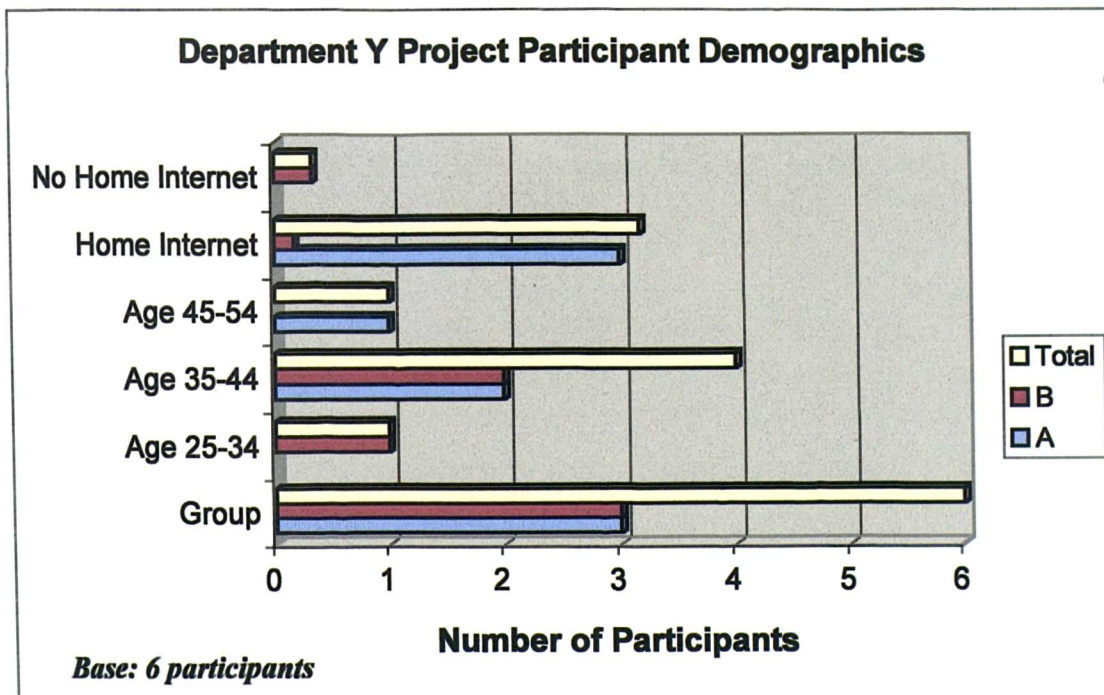


Figure 30 1. Demographics of Department Y Participants

1.1.2 User Profile - Computers and Technology Habits and Attitudes

All the participants use computers both at work and at home on a daily basis. Computer usage is mainly for preparation of presentations, e-mail, Internet, word processing and spreadsheet. The main software used is Microsoft Office products, which minimises any potential software incompatibility problems, across the department. Nearly half the participants also use computers for software engineering.

Included in the questionnaire are statements, which measure specific thoughts, attitudes and cognitions that people have when working with computers and technology or when contemplating working with technology. These statements have already been psychometrically tested as a measure for technophobia¹²⁵, by Drs Rosen and Weil in the US. The higher the score on attitudes to technology, the less comfortable and confident respondents are likely to be with technology and the more likely they are to be technophobes. In this case it is not the individual scores that are of particular significance, but rather the comparative scores of the participants. Group A & B distinctions are for the researchers purposes of identification only.

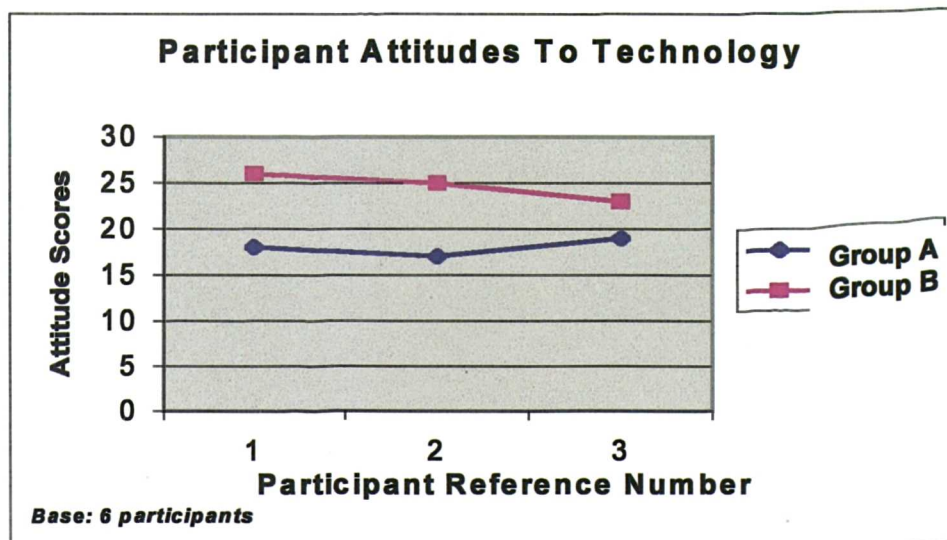


Figure 31 . Attitudes to Technology of Department Y Participants

Figure 31 shows a distinction between participants' attitudes to technology. Participants that tended to have a lower attitude score, indicating they are more technology oriented, are more comfortable and confident with technology and computer usage. The notes taken from observing the participants also support these findings.

Participants with the lower attitude scores were more confident in their approach to and use of the security software used in the pilot. This may also be due to the fact that the 3 respondents in Group A had knowledge of or were currently using some kind of security software*. This is not to say that Group A participants were more competent, but rather they had more knowledge and experience of the technology under examination.

As with the previous results, the actual scores awarded to participants on thoughts about computers and technology are not important. It is the comparative scores between participants that are important. In this case, the difference between participants' thoughts on computers and technology is less distinctive than their attitudes, as we can see in Figure 32.

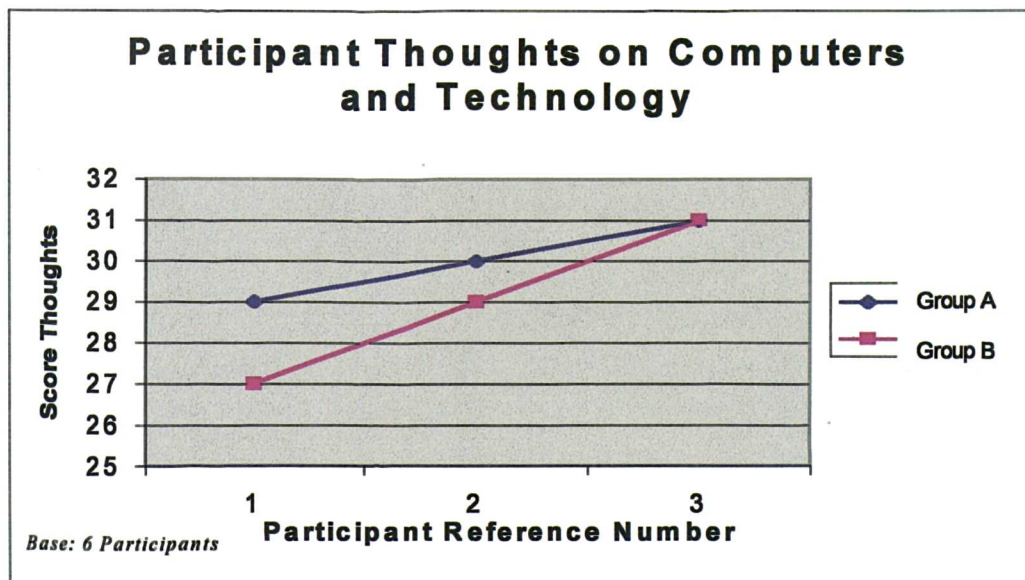


Figure 32 1. Thoughts on Computers and Technology of Department Y Participants

* One respondent was familiar with Pretty Good Privacy (PGP), another was familiar with PGP and Entrust software, while the third was aware of the theory of encryption.

However, participants with a higher score in the thoughts on technology and computers rating, indicated an enthusiasm for technology and computerisation. This is supported by the fact that the higher the participants scored on the thoughts to computers and technology, the more likely they were to have an Internet link at home.

1.1.3 User Opinions on the Current Process

When questioned about the existing examination process, the Department Y participants believed that it was currently “too slow”, “inconvenient” and “cumbersome”. The majority of participants felt that the current system needed to be modernised and made electronic. Some of the comments made were:

- E-mailing examination papers would save time both for the administration and the academic staff
- Using existing Internet and e-mail resources would save private courier cost
- Electronic examination papers are more manageable
- E-mail would be more convenient as it allows the sending and receiving of examination papers from any location
- There needs to be some exam paper version control system, where the version sent is the version that will eventually be submitted as the final version for students
- Direct communication between the external examiner and the lecturer was seen to be advantageous both in terms of controlling final versions, incorporating amendments to the lecturer’s specification, and also as a means of convenience and saving time
- By having electronically secure examination papers, this adds an element of security and will avoid issues such as keeping examination papers locked up and mislaying examination papers

One respondent felt that the current examination process was adequate and there was no desperate need for change. In this case the exam originator was in the same building as the administrator and it was merely a matter of walking to the administrator’s office to submit the paper.

1.2 Task Performance Measurement

A measure of success of the electronic transmission process, is whether time and money are actually saved using the system. Both processes are described below and the time taken and costs incurred for the preparation of examination papers in both the traditional and secure electronic systems were measured and compared.

1.2.1 The Traditional Process

This method is the current method of examination preparation and submission, where the process of preparing examination papers is a series of stages outlined in Figure 33.

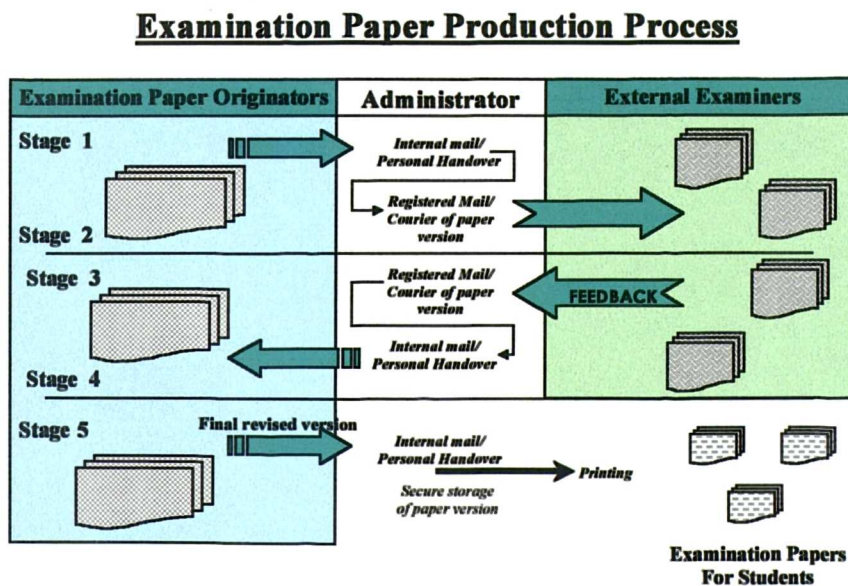


Figure 33 . Department Y Examination Paper Production Process

These stages can be defined further.

Stage 1 - The lecturers originate examination papers which are sent to (by internal mail or handed personally) and collated by the administrator.

Stage 2 - The administrator then arranges for the relevant printed examination papers to be sent by registered mail to the relevant external examiner for feedback.

Stage 3 - The external examiner(s) returns the examination papers (with feedback) by courier/registered mail.

Stage 4 - The administrator receives and collates the examination papers for distribution to the relevant examination originator for necessary revision by internal mail or personally.

Stage 5 - The final stage is the stage where the revised final versions of the examination papers are sent to the administrator for printing and distribution amongst the students. In the IT Institute, this is carried out by the administrator.

1.2.1.1 Time and Cost of the Process

The time and cost taken for traditional transmission of the examination papers was measured for 2 papers selected at random.

PAPER I			
STAGE	TRANSMISSION TIME	COST	COMMENTS
I	48 hours		<i>In this case, the originator completed the examination paper but had to wait 48 hours before being able to "hand it" to the administrator securely.</i>
II	1 day	£7.30	<i>All the examination papers are collated and sent off to the respective external examiner in a batch. Sent by courier next day delivery.</i>
III	3 days		<i>The cost incurred here is by the external examiner. However in this instance, the documents were sent by registered mail.</i>
IV	1 day		<i>Internal mail was used by the administrator in this instance</i>
V	2-5 mins		<i>The originator returned the document by hand.</i>
Total	7 days	£7.30	
Key: I - Originator to Administrator II - Administrator to External III - External to Administrator IV - Administrator to Originator V - Final Version From Originator to administrator			

Table 21 . Time and Cost of Traditional Transmission (Paper I)

PAPER II			
STAGE	TRANSMISSION TIME	COST	COMMENTS
I	2-5 mins		<i>In this case, the originator completed the examination paper and was able to "hand it" to the administrator securely immediately since they were in the same building.</i>
II	1 day	£7.30	<i>All the examination papers are collated and sent off to the respective external examiner in a batch. Sent by courier next day delivery. This cost was already incurred .</i>
III	3 days		<i>The cost incurred here is by the external examiner. However in this instance, the documents were sent by registered mail.</i>
IV	2-5 mins		<i>The administrator returned the document by hand</i>
V	2-5 mins		<i>The originator returned the document by hand.</i>
Total	4 days	£7.30	
Key: I - Originator to Administrator II - Administrator to External III - External to Administrator IV - Administrator to Originator V - Final Version From Originator to administrator			

Table 22 . Time and Cost of Traditional Transmission (Paper II)

The total time taken upto stage 5 (but not including printing and distribution) was between 4-7 days. This includes transit time only and not processing time since the processing time can be variable according to the time taken by the respective stakeholders, to produce the necessary documents.

Courier costs also vary according to the number of external examiners. In this case, both examination papers were being delivered to the same external examiner , so only a total of £7.30 was incurred for both papers.

1.2.2 The Secure Electronic Process

The secure electronic process was designed to mirror the traditional process. This was to make sure that the only variable in the two processes being compared, was the method of transmitting the examination papers electronically. The stages are the same, but submission is by secure electronic transmission rather than physical forms of mailing and delivery systems. All participants who were selected randomly, were willing to participate in the project at the outset, although this has to be treated with caution since an incentive[†] was used and might have created a bias in this instance.

1.2.2.1 Time and Cost of the Process

The time taken and additional costs for the transmission of a document, from each process stakeholder in the outlined stages was measured. The results are recorded in two sections since two papers were sent to one external examiner and four of the total sample were sent to a second external examiner.

The first set of 2 papers was sent to the same examiner and the transmission time and cost are listed in Tables 23 and 24.

[†] £20 book token

PAPER I - EXTERNAL EXAMINER A.			
STAGE	TRANSMISSION TIME	COST	COMMENTS
I	2-5 mins	Nil	
II	< 1 hour	Nil	
III	< 1 hour	Nil	<i>This was edited and returned by e-mail when completed</i>
IV	< 1 hour	Nil	<i>The file was forwarded directly to the originator but the external examiner had encrypted the comments for the administrator only and not for the originator. The administrator had to re-encrypt the document for the originator and re-send the file.</i>
V	< 1 hour	Nil	
Total	4 hours	Nil	

Table 23 . Time and Cost of Secure Transmission I (Examiner A)

PAPER II - EXTERNAL EXAMINER A.			
STAGE	TRANSMISSION TIME	COST	COMMENTS
I	2-5 mins - 24 hours		<i>This was transmission time. However since the participant did not have an Internet connection at home, 24 hours passed before the document could be transmitted electronically</i>
II	< 1 hour		
III	6 days	£7.30	<i>This was encrypted incorrectly by the participant. Both the administrator and the participant were not aware of the type of the error, one week passed and in a state of panic, the process reverted to paper. 6 days later, the error was rectified, by the help desk. The document was sent to the external examiner again securely and electronically and the electronic process continued.</i>
IV	<1 hour		
V	< 1 hour		
Total	7 days	£7.30	
Key: I - Originator to Administrator II - Administrator to External III - External to Administrator IV - Administrator to Originator V - Final Version From Originator to administrator			

Table 24 . Time and Cost of Secure Transmission II (Examiner A)

For one of the two papers, where the system worked effectively, both technologically and by the users, the total transition time between the parties by secure e-mail took 4 hours with no additional costs. Both the originator and the external examiner were out of the UK at the time that the interchange took place, which illustrates more graphically the impact of the system when it does work effectively.

In the second instance, although it took much longer (7 days), it did not take longer than the traditional means of transmission. But there was an additional cost. This however is down to user experience and understanding of the software and messages which should improve with increased usage and training.

The second batch of examination papers were sent to another examiner (external examiner B), the time and cost of the process are listed Table 25.

PAPER I - EXTERNAL EXAMINER B.			
STAGE	TRANSMISSION TIME	COST	COMMENTS
I	2-5 mins - 2 weeks		<i>The user was unable to register because of network problems. Also the user was in Paris at the time and would have unwittingly broken French law had encryption been used on French territory. The user had to wait to return to the UK before the encrypted document could be sent.</i>
II	14 days	£7.30	<i>Reverted to Paper transmission and delivery because the external examiner did not register. The examination papers were batched.</i>
III	5 days		
IV	< 1 hour		
V	< 1 hour		
PAPER II - EXTERNAL EXAMINER B.			
I	2-5 mins - 24 hours		<i>This was transmission time. However since the participant did not have an Internet connection at home, 24 hours passed before the document could be transmitted electronically.</i>
II	14 days	£7.30	<i>Reverted to Paper transmission and delivery because the external examiner did not register. The examination papers were batched.</i>
III	5 days		
IV	< 1 hour		
V	< 1 hour		
PAPER III - EXTERNAL EXAMINER B.			
I	2-5 mins		<i>The user sent the document electronically as soon as it was completed</i>
II	14 days	£7.30	<i>Reverted to Paper transmission and delivery because the external examiner did not register. The examination papers were batched.</i>
III	5 days		
IV	< 1 hour		
V	< 1 hour		
PAPER IV - EXTERNAL EXAMINER B.			
I	2-5 mins		<i>The user sent the document electronically as soon as it was completed</i>
II	14 days	£7.30	<i>Reverted to Paper transmission and delivery because the external examiner did not register. The examination papers were batched.</i>
III	5 days		
IV	<1 hour		
V	< 1 hour		
Key: I - Originator to Administrator II - Administrator to External III - External to Administrator IV - Administrator to Originator V - Final Version From Originator to administrator			

Table 25 . Time and Cost of Secure Transmission (Examiner B)

In this case, the whole process took about 19 days and the additional cost was £7.30 (for guaranteed next day delivery) as well as the added time of the administrator to re-organise the process in a short time. There was also pressure on the external examiner to provide feedback within a shorter time scale than usual, which also potentially jeopardises quality of feedback. In this case the main reason for lack of success was that the external examiner did not take part in the electronic experiment. The examiner was visited personally and was extremely supportive of the whole experiment. No reason was given as to why he did not take part in the pilot. As such the whole process was delayed by over 2 weeks. The pilot was over-ridden and the papers were sent by courier in a state of extreme delay which jeopardised the examination preparation deadline. The fact that the originators sent their papers to the administrators securely and speedily, indicated some success in one stage of the process.

In the two instances involving Examiners A and B, we can see that in second case, the Secure Electronic Process was totally unsuccessful, in the second the new process was successful. It is also clear that the installation process and co-operation of the users is a crucial part of the success of the process. The results of the " experiments" are summarised in Table 26.

METHOD OF PAPER TRANSMISSION	TIME THE PAPER IN THE SYSTEM ONCE SUBMITTED BY ORIGINATOR					Total Time	ADDITIONAL COST
	I	II	III	IV	V		
Traditional	2-5 mins	1 day	3 days	1 day	1 day	6 days	£7.30
Successful Secure Electronic	2-5 mins	1 hour	1 hour	1 hour	1 hour	4 hours	None
Key: I – Originator to Administrator II - Administrator to External III - External to Administrator IV - Administrator to Originator V - Final Version From Originator to Administrator							

Table 26 . Comparative Times and Costs of Traditional and Secure Electronic Processes

Thus, when the electronic submission process is used to its full potential, it is faster and more cost effective than the traditional transmission process. The following sections will deal in more detail with the factors of success and failure encountered in the pilot.

1.3 Key Success and Failure Factors of the Department Y Pilot

The following section will summarise the range of problems encountered both by the users and the technology which contributed to the success and failure of the secure electronic transmission pilot at the Department Y.

1.3.1 The Users

The users of the pilot encountered a number of difficulties. The user stakeholders have been categorised according to their role in the examination process, in order to understand the needs and requirements of users at each stage.

- I. The Administrator** - found it difficult to grasp the concept of secure transmission of electronic documents. The demography of this user is aged 45-54 who does not have a home Internet connection and has never used security software. However the attitude and thoughts scores indicated that this participant was not a technophobe, but rather needed more intensive and structured training in the use of the software and understanding the concept of security and authentication and the new process.

- II. The Originators** – there was a distinct difference in the needs and requirements of these users. Those who had not had experience or knowledge of security software before:
 - Needed documentary support
 - Encountered problems that were mainly with encrypting documents for the intended recipients. There was a problem understanding that the document had to be encrypted for a particular recipient in order that only they could decrypt it. This showed a necessity for explanation and documentation of the concept of and actual process of sending secure examination papers.

Other problems encountered were password problems. With this software passwords have to be a minimum of 8 characters of which one has to be numerical and uppercase. Participants found this difficult to remember and three of the six forgot their passwords. However those that did not, used a password that they regularly use elsewhere. This again suggests a necessity for explaining and educating users on the necessity for secure passwords and making practical suggestions, which would aid users to remember their passwords.

III. The External Examiners – the attitude and thoughts scores of both these participants were very similar. Both were technophiles, confident and comfortable with computer usage, and were enthusiastic about the project. However, the respondent who used the software successfully had previously used security software, had a home Internet connection and was in the age group 35-44. The respondent who did not use the software, had not used security software previously, did not have a home Internet connection and was in the age group 45-54.

1.3.2 The Technology

Network difficulties delayed installation and training. There was a period of a week when the internal networks were not fully operational due to the failure of a piece of hardware. The technical support department, which has the responsibility for dealing with the University networks, did not have the resources to fix the problem immediately, which lengthened the delay. This network problem occurred at the time when Department Y participants were due to have Entrust installed, become registered and trained in the use of the software. Further problems also had an impact on the Entrust security software where it was unable to register new users. The problem was due to the university's network administrator who had modified the DNS tables for the university. These translate user-friendly names into computer-friendly numbers (e.g. venables-0068.uni-s.ac.uk rather than 146.87.80.68). The software provided to end-users referenced the central server by its name rather than its number, as this improves mobility and failure recovery. Therefore, the unexpected change in the name of the central server caused the security software to fail.

1.4 Implementation of the Process

The participants were asked whether the new process should be implemented university wide and how this could be best done. The majority of participants felt that an electronic means of submitting examination papers would be more convenient and beneficial in terms of time saved, administration and costs. However a number of improvements had to be made in order that the process becomes successful. Those suggested were:

- An analysis of the whole process of examination submission. For example, some participants felt that originators should communicate directly with the external examiners in order to receive the feedback immediately, to ensure that the final version submitted to the students was that intended by the originator. It was felt that the administrator should be more as a supporter and timekeeper rather than a controller of the process. It was also felt that there should be an internal quality assessment process to improve academic quality and standards.
- It was necessary to have a level of commitment from all members involved in the examination process – from the originators, the administrators and the external examiners
- The process must be consistent – either all electronic or all paper based. It was not workable to have a mixture of processes since there was no consistency in administration, which would require more administrative time for both the administrators and the external examiners.
- All users need to be registered and trained in the process before embarking on such a time critical project
- Ensure that password retrieval is an easy process, and introduce some mechanism so that passwords can be remembered

All the participants from Department Y would use the process again and all thought it was a better method of examination paper submission and with improvements and analysis of the process overall, should be implemented throughout the whole organisation.

2. Department Z

2.1 The Sample

The population of exam papers from Department Z, were selected only from the IS and CS topics, since the MS related papers had to be excluded because they did not fulfil the sample selection criteria. The MSs related papers and answers are prepared by hand and not in an electronic format, which is a necessary requirement for the electronic transmission process being used here. Another reason these papers were excluded was that the mathematical software used in some cases is extremely specialised which would have excluded the administrator, the examinations office and some external lecturers from participating in the project.

Six papers were selected randomly. Two of the papers for the courses selected had been running for more than 5 years. Two had been running for 3 years, 1 for 2 years and 1 course was new. One of the lecturers had been running the course for 5 years or more, 3 had been running the course for 3 years, 1 had been running the course for 2 years and 1 lecturer was new to the courses. All examination papers were prepared electronically. The non-confidential attributes are summarised in Table 27.

The Sample of Examination Papers Selected					
Subject	Length the course has been running	Length the current lecturer has been running the course	No. of people involved in setting questions	Length of exam In hours	Content of Exam
IS	0 yrs	0 yrs	2	2	text
IS	2 yrs	2 yrs	1	1.5	text
CS	2yrs	2yrs	2	2	text
IS	3 yrs	3 yrs	2	2	text and table
IS	3yrs	3yrs	1	1.5	text
CS	6/7 yrs	3 yrs	1	2	text & graphics

Table 27 Department Z Sample Group Attributes

Figure 34 illustrates the Department Z Department's Examination paper sample selected.

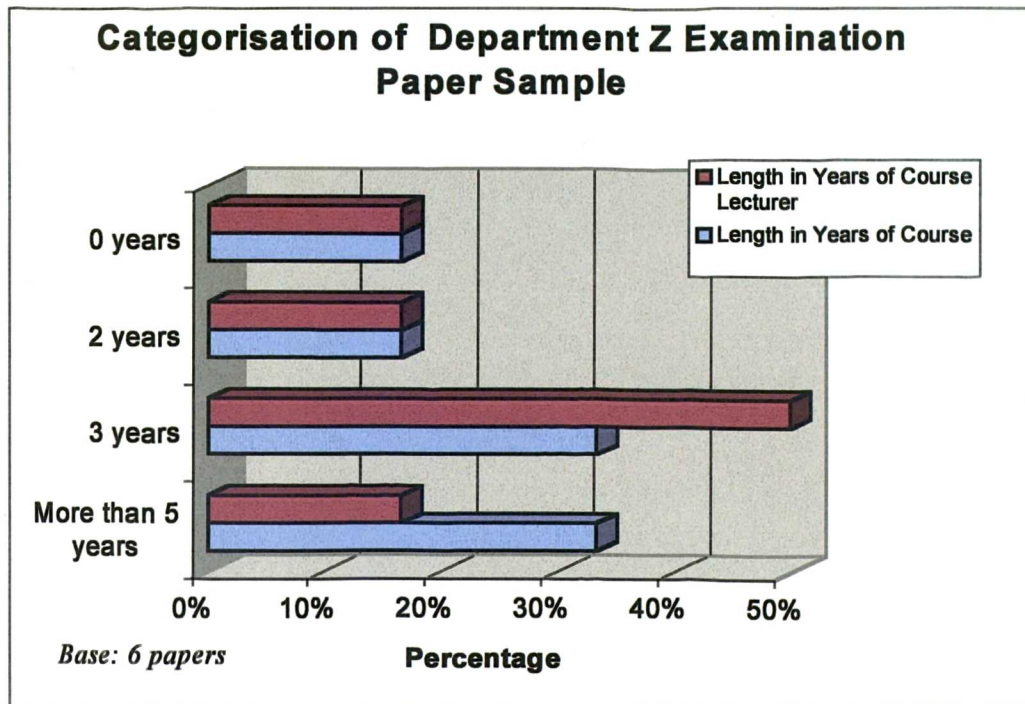


Figure 34. Categorisation of Department Z Samples

In this department, there is a quality assessment system, where originators send the questions to the internal quality assessors before submitting it to the examination administrator. As such, some of the papers selected have dual role participants. Thus the total number of papers selected was six, but the number of participants is nine. However, of those papers selected, one was prepared manually and not electronically and thus two participants had to be discounted. For another paper selected, the originator refused to co-operate mid-pilot and thus had to be discounted. Thus the final total sample of participants was six.

2.1.1 User Profile - Demographics of Department Z Participants

All the Department Z participants were lecturers with postgraduate qualifications. The main age group of participants was between 35-44. Figure 35 illustrates the demographics of the examination project participants.

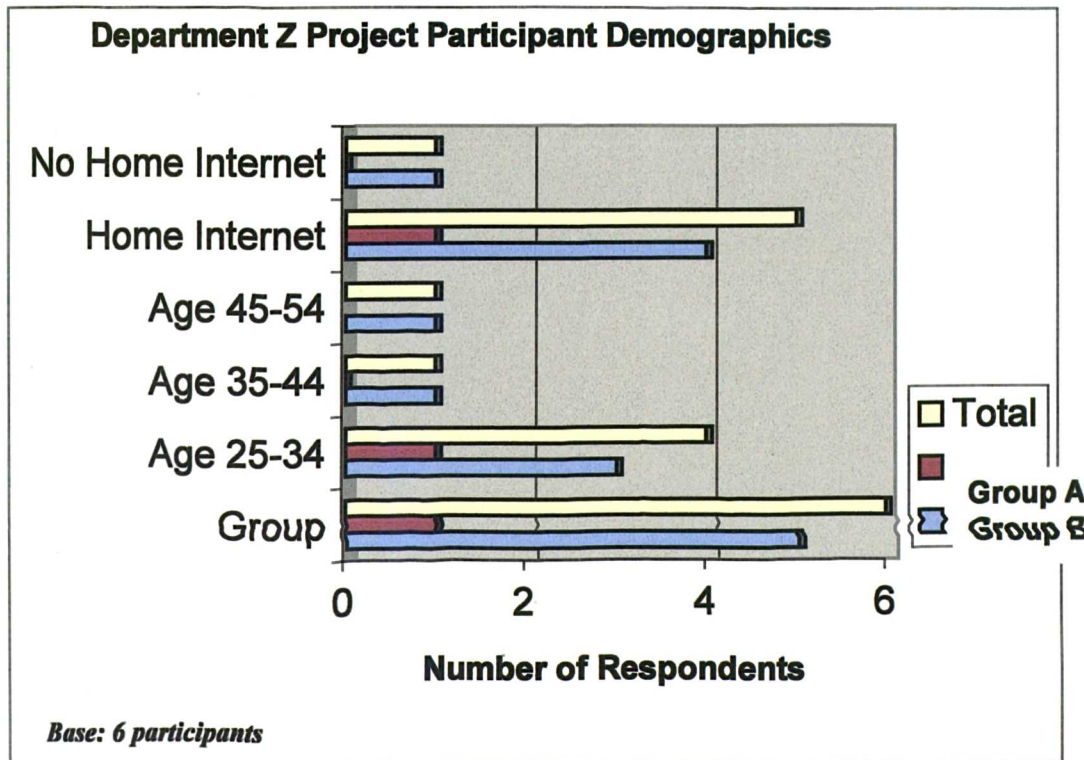


Figure 35 . Demographics of Department Z Participants

2.1.2 User Profile - Computers and Technology Habits and Attitudes

All the participants used computers both at work and at home on a daily basis. Computer usage was mainly concentrated in the area of presentations, e-mail, Internet, word processing and spreadsheet. The main software used is Microsoft Office and Lotus mail products, but the operating and administration systems in this case were mainly Windows NT and Novell. This begins to raise the problems of software compatibility across departments. Nearly half the participants also use computers for software engineering.

As with the Department Y participants, included in the questionnaire are statements, which measure specific thoughts, attitudes and cognitions that people have when working with computers and technology or when contemplating working with technology. These statements have been psychometrically tested as a measure for technophobia using the same measures as previously. In this case it is not the individual scores that are of particular significance, but rather the comparative scores of the participants. The higher the score on attitudes to technology and the lower the scores on attitudes, the less comfortable and confident the respondent is likely to be with technology, and the more likely they were to be technophobes.

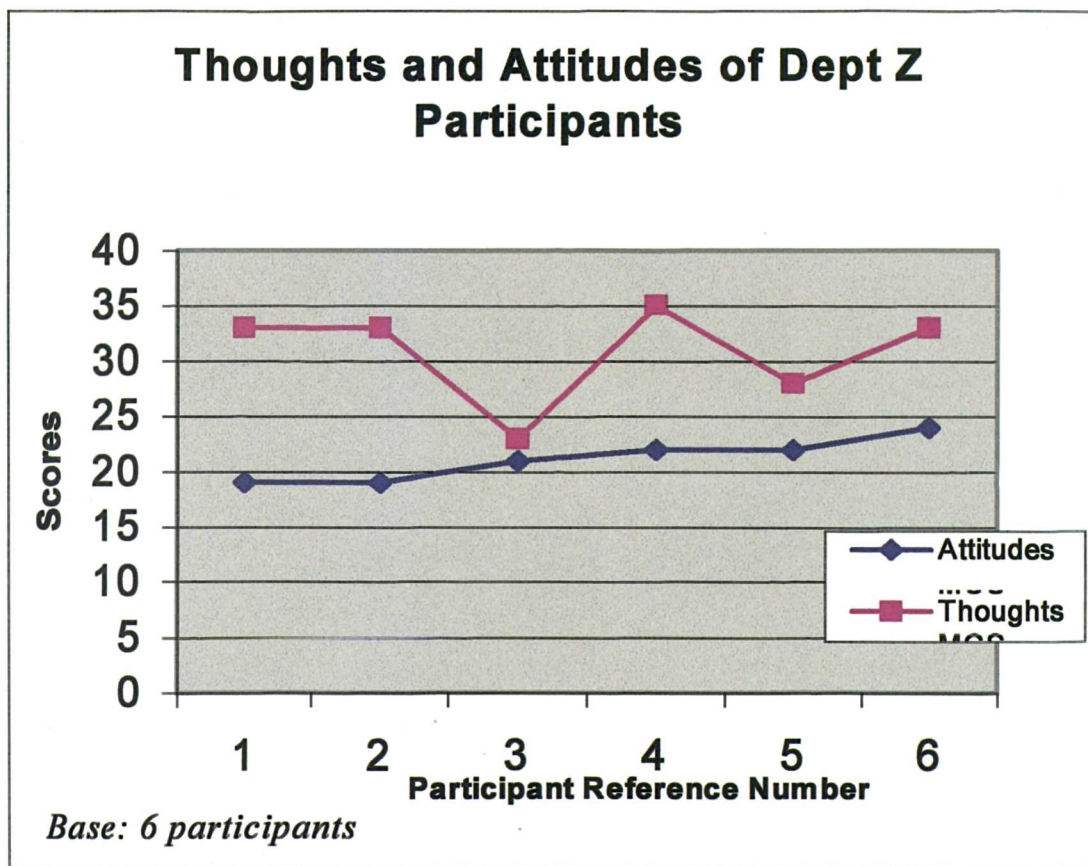


Figure 36 . Attitudes to Technology of Department Z Participants

Because of the lack of participant completion and co-operation in the project, information was limited, but showed similar participant profiles with no real distinction.

One respondent's score on thoughts about computers and technology was lower than the other participants, which indicates that the respondent is not amenable to computerisation. This was borne out when the same respondent felt that implementing the new electronic process would be full of problems and that there were no benefits whatsoever. This respondent was also in the 45-54 age category. Whereas, the younger the respondent, the more the attitude and thoughts scores indicated they were responsive to and enthusiastic about technology and new computerised processes.

2.2 The Examination Process

The examination process at Department Z differs from that in the Department Y because of the involvement of the examination office in the printing and distribution process. The following section will describe the examination preparation process as it is currently used in the Department Z Department and the pilot process.

2.2.1 The Current Examination Process

The current method of examination preparation and submission is illustrated in Figure 37. The lecturers originate examination papers, which are sent (by internal mail or handed personally) to an internal quality assessor. The papers are returned to the originator who then sends the amended papers to the exam administrator. The administrator then arranges for the relevant printed examination papers to be sent by registered mail to the relevant external examiner for feedback.

The next stage is where the external examiner(s) returns the examination papers (with feedback) by courier/registered mail. The administrator receives and collates the examination papers for distribution to the relevant examination originator for necessary revision by internal mail or personally.

The final stage is the stage where the revised final versions of the examination papers are sent to the administrator. The administrator (or originator[‡]) then sends the examination papers to the exams office for printing. Once the papers are printed they are returned to the administrator for distribution amongst the students.

Examination Paper Production Process

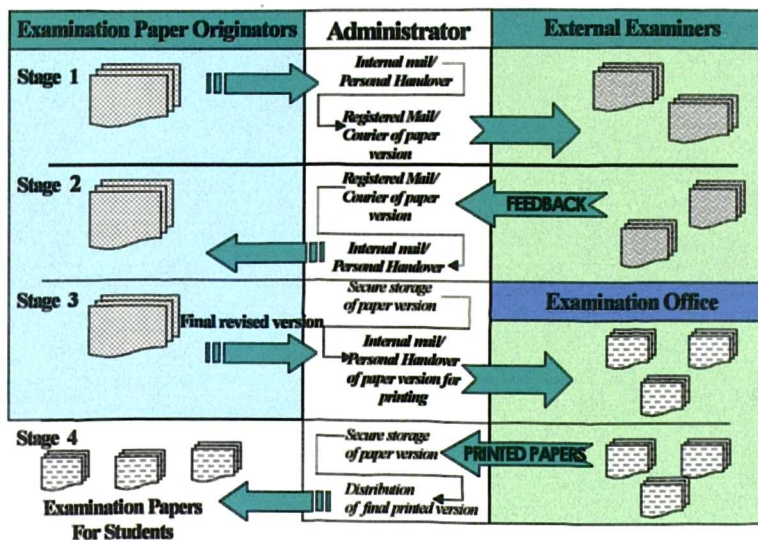


Figure 37 . Department Z Examination Paper Production Process

2.2.2 User Opinions on the Current Process

Half of the participants felt that the current Department Z Examination process was adequate and there were no problems. Those who felt it was satisfactory and did not need any change tended to be in the higher age group, including the examination administrator. The younger the respondents, the less likely they were to have been running the respective courses for a long period of time, and the more likely they were to be critical of the existing system. Figure 38 gives an indication of the levels of satisfaction by age groups.

[‡] If the deadline is missed

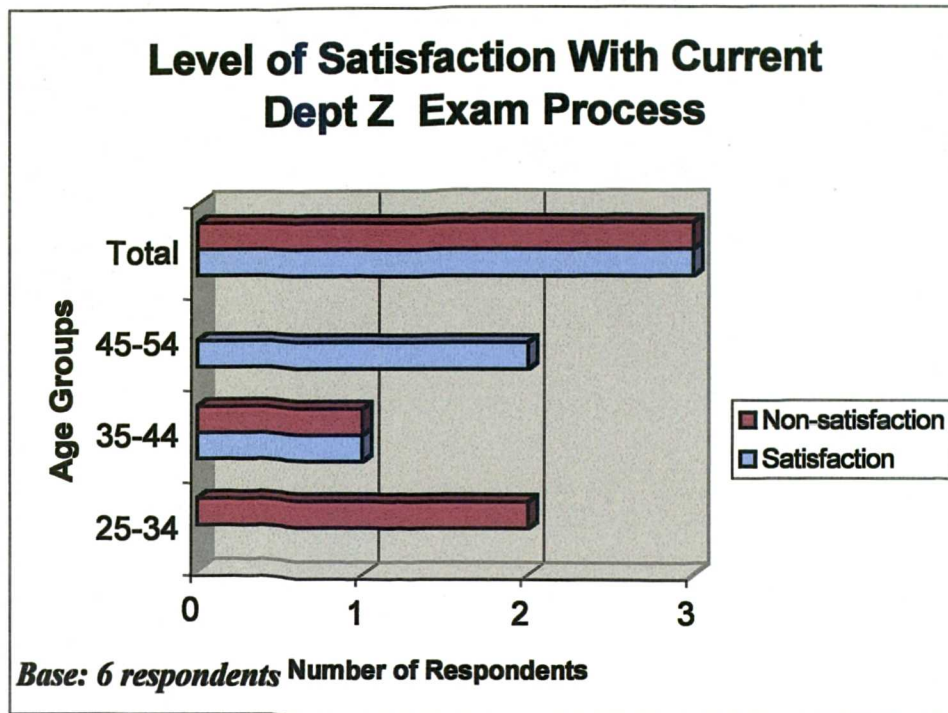


Figure 38 . Levels of Satisfaction of Department Z Participants

Of those who were critical of the current system, the comments were that it was:

- Antiquated with no flexibility
- Slow
- Insecure
- Poorly administered – lack of organisation and information
- No consistency in exam preparation format or software used
- Too much paper work

All the participants were prepared to send examinations by e-mail, so long as it was secure and the system introduced was proven to improve the current process. Some of the comments made were:

- E-mailing examination papers would save time
- Electronic examination papers are more manageable
- More convenience and flexibility by having the ability to send and receive examination papers from any location

- One respondent felt that the current examination process was adequate and that the current process first should be analysed independent of the technology and then amendments made. This respondent also felt that any new process should not be made compulsory or imposed forcibly.
- It was also felt by a number of respondents that the system had to be tested adequately before being implemented. The fact that a time critical process such as the examination production process could be jeopardised by a technical hitch was seen to be extremely dangerous
- One respondent felt that more documentation and explanation of the new process was necessary and that the system suggested was incomplete.

2.3 Key Success and Failure Factors of the Department Z Pilot

The majority of participants who were selected randomly, were unwilling to participate in the project at the outset and had to be persuaded by explaining the project and using incentives[‡]. This is useful because it mirrors the likelihood of meeting resistance to change elsewhere in the organisation. The pilot in the end was not used by any of the participants due to a combination of reasons, which were both technical and user orientated.

2.3.1 User Resistance To Change

The importance of the technical problems, discussed in the next section, were magnified by the software conflict problems experienced by the administrator, who was the central point in the department's exam preparation process. Alternative ways^{**} were suggested to allow the administrator to participate in the project, but the administrator ultimately decided that to do so would have too much impact on her working practices. The profile of this user is aged between 45-54, does not use a computer or Internet connection at home. Since this user withdrew from the project, it was not possible for anyone from the Department Z to participate in the pilot. Thus an analysis of the Department Z's use of the secure electronic examination preparation process could not be made.

[‡] a £20 gift voucher

2.3.2 The Technology

The network problems encountered by the Department Y also had an impact on the Department Z 's installation process. In addition to this, a combination of technical and operational factors also delayed matters further. There are a wide variety of computers in use throughout the university with different operating systems^{††}, network protocols^{‡‡}, and hardware attributes^{§§}.

This is the case with the Department Z. Although the Entrust security software should be able to work on any Microsoft Windows, Macintosh and Unix platforms, in one instance there was a configuration problem with the administrator's computer. It was not possible to install Entrust on this machine and although it is highly likely that the configuration of Win 3.1 and Lotus Notes was the cause of the problem^{***}, it was not possible to determine the exact cause.

2.3.3 The Examination Office

As part of the pilot project for the Department Z Department, the administrators in the examination office were involved. The administrators took part in the implementation stage of the project but due to the withdrawal by the Department Z Department, the administrators could not continue in the project. The findings from the first stage showed that the users were in the younger age group (18-35), had no higher education qualifications, did not use a computer or Internet connection at home. However, the users' attitudes and thoughts to technology and computer usage indicated that they were supportive of technology but apprehensive about new technology. Notes taken during installation revealed that although the users initially required quite intense support they were extremely responsive to and enthusiastic after training.

^{**} Install the software on a computer in a different office, have a trusted proxy to collect and encrypt the papers

^{††} Windows 3.1, Windows 95 and Windows NT Macintosh OS Unix

^{‡‡} Novell Netware, POP3 and Lotus Notes

^{§§} Memory, disk space, CD-ROMs

^{***} Computers using a combination of Windows 3.1 and POP 3; Windows NT and Lotus Notes were able to successfully install and run Entrust

From a technological point of view, one issue which was predominant, was the lack of software compatibility across departments in the organisation. The examination office did not have any version of Microsoft Office installed and was still on Windows 3.1. Its computing equipment was extremely old^{†††} with the specification of the machines unable to run the security software effectively. The participants in the project had to exchange equipment with other colleagues in the office in order that the pilot software could run at an acceptable speed.

No further assessment could be made after the implementation stage.

6.3.4 Summary

The fact that Uni X is not an SME has most impact on the areas of decision making because of the bureaucratic and hierarchically formal structure of the organisation. Thus, the decision making process of Uni X will not be included in the overall analysis, since this could distort the findings from the other case studies. This section pulls together the data from the actual implementation and usage of the security solution by two groups in the Uni X case study. It shows three main areas that have an impact on the implementation and use of IT related solutions in organisations. These identified factors are a) users, b) the technological infrastructure and the c) business process infrastructure.

6.3.4.1 The Users

The questionnaires, psychometric testing and observation of users revealed a number of issues in identifying factors of success for implementing a security solution. Some of these were common to all users. For example:

- Passwords - creating, remembering and storing passwords securely
- Human Computer Interface (HCI) - ease of use, recognition of icons, integration of security functions within commonly used applications (such as e-mail)
- Support - in both verbal and written form

^{†††} 386 machine with no CD Rom Drive

- **Training and education - both in the concepts of security and the actual usage of the software**

The research also identified three main user profiles which have an impact on the use of the security solution. These are defined as being the supporter, the potential supporter and the resister.

i) The Supporter

The supporter is a user who is enthusiastic about technology and computer usage. This user believes that automation will enhance the quality of business processes within the organisation, by improving the speed, convenience, administration and costs of the existing processes. This user will actively support the implementation of technology and computers to potentially automate paper based processes and needs no real support post implementation. The profile of this type of user is that they:

- **Are relatively new to the organisation or process**
- **Are between the ages of 25-44, but tend to be concentrated more in the 25-34 age group**
- **Score relatively high on thoughts and relatively low on attitudes to computers and technology. This indicates they are more confident users and less intimidated by and more comfortable with and enthusiastic about technology. They have positive thoughts and cognitions towards working with computers and technology and tend to have an Internet connection at home**
- **Have already used, has a knowledge or understanding of security and encryption software.**

ii) The Potential Supporter

The potential supporter is a user who is enthusiastic about technology and computer usage, but needs more support with the introduction of new software and automated processes. This user also believes that automation will enhance the quality of the examination production process and is prepared to support it actively once the process is understood and there is an infrastructure to facilitate and assist users when necessary. The profile of this type of user is that they tend to:

- Be relatively new to the organisation or process
- Be newer lecturers and newer courses of about 2 years or less
- Be between the ages of 25-44
- Need practice, training, and more support from documentation.
- Have no Internet connection at home
- Score relatively similar scores on both attitudes and thoughts to computers and technology. This suggests they are relatively confident and enthusiastic about technology, but need more support

iii) The Resister

The resister is a user who is relatively neutral about technology and computer usage and prefers the more established paper based processes. This user needs to be shown proof positive that automation is an improvement before they are prepared to implement and use any new electronic system. They see new processes as an inconvenience, a source of unnecessary extra burden on their current workload. The profile of this type of user is that they tend to:

- Have been in the department or part of the process for longer than 3years
- Be between the ages of 45-54
- See no current problems or inadequacies in the existing method of examination preparation
- Have lower scores on thoughts and attitudes towards computers. This suggests they are not very enthusiastic about technology and computerisation.
- Have no Internet connection at home

Before any kind of change can take place, a full assessment of the types of user in the organisation must be made. By identifying the type and the profile of the respective users, so it is possible to design an implementation process tailored for their differing needs and requirements, in order to facilitate a system change and increase its probability of success. As the findings from the Department Z Department have shown, without the support of the users, no system can be successfully implemented.

6.3.4.2 The Technology

The findings revealed many technological issues, which are crucial to the successful implementation and operation of the security solution. In particular:

- The organisation's network infrastructure must be adequate to support time critical systems.
- The technical support service must be of a standard, which deals effectively, and efficiently with problems that arise within a time scale that causes minimal disruption to users.
- There must also be an adequate network back up system to support users in case of longer-term infrastructure problems.

The case study also highlighted the problem of hardware and software incompatibility within the organisation and with external stakeholders. The diverse types of hardware, network infrastructures, operating systems and software that exist among different stakeholders, has a large impact on the successful operation of the pilot.

This caused problems with:

- Installation of the security software
- Opening and printing electronic documents sent between the different parties

These issues must also be addressed before an organisation-wide electronic process is introduced.

6.3.4.3 Business Processes

The case studies revealed that a detailed analysis of the organisation's administrative processes is needed, including:

- Identifying the degree of stakeholder involvement in the process selected for change.
- Involvement by all parties and stakeholders in a consultative stage.

The electronic process designed and implemented for the pilot, attempted to mirror the existing paper process. However, complete business process re-engineering would be needed to make sure the automated system made definite and measurable improvements in cost, time and efficiency. Again the co-operation and input of all stakeholders would be needed. Once an automated process was designed, it must be fully tested before implementation, including a trial period of intensive usage by all types of user to identify any problems and make any necessary modifications.

6.4 Case Studies Conclusions

This section draws on all the data gathered during the course of the case studies. The aims and objectives of the case studies were to answer the research questions,

- Does the security solution developed actually work when used by SMEs?
- What benefits are achieved for SMEs by secure use of the Internet?
- What is the process of implementation of the security solution by SMEs?

However, some of the issues raised, related to the pre-implementation stage and addressed what security actually means to SMEs.

- (i) There was no consistent frame of reference for SME security needs. Different companies have different security needs. Using Howards' taxonomy of complete computer and network attack (Chapter 2 Figure 2), we can begin to understand the different SME perceptions of security and assess their needs. *Attackers* are largely seen by the majority of SMEs as external. The *tools* used to perpetrate the attack are mainly virus (script/program) or user command where the *access* is by unauthorised access. The *results* include corruption and/or disclosure of information and the *objectives* are damage or financial gain (in the case of competitor espionage). The main security needs identified in these case studies are the prevention of virus attacks and unauthorised access to sensitive corporate records.
- (ii) The pervading attitude among SMEs to security of electronic data being transmitted was apathy and cure rather than prevention. There was a general consensus that until a security breach occurred, there was no real need for a security and authentication solution.

Although SMEs were aware of a need for security, there was no clear understanding of security in terms of electronic data authentication and security as defined in this research project. However, once the software was introduced the research questions could be addressed. Firstly, the question of whether the security solution developed actually works when used by SMEs. In the instances where it was implemented and used in accordance with the recommended instructions and guidelines, the security solution worked providing confidentiality, integrity, non-repudiation and authentication of electronic data. But two main areas of weakness, which could potentially compromise the service, were identified as the users and the network infrastructure.

- **The Users** - profiling users assessing their attitudes and thoughts on technology other issues also such as forgetting or revealing their unique identifying passwords or not understanding the encryption, digital signing and verification procedures.

- **The Network Infrastructure** - by having an inadequate network with regular interruptions to Internet access, operating systems hardware and software not compatible with the security software.

The benefits of the security solution to SMEs were mainly linked to the transmission of electronic data - namely increased speed, savings in terms of cost and improved process efficiencies, such as cutting out redundant administrative processes.

The findings from the case studies began to address the final research question - identifying the process for implementing the security solution by SMEs. Guidelines were beginning to formulate for implementation of a security solution and included assessment of users, training and educating users in the concept and importance of security, user support, technology, usability, compatibility and integration the need for business process analysis and re-engineering to incorporate the security solution.

The next chapter describes the second stage of research carried out to define further SME perception of security, attitudes to data security and identify any security infrastructures currently being used.

Chapter Seven

Further Research (I)

7. Further Research (I)

The findings from the initial telephone survey in 1996/7(Appendix 6) indicated a knowledge gap in SMEs about the Internet its benefits and drawbacks. It also showed that only 1 in 3 SMEs in the Greater Manchester region were connected to the Internet and of those that were connected, usage was limited to e-mail and "browsing" for information. There was a marked lack of awareness and concern about transmitted data security issues. The main priorities for SMEs were practical issues of support and training in the use of the Internet.

The findings from the case study stage confirmed that there was no consistent frame of reference for SME electronic data and security needs. They also showed an overall attitude of apathy and lack of awareness amongst SMEs on the issue of securing electronic data transmission.

Both sets of findings also raised more questions that needed answering. For this reason, the research was undertaken to clarify the lack of participation in the project by SMEs and to explore further changes in,

- SMEs perceived security needs and attitudes to security
- Internet usage patterns and SME network infrastructures
- The viability of the security solution designed for use by businesses

The methodology used to answer these questions was twofold.

- (i) A number of depth interviews with managerial decision-makers to explore more deeply, user attitudes to secure electronic transmission of data and the security and authentication service in particular.
- (ii) A time series survey where the sample of Greater Manchester SMEs used in the 1996-97 telephone survey were contacted again in 1999, to assess their progress in technology usage and any changes in attitudes or usage patterns.

This chapter will describe the research in more detail.

7.1 Depth Interviews

The aims of the qualitative depth interviews were to assess the viability to businesses of the security solution by:

- Beginning to explore the characteristics of different industry sectors which would make them more or less amenable to a Trusted Third Party (TTP) service
- Gauging the reaction of businesses to a TTP service
- Identifying the decision making process and criteria that might lead to the implementation of the security solution.

7.1.1 Methodology

Thirteen companies from the retail, manufacturing and service industry sector were selected randomly from the regional Chamber of Commerce database, for face-to-face structured depth interviews. The interviews were carried out in February 1998, on the respondent's premises and lasted about 40 minutes. The guideline for the topic areas put to each of the respondents is included in Appendix 18. Incentives* were offered to the respondents to secure the interviews. The interviews were carried out with managerial personnel according to Market Research Society's (MRS) rules and conditions, which emphasises respondent confidentiality at all times, thus the contact details are not included in this study. A profile of the sample of respondents interviewed, is summarised in the Table 28.

RESPONDENT'S TITLE	TYPE OF COMPANY	INDUSTRY SECTOR	SIZE OF Company No. Employees
IT Manager	Components Engineering Company	Manufacturing	<200
Financial Director	Clothing Manufacturer	Manufacturing	100
Head of Communications	Engineering Company	Manufacturing	50
Communications Manager	Alarm Systems Manufacturer	Manufacturing	72
Systems Manager	Franchised vehicle dealer	Retail	25
IT Manager	Motorcycle Retailer	Retail	20
Database/IT manager	Large Retail Optician	Retail	250
Strategy and Development Manager	Insurance Retailer	Retail	300
Insurance Systems Manager	Insurance Underwriters	Service	100
Facilities Manager	Car Breakdown and Recovery Service	Service	>250
Business Systems Manager	Building Society	Service	>200
IT Manager	Solicitors Firm	Service	15
IT Manager	Primary Commodities Broker	Service	10

Table 28 Profile of Depth Interview Respondents

* £20 gift vouchers

7.1.2 Findings

The depth interview participants were mainly from companies with more than 50 employees. Only 30% of the sample were very small companies with no fewer than 10 employees. The findings will show a more organised corporate infrastructure and more formalised business and decision making processes than those in very small companies. The main findings of the depth interviews have been summarised and structured into four areas covering the organisational infrastructure, e-mail usage and uptake, future communications and business strategies and trusted third parties.

7.1.2.1. Organisational Infrastructure

Decisions about implementing new technology and IT facilities are made at director level, based on the presentation of a business case showing the advantages and disadvantages of the new technology to the organisation. In larger companies, a project team would be set up headed by the IT manager, to develop a plan outlining the cost/benefits to the organisation and stages of implementation.

Technologically, the majority of the larger companies (with more than 50 employees) had AS400 networks with LAN/private connections with their branches. Internet connection was through a single gateway at head office controlling incoming and outgoing packets of information including e-mail. In smaller companies, Internet connection is mainly limited to a stand alone PC with a single link via an Internet Service Provider (ISP) and modem.

Fax is used extensively by all the respondent organisations. The general opinion among respondents was that fax will be replaced by e-mail since it provides fast and immediate communication at a lower cost. The majority of companies felt there was no need for added security when sending a fax and would send anything by fax. Because they were less familiar with e-mail, the majority of respondents did feel that e-mail was less secure than fax and respondents also felt that postal mail would be

eventually replaced by e-mail. But, before this could happen, many issues would first have to be resolved. Such as,

- The quality and integrity of the message which recipients would finally receive.
- The legal requirements of having/sending electronic documents and hard copies of these.
- Security and confidentiality of information.

Retail and manufacturing organisations in particular felt that mailing brochures and attractive literature would be hard to replace in the short and medium term and that there was no substitute for sending or receiving physical goods. But where couriers or special delivery services were required for documents, a TTP e-mail service could be a replacement.

7.1.2.2 E-mail Usage and Uptake

The introduction of e-mail facilities in the respondent organisations was relatively recent mainly within the past six months to two years. For the majority of respondent companies, e-mail was used most extensively for internal communication purposes. The average spread of e-mail usage in an organisation was estimated to be about 15% -25% of all employccs but did not include internal e-mail usage. In most cases, external e-mail access was available mainly to managerial staff and specific departments such as marketing, sales and design who have contact with customers and suppliers.

The respondents felt that one of the major concerns about e-mail and one of the most common reasons for lack of implementation and usage of it, was employee technophobia - a fear of the technology with which they were unfamiliar and unaware. From a managerial perspective the main security concerns were over computer virus infections from Internet downloads and the need for e-mail filtering to control the information and systems overload caused by junk e-mail.

All these factors contributed to the delay or under use of e-mail in organisations.

7.1.2.3 Future Strategies

For the respondent companies in the service sector in particular, the future communication strategy was to develop a "paperless office" where paper documents would no longer be in circulation. In some of the organisations, this had become a reality on an internal basis, where memos and internal messages were mainly electronic. But communication with external stakeholders, was still based largely on paper and fax.

While all the respondents believed that e-mail would become the future communication medium, opinions on the degree and speed to which this might happen varied from sector to sector and reflected the overall attitude to and implementation of the Internet.

The Service Sector - particularly insurance (underwriters) and law - were leaders and were encouraging their trading partners to communicate by e-mail. Because this sector delivers a service the speed and reliability of communication is crucial to providing a better service.

The Manufacturing Sector - were laggards where implementation of the Internet and e-mail was a slow process and traditional manufacturing (e.g. heavy engineering, clothing manufacturing), were particularly slow to use this medium unless specifically requested by their trading partners. Of the manufacturing organisations using e-mail, this was mainly internal or external for the transmission of technical drawings and specifications.

The Retail Sector - retailing in this instance is considered part of the service sector. Although electronic means of communication are being introduced, until this became prevalent with their customers, it limits their own use of electronic communication.

7.1.2.4 Trusted Third Party

The trusted third party security service was explained to respondents. Very few respondents had heard of digital encryption and certification authorities and none were using it. However, the respondents from the service sectors were particularly positive about this service mainly because they were already using e-mail extensively and could see the benefits of digital signatures and a trusted third party service. The manufacturing sector in particular could see no need for such a service. The respondents felt that the best way to sell such a service would be to explain exactly what it does, how it will benefit the company, and emphasise the ease of installation and use.

7.1.3 Conclusions

The depth interviews provided a wealth of detailed information allowing a deeper understanding of the research issues raised. The data gathered from these depth interviews, supported the earlier findings from the case studies and first stage of the telephone survey. That:

- There was neither an awareness of nor a perceived need for a security and authentication service. However, once the concept was explained, there was an overall enthusiasm for a TTP service.
- The security needs identified by SMEs concentrated on virus prevention/protection and controlling volumes and filtering of e-mail.
- E-mail usage and implementation is increasing in organisations. Larger organisations who are dealing in the service sectors are the early adopters of the Internet and e-mail with manufacturing companies being laggards.
- SME network infrastructures were designed in a way that ignored data security in transmission.
- Employee technophobia is a barrier to the use and implementation of IT in organisations.
- E-mail is seen to be the eventual substitute both for fax and paper mail.
- The decision making process for implementation of new communications related technology is based on the presentation of a business case defining clearly the benefits to the company and detailing the costs involved.

7.2 Telephone Interviews

A time series telephone survey was conducted in the final stages of this research project. This quasi-experimental method was used to measure the impact of information dissemination and also any changes in Greater Manchester SMEs usage and attitudes to the Internet, e-mail and security. The original sample of SMEs selected in 1996 for the telephone survey (Appendix 6) was used again to ensure that the sample population of organisations was constant. Only the organisations that had given a response in the original survey were contacted, to obtain an accurate picture of the changes in each organisation.

The sample was made up of exactly the same 119 companies, which had given a response in the 1996/7 survey. The companies were contacted by telephone again and the respondent requested was the IT manager of the organisation. Since the majority of the sample consisted of small or medium sized organisations, often there was no IT manager, so instead, either the owner/manager responded or the person who dealt with IT issues replied to the questions (appendix 7). The following questions were asked:

- Was the organisation connected to the Internet?
- For what purpose were they connected to the Internet - E-mail ; web browsing; ftp or other
- What did they use the Internet for?
- Did they have a web page? If so what was the address and what was it used for e.g. just a presence? to take orders over the Internet i.e. electronic commerce
- Number of employees to determine any changes in size
- What security features they had installed
- What they used e-mail for - whether it was purely internal, whether they received information and orders from their customers and suppliers by e-mail etc.

This information gathered was then compared to that collected 2 years ago to gauge the degree of change in attitudes to the physical presence and usage of the Internet in the organisation.

7.2.1 The Telephone Sample

The sample for the 1999 telephone survey was made up of the same 57 respondents from the service sector as those in the 1996/7 telephone survey. These included:

- Travel agencies
- Employment and training agencies
- Transport and road freight
- Consultancy (business and IT)
- The professions (accountancy, law)

Fifty four respondents were from the manufacturing sector comprising:

- Electronics and engineering
- Software development (here considered manufacturers of software)
- Textiles
- Chemicals
- Machinery manufacturing industries

There were also 8 companies in wholesaling and retailing of goods herein defined as the trading sector.

The rate of response in this survey was 71%, slightly lower than the 82% of the 1996/7 survey sample. The non-respondents were made up of 9% who refused to participate and 20% unobtainable numbers. The unobtainable numbers in the 1999 survey were concentrated in the group of companies with less than 50 employees, where nearly two thirds of these companies had not been connected to the Internet in 1996 and had felt that the Internet would be of no benefit to them. Whilst it might be tempting to conclude that Internet connectivity had some relation to the change in circumstance of the organisations, more research would have to be conducted to identify the factors responsible for the change in circumstances, which is beyond the scope of this project.

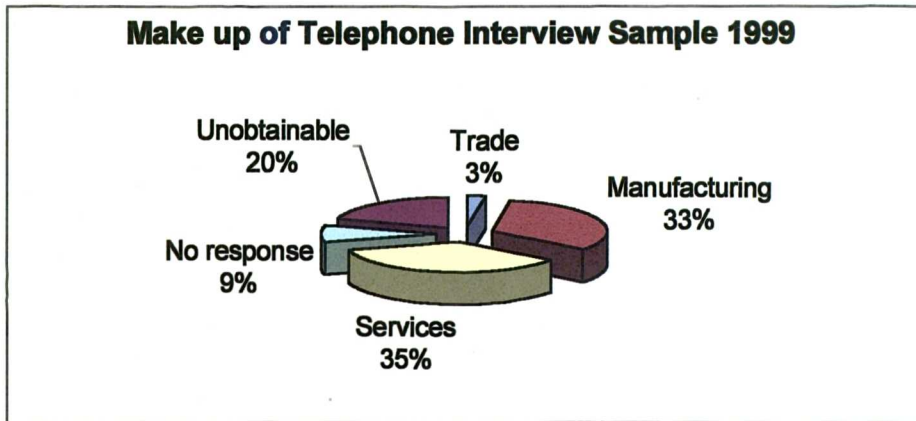


Figure 39 . The 1999 Telephone Survey Sample

Table 29 illustrates the breakdown of the sample of respondents in the telephone survey, according to company size by number of employees.

Number of Employees	Manufacturing Sector	Services Sector	Trade	TOTAL	% age of Total Sample
<50	29	27	2	58	70%
50-100	3	8		11	13%
101-200	3	4		7	8.5%
>200	4	2	1	7	8.5%
Total	39	41	3	83	

Table 29 . Breakdown of Respondents Company Size & Industry Sector (1999)

7.2.2 Survey Findings

This survey traces the trend and growth in Internet usage by small and medium sized businesses in the Greater Manchester region. In 1996, It was found that 34% had the Internet installed and 66% had no Internet.

Company Size by No. of Employees	1996 Total %age of		1999 Total %age of	
	Internet	No Internet	Internet	No Internet
<50	22%	78%	64%	36%
50-100	69%	31%	91%	9%
101-200	62%	38%	71%	29%
>200	88%	12%	100%	-
Total	34%	66%	71%	29%

Table 30 . Percentage of Companies Connected to the Internet by Size

By 1999, 71% of all SMEs had the Internet and 29% had no Internet, indicating a rate of growth in Internet penetration of over 100% in the past 2 years.

The greatest change has been in companies with less than 50 employees. The reason for this high degree of change is the fact that the smaller the company, the slower and less likely they are to introduce new technology. Although the change is greatest in very small companies, the larger companies are already starting from an Internet connectivity base of over 60%. Throughout the survey, there was found to be a positive correlation between the size of an organisation and its connectivity to the Internet.

The usage patterns and changes in the respective sectors are identified in more detail. The figures are shown as a percentage of the total sample size of companies, which participated and co-operated in the survey at that specific period of time.

7.2.2.1 The Service Sector

In the Service Sector, the number of companies which are currently connected to the Internet is almost double that of two years ago. As a proportion of the total respondents in the service sector, 46% were connected to the Internet in 1996 and 54% were not connected.

In 1999, 85% of respondents in the service sector were connected to the Internet and only 15% were not connected. The rate of growth of connectivity has more than doubled and has been greatest in the group of companies with less than 50 employees. Companies with up to 100 employees has also increased, but less dramatically. By grouping the respondents into size of organisation, we can get a better picture of the pattern of changes of SMEs in each sector.

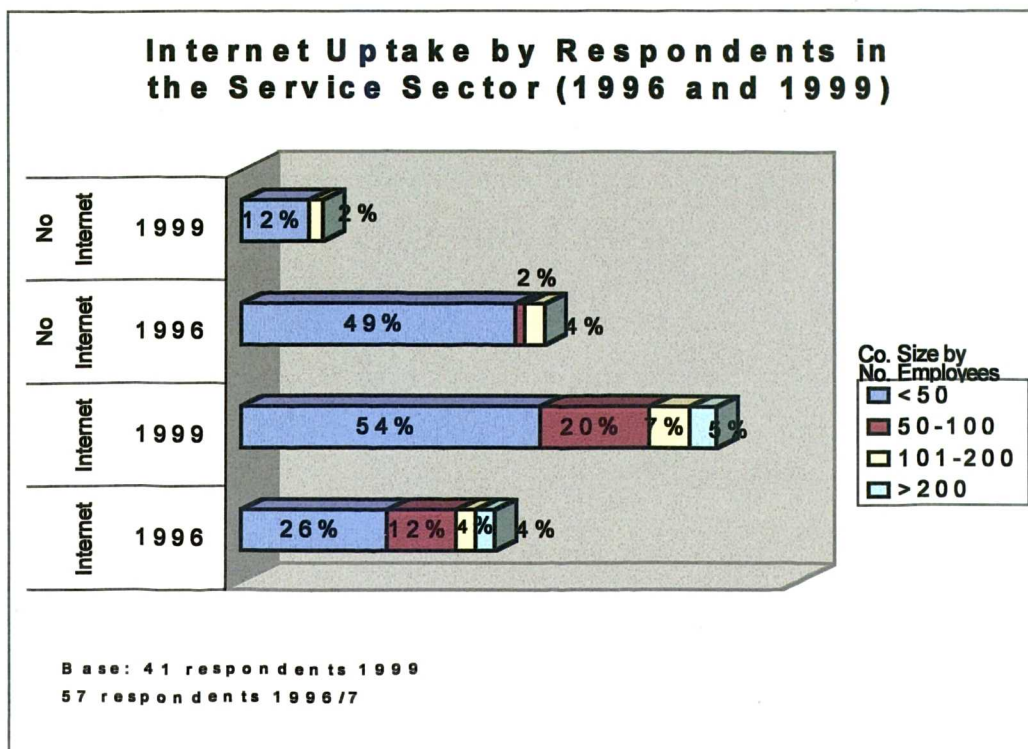


Figure 40 . Internet Uptake in The Service Sector

a) Companies with less than 50 Employees

All the respondents connected to the Internet in 1996 were still connected in 1999. Whereas in 1996, the usage was basic and mainly limited to e-mail and browsing for information, by 1999, the use of the Internet by this group had become more sophisticated. Two thirds of the companies connected to the Internet in 1996 had installed a security infrastructure, which included encryption facilities and firewalls, mainly for e-mail by 1999. All had a web site, with two thirds using it for developing an electronic commerce strategy where products or services could be sold or provided via the web site. The types of companies, which had developed such a level of sophisticated usage, were concentrated in consultancy and Information Technology service areas.

Nearly one in five of the companies not linked to the Internet in 1996 were still not linked in 1999. These were mainly traditional service providers, such as architects, security services, freight and travel agents. Of these, one had a web page hosted by a third party, one company was not interested because they could see no benefit to their

company and the other 3 companies were considering installing the Internet and had plans to come on-line within the next 6 months.

Of those companies not linked to the Internet in 1996, about one in five had felt that there was no benefit of having the Internet and would never use it. These companies would not co-operate with the 1999 survey so their present status is unknown. These were mainly in the traditional service sector - freight, accounting and marketing/promotions.

Nearly half of the respondents who were not linked to the Internet in 1996, had become linked in 1999, but security was not an issue for them and the Internet was used mainly for e-mail, a source of information and file transfers from head offices to branch offices. Over three-quarters of these recently connected companies had a web site, which was used mainly for maintaining an advertising presence. Only 15% were using it in a more sophisticated way, for electronic commerce providing a product or service via the Internet. The majority of the corporate web sites had only been set up for six months or less from January 1999. The companies that were found in this group were mainly in the training, recruitment, travel and accounting service sectors.

Of the respondents that did not participate in the 1999 survey, nearly half were from the service sector with less than 50 employees with a) no connection to the Internet, b) the belief that the Internet held no benefit to the company and c) no interest in learning more about it. The companies in this group were mainly in the marketing, training and security service sectors.

b) Between 50-100 Employees

Nearly 90% of companies of this size, were connected to the Internet in 1996 and had been using it mainly for e-mail facilities and as a source of information. There were, however, some notable changes in the extent and sophistication of both usage and attitudes towards e-mail amongst this group over the 2 year period. None of the respondents who were connected to the Internet in 1996 considered security an issue or a consideration. Only two out of the seven respondents in 1996 had web sites, but

these were not used or integrated into any business growth or marketing strategies. The web sites were set up merely to assert a presence on the Information Superhighway because *"it was the thing to do"*^{*}. By 1999, six of the seven respondents had a web site. The same two respondents who had a web site in 1996, had developed it further to allow e-commerce and placing of on-line orders for their services.

By 1999, over 70% of the respondents connected to the Internet had developed a security infrastructure, which included the installation of a firewall or the development of an Intranet.

Of the respondents, who did not have any security, neither did any of these have a policy about the use of e-mail and the Internet. They felt that in the organisation at the moment, everything was *"fly-by-night"*^{*} and the use of the Internet was growing in the organisation with no clear strategy. The majority of the respondents in this group were mainly from the consultancy, project management and IT related services.

By 1999, the sole respondent who had not been linked to the Internet in 1996, was now connected. Initially the company had felt that it could not benefit the organisation (a travel agent) and were not interested. In 1999, the company had developed a website, was connected to the Internet used as a source of information and e-mails with customers and suppliers. Although, there was no awareness for the need of any security measures, the respondent felt that further training was needed to fully benefit from the facilities already on offer.

c) Between 101-200 Employees

Half of the respondents in this group, had been connected to the Internet in 1996 where they had been using it mainly for e-mail. In 1999, these companies were using the Internet in a more sophisticated way and incorporating security features such as a firewall, and intranet, with the web site over which they took orders being hosted by a third party. These companies again were mainly in the high tech area of the service sector.

^{*} A quotation from one of the telephone interviews in the service sector of size 50-100 employees

Only one of the two respondent companies not connected to the Internet in 1996 was still not connected in 1999. The main reason was that this company provided financial services and felt that the Internet was far too insecure for its business transactions. Although they currently did not have a web site, the opinion of the respondent was that the bureaucracy had *"not got around to doing it yet"*.

The other respondent who was not linked to the Internet in 1996, also from the financial services sector, had developed a very sophisticated web site allowing access to a myriad of on-line services to registered and authorised customers only. Although they did not have access to the Internet, they did have an intranet and firewall for receiving and sending e-mail.

d) More than 200 employees

Of the 2 respondents in this group, both had been linked to the Internet in 1996 but did not have a web site nor did they have any security features installed. By 1999, they had developed a web site allowing them to provide their service over the Internet. Both companies still believed that security was not necessary since they believed no confidential information was ever sent over the Internet.

7.2.2.2 The Manufacturing Sector

In the manufacturing sector, the rate of growth has been even more dramatic, with overall connectivity having more than doubled. The rate of change in the companies with less than 50 employees is great, with the number of companies now connected almost triple that of 2 years ago. In the group of companies with 101-200 employees, the figures suggest that Internet connectivity has fallen. This can be explained by the fact that almost half the respondents in this group were unwilling to participate in 1999. By looking at the individual figures, a more accurate picture reveals that connectivity to the Internet has increased.

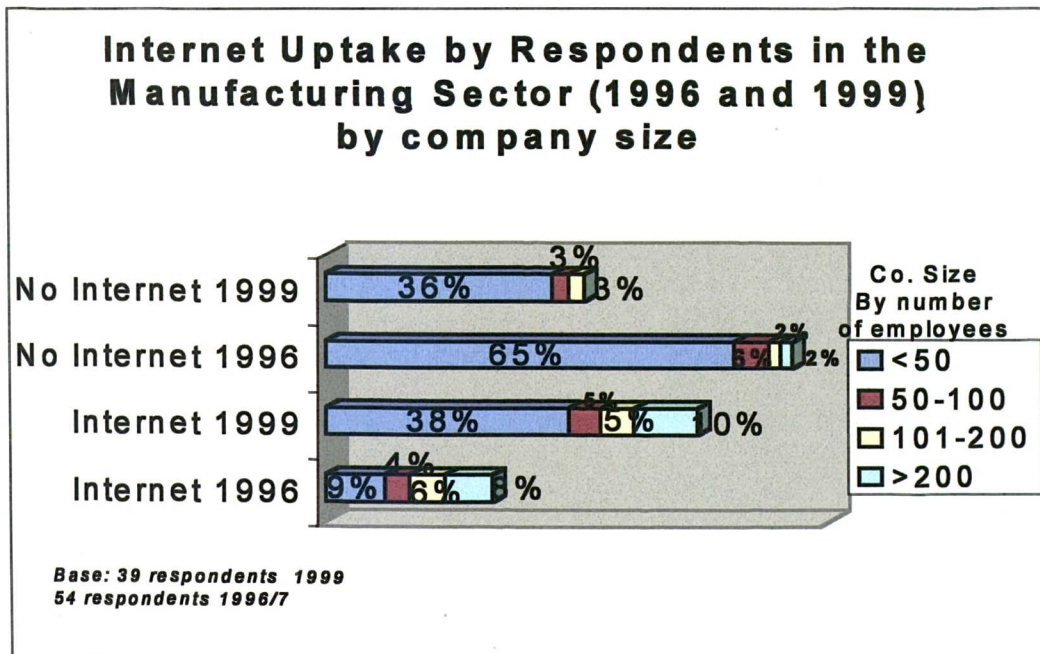


Figure 41 . Internet Uptake in the Manufacturing Sector

The findings from the manufacturing sector respondents are presented in the following sections according to the company size by numbers of employees.

a) Less than 50 Employees

All 4 respondents who were connected to the Internet in 1996 were still connected in 1999. As in the service sector, they had developed a web site and in some cases were trading goods and services via their web site. All the respondents felt that security was not an issue for them and they were using the packages for e-mail and Internet browsing that was already available on their computers' operating systems.

Of the 25 respondents who were not connected to the Internet in 1996, a third still had not come on-line by 1999 stating the same reasons - that they were too small, they could see no benefit to their organisation, they were not sophisticated enough and that they had neither the time nor money to look into it. Another tenth were in the process of getting more information about the benefits of being connected to the Internet. These respondents were mainly in the traditional manufacturing sectors such as chemicals, leather, food, machinery and textiles.

Of the remaining 25 respondents who were not connected to the Internet in 1996, nearly half had come on-line by 1999. In 1996, the opinions of these respondents had been that the Internet and e-mail would be of no use to their business, that they were too small and unsophisticated, that they were not interested because they were too busy running the business. Of all the respondents who have since come on line, half were in the process of having a web site designed within the next six months, and half already had a web site and were taking orders over the Internet. Only one respondent was aware of security and was using e-mail security facilities. The respondent would not reveal any more details. Two thirds of respondents in this group were from the traditional manufacturing sector such as textiles, clothing, machinery, cards, lifts and one third from the modern manufacturing sector - software, electronics and hi tech glass manufacturing.

b) Companies with Between 50-100 Employees

As in the service sector sample, the number of respondents in this group is very small. However, of the three respondents who co-operated, two which had been connected to the Internet in 1996 were still connected. They had a firewall-based security infrastructure and already had a web site. Both companies showed a rate of growth, where the number of employees had doubled over the past 2 years. These were in the modern manufacturing sectors of software and electronic engineering.

The sole respondent in this group from the traditional machine manufacturing sector, had no Internet connection in 1996 and was still not on-line by 1999. Although the respondent claimed he was "*thinking about it*", this showed a change in opinion from 1996 when the company was adamant there was no need for it.

c) Companies Between 101-200 Employees

Only 2 of the original 4 respondents in this group took part in the 1999 survey. One respondent had already been linked to the Internet in 1996, but had since developed a web site and was now using it as a tool for expanding its market. This respondent was from the the electronics sector.

The other respondent, was not connected to the Internet and had wanted more information in 1996, but had felt the need for getting connected. In 1999, the respondent was in the process of getting connected. This respondent was in the machinery manufacturing sector.

d) Companies with over 200 employees

Of the four respondents in this category who took part in the 1999 survey, three had been connected to the Internet in 1996 and were still connected in 1999. One of the respondents, an electronics manufacturer, in 1996 had an e-mail system which only one person could access. By 1999 an ISDN line had been installed and all employees were using e-mail and had access to the Internet but there was no security infrastructure in place. The other two respondents had set up a web site and were conducting business electronically.

One of the respondents, an electronics manufacturer, was in the process of getting connected to the Internet in 1996. By 1999 it had a web site, was conducting business over the Internet and was a frequent user of e-mail.

7.2.2.3 The Trade Sector

Because the rate of response was so low in 1999 and the original sample size was so small (8 respondents), the changes noted in this sector must be used with caution. Of the 3 companies that responded, one was connected to the Internet while the other 2 were not, compared to 1996 where all 7 of the responding companies with less than 50 employees were not connected to the Internet. Overall this shows a similar trend to the other sectors.

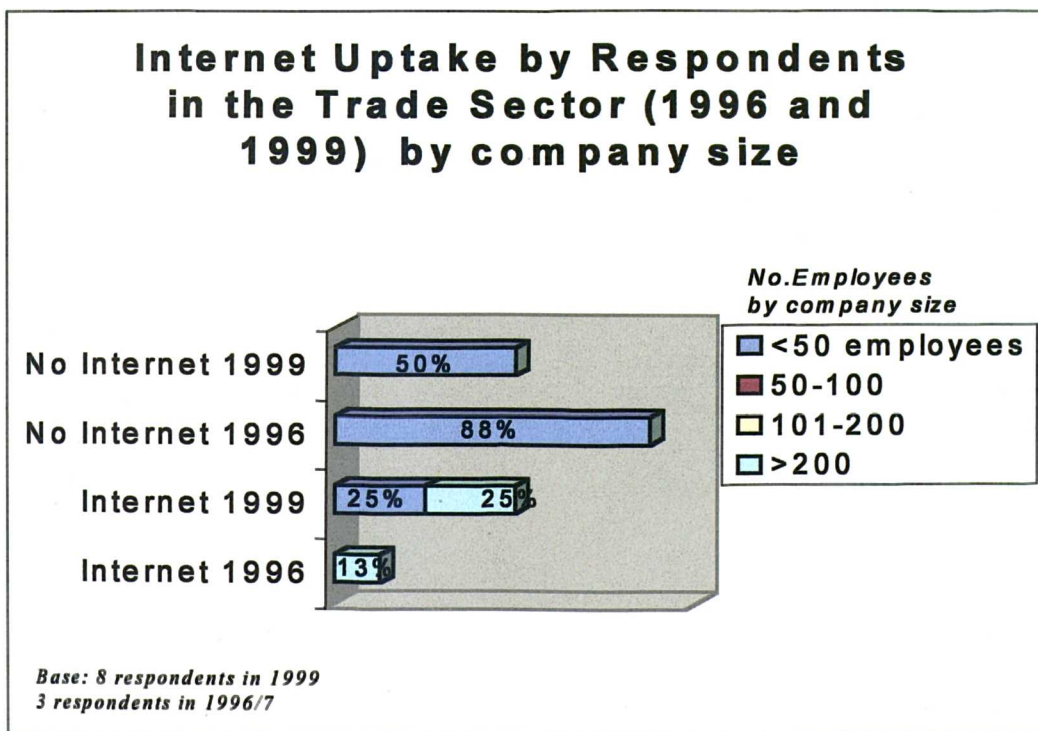


Figure 42 . Internet Uptake in the Trade Sector

7.2.3 Summary and Conclusions

The aims of this telephone survey were to identify:

- SMEs perceived security needs and attitudes to security
- Internet usage patterns and SME network infrastructures
- The viability of the security solution designed for use by businesses

The survey found that over the past two years:

- There was a growth of over 100% in connectivity to the Internet by SMEs
- Overall, there was a higher rate of connectivity to the Internet in the service sector than in the manufacturing sector
- The rate of growth of connectivity to the Internet was higher in the manufacturing sector than the service sector
- The usage of the Internet by respondents in the service sector was more sophisticated. Manufacturing sector users were less sophisticated needing more time to become convinced about the benefits of the Internet to their respective businesses.
- None of the respondents had disconnected or ceased to use the Internet facilities.

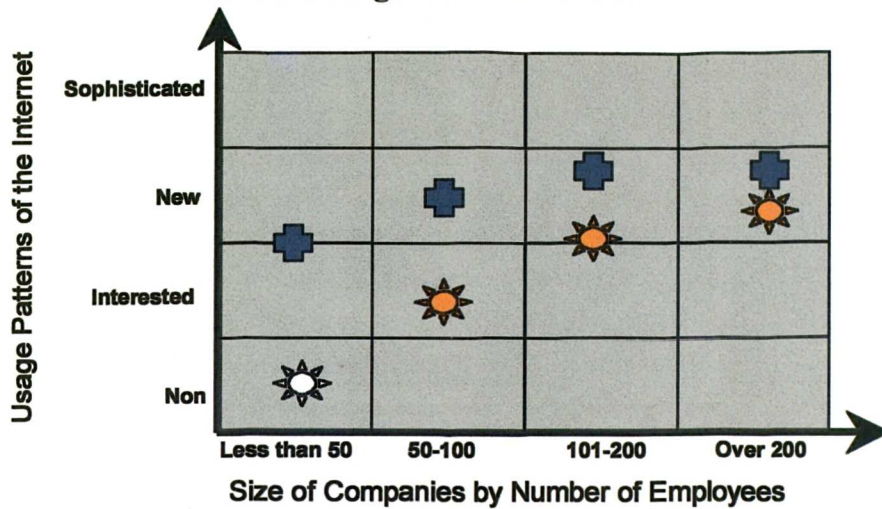
Over the past 2 years there has been a growth in connectivity and use of the Internet by regional SMEs of over 100%. This pattern has been repeated across the manufacturing, service and trade sectors respectively. The most dramatic rate of growth has been in the very small companies with fewer than 50 employees, but the largest proportion of companies not connected to the Internet also come from this group. From the survey, the usage and development pattern in both the manufacturing and service sector is similar, we can identify four general types of users.

(a) The Non User - These were not connected to the Internet in 1996 and are still not connected to the Internet in 1999. They believe the Internet is a waste of time, is of no use to their organisation and that they are too busy making business to deal with issues such as the Internet.

- (b) **The Interested User** - In 1996, these companies were not connected and felt either they did not have the information, resources or time for the Internet. However, by 1999, they are in the process of getting connected or will become connected within the next 6 months.
- (c) **The New User** - Although not connected in 1996, they had become connected by 1999 (within the past 12 months). They were still "experimenting" with the new facilities and although the majority had a web site it was mainly to have a presence on the Internet, rather than an integrated part of their marketing and business strategy. These were still unaware of the more complex issues such as security and were still training personnel in the use of e-mail and the Internet. However, those in the manufacturing sector tended to have a more developed web site. The manufacturing companies in this grouping tended to be the more "modern" manufacturers such as electronics and machinery parts. The service companies in this grouping tended to be the more "traditional" service providers such as travel agents and estate agents.
- (d) **The Sophisticated User** - These companies had been connected in 1996, where the Internet was being used mainly for e-mail and browsing for information. Security was not an issue for the majority and very few had a website. By 1999, their use of the Internet had become more sophisticated. They had developed electronic commerce, a security infrastructure and e-mail communication with suppliers and customers. In the majority of cases, the sophisticated user had a well designed web site with an integrated electronic commerce package where goods/services could be ordered on-line. The types of companies were in the "modern" manufacturing and service sectors such as electronics, software, IT and other consultancy services.

Figures 43a and 43b illustrate the different profile and type of business Internet user by sector and size of organisations over the two periods of the surveys. The figures are not intended to be mathematically accurate, but show the general profile of the majority of company in each company size grouping.

Internet Usage Patterns by Companies in the Service and Manufacturing Sectors 1996/1997



Key:



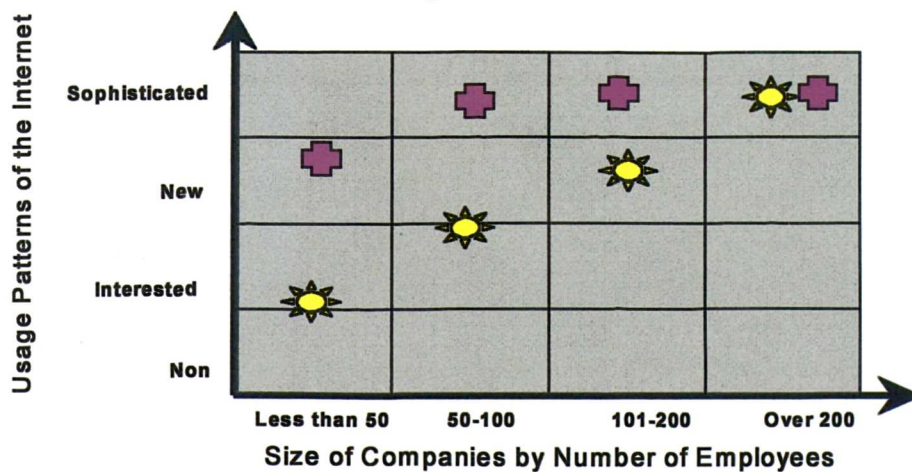
-  Companies in the Service Sector
-  Companies in the Manufacturing Sector

Figure 43a . Usage Patterns of the Internet in Manufacturing & Service Companies (1996/1997)

Internet Usage Patterns by Companies in the Service and Manufacturing Sectors 1999



Key:


-  Companies in the Service Sector
-  Companies in the Manufacturing Sector

Figure 43b . . Usage Patterns of the Internet in Manufacturing & Service Companies (1999)

In the service sector, we can see that the majority of users are sophisticated, with a large proportion also being new users. Only a small proportion were non-users, these were mainly very small companies in the security service, freight handling sector. In this case, the larger company, which was a non-user, was based in the financial sector and had fears about the lack of security which prevented their connection and use of the Internet. The new and sophisticated users tend to be mainly training, consultancy and IT service providers.

Despite the highest rate of growth in connectivity to the Internet being in the manufacturing sector, particularly in very small companies of less than 50 employees, three times as many companies in the manufacturing sector are not connected to the Internet than the service sector. The profile of manufacturing companies that are not connected are mainly in the traditional areas such as machinery, textiles, toy and leather manufacturing, whose opinions about the Internet remain unchanged. However, a higher percentage of the companies who were not connected than previously, did mention that they were interested in finding out more about the Internet. So still manufacturing companies are lagging behind the service sector.

Chapter Eight

Further Research (II) - Additional Findings

8. Further Research (II) - Additional Findings

This chapter provides a profile of the types of network infrastructure found in SMEs. By identifying the types of network infrastructure, this gives an indication of the degree of IT and Internet development, usage and popular network configurations in SMEs. This also allows the recognition of different types of security features implemented and thus the security needs, as they are perceived by SMEs. The analysis here is based on the data gathered from the case studies, depth interviews and telephone surveys in chapters 6 and 7. It is not intended as a quantitative study of network infrastructures found in SMEs.

8.1 Network Infrastructures in SMEs

The data gathered from the primary research found a number of different approaches to configuring networks in relation to the Internet. Five common types of infrastructures were identified and are described in more detail in the remainder of this section. The following network typographies and definitions are unique to this study and are not intended to reflect any other work carried out elsewhere.

(a) **"INTRANET INFRASTRUCTURE"** - this kind of infrastructure was seen in larger organisations (more than 100 employees) with nation-wide branches, where the branches were connected to head office by an intranet and only internal e-mail and file share/transfer facilities are available. The level of usage was relatively sophisticated in that e-mail, file transfer and database sharing facilities were used extensively, but concerns about security prevented the availability of company-wide Internet access. Although the companies tended to have web sites hosted by independent third parties, the web site was used mainly as a means of staking a corporate presence on the Internet.

- (b) **"SECURED SINGLE POINT INTERNET ACCESS"** - the types of organisation with this infrastructure tended to be larger than 100 employees, with several nation-wide branches, providing access to the Internet at only one point - head office. This access was controlled by a firewall infrastructure, providing a layer of security that the organisation felt was adequate. These types of organisations also host their own web site and are sophisticated users of Internet based facilities - namely e-mail, the Internet for sourcing information and also electronic commerce.
- (c) **"SECURED MULTI-POINT INTERNET ACCESS"** - companies with this infrastructure, tended to be larger companies with more than 100 employees in the modern sectors of manufacturing and services - such as software development and IT/consultancy. In this case the users were also sophisticated, using e-mail and Internet facilities extensively. They hosted their own web site and had developed some form of electronic commerce strategy. They had a firewall infrastructure with Internet access to the majority of personnel in the organisation. There was also an intranet for the transfer and sharing of confidential or company sensitive files.
- (d) **"DIRECT CONNECTION TO THE INTERNET"** - this kind of infrastructure was found in small companies with less than 100 employees. The users tended to be relatively new users of the Internet, with no network security facilities or infrastructure. The users had access to the Internet and used e-mail extensively. They tended to have web sites, developed and hosted by third parties, took orders over the Internet and had their own e-mail addresses. If they did use security facilities, they tended to use the features available in application software such as passwords and encryption features provided in e-mail packages.

"SINGLE CONNECTION" - the category of company with this type of infrastructure tended to have less than 50 employees. In this case, the connection to the Internet was via a single computer. They had a web site hosted by a third party with e-mail being spooled and forwarded to a single e-mail address accessible at a single terminal in the company. There was no network security infrastructure, but where security was used, it was security available through software applications, mainly password protection of documents. Companies were relatively new users still experimenting and learning about the Internet, how to use it, and what it can do for the organisation.

8.2 Conclusions

The different profiles of SME network infrastructures, tend to reflect the sophistication of IT usage and size of the respective organisation. That is, the smaller the company the more likely Internet use is limited to browsing for information and e-mail. The infrastructure tends to be networked computers with a single stand alone computer and modem connected to the Internet. It has also been shown that being a small company is not a limiting factor to gaining a presence on the Internet. Even very small companies develop an Internet presence and conduct electronic commerce through a third party host. It is also more likely that these companies do not have a security infrastructure and do not see the need for one.

The larger the company, the more sophisticated the network infrastructure and usage of IT and the more likely a security infrastructure would be integrated. The kind of security perceived by these organisations and reflected in the infrastructure, focuses on the fear from outside attack. Thus these organisations have implemented network features controlling access, protecting the network from unauthorised access, controlling and filtering traffic travelling through the network. None of the organisations contacted, defined security in terms of integrity, confidentiality, authentication and non-repudiation of static or transmitted electronic data and none had implemented an electronic data security and authentication infrastructure as that designed in this project.

Chapter Nine

Discussion of Findings (I)

9. Discussion of Findings (I)

This chapter develops an analytical framework based on the primary research carried out during the course of the project. Using critical success factor methodology, a set of key areas of activity are identified as being necessary for the successful implementation and use of a security solution in SMEs. Although based specifically on security, this framework could also be applicable to more general IT and Internet related technologies. Where this chapter mentions IT projects and new technology, it uses the terms interchangeably and refers specifically to security solutions and more generally to IT and Internet related technologies.

9.1 Framework for Analysis

The collated results of the primary research have identified two main factors, which impact on the implementation of a security authentication infrastructure in particular and an IT infrastructure in general. The following matrix has been created to explain these factors and their influential interaction on the outcome of the implementation process.

Framework for Analysis of Implementing IT Projects

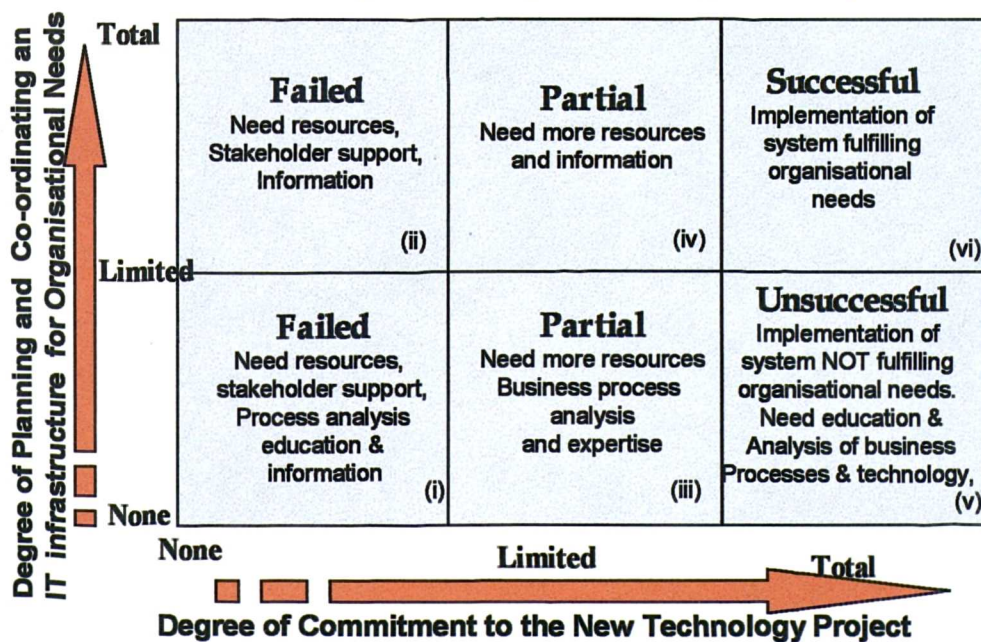


Figure 44 . Factors for Implementing New Technology

The two main critical factors for success identified, are the degree of commitment to IT strategy by the organisation and the degree of planning and co-ordinating the technology infrastructure to organisational needs. These are discussed in more detail in the following sections.

9.1.1 Commitment to IT Project

One of the factors in the matrix is commitment. Commitment is necessary from all the relevant stakeholders involved. The depth interviews (Chapter 7.1) identified the process of developing corporate commitment. This includes pressure from external and/or internal stakeholders or persuasion and incentives to external stakeholders from the organisation.

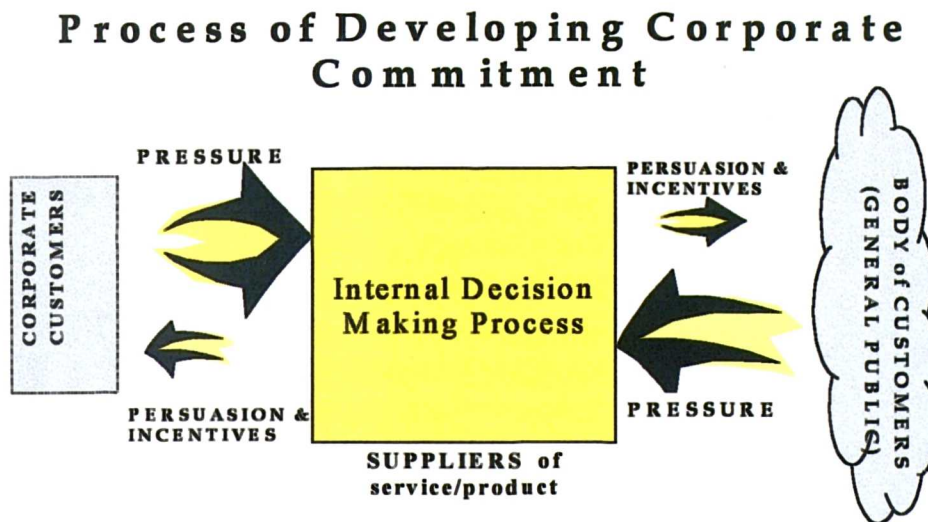


Figure 45 . The Process of Developing Corporate Commitment

In business-to-business relationships, the "corporate customer" group of stakeholders, has the economic power to insist that suppliers use a certain type of administration system. Historically, this is how EDI was introduced¹²⁶ and used, by the application of pressure from corporate customers on their suppliers. This is particularly true of corporate customers such as the large supermarket or retail chains, Marks & Spencer and Asda. The other group of external stakeholders is the body of customers made up of the general public. This is where the volume of numbers would influence the suppliers to provide a certain kind of product or service.

While the suppliers can, to a certain extent, influence their customers to adopt a new service or protocol, this influence is largely based on a series of incentives and information dissemination or education programmes, which would convince customers of the benefits of the proposed service. Without commitment from external stakeholders, the organisation will not have a third party with whom to use the new technology and so it will be used either exclusively for internal purposes - minimising the cost benefits, or the new technology will be abandoned.

The internal stakeholders include all levels of the organisation from directors, to managers to employees. Commitment can be measured in terms of:

- **Allocation of financial, human and training resources** - this shows the degree of support from the management level of the organisation which ultimately will drive the decision to implement and integrate new technology within an organisation.
- **Support and endorsement by stakeholders** - the degree of co-operation can be gauged by questionnaires and consultation groups (as suggested by Drs Rosen and Weil)¹²⁵ indicating a willingness to take part in training and information dissemination programmes. Attitudes towards the implementation and use of new technology also reveal the degree of stakeholder support. The lack of committed and proper use of the new technology will minimise the benefits and could be destructive to the whole process.

Three measures of commitment are included in the matrix. These are defined as:

- **Total commitment** - allocating financial and human resources to the planning, development and implementation of IT projects and infrastructures. Total commitment also includes support and endorsement of IT strategy and plans at all levels of the organisation - from the user to the director/owner. External stakeholder commitment is also necessary to the use and implementation of new technology.

- **Limited commitment** - includes agreement, commitment and endorsement of the plans by all levels of personnel in the organisation, but there are insufficient resources to be allocated to the implementation of the plans.
- **No commitment** - is where either or both internal and external stakeholders have not bought into the plan and will neither support nor endorse it either verbally or with resources.

The findings from these case studies showed, that internal stakeholder commitment (from user to director level), is equally as important as external stakeholder commitment to successful implementation. Internal stakeholder commitment is achieved through a training and education programme discussed in more detail in the next section.

9.1.2 Planning & Co-ordinating IT Infrastructure in Organisations

The second factor in the matrix is designing and implementing an IT infrastructure to fulfil and support the processes, needs and requirements of the organisation. This factor is equally as important as commitment. It includes understanding current business processes and how these can be improved and developed in line with the organisation's plans for strategic growth, by designing and implementing an IT infrastructure to support these business needs.

In order to take advantage of the new technology, organisations must recognise the need for re-engineering business processes to incorporate IT and the need to manage this change process.

As Brynjolfsson¹²⁷ et al identify, the difficulties many organisations have had *"depends in large part on inadequate recognition of interdependencies among technology, practice and strategy"*. Milgrom and Roberts¹²⁸ have shown mathematically how interaction can make it impossible to successfully implement a new and complex system in a de-centralised and uncoordinated manner. Thus, managers must plan a strategy that takes into account and co-ordinates the interactions among all the components of a business system.

From the case studies, three main components are identified. These are:

- A full analysis and understanding of existing processes and planning for IT integrated process re-engineering,
- Users including user profiling and assessment and development of appropriate education and training programmes
- Audit of current and assessment of future technological infrastructures

a) Analysis and Re-engineering of Current Business Processes

Existing business processes in the organisation should be assessed and evaluated in terms of efficiencies, adding value and allocating resources. Then in consultation and with the co-operation of all the departmental stakeholders, there should be a discussion on how best to improve the process in order to achieve the organisation's business aims and objectives to a level of workable satisfaction.

Once the consultation stage is complete, a new process incorporating the technology should be designed and a pilot stage set up for testing within a department. Once the pilot stage is completed, improvements based on a process of feedback and evaluation should be made and the pilot implemented throughout the organisation.

b) The Users

An assessment of the technology end-users should be made in order to develop a broad profile of user types within the organisation. This profile should include basic demographic details as well attitudes and thoughts about computer technology.

Then, a training and education programme should be designed to maximise understanding of the new processes. This will improve levels of co-operation and thus effective usage of the new processes, which will maximise the benefits for the organisation.

Issues of usability of the new technology must also be included here. An evaluation and assessment of the new technology by the potential users should first be made to identify any major user problems and also contribute to the design and development of the training programme. User evaluation of the new technology could contribute to the abandonment, modification or replacement of the proposed new technology depending on the feedback by the users .

The training and education programme should incorporate information on two levels:

- **The broader level** - explaining the new process, its benefits to the organisation and the user, drawing on the positive implications of the change, while explaining how the negative implications are to be overcome.
- **A more detailed level** - including training in the actual usage of the software providing documentary support and an explanation of the concept of and the necessity for certain procedures to be followed. For example in this case, the necessity for password creation protocols and suggestions of how to remember secure passwords.

As well as training and education programmes, there is a need for an instant and high quality technical support and maintenance service for users to cope with any potential technical problems they might have.

c) The Technology

This area is the most complex, as it addresses the whole technological infrastructure of the organisation – in terms of the hardware, software and support services. An overall assessment of the organisation's infrastructure must be examined carefully and the following issues addressed:

- The quality of technical support, the working guidelines and a minimum level of service which is acceptable for networks hardware and software
- The number of time and delivery critical processes throughout the organisation, which are reliant on the existing organisational infrastructure
- Back-up procedures to support critical processes in case of network failures which cannot be dealt with instantaneously
- A ubiquitous hardware and software policy throughout the organisation to ensure,
 - inter-organisational compatibility
 - commercially preferential rates with manufacturers and/or suppliers
 - replacement and upgrade issues
 - preferential service agreements with third parties

In this case and from the findings of the case studies, the software that is being used (Entrust Technologies software) must also be examined carefully and again a minimum level of service agreement must be made with the suppliers. Similarly back-up procedures must be in place to ensure that any alteration made by the system administrators are not visible to the users. Also password retrieval/changing processes must be readily available, as this will always be the predominant issue for users.

9.2 Applying the Matrix to the Case Studies

Each quadrant in the matrix summarises the impact of the interaction of the major factors and outcomes on the success or failure of the design and implementation of an IT system.

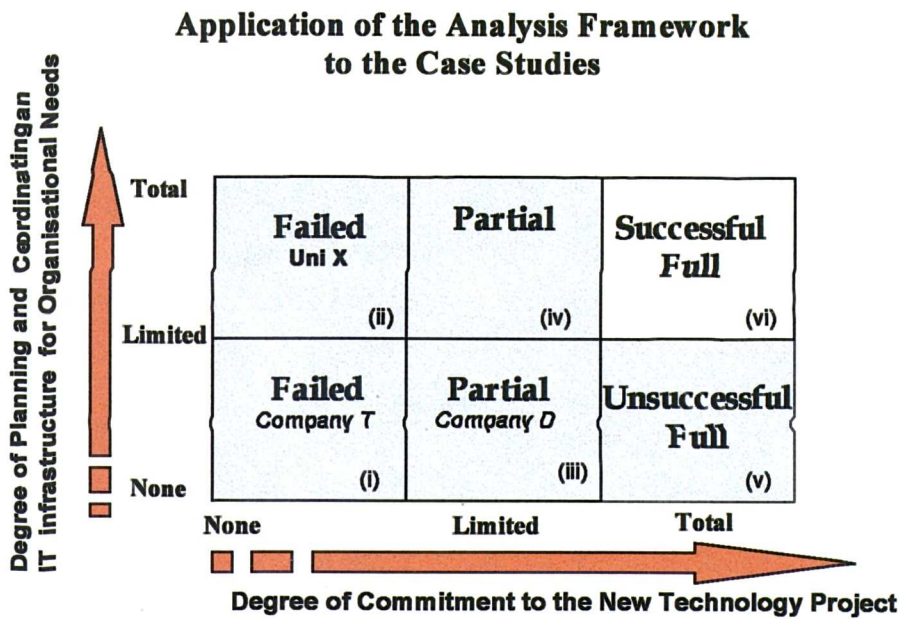


Figure 46. Factors for Implementing New Technology

Quadrant (i) - When there is no commitment to the implementation of new technology and no strategic planning and co-ordination of the technical and business processes to the organisation's need, there will be a failure in the implementation. What is needed firstly is commitment from the stakeholders. This is achieved through a process of education and information about the technology, the facilities available, its applicability and the benefits to the organisation needed to promote the successful planning and implementation of IT strategies. There is also a need for resource allocation from the organisation for the project.

Company T falls into this category. The fact that Company T took part in the pilot project, shows that the internal stakeholders were committed in terms of knowledge, education, information and enthusiasm for the new technology. The external stakeholders were not committed. Ultimately the security and authentication service failed to be implemented after the pilot because,

- The company could not use the new technology with external stakeholders and it was unfeasible to offer incentives to partners or customers, since being a small organisation resources were limited.
- There was no cost benefit to the organisation implementing such a service for internal purposes only, since internal stakeholders were located in the same office.

In order for this company to implement the security and authentication service, an information dissemination and education programme would have to be launched for all external stakeholders and incentive schemes would have to be introduced to encourage the implementation process. So although there was an internal commitment, there was no external commitment, which has equal importance in the eventual implementation outcome. Neither was there any analysis of business processes or planning and co-ordination to integrate the solution into the organisation's business processes.

Quadrant (ii) - With an understanding of the technological infrastructure, facilities and benefits to the organisation, but no concrete stakeholder commitment or resource allocation, then IT strategies will not be implemented. However, this situation is more positive since there is an understanding of organisational needs and the supportive IT infrastructure. Since there is an understanding of organisational needs, then this implies a degree of commitment from internal and external stakeholders. This situation will change with the availability of resources.

University X falls into this category. There was an understanding of the need for re-aligning current processes. Although the organisation took part in the research project's pilot, it did not implement the solution. The findings from this case study should be used with caution, since this is a large organisation and not an SME. Because the organisation is large with a large number of departments, the process dynamics of each of the departments varies which means that process re-engineering issues and technology specification issues plus the organisational politics and bureaucracy would have an impact on the way that implementation decisions are made. To make sure that the findings remain valid for SMEs, the process re-engineering and compatibility issues are underestimated in this case. However, the stakeholder issues can be analysed using this framework as the departments can be seen as individual SME groups of users. It was the lack of commitment from the internal and external stakeholders, despite incentives offered, that was one of the main reasons in the failure of the implementation of the security solution. In this case, an education programme was required to explain and clarify not only the concept of security and authentication, but also the re-engineered process for which security and authentication was being used.

Quadrant (iii) - With limited commitment and no understanding, there will be a partial implementation of new technology. However, planning for systems will be made and budgets allocated, but the lack of understanding will lead to the implementation of a system, which does not fulfil the aims and objectives of the organisation. Thus the organisation will not maximise their investment and the implementation process will be a partial failure.

Company D falls into quadrant (iii). Although the company did not take part in the project's security and authentication pilot, this was not due to a lack of commitment. Internal stakeholders at all levels of the company had a strong enthusiasm for and commitment to new technology. External stakeholders had also been identified as being willing and able to participate in secure and authenticated transmission of electronic data. In this case, although resources were limited budgets had been allocated for new IT projects. This company had a current system which provided security and authentication facilities. However, the reason there was a partial failure was because of the lack of knowledge and expertise amongst technical staff who were unable to assess the existing system, its facilities and their applicability to the needs of the organisation. So, more expert training was needed for technical staff in order to maximise current and future new technology.

Quadrant (iv) - With a full understanding of the organisation's IT environment, planned system and business processes, but only limited resources, there will be a partial implementation of the system. Although only partial, there is a commitment to the project and because of the wider understanding of the benefits to the organisation, an informed decision can be made about the phases for implementation and budgeting resources for future development. Although partial implementation will take place, this will be more a staged implementation governed by resource limitations and will most likely develop into a successful implementation.

Quadrant (v) - With total commitment to the implementation of an IT strategy but little or no understanding of the system and the organisation's needs, although a system will be fully installed, the system designed will not be adequate to the organisation's needs. For the future this will be costly since the system will not be an organic infrastructure on which future needs and requirements of the organisation can be built. In this case, more information and education is also required. In the majority of cases where implementation of systems fail, there has been no understanding of the needs of the organisation and the IT system being designed and installed. One of the biggest examples is the Taurus project¹²⁹, where the London Stock Exchange had commissioned an IT system for hundreds of millions of pounds in the early 1990's which had to be abandoned in the development stage, because it

was totally taken over by the technology and was not meeting the organisation's objectives.

Quadrant (vi) - With total commitment in terms of resources and a full understanding of the organisation's business and IT environment, this will lead to the successful implementation of a system with a full array of features commensurate to the requirements of the organisation and on which they can develop and build for the future.

9.3 Conclusions

The collation and analysis of the primary research carried out during the course of this project has led to the development of a framework identifying the critical factors of success for the introduction of new technology in SMEs. This framework consists of two main factors, the degree of stakeholder commitment to the new technology project and the degree of planning and co-ordination to match the new technology infrastructure to the organisation's needs.

Before any process is introduced, the commitment and co-operation of all stakeholders is needed. A measurement of this is the resources allocated to the organisation for implementing the new technology and the degree of stakeholder willingness to use and support for the new technology. A full understanding of the organisation's business needs and current processes is also needed to develop a strategy to co-ordinate and plan for the design and development of an IT infrastructure which meets the organisations' needs. Once an assessment is made, then the process for the design and development of the technology and implementation must begin to ensure that the new improved business processes are not driven by the technology. In order to increase the probability of successful implementation and process re-engineering, it is necessary to address the issues of:

- Educating and training stakeholders in a way that will encourage their commitment to the process. Without a basic level of commitment, no project can be successful.

- **Technical Support** – ensuring that time-critical processes are not jeopardised by failing technology or network infrastructure and that there is support for users and equipment.
- **Compatibility of technologies** – software and hardware issues.
- **Usage of the software** – particularly addressing the issue of forgetting passwords and integrating new technology in a way that encourages users to use it.

Although none of the case studies actually implemented the new technology after the pilot stage, using this analytical framework, one of the main reasons was a lack of commitment and motivation by external or internal stakeholders to use the new system. Another reason was a lack of technical knowledge and training for IT staff to assess facilities available in existing technological systems and matching these to the organisation's needs. The benefits of the analysis framework, are that organisations can identify the reasons for lack of successful implementation and develop strategies to counteract any potential areas of weakness as defined in this chapter.

Chapter Ten

Discussion of Findings (II)

10. Discussion of Findings (II)

This chapter develops a theoretical framework describing the correlation between the organisational lifecycle stages of growth and development and the network infrastructure being implemented by them. This framework is based on the collation and analysis of the primary research findings carried out during the course of this study. The information gathered was not based on technical documentation and plans, but a verbal description of the networks in the respective organisations. Thus, the networks identified are based on concepts and recognising common main features rather than detailed technical equipment, specifications and configurations.

10.1 Organisational Lifecycles and Network Infrastructures

Organisational growth and change is illustrated by the concept of a lifecycle, where organisations go through the stages of birth, growth, maturity and eventually decline and death¹³⁰. As an organisation moves through the lifecycle, each stage is associated with specific characteristics of structure, control systems, goals and innovation. Also relevant in this case is the development and integration of IT infrastructures and networks as company circumstances and requirements for information sharing and needs change. These changes are summarised in Figure 47, adapted from Richard Daft's¹³¹ definitions of the stages of development and growth in an organisation's lifecycle which is detailed in the remainder of this chapter.

When organisational development is plotted against organisational size, there is a positive correlation suggesting that as an organisation develops, so it increases in size.

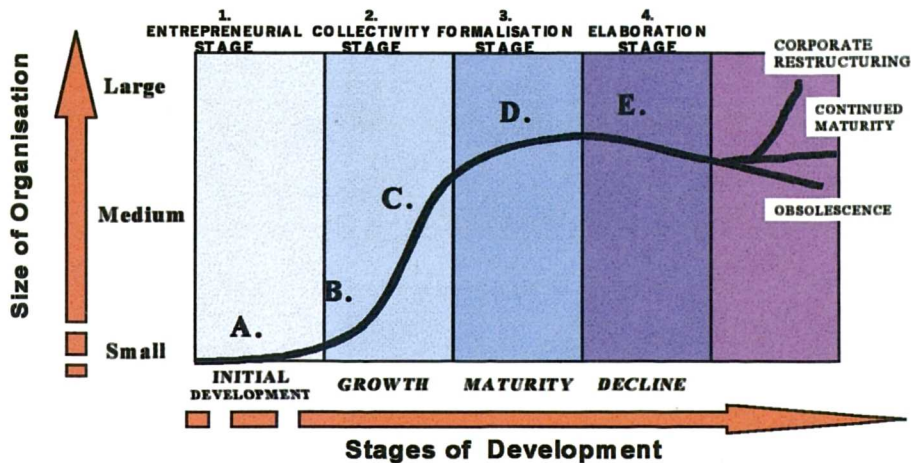


Figure 47. Network Infrastructure and Organisational Lifecycle

The stages of an organisation's growth and development have been categorised into a lifecycle framework, ranging from the entrepreneurial to the elaboration stage. Within this lifecycle framework, the IT/network infrastructure have also been categorised into models ranging from Figures 48a-e.

The following section will categorise organisations according to their position in the lifecycle. The organisational and IT infrastructures (models A-E) identified, will be generally described for each category. It must be noted however, that the infrastructures recognised in the stages of the organisations' lifecycle, are not mutually exclusive. Thus, where some observations and generalisations of network infrastructures have been made, these could and have been applied across the next stage of organisational development. This is particularly true of organisations in different industry sectors. For example, an IT based organisation at the entrepreneurial stage, will have an IT infrastructure of an organisation at the collectivity stage of the life-cycle although its organisational infrastructure is still entrepreneurial.

I. The Entrepreneurial Stage

The Organisational Infrastructure - At this formative stage of the organisation's life, the emphasis is on creating a product or service and surviving in the market place. The founders are entrepreneurs devoting their full energies to the production and marketing of their products or services. At this early stage, there is generally a sole or single range of product or service being offered. Initially, the organisation is small, informal and non-bureaucratic. The hours of work are long and the control and reward systems are informal and based on the owner's personal supervision and judgement. Growth in this stage is from a creative new product and service and as the company grows, there is a need for management, leadership and provision of clear direction.

The Technological Infrastructure - The IT requirements and development of an infrastructure are based on information share and information gathering with the underlining criteria of cost effectiveness and maximisation of investment in IT. Figure 48a illustrates the basic main features of network infrastructure which support the criteria of an emerging company at the Entrepreneurial stage.

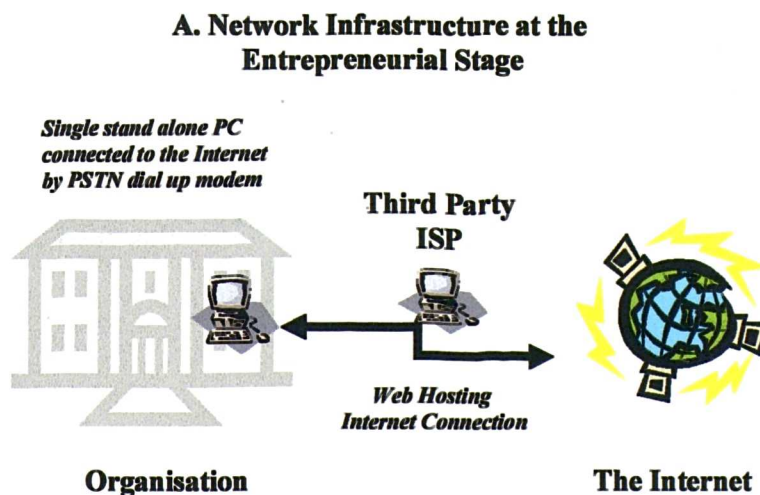


Figure 48 a. Network Infrastructure at the Entrepreneurial Stage

At this stage, internal and formal information share is minimal, since there are few employees and a single location where communication is largely on an informal and verbal basis. The basic IT set up is a PC with standard e-mail account using a modem via an ISP. Information security at this stage has relatively no priority since the business is concentrating its limited resources on profit earning. Although the information on the PC is open to external interference, it is still relatively secure for the following non-technical reasons:

- The organisation is a start up, it is still relatively unknown and less likely to come under attack from outsiders
- Connection to the Internet is on a dial-up basis where costs must be minimised, so access to the Internet will be limited and when the PC is not on-line, information is relatively secure from external tampering.

At this stage, security is concentrated on external security - CCTV, locks etc - to protect against the theft or damage of equipment. Information security is largely provided by the facilities in-built in operating systems and application software and is based on password access.

As the company grows, the facilities available would be a basic Internet presence, advertising the company and its products and a single e-mail account with the company's own domain name. With growth comes an increase in the number of employees and while the basic facilities remain the same, internal information sharing requirements increase. The information now becomes accessible from all PCs in the company by developing a local network. At this stage, information security is still not a high priority issue. Not only because awareness is relatively low and money making business priorities take precedence, but also since only one standalone machine provides a single gateway to the Internet, company information stored on the company's network is relatively secure from external attack. The basis of information security at this stage, is still largely provided by the application software being used on the PCs rather than bespoke security specific software.

B. Network Infrastructure at the Entrepreneurial/Collectivity Stage

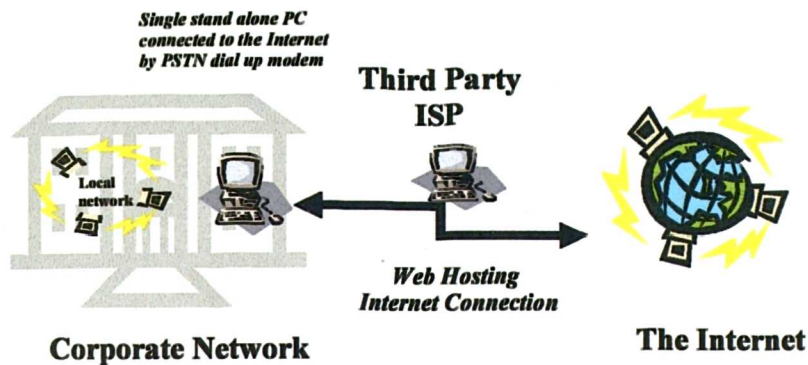


Figure 48 b. Network Infrastructure at the Entrepreneurial /Collectivity Stage

The model illustrated in Figure 48b is applicable to organisations in the late entrepreneurial or early collectivity stage of an organisation's lifecycle. This framework does not imply that organisations must grow. An organisation may stay at the entrepreneurial stage throughout its life.

II. The Collectivity Stage

The Organisational Infrastructure - This is the organisation's youth. The organisation begins to develop clear goals and objectives for growth of the company. The company has developed a foothold in the market and its focus is no longer purely survival but continued and rapid growth. The number of employees increases and with it, come the beginnings of division of labour and separate departments to deal with different areas of the organisation such as sales, distribution, finance, marketing. At this stage, employees still feel that they play a contributory part to the success of the organisation. The structure is mostly informal and pre-bureaucratic although some procedures are emerging. It is relatively small and communication and control are mainly informal although a few formal systems begin to appear. These include more formal systems of communication such as written memos, agendas to meetings, as well as rewards and contributions systems. As the company grows, so does the

position of managers, their responsibilities and their autonomy. Managers begin to delegate tasks which they had previously performed themselves and their roles are more involved with developing strategy and corporate direction. There is a greater need to introduce mechanisms to control and co-ordinate departments without supervision from the top. The major product or service being offered, develops variations. Innovation and new ideas come more from employees than the company founders.

The Technological Infrastructure - Gradually as the number of employees grow so the number of PCs increase and become networked as internal information needs to be shared across more people and departments and locations. Improved hardware and software is needed to accommodate the increased information flow between members of staff.

C. Network Infrastructure at the Collectivity Stage

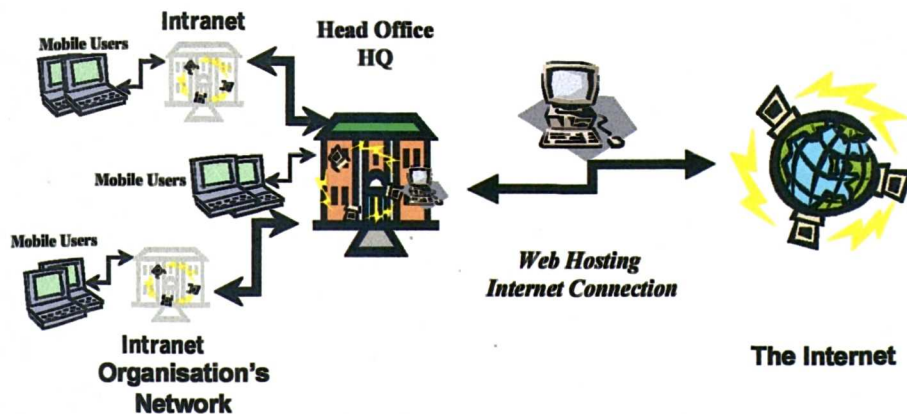


Figure 48 c. Network Infrastructure at the Collectivity Stage

Growth increases the number of offices, so the technological needs are duplicated across the sites. Information is shared across sites by e-mail. At this stage, security is maintained by having a stand alone PC and only head office is connected to the Internet or at other sites, connectivity is by a single stand alone machine. Dial-up

ISDN lines might be introduced to provide more secure access to the intranet improving speed and availability of the information.

III. Formalisation Stage

As the organisation moves from the collectivity stage to the formalisation stage, more sophisticated software and hardware is needed to organise and manage the growing volume of information at each location. Information will need to be accessible instantaneously across the different sites securely and quickly.

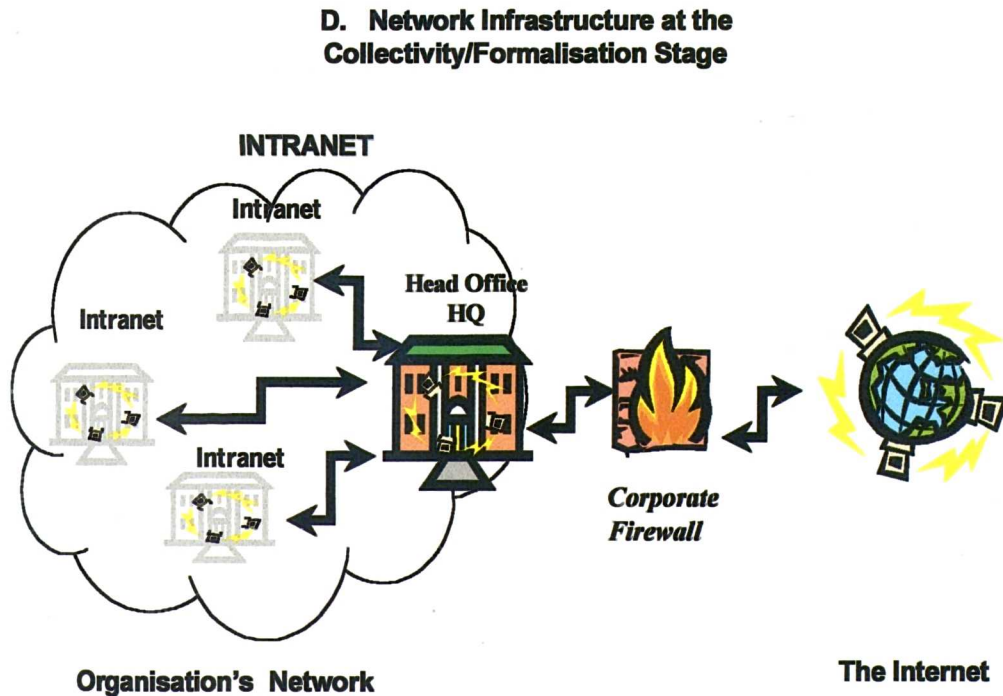


Figure 48 d. Network Infrastructure at the Collectivity/Formalisation Stage

More sophisticated web sites are designed and hosted by third parties to integrate electronic commerce into the sales and marketing strategy of the organisation. This allows:

- The sharing of information internally across the organisation
- Taking orders over the Internet
- The sharing of information with stake-holding parties such as customer and supplier accounts and order reviews.

The installation of a firewall provides secure access to the Internet for the organisation. All employees have access to the Internet from their desktops and individual e-mail accounts.

The Organisational Infrastructure - At the formalisation stage, the organisation is entering mid-life. It is becoming bureaucratised and seems to be getting too large and complex to be managed through formal programs. Communication is more formal, management is even more involved in developing strategies and planning for future growth and development of the organisation. The systems put in place are developed and added to, with more rules, policies, procedures and control systems. A clear hierarchy emerges where managers delegate and control, more departments are set up to deal with separate tasks. Innovation, which was once the responsibility of the original founders and employees, may become restricted to separate innovation groups. The products or services have developed to include a range of related products and/or services. The goal of the organisation is now internal stability and expansion into other markets and other countries.

The Technological Infrastructure - The volume of data and sophistication of systems now need to be managed by dedicated IT support teams. Information is increasingly centralised and shared across locations, where the network links are leased lines that are private and on-line at all times. This maximises access and security while minimising costs. Servers at each location provide local authentication and data access and all the information is consolidated centrally in one location and external e-mail is managed and distributed to other locations. Internet access is centrally located and controlled by the head office. Firewalls are installed at each

location to ensure maximum security. Formal IT policies, such as the use of e-mail, the Internet and security are developed centrally and distributed for implementation by all employees. Usage of systems is monitored to ensure non-abuse of the facilities provided - such as the downloading of pornography or sending abusive e-mails.

It is at this stage that an organisation's high profile and increasingly accessible system, to internal and external stakeholders, makes it more vulnerable to external attacks. The organisation becomes more interested in developing and implementing systems, that will increase its security, for example the implementation of a Public Key Infrastructure (PKI) which can provide military strength security for both static and transmitted data.

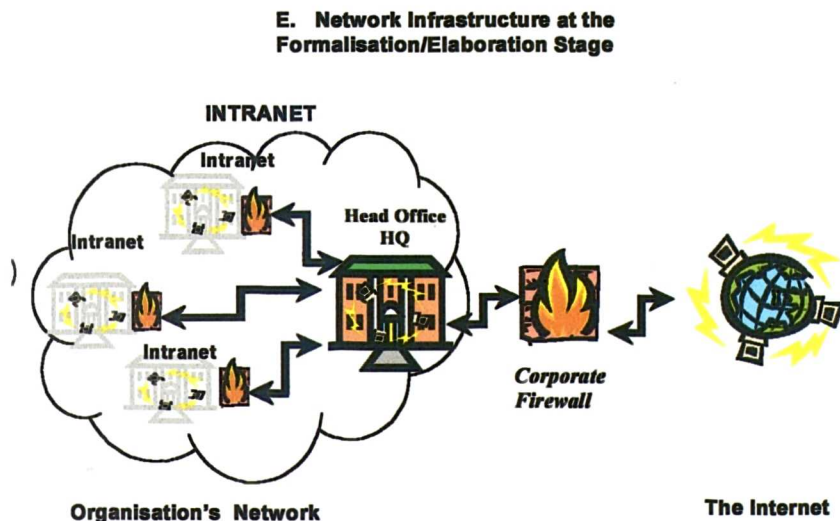


Figure 48 e. Network Infrastructure at the Formalisation/Elaboration Stage

IV. Elaboration Stage

The organisation has now reached maturity and enters periods of stagnation and temporary decline if action is not taken to renew or re-align it. It is large and bureaucracy is at its limit where employees work within the organisation without adding to the bureaucracy. Roles, procedures, reward and control systems are extensive and tailored to individuals. Organisational stature and reputation are important and innovation is institutionalised through Research & Development

departments. There is a range of multiple products or services, some of which are not cost-effective to produce or provide.

Streamlining the organisation, through employee redundancies, shrinkage and restructuring, will allow it to overcome the over-bureaucratisation resulting in slow responses to changing environments, stagnation and decline. Developing a team approach with more small company thinking is seen as a strategy to counteract these adverse consequences. Periodic revitalisation is important for mature organisations to prevent gradual decline into obsolescence.

10.2 Application of the Framework

This framework was developed as a general basis to facilitate the understanding of growth and development of network infrastructures in organisations of different sizes based on Daft's definition of organisational structures. The framework must be applied generally, since there will undoubtedly be slight differences in network elements from those identified in any specific model.

If we apply the framework to the three main case studies of this research project, we see that:

- **Company T** - fits in with the network infrastructure at the late entrepreneurial stage of development (Model B). The organisational infrastructure of company T is relatively informal with very few formal procedures and systems for communication. Employees mainly communicate with each other face-to-face because of the small number of employees and sole location of the premises. The network infrastructure in Company T is a local network, where a series of computers at the same location are linked together by network cables enabling information flow and sharing between the small number of staff. Connection to the Internet is via a modem accessible only through a single stand-alone PC through an Internet Service Provider (ISP). Because of the limited use of the Internet throughout the organisation, security is not an issue and thus it is not incorporated into the infrastructure.

- **Company D** - fits in with the network infrastructure at the later collectivity stage of development (Model C). Company D has experienced rapid growth in terms of number of employees and turnover. The structure of the organisation is still relatively informal, but systems are beginning to be implemented and innovation comes mainly from employees rather than the directors or owners. Managers and directors although involved in projects, have had to delegate responsibility to other employees whereas before they were undertaking a large number of the tasks themselves. The network infrastructure in Company D has been developed to support the changing structure and needs of the organisation. The network varies slightly from the modelled infrastructure (Model C), in that the organisation is more aware of security and has included a firewall and installed ISDN lines at homes of home-working sales staff for a more secure connection to the corporate intranet. None of the employees have desktop access to the Internet and access is limited to pre-assigned stand-alone computer terminals.

- **University X** - this organisation has entered the formalisation stage. It is heavily bureaucratic, managed by a large number of complex and widespread formal programs, pre-set rules, regulations and procedures. There is a clear hierarchy within the organisation and a large number of departments dealing with separate tasks. The technological infrastructure mirrors that illustrated in Model D. The network is sophisticated with a series of intranets at different sites and locations. The volume of data and the networks are managed by a number of dedicated IT support teams. Information is largely centralised and shared across locations where the network links are on-line all the time. Servers at different locations provide local authentication and data access and Internet is available to all authorised users but is centrally controlled. The only difference in this case is that there is no firewall infrastructure, which is prominent by its absence in such a large and sophisticated organisation and network infrastructure.

10.3 Conclusions

The models and frameworks identified and defined in this chapter, do not suggest that all companies progress through the different stages of growth and development in their respective lifetimes. Nor do the models intend to pigeonhole network infrastructures according to an organisation's size. Networks are organic systems and it would be impossible and foolhardy to try and encompass all the possible permutations and combinations of network systems into a number of models. The models developed here, are intended to give a basic guide to the type of networks that have been implemented commercially in certain types of organisations. These models are neither mutually exclusive nor definitive, they do not take into consideration detailed usage of the Internet or other IT system by the respective type of organisation.

The models are a means of measuring and comparing network infrastructures in organisations, with some of those identified as a result of this project. These models can be used as a yardstick to show any potential strength or weakness compared to those identified. When used to analyse organisations and their infrastructures, the models have shown that, Company D, is very aware of security but does not have a complete range of Internet based facilities company-wide, which potentially might affect its growth and development. In the case of University X, it highlights the fact that security features are underdeveloped in proportion to the organisation's size, infrastructure and the range of services it delivers. Company T seems to have implemented an infrastructure which is in harmony with the organisation's size, infrastructure and current needs. Having said this however, it does emphasise the fact that the network is underdeveloped in terms of limited access to Internet based facilities and services by all employees.

It should be noted that these models would have to be tested on a larger number of companies to develop a degree of confidence in their applicability to a range of companies. The organic nature of networks coupled with the rapid changes and modifications in technology and its applicability, means that these models are valid for a certain point in time and must be constantly updated by further research to ensure their validity in the period of time for which they are being used.

Chapter Eleven

The Best Practice Guide for SMEs

11. The Best Practice Guide for SMEs

One of the aims and objectives of this research project was to produce a “Best Practice” guide for SMEs based on the observations made during the course of this study. This guide is intended to be used by SMEs as the starting point to:

- Defining their business and IT requirements
- Becoming aware of their existing networks and business processes
- And finally understanding the critical success factors for implementing a security solution or other Internet related solution within an organisation.

This guide lays down the foundations for SMEs in the planning and implementation of data security solutions in their organisations. It is based on the findings of the primary and secondary research carried out during this project and incorporates the theoretical frameworks developed and defined in chapters 9 and 10. The key points are to:

1. Define use of the Internet within the organisation. This includes identifying who the users will be; how and where they will access the Internet; and other Internet related facilities and services available.
2. Define security and security needs by the organisation. Different companies have different perceptions of their organisation's need for security. Howard's taxonomy of Complete Computer and Network (Figure 2 Chapter 2.3.3.2.1) could be used to identify the different kinds of security required for IT equipment and services. There is a need for companies to recognise the different types of security ranging from security of premises, to security of networks and security of electronic data being stored and transmitted over the Internet.
3. Outline the general infrastructure of the organisation's network, identifying key features. This coupled with the structure of the organisation can then be mapped against the network infrastructure framework developed in Chapter 10. By comparing the organisation's own network against the general network

infrastructure found in organisations of similar structures, any particular similarities or differences can be identified. Any differences in the general network features would be highlighted, leading to more detailed examination and evaluation and, determining whether the differences are particularly advantageous or detrimental to the organisation. This could be used both for a closer analysis of network security and also as a basic benchmark for network development for SMEs. The University S case study, showed that for an organisation with its defined size and structure a missing feature was a effective security infrastructure, highlighting the need to explore further the issue of network security in the organisation. It must be noted however, that the infrastructure framework is not a means for definitive analysis, but rather a tool for highlighting potential problems.

4. Using the analytical framework developed in chapter 9, the critical success factors for the implementation of a security solution specifically and new technology in general, are a commitment to the IT project by all stakeholders and a high degree of planning and co-ordination of the IT infrastructure to suit the organisation's needs. These factors are refined by the model into more detailed variables to include:

- Business Process Re-engineering
- Assessment and profiling of users
- Training and Education of Users
- Allocation of human, financial and training resources
- Support and co-operation from internal and external stakeholders

The matrix designed in chapter 9 can be applied at the planning stage of an IT related project to ensure that all the key issues are addressed. It can also be applied as a means of assessing and evaluating an organisation mid or post implementation to understand the reasons for success or failure and isolate the relevant areas.

This Best Practice guide is specifically tailored to the implementation of a security solution in SMEs. It can however, be generally applicable to IT related projects since the majority of components identified as being key to the implementation of a security solution, are also relevant to a range of Internet related new technology.

Finally, it must be underlined that technology is an area in which changes and modifications are constant and rapid. The findings on which this Best Practice guide is based, is a snapshot at a particular point in time (1998/9). The research must be constantly updated to ensure that the information on which the frameworks are developed is still valid for the period in which it is being applied. This is particularly true for the definition of network infrastructures in organisations.

Chapter Twelve

Conclusions

12. Conclusions

The importance of technological innovation as the catalyst to economic re-generation and growth is well known by business, government and academia. The Internet is one such technological innovation that has provided a cost-effective medium of communication and instantaneous global accessibility. The research undertaken in this project concentrated on the design and implementation of an authentication infrastructure to add security features for using the Internet by SMEs. The reason SMEs were targeted, is that they are potentially the group of companies that are likely to benefit most from the Internet, by evening out the advantages of large market size and global reach attained by larger multi-nationals at considerable high cost. The reason authentication and security were selected is because the Internet is fundamentally insecure. Effective introduction of an authentication infrastructure would:

- Detect any message that had been tampered with or altered illegitimately during storage or transmission
- Introduce unique digital signatures and authenticated acknowledgements of delivery and receipt to the authorised parties providing proof that the message originated from the sender
- Provide confidentiality that the message is readable only by those for whom it is intended

Without these features, it was thought that it would be very difficult for the Internet to achieve the status of a commercially trusted communications medium, to eventually replace paper-based communications.

12.1 The Research Study

The hypotheses that were tested during the course of the study were:

- *H₁ - The most appropriate authentication infrastructure for SMEs is Public Key Infrastructure (PKI) and Trusted Third Party supplied Certification Authorities (CA)*
- *H₂ - When the security service is adopted and used by SMEs this would be commercially beneficial to them and a provide a means of their company's maintaining a competitive edge*

The aims, objectives and related research questions asked and the final research findings answered by this research project are summarised in Tables 31a and 31b.

AIMS & OBJECTIVES	INITIAL RESEARCH QUESTIONS	FINAL RESEARCH FINDINGS
Contribute to the development of a secure and authenticated infrastructure for the exchange of information over the Internet for the benefit of SMEs.	1. Can a security and authentication infrastructure be developed to provide SMEs with trust, integrity, confidentiality and non-repudiation when using the Internet for transmitting electronic data?	A Certification Authority based on a public key infrastructure could provide security and authentication as defined in the question.
	2. Does the security solution developed actually work when used by SMEs?	When used, technically, the security solution functioned successfully. But other human and corporate issues were raised.
Identify whether the implementation of this security solution enables small and medium-sized enterprises to carry out their business operations/management more effectively and more profitably.	3. What benefits are achieved for SMEs by secure use of the Internet?	Successful implementation and use of the security system led to improvements in costs, process time and efficiency and necessity for human resources. Unsuccessful use of the system was more disruptive and costly. Other issues and questions were raised and were addressed by further research.
Study how the security solution is implemented by SMEs and how the new infrastructure is integrated into current business practices, processes and procedures.	4. What is the process of implementation of the security solution by SMEs?	The successful implementation process involves both a commitment to the project from internal and external stakeholders and detailed planning and co-ordination of the IT infrastructure in the organisation.

Table 31 a. Summary of the Research Project's Aims, Questions and Conclusions

Understand and clarify the reluctance of SMEs to join the research project.	5. What is the pattern and level of Internet usage by SMEs?	At the beginning of the project SME use of the Internet was relatively basic and connectivity to the Internet was 1 in 3 SMEs. By the end of the project, use of the Internet had become more sophisticated and connectivity had risen to 2 in 3 SMEs.
	6. What are the attitudes to and how are the Internet and security issues perceived by SMEs?	Initially attitudes to the Internet were vague and based on a "wait and see attitude" since the Internet was a totally new concept. Security was a non-issue for the majority of SMEs. By the end of the project, the Internet was seen as providing a large array of beneficial facilities and security issues were largely centred around preventing unauthorised access rather than authentication and protecting data integrity.
	7. Was the security solution designed a viable service for use by business?	Once explained to SMEs, all could see the benefits of such a service and all believed that it was a viable and very useful service. However there was a large knowledge gap on the topic of data security and authentication.
Based on the observations made, produce a "Best Practice" guide for SMEs.	8. What is the contribution to knowledge of this research project?	<p>Although the project was ahead of its time in terms of SME awareness, the main contribution to knowledge is:</p> <ul style="list-style-type: none"> ▪ SME perception of security is minimal and limited to widespread concepts centred around preventing unauthorised access to networks ▪ A framework has been designed and can be used to support SMEs in the successful implementation of IT projects ▪ A second framework has been designed as a rough guideline against which network infrastructures can be gauged to help highlight areas of weakness and strength ▪ A best practice guide has been developed based on this research project

Table 31 b. Summary of the Research Project's Aims, Questions and Conclusions

The research questions and answers are discussed in more detail.

The security authentication infrastructure was designed and developed by a process of primary qualitative and quantitative, and secondary research. The primary research (focus groups and telephone survey) revealed a large gap in SME knowledge, training and support when it came to IT in general and the Internet in particular. The main priorities for the majority of SMEs were information dissemination, practical training and understanding the cost benefits of the new technology. For over 90% of respondent SMEs, Internet security was not an issue. The selection of the technology core was by analysis of secondary sources (technology reports and journals) and structured evaluation of the commercially available authentication and security software.

The security authentication infrastructure designed was based on these primary research findings and included a technological core, which delivered the operational authentication and security facilities. The technological core - a public key encryption technology structure (PKI) - was found to be the most effective system for delivering authentication and security services according to the requirements of the project. Other layers in the authentication infrastructure included verification and operational procedures and processes; user training, information and support; and building up an external "corporate image" of integrity and trust for the service provider. The complete authentication infrastructure developed, was able to provide integrity, authentication, confidentiality, non-repudiation and an environment of trust for static storage and transmission of electronic data cost effectively by SMEs.

Thus the first hypothesis was proved and the first research question was answered affirmatively. This concluded the first part of the project.

The process of installation of this security and authentication infrastructure in SMEs was examined by case studies. Technologically, the security solution worked when the other factors (such as human users and network infrastructures) operated correctly. The successful use of the technology revealed that there were cost benefits to the organisation in tangible terms of:

- Time taken to carry out and complete certain business processes
- Cost savings by substituting communication channels (for example, authenticated e-mail as opposed to registered mail/couriers)

There were also intangible benefits to the organisation, such as improved speed of processes, increased efficiency, instant accessibility, wider geographic reach and a reputation for being technologically advanced. All these would impact indirectly on the benefits to the organisation in terms of improved reputation and service delivery.

The unsuccessful use of the technology revealed that more cost, labour and time were incurred and process efficiencies were totally destroyed by mis-using the security service. The unsuccessful use of the technology was identified as being as a result of the users and the existing network infrastructure rather than the security service itself. This then raised issues, which were addressed by the development of the implementation process analysis matrix.

Thus, tentatively it can be said that the second hypothesis is correct. However, with only one case study as evidence of this hypothesis, more research would have to be carried out to confirm with more certainty that the hypothesis was accurate.

The case studies identified the critical success factors for the implementation of a security solution in particular and an IT and Internet related solution in general. Broadly, these factors were:

- A commitment by both internal and external stakeholders in the organisation in terms of allocation of resources and co-operation and support. Both of these were needed to achieve commitment.
- The degree to which the IT infrastructure implementation process had been co-ordinated and planned to fit the needs of the organisation in terms of overall business strategy, re-engineered business processes, user information dissemination and training and existing technology.

The factors identified were synthesised into a matrix that could be applied to organisations before, during and after the implementation process.

In order to understand the lack of response by SMEs in taking up the initial invitation to implement an authentication infrastructure, further qualitative (depth interviews) and quantitative (time-series telephone survey) research was conducted. The research identified types of SME Internet users and network/IT infrastructure models in organisations at different stages in their lifecycle.

The profile of SME users of the Internet was categorised into *non users*, *interested potential users*, *new users* and *sophisticated users* according to their Internet connectivity status, degree of e-mail and Internet usage and the degree to which organisations had developed a business strategy incorporating electronic commerce. It was found that the majority of sophisticated users were in the service sector (mainly IT services) with a large number of new users also coming from the service sector (training, consultancy services). The largest proportion of new users and the largest proportion of non-users, were from the manufacturing sector. New users were mainly in the electronics and software industry, with non-users and machinery manufacturing concentrated in traditional textile, toy, machinery and leather manufacturing.

The complexity and sophistication of IT infrastructures on the whole were positively correlated to the size of the organisation. In terms of the infrastructures identified, these ranged from single point access to the Internet by a modem connection via a telephone line from a stand-alone machine, to an intranet/Internet infrastructure through ISDN connections with installed firewall network protection technology.

Overall, a clear picture emerged that although the authentication infrastructure designed during the course of this research project delivered all the technological and service features required of it, the failure in implementation was mainly as a result of the authentication infrastructure being introduced ahead of its time to a commercial environment with little or no knowledge of Internet technology and the infrastructure required to ensure its secure use. The target SMEs, were not yet ready on a user, technology or business process level to implement it within their organisations.

12.2 Limitations of the Study

There are a number of limitations, which must be taken into account while considering the findings of this research project. These limitations relate mainly to the research methodology and the new technology environment in which the project is set.

i) Research Methodology - there were many limiting criteria for this project namely:

- The exclusion of non-SMEs not in the European Union defined objective II area.
- The exclusion of organisations outside the Greater Manchester region.
- Limited funding which impacts on the accessibility of technology.
- The fact that only three case studies could be recruited to participate in the project had a limiting impact on the applicability of the finding from this section.

Having noted these limitations, it can be argued that the impact is not so adverse that it brings into question the validity of the findings since:

- SMEs constitute over 80% of businesses in the UK and thus selecting only SMEs validates this group as being relatively representative of the business population.
- Although the EU defined objective II areas are thought to represent 31% of the population, the fact that these regions are concentrated in mainly urban industrial areas again indicates that they represent a higher proportion of the business population.
- Greater Manchester is the second city in the UK with similar infrastructures and facilities in other cities across the UK. By selecting it at the exclusion of other regions, does not really invalidate the findings, since businesses are more homogenous in behaviour than individuals and are more likely to be replicated across regions.
- The limitation of funding is a criterion faced by many commercial and social organisations. It represents real life situations - no research is ever conducted without this funding limitation.
- Further research was introduced to support the limited response from the statistically minute data gathered from the case studies.

ii) **The Environment of New Technology** - one of the greatest limitations of the study, mainly relates to the fast changing nature of the IT environment, where trends and technological developments and social/business applications of it, can affect the relevance of findings. Thus, this research can only be said to be true for the point in time at which the research was undertaken.

The technological core of the security and authentication infrastructure is centred around software that is regularly being upgraded and updated. This affects the quality and range of facilities available for authentication and security. Not only this, but the authentication infrastructure fits into the current Internet infrastructure. In the future, the actual Internet technology infrastructure may change to incorporate security facilities at source. Furthermore, the Internet may be superseded by an alternative

technology, which would make the content of these findings obsolete. This is a fact of "modern day life" and is true of any research project. In this case, the emphasis is more on the implementation and integration process rather than the technology alone. Overall, this whole project of a necessity has had to be organic, where methodology is adapted to incorporate new queries and questions that arise because of the changing nature of the IT environment.

12.3 Implications of the Study

This research was conducted over a three year period and concentrated on SME implementation and usage of an IT infrastructure in general and security authentication infrastructure in particular. The implications of this research are that SMEs are increasingly becoming aware of the importance of the Internet and its related facilities to their organisations. The SMEs in the service sector are faster to adopt new technology and although the manufacturing sector lags behind, they are beginning to adopt the new technology at a slower pace. However, for the majority, security is still not an issue. Companies are still in the embryonic stage of Internet usage and do not fully appreciate the implications of not having a security and authentication infrastructure. But as the trend moves towards increased, more sophisticated and profitable use of the Internet, both socially and commercially, the Internet will become more of a target for unauthorised intrusion and tampering. As more high profile incidents of security breaches occur, they will be publicised and security and authentication will increasingly become an issue for the majority.

12.4 Recommendations

The two most important factors for successful implementation of a security and authentication service in particular and IT related solution in general, are organisational stakeholder commitment and co-ordinated and planned design and implementation of an infrastructure which will support and match the business needs of the organisation. Education and information about the Internet, authentication and electronic data security still needs to be filtered through to SME users, providers of IT services and technology and business support organisations. This information and education process must underline the importance of incorporating three main elements to developing and implementing a security solution in particular and IT solution in general. These are:

- **Business process re-engineering** - an independent analysis of business processes in the organisation, highlighting strengths and weaknesses of current processes and underlining how these processes can be improved in accordance with the organisations' needs and business plans for growth and development.
- **Technology Audit** - must identify the current technology infrastructure in the organisation, design and incorporate the current or new technology to deliver the re-engineered business processes.
- **Support and Training** - the most crucial aspect of any successful IT strategy is the practical every day usage of the system. Thus, a practical training program and support infrastructure for end-users must be designed and implemented in co-ordination with the technology implementation.

12.5 Future areas of study

Future areas of study, on which to build from the findings of this research project, are:

- A further exploration of the use of Public Key Infrastructure (PKI) in more detail - exploring the cost benefits to organisations of all sizes and in different industry sectors and government; and the different applications and usage for PKI.
- More quantitative evidence on the use and cost/benefits of a security and authentication infrastructure.
- Testing the IT Implementation matrix further by applying it to a number of organisations, to build up quantitative evidence to support the framework.
- Continue the time series research to assess the changes in IT infrastructure and usage over another period of time - to see the impact of any new technology on the organisations
- Chart and record the types and incidents of security breaches occurring in all sizes of organisations and across sectors. This would identify the kind of security infrastructure needed and whether what is installed is effective or not.

Research of any kind is an ongoing process and this is particularly true of the fast moving environment of new technology. In order to ensure that the results of this research project are maximised, they should be used as a foundation for further investigation on the use and implementation of security and new technology.

Chapter Thirteen

Epilogue

13. Epilogue

The bulk of this research project was designed, developed and implemented over the period 1996-1998. The research topic is based on an environment where new development and application of innovative technology is constantly being updated in time periods of 18 months or less. As such, this final chapter is a post-script to the study, placing the technology used and the findings, in the updated context of the environment as it stood in 1999. The opinions stated here arose from the research but are not directly substantiated by it.

This chapter shows that the Internet is not a short-term phenomenon but has in fact proved to be the new communications medium of the 21st century. It also shows that the technology and practices on which the security solution was designed, are still valid and that the technology used is still legally viable and will potentially be recognised in law as a means of authenticating electronic documents originating from individuals or entities. It also confirms that the use of the Internet and its related facilities are still growing in the commercial and social sectors, that the technology is still in use and being developed further.

The validity and relevance of this research project, even after a year, will be emphasised by looking at:

- The role of government in promoting e-commerce and introducing a supporting legislative infrastructure.
- The figures showing the rate of growth in the proliferation and use of the Internet in both commercial and social sectors.
- Published case studies showing the application of Internet technologies for the benefit of commercial and public organisations.
- The impact of the new technology on traditional management thinking and business practices.
- And finally the fact that innovative new Internet related technologies and products continue to be developed.

13.1 The Role of Government

The new Labour government elected in June 1998 is a positive supporter of the Internet and e-commerce. It recognised the importance of this new technology and produced a draft of the Electronics Communications Bill for consultation in July 1999, which promoted electronic commerce and Internet usage and introduced a supporting legislative and regulatory framework.

The Government's aims¹³² are that by 2002, 25% of government services will be available on-line, growing to 50% by 2005 and 100% by 2008. The Government also expects that 90% of their routine procurement will be done electronically by 2001. The white paper¹³³ listed a number of initiatives to promote trust and confidence in electronic commerce including:

- The setting up of a new body to accredit e-commerce codes, which meet consumer concerns and which will be identified by a "hallmark".
- Proposals taken forward in Europe to ensure that if an on-line trader in one country mistreats consumers in another country, proportionate and effective enforcement action will follow.
- An investment of £3.5 million to develop new IT systems for Citizens Advice Bureaux (CABx) to give advisers direct access to information on consumer and other issues. These systems are being extended so that the public can gain access at libraries and other public places.
- Setting up a "Consumer Gateway" web site to enable people to find sites on the World Wide Web that give consumer information easily.

The Electronics Communications Bill covers legislation to govern the use of the Internet. The proposed legislation¹³² concentrated on the kinds of security issues addressed in this research project, for example:

1. **Cryptography service providers** - including electronic signature, integrity and confidentiality services. There will be a voluntary register of approved providers of confidentiality, authenticity and integrity of electronic data. The

licensing body and criteria for approval are yet to be detailed

2. **Facilitation of Electronic Commerce** - there will be legal recognition of electronic signatures including the use of electronic communication or electronic storage of information as an **alternative** to traditional means of communications and storage. There will also be modification of current legislation preventing the use of electronic communication in place of paper. The European Commission produced a draft directive on electronic signatures in May 1998, whose main aim is to ensure legal recognition of electronic signatures. The Commission aims to have this directive adopted as soon as possible and implemented by Member States before 31 December 2000¹³⁴. At a global level, UNCITRAL is also working to develop global guidelines to ensure legal recognition of electronic signatures and the European Commission's proposal for a draft directive, aims to be fully compliant with the future UNCITRAL's guidelines.

3. There will be **new powers to assist law enforcement agencies** in making intelligible, lawfully obtained or intercepted encrypted electronic data. This will be by disclosure of the material rather than the encryption keys. There are a number of safeguards where disclosed material will be:
 - Seized under a judicial warrant
 - Intercepted by a warrant from the Secretary of State
 - Lawfully obtained by a law agency under statutory powers
 - Lawfully come into the possession of the law agency e.g. if it was handed over voluntarily

Not only this, but the policy on cryptography also changed by the end of the period of the project in 1999, both in the UK and internationally, despite the continued efforts of the US to control the technology. On May 15, 1998, the European Commission adopted a Proposal for a Council Regulation calling for a notification procedure for intra-Community transfers of cryptographic products instead of the current authorisation/licensing scheme.

In 1999, a detailed survey of embassies, United Nations missions, government ministries, trade boards, and information offices of 230 countries and territories carried out by the Electronic Privacy Information Center¹³⁵ (EPIC), found that overall there is a growing awareness world-wide, of encryption and an increasing number of countries have developed policies driven by the OECD guidelines. Most countries have no controls on the use, manufacture and sale of cryptographic products. This is true for both leading industrial countries and for developing countries. Many countries have recently adopted policies expressly rejecting requirements for key escrow systems. Most notably, in January 1999, France which has long since restricted the use of encryption, reversed the policy and announced that people will be able to use encryption without restrictions. Prime Minister Lionel Jospin¹³⁶ announced that users will be able to use 128 bit encryption (such as PGP) immediately without permission of government. In June 1999, a "Cornerstones of German Encryption Policy" was released, which recommends no restrictions on the development, production or use of encryption products in Germany. In 1998 the Finnish government announced a new encryption policy¹³⁷ calling for no domestic restrictions on the development and use of encryption products and relaxed policies on exports:

*"Finland supports free trade and use of cryptographic products. In Finland, the use of strong encryption should not be restricted by legislation or international agreements ... Finland's aims are to examine the restrictions on cryptographic products so that control lists correspond to technical development, and to ensure that the necessary restrictions will not unreasonably impede normal foreign trade of industry and businesses."*¹³⁸

In the past year (1998/9), Canada and Ireland have also announced national cryptography policies based on the OECD Guidelines, favouring the free use of encryption.

There are a small number of countries around the world that do restrict encryption, but these mainly have strong authoritarian governments. The countries include Belarus, China, Israel, Kazakhstan, Pakistan, Russia, Singapore, Tunisia, Vietnam,

and Venezuela. For many countries, cryptography policy is not a significant national issue and the controls do not appear to be enforced. However, all countries have noted the importance of security of electronic information to the development and growth of electronic commerce and the need to protect privacy online.

The dominant role that state security agencies in the U.S. hold in the development of encryption policy, manifested itself in the pressure applied by the US on the Wassenaar Agreement (WA) extending the Dual-Use Control List on December 3, 1998, to include encryption hardware and software cryptography products above 56-bits. These include Web browsers, e-mail applications, electronic commerce servers, and telephone scrambling devices. Other mass-market products, such as personal computer operating systems, word processing, and data base programs having strengths over 64-bits are subject to controls for two years. These controls must be renewed and approved unanimously, otherwise they will be cancelled. There remains confusion over the control list's distinction between 56 and 64-bit encryption, but it appears that participating states are obligated to establish new export controls over "mass market" encryption software that uses keys longer than 64-bits. They must also restrict other symmetric encryption software and hardware having keys longer than 56-bits (unless a formal export license is issued by the respective national government). The restrictions do not apply to encryption products that protect intellectual property, such as digital watermarking for items like videos, cassettes and DVD disks. Neither are the new WA controls applicable to the "intangible" distribution of cryptography, including downloads from the Internet.

Despite this, several countries such as Canada and Germany have indicated that they do not plan to impose new strict restrictions on exports of mass-market software. The Swiss government indicated that *"the upcoming minor changes to Switzerland's export controls on cryptographic goods as a result of the December changes to Wassenaar will not alter the liberal Swiss Cryptography Policy."*¹³⁹

Overall, recent trends in international law and policy are towards continued relaxation of controls on cryptography. The fact that the United States government continues to lead efforts for encryption controls around the world and the impact that this will have is still difficult to gauge, but the influence of the US in this case seems to be

diminishing.

13.2 The Growth in Certification Authorities and Trusted Third Parties

Another factor in gauging the relevance and validity of the security solution designed in this research project is an assessment of the commercially available security and authentication service providers. The relaxed legislation of cryptography and CA procedures has had an impact on the commercial growth of the security and authentication service providers. Since the late 1996, PKI has increasingly become the standard around which legislation and electronic commerce are being built. The organisations set up in that period were mainly non-profit making organisations tied in to research projects, or commercial organisations still beta testing their products and services and not offering a fully comprehensive Certification Authority service particularly in Europe.

In 1999, numerous commercial spin-offs have grown from research projects and many organisations have developed a business strategy providing security services, as the interest and establishment of electronic commerce into the mainstream has increased. Business partnerships have formed with telecommunications and software companies. In 1999, some clear players in the CA market have emerged, but the service is still in its infancy and services are still being developed. The pattern of CA development is consistent with the era of globalisation and global recognition of brands. CAs are developing as a value added service to existing global multi-national telecommunications or service corporations where a corporate brand name is trusted to provide validation and authentication of customers services. The trend of the certification authority being either based on its own or licensed software, is continuing. The most dominant PKI software provider for independent CAs is Entrust Technologies, who have a strong first mover advantage and seem to be maintaining their edge over the competition. However, other software manufacturers such as Baltimore Technologies are slowly developing a database of users.

Verisign (who have developed a CA in association British Telecommunications Company called BT Trustwise¹⁴⁰) and Belsign (who have launched Globalsign in association with KBC Bank (8%) and ING Barings Bank (15%) have become the

dominant Trusted Service Providers in Europe. Both companies are setting the standard by associating with and partnering, private and public organisations. These organisations are concentrating more on the commercial side, offering business-to-business security services, securing and authenticating servers and offering PKI consultancy to corporate customers. Personal authentication services are being limited to minimum security Class 1 certificates based on e-mail addresses. The software for creating a public and private key for use with both these CAs is embedded in the browser or e-mail packages and it is not dedicated software that is necessary for key creation.

In May 1999, a certification authority service was set up by the Post Office called Viacode¹⁴¹. This differs from the other providers in that the Post Office will provide secure e-commerce services for businesses involving rigorous proof of identity and offering a guarantee of service up to a value of £100,000. It also offers secure server ids to restrict access to web sites, companies can select a 'club' of users as large or as small as they wish. Royal Mail's "certification" process is initially only available in a form suitable for business customers. Certification of private individuals will be a service for the future. ViaCode is based around security software developed by Entrust Technologies. This works with most popular business software including e-mail, Web browsers, spreadsheets, word processors and electronic forms.

Thus, the technology used and security solution designed at the beginning of this project is still relevant and valid and is increasingly becoming the norm for security and authentication practices in 1999.

13.3 Continued Internet Growth

During 1998 and by 1999, a large number of surveys by a number of research organisations had been carried out and continue to be carried out to determine the current and predicted size and rate of growth of the Internet. None of the figures actually tally with each other, but Table 32 gives an indication of the size of the Internet and rate of growth from the myriad of published figures.

YEAR	NUMBERS OF INTERNET USERS IN THE UK	RATE OF GROWTH
1997	4 million to 7 million	
1998	6.5million to 10.6 million	50-60%
1999 - 2001	10 million to 25 million	estimates for growth of between 50% to 160% p.a.
SOURCE: WWW.NOP.COM (3/3/99) ; WWW.IDC.COM (5/7/98); WWW.FORRESTER.COM (6/4/98); WWW.DATAMONITOR.COM (10/9/98); WWW.MIDS.ORG (29/6/98).		

Table 32 . Internet Users in the UK

Although the actual figures are numerically inconsistent (probably due to the differences in methodologies questioning and sampling techniques) the overall trend is clear. There is a large growth in the rate of connectivity to the Internet in the UK and the rest of the world.

A survey by the Guardian/ICM¹⁴² in January 1999, found that the Internet was no longer just the specialist preserve of academics, scientists and "Net nerds", but is becoming a mass medium widely used by the public. The survey showed that nearly half of the adult population in the UK were connected (43%) with a further 14% planning to come on line by the end of the year - a rate of expansion more than double 1998's 1% every 2 months. It also showed that British users were attracted by the huge amount of information available, but felt overwhelmed by it and were frustrated by the time it takes to find the information relevant to them. Typical home users were still men in their mid 20's to 30's, of the social class ABs* (33%) followed by C1s, white collar workers (16%). Only 2% of DE semi-skilled and unemployed users are linked at home. Overall Internet use at home in the UK at 14% is still far behind those

* Professional and Senior management

in the US (27%) and Scandinavian countries such as Sweden (21%), but the biggest rate of growth is expected in home Internet access over the next year. Use of the Internet in 1998/99 was mainly searching for information regarding employment, travel, searching for a particular company, reading newspapers online, searching for financial information.

A report by NOP¹⁴³ revealed that 1.3 million users shopped online in the second half of 1998, making a total of some 4.8 million purchases and spending £470 million between them.

"With users becoming more familiar with the Web as a primary source of information . . . their confidence in using it for an increasingly complex range of activities is also growing". ¹⁴³

13.3.1 Proliferation of E-mail

During 1998 and up to the first half of 1999, with the exponential growth of the Internet and offers of free Internet connection, e-mail was rapidly becoming a ubiquitous tool for business and personal communication. According to a 1998 survey by the European Electronic Messaging Association (EEMA) ¹⁴⁴, 72 million employees across Europe will be using e-mail by the Year 2000, sending over 4.1 trillion e-mail messages per year.

Despite the enormous strides in technology, the standards for handling e-mail on the Internet, Simple Mail Transport Protocol (SMTP), still lack the features such as delivery notification and directory services. These concerns were voiced by business, and this was one of the reasons delaying the introduction of e-mail commercially. The EEMA survey¹⁴⁴, revealed that 53% of respondent businesses were so concerned about security they did not use it for commercial purposes. EEMA amongst other organisations, are still working to agree and improve standards for e-mail directories that will allow Internet users to look up e-mail addresses and encryption keys of trading partners more easily.

Although e-mail and browser software providers are increasingly developing features within e-mail packages to provide delivery notification and security options, these settings can be altered or disabled by users and the security features are often minimal and incompatible across different types of e-mail software. Furthermore, the recent trend in the mass availability of free e-mail accounts including Yahoo, Excite and Hotmail have highlighted a host of vulnerabilities that could and have allowed hackers to take control of users' accounts because of a lack of basic security. One example is that the free mail accounts do not limit the number of logon attempts. This opens the door for hackers to launch brute-force password attacks since these sites do not use the Secure Sockets layer protocol for authentication and encryption¹⁴⁵ as of February 1999.

Another increasing trend of e-mail usage is information warfare and sabotage. Whereas previously viruses were largely transferred through sharing unsafe software, now with e-mail and the Internet, transfer of viruses is becoming more easy and deadly. New generations of viruses are taking advantage of the complexity of the latest computer operating systems to spread software devices that propagate themselves, find information of interest and send it to a specified location via the Internet. One such virus, Caligula, travels in Word documents and even in PGP where it can copy the "keyring" file which is the heart of the program for its perpetrator. Another recently discovered virus Picture.exe targeted America Online, where it stole users' passwords and user names and mailed them to an address in China. Similarly the Happy.exe virus hidden in an electronic greeting card copies e-mail logs from the user and mails itself out with every new e-mail¹⁴⁶. Thus, already the security needs of organisations using e-mail have to incorporate new and modified means of attack and threat.

13.3.2 Security

In 1998, security was one of the biggest worries for business and consumers. Customers were still concerned that hackers might get hold of their credit card details. Only 55% of companies had a formal security policy and nearly all were far from adequate¹⁴⁷ not covering major issues such as data and network security. More than 80% of companies¹⁴⁸ said that security was the leading barrier to expanding electronic links with customers and partners. Security was increasingly becoming an important issue in organisations, which was forcing them to introduce more practical measures.

In a Global Information Security Survey 1998¹⁴⁹ of 4300 IT professionals in 35 countries, it was found that Year 2000 projects were overtaking security in prominence, importance and proportion of IT budgets. For the majority of organisations, the most common access to the organisation's electronic data was through dial-up (69%), leased line (29%), ISP/Internet (20%), Virtual Private Network over the Internet (7%). There had been a 50% increase in Internet connectivity by respondents. The main use of the Internet by these companies was mainly to save costs, but the Internet also offered the opportunity to develop new market opportunities. For many organisations, one of the barriers to electronic commerce was the lack of security - that is opening up their systems to the public domain - inadequate technology in terms of being able to support the volumes of traffic securely and speedily and unclear Returns on Investment (ROI).

Of those who did use the Internet, only 7% used secure e-mail, 5% used digital certificates, while 60% relied on password authentication for Internet access, 19% used encryption with their Internet connection and 35% didn't plan using the Internet at all. 75% of IT professionals had some level of confidence in their ability to defend from internal attack and this increased to 83% that felt confident they could defend from external attack.

The main security measures implemented in organisations were security policies and system based products - namely security tools (65%), active monitoring against unauthorised intrusion (58%) and firewalls (50%). However, organisations felt that the greatest security risk came from industrial espionage, competitors and business

partners. But the highest risk they felt was of malicious damage which might have adverse affects on the business, believed to come from external sources - hackers, computer terrorists and unauthorised users and internal sources - former employees, competitors, contract workers. Over 90% of IT professionals rated security as very or extremely important. This awareness in the importance of security had risen over the years and was increasingly receiving a commitment from management who were beginning to allocate larger budgets.

Having said this however, in reality, it was found that there was a decrease in actual network monitoring and security policy compliance monitoring. The security solutions implemented were:

- Technology measures - password authentication (58%); firewalls (55%); encryption (17%); Secure Socket Layer (SSL) (11%)
- Other measures - security awareness training (30%); physical security tools such as bolts and locks (35%) and risk analysis (31%)

The majority of companies acknowledged that employee awareness of the risks and dangers of security breaches is one of the greatest obstacles to implementing IT security in an organisation.

Although the awareness of the need for security was increasing among businesses, the image of the hacker was still the mischievous "techie" who saw hacking as a challenge. One such hacker hacked into Germany's biggest on-line service by introducing a Trojan Horse programme in a software tool offered free to customers who completed a registration process. This unwittingly passed on customer access codes and passwords to the hacker, who is largely motivated by the challenge of an organisation with sophisticated security - *"it was no fun to hack into organisations that had no encoding system that needed to be cracked"*¹⁵⁰.

Towards the end of 1998, attempts to dispel the fears and myths about security on the Internet were being made.

"the basic proposition that the Internet is insecure is diminishing as people become familiar with it. The more you become familiar with the existing systems out there, the more you realise that it's a lot more secure than handing over your credit card at a restaurant"¹⁵¹

Explosive growth of the Internet has led to a 600% increase in cyber fraud. The number of reported Internet crimes leapt from 1,280 to 7,752 according to the US National Consumers League¹⁵². Some commentators believe that encryption will help reduce the theft and misuse of private data but will do little to prevent the overwhelming majority of Internet fraud. The real challenge for the future went beyond basic encryption and security systems into authentication routines that would allow companies to verify purchase orders and have transactions witnessed with legal status. This has been the central topic of the research topic undertaken in this study, underlining the fact that data security and authentication in 1999 is a crucial development for the future of electronic commerce and Internet use.

13.4 The Application of Internet Technology

The case studies conducted under this research project showed the cost benefits of integrating Internet based technology into organisations. Since the commencement of this project, organisations world-wide have applied Internet technologies in a number of ways. A brief summary of some published case studies show that both commercial performance and public services are being improved by the application of Internet technology in a number of different ways. Some of these include:

- **A new business model** for attracting customers, where the operation is totally Internet based e.g. The Prudential's Internet banking service egg.com and the now legendary Amazon.com (Internet book retailers)¹⁵³. Amazon.com started in a garage by Jeff Bezos in 1994 and is now worth \$5.5 billion (December 1998) on the American NASDAQ Stock exchange. All this despite accumulating a total deficit of \$115.6 million. However customers and investors continue to have confidence in the company, which is viewed by many as the model for E-companies in the new millennium. The value added is that the company not only sells books, but

also offers a customised service - information about books, which particularly interest them. Bezos sees his company as an "*information broker ... the consequence is that we have 2 sets of customers: consumers looking for books and publishers looking for consumers*".¹⁵³

- **Where it is part of the existing business model and it is used for providing a better service to existing customers e.g. Charles Schwab Inc. (stock brokers) who have customised their web pages based on their customer preferences for stock reports, related research and account balance information¹⁵⁴. Within 6 months of getting on the Internet, 90% of its 2 million active online accounts representing \$145 billion, are trading over the Web. The volume of business is reported to be 4 million transactions a day.**

- **Improvement in an organisation's internal procedures and communications and realising economies of scale e.g. BMW's company-wide use of PC conferencing and application sharing to allow virtual collaboration of employees and other experts who are based in different sites and locations, to work on the same project more efficiently. The key benefits of this are reduction in development times and costs, more effective information and application sharing among different parts of the company as well as social benefits relating to employees being able to interact with families while working away from home. Daimler Chrysler (car manufacturers) introduced an on-line supplier incentive program (SCORE) for 1,500 of their suppliers. This program involves sharing cost savings with suppliers who propose ways to build cars more economically. The extensive use of e-mail makes available every step of the process in a proactive manner to all the parties concerned. Automated reports are available to teams of suppliers on demand. In 1998, it was reported that this program saved the company \$92 million¹⁵⁵.**

- **Extending its brand position, achieving sufficient sales volumes and providing customers with outstanding value and a unique shopping experience e.g. Amazon.com¹⁵⁶ and Toys R Us.** The latter reported a net loss of \$422 million for the first nine months of 1998 and has led them to look at the Internet and the threats and opportunities it offers. Toys R Us intends to close down 90 US and 50 European stores but to increase its on-line presence and develop it further from a site for posting its company history and press releases, to a fully functional e-commerce site. The number of visitors to their site has increased four-fold from 10,000 in June 1998 and orders are also reported to have increased. The company has invested in technology and now has 11 servers and is managing more than 4,800 items. It is integrating the retail stores with the web site sales strategy by promoting the most popular items in stock and available from their stores. Customers may also return any defective goods bought on-line to the stores.¹⁵⁷

Despite all the advantages and benefits illustrated, there are risks which include competition from other on-line suppliers, manufacturers and retailers around the world, dependence on vendors/distributors and management of growth arising from the size of the market. There is also the added risk of IT investment and spending, in an environment which experiences such rapid evolution and shrinking lifecycles, is wasted on unusable or obsolete technology. These risks must be identified by the organisations and built into the business growth and development strategies.

The author also believes that another very big risk to the future of e-commerce is the hype that surrounds Internet companies and e-commerce being fuelled by third party financial investment organisations. These financial investment corporations are inflating the value of Internet companies founded on potential future cash-making projections, rather than current sound business performance and practices. There is a risk that once the actual value of these Internet companies based on financial performance is realised, then this could be potentially disastrous for the overall confidence in Internet businesses. Amazon.com have yet to become profitable and are continually showing extensive operating losses since its birth. These losses are

expected to continue in the next few years until it reaches profitability. But it is still attracting hefty investment and market confidence, which has made it one of the leading Internet companies on the stock market ¹⁵⁸. The recent price war between competing companies - Amazon.com and Barnes and Noble - shows that although the Internet is a licence to make money in the short-term for shareholders¹⁵⁹, in the longer term, real issues of performance profitability and sound business practice will come into play in the future survival of these companies.

Governments world-wide are becoming involved in Internet based technology projects to improve the socio-economic infrastructure of cities and also as a means of regeneration for declining economies which were once reliant on traditional heavy industry.

The Naestved Info-Society 2000 project¹⁶⁰ in Denmark is one which aimed to physically construct an IT infrastructure and integrate IT into every aspect of society including schools, public services and business. It aimed to create a highly skilled workforce and thereby build a stronger competitive advantage for the city in attracting investment. The project consisted of two phases - 1) the construction of the cable network infrastructure 2) the development of regional services on the Internet. By 1998, all 22,000 households in the city had the choice of being connected to an ISDN network. Over 25% of the population are connected (1998) and this figure is growing.

The Naestved project is being used to encourage citizens and businesses to use the new infrastructure and take advantage of the opportunities it presents. By the end of 1998, there were regional public and business service directories and business development schemes, which will support SMEs with the implementation and use of IT in their organisations. PCs were being introduced into schools with the goal of having at the most one PC per 5 children. Free training was being offered to teachers. The local council had set up open data centres offering guidance, advice and training to the unemployed, disabled and the young.

The city is now (1999) piloting a digital signature project where business on-line will be conducted using a digital signature. The pilot will cover:

- The use of digital signature and smart cards within the City administration and e-mail
- Exchanging legally binding documents between the city administration and citizens
- Smart forms - the use of digital signature in electronic forms and in government purchasing

It will involve between 500-1,000 community employees and about 100 SMEs in the first half of 1999, using smart cards and a third party certification authority. At the time of writing a report still had not been published with initial findings from this pilot project.¹⁶¹

There are a number of similar projects around the world, from the US where these are known as "smart communities" to Singapore's "intelligent island". In Villena, the South of Spain, a similar project called Infoville is being piloted¹⁶². Innovative government programmes were being set up enabling the accessibility to computing equipment, training, city hall and regional government services, medical appointments scheduling, staying in touch with children's schools and buying from local merchants. One of the more ambitious smart community projects is now underway in the Francophone Wallonia region of Belgium where a network is being created to encompass e-mail, database access, video-conferencing and electronic commerce. There are nearly 400 projects representing more than 160 cities and regions covering visual arts in Ireland to the democratisation process in South Africa¹⁶³

The results of these projects are yet to be published in full and analysed. But again the trend is towards increased implementation and usage of Internet technology underpinned by a security infrastructure based on digital signature technology and authentication.

13.5 The Impact of Technology on Management Thinking

As has already been identified in this research project, there is a need for a change both in management thinking toward new technology and a re-engineering of business processes to maximise the myriad of resources and opportunities offered by the new technology. Greco¹⁶⁴ points out that current working practices have been based on the dominant business model created by Sloan in the early 1900's for General Motors. This highly structured model of command and control, where employees are viewed as an overhead is and will continue its descent into obsolescence in the 21st century. Greco stresses that companies must develop a better understanding of their processes and the realisation that organisations increasingly belong to a web or network that extends far beyond itself and includes outsourced workers, suppliers and external customers. The new model is complex and includes factors such as globalisation, new technology and the perception of employees as assets rather than expenses. Herman and Gioia¹⁶⁵ also identify this trend of employees as stakeholders where their contribution to the organisation is meaningful and collaborative. They believe that workers will become more like independent *intrapreneurs*, where they will come together.

*"as needed, provide a particular function, disband and then merge into some other form to complete some other functions. We are seeing that now with outsourcing, contingency workers, people working at home part of the time. It's very fluid, very amoeba-like structure, where cells divide and come together again and again"*¹⁶⁶

They also see the roles of managers changing to concentrate more on productivity, strategising and problem solving.

*"Their roles will encompass ... managing information flows, hiring and retaining qualified people as the competition for talent intensifies, monitoring intellectual property and keeping up with technological advances"*¹⁶⁷

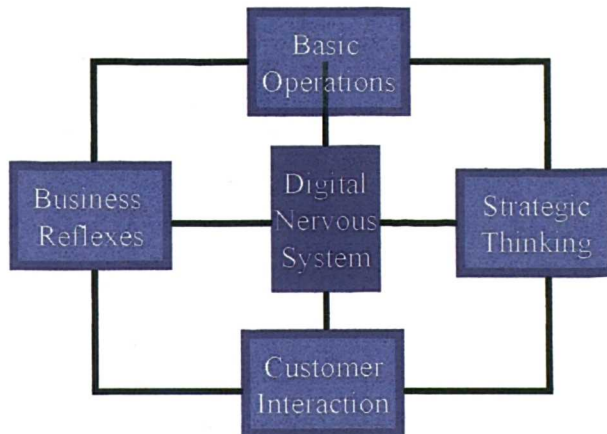
Bill Gates, one of the most powerful players in the IT industry, also believes that the implications for businesses to re-engineer their processes in order to maximise the use of their information is crucial to survival in the 21st Century. According to Bill Gates¹⁶⁸, business will change more in the next 10 years than it has in the past 50. The 1980's were about quality, the 90's about re-engineering the 2000's will be about speed. That is, how quickly business will be transacted and the speed of improvements in quality and business processes. Manufacturers or retailers will respond within hours to changes in sales, changing their traditional definition of a product company, to a service company offering a product. Gates feels that very few companies are using digital technology to build and develop new processes that will radically improve how they function, give them the full benefit of their employees' capabilities and give them the ability to respond speedily and compete in an emerging high-speed business world. Gates believes there are going to be 3 fundamental business shifts that will occur as the result of the digital age:

- Most transactions between consumers and business; business and business; and consumers and government will become direct digital transactions. Intermediaries will either become obsolete or develop into something else.
- Customer services will become the primary value-added function in every business. Human involvement in service will shift from the routine low-value tasks to a high value personal consultancy on important problems, issues or desires of the customer
- The pace of change in transactions and the increased need for personalised attention to customers will increasingly lead companies to adopt digital processes or perish.

Gates believes that companies are not using information well, although they are spending on the infrastructure - namely the network, PCs, e-mail and basic business application. Gates estimates that companies are only getting 20% of the benefits from their investment in technology. In order to get the full benefits, he points out that a new digital infrastructure must be developed. Using an analogy of the human nervous system, Gates develops the idea of a digital nervous system consisting of both hardware and software, where digital processes enable a company to perceive and react to its environment, to sense competitor challenges and customer needs and to

organise timely responses. Businesses must develop an ideal picture of the information it needs to run the business, to understand markets and competitors. This type of information must be available to the right people, in the right format, ready for immediate action and this is what the systems must be developed to do.

Anatomy of the Digital Nervous System



Source: *Business @ The Speed of Thought* W.H.Gates

Figure 49 . Anatomy of the Digital Nervous System

A digital nervous system comprises the digital processes that closely link every aspect of a company's thoughts and actions. Basic operations such as finance and production, plus feedback from customers, are electronically accessible to a company's knowledge workers who use digital tools to quickly adapt and respond. The immediate availability of accurate information changes strategic thinking from a separate stand-alone activity to an ongoing process integrated with regular business activities.

Joe Firmage¹⁶⁹, founder of a US Web research company, also identifies the need for re-designing business strategies and processes to incorporate current new technology. He points out that many companies have not thought through their e-commerce strategy. They believe they should have a web site but don't have any idea what that site should achieve and what they want to do with it. A common attitude is to launch a web site and see what happens. Companies frequently fail to look at the figures or develop a business case for the Internet. E-commerce allows companies in all

industries to give all customers superior customer service at very little cost. For example on-line catalogues, sales and tracking of purchased products.

Again the mindset of most businesses, especially SMEs, is within the traditional business model. Companies see the Internet as a potential distribution channel, as well as a means for reaching a specific group of people and building brand awareness. But, the Internet has developed a new sales model. Everything is done from the user's perspective - allowing a forum for discussion, a means for building relationships with customers and identifying their shopping habits and interests. Firmage¹⁷⁰ sees the need for better-screened, trained and educated employees as essential to maximise business use of new technology. According to Firmage, one of the biggest barriers is the lack of resources to integrate e-commerce systems into their existing infrastructures.

Firmage warns, that unless British retailers set up strong well-promoted web sites and e-commerce operations within the next 12 months, they will be swamped by US corporations planning on-line operations to sell products around the world. His research showed that British firms are falling behind their US counterparts who are estimated to hold 75% of the world's Internet transactions. The main reason being that British firms are largely apathetic about the threats and opportunities of the Internet and have yet to win any meaningful share in this fast growing market. Big brands built on the Internet such as Amazon.com, are web-only brands and are equally as well known on both sides of the Atlantic. But in time he feels that these will have a negative impact on the British retail market. However, the majority of industry stakeholders agree that in this new IT environment, there is no template and constant evaluation is necessary.¹⁷¹

13.6 Future Technology and Trends

As we have seen, technology is constantly changing and developing and new technology is being invented. With these innovations, come new applications of technology. A report by IDC¹⁷² suggests that growth in the UK electronic commerce market will be spurred on by the introduction of new technologies. The technology is too complex to discuss in detail here and is beyond the scope of this study, however some of these new technologies and their potential uses are briefly described in the following section.

13.6.1 Smart Card

This technology has been around for many years, initially with less sophisticated magnetic strips. Smart cards have advanced and are now effectively a computer the size of a credit card with an embedded microprocessor chip. There are about 80-100 proprietary smart cards each of which is used for storing different kinds of information e.g. storing health records, telephone cards, etc. This means that the smart card application and operating system is installed on the smart card and the issuer controls which application is required.

The advantages of smart cards are that they can have multiple uses, they provide an added layer of security as they are difficult to forge and are tamper resistant. A smart card can protect itself with a pass phrase or PIN number and also locks itself if the PIN number is input incorrectly a pre-set number of times. A cryptographic smart card has the further advantage that the private key is generated on the card itself removing the risk that the profile generated with the private key cannot be accessed for use in a brute force attack. Also calculating the unique hash and storing it on the smart card, which is encrypted, creates a digital signature.

13.6.2 Biometrics

Systems are being developed to store, capture and recall people's unique biological characteristics. Examples of this include:

- Photo fingerprints at a standard workstation¹⁷³ which will avoid the necessity for providing documentation or remembering passwords. Fingerprint verification has been used in cash machines since 1997 in South Africa. In Spain the social services department is paying benefits using Identicator Technology's finger-imaging system with smart cards (described below).
- Dynamic signature verification where a touch sensitive pad is used to capture the speed and style of a signature not just its appearance trialed in the UK in Liverpool and Tyneside for people claiming employment benefits and a canteen in Pentonville prison¹⁷⁴.
- Face recognition systems to identify trouble makers in a crowd used by Watford FC¹⁷⁴
- Iris recognition is also a unique personal identification method being used by Iris Recognition Automated Teller Machine being piloted in the US (Bank United), Spain (Argentaria), Italy (Banco Ambrosiano Veneto), Norway (Den Norske), Turkey (Akbank)¹⁷⁵.
- Voice Recognition - where unique voice matching enables individual verification used in telephone banking by Chase Manhattan Bank.

The introduction of these technologies could eliminate some of the problems identified in the research project, which made security software vulnerable, by users forgetting or being careless about storing and divulging their passwords.

13.6.3 Internet II ¹⁷⁶

Research is being carried out in the US to develop Internet-II, a network that will be almost 1000 times faster than the current Internet with the ability to store terabytes of data. This is being designed primarily to offer high speed communications between more than 100 university and research centres in the US. With funding both from the private and public sector, the new network is a combination of leading edge fibre technology and routing technology which will enable the most advanced applications¹⁷⁷. This is expected to become available to the public in the near future, but exact details are currently unavailable.

A standard is also being developed which will make the resources of the Internet's World Wide Web available audibly over the telephone¹⁷⁸.

13.7 Conclusions

The post script to this research study finally concludes that the Internet, related technologies and applications of that technology is increasingly moving into the mainstream of social and commercial use, with Internet usage in all socio-economic sectors continuing to grow. The benefits of the Internet to business in terms of improved costs and process efficiencies have been well documented. The impact of the new technology on traditional management thinking is being voiced by leading figures in business and academia. Governments are promoting the Internet and related technologies as the medium for the future growth, development and competitive advantage of nations. In the UK, the government is taking direct action in the promotion of the Internet by enabling and encouraging its own national administration services to be carried out over the Internet. It is also taking indirect action by building legal and regulatory support infrastructures and facilitating the development of other social, commercial and financial infrastructures.

Security measures focusing on encryption and authentication technology are increasingly becoming the foundation for delivering Internet related security. The government has recognised this trend and has incorporated security issues into legislation. The growth of commercial security and authentication service providers is a testament to the fact that security is becoming one of the dominant issues in the 21st century. New technology is being developed to improve the network infrastructure and application of it.

The above factors underline the fact that the research project undertaken was ahead of its time. The project's findings and technology are still relevant, highly valid and can be used as a foundation on which to develop and grow the issues of security and Internet usage in SMEs. At the beginning of this project there was not yet a proliferation or widespread use or awareness of the Internet or security. However it was and still is a crucial topic as the Internet is increasingly used for commercial purposes, so crime will move from the streets to the Information superhighway. This project is the first step in trying at best to develop an infrastructure, which thwarts the criminals, and at least raise awareness of SMEs in particular, of the different types of security needed and the framework for implementation in organisations.

APPENDICES

Appendix 1 - Economic Regeneration Using IT

This appendix includes the paper *Economic Regeneration Using Information Technology* presented at the Business & Economics Society International - Rome, June 1998 by R.Tassabehji and M.Vakola.

It is a self-contained paper where references, figures and tables referred to are included in the paper and do not refer to any other references, figures or tables referred to in the main body of this PhD report.

Economic Regeneration Using Information Technology

A Case Study - by R.Tassabehji, M.Vakola.

1. Introduction

This paper will discuss the impact of information technology on economic growth and the development of business for the 21st century. The "information revolution" and the creation of the "information society"¹ will be put in the context of an economic cycle. Business and the economy are inextricably linked with the development and implementation of new technology. Growth and development of any modern economy has been recognised by many economic theorists such as Kondratieff, Schumpeter, Mensch and Porter, to be based on innovation and new technology. The old economic factors of land, capital and labour are no longer enough to determine the success of businesses in a "modern" economy. New factors include technology and the capacity of an industry or economic cluster to innovate and adapt new technology to advance business success.

However, tied into this, is not only the business community but also the larger social milieu in which innovation is nurtured. The business community is not isolated, but is an integral part of the social community. It does not stand on its own, but relies on education, the community and society at large to develop and deliver an "innovative milieu"² in which technology can be developed. This paper will discuss the GEMISIS 2000 project currently taking place in Greater Manchester. This project is a test bed for the new social co-operation model for regional economic growth, regeneration and business in the 21st Century.

1.1 The Economic Cycle of the 21st Century.

There are several schools of thought on how and why nations have attained economic growth and success. Far from being single ideological theories, the several schools of thought sometimes share common premises – one such premise is that innovation is an enzyme which acts on the four economic factors of production first identified by Adam Smith⁽¹⁾. Refining Kondratieff's *Long Wave Theory*⁽²⁾, Schumpeter⁽³⁾ maintained that economic development appears in the form of innovation, which occurs in cycles. Schumpeter assigns technological innovation an almost exclusive role, as the engine of economic development. He insists that the opportunities for technical innovations are very unevenly spread across different sectors of the economy and are not continuous over time, but occur in explosive bursts as entrepreneurs realise the economic potential arising from new combinations of technical and organisational change. Mensch⁽⁴⁾ updates Schumpeter's theory, giving it an empirical base in history, where clusters of basic innovations take place and generate completely new sectors. He stresses that only innovation can overcome depression and that government must implement an aggressive innovation policy to stimulate the search for new and basic innovation.

¹ The Information Society is the name most commonly used to describe a world-wide phenomenon in the late 20th century. The simplest way to describe the Information Society is "a society in which economic and cultural life is critically dependent on information and communications technologies and where people get the full benefits of that technology at work, at home and at play." It is facilitated by a global telecommunications infrastructure and the emergence of a global economy. Everyday manifestations of that technology range from ATMs for cash withdrawal and other banking transactions, to mobile phones, faxes, teletext television information services and computers. The Information Society will enhance leisure time, enrich culture and help relieve pressure on our cities and towns by enabling people to work from home, or in other teleworking environments. It will also offer new opportunities to enhance national productivity, competitiveness, employment and lifelong learning. The first countries to enter the Information Society will reap the greatest rewards. They will set the agenda that others must follow.

Information Society Commission, 1998.

² Camagni 1992

Figure 1 represents the Kondratieffian Business Cycles in the context of historical economic premise and technological innovation.

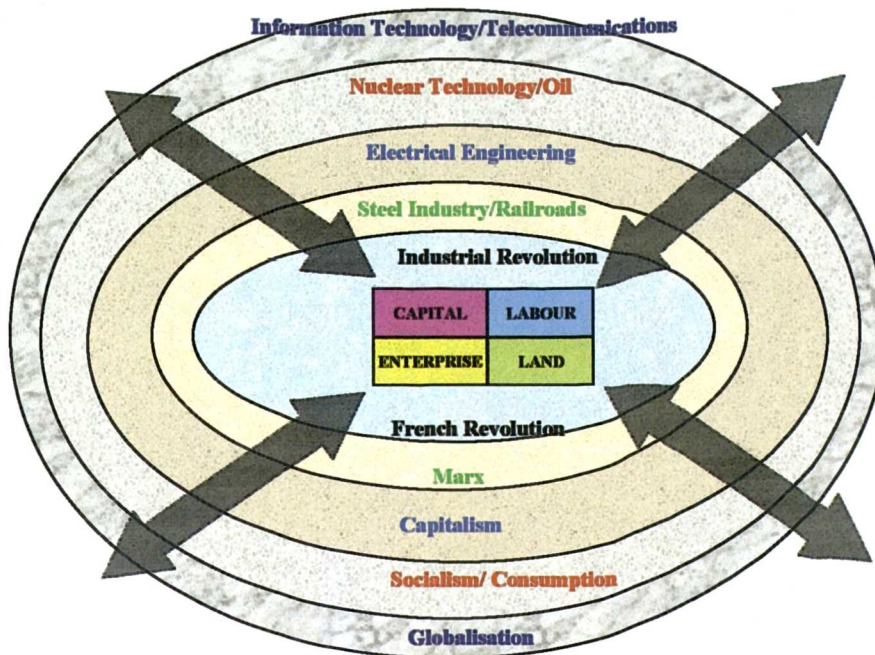


Figure 1. The Kondratieff Business Cycles in Historical Context

The technological innovation which triggers off each economic cycle, has an impact on the four economic factors of production – namely land, capital, labour and enterprise. Table 1 broadly summarises the dates of the economic cycles, the political milieu of the time, the main influential innovation and a brief outline of some of the impact on the economic factors of production.

Economic Cycles	Politico-Economic Influences	Technological Innovation	Impact on Factors of Production
First Wave (1780's – 1830's)		Industrial Revolution (I) Iron Industry/Textile Industry/ Steam technology	Land – Iron and coal resources Capital – overseas trade, sophistication of trading and banking systems Labour – division of labour/factory workers/increased population Enterprise – Investment by landowners in new industry
Second Wave (1830's – 1880's)	<i>Marx</i>	Industrial Revolution (II) Steel Industry/ Railroads	Land – Pig Iron coal resources Capital – joint stock banks, issuing of notes alongside gold, stable banking system Labour – improved conditions and education for workers Enterprise – Investment by the State and venture capitalists

Third Wave (1880's – 1930's)	Capitalism	Electrical Engineering/ Electricity/Motor manufacturing	Land – Coal, petroleum, other metals and semi-conductor Capital – increased overseas trade, development of international financial markets Labour – More skilled labour, demise of child labour, improved education and conditions Enterprise – Inter-war speculation
Fourth Wave (1930's – 1990's)	Socialism Unionism Consumption	Nuclear technology/ Oil / Electronics/ Micro- processing technology	Land – Aluminium, silicone, petroleum Capital – increased international investment, sophisticated financial markets Labour – Highly skilled labour, universal education and basic standards of living, integration of Trade Unions into common working practices Enterprise – International investment
Fifth Wave (1990's –	Globalisation International Integration	Information Technology/ Telecommunication Technology/ Bio- technology and Genetic engineering	Land – recycled/ environmentally friendly materials Labour - Workers skilled in knowledge- based products and services rather than in manufacturing Capital - Money like information is now only data single-market world Enterprise – Monopolistic media and IT, priv institutional investment for the many (e.g. pension schemes)

Table 1. Economic Cycles and Factors of Production

As each economic cycle has been completed, this has shifted the importance of the four economic factors of production as the sole catalyst for economic growth. Porter (6) emphasises this fact, maintaining that the prosperity and competitive advantage of a nation is no longer as a result of a country's natural endowments and its labour force, but rather on the ability of its industry to innovate and upgrade. Despite the fact that the economy goes through the phases of *Prosperity, Recession, Depression, and Recovery*, after each wave the new innovation builds on the framework that has been developed before. Far from being mutually exclusive cycles, each new cycle is a product of the economic development and technical innovation that has gone before.

1.1.1 Catalysts of Innovation

In order to understand the impact of innovation on an economy, we must understand the factors which give rise to innovation. According to Schumpeter (5), clustering of innovation is caused by the motivation and the action of the entrepreneur i.e. the socio-economic milieu in which innovation is nurtured. This is taken further by other socio-cultural and institutional relativists who underline the impact of historical formation of social institutions and political environments on the development of firms and industry and their respective economic success. Hart (6), Zysman (7) and Cox (8) look at the relationships between State and Civil societies, how they are organised and institutionally linked, as a result of historical and contextual factors inherited from the past. The shift and development of societal relations marks a shift in the nation's ability to develop and diffuse technological innovations. David Landes (9), maintains that rich nations continue to prosper, because of their relative ability to exploit science, technology and economic opportunity largely as a result of national attitudes about a myriad of cultural factors. Landes contrasts the characteristics of successfully industrialised nations - such as a predisposition for hard work, open-mindedness and a commitment to democracy, thrift, honesty, patience, and tenacity - with those of non-industrial countries, arguing that until these values are internalised by all nations, the gulf between the rich and poor will continue to grow. For Landes, the

ability to effect an industrial revolution is dependent on certain cultural traits, without which industrialisation is impossible to sustain.

There are many other theories which attempt to account for innovation. Porter recognises the importance of innovation to the success of a nation, but discounts the importance of State intervention, expounding a theory of Darwinian type market forces on the theory of the firm, which leads to the clustering of innovation and ultimately economic success. Others (Camagni ⁽¹⁰⁾, Jaskari ⁽¹¹⁾) see the importance of State intervention and policy in creating an "innovative milieu", a combination for the interaction of local innovativeness and synergy, to an economy's regeneration and growth. As we have seen, the fifth Kondratieff wave is being driven by information and communication technology. According to Jaskari, an "innovative milieu" allows technology imitation and technology creation capability, fast reaction capability, capacities for shifting resources from declining spheres of production utilising the same fundamental know-how, capability of regeneration and restructuring of local economy hit by external turbulence. It also involves local socio-economic fabric. That is because externally driven growth may seldom generate a sustained development process in the long term, and may more easily create only "cathedrals in the desert" (Camagni (10)). Jaskari (11) presents a case study of the intervention of State policy in the creation of technology centres in Finland, developing a "network economy", which is a co-operative system between firms. He sees this as the way of the future.

The EU has recognised the importance of innovation in the growth and development of their member economies and in particular the importance of technology. The European Union's series of Framework policies (Appendix 1) has played an important part in promoting and nurturing new successful sectors and restructuring old declining traditional manufacturing based sectors. Far from seeking to replace national initiatives and powers, the principal role of EU action is to extend, complement and enhance the research activities of the Member States in order to address the three major weaknesses of European RTD³ vis-à-vis its competitors

- A proportionately lower level of investment in RTD;
- A lack of co-ordination at the various levels of the research and technological development activities, programmes and strategies in Europe;
- A comparatively limited capacity to convert scientific breakthroughs and technological achievements into industrial and commercial successes.

One such project currently being undertaken in the North of England is the Gemisis 2000 project. Funded by European Regional Development Fund (ERDF), Single Regeneration Budget (SRB) and Framework IV (ACTS).

1.2 GEMISIS 2000 – A Case Study

1.2.1 Description of the project

GEMISIS 2000 is a collaboration between the University of Salford, Cable and Wireless Communications, the City of Salford, the City of Manchester and Manchester Training and Enterprise Council. The project aims to develop user driven applications that exploit the sociological, economic and technological benefits of the Information Superhighway in order to assist in the regeneration of the North West of England. GEMISIS 2000 has been working since July 1995 to develop applications capable of exploiting the broadband fibre optic cable. The strategy is to create a number of GEMISIS 2000 Service Areas (GSAs); Business, Education, Health and Community ⁽¹²⁾.

1.2.1.1 GEMISIS 2000 Business Services

The Virtual Chamber or "TVC" is a major project which has been developed under the GEMISIS 2000 'umbrella' by a collaboration of private and public organisations and is dedicated to helping businesses expand and prosper. The focus of the project is on delivering effective services to over 450 business harnessing the considerable expertise which this collaboration brings to bear.

³ Research and Technological Development (RTD)

The project features the electronic delivery of the types of service which have traditionally been demanded by businesses and delivered by agencies such as Chambers of Commerce, Training and Enterprise Councils (in respect of business services) and Universities (in respect of professional education, technology transfer and R & D support). Businesses will be offered a 'ladder of opportunity' to progress from narrowband through mediumband up to broadband services.

Subscribed companies can have access to a range of services ranging from marketing, IT and financial consultancy where members can select relevant areas of research activity in which to contribute and participate. These services will be particularly useful to SMEs which don't have the resources or access to specialist knowledges. The TVC will allow small and medium sized companies to understand and realise not only how to learn new skills and methods in order to use technological applications effectively but also how to use information technology in order to become more productive, creative and competitive.

1.2.1.2 GEMISIS 2000 Community Service Area

GEMISIS 2000 is working in collaboration with the City of Salford to research and examine, as well as implement, the use of technologies to promote economic regeneration. The main activity is focused on the development of a 'Community Campus', linking key sites across the community via technology : the Local secondary school, the Library, the Health Centre and a Learning Centre (the Information Society Development Unit).

This effort seeks to enhance the opportunities available to citizens of the community, to avoid their exclusion from the 'Information Generation' by offering a range of opportunities to access, train and re-train in the use of technology. Many applications have been developed like a formal and informal facility providing access and training in the use of new technologies and the Internet.

1.2.1.3 GEMISIS 2000 Education Service Area

The recent growth of interest in the Internet and the services it provides, has affected teachers and managers in schools and they have begun to appreciate its potential as a medium for supporting and enhancing teaching and learning. GEMISIS 2000 is working with representatives from Higher Education, Further Education colleges and schools to develop the GEMISIS 2000 Education Intranet, capable of delivering applications and services to users. These services and applications will include:

- multimedia curriculum support materials,
- fast access to a wide range of previously identified educational 'hot sites' from the Internet, opportunities for teachers to pool and share their own course materials,
- an information forum for Further Education colleges to access and share information,
- notification of local and national events.

1.2.1.4 GEMISIS 2000 Health Service Area

GEMISIS 2000, directed by Professionals from the Primary and Secondary Health Care Sector is developing Health Care applications and services. These applications and services will be accessed via a GEMISIS 2000 broad band telecommunications network. The purpose of developing a Health Care Service Area is to determine whether information services and applications delivered via Informing Communications Technologies (ICT's) improve Citizens' quality of life. The Service Area will also endeavour through promotional work act as a positive influence on life style choices in Salford and Greater Manchester.

1.2.2 THE SOCIAL CO-OPERATION MODEL

The model being piloted by the Gemisis 2000 project is one of economic social co-operation, where the information technology revolution is being applied to all sectors of the socio-economic community

to the benefit of all. This is intended to create an environment where innovation and thus growth is internally driven and will ultimately be sustainable.

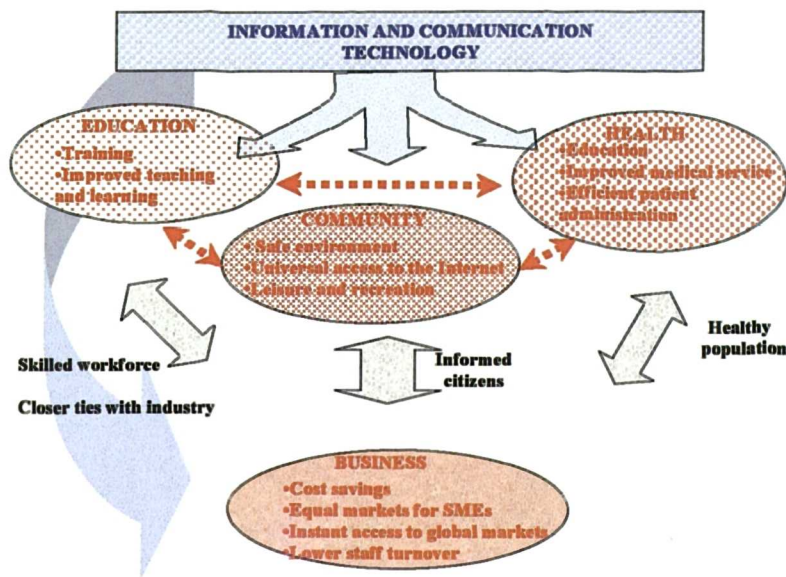


Figure 2. The Social Co-operation Model of Business in the 21st Century

Both private and public sectors have already recognised the importance of technology not only for direct commercial benefit but also for social regeneration and advancement. The public sector is driving the development of technology for the benefit of all while the private sector is focusing on the direct exploitation of that technology for economic benefit. This co-operation will lead to an environment, which directly promotes social advancement and well being, as well as economic growth and prosperity.

The GEMISIS 2000 project will create a milieu which not only exploits Information and Communication technology, but one which will encourage more innovation. Gemisis 2000 is set up in order to evaluate the implementation of the new technological applications in four core sectors, as a future model of economic and business growth of 21st century.

Within this context, GEMISIS 2000 will evaluate the impact of the new technology on business, community, education and health. The implementation of IT is translated in a number of different outcomes for the benefit of the community.

1. **Business** - Fundamental to the GEMISIS 2000 project is its unique partnership between private and public organisations in order to offer the opportunity to SME'S which have less resources to compete with large rivals. The Virtual Chamber (TVC) will try to offer business services using information technology.
2. **Community** - will address issues such as inner city safety with the use of CCTV which will lead to reduction of the crime rate, urban enjoyment and leisure. The use of interactive multimedia for heritage interpretation⁴ and providing Internet access to all members of the community. This will raise awareness and increase knowledge of both the new technology and their environment.

⁴ It is project concerning the use of interactive multi media in the museums and libraries for educational purposes

3. **Education** – The GEMISIS 2000 network offers connectivity between secondary schools, colleges and institutions of higher education and the University of Salford which has led to an improvement in learning and teaching by providing access to a wider database of resources. There is also the opportunity for more access and closer ties to the industrial world, where businesses and industries can mentor projects, offering real-life experience and knowledge as well as vocational guidance.
4. **Health** - Projects under the health service area will offer a better quality of life using information technology. More specifically they will develop and evaluate education packages aimed at patients and the general public on health issues like heart disorders, which will aid disease prevention. Another project is the development of real-time medical responses to patients improving medical services, waiting lists and administration costs.

Although the Gemisis 2000 project is based on four separate sectors, there are no real distinctions between the service areas, but in fact they overlap and interact to provide an environment of co-operation and mutual co-existence. This milieu is created by the fact that individuals working in each of the sectors have a grounding in IT. Members of the sectors are no longer limited to their profession or area of expertise, but are having to become part of a working team which is multi-skilled and multi-tasking. Information has not only had a direct impact on business and working patterns, but also social interaction. For example, the members of the education service are not only teachers or educationalists, but also people from business and IT backgrounds who have an awareness of and ties with other socio-economic sectors. Within the working teams, all members have similar objectives in developing the technological infrastructure, but different ways of ultimately using that technology. This enables them to co-operate together, by communicating their own needs and requirements, while understanding the needs and requirements of other sector members. The practice has shown that although a project belongs to one service area, it cannot exist alone, but requires and achieves interaction with the other service areas in order to meet its objectives. This co-operation will drive the implementation and use of technology in all sectors of the community and is the basis of the social co-operation model described in figure 2.

We have here broadly discussed the main projects being evaluated. But the potential for further use of IT is vast. The improvement across these three sectors will lead a more informed, healthy, educated and skilled population. This will impact directly on business by providing a more productive and creative workforce. A healthy and safe environment will not only directly affect the social community but will provide the impetus for setting up new businesses and regenerating existing ones. Thus the business community is not isolated, but is an integral part of the social community, where mutual co-operation will develop closer ties and a sense of ownership and mutual responsibility. The future economic growth will not only be based on the business development but also on the enhancement of an individual's life using information technology.

1.3 Conclusions

The Gemisis 2000 Project is a testbed for the use of innovation and technology in developing the socio-economic fabric of the future. All elements of a modern society impact directly or indirectly on an economy. As such the GEMISIS 2000 project is a collaboration between the public and private sectors to develop the business model of the 21st Century. Information Technology has been the catalyst which facilitates this collaborative co-operation. By providing the funding, both the private and public sectors can promote the use of information and communication technology, to enhance and improve skills; education and knowledge; health and a more secure environment which not only directly benefits the local community but ultimately impacts on the business community to generate local development growth and prosperity.

REFERENCES

¹ Smith A. *Wealth of Nations* (1776)

² Kondratieff N., (1935) *Long Waves in Economic Life* . *Review of Economic Statistics* Vol.17.

³ Schumpeter , J. (1939) *Business Cycles: A Theoretical, Historical and Statistical account of the Capitalist Process* . MacGraw Hill (New York)

⁴ Mensch, G. (1979). *Stalemate in Technology*. Ballinger Publishing Co.

⁵ Dassbach, C.H.A (1998) *Entrepreneurial Motivation and the Clustering of Innovations: A Reconsideration of Schumpeter's Theory of Kondratieff Cycles*

⁶ Hart J.A. *Rival Capitalists* Cornell University Press 1993.

⁷ Zysman, *Governments, Markets and Growth*. Cornell University Press 1990.

⁸ Cox The State, Finance and Industry: *A Comparative Analysis of Post-War Trends in Six Advanced Industrial Economies* (1986)

⁹ Landes, D.S. , *Wealth and Poverty of Nations*

¹⁰ Camagni,R. (1992) *The Concept of Innovative Milieu and its Relevance for Public Policies in European Lagging Regions*. Paper presented at the 4th World Congress of the Regional Science Association, Palma de Mallorca 26-29 May 1992.

¹¹ Jaskari H, *A Strategic Approach on Local Development – Finnish Local Technology Policy in Transition* (<http://www.uta.fi/aitokset/alue/netpubli/nepu196>) Originally published in: Oulasvirta, Lasse (ed.). (1995). *Finnish Local Government in Transition*. Finnish Local Government Studies. Vol. 22. N:o 4.

¹² <http://www.gemisis.co.uk/services>

Appendix Two - History of EU Framework Funding for IT

The European Union (EU) have had a strategy of funding to support the development of new technology and its use by business throughout the EU. The types of research projects and time periods are summarised in the following table.

	Time Span of Funded Projects	Description of Project Criteria and Aims
First Framework	(1984-1987)	Grouping of research activities.
Second Framework	(1987-1991)	Develop the technology of the future IT, Electronics, materials, industrial technologies.
Third Framework	(1990 – 1994)	Developing and disseminating research findings.
Fourth Framework	(1994 – 1998)	Promoting co-operation with and between different projects, countries and international organisations. Stimulation of training and mobility of researchers. Technology stimulation measures for SMEs.
Fifth Framework	(1998 – 2002)	Creating a user-friendly information society. Promoting competitive and sustainable growth. International co-operation promotion of innovation and encouragement of SMEs. Confirming of international role of community research.

Source: www.eu.org/funding.html (6/98)

Appendix 3 Definition of ERDF Objective Areas

Throughout the 1994-1999 programming period, the European Regional Development Fund (ERDF) concentrates assistance on 4 priority Objectives corresponding to 4 kinds of regions.

They are:

- Objective 1: promoting the development and structural adjustment of regions whose development is lagging behind.
- Objective 2: converting the regions or parts of regions seriously affected by industrial decline.
- Objective 5b: facilitating the development *and structural adjustment of rural areas*.
- Objective 6: development and structural adjustment of regions with an extremely low population density.

Regional eligibility is established by the European Council or the European Commission in partnership with the Member States.

For Objective 2, there are three key eligibility criteria for areas smaller than or equal to NUTS level III:

- an unemployment rate above the Community average,
- a percentage share of industrial employment higher than the Community average,
- a decline in this employment category.

Secondary criteria allow the extension to include areas adjacent to Objective 1 or 2 areas, smaller areas meeting the main criteria, as well as other areas, in particular in urban districts, which are facing the threat of severe worsening of unemployment, problems related to the regeneration of derelict industrial sites and the impact of the restructuring of the fisheries sector.

The European Commission decided the list of Objective 2 eligible areas in 1994. Areas from three new Member States (Austria, Finland and Sweden) were added in 1995.

Member State	Million inhabitants	% of national population
Belgium	1,40	14,0
Denmark	0,44	8,8
Germany	7,00	8,8
Spain	7,90	20,3
France	14,60	25,9
Italy	6,30	10,8
Luxembourg	0,13	34,2
Netherlands	2,60	17,3
United Kingdom	17,70	31,0
Austria	0,637	8,2
Finland	0,787	15,5
Sweden	0,965	11,0
Total EU	60,459	16,4

Source : www.inforegio.org/wbpro

Objective 2 populations 1994-1996 (1995-1996 for Austria, Finland and Sweden)

In the North West area, these areas are defined

Objective 1 Objective 2

Merseyside

Greater Manchester - Only

- Bolton and Bury TTWA (part)
- Manchester TTWA (the whole of the TTWA in the county except Stockport District bar 2 wards [Brinnington and South Reddish] and Trafford District bar 4 wards [Davyhulme East, Clifford, Park and Talbot])
- Oldham TTWA
- Rochdale TTWA (part)
- Wigan and St. Helens TTWA (part)

Lancashire - Only

- Accrington & Rossendale TTWA
- Blackburn TTWA
- Bolton and Bury TTWA (part)
- Burnley TTWA (except Sabden ward)
- Liverpool TTWA (part i.e. the wards of Birch Green, Digmaor, Moorside, Skelmersdale North, Skelmersdale South and Tanhouse in West Lancashire District)
- Pendle TTWA (the whole of the TTWA except the wards of Boulsworth, Coates, Foulridge and Pendleside all in Pendle District)
- Rochdale TTWA (part)
- Wigan and St. Helens TTWA (part i.e. the wards of Upholland North and Upholland South in West Lancashire District)

Cheshire - Only

- Liverpool TTWA (part)
- Widnes & Runcorn TTWA
- Wirral & Chester (part i.e. Ellesmere Port and Neston District)

Objective 5b

Lancashire

Lancaster District - Only the wards:

- Arkholme
- Caton
- Elle (Over Wyresdale parish)
- Halton with Aughton
- Hornby
- Kellet
- Ribble Valley (Ribchester parish)

Pendle District - Only the wards:







- Foulridge
- Pendleside

Ribble Valley - Only the wards:

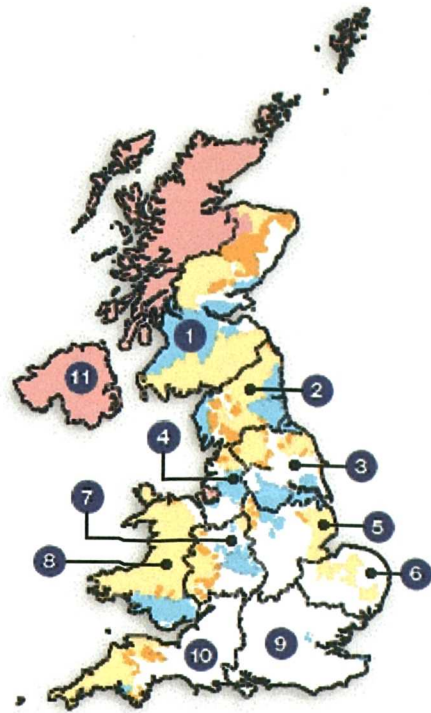
- Aighton, Bailey, Chaigley
- Bolton by Bowland
- Bowland Newton and Slaidburn
- Chatburn
- Chipping
- Gisburn Rimmington
- Grindleton and West Bradford
- Waddington
- Wiswell and Pendleton

Wyre District - Only the wards:

- Brock
- Calder
- Duchy (Cabus parish)
- Wyresdale (Nether Wyresdale parish)

1	
2	
2p.	
5b	
5b p.	
6	

p. = PARTIALLY ELIGIBLE



- 1 [Scotland]
- 2 [North]
- 3 [Yorkshire and Humberside]
- 4 [North West]
- 5 [East Midlands]
- 6 [East Anglia]
- 7 [West Midlands]
- 8 [Wales]
- 9 [South East]
- 10 [South West]
- 11 [Northern Ireland]

The source of this information is from the web site www.inforegio.org/wbpro viewed on June 1998.

Appendix 4 - Firewalls

One of the oldest and simplest lines of defence in any system is the use of firewalls. There are 2 main types of firewall; network level and application level firewalls. The most basic level is the packet filter, which works at the network level. It can also be the most cost effective, because it comprises an edge router, one of the most basic building blocks of the network. This can be configured to accept or deny certain types of communications. Information is presented to the router in units of data called packets. Each packet starts with information about its source and intended destination. A packet filter simply accepts or denies the traffic depending on how it has been configured. However, this is not too complex and can easily be spoofed by an experienced hacker who can disguise the true source of the destination packet. Other disadvantages are that it is difficult and time consuming to set up filter tables and some features such as FTP and DNS, do not run effectively since they require an incoming call from an unknown host which is blocked by the filter. Also mobile users cannot be supported since random port numbers cannot be listed on the filter tables.

This can be made more sophisticated by routing traffic to a bastion host, a server within the network that is armed with all sorts of software security devices. The bastion host can also be used in Intranets to prevent unauthorised network users accessing sensitive internal data.

The firewall at the application level consists of proxy servers placed between the edge of the network and the Internet and act like a quarantine. Information is stored and collected from the other side, rather than pass through the firewall. The advantage here is that the addresses of the nodes inside the network can be masked making it more difficult for hackers to spoof themselves inside the network. Sophisticated logging and auditing of traffic can be conducted which adds more security. Application firewalls can also be used to segregate sensitive areas of the Intranet to prevent one department from accessing the other's data.

State watching firewalls have also emerged as another method for restricting unauthorised access to the network. This is based on analysing patterns of traffic passing through the gateway. These are similar to the network level firewall, but with the additional step of associating computer operating system ports with the connections. When a connection closes, the firewall blocks access to the closed port until they are opened in an approved manner. This added check could stop a hacker from capturing a port.

While firewalls provide a level of protection, they cannot secure against security breaches from within. For instance, viruses from infected floppy disks or maintaining password confidentiality. No firewall can ever protect against trusted users abusing their network access privileges or even unwittingly passing them on.

Appendix 5 - EDI over the Internet

EDI - A Definition

EDI (Electronic Data Interchange) is a standard format for exchanging business data. The standard is ANSI X12 developed by the Data Interchange Standards Association. ANSI X12 is closely co-ordinated with or is being merged with an international standard, EDIFACT. An EDI message contains a string of *data elements*, each of which represents a singular fact, such as a price, product model number, and so forth, separated by delimiters. The entire string is called a *data segment*. One or more data segments framed by a header and trailer form a *transaction set*, which is the EDI unit of transmission (equivalent to a *message*). A transaction set often consists of what would usually be contained in a typical business document or form. The parties who exchange EDI transmissions are referred to as *trading partners*. EDI messages can be encrypted and decrypted. EDI is one form of e-commerce, which also includes e-mail and fax.

EDI and the Internet

Very little quantitative research about companies in the UK using EDI has been done recently, although in 1994 it was estimated that around 10,000 UK companies use EDI and the number is thought to be growing at a rate of 20-30% per annum¹. The UK is one of the more advanced markets in Europe in terms of EDI adoption partly due to sponsorship by the DTI in the late 1980's. Much of the research has looked to the US as the leaders in technology implementation for business, and the trend is for the US to implement new systems and the UK and Europe to follow. This has been the case for both EDI and the Internet.

In the past, the majority of EDI transactions have been carried out over private and secure VAN's. However, with the ever-increasing pressure for businesses to cut costs further, many innovative companies, which use EDI, are looking to exploit the advantages of the Internet to make further savings. In the US by September 1995, it was known that over

45 organisations were using the Internet to exchange production EDI data². These organisations include:

- Duke Power Company - the sixth largest investor-owned electric utility in the US
- Banc One - a leading US bank will receive remittance advice's and payment orders from libraries via the Internet
- National Semi-conductor Corporation is using it for transmitting EDI invoices to its customers
- 12 educational institutes are piloting EDI over the Internet and 52 more are in the planning stages
- The Federal Government of the US is in the process of implementing EDI over the Internet for its procurement programme.
- The Wright Patterson Airforce Base and Veterans Administration Medical Centre in California are procuring supplies from 2,500 vendors using EDI over the Internet.

All the organisations named have encountered no real problems with EDI over the Internet and the majority have been "very satisfied with the reliability of the Internet". All have cited cost savings as the driving force for using EDI over the Internet.

The Advantages of EDI over the Internet

The benefits of the Internet over VAN's for use of EDI are listed below:

Internet	VAN
1. Cheaper and less complicated pricing than VAN's - It is estimated that between 60-80% cost savings are made	
<ul style="list-style-type: none"> Price is based on an annual membership fee with an Internet Service Provider (currently £80 including VAT). The only other cost is the cost of each connection to the Internet which is the unit price of a local telephone call (even if the connection is International) 	<ul style="list-style-type: none"> Price is based on the number of characters and the number of transactions and inter-connect fees
2. End-to-End EDI	
<ul style="list-style-type: none"> The message is sent by the one trading partner and received by the other trading partner even if different Internet Service Providers (ISP's) are used 	<ul style="list-style-type: none"> The message is handled by the VAN service provider
3. High speed network access	
<ul style="list-style-type: none"> Most ISP's offer T1 connections (1.54mbps) and some offer T3 connections (45mbps) this is improving all the time. Messages are typically delivered within seconds or minutes even when different ISP's are used. 	<ul style="list-style-type: none"> VAN's do not offer this speed of access it is usually 56kbps
4. Interconnections between ISP's are transparent.	
<ul style="list-style-type: none"> Sending a message to a partner of a different ISP is just as easy as sending a message to one who is on the same. 	<ul style="list-style-type: none"> Exchanging messages with a partner on a different VAN, involves the process of gaining an agreement between the 2 VANS where tables must first be updated
5. The range of applications offered is wider	
<ul style="list-style-type: none"> The Internet supports a wide range of applications including e-mail, remote login, file transfer, World Wide Web, bulletin boards etc. 	<ul style="list-style-type: none"> VANs support only EDI related services
6. Connectivity to millions of businesses worldwide	
<ul style="list-style-type: none"> The Internet has global connectivity On-line global market-place 24hours with millions direct access to millions of customers and suppliers 	<ul style="list-style-type: none"> VANs have a limited connectivity - usually one dominant trading partner insists that the other partner joins
7. Reliability	
<p>It is reliable because it is standards based. Internet Protocol (IP) supports adaptive packet routing, where if it fails, packets are automatically re-routed.</p>	<p>It is reliable, with services including audit trails, status reports, translation consulting etc.</p>
8. Interchangeability of Service Providers	
<ul style="list-style-type: none"> It is easy and inexpensive to change ISP's 	<ul style="list-style-type: none"> It is not easy to change service providers

The Technology

Initially, the main question is how can EDI be sent over the Internet. There are two Internet applications being used for EDI - FTP (File Transfer Protocol) and E-mail. The advantages and disadvantages of each are summarised below:

	Advantages	Disadvantages
FTP	<ul style="list-style-type: none"> • Able to handle large transaction set (>100MB) • Easy to use - drag and drop facilities 	<ul style="list-style-type: none"> • Requires login ID and password for each trading partner • The two trading partners must agree on directory names and file names before EDI data can be exchanged • Requires much administration and does not scale well with a large number of partners • Added insecurity of sending passwords and login ID's over the Internet • The sender and receiver have access to the directories and files on each other's machines
E-Mail	<ul style="list-style-type: none"> • Provides store and forward features - queuing data and retrying deliver • More secure does not require login and passwords and does not give access to recipient's files/directories • Easier to administer • Very fast as often the sender's server communicates directly with the receiver's server • Easy to use, simply attach the EDI message to the e-mail message • Software is available to handle EDI transactions via e-mail* 	<ul style="list-style-type: none"> • May not be able to handle large files

Thus, realistically for the majority of EDI, Internet e-mail would be a better choice than FTP since it is more secure and requires less administration.

Internet Security Issues.

One of the major concerns many organisations have about EDI over the Internet is security. There are two types of security which must be taken into account namely Transaction security and Host security.

*Premenos California.

Issues regarding security of the Hosts connected to the Internet are more common and protective measures are :

- To use dial connection instead of dedicated connection - this would be particularly relevant to the smaller companies
- For dedicated users of the Internet installation of protective firewalls and proxy servers - this would be relevant to large and other multi-national organisations.
- Establish and enforce proper security guidelines and policies for example, not sending passwords in “the clear” over the Internet.

Transaction Security - this would be particularly relevant to the transfer of messages over the Internet. Some of the security problems include :

- modification of information in transit
- unauthorised access to the mailbox at the ISP run mailbox
- Repudiation of receipt

Some of the measures which can be implemented to protect transactions are:

- Encryption
- Digital Signatures
- Trusted Third Parties

These measures would protect the integrity of messages, verify the origin, protect against repudiation of the message and the origin and also provide confidentiality.

Internet EDI Security Issues

Focusing specifically on fears of lack of security for EDI over the Internet, we will compare the services offered by VANs and analyse whether these are also available by using the Internet.

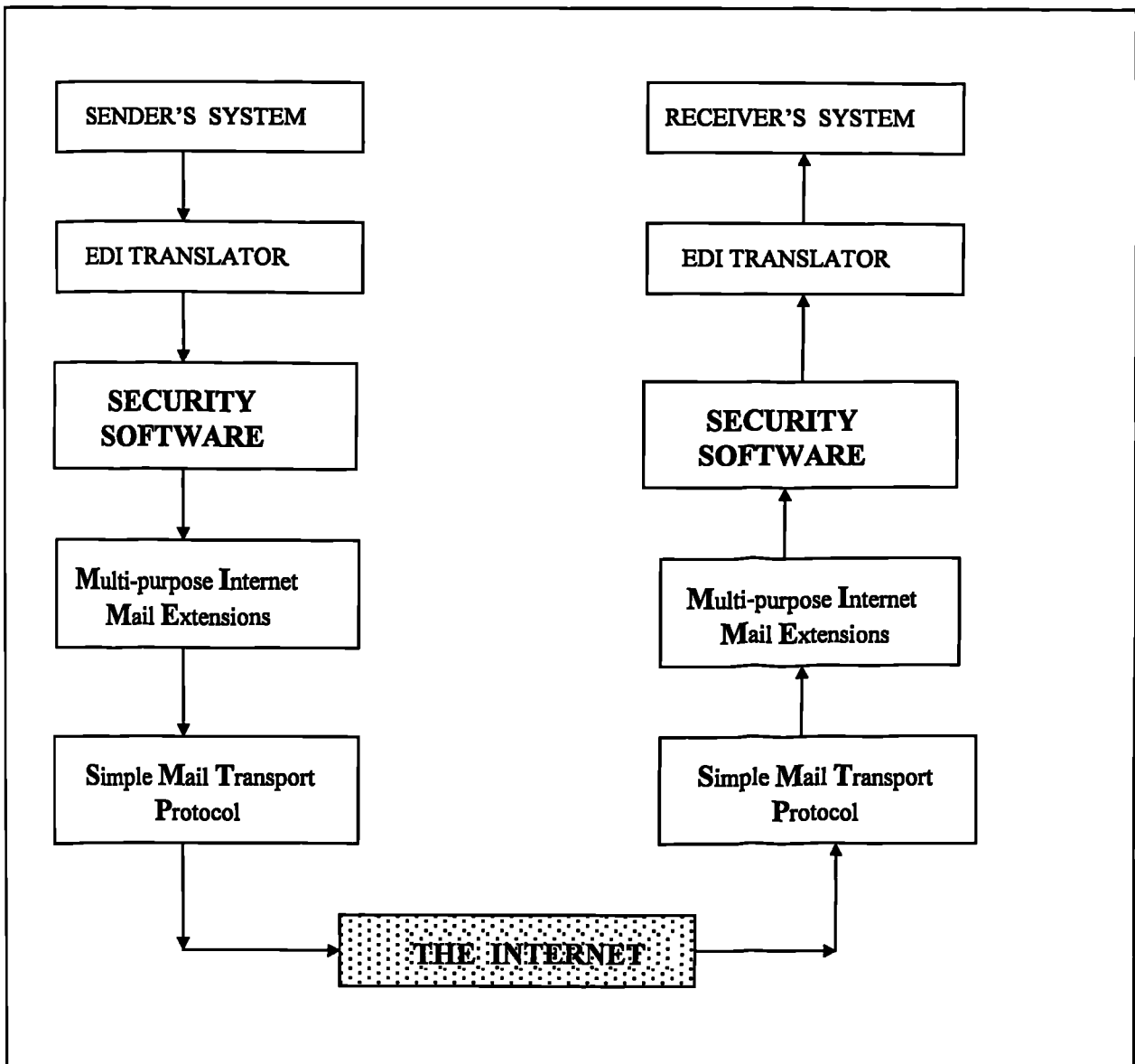
VAN providers offer the following EDI services as standard:

- Audit Trails
- Status Reports
- X12 Compliance Checking
- Translation Services

Which leads to the following questions to be raised with regards to EDI over the Internet:

1. How do I know who sent it (Authentication)
2. Did it arrive exactly as sent (Integrity)
3. Can the sender deny sending it (Non-Repudiation)
4. Can the receiver deny having receive it (Non-Repudiation)
5. Can anyone else read it (Confidentiality)
6. How can the message be tracked i.e. an audit trail be created

The pilot study we are proposing can deal with the above issues. The diagram illustrates the processes involved in sending EDI over the Internet via e-mail.



SMTP moves e-mail messages from the sender to the receiver's system. It supports only text and cannot handle attachments. It supports negative delivery notifications but not positive delivery notification, thus the necessity of MIME.

MIME is the set of extensions to the Internet e-mail that provides support for non text data and multiple body parts. MIME object is carried within an SMTP message - where MIME object would contain the EDI data. This data can be encoded as printable text to preserve integrity of data as it passes through SMTP systems. The sender's MIME software encodes the non-text data and the receiver's MIME software decodes it into its

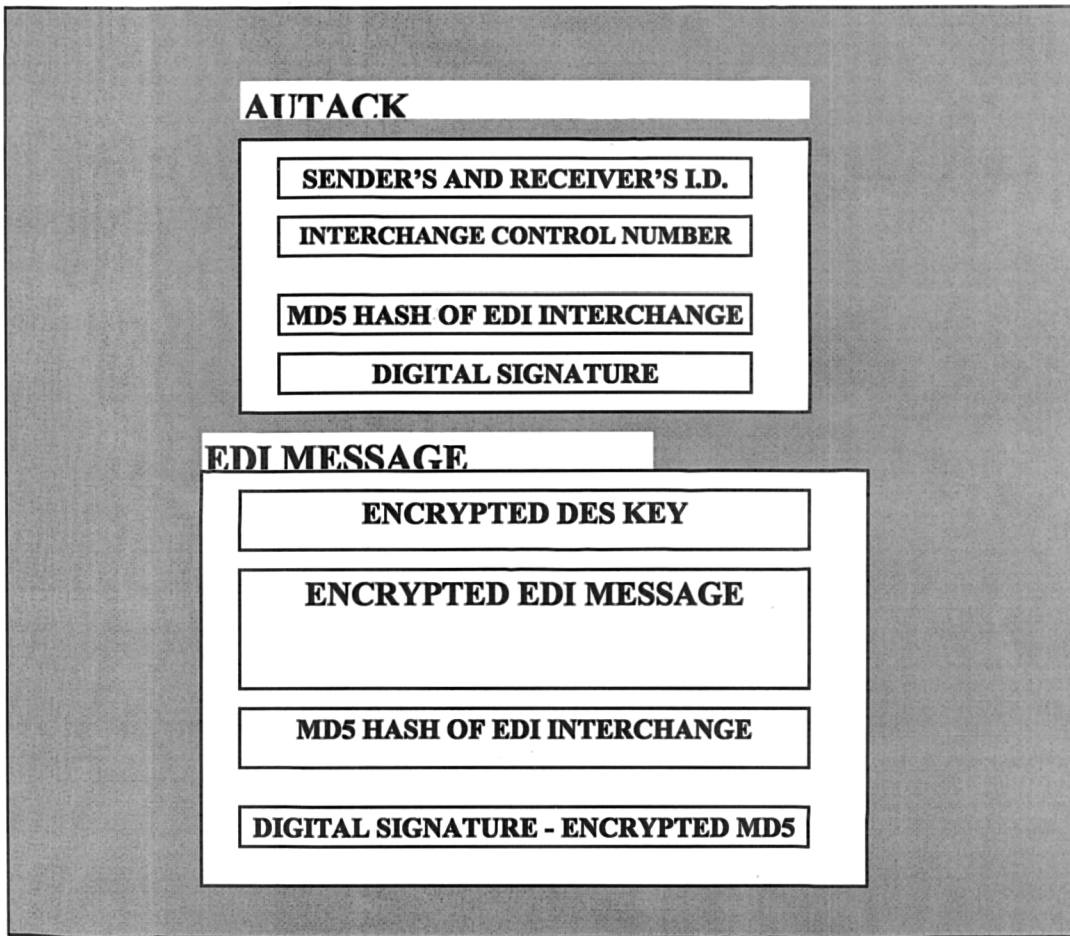
original form. The EDI interchange is placed within a MIME body part. The MIME object specifies the content type for each body part. Content types have been defined for X12, EDIFACT and data in mutually agreed upon formats.

To deal with the issues the following will be installed:

- **Authentication** - a digital signature where only the recipient with their own private digital key (created by an algorithm of at least 512 bits preferably 1024 bits) can have uniquely made the signature.
- **Integrity** - a one way hash algorithm at least 128 bits - the hash value of the EDI message is calculated and sent with the EDI interchange. The recipient calculates the hash value of the message received using the same algorithms. If they are identical this proves the message has not been changed in transit.
- **Non-Repudiation** -
 - by sender - through the digital signature
 - by recipient - AUTACK (Authenticated Acknowledgment) sends
 - acknowledgment of receipt of the message.
- **Confidentiality** - The use of encryption algorithms triple DES of 128 bit length
- **An Audit Trail** - there is in fact the Network trace programme "Trace Route"
 - this traces the route traversed by a packet from source to destination.

So in order to incorporate all the measures to ensure the EDI message is delivered and received securely, the structure of the message is illustrated below:

MIME ENVELOPE



In Summary

The greatest benefits of EDI over the Internet are :

- Adoption of common standards and proven inter-operability of systems
- Adoption and deployment of a distributed directory service capability
- Ubiquitous network coverage from many service providers
- Layering of applications over existing application
- A standards process which all vendors have equal access to
- Widely available public domain software.

REFERENCES

- ¹ Cox and Ghoneim Drivers & Barriers to Adopting EDI, Imperial College ,London., 1994.
² Lyons, R., EDI over the Internet E-Comm September/October 1995.

Appendix 6 - SME Perception of the Internet - A Regional Study

This paper was presented for publication in 1998 and was unsuccessful. It was presented again in December 1999. It is still being considered.

The telephone survey carried out in 1996/7 is described in detail in this paper, the details of the focus groups are also included in this paper.

SME PERCEPTION OF THE INTERNET

A REGIONAL STUDY

R.Tassabehji

Abstract

Much has been written about the benefits and pitfalls of the Internet to businesses, namely that it :

- is a cost effective low risk way of marketing and freeing employees from tasks of drudgery
- can give an edge over competitors who lack the foresight or curiosity to use the Internet
- is a great leveller, where large and small organisations can compete equally
- offers all businesses a global market for their goods and services
- is potentially a means of gaining long-term competitive advantage when integrated into the growth and development strategy of a business .

This paper concentrates on the small and medium sized enterprises (SMEs) in the Greater Manchester region. It describes the research undertaken to assess the usage patterns of the Internet in these SMEs. The results suggests that information about the Internet and its business benefits is not reaching SME's mainly because it is not presented in a way which encourages understanding and thus implementation . This is extremely disadvantageous both to SMEs directly and to the future economic growth and competitiveness of a nation indirectly. The paper addresses these issues by proposing a practical framework, which is palatable to SME's both before and after implementation, by which the IT industry and other interested bodies can encourage SMEs to adopt Internet technology.

Introduction.

The first section of this paper, will outline the general ideas and thinking published in commercial and academic journals, on the use of the Internet in business . The second section will describe the research undertaken and the results collated by the author. The third section will discuss the results as they impact on SMEs and the growth and development of the economy. The final section will present a framework by which the IT industry and other interested bodies can encourage SMEs to make the best use of the Internet.

Current Thinking and Ideas on the Internet.

Much has been written about the Internet and its potential benefits and problems to businesses . Overall, the attitude towards the Internet is positive, more so in the US than the UK. This is mainly because the UK and the rest of Western Europe lags behind the US in the physical proliferation of computers and in the prevalent IT culture. The European average per capita IT spend is \$276 compared to \$542 in the US. The European average number of PCs per white collar worker is 76 per 100 compared to 104 per 100 in the US [Information Strategy 1997]. There is also a negative portrayal of the Internet in the UK media, where the popular press has tended to concentrate on the seamier side of the Internet - for example the ease of finding and downloading pornographic material.

Among the papers that have been written, many see businesses currently using the Internet, largely as a marketing tool [Hagel and Armstrong, 1996]. The Internet is the great leveller, "where nobody knows how big or small you are" [Dellacave, 1996]. Once a company is on the Internet it becomes a multi-national organisation with access to global markets and direct contact with customers world-wide. Early involvement in the Internet is seen as a low cost, low risk strategy that can give many organisations an edge over their competitors who lack the foresight or curiosity to use the Internet to their advantage. "It is not too difficult for smaller businesses to outperform larger ones" [Dellacave, 1996]. When recession hits, the added advantage will be that the technologically enabled will have

processes in place which will make them more efficient and thus able to ride out any recessionary storm without too much financial outlay to the organisation [Traynor Kitching & Associates, 1996]

Other advantages of the Internet are that it provides global reach, and allows head-to-head competition with larger firms. By removing barriers to communication with customers and employees, namely by removing the obstacles of time zones, geography and location, it creates a “frictionless business environment” [Quelsch & Klein, 1996]. Thus, value is gained as the Internet provides the means for people to interact with each other instantaneously and at their convenience [Hagel & Armstrong, 1996].

The current expansion of the Internet is being driven by marketing initiatives, mainly because of the potential problems with the Internet when used for business, which include :

- the type of information presented electronically is limited by bandwidth
- regulations for example those governing export controls, and country specific industry standards
- legal issues such as copyright laws, recognition in law of electronic contracts
- security concerns

Spar & Bussgang [1996] also stress that until the Internet’s lack of rules are dealt with, then growth and development of the Internet for business communications and transactions will be limited. There is already developing an emerging and distinctive demographic profile of current users who are more likely to buy goods under \$50 over the Internet. These buying patterns might become more difficult to change once they are established over time. For organisations to realistically embrace the Internet as an integrated business tool the following requirements must be met :

- a clear definition of property rights
- safe and useful means of exchange
- an internationally agreed practice for locating and punishing violators of on-line rules

Not only this, but also human resource issues linked with the Internet will have to be resolved [Sunoo, 1996], for example by :

- establishing fair guidelines of responsibility for additional training and time taken to use the Internet between employees and employers
- finding new ways of measuring work processes.
- setting up policies and procedures for outlining terms and definitions to prevent lawsuits due to actions by employees (for example downloading illegal material, or sexual harassment by e-mail)

For many industries, technology is becoming inextricably linked into elements of the value chain [Hornbach, 1996], competitive strategy [Karimi et al, 1996] and a means of developing longer term competitive advantage [Ross et al., 1996]. Ross et al. [1996] maintain that in order to develop long term competitiveness by using IT, then the organisation must have:

- a strong IT staff
- a re-usable technology base where technology platforms and databases are integrated and company compatible
- partnership between IT and business management where management have an understanding of both IT and business issues.

In a survey of 214 businesses Karimi et al [1996] found that a direct relationship exists between companies which are increasingly becoming technologically based and are willing to increase IT investment, and a company’s current level of IT maturity and size. Thus, the more willing a company is to increase IT investment, the more likely it is to be larger and to have a mature IT infrastructure and thus a competitive advantage which is sustainable in the long run. In fact in a survey of the top 100 European IT Investors in Europe [Information Strategy 1997] - Reuters, Barclays Bank, ING NV, Phillips NV, Zurich Insurance, Siemens, were in the top 10 list. These same companies are also among the leading players in their respective industries.

Despite the problems voiced, the importance of technology in the future growth and development of business is clear. For many industries, the Internet is seen as a particularly important advance where the

low marginal cost nature of its products and services offers SME's the same opportunities as larger organisations. Keegan [1997] also sees the explosive growth of the Internet as a means of shifting the balance of economic power back from multi-national corporations to "everybody". He feels the Internet has a "socialist egalitarian quality" which enables all users to perform a myriad of tasks from browsing databases to downloading video clips and audio records at a very low and still falling cost. Keegan recognises the importance of the Internet suggesting that it is developing its own economy and is no longer an electronic island remote from the rest of the world. He cites Microsoft being forced by Netscape to give away free products, as an example of the way in which the economic environment of the 1990's is changing. Whereas it is common for everything to have a commercial rate, currently in the US consumers wanting the same product are contacting each other through the Internet to negotiate bulk discounts cutting out the middle man. This according to Keegan has changed the face of the economy of the future.

As we can see, most of the published material related to the Internet deals mainly with post-Internet-implementation issues. This implicitly suggests that there already exists a business community using the Internet. This research is intended to analyse the role of the Internet in SMEs, how it is being used and whether it is benefiting their businesses directly and the health of the economy indirectly. The study has concentrated on SMEs because of the importance of their impact on the economy. According to the Department of Trade and Industry [DTI, 1996] in the UK small companies with less than 100 employees provide over 50% of all the UK's non-government employment and contribute nearly 50% of output.

The Research

The research methods used in this study were two-fold and included :

- telephone interviews
- discussion (focus) groups

The aim of the telephone interviews was to get an indication of the SME uptake and usage of the Internet in a variety of industry sectors in the Greater Manchester area. For our purposes, SMEs are companies with less than 250 employees. The focus groups were a means of gaining a deeper understanding of SME attitudes to the Internet - both those who already had an Internet presence and those who had none.

Methodology

Telephone Survey

A sample of 145 small and medium sized businesses in the Greater Manchester/Salford area was selected from the Chamber of Commerce and local business listings . The companies were contacted by telephone and were asked to give information about :

- the business - a brief description of what the business does and their size in terms of employees and turnover
- the Internet - whether they were linked or not and if not why not
- if yes for what purpose was the Internet being used by the company.

The Sample

The sample was made up of 57 respondents from the service sector, including:

- travel agencies
- employment and training agencies
- transport and road freight
- consultancy including IT
- the professions (accountancy, law)

Fifty four respondents were from the manufacturing sector comprising :

- electronics and engineering
- software development (for this purpose it is considered to be manufacturing a product - software)
- textiles
- chemicals
- machinery manufacturing industries.

There were also 8 companies in wholesaling and retailing of goods herein defined as the trading sector. Of the sample, there were 26 no responses.

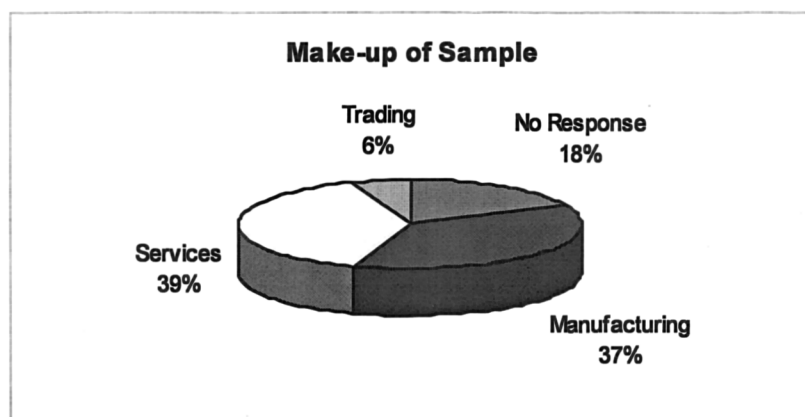


Figure 1. Make up of the Telephone Survey Sample

The following table shows the breakdown of the sample in terms of company size. Seventy five percent of the total sample had less than 50 employees, with only 11% having between 50 and 100 employees and 14% having more than 100 employees.

Number of Employees	Manufacturing Sector	Services Sector	Trade	TOTAL	Percentage of Total Sample
<50	40	43	7	90	75%
50-100	5	8		13	11%
101-200	4	4		8	7%
>200	5	2	1	8	7%
Total	54	57	8	119	

Table 1. Breakdown of the Telephone Survey Sample by Company Size and Industry Sector

Focus Groups

Two groups of between 4-12 business non-users of the Internet and two groups of business users of the Internet were recruited from small and medium sized companies in the North West of England. A series of guideline questions were asked (A 1) in order to establish:

- an understanding of the types of business problems which SMEs experience, and whether they can realistically be solved by the Internet,
- attitudes and sources of information on technology
- their attitudes to the Internet, and where businesses feel the Internet will be 2-5 years from now.

Main Findings

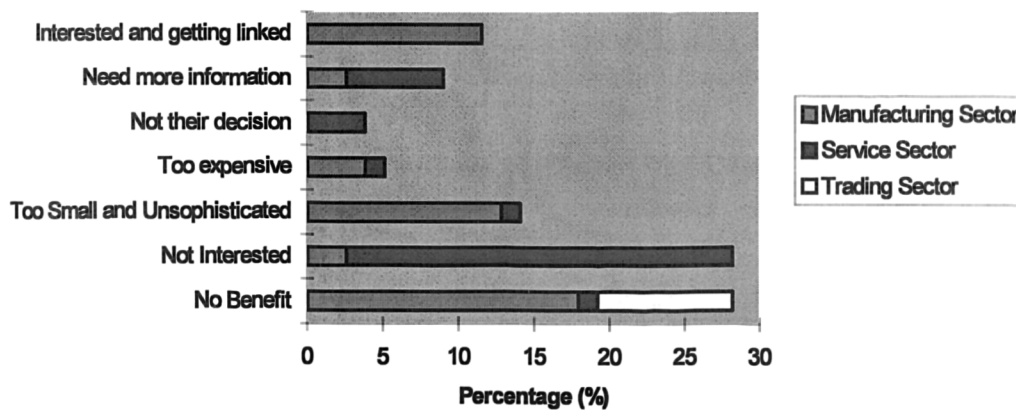
Telephone Survey (A2)

Although not exhaustive, this survey shows a trend of Internet usage by small and medium sized businesses. The take up of the Internet by English SME's is still only around one in three.

Companies which have more readily adopted the Internet are those in the service sectors particularly consultancy, training and recruitment, promotions and advertising agencies and transport companies. The financial service sector mainly accounting firms (excluding banking), seems particularly uninterested in the Internet. Of those in the manufacturing sector, the electronics, engineering and software development companies are the main areas of Internet take up. The more traditional manufacturing sectors such as textiles, chemicals, toys and machinery seem uninterested in the Internet and unaware of any benefits it could have to their businesses.

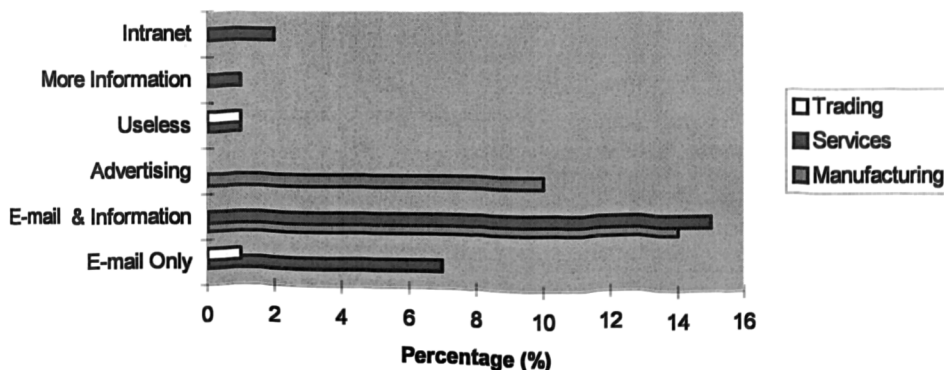
Of those that had not yet taken up the Internet, over 70% maintained that it had no benefit to their business, believing their companies to be "too unsophisticated", "not that type of company" or "not advanced enough" to be using the Internet.

Figure 2. Responses of Internet Non-Users



For the majority of Internet business users, the medium is used primarily for communication purposes. Of the Internet business users, all use it for e-mail; over 70% of users in the more service orientated sectors also use it for gathering information; while around 50% also use the Internet for advertising/marketing their company and products.

Figure 3. Responses From Internet Users



Having said this however, doubt was expressed by respondents about the benefit of advertising on the WWW. One respondent in the manufacturing sector, indicated that in one week only 4 people had browsed his company's site and of those, 3 were "anoraks" i.e. computer enthusiasts rather than potential customers. Another respondent believed the Internet to be "useless" and if he could, he would "remove it from every machine", except for e-mail which he thought was "wonderful".

The Focus Groups

In order to understand the nature of common businesses problems and whether these could realistically be addressed by technology, respondents were asked to specify the most common problems they encountered in every day working life. The most common problems indicated by respondents (A 3) were :

- cash flow - due to late payments and poor stock control
- marketing and sales - not reaching the right target customers, and the most effective advertising medium
- Training and technical support - or lack thereof, where technology in organisations is not felt to be used to its full potential mainly because of lack of training and inadequate technical support.

Attitudes towards technology give an indication of a company's willingness to adopt new technology to its benefit . While overall the participants in the focus groups were enthusiastic about technology and computers in general, and the Internet in particular, care must be taken since the groups were self selecting in that those who actually attended were already interested in Internet technology and enthusiastic about learning more to help their businesses. This does not nullify their opinions, which included the favourable and the unfavourable, but it does not mean that we cannot extrapolate from here to predict the opinions of all SME's.

Table 2. Opinions on the Technology

Favourable	Unfavourable
"Difficult to imagine running a business without computers" "You can see the benefits straight away even with word processing packages" It reduces the number of employees It frees up people to engage in money making tasks rather than in tedious time wasting administrative tasks Flexible working practices (having a laptop) Access to other people's files through networking "It's Great ... it's magic" "We can do double the work with computers"	For small companies if a computer goes down it is a problem Volatile IT industry with ever reducing product life cycles Businesses can make expensive mistakes by investing in obsolete systems Cheating IT salesmen who sell businesses hardware and software they don't need "they get away with murder" Inadequate training and not enough understanding of the technology "We don't know what questions to ask to get the right answers" Inadequate technical support

The majority of group members felt that they did not have adequate training and any attempts to get training or support from their existing Internet Service Providers and computer hardware/software providers were inadequate and not useful often discouraging them from using the Internet.

When asked about sources of information on technology, both users and non-users indicated that the main source of information was specialist IT magazines and TV and radio advertising. Other sources of information included trade fairs and computer shops - such as PC World and Dixons. Smaller computer shops were found to be more helpful as staff were prepared to spend more time with the customer answering questions and perhaps more surprisingly, were also found to be more competitive on price. Young people were also a good source of information as were software suppliers and maintenance engineers.

On the whole though, for the smaller and medium sized companies which did not have IT dedicated departments, it was a matter of learning by doing and finding out for themselves, which was often found to be stressful and frustrating. Many respondents contacted "help-lines" and were dissatisfied because of:

- having to wait at the end of the telephone for hours,
- inadequate explanations,

- never fully solving problems.

General attitudes about the Internet were largely positive. All the respondents could see the potential for the Internet . Given the education and training all felt that it would benefit their business by offering a faster, more efficient and effective way of communicating and transferring information than fax or post.

As an advertising tool, group members felt the Internet could act instead of or along side company brochures which would be particularly effective because of its multi-media, for example, having a demonstration video of products on-line. Some reservations were expressed over Internet advertising because respondents believed :

- it was globally accessible, the products a company advertised must conform to the respective country's laws and regulations
- there was a fear that the company would be smothered with demands for products which were not lucrative to the company
- of easy access, it would be time consuming dealing with both the relevant and irrelevant queries. In one case, a company had a web site with product information and was receiving e-mail for a product brochure. These requests were ignored by the company which felt annoyed at receiving time-wasting e-mail since the web site was considered to be the brochure.
- the potential customer would initially have to be in the Internet mind set to actually look for the site on the web.

The respondents were very positive about the effectiveness of the Internet as a means of communication. They felt that e-mail was "fast flexible, fantastic". Some comments on the Internet included:

Negatives	Positive
It sounds expensive It is very slow Used largely for recreational purposes Because it throws up thousands of entries for a query it is virtually useless It is a mess with no order or strategy. It is unstructured and so difficult to use. There is much ignorance about the Internet and how to use it "I'm lost when it comes to the Internet ... I don't know what you can get from it" "Nobody in our office knows how to use it" The information changes by the hour It is cheaper to use CD-ROM for useful information The Americans have priority over the Internet , " they can kick you off at any time" A fear of being "left behind" Competitors can find out if you have visited their web sites	Fast, flexible cost effective way of communicating It can be used for communication - e-mail is particularly useful It is crammed with wide ranging and diverse information It has huge potential Easy file transfer It is like having the office wherever you go The Internet is as reliable if not more so than any other piece of computer software You can deal with more than one person at a time at different locations around the world. It gives a high tech progressive image to the company It is very useful for advertising " we will be able to get in with bigger companies and expand the business"

Table 3. Opinions on the Internet

All the group members believed that the Internet is here to stay and is not merely a fad which would fizzle out in a few years time. Many compared the Internet to the fax - where initially nobody had fax and now all companies use fax and wouldn't know what to do without it.

An indication of the cross section of opinions is included in the following table :

In a year everybody will be using it like the fax I don't see people trusting computers to the extent that written records will be completely eradicated Businesses must look to get into the Internet so that they have a say in the way it develops The Internet must gain the simplicity of use of CEEFAX if it is to take off
--

To improve the Internet more people would have to use it as a source of information. "You can go from knowing nothing to being an expert on a topic by using a clippings agency.
 Service providers like AOL and CompuServe must address customer needs rather than saying here's the Internet
 It passes the test - if it was taken away tomorrow we would miss it
 The new generation is growing up with this technology and so are not frightened of it, they will move it forward
 The Internet will be used more often at home
 PC's will become dedicated to the Internet
 Realistically, it will be the home users who will drive Internet development

Table 4. Opinions on the Future of the Internet

With regards to security, an even larger awareness gap was found to exist. The majority of respondents were aware that the Internet was not a secure medium for financial transactions. One respondent felt that "the only secure computer is an unplugged one". When discussing e-mail security, few participants from both the telephone interviews and focus groups outside the IT industry were aware of potential security breaches. Of those who did use e-mail, they believed that nothing they were sending over the Internet was important enough to be protected by security measures. Some users when told of the potential security pitfalls of the Internet, felt that only when they had experienced a security problem, would measures be taken. Inexperienced users felt that security is not a priority, but rather that learning how to use the system to its full potential and "properly" is more important.

Discussion of Results

The results from both the focus groups and the telephone surveys, show that there is not much Internet uptake by SMEs (around 1 in 3). This is consistent with results of other published surveys, where figures for Internet up take by companies in the UK range from 30% to 55% [Surveys, 1996].

Attitudes towards technology and the Internet are again consistent with the other studies mentioned previously, which found that many companies felt technology is making work easier, increasing efficiency in sales and marketing tasks, and that for smaller non-technology oriented companies, there is little training and a sense that staff must "muddle along". This then seems to suggest that the results are representative of a larger population sample.

These findings show that far from being ready to discuss and tackle issues of post-Internet-implementation, SMEs in the Greater Manchester region are not yet at this stage and the majority of the literature as we have seen deals mainly with post-implementation issues and strategies.

If as suggested, the results here are found to be replicated in other regions of the UK and Europe this bodes ill for the region's economic growth and development. By applying Kondratieff's modified theory of global economic growth, which asserts that growth occurs in a series of long waves lasting around 50 years [Schumpeter 1934, Mensch 1979] we can see the importance of this current new wave of technology. According to Dicken (1994), the fifth Kondratieff cycle began in the 1980's-1990's and is associated with Information Technology. Freeman & Perez (1988) agree that the new techno-economic paradigm around which the next wave of global economic growth will cluster is also IT. Information Technology is here defined as the convergence of two initially distinct technologies around information:

- communications technology - which is concerned with the transmission of information e.g. satellites, fibre optic cables etc
- computer technology - which is concerned with the processing of information e.g. the development of chips, Artificial intelligence, etc.

Contemporary commentators identify this specifically as the information super-highway (although it should be noted that the US now stopped this term in favour of simply "The Internet").

"The new telecommunications technologies are the electronic highways of the information age. Communication technology is equivalent to the role played by railway systems in the process of industrialisation" [Henderson J and Castells M (eds) 1987]

But what we have found here in this research is what Porter [1994] identified, that while new technologies do act as a stimulus to strategic innovation which shifts competitive advantage,

“It is hard for firms steeped in an old technological paradigm to perceive the significance of a new one and it is often even harder for them to respond to the notion” [Porter 1994p.46]

It was found here, that SME non-adopters of the Internet are mainly concentrated in the traditional sectors of manufacturing such as textiles, chemicals, toys and machinery. These are the laggards and there is a serious danger that these firms will not survive. Because they are so steeped in the old technological paradigm, they cannot perceive the significance of the new technology. They are unable to understand that as the new technology filters down into the technologies of products and processes, the knowledge they have will become obsolete and unusable in the new techno-environment.

SME early adopters of the Internet were found to be in the higher tech industries. In the service sector these were in areas such as training and recruitment, advertising and promotion, and transport. These are areas in which the UK economy is relatively strong. Similarly, with manufacturing, firms in the electronics, software development and engineering sectors were also among the early adopters.

Porter [1994] also identifies that the geographic clustering of new technology stimulates competitive advantage. He cites the US and Japan as clear leaders with the East Asian Tiger economies (South Korea, Singapore, Hong Kong and Taiwan) as developing an increasingly strong competitive presence. Again this is being borne out in the figures for growth of the Information and Communications Technology markets.

Country	Growth in the Information and Technology Market from 1995-1996
The US	10%
Asian Tiger Countries	>13%
Europe	7.2%
Source: EITO 1997 Report Eurobit Frankfurt	

Table 5. Growth in International Information and Technology Markets

In fact, at the World Economic Forum February 1997 for charting the future of globalisation [Elliot, 1997], the President of Intel, Andy Grove, warned that Europe was lagging behind the US in the use of digital technology as an integrated part of their competitive business and country policies and is also forecast to fall behind the emerging markets in the use of PCs.

The European Commission is aware of these problems across Europe and warn that UK and European Businesses must keep pace to remain competitive. The Chair of the EICs Communications Group notes that [Abercrombie 1997]:

“Some companies ignore the benefits of IT because it is seen as too complicated to keep abreast of the latest developments, while others are gaining a tremendous amount of new business”

The European Commission is already developing a Fifth Framework programme which provides funding for research and development for small and medium sized enterprises(SMEs) to improve Europe’s international competitiveness and strengthen its scientific and technological base.

In a study of the leading 100 largest European IT investors over a third of IT directors taking part in the survey [Information Strategy 1997] complained of a lack of awareness of IT’s potential among top management. They feel that this lack of understanding and awareness remains a barrier to putting information strategies in place and as we have seen this is magnified manyfold in SMEs.

“The Internet and the Web are still being tested by most European companies. Too few have recognised their business potential ... but the potential to exploit information technology for competitive edge will only grow more intense”

The industry leaders such as Reuters, Barclays Bank, Philips and Siemens were maintaining their leading edge by turning their IT divisions into service companies providing services to their own company and also by selling spare capacity on the open market. Many have created fast response teams dedicated to exploring new business opportunities for IT.

Putting our research into this context is cause for concern and the UK government also seems to be aware of the importance of SMEs and new technologies to the economy. Ian Taylor [1997], Former Minister of Science and Technology at the ISI conference observed :

“We know there is more to do in order to make smaller UK companies aware of the practical benefits and competitive edge that information and communication technologies can provide”

Subsequent to this study, a report commissioned by the DTI “UK Businesses and IT” found that 79% of large UK companies consider IT to be essential to improving business competitiveness and that 60% believe their staff do not have sufficient understanding of IT to fully exploit its opportunities. 20% of large companies surveyed said they provide no IT training. More than 60% of SMEs felt their staff had a good understanding of IT although half (48%) offered no IT training. The report could not include any detail for explaining this anomaly. However, it could be that smaller companies have lower expectations of their staff in terms of IT knowledge than larger firms. *From our research findings it is more likely that the people judging them have no knowledge themselves and thus have no meaningful criteria to make an informed judgement.*

In line with the EC’s findings, a report published by the Institute of Public Policy [Lawder and Wastell 1997] recommends that firms should be encouraged to win new business via the Internet and e-mail by the government offering more on-line information . The report also recommends that the Government should encourage academic institutions to support electronic networking between businesses. The authors of this paper are currently involved in such a project [GEMISIS].

The results of this research and issues raised by leading commentators, reveal that there exists a large knowledge, training and technical support gap between SMEs and the IT industry. The main priorities for the majority of SME non-users and first time users is :

- basic information about what IT and the Internet can do for a business
- the costs and potential savings involved
- practical training on how to use the Internet

The next section will explain the results as they impact directly on SMEs. It will propose a strategy which can be adopted by the stakeholders in the IT industry for bridging the technology gap in SMEs and encouraging them to adopt the new technology . The strategy suggested draws on the references mentioned in the previous sections.

Bridging the SME Technology Knowledge Gap

The following model was developed in order to explain the findings of our research and to develop a framework which can be used to address the issues discussed. The model will show the reasons why the message is not filtering down to SME grass-roots, and how SMEs should be approached. It will summarise the key success factors for SME implementation of the Internet and other information systems, into their respective organisations.

The results of this study have shown that there are two main areas of concern when introducing the Internet into a company. These have been modelled into a pre-implementation stage and post-implementation stage. Neither of these stages are mutually exclusive, but for the purpose of this study, they have been modelled separately. The models analyse the processes taking place at each stage. A strategy is developed, which the IT industry can use as a framework for the implementation of the Internet in SMEs. By using this framework, not only will there be short term benefits, but in the longer term SMEs will develop a propensity to invest in and use technology for the benefit of their businesses.

Stage One - Pre-Implementation

The pre-implementation stage, is where SMEs still have not made the commitment to install or use any new system. Thus, information and knowledge should be targeted at SMEs in a form which will break through the outer layers of awareness and conviction of the decision maker in the organisation. This process is illustrated in the figure 4.

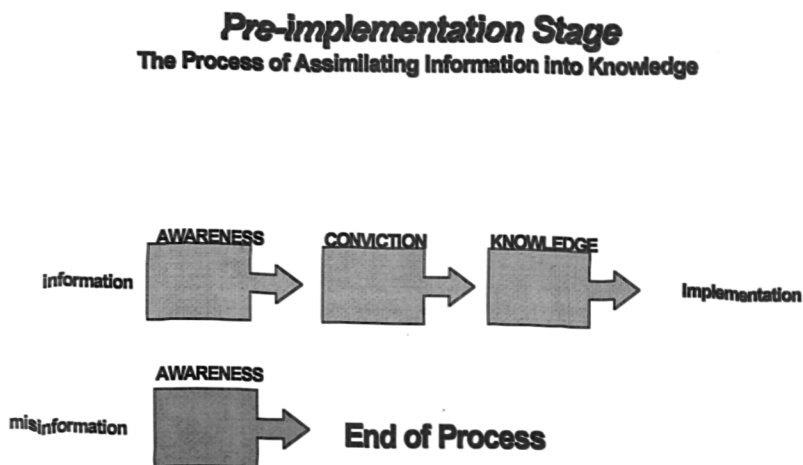


Figure 4. Pre-implementation Decision-Making Processes in SMEs

Misinformation, for example scare stories about the proliferation of pornography on the Internet, or the perception that new technology is too costly and complicated to use with no real benefits, will lead to a lack of conviction that the Internet is able to achieve business related objectives and thus non implementation of the system. The information could also be assimilated into bad knowledge

The information being given to SMEs should be specifically targeted at them, covering practical business related issues. Although each company is different, with distinct needs, the general areas should cover :

- costs - hardware, software, registration and on-line usage
- savings - in terms of both financial e.g. international communication at local rates) and time e.g. removing the drudgery of re-keying information)
- new business potentials e.g. advertising on the Net and cost benefits of this
- ease of use - degree of training and competence required
- associated services - such as e-mail, the on-line information resources

In order to get SMEs to benefit from the Internet, it is crucial for the IT industry to marry its enthusiasm for the technology, with an understanding of the business requirements of the SMEs. Thus, information about the Internet and associated services must be tailored in a way that SMEs will be able to understand and assimilate.

Once this level of awareness is achieved through correct information dissemination, then the potential implementers will attain conviction by assimilating this information into knowledge (by further requests for information in order to gain understanding). This knowledge will then be the basis on which SMEs can make informed decisions which will benefit their respective businesses.

Stage Two - Post-Implementation.

Once the first stage has been completed and the new technology has been implemented, most in the IT industry believe that their involvement in the process is complete. But this is not the case. With SME's in particular, the process has just begun. Again there are layers at this stage that must be reached before users of the Internet and other information systems become satisfied and are able to use the respective system to its full potential.

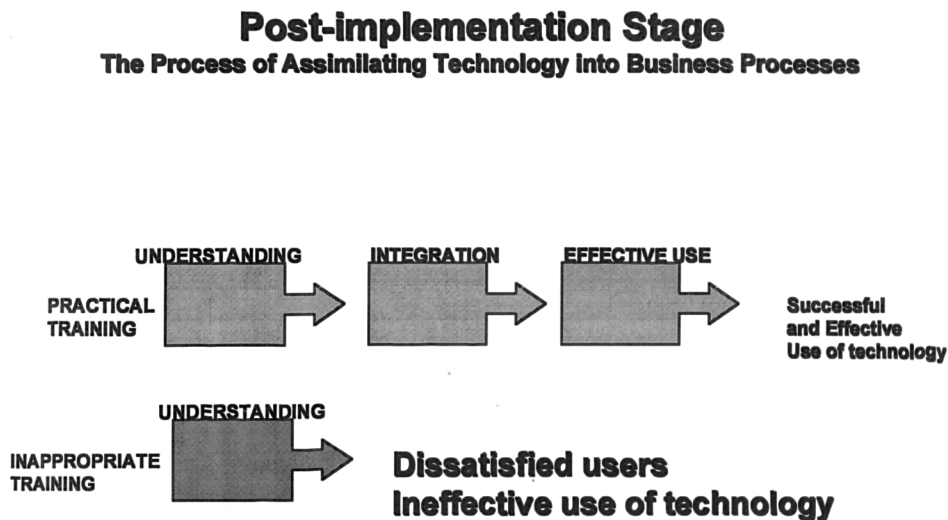


Figure 5. Post-implementation Satisfaction Processes in SMEs

The first step is to achieve understanding through training of staff. At this stage, the technological knowledge of staff must be assessed. As we have seen, the “younger” generation (under 30’s) tend to be more comfortable, confident and knowledgeable about computer. With SMEs in particular, staff often have to be multi-skilled dealing with more than one type of task in the company. Thus, training should cover basic aspects of computation including :

- practical hands-on training i.e. which buttons to press to achieve which tasks
- information about the type of system the organisation has, what it can realistically do and its limitations
- general information about the technology presented in a non-technical way to remove the mystery, aura and fear to experiment
- a more advanced level of training for the more technically competent who can then transfer their knowledge to other members in the organisation.

Once this level of understanding has been achieved, then and only then can the system be integrated into the company’s everyday business processes. The resistance to new technology is often due to lack of information, understanding and training of employees. A new system can become a white elephant in organisations because staff do not understand the benefits or the practical mechanics of using computers and thus avoid using it . Once the new technology/system has become integrated into everyday business practices and processes, then it is used effectively. Effective and integrated usage of information systems in general and the Internet in particular will develop an organisation which can benefit from the technology and will be more receptive to future developments of new technology.

Key Success Factors for SME Internet Implementation

The following table summarises the key success factors for an Internet implementation strategy drawing on the analysis from the above models and contemporary commentators (Karimi et al 1996). While the table divides the factors into two stages these are in fact mutually inclusive and each cannot be taken separately. The IT industry must work closely with SMEs to address the issues summarised below. This will raise awareness and bridge the knowledge and technology gap that so clearly exists in SMEs.

Key Success Factors	
Pre-Implementation	Post Implementation
Encourage information system/Internet objectives and activities to be based on SME business objectives and processes Obtain visible support and commitment from managerial decision makers Provide good understanding of business benefits and costs Ensure a clear definition of responsibility for IT both in the short and long term	Ensure the new system are marketed and sold to all managers and employees Provide comprehensive guidance and training to all Develop integration with existing business processes and systems

Table 6. Summary of Requirements From the IT Industry and SMEs

Conclusion

Although not exhaustive, the snap-shot view taken here of the Internet uptake by SME’s in one region of the UK , is consistent with findings on both sides of the Atlantic. It clearly shows, that despite the much extolled benefits of the Internet to businesses by writers in academia and the technology media, the message seems not to be reaching small and to a lesser extent medium sized businesses. The opportunities offered by the Internet to SMEs enabling them to close the competitive gap with larger organisations are being squandered, and there is a fear that SME’s will be further disadvantaged by ignoring the Internet.

What is required is for the IT industry to be aware of the technological needs of SMEs and target their information accordingly in order to close this gap. SMEs with non-IT dedicated departments undergo two stages in the process of introducing new technology to an organisation.

- **The pre-implementation stage** - awareness must be created by offering relevant business related information whereby the SME will actively seek more information to gain knowledge and attain conviction. Only then will implementation be possible.
- **The post-implementation stage** - training and education of all staff , ranging from basic practical hands-on button pushing to a wider understanding of the benefits and limitations of the installed system, leads to the long-term effective use of the technology through integration into the everyday business processes of the SME's.

The research here reveals, that a failure at either stage leads to dissatisfaction among SMEs, where negative feelings about the whole "technology" experience leads to a diminished likelihood of the companies implementing and thus benefiting from the next generation of technology and information systems. Unless the message that the Internet and other new technology is a tool for gaining competitive advantage and achieving further efficiencies in business processes, is filtered down to SMEs then the gap between small, medium and large enterprises will continue to widen and suppress the development and growth of SMEs which will harm not only the SMEs themselves, but will also impact negatively on the economy at large.

A1 - Discussion Guide for Focus Groups

Background

This information will be gathered beforehand when inviting members into the group.

Information will include:

Company information - turnover, number of employees, type of business, role of the member in the organisation

Type of technology installed and currently used in the organisation

2. Internet Specific

For NON-USERS

What do you think about computers and technology?

What do you know about the Internet?

Where did you get your information? Who normally tells the organisation about new technology, software etc. ?

What has prevented your organisation from being linked to the Internet? Is it cost ? Is it lack of trained personnel? Or is it the fact that it can't help the organisation?

What are the common problems you encounter in everyday running of the business? e.g. late deliveries, late payment, wrong goods ordered? Administration problems etc..

When you first meet a new customer or supplier, what procedures do you go through to make sure they are trustworthy partners?

What does security mean to you?

Is security an issue in everyday business life? If so what security measures do you have in place? Are these adequate?

Do you think the Internet could be a useful tool in running the business more efficiently and cost effectively. If not why not if yes how do you think it can be helpful?

What would you like the Internet to do for your business? What price are you willing to pay for such a system?

Do you think the Internet is safe for doing business ? What security measures would you like? How much are you willing to pay for security?

For USERS:

What is the Internet currently used for in the organisation i.e. is it used for sales, purchases, other business transactions? Marketing and advertising? Pressure because everybody else is using it? Getting information for the business? An alternative way to send messages? Pure entertainment? One or more of these is valid. Who has access to the Internet? Does everybody in the organisation have access to the Internet? Who uses it the most and what for?

What type of training is given/offered for Internet users? In-house, college courses, specialist trainers?

What are the costs of having the Internet - Financial? Social? Time issues? Others?

What are the benefits/advantages of the Internet?

What are the disadvantages/problems of the Internet?

What does security mean to you?

Do you worry about security when using the Internet? Why?

What security measures do you currently have in place? Are they adequate?

What security measures would you like to see?

How much would you be prepared to pay for secure use of the Internet?

What would you like the Internet to do for the business? Do you feel it is currently fulfilling the needs of the business? If not why not?

What do you think the relationship between business and the Internet will be in 2 -5 years from now? What would you like that relationship to be?

Added contributions from members.

A2 - Results of the Telephone Survey

Of those who replied, 34% had the Internet installed and 66% had no Internet. If we look at the figures per size of company, we can see (as one would expect) that as the size of the company increases, so does the propensity to install the Internet.

Company Size by number of employees	Internet % age	No Internet % age
<50	22	78
50-100	69	31
101-200	62	38
>200	88	12

For companies with less than 50 employees, over 75% do not have the Internet. Of these 51% are in the manufacturing sector, and 40% are in the service sector. Similarly, with companies who have the Internet, 63% are in the service sector and 34% are in the manufacturing sector.

No. of Employees	The Service Sector			The Manufacturing Sector		
	Internet	No Internet	Total	Internet	No Internet	Total
<50	15	28	43	5	35	40
50-100	7	1	8	2	3	5
101-200	2	2	4	3	1	4
>200	2	0	2	4	1	5
Total	26	31	57	14	40	54

Thus, as a percentage of those in the service sector, it is almost 50% who do and do not have the Internet, the majority of the have nots predictably being in the smallest sized companies. In the manufacturing sector, the proportion of Internet have to have nots is 1:4. This shows that the trend is more that the service sector is getting "linked", whereas the manufacturing sector is lagging behind.

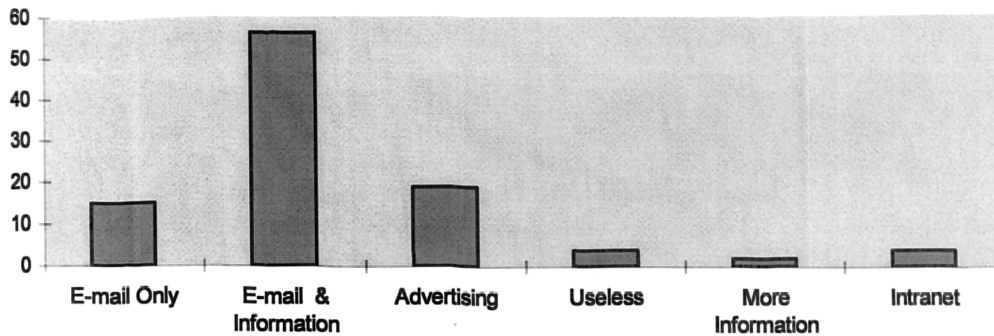
Internet Non-Users

Of the Internet non-users, over 70% of respondents cited that the Internet was of no benefit to their business, that they were too unsophisticated and small or that it was too expensive to implement. Only 11% were interested and were in the process of being linked while another 9% felt that they needed more information to make an informed opinion about the Internet.

Internet Users

Of the respondents who already had the Internet installed, 100% used it for e-mail while over 70% used it for information and over 50% had a web site which was used to promote the company's goods and services.

Percentage Responses from Internet Users



Of those who were using the Internet, some found it to be a waste of time, and had yet to justify its existence. One respondent said that if he could, he would remove it from every single machine.

When questioned about security, and whether they felt that security over the Internet was an issue, 90% of respondents felt it was not an issue, since they believed none of the information they were sending over the Internet was so confidential that extra security measures needed to be introduced. Several respondents in the service sector felt that security was not an issue only because they had not yet mastered the Internet and e-mail. Of the 10% who were aware of security, half were using the Intranet for security purposes, one was using Lotus Notes for security and one company had a full firewall security measure installed. The latter respondent was actually a software development company.

Recommendations

A lot of information needs to be disseminated to small and medium sized businesses in a way that they can assimilate and digest themselves. Only once the Internet and its usage has been understood and a level of competence attained, can security become an issue.

A3 Focus Groups

The most common business problems indicated by respondents from all groups were :

Cash flow	due mainly to late payments from customers <i>"The bigger they are the worse they are .. they take advantage of their size and clout"</i> also affected by over stocking
Marketing and Sales	reaching the right target customers <i>"sometimes we get requests for products which have nothing to do with our company"</i> <i>"we are paying large amounts on advertising but not increasing business"</i> the most effective advertising correct stocks for customers
Recruitment	finding the right people for the right job
Having an regular flow of work	<i>"sometimes we are very busy and at others we are not so busy"</i>
Lack of Training & Technical Support	especially on computers <i>"because of lack of training we are only using the technology to 70% of its potential use"</i> .

References

- ABERCROMBIE S, (1997) Europe on IT UK . *Euro-Info Centres* www.ispo.cee.be/ecommerce
- DICKEN P (1992) *Global Shift - The Internationalization of Economic Activity* Paul Chapman Publishing.
- EITO 1997 Report *Eurobit* Frankfurt
- FREEMAN C AND PEREZ C (1988) Structural Crises of Adjustment, business cycles and investment behaviour . In *Technical Change and Economic Theory* (DOSI G FREEMAN C NELSON R SILVERBERG G SOETE L Eds), Pinter, London.
- HENDERSON J AND CASTELLS M Eds (1987) - *Global Restructuring and Territorial Development*. Sage, London.
- HORNBAACH, K (1996) Competition by Business Design. *Long Range Planning* Vol. 29, no.5 pp616-628.
- TAYLOR I (1997) Minister of Science and Technology at the ISI conference *PC Week* 11/3/97
- KARIMI , GUPTA and SOMERS, IT and Strategic Response to Globalization. *Journal of Management Information Systems*, Vol. 12 No.4 Spring 1996 p.55-88.
- KEEGAN V (1997) Internet Users of the World Unite . *The Guardian Economics Notebook* 30/9/97
- LAWDER G WASTELL (1997) A Small Firms On-Line *Institute of Public Policy Report* (UK)
- PORTER M. *Competitive Advantage of Nations* Macmillan 1994.
- QUELSCH JA AND KLEIN LR (1996) The Internet and International Marketing *Sloan Management Review* , Spring,1996.
- ROSS JW, BEATH CM, GOODHUE DL, Developing Long-Term Competitiveness Through IT Assets *Sloan Management Review* Fall 1996
- MENSCH, G (1979) *Stalemate in Technology. Innovations Overcome the Depressions*, Ballinger, New York.
- SCHUMPETER J , *The Theory of Economic Development*, Harvard University Press, 1934.
- SUNOO, BP (1996) Loafing on the Job *Personnel Journal* December1996.
- Surveys:
- 30% of businesses are connected to the Internet {*PC World* 25/12/96}
- A survey of the top 1,000 companies in the UK revealed that 38% are on-line and 42% would have to get linked to the Internet in the foreseeable future {*Internet World* November, 1996}
- The percentage of all business non-users of the Internet fell from 52% in April 1996 to 45% in January 1996 {source: The Internet Black Box Survey - *Computer Weekly* February 1996}
- The DTI - (1997) Ryle S Time we went walkies on the net Gromit -. *The Guardian* 7/1/97
- The DTI (1997) "UK Business: Moving into the Information Society" 1997.
- TRAYNOR KITCHING AND ASSOCIATES (1996) UK Business and the Internet
- HAGEL AND ARMSTRONG (1996) *Harvard Business Review* 1/5/96
- SPAR AND BUSSGANG (1996) *Harvard Business Review* 1/5/96
- DELLECAVE T JNR (1996) How do you stack up? *SMT* December 1996 pp 34-37
- Information Strategy* A Survey of the Top 100 Companies in Europe who are the biggest IT Investors 22/1/97
www.info-strategy.com/t100_pnl.htm -
- ELLIOT L (1997) Seeing Network Visions *The Guardian* 4/2/97 World Economic Forum for charting the future of globalisation,
- TAYLOR P (1997)World ICT Markets. *Financial Times* 5/3/97

Appendix 7 - Telephone Interview Questions

OPEN ENDED QUESTIONS POSED TO TELEPHONE RESPONDENTS IN 1996/7 AND 98/99

1. Size of company by number of employees
2. Position of respondent in the company
3. Description of Business Activity
4. Do you have a security policy? If not why not?
5. If yes what areas are covered by the security policy?
6. Do you use E-Mail ? If not why not
7. What do you use e-mail for?
8. What would you not use e-mail for? Who do you use it with?
9. Are you linked to the Internet? If not why not?
10. If yes a)how long have you been using the Internet?
b) How are you linked to the Internet?
c)what kind of network to you have and what do you use it for? -
(e.g.intranet or other (please give a description))?
11. What do you use the Internet for in your business?
12. What kind of security features do you have? Why?
13. Do you have a web site? Since when?
14. What is the web site used for?
15. Can you give me the address of the web site?

Appendix 8 - Certification Practice Statement

The following Certification Practice Statement (CPS) is included as a self-contained document and does not include pagination consistent with this study. References within the document refer to the document itself. The document is 22 pages long and the appendices referred to within the document are appendices included within the CPS only.

Certification Practice Statement¹

©Copyright 1997 TrueTrust Ltd.

Document History

Version Number	Date of Issue	Comment
0.1	18 June 1997	Initial Private Circulation
0.2	24 June 1997	Feedback from above, plus addition of Ethical Policy
0.3	1 July 1997	Minor Corrections to 0.2
1.0	2 September 1997	Legal Revision of Appendix A Incorporation of comments from Entrust. First Public Release.

Document Circulation

The document has an uncontrolled circulation, but the master copy is always available from the World Wide Web at <http://www.truetrust.ltd.uk>

¹ - The GEMISIS CA has adapted this document from the CPS created by TrueTrust Ltd. with their permission. Copyright remains with TrueTrust Ltd. This document is a working document and is liable to change without prior notification. The document provides a detailed statement of the certification authority's practices which need to be understood and consulted by subscribers and certificate users.

This document is protected by copyright laws and no part of this document may be published, copied, circulated or used either in part or in its entirety without the prior written notification and permission of TrueTrust Ltd. However, the complete document may be copied and used for personal study on the condition that it is clearly and prominently stated that it is the property of TrueTrust Ltd, and this copyright notice accompanies such a copy at all times.

Glossary of Terms

Authentication registrar	The person nominated by the client company to administer the procedures of the company registration authority (RA)
Authenticator	The body or person who performs the authentication procedures, for example the CA, or an RA or an authentication registrar
Authority Revocation List (ARL)	List of revoked CA certificates
CA certificate	A certificate where the certificate subject is a CA
Certificate Policy	A stated purpose of applicability of a certificate
Certificate Revocation List (CRL)	List of revoked user certificates
Certificate Subject	The entity whose name appears in a certificate
Certificate User	The entity that uses the security software, private keys and certificates
Certificate	Digital information securely binding an entity's name to its public key (and implicitly to the private key that matches the public key)
Certification Authority (CA)	A trusted third party that verifies its members and issues certificates to them according to the criteria laid down in its Certification Practice Statement.
Certification Practice Statement (CPS)	The rules, guidelines and practices by which the issuing CA and its authorized entities will operate
Client Company	An organisation applying to the CA for membership
Company RA	A registration authority appointed by a company for its own end-users
Customer	The client company
Decryption private key	A entity's private key used for decrypting information
Direct end user	An end user who does not use the services of a Company RA
EDI	Electronic data interchange - the transfer of structured information from one computer system to another
Encrypting key pair	The decryption private key and the encryption public key
Encryption public key	A entity's public key used for encrypting information (the key is widely known and allows people to encrypt information for that entity).
End user	A certificate user that is a person (rather than a computer application)
Entrust administrator	The role required by Entrust to create, revoke and otherwise administer end-user certificates
Entrust Client	The software to be installed and used by end users
Entrust Manager	One part of the Entrust software used to operate the certification authority (the other parts are Entrust Server and Entrust Directory)
Back-up keys	Copies of users' private decryption keys held securely in encrypted format by the Issuing CA for the purpose of recovery of the user's data after a disaster.
GEMISIS CA	In this project it is the issuing CA
ICE-TEL	EC IV framework research project establishing a certification hierarchy throughout Europe.
ICE-TEL RA	A member of the ICE-TEL project authorised by the issuing CA to act as a registration authority
Issuing CA	The top level CA applying and administering this CPS to itself, its subject CA's, RA's and its customers
Key	A set of 1 or more large random numbers
Master key	The key used by Entrust to encrypt CA data held on computer media
Peer Issuing CA	A top level issuing certification authority whose CPS has been approved by this issuing certification authority
Personal Security Environment (PSE)	The area where Entrust client stores all security information. This is also known as the User's Profile
Private key	A key known only to the owner
Registration Authority (RA)	An entity authorised by the Certification Authority to perform the authentication procedures laid out in the CA's Certification Practice Statement
Revoked User	An end-user who has had his certificate withdrawn
Security officer	The role required by ENTRUST to set the security policy by which the CA operates.
Signing key pair /	This consists of the signing private key and the verification public key

Signing keys	
Signing private key	A entity's private key used to create a digital signature
Subordinate CA/ Subject CA	A certification authority authorized and appointed by the issuing CA to administer and apply this CPS on its behalf
Super-user	A UNIX system administrator
TrueTrust Ltd.	A commercial Certification Authority contributing its time and expertise to the GEMISIS research project
User certificate	A certificate where the certificate subject is a user
Verification public key	An entity's public key, made widely available as a certificate, to allow the certificate user to verify the digital signature of the entity.
X.500 directory	An internationally standardised repository used to store information about users

Note. The use of masculine in this document implies the feminine, and vice versa.

Table of Contents

1. INTRODUCTION	1
2. COMMUNITY OF CERTIFICATE SUBSCRIBERS	1
2.1 SUBORDINATE CAS	1
2.2 REGISTRATION AUTHORITIES	1
2.2.1 ICE-TEL Consortium Members	1
2.2.2 Company RAs	2
2.3 CERTIFICATE USERS	2
2.4 PEER CAS	2
3. APPLICABILITY OF ISSUED CERTIFICATES	2
3.1 SUITABLE APPLICATIONS	2
3.2 PERMITTED APPLICATIONS	2
3.3 PROHIBITED APPLICATIONS	2
3.4 STANDARDS	2
4. IDENTIFICATION AND AUTHENTICATION POLICY	3
4.1 IDENTIFICATION AND AUTHENTICATION OF REGISTRATION AUTHORITIES	4
4.1.1 Identification and Authentication of ICE-TEL RA's	4
4.1.2 Identification and Authentication of Company RA's	4
4.2 IDENTIFICATION AND AUTHENTICATION OF END USERS	4
4.2.1 By the Gemisis CA or the ICE-TEL RA	4
4.2.2 By the Company RA	5
4.3 ETHICAL POLICY	5
4.4 POST AUTHENTICATION AUDITING	5
4.4.1 List of Documentation Required	5
4.4.2 Authentication Audit Procedures	5
4.5 CERTIFICATION PROCEDURES	6
4.5.1 Initial Certification	6
4.5.2 Routine Annual Re-keying and Certification	6
4.5.3 Revocation Policy	6
4.5.4 Re-keying after revocation	6
4.6 RECOGNITION OF TRADEMARKS AND RESOLUTION OF NAME DISPUTES	7
4.6.1 Trade marks	7
4.6.2 Allocation of Names	7
4.6.3 Resolution of Name Disputes	7
5. KEY MANAGEMENT POLICY	7
5.1 GEMISIS CA	7
5.1.1 Key Generation	7
5.1.2 Key Storage	7
5.1.3 Key Usage	8
5.1.4 Archiving and Destruction	8
5.2 THE RA AND END USER	8
5.2.1 Key Generation	8
5.2.2 Key Storage	8
5.2.3 Key Usage	9
5.2.4 Key Archiving and Destruction	9
6. LOCAL SECURITY POLICY	9
6.1 GEMISIS CA	9
6.1.1 Physical Controls	9
6.1.2 Software Controls	9
6.1.3 Procedural Controls	10
6.1.4 Personnel Controls	10
6.2 THE REGISTRATION AUTHORITIES	10

6.2.1	<i>Software Controls</i>	10
6.2.2	<i>Personnel Controls</i>	10
6.2.3	<i>Physical Controls</i>	11
6.3	END-USERS.....	11
6.3.1	<i>Software Controls</i>	11
7.	TECHNICAL SECURITY POLICY	11
7.1	COMPUTER CONTROLS.....	11
7.2	NETWORK SECURITY CONTROLS.....	11
7.3	ASSURANCE.....	12
8.	OPERATIONS POLICY	12
8.1	KEY REVOCATION.....	12
8.1.1	<i>By the GEMISIS CA</i>	12
8.1.2	<i>The RA</i>	12
8.1.3	<i>The End-User</i>	12
8.2	PRIVATE KEY COMPROMISE.....	12
8.2.1	<i>Compromise of the GEMISIS CA's Private Key</i>	12
8.2.2	<i>Compromise of the Registration Authority and End-User's Private Keys</i>	12
8.3	KEY CHANGEOVER.....	13
8.3.1	<i>By the GEMISIS CA</i>	13
8.3.2	<i>By RAs and End Users</i>	13
8.4	GEMISIS CA TERMINATION.....	13
8.5	AUDIT LOGS.....	13
8.5.1	<i>The GEMISIS CA</i>	13
8.5.2	<i>The End Users</i>	13
8.6	ARCHIVES.....	13
8.7	DISASTER RECOVERY.....	14
8.7.1	<i>The GEMISIS CA</i>	14
8.7.2	<i>The RA and End Users</i>	14
8.8	COMPLIANCE AUDIT.....	14
8.8.1	<i>The GEMISIS CA</i>	14
8.9	CONFIDENTIALITY.....	14
8.9.1	<i>The GEMISIS CA</i>	14
8.9.2	<i>The RA and End User</i>	14
9.	LEGAL PROVISIONS	15
9.1	WARRANTIES AND DISCLAIMERS OF WARRANTIES.....	15
9.2	LIABILITIES AND LIMITS OF LIABILITIES.....	15
9.2.1	<i>The GEMISIS CA and the ICE-TEL RA</i>	15
9.2.2	<i>The Company RA</i>	15
9.3	FEEES.....	15
9.4	APPLICABLE LAWS OF BUSINESS.....	15
9.5	ARBITRATION.....	15
10.	POLICY ADMINISTRATION	16
11.	APPENDIX A THE SERVICE CONTRACT WITH MANCHESTER TRAINING AND ENTERPRISE COUNCIL	17
11.1	SCHEDULE B ENTRUST/CLIENT SOFTWARE LICENSE.....	18
12.	APPENDIX B THE CERTIFICATE END USER VERIFICATION FORM	19
13.	APPENDIX C THE ENTRUST AUTHORISATION INFORMATION FORM	21
14.	APPENDIX D. THE ETHICAL POLICY OF THE GEMISIS CA	22

1. Introduction

This Certification Practice Statement describes the practices and procedures used by the GEMISIS CA when generating, storing and using its private keys, and issuing, distributing and publishing certificates and certificate revocation lists. This Certification Practice Statement indicates the level of security applied by the GEMISIS CA to the protection of its keys, certificates, computer systems, and operating environment. It also describes the responsibilities of its customers and end users when generating, storing and using their private keys and the certificates of the GEMISIS CA. This Certification Practice Statement can be used when determining the trustworthiness of certificates issued by the GEMISIS CA, and the trustworthiness of data encrypted and digitally signed by certificate users of the GEMISIS CA.

2. Community of Certificate Subscribers

The following table illustrates the hierarchical structure of the different entities discussed in this document. The Issuing Certification Authority in this case is the GEMISIS CA and will be referred to in this document as such. The Issuing CA selects and has ultimate jurisdiction over subordinate CA's, Registration Authorities (RA's) and End users. The practices and requirements for each respective entity will be described below.

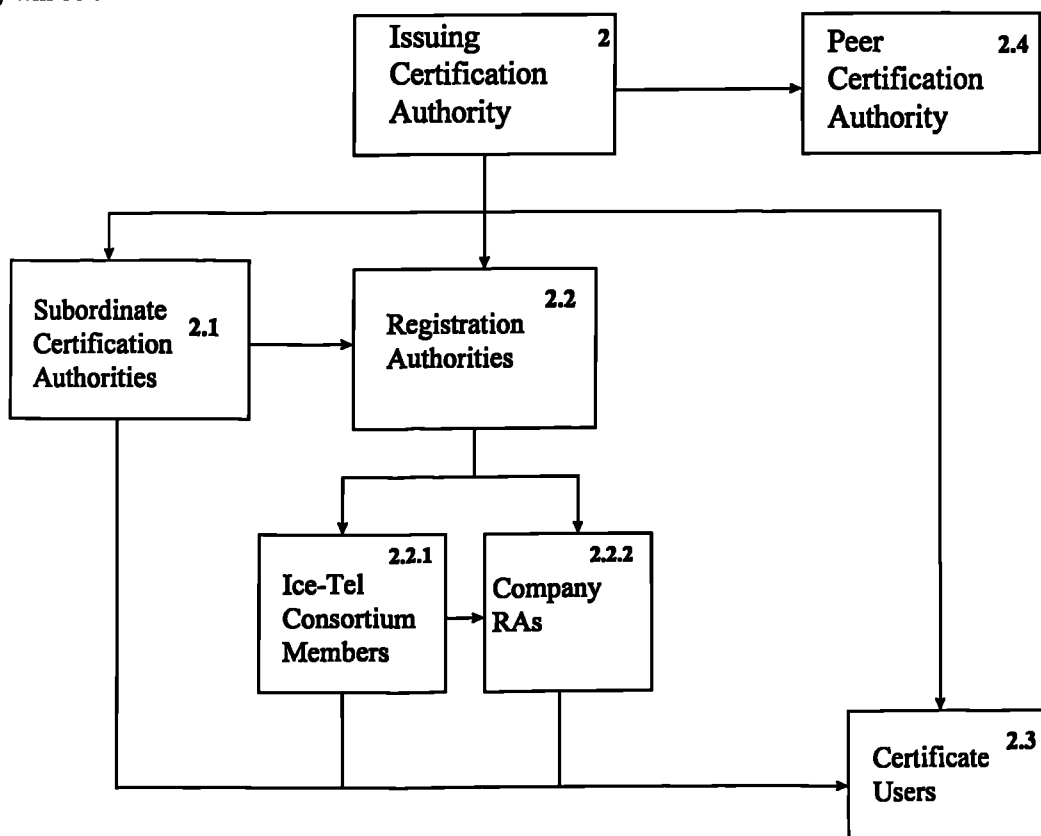


Figure 1. Community of Subscribers

2.1 Subordinate CAs

There are no certification authorities allowed to act as subordinate CAs for the GEMISIS CA.

2.2 Registration Authorities

The registration authorities allowed to verify end users on behalf of the GEMISIS CA are:

2.2.1 ICE-TEL Consortium Members

Operators of the ICE-TEL CAs personally authenticated by the GEMISIS CA

2.2.2 Company RAs

GEMISIS CA authenticated companies who can authenticate their own employees within their own registered site.

2.3 Certificate Users

Users that have been authenticated by the GEMISIS CA or by GEMISIS CA approved RA's. Certificate users will be predominantly end users within small and medium sized companies.

2.4 Peer CAs

A top level CA whose Certification Practice Statement for a specific certificate policy has been approved by the GEMISIS CA, and is willing to have a cross certificate issued by the GEMISIS CA. There are currently no approved top level CAs but these will be added in due course.

3. Applicability of issued certificates

This section describes the suitable and restricted use of issued certificates

3.1 Suitable Applications

- encryption of company documents
- encryption of sensitive data to be accessed only by certified personnel
- protection of all types of files stored on a computer such as graphics, ASCII text, spreadsheets, presentations, programme code, word processor files etc.
- e-mail communication over the Internet/Intranet with other certified users, of both secured text messages and secured file attachments
- file transfer over the Internet/Intranet of secured files

3.2 Permitted Applications

Use of GEMISIS CA issued certificates are unrestricted for applications that only require authentication, confidentiality and/or integrity between certified users.

3.3 Prohibited Applications

Applications that make use of the following services:

- Electronic Funds Transfer
- EDI
- Any other service requiring authorisation

must not be used with GEMISIS CA issued certificates without the communicating parties undertaking external authorisation between themselves.

The GEMISIS CA certificates provide no in built authorisations or permissions.

3.4 Standards

Encryption

- DES (FIPS PUB 46-2)
- CAST
- DES-CBC and CAST-CBC (FIPS PUB 81)

Digital Signatures

- RSA (PKCS#1)

Hash Functions

- MD2 (RFC1319)
- MD5 (RFC1321)

Key Management

- RSA key transfer (RFC1421 and RFC1423)

Integrity

- MAC (FIPS PUB 113)

Random Numbers

- ANSI X9.17

Certificate formats

- Certificates (X.509(1993))
- CRLs (X.509(1993))
- RSA identifiers and formats (RFC1422 and RFC1423)

File Envelope Format

- PEM (RFC1421)

Directory Protocols

- DAP/DSP (X.500)
- LDAP (RFC1777)
- LDAPD (University of Michigan)

Client Management Protocol

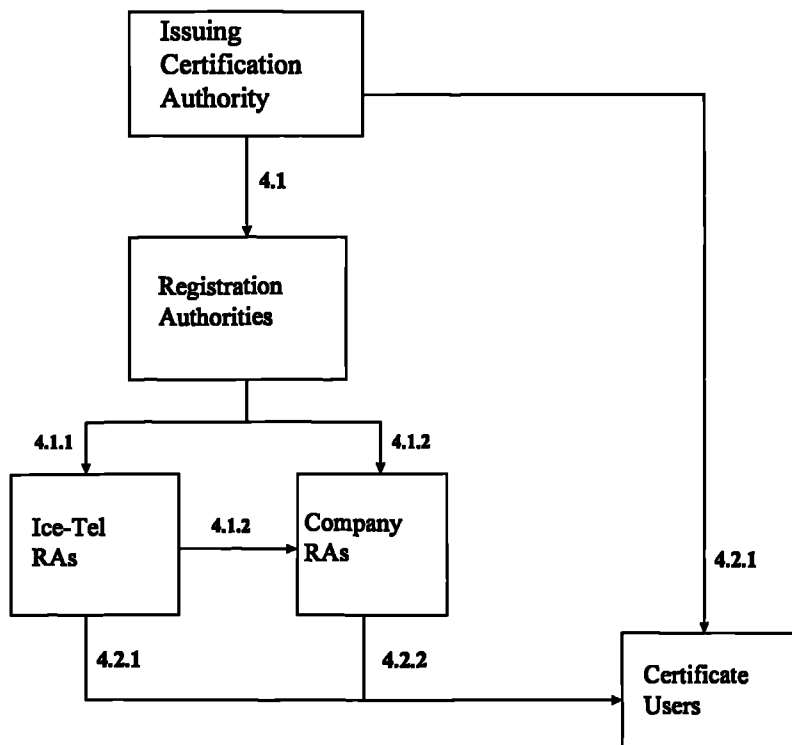
- SEP (Northern Telecom Security Exchange Protocol, built using Generic Upper Layers Security standards)

APIs

- GSSAPI (RFC1508 and RFC1509)
- SPKM (proposed Internet Standard)

4. Identification and Authentication Policy

This section describes the processes for identification and authentication of registration authorities and end users by the GEMISIS CA and also the processes for identification and authentication of end users by the registration authorities. In addition, the GEMISIS CA operates an ethical policy, as described in section 4.3.



4.1 Identification and Authentication of Registration Authorities

The GEMISIS CA will identify and authorise its Registration Authorities by following the procedures described below.

4.1.1 Identification and Authentication of ICE-TEL RA's

The identification and authentication of ICE-TEL RAs is based on the personal relationships between the operators of the GEMISIS CA and those within the ICE-TEL project. Authenticated ICE-TEL RA's will follow the Company RA verification processes laid out in section 4.1.2 and the end user verification processes laid out in section 4.2.1. Countries in which ICE-TEL project partners currently operate are: Austria, Denmark, Estonia, Germany, Greece, Ireland, Italy, Norway, Portugal, Slovenia, Spain, and Sweden.

4.1.2 Identification and Authentication of Company RA's

Stage 1. Verification of the Company

The client company applying to become a GEMISIS authenticated RA will be verified initially as an end user in accordance with the procedures laid out in section 4.2.1.

Stage 2 - Selection of the Authentication Registrar

Nomination of the Authentication Registrar will be determined by the client company's officials, preferably in accordance with the GEMISIS CA's guidelines. The final nomination and selection of the Authentication Registrar is the sole responsibility of the client company. The following guidelines are recommended. The Authentication Registrar should have:

- been working for the client company for more than 18 months
- an exemplary conduct record and be trustworthy
- an understanding of the usage of certificates in the organisation
- a close working relationship with the personnel department and have access to personnel records
- a knowledge of the employees in the organisation
- a close working relationship with those who make decisions about access to and usage of certificates
- a good working knowledge of computing
- a willingness to train authorised users in the use of the security software

Once the Authentication Registrar has been nominated internally, this must be made known to the GEMISIS CA.

Stage 3 - Authenticating and Validating Users

Once the end user has been selected by the company officials (in accordance with their own internal policies) then the Authentication Registrar will :

- authenticate and validate each end user by using the procedures of 4.2.2
- complete the Certificate End User Verification form (see Appendix B The Certificate End User Verification Form), and
- return it to the GEMISIS CA as digitally signed Email.

It is essential that the Authentication Registrar keeps a record of authorised end users.

Stage 4 - Issuing Certificates

When the GEMISIS CA receives the verification form, it will register the end user with Entrust, and return the Entrust Authorisation Information form (see Appendix C The Entrust Authorisation Information Form) to the Authentication Registrar by encrypted digitally signed Email. The Registrar must record each user and maintain auditable records for annual inspection by the GEMISIS CA.

4.2 Identification and Authentication of End Users

4.2.1 By the Gemisis CA or the ICE-TEL RA

The Authenticator will carry out the identification and authentication procedure described below:

Each customer must provide 2 trading references and one bank reference which will be taken up by the authenticator. If these are satisfactory, the authenticator will visit the site of the user, to install the security software and confirm the operating address of the user.

4.2.2 By the Company RA

The recommended procedures for internal verification of end users by the Authentication Registrar are :

- Receive written authorisation that the named employee is to become a user of the certificate
- Physically identify the user
- Physically check employee identification documents cross checked with company personnel records.

4.3 Ethical Policy

The GEMISIS CA operates an ethical policy, which is designed to minimise its participation (either directly or indirectly) in the use of the Internet for illegal, immoral or corrupting practices. The Ethical Policy of the GEMISIS CA is reproduced in Appendix D. The Ethical Policy of the GEMISIS CA). Each subordinate CA, Registration Authority and end user must subscribe to this ethical policy before it will be authenticated by the GEMISIS CA. To this end, each entity must complete the Ethical Use of the Internet self certification form in Appendix D and submit this to the GEMISIS CA with its initial application form. GEMISIS CA reserves the right to refuse authentication or continuing authentication of any entity which fails to satisfy the Ethical Policy of the GEMISIS CA.

4.4 Post Authentication Auditing

The Authenticator will carry out an authentication audit of Company RAs and direct end users once a year between months 6 and 12 of their membership.

4.4.1 List of Documentation Required

The auditor will check that the following records signed and authorised by the authenticated official are available and up-to-date. These records must be kept by company RA's and end users:

- A list of all the people who are authorised to use any given certified user name and have been given the password to access the corresponding private keys.
- A record of the date each time a password has been changed (but not a record of the password).
- A list of authorised employees who have left the company and their dates of leaving.
- A list of people whose authorisation to use a certified user name has been revoked and the dates of revocation.
- A list of users who have had new certificates issued along with the reasons and the number of times this has happened.

These records must be updated each time there is a change . These records should be available to the GEMISIS CA and the ICE-TEL RA's at all times.

4.4.2 Authentication Audit Procedures

4.4.2.1 Of direct end users and Company RAs by the GEMISIS CA and ICE-TEL RAs

The direct end user and Company RA will send the required documentation to their authenticator at least once per year, when requested to do so. The auditor will return a brief audit report on the working practices of the respective entity (Company RA or end-user) for their benefit. If deficiencies are found, recommendations for counteracting any breaches in procedure will be made. The entity must then send written confirmation that they will implement any recommendations made by the auditor in a timely manner, in order to ensure more effective security working practices.

4.4.2.2 Of End Users by Company RAs

End users will be audited by their Authentication Registrar. It is the responsibility of the Authentication Registrar to maintain the documentation required for audit which should be sent to the GEMISIS CA or ICE-TEL RA for review when requested by them, at least once per year. Both the ICE-TEL RA and the GEMISIS CA may note breaches in procedure and either may make recommendations for improvements. The end user must then confirm in writing that they will implement the recommendations made by the auditors.

4.5 Certification Procedures

4.5.1 Initial Certification

4.5.1.1 Of Company RA

Initial certification of a Company RA will be carried out by the GEMISIS CA, during the installation of the security software at the customer's site by a GEMISIS technician or ICE-TEL RA technician.

4.5.1.2 Of End Users Authenticated by a Company RA

Initial certification of an end user having a Company RA will take place during the time when the Authentication Registrar installs the security software on the end user's PC. The Authentication Registrar is also responsible for demonstrating the use of the security software to the end user.

4.5.1.3 Of Direct End Users

Initial certification of a direct end user will take place when the security software is being installed on his PC by a GEMISIS technician or ICE-TEL RA technician. The authenticator will visit, install and also demonstrate the use of the security software to the end user.

4.5.2 Routine Annual Re-keying and Certification

This section deals with the renewal of the Registration Authorities and end users association with the GEMISIS CA.

4.5.2.1 Company RA

Subject to satisfactory annual audit and continuing payment of subscription fees, a customer will be allowed to continue to operate a Company RA. Certificates will be automatically renewed. If the audit is found to be unsatisfactory then the company will only be allowed to continue with direct end users (which will be charged at the appropriate rate), until such time as the Company RA assures the GEMISIS CA that such breaches will not occur again.

4.5.2.2 End-users

Subject to satisfactory annual audit and continuing payment of subscription fees, end user certificates will be automatically renewed. If the audit is found to be unsatisfactory then certificates will continue to be valid only if the customer agrees to implement more secure working practices. A fresh audit will be held after 3 months and, if this audit is still unsatisfactory, the end user certificates will be immediately revoked and all outstanding fees refunded (less an administration charge).

4.5.3 Revocation Policy

4.5.3.1 For Company RA's and End-Users

The key will be revoked in the following circumstances :

- if the holder is found to have ceased trading
- if the holder is found to have changed address without notification of the new address to the authenticator
- if the security of the unique password has been compromised
- if the holder has left the organisation
- if the GEMISIS CA receives a message signed with the signing private key authorising the GEMISIS CA to revoke the certificate
- if the GEMISIS CA receives written notice from an authorised body and confirmed by telephone that the password has been forgotten or lost.

4.5.4 Re-keying after revocation

The GEMISIS CA will re-key within one working day after receiving instructions to re-instate the certificate from the authorised end-user or RA if the password has been forgotten or lost. If however, the GEMISIS CA is re-keying because security has been compromised, re-keying will occur only after receiving assurances that recommendations to implement more secure working practices will be

adhered to. Subsequent annual audits will pay close attention to ensuring that these recommendations have been implemented.

If the same security compromise occurs more than one time for a particular end user then the GEMISIS CA reserves the right to refuse to re-key that user, and will instead refund all outstanding fees (less an administration charge).

In all cases of key renewal, a charge will be made to cover administration costs for issuing a new certificate and any retraining required.

4.6 Recognition of Trademarks and Resolution of Name Disputes

4.6.1 Trade marks

Trade marks will not be used and are not recognised by the GEMISIS CA and its authorised bodies

4.6.2 Allocation of Names

Names allocated in the UK will be made in accordance with the procedures of BS 7453: Procedures for the UK Name Registration Authority. Any costs associated with registering the names of unlimited companies or partnerships must be borne by those organisations. For other countries in the EC, the authenticator will endeavour to use whatever accepted local procedures and standards are in place. Legal documentation must be presented to the authenticator proving legal title to the name according to the registration rules and regulations in the respective country of operation. Whoever has legal title to the name will have access to that name in their certificate.

4.6.3 Resolution of Name Disputes

If name disputes arise the authenticator will not be involved in settling disputes and the users will not be authenticated until such disputes have been settled.

5. Key Management Policy

This section defines the security measures taken by the GEMISIS CA to protect its keys and passwords.

5.1 GEMISIS CA

5.1.1 Key Generation

The (symmetric) CA master key is generated automatically during the installation and configuration of the Entrust server software. The CA master key does not expire.

The (symmetric) Entrust/Manager master key is generated automatically during the installation and configuration of the Entrust server software. The Entrust/Manager master key does not expire.

The (asymmetric) CA signing key pair is generated automatically during the installation and configuration of the Entrust server software. The CA key pair has a fixed lifetime of 20 years.

5.1.2 Key Storage

The CA master key is stored securely in the Entrust/Manager database. It is encrypted under symmetric keys derived from the Entrust password of each Security Officer and Entrust Administrator.

The Entrust/Manager master key is stored securely in the Entrust/Manager database. It is encrypted under symmetric keys derived from the Entrust password of each Security Officer and Entrust Administrator.

The CA signing private key is stored securely in the Entrust/Manager database. It is encrypted using the CA master key.

The CA verification public key is stored in a self-signed certificate. The certificate is distributed to end users at the time they use Entrust/Client to create a new user name. User's store this certificate securely within their profile (PSE).

5.1.3 Key Usage

The CA master key is used to encrypt the CA signing key pair.

The Entrust/manager master key is used to encrypt all data (except the CA signing private key) that is stored in the Entrust/Manager database.

The CA signing private key pair is used by Entrust/Manager to sign:

- the CA verification public key certificate
- the Entrust/Manager protocol verification public key certificate
- Certificate Revocation Lists
- Authority Revocation Lists
- all end user certificates

The CA verification public key is stored in a certificate and is used by Entrust/Client to verify the authenticity and integrity of all digital signatures.

5.1.4 Archiving and Destruction

The CA master key can be changed at any time, subject to the approval of at least two Security Officers. The old key will be discarded.

The Entrust/Manager master key can be changed at any time, subject to the approval of two Security Officers. The old key will be discarded.

The CA signing key pair cannot be modified or revoked (this is a limitation of the current version of Entrust)

5.2 The RA and End User

5.2.1 Key Generation

The (asymmetric) encryption key pair is generated by Entrust/Manager when an Entrust Administrator uses Entrust/Admin to create credentials for a new user. Encryption keys are valid for two years .

The (asymmetric) signing key pair is generated by Entrust/Client when the user uses Entrust/Client to create a new user name. Signing keys are valid for two years.

5.2.2 Key Storage

The encryption public key is stored in a certificate, signed with the CA signing private key. This certificate is sent to the user in a secure manner, and is made available in the Entrust X.500 directory.

The decryption private key is sent to the user in a secure manner. It is stored securely in the user's profile (PSE) encrypted using a symmetric key derived from their password.

A copy of the decryption private key is stored securely in the Entrust/Manager database. It is encrypted using the Entrust/Manager master key.

The signing private key is stored securely in the user's profile (PSE) encrypted using a symmetric key derived from their password. This key is not sent to Entrust/Manager.

The verification public key is sent to Entrust/Manager in a secure manner. This key is stored in a certificate, signed with the CA signing private key, which is returned to the user. It is not stored in the Entrust X.500 directory, since it is sent with each message that is digitally signed by the user.

5.2.3 Key Usage

The encryption public key can be used only during its defined period of validity (two years from when it was issued, unless it is revoked sooner). When the key is 80% of the way through its period of validity, Entrust/Client will automatically contact Entrust/Manager and request that a new key pair is issued.

The decryption private key does not expire, and can be used at any time.

The signing private key can be used during the first 70% of the defined period of validity (16.8 months from when it was issued, unless it is revoked sooner). When the key is 50% of the way through its period of validity, Entrust/Client will automatically generate a new key pair and contact Entrust/Manager to update the certificate containing the verification public key.

The verification public key can be used only during its defined period of validity (two years from when it was issued, unless it is revoked sooner). After the validity has expired, the key can still be used to verify messages. However, a message will appear warning the user that the signature should not be trusted.

5.2.4 Key Archiving and Destruction

Old versions of the encryption public key and the decryption private key are archived within the user's profile (PSE) and within the Entrust/Manager database.

6. Local Security Policy

This section describes the non-technical security controls used by the GEMISIS CA and its registration authorities and end-users.

6.1 GEMISIS CA

6.1.1 Physical Controls

- Access to the CA building is controlled, with only authorised persons having key-cards able to open the entry door.
- A strong fireproof door with 5-lever mortise lock controls access to the CA office - keys have only been distributed to a limited number of CA trusted personnel. Cleaners and security guards do not have keys.
- Metal bars are fixed across all external windows.
- The computer running the Entrust server is chained to the floor.
- A fireproof safe is chained to the floor and stores the following:
 - ⇒ lists of certificates issued
 - ⇒ lists of revoked certificates
 - ⇒ back-up keys
 - ⇒ Entrust manuals
 - ⇒ Entrust set-up disks
 - ⇒ sealed copy of UNIX user passwords
 - ⇒ archived records
- Access to the safe will require the presence of at least two TrueTrust Ltd. directors simultaneously.

6.1.2 Software Controls

Each Entrust Security Officer and Administrator has their own password for logging onto Entrust Manager. This password:

- must be at least 8 alphanumeric characters with at least one upper case letter, one lower case letter, and one digit
- must not be a subset of their user name
- must not be written down but remembered by the individual
- must not be revealed to anyone.

At least two administrators must present their passwords before the private signing key of the GEMISIS CA can be accessed. At least two security officers must present their passwords before the security policy can be altered.

6.1.3 Procedural Controls

This section describes the different roles and responsibilities of personnel in the organisation.

- a) **Security Officers** - Four security officers are responsible for determining the security policy of the GEMISIS CA, where at least two of the four will be required to authorise any changes to the security policy. The four security officers are the four directors of TrueTrust Ltd.
- b) **Entrust Administrators** - will be trusted employees of GEMISIS and the University of Salford.
- c) **Installation Service** - Full time employees of the GEMISIS 2000 project will have the responsibility for installing the Entrust Client software and training member companies in the use of the hardware and software involved in the virtual chamber of commerce project. Directors of TrueTrust Ltd. will be responsible for overseeing the installation of the security software and training of the GEMISIS engineers.
- d) **Issuing digital certificates** - this will be the joint responsibility of the Entrust administrators.
- e) **Technical Support/help-line** - first line support will be the responsibility of the three GEMISIS engineers trained by TrueTrust Ltd. Second line support will be the responsibility of the employees of TrueTrust Ltd.. Final support will be the responsibility of ENTRUST Technology's support engineers.
- f) **Verification service** - will be carried out by a GEMISIS research engineer.
- g) **Administration** - TrueTrust Ltd. will operate the customer database and records.

6.1.4 Personnel Controls

This section describes the procedures for training and recruitment of the GEMISIS CA personnel.

- The TrueTrust security officers and administrators are all directors of the company who are well known to each other, and have been in a position of trust and responsibility for some time.
- All GEMISIS engineers will be recruited in accordance with the rules and regulations of the University of Salford, with at least 2 references taken up.
- Training of the GEMISIS engineers will be carried out by TrueTrust directors, who between them have a strong grounding and long experience in University education and teaching.

6.2 The Registration Authorities

6.2.1 Software Controls

Both types of registration authority (ICE-TEL and Company) need to take extreme care of their passwords which control access to their keys. The following guidelines should be followed to maintain the security and integrity of the keys. The password:

- must be at least 8 alphanumeric characters with at least one upper case and one lower case letter
- must not be a subset of the user name
- must not be written down but remembered by the individual²
- must not be revealed to any unauthorised certificate users

6.2.2 Personnel Controls

The person occupying the position of authentication registrar for the registration authority must be technically competent since he/she will be responsible for the Installation Service i.e. responsible for

² If the password is written down for backup purposes, then it should be strongly protected, for example, be placed in a sealed envelope (signature and sellotape across the seal) and stored in a safe place - verification that strong protection is used will be part of the annual audit.

installing the end user Entrust Client software. Further criteria for the appointment of this person are specified in Section 4.

6.2.3 Physical Controls

It is strongly recommended that the RA keeps the machine containing the signing key file in a locked office.

6.3 End-Users

6.3.1 Software Controls

Each end-user needs to take extreme care of the password controlling access to his/her private keys. The following guidelines must be followed in order to maintain the security and integrity of the keys. The password:

- must be at least 8 alphanumeric characters with at least one upper case and one lower case letter
- must not be a subset of the user name
- must not be written down but remembered by the individual
- must not be revealed to any unauthorised certificate users

7. Technical Security Policy

This section describes the technical security controls used by the GEMISIS CA.

7.1 Computer Controls

Separate log-in accounts are used by each of the authorised Entrust administrators and log in is only allowed at the console on-site.

Log-in as Super-user can only be performed when two directors of TrueTrust are present, since a split password is used i.e. the Super-user password is divided into two parts: one part is known by the system administrator and technical director; and the other part is known by the other directors.

Access controls - discretionary access control is included in the Entrust software and is set-up to ensure that at least 2 of the TrueTrust senior personnel are required to access the programme and computer.

There are on-site and off-site backups of :

- all Entrust software disks
- all back-up keys
- all issued certificates
- all certificate revocation lists
- CA private keys
- Super-user passwords

Back-ups will be created once a threshold of five new users have been issued with new certificates or five certificates have been revoked.

7.2 Network security controls

The following features are disabled:

- remote log-in (Telnet)
- in-bound FTP
- X-Windows connection
- Remote job execution
- Direct root log-on

In addition,

- rhost files have been removed
- a network monitoring programme has been installed
- the Entrust Audit tool logs every action
- TCP access is only be allowed to the web server, directory server and mail server

7.3 Assurance

The technical level of assurance is achieved by :

- Periodically running the Securities Administrators Tool for Analysing Networks (SATAN) - an attack simulation programme - to detect potential system security breaches.
- Knowing that usage of the system and network is logged and auditable.
- Having installed physical and network security measures as described above.

8. Operations Policy

This section describes the operating procedures for the certification keys.

8.1 Key Revocation

8.1.1 By the GEMISIS CA

There is only one point of distribution for CRLs and this is within the Entrust directory. Private keys will be revoked within one working hour after notification. The CRL will be published at 8.00pm on the day of revocation. CRLs are issued daily at 8pm, and are valid until midnight the following day. When subordinate or peer CAs are certified, ARLs will be issued every 6 hours.

Note. At no time does the GEMISIS CA actually know the private signing key of any RA or end user, and therefore this information cannot be held in escrow and cannot be revealed to third parties by the GEMISIS CA (the only way is by the end user compromising their Entrust password).

8.1.2 The RA

- Notification - The RA should notify the GEMISIS CA via a signed message or authenticated out of band exchange as soon as its key compromise or loss is detected .
- Retrieval - Client software is configured to download CRL's from the GEMISIS CA directory the first time each day that the client PC attaches to the Internet.

8.1.3 The End-User

- Notification - The end-user should notify in person either the local RA or the GEMISIS CA via a signed message or authenticated out of band exchange as soon as its key compromise or loss is detected.
- Retrieval - Client software is configured to download CRLs from the GEMISIS CA directory the first time each day that the client PC attaches to the Internet.

8.2 Private Key Compromise

8.2.1 Compromise of the GEMISIS CA's Private Key

The key of the GEMISIS CA will be assumed to be compromised in the following cases:

- break in to the office holding the CA and theft of the computer system running the CA,
- break in to the office holding the CA and theft of the safe holding the backup information
- some other security breach that the directors consider could have compromised the CA private key.

In this event the GEMISIS CA will :

- generate new CA key pairs
- revoke all certificates of all subjects
- notify and re-issue certificates to all subjects
- record details of how the security was compromised and review its procedures

8.2.2 Compromise of the Registration Authority and End-User's Private Keys

Keys will be assumed to be compromised if some unauthorised user gains access to the PSE (profile) of the user, or the user inadvertently divulges his password to another user. If the user leaves the employ of the company and is the sole user of a private key then revocation should take place. If the user is one of several authorised users for a particular private key, then compromise should be assumed unless the company can be sure that the employer does not have a copy of the Entrust Client software and PSE,

and the password is changed immediately after he leaves the employment of the company. Once the GEMISIS CA is notified that the private key has been compromised then the GEMISIS CA will:

- revoke the certificate
- record the reason why the certificate was possibly compromised
- review the user's procedures and make sure the user understands the necessity for secure passwords and if necessary give advice on password selection
- re-issue the user with new keys and certificates.

8.3 Key Changeover

8.3.1 By the GEMISIS CA

In the event that it becomes operationally necessary to replace the keys of the GEMISIS CA, for example, due to a new software release, or the decision to use longer key lengths, then the GEMISIS CA will:

- generate new CA key pairs
- revoke all certificates of all subjects
- notify and re-issue certificates to all subjects

8.3.2 By RAs and End Users

This is described in Section 5.2.3.

8.4 GEMISIS CA Termination

The GEMISIS CA will terminate operations in December 1988, at which time the directors of TrustTrust Ltd will determine if it is commercially feasible to take over the operation.

8.5 Audit logs

8.5.1 The GEMISIS CA

The following list of audit logs is kept by the GEMISIS CA:

- Network Usage log
- UNIX Super-User Logons
- Entrust Server log

Access to these audit logs is controlled by the root password where at least two directors are required to provide the two part password. The logs will be archived and removed from the primary system every 6-12 months or when it is over 1MB in size. The audit log copy will be stored for 5 years.

8.5.2 The End Users

The customers are advised to keep a log of all authorised certificate users for at least 3 years.

8.6 Archives

The GEMISIS CA will keep archives of :

- the CA's expired private keys
- certificates issued
- audit logs
- back-up keys
- CRLs

The archives will be stored for 5 years in a fireproof safe. The archive will be created at a convenient time (between 6-12 months) within the boundary of 1 MB of information .

8.7 Disaster Recovery

8.7.1 The GEMISIS CA

The GEMISIS CA service will normally be operational 24 hours a day, 7 days a week. In the event of a disaster where damage has been done to the equipment but the CA's private key has not been compromised then the back-ups of :

- software disks
- back-up keys
- issued certificates
- certification revocation lists
- the CA private key

(either on-site or off-site depending on extent of damage) will be used to restore the system. During the GEMISIS pilot, the CA will expect to be operational again within 5 working days. When an operational service by TrueTrust is available, the service will expect to be restored within 1 working day. Whenever the CA service is not available over the Internet, a telephone hot line will be available 8am to 8pm to inform customers for the reason for the network outage, the estimated time for a restored service, and to receive and give new revocation reports.

8.7.2 The RA and End Users

In the event of a disaster where damage has been done to the equipment and the key has not been compromised then the GEMISIS CA will:

- re-install the software (if required)
- re-issue the user's certificates

8.8 Compliance Audit

8.8.1 The GEMISIS CA

The GEMISIS CA will undergo a procedures compliance audit carried out by an independent internationally recognised expert at least once annually. The auditor will provide a written report stating both the noteworthy areas and also any deficiencies and recommendations for improvement of procedures. The TrueTrust Ltd. board of directors will discuss the report within a week of its submission and will immediately act on any deficiencies found in the report. The TrueTrust Ltd. board will provide a summary report for their end-users (endorsed by the auditor) within one week of the audit, except in exceptional circumstances where a serious deficiency is noted, and then only after action has been taken to remedy such deficiency.

8.9 Confidentiality

8.9.1 The GEMISIS CA

The back-up user decryption keys, the Super-user and Entrust passwords and the CA's private keys will remain confidential and will not be made available to anybody unless a relevant court order is produced from the law enforcement authorities. In the case of a law enforcement officer having a warrant to access a user's back-up decryption key, the user will be informed of this as soon as possible. A user's private decryption key will only be released to the user, after an authenticated request from the user, and then only by a personal visit to the user's site by an employee of GEMISIS. Under no circumstances will a user's decryption key be released to anyone other than the user or a law enforcement officer possessing an appropriate court order. In particular, no employee of GEMISIS CA or director or employee of TrueTrust Ltd will access a user's back-up decryption key. All other information such as logs and customer databases, which are not security related are available to authorised auditors.

8.9.2 The RA and End User

The password to a user PSE (profile) must remain confidential to the authorised users of the PSE.

9. Legal Provisions

The contracts between the customer and the Manchester TEC, and between the customer and the University of Salford form part of this CPS. These contracts are listed in Appendix A.

9.1 Warranties and disclaimers of warranties

See Appendix A The Service Contract with Manchester Training and Enterprise Council

9.2 Liabilities and Limits of Liabilities

9.2.1 The GEMISIS CA and the ICE-TEL RA

The GEMISIS CA and ICE-TEL RAs will not be liable for any loss or damage suffered by the user or any third party through the use of the software or the certificate whether now or in the future as a result of:

- inappropriate use of the certificate and security technology by the user or third party
- the user not keeping their password secure
- the user or Company RA failing to inform the GEMISIS CA or ICE-TEL RA immediately of any keys that have been compromised or users whose authorisation to use their respective keys have been revoked
- lack of performance by the software, network hardware or other aspect of the technology
- intentional or unintentional deception by any client of the CA.

In the event that a user's password is compromised, the end user is liable for any loss suffered by a third party as a result of successful verification of messages digitally signed with the revealed signing public key until the compromise is reported to the GEMISIS CA and the next CRL has been issued.

In the event that either a GEMISIS CA or ICE-TEL RA private key is compromised, then the compromised party would normally be liable for the direct losses sustained by a customer as a result of such compromise. However, due to the fact that this is a research project provided free of charge (or at cost) to customers, then the maximum liability by the compromised party will be to reimburse any fees paid by the customer, and to provide the service free of charge from the time of compromise until the end of the project.

9.2.2 The Company RA

The company RA is responsible and liable for all end users of the certificates in their company including authorised and unauthorised users.

Obligations of Company RA's and End Users

The obligations of all company RA's and end users are to take all the necessary precautions to keep their PSEs (user profiles) private and secure and to inform the certification authority of any loss or compromise of their keys immediately.

To understand the purposes and uses of the security software and to use it in the appropriate manner as laid down in this CPS

9.3 Fees

No standard fees will be charged until the GEMISIS project is complete (December 1988). Thereafter, TrueTrust Ltd. will provide the same service at a commercial rate if the directors deem such a service to be viable. However fees will be charged during the GEMISIS project, at the applicable rate, for any re-keying and re-training that needs to be provided due to key compromise, key loss, or inappropriate security procedures by the customer.

9.4 Applicable laws of business

This CPS is governed by the laws of the United Kingdom.

9.5 Arbitration

In the event of a dispute the parties agree to have their case heard by an independent arbiter appointed by the British Computer Society.

10. Policy Administration

The authorities responsible for the operation of this CPS are Manchester TEC and The University of Salford/GEMISIS 2000 project.

This is a working document and thus changes to this document can be made without prior notification.

This CPS is available on the World Wide Web from TrueTrust Ltd. at <http://www.Trustrust.ltd.uk>.

The contact person regarding this document is:

Dr D W Chadwick, IT Institute, University of Salford, M5 4WT. Tel +44 (0)161 745 5351 Fax +44 (0) 161 745 8169 Email D.W.Chadwick@iti.salford.ac.uk

This document is protected by copyright laws and no part of this document may be published, copied, circulated or used either in part or in its entirety without the prior written notification and permission of TrueTrust Ltd. However, the complete document may be copied and used for personal study on the condition that it is clearly and prominently stated that it is the property of TrueTrust Ltd, and this copyright notice accompanies such a copy at all times.

11. Appendix A The Service Contract with Manchester Training and Enterprise Council

The following clause is incorporated in a covering letter sent by the TEC to the customers of the TVC.

Clause on Security Service

An optional security service is available which allows the customer to encrypt data files stored on his computer, and to send and received encrypted and digitally signed electronic mail messages across the Internet and between TVC members. This optional service is provided free of charge to the customer for the first end user license, under the terms and conditions specified in Appendix Z. If the customer wishes to partake of this service, they agree to be bound by the terms and conditions specified in Appendix Z.

Appendix Z to Company Contract with Manchester TEC

The University of Salford, as a member of the GEMISIS 2000 project, is offering members of The Virtual Chamber a unique opportunity to enjoy the benefits of a pilot project at the cutting edge of technology. The project "Secure Use of the Internet", is offering members a Trusted Third Party (TTP) authentication and certification authority service, using the very latest advances in encryption and digital signature techniques.

The authentication and certification services will allow members to reap the low cost benefits of the Internet, with the added security measures normally only associated with private networks. The services will provide the following facilities:

- **Message and File Integrity** - this ensures that a message or file has not been tampered with or altered during storage or transfer,
- **Sender Authentication** - this confirms the origin of a message or file,
- **Message Non-repudiation** - through unique digital signatures and authenticated acknowledgements both dispatch and receipt of a message can be confirmed (making subsequent denial hard to substantiate)
- **Message and File Confidentiality** - this ensures that only authorised people can read a message or file.

These facilities will give members a viable method of conducting secure electronic commerce over the Internet.

Those who take up the security services will receive:

- **easy to use high security software**
- **a zero-cost license until December 1998**
- **free installation and training**
- **a key management service**
- **advice from leading experts in the field**
- **an infrastructure on which to build secure electronic commerce practices over the Internet**
- **access to a Best Practice Guide.**

The security software being used for this project is the market leading product in the field and has previously been used only by governments and large or multinational companies. It has been developed by Entrust Technologies (a subsidiary of Northern Telecom), one of the world's leading security software developers.

The Certification Authority providing the security services is conducted in accordance with procedures laid down in a Certification Practice Statement (CPS). These procedures govern how the Certification Authority will operate technically and deliver the authentication and certification services to its members. The CPS is available for all members to inspect by contacting Dr D W Chadwick at the IT Institute, University of Salford, telephone 0161 745 5351. The CPS has been developed in accordance

with ISO9000 accreditation standards and guidelines being developed by the Internet PKIX working group. It will evolve with time in order to include all the latest advances and improvements to ensure that a state of the art service is delivered at all times.

11.1 Schedule B Entrust/Client Software License

(see separate document)

12. Appendix B The Certificate End User Verification Form

This form must be completed and digitally signed by the Authentication Registrar, and sent electronically to the GEMISIS CA. The Authentication Registrar may optionally wish to print out the form and have it traditionally signed by the applicant and himself for his own records. The completed form will be printed, filed and stored electronically by the GEMISIS CA, along with the digital signature. The applicant whose details are on this form will be registered and a digitally signed encrypted message will be sent back to the Authentication Registrar containing the Entrust Authorisation Information. The Authentication Registrar can then install the Entrust Client on the end user's system.

GEMISIS CA Authentication Registrar Certificate End User Verification Form	
Name of Company : Address of Company:	
Name of Applicant:	
Position in the Company:	
Responsibilities and Duties:	
Number of years at the Company:	
The Applicant has read and understands the Certification Practice Statement and agrees to abide by it.	
Name Of Certificate End User (as it is to appear in Entrust Client): Signature of Applicant: Date:	
The Authentication Registrar on behalf of his company has personally verified that the above Applicant has been authorised to have a certificate issued to him in the name of Certificate End User, and agrees to abide by the rules of the CPS. The company takes complete and sole responsibility for decisions made by their nominated Authentication Registrar.	
Name of Authentication Registrar : Signature of Authentication Registrar: Date:	
For internal use only Received by:	

Date:

13. Appendix C The Entrust Authorisation Information Form

GEMISIS CA Authentication Registrar Entrust Authorisation Information for Certificate End User	
Name of Company : Address of Company:	
Name of Applicant:	
Name Of Certificate End User (as it appears in Entrust Client):	
Name of Authentication Registrar:	
Entrust Reference Number (8 digits)	
Entrust Authorisation Code (12 chars):	
Suggested Entrust User ID (max 8 chars):	

14. Appendix D. The Ethical Policy of the GEMISIS CA

The GEMISIS CA will not knowingly aid or abet the use of the Internet for the following activities:

- transmission of pornographic material
- money laundering
- trafficking in drugs
- production, supply or trading in instruments of torture
- production, supply or trading in weapons where they may be used for offensive, oppressive or terrorist activity
- production of tobacco and tobacco based products
- any activity which purposefully causes a serious negative impact on the environment
- criminal activity of any kind

Applicants to the GEMISIS CA must complete the following Ethical Use of the Internet self certification form. The decision to accept or reject an application rests solely with the GEMISIS CA.

Ethical Use of the Internet Self Certification Form	Yes	No
Do you manufacture or sell military equipment for export?	Please state countries:	
Do you manufacturer or sell instruments of torture?		
Have you contravened any environmental legislation or regulations?	Please attach details	
Do you grow tobacco or manufacture tobacco products?		
Are you involved with pornographic material?		
Are you involved in criminal activity of any kind?		

Appendix 9 - Technophobia Measurement Instruments Information

These tests were devised by Larry D. Rosen, Deborah C. Sears and Michelle M. Weil¹ based on the completed questionnaires of a large number of users.

COMPUTER ANXIETY RATING SCALE (Form C)					
The items in this questionnaire refer to things and experiences that may cause anxiety or apprehension. For each item, place a check under the column that describes how anxious (nervous) each one would make you at this point in your life.					
	Not at All	A Little	A Fair Amount	Much	Very Much
1. Thinking about taking a course in a computer language					
2. Taking a test using a computer scoring sheet					
3. Applying for a job that requires some computer training					
4. Sitting in front of a home computer					
5. Watching a movie about an intelligent computer					
6. Looking at a computer printout					
7. Getting "error messages" from the computer					
8. Using the automated bank teller machine					
9. Visiting a computer store					
10. Being unable to receive information because the "computer is down"					
© 1985, 1988 Larry D. Rosen, Deborah C. Sears and Michelle M. Weil					

COMPUTER THOUGHTS SURVEY (Form C)					
Please check the box that indicates how often you currently have each of the following thoughts when you use a computer or think about using a computer.					
	Not at All	A Little	A Fair Amount	Much	Very Much
1. I am going to make a mistake.					
2. This will be fun.					
3. Everyone else knows what they are doing.					
4. I enjoy learning about this.					

¹ www.technostress.com

5. I like playing on the computer.					
6. I feel stupid.					
7. People will notice if I make a mistake.					
8. This will shorten my work.					
9. I am totally confused.					
10. I know I can do it.					
© 1988 Michelle M. Weil and Larry D. Rosen					

GENERAL ATTITUDES TOWARD COMPUTERS SCALE (Form C)					
The following statements address general attitudes toward computers. Place a check under the column that describes your level of agreement (Strongly Agree, Agree, Neutral, Disagree, or Strongly Disagree) to each statement.					
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1. Computers can save people a lot of work.					
2. It takes a good math background to learn to use a computer.					
3. You need to know how to use a computer to get a good job.					
4. Computers can help solve society's problems.					
5. Computers are taking over.					
6. Computers can increase control over your own life.					
7. Computers increase the amount of time we have for other activities.					
8. Men are better with computers than women.					
9. Computers may eventually act independently of people.					
10. In the future there will still be jobs that don't require computer skills.					
© 1985, 1988 Deborah C. Sears, Larry D. Rosen and Michelle M. Weil					

Appendix 10 - CA Validation Forms

The series of forms were developed as a part of the process of verifying and validating users of the Certification Authority. The forms had to be completed in order to ensure that each respective member is a trusted member and they are who they claim to be.

Once the forms were received and the verification procedures were found to be completed in a positive way, then the user was given a unique key.

The Appendices referred to in pages 323-348 are appendices located within the series of forms only and do not refer to the Appendices in this PhD study.

Gemisis CA (TT1A)

Agreement to Subscribe to the Secure Certification Services

Contact Name:		Position :	
Company Name & Status (private, Ltd., plc):			
Contact Postal Address:			
Company Telephone Number:		Fax Number:	
Contact E-Mail Address:			
Registered Office: (If different from above)			
Are you a Subsidiary company or part of a group of companies?			<input type="checkbox"/> Yes <input type="checkbox"/> No
If Yes please state the main name and address of the Group or parent Company and the percentage owned by them			
Number of employees:			
What are your main business activities?			
What is your current turnover?			
What are your current e-mail and Internet facilities?			

PLEASE STATE:			
Name and address of Bank referee			
Name and address of Trade referee 1			
Name and address of Trade referee 2			
PLEASE LIST THE NAMES OF PEOPLE WHO ARE AUTHORISED TO ACT ON BEHALF OF THE COMPANY IN APPROVING EMPLOYEES TO HOLD DIGITAL SIGNATURES ISSUED ON BEHALF OF THE COMPANY			
NAME: (Block Caps)		POSITION:	
SIGNATURE:		DATE:	
NAME: (Block Caps)		POSITION:	
SIGNATURE:		DATE:	
NAME: (Block Caps)		POSITION:	
SIGNATURE:		DATE:	
NAME: (Block Caps)		POSITION:	
SIGNATURE:		DATE:	
We have read the terms and conditions of this contract and agree to abide by them.			
SIGNED		POSITION	
NAME (BLOCK CAPS)		DATE	

Please apply company stamp here.

Gemisis CA (TT1b) Ethical Business Policy		
Please note that Gemisis CA operate an ethical business policy. In order to assess your ethical status, please complete the following:		
Name Of Applicant :		
Address of Applicant:		
	Yes	No
Do you manufacture or sell military equipment for export?	Please state countries:	
Do you manufacturer or sell instruments of torture?		
Have you contravened any environmental legislation or regulations?	Please attach details	
Do you grow tobacco or manufacture tobacco products?		
Are you involved with pornographic material?		
Are you involved in criminal activity of any kind?		

Appendix B - Bank reference request

Dear Sirs,

Company X has applied to become a member of TrueTrust Ltd Certification Authority. Our company offers security services which enable members of the business community to use the Internet securely. All prospective members of our certification authority must pass a series of verification procedures before we can provide prospective customers with the respective security services .

Thus we request that you complete the following questions and return the enclosed form by post, stamped with the official Bank stamp and signed by yourselves. We thank you in advance for replying by return as any delays will be detrimental to your customer.

We appreciate your kind co-operation.

Yours faithfully,
p.p. Gemisis CA

GEMISIS CA
Request for Bank References

Name Of Applicant :

Address:

**Number of years in
business:**

**Number of years
dealing with your
Bank:**

**Name of applicant
company's
Owner/ Managing
Director:**

Other Directors:

Signed :

Name (in block letters):

Date :

**Bank Name and
Address:**

Telephone :

Fax:

E-mail :

**Please stamp with the
official Bank Stamp:**

Appendix C - Trade reference request

Dear Sirs,

Company X has applied to become a member of TrueTrust Certification Authority. Our company offers security services which enable members of the business community to use the Internet securely. All prospective members of our certification authority must pass a series of verification procedures before we can provide prospective customers with the respective security services .

Thus we request that you complete the following questions and return the enclosed form by post, stamped with the official company stamp and signed by yourselves. We thank you in advance for replying by return as any delays will be detrimental to your customer.

We appreciate your kind co-operation.

Yours faithfully,
p.p. Gemisis CA

**GEMISIS CA
Request for Trade References**

Name Of Applicant :

Address:

**Number of years
trading:**

**Contact Name at
Company X :**

**Name of Owner/
Managing Director:**

Signed :

Name (in block letters):

Date :

**Bank Name and
Address:**

Telephone :

Fax:

E-mail :

**Please stamp with the
official Company**

Stamp:

Gemisis CA

(TT2)

Companies House registration check list

Company Name:		
Company Address:		
Year of Incorporation:		
Turnover Current Year: Previous Year:		
Directors:		
Checked by:		
FOR INTERNAL USE ONLY		

TrueTrust Ltd. (TT3)

Verification Check List

Contact Name:			
Company Name:			
Address:			
Address and Details Confirmed by:			
Bank		*	
Trade referee 1		*	
Trade referee 2		*	
TrueTrust visit		*	
Ethical Policy Approved			*
Application :			
Accepted		*	
Rejected		*	
Appointment for Installation:			
Date of appointment			
*			
* Signed and dated by a TrueTrust representative			
FOR INTERNAL USE ONLY			

Appendix F - Appointment confirmation

Dear,

Further to our telephone conversation , we confirm that our technical engineer (*insert name*) will be visiting your site at (*insert address*) on (*insert date and time*).

Please make sure that the person you have nominated to be responsible for using this software is available for at least 3 hours in order to allow our engineer to provide instructions in the use of the software. Also please make sure that you think about a password - a minimum of 8 characters - at least one of which should be upper case, one of which should be lower case and one of which should be a number.

We remind you that there is also a help-desk available for any queries which might arise after installation.

If you wish to change the appointment please contact us at least 2 days in advance to allow us to re-arrange our engineer's schedules.

Your sincerely,

Appendix G - Letter of denied membership

Dear

Unfortunately, your application to TrueTrust Ltd. for certification has been unsuccessful.

Enclosed please find a cheque for the original amount remitted less £25 deducted to cover administration costs.

If you have any queries please do not hesitate to contact us.

Yours sincerely,

**Gemisis CA (TT6)
Confirmation of Installation**

Contact Name		Position :	
Company Name:			
Postal Address:			
Telephone Number:		Fax Number:	
Date of Installation:			
Time of arrival :			
Time of completion:			
The Entrust Software was successfully installed and I confirm that I have been shown how to use the system			
Company representative			
Name:			
Signed:			
Date:			
Gemisis CA Engineer			
Name:			
Signed:			
Date:			

Gemisis CA

Revocation Form

Company Name:			
Postal Address:			
Telephone Number:		Fax Number:	
Revocation Request Details			
Communicated by:			
<input type="checkbox"/> Telephone			
<input type="checkbox"/> E-mail			
<input type="checkbox"/> Fax			
<input type="checkbox"/> Other (please state)			
.....			
Details of certificate to be revoked			
Name of user :			
Revocation Request Authorised by - Name of Company Representative:			
Position :			
Date and Time of revocation request:			
Date and Time revocation carried out:			
*Signed			
* Signed and dated by a TrueTrust representative			
FOR INTERNAL USE ONLY			

Gemisis CA

Help Desk Enquiry

Contact Name:			
Company Name:			
Postal Address:			
Telephone Number:		Fax Number:	
Date and Time Contacted:			
Details of the enquiry:			
Action taken by Helpdesk			
Length of Course:			
*Signed			
* Signed and dated by a TrueTrust representative			
FOR INTERNAL USE ONLY			

**Gemisis CA (TT5B)
Authentication Registrar
Certificate End User Verification Form**

Name of Company :	
Address of Company:	

Name of Applicant:	
---------------------------	--

Position in the Company:	
---------------------------------	--

Responsibilities and Duties:	
-------------------------------------	--

Number of years at the Company:	
--	--

The Applicant has read and understands the Certification Practice Statement and agrees to abide by it.

Name Of Certificate End User (as it is to appear in Entrust Client):	
Signature of Applicant:	
Date:	

The Authentication Registrar on behalf of his company has personally verified that the above Applicant has been authorised to have a certificate issued to him in the name of Certificate End User, and agrees to abide by the rules of Gemisis CA's CPS. The company takes complete and sole responsibility for decisions made by their nominated Authentication Registrar.

Name of Authentication Registrar :	
Signature of Authentication Registrar:	
Date:	

For internal use only	
Received by:	Date:

**Gemisis CA (TT5C)
Authentication Registrar
Entrust Authorisation Information for
Certificate End User**

Name of Company :

**Address of
Company:**

Name of Applicant:

**Name Of
Certificate End
User (as it appears
in Entrust Client):**

**Name of
Authentication
Registrar:**

**Entrust Reference
Number (8 digits)**

**Entrust
Authorisation Code
(12 chars):**

**Suggested Entrust
User ID (max 8
chars):**

Gemesis CA (TT4B)
Entrust Authorisation Information for
Certificate End User

Name of Company :	
Address of Company:	
Name of Applicant:	
Name Of Certificate End User (as it appears in Entrust Client):	
Entrust Reference Number (8 digits)	
Entrust Authorisation Code (12 chars):	
Suggested Entrust User ID:	
Date and time of Appointment:	

Gemisis CA (TT5A)
Nomination Form for Authentication Registrar

Name of Company :	
Address of Company:	
Name Of Nominee:	
Position in the Company:	
Responsibilities and Duties :	
Number of years at the Company:	
The Nominee has read and understood the requirements of the role of Authorisation Registrar and agrees to undertake the role.	
Signature of Nominee:	
Date:	
The proposers on behalf of their company have read and understood the requirements of the role of Authorisation Registrar and have nominated the above named person to fulfil this role. The company takes complete and sole responsibility for decisions made by their nominated Authorisation Registrar.	
Name of First Proposer (Owner/ Managing Director):	
Signature of first proposer:	
Date:	
Name of Second Proposer (Senior Manager/Director):	
Signature of second proposer:	
Date:	
Company Stamp:	
For internal use only	Received by:
	Date:

**Gemisis CA (TT4A)
Certificate End User Application Form**

Name of Company :	
Address of Company:	
Name of End User:	
E-mail address:	
Position in the Company:	
Number of years at the Company:	
Name Of Certificate End User (as it is to appear in Entrust Client):	
Signature of End-user:	
Date:	
<p>The above Applicant has been authorised to be issued with a digital certificate on behalf of the above named company and agrees to abide by the rules of the CPS. The company takes complete and sole responsibility for decisions made by their representative below.</p>	
Name of Authorised Company representative:	
Signature of Authorised Company representative.	
Date:	
<p>For internal use only</p>	
Received by:	Date:

**ENTRUST/CLIENT SOFTWARE LICENSE
(TT7)**

GRANT OF LICENSE: Subject to the terms and conditions of this license agreement, Entrust Technologies Limited., an Ontario corporation (Entrust), hereby grants the customer ("Customer") the non-exclusive right to use the following number of copies of Entrust software (the "Software"):

The SOFTWARE will remain the sole and exclusive property of Entrust and its technology providers, including any related copyright, trademark, and patent rights.

RESTRICTED USE: Customer may make an additional copy only for back-up or archival reasons for each computer where the Software is installed. Customer may not modify or otherwise copy the Software. Customer may not reverse engineer, de-compile or disassemble the Software. Customer may make one copy the Software documentation for each copy of the Software licensed. Customer shall hold the Software in confidence for the benefit of Entrust.

NO WARRANTIES: To the extent permitted by law, Entrust disclaims all warranties and conditions, either express or implied, including but not limited to implied warranties of non-infringement of intellectual property rights, merchantability and fitness for a particular purpose, with respect to the SOFTWARE and the accompanying written materials.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES: In no event shall Entrust be liable for any consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption or loss of business information) arising out of the use of or inability to use the Software.

EXPORT RESTRICTIONS: Export of the Software outside of the United Kingdom may require approval of the appropriate Government export and import authorities.

TRANSFER: Customer may only transfer its rights under this Agreement if Customer transfers all copies of the Software and all written materials, and the recipient agrees to the terms of this Agreement. Any transfer must include the most recent update of the Software and all prior versions. Entrust may, without notice and without Customer's consent, transfer this Agreement to an affiliate carrying on business in the jurisdiction where Customer's address is located.

TERMINATION: Entrust may terminate this Agreement if Customer or Customer's permitted assignee breaches this Agreement and such breach remains unremedied for 30 days.

GOVERNING LAW: This Agreement is governed by the laws of England..

Should you have any questions concerning this Agreement, or if you wish to contact Entrust for any reason, please write Entrust Technologies Limited, 750 Heron Road, Suite E08, Ottawa, Ontario K1V 1A7 Canada.

IN WITNESS WHEREOF, the Customer has signed this Agreement on the date noted below:

Customer

By: _____
Authorized Representative

Name: _____

Title: _____

Date: _____

Address: _____

Address: _____

The Service Contract with Manchester Training and Enterprise Council

The following clause is incorporated in a covering letter sent by the TEC to the customers of the TVC.

Clause on Security Service

An optional security service is available which allows the customer to encrypt data files stored on his computer, and to send and received encrypted and digitally signed electronic mail messages across the Internet and between TVC members. This optional service is provided free of charge to the customer for the first end user license, under the terms and conditions specified in Appendix Z. If the customer wishes to partake of this service, they agree to be bound by the terms and conditions specified in Appendix Z.

Appendix Z to Company Contract with Manchester TEC

Dear Subscriber

As you will know, as part of your Virtual Chamber Subscription, you may take advantage of a computer security service made available to you at no cost by the University of Salford. Further details are set out in Appendix One.

As you will appreciate, there are certain conditions which must be observed by you if you decide to take the service. We are not able to enter into separate discussions with each potential customer about these conditions and they must therefore be accepted as presented if you are to take the service. The conditions are as follows:

1. You will give us the contact name and address of two trade referees and a bank referee and authorise them to complete a reference form which we will supply. (If there are any charges raised for this, you will have to meet them).
2. The service the University offers to you requires the use of software from a company called Entrust Technologies. That software will be provided under the terms of Entrust Technology's Software License, which is set out in Appendix Two. You must sign and at all times observe the conditions of the License.
3. We will do our best to install the software at your site within 30 days of your agreeing to take the service, and to support the installation as provided in Appendix One.
4. It will be your sole responsibility to ensure the key issued to you and your unique password are kept secure. We will have to charge you for any new keys. You

must inform us immediately one of your certified users leaves you, or when you suspect a key or password has been compromised.

5. You will allow us (or our agents) to audit your use of the service, and for this you will provide us with such information as we require.
6. You will appreciate that your use of the service presents research opportunities to the University, and because of that we offer it to you at no cost. In return, we require you to provide to our researcher reasonable access to appropriate members of your staff and that they provide reasonable assistance and information for the purposes of the research project. (We would expect this to involve you for approximately two hours in each six month period).
7. Given that our provision of the services is at no cost to you, and that the research nature of our interest, you accept that the University cannot accept any liability whatsoever to you or any other person in respect of any failure, delay or suspension of any aspect of the service or any claims, damages, loss or expense of any kind arising from the use of the services, or from any other involvement we may have (except for claims in negligence involving death or personal injury).
8. We can terminate at any time your use of the service if we have reasonable grounds to believe that you are in breach of any of these conditions or conditions relating to your membership of the Virtual Chamber.

We hope that you will wish to take up the services, and will indicate this, and your acceptance of the above conditions, by signing and returning the Entrust Software Licence to Dr D W Chadwick, IT Institute, University of Salford, M5 4WT.

Yours sincerely

E O Evans, Legal Officer, University of Salford

Appendix One

The University of Salford, as a member of the GEMISIS 2000 project, is offering members of The Virtual Chamber a unique opportunity to enjoy the benefits of a pilot project at the cutting edge of technology. The project "Secure Use of the Internet", is offering members a Trusted Third Party (TTP) authentication and certification authority service, using the very latest advances in encryption and digital signature techniques.

The authentication and certification services will allow members to reap the low cost benefits of the Internet, with the added security measures normally only associated with private networks. The services will provide the following facilities:

- **Message and File Integrity** - this ensures that a message or file has not been tampered with or altered during storage or transfer,
- **Sender Authentication** - this confirms the origin of a message or file,
- **Message Non-repudiation** - through unique digital signatures and authenticated acknowledgements both dispatch and receipt of a message can be confirmed (making subsequent denial hard to substantiate)
- **Message and File Confidentiality** - this ensures that only authorised people can read a message or file.

These facilities will give members a viable method of conducting secure electronic commerce over the Internet.

Those who take up the security services will receive:

- **easy to use high security software**
- **a zero-cost license until December 1998**
- **free installation and training**
- **a key management service**
- **advice from leading experts in the field**
- **an infrastructure on which to build secure electronic commerce practices over the Internet**
- **access to a Best Practice Guide.**

The security software being used for this project is the market-leading product in the field and has previously been used only by governments and large or multinational companies. It has been developed by Entrust Technologies (a subsidiary of Northern Telecom), one of the world's leading security software developers.

The Certification Authority providing the security services is conducted in accordance with procedures laid down in a Certification Practice Statement (CPS). These procedures govern how the Certification Authority will operate technically and deliver the authentication and certification services to its members. The CPS is available for all members to inspect by contacting Dr D W Chadwick at the IT Institute, University of Salford, telephone 0161 745 5351. The CPS has been developed in accordance with ISO9000 accreditation standards and guidelines being developed by the Internet PKIX working group. It will evolve with time in order to include all the latest advances and improvements to ensure that a state of the art service is delivered at all times.

Appendix Two ENTRUST/CLIENT SOFTWARE LICENSE

GRANT OF LICENSE: Subject to the terms and conditions of this license agreement, Entrust Technologies Limited., an Ontario corporation ("Entrust"), hereby grants the customer ("Customer") the non-exclusive right to use the following number of copies of Entrust software (the "Software"):

The SOFTWARE will remain the sole and exclusive property of Entrust and its technology providers, including any related copyright, trademark, and patent rights.

RESTRICTED USE: Customer may make an additional copy only for back-up or archival reasons for each computer where the Software is installed. Customer may not modify or otherwise copy the Software. Customer may not reverse engineer, de-compile or disassemble the Software. Customer may make one copy the Software documentation for each copy of the Software licensed. Customer shall hold the Software in confidence for the benefit of Entrust.

NO WARRANTIES: To the extent permitted by law, Entrust disclaims all warranties and conditions, either express or implied, including but not limited to implied warranties of non-infringement of intellectual property rights, merchantability and fitness for a particular purpose, with respect to the SOFTWARE and the accompanying written materials.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES: In no event shall Entrust be liable for any consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption or loss of business information) arising out of the use of or inability to use the Software.

EXPORT RESTRICTIONS: Export of the Software outside of the United Kingdom may require approval of the appropriate Government export and import authorities.

TRANSFER: Customer may only transfer its rights under this Agreement if Customer transfers all copies of the Software and all written materials, and the recipient agrees to the terms of this Agreement. Any transfer must include the most recent update of the Software and all prior versions. Entrust may, without notice and without Customer's consent, transfer this Agreement to an affiliate carrying on business in the jurisdiction where Customer's address is located.

TERMINATION: Entrust may terminate this Agreement if Customer or Customer's permitted assignee breaches this Agreement and such breach remains unremedied for 30 days.

GOVERNING LAW: This Agreement is governed by the laws of England

Should you have any questions concerning this Agreement, or if you wish to contact Entrust for any reason, please write Entrust Technologies Limited, 750 Heron Road, Suite E08, Ottawa, Ontario K1V 1A7 Canada.

IN WITNESS WHEREOF, the Customer has signed this Agreement on the date noted below:

Customer

By: _____
Authorized Representative

Name: _____

Title: _____

Date: _____

Address: _____

Address: _____

Address: _____

Appendix 11 - TRAINING PROCEDURES

The following document will lay down the procedures for Training Certification Authority employees.

There are four major areas in which training will be required:

1. Engineers

The responsibilities of the engineers are to install the software at the premises of the client and to train the end-users in the use of the software.

- **Customer Services** : All engineers must understand that they are the physical representation of the certification authority to the client on site. Since the certification authority offers security services, CA representatives must instil trust in the clients. The code of conduct for engineers must at all times be:
 - * Pleasant - in manner showing a willingness to provide on-site service to the satisfaction of the client. If you are in a bad mood or have had a bad day for any reason, keep it to yourself first impressions count. Clients do not want to be the butt of your temper.
 - * Polite - no matter how annoying clients are engineers must be polite at all times - counting to 10 helps and also reminding yourselves that ultimately clients are the source of your salary. If the client becomes too demanding then explain that you are not in a position to authorise such work and refer to a senior member of staff in the CA.
 - * Punctual - of the engineer is going to be late for an appointment he/she must contact the client and inform them of the delay. If the appointment has to be cancelled for any reason, then the client must be informed as soon as possible and at least 48 hours before the appointment date
 - * Patient - end-users do not have the same knowledge as engineers, some are afraid of computers and not confident using them. Engineers must be extremely patient with clients, they must be willing to spend time and answer questions (no matter how basic) courteously and to the satisfaction of the end-user.
- **Technical Installation** : The installation procedures are relatively basic and the engineer should already have a good technical knowledge of hardware configuration and software installation. Thus the training will consist of the following steps:
 - * The engineer will read the manual in advance of the actual training
 - * The engineer will read the CPS in advance of the actual training
 - * The technical director of the certification authority will run through the installation procedures with the engineer in front of the computer

- * The engineer will perform 2 trial installations in the presence of the technical director
- * If on site the engineer is not able to resolve an installation problem by referring to the trouble shooting section of the manual then :
 - ⇒ he/she will contact the technical director by telephone
 - ⇒ If the problem is still not resolved then the engineer will have to contact the software manufacturers. If they are unable to resolve the problem on site, then the engineer will return at a later date after consultation with the software manufacturers.

2. End-users

A presentation will be given to the users explaining the security infrastructure being introduced and giving a live demonstration of the software.(See appendix - presentation)

The level of competence of end-users will vary from the completely inexperienced and terrified to the knowledgeable. But the software is relatively easy to use and so training end-users is not expected to be too time-consuming. The stages are detailed below.

- * First assess the level of the user's competence.
 - ⇒ If they are experienced users and have a good understanding of the technology and the concept of digital certificates, then the engineer may include more advanced explanations of the system configuration.
 - ⇒ If the user is inexperienced do not blind them with science and technical terms. Show them which buttons to press to perform which functions. Make sure they understand in layman's terms exactly what functions the software can perform, how to make the software perform those functions and not to panic in the event of it not working. Give a brief summary of scenarios of the software not working and what to do to make it work. If the users go through the list and still the software does not work then they are advised to contact the GEMISIS CA helpline.
- * Run through the concept of digital signatures, encryption and security.
- * Ensure the users understand the process for creating secure passwords and the importance of not revealing them to anybody. Also that if this is breached, then the CA must be informed immediately for revocation of the certificate.
- * Run through procedures in front of them explaining clearly what you are doing and why you are doing it
- * Let them run through the procedures themselves explaining in their own words what they [Think] they are doing and allow them to ask questions. If they are making mistakes allow them to make those mistakes but correct them immediately afterwards and explain clearly why they made the mistake and how to correct it.

- * If possible show the circumstances in which the software might not work and show the users how to “troubleshoot” .
- * Always make sure that the users understand how and when to use the software. Be patient allow them to ask questions, ask questions of them to make sure they understand. Do not make them nervous or afraid to ask questions.
- * Make sure the users have a copy of the CPS and a copy of the manual and insist upon them the necessity for reading these documents.

3. Administration Staff

Any recruited administration staff should have a working knowledge of MS Access as well as Word and other secretarial experience. The initial training will be an introduction to the CA what it does, what it means . Within a month of the administrator’s recruitment to the company, the installation engineer will train the member of administration staff in the use of certificates , since certified documents will be sent and received on a regular basis.

The responsibilities and training of the admin. Staff are outlined below.

- **Customer Service** - For administration queries only. The same rules apply as those for all employees of the company since they represent the certification authority to the client. The code of conduct for admin. staff at all times must be:
 - * Pleasant - in manner showing a willingness to help to the satisfaction of the client. If you are in a bad mood or have had a bad day for any reason, keep it to yourself first impressions count. Clients do not want to be the butt of your temper.
 - * Polite - no matter how annoying clients are admin. staff must be polite at all times - counting to 10 helps and also reminding yourselves that ultimately clients are the source of your salary. If the client becomes too demanding or rude then explain that you are not in a position to deal with this problem and refer to a senior member of staff in the CA.
 - * Punctual - if you promise the client some information or to telephone with an answer then do it promptly. Nobody likes to be told they will ‘phone back if they are not
 - * Patient - the client might be tetchy, rude or impatient - be calm at all times and spend time and answering questions (no matter how basic) courteously and to the satisfaction of the client. It will pay dividends in the long run. If attacked the best form of defence is to pacify the client. If they do not have an opponent they can’t have a fight. Be the voice of reason and explain you are doing your best to help them.
 - * If the queries are technical politely refer the client to the help-line (including the number)
- **Administration Procedures**

The basis of the administration task is to log every activity that occurs in the company so that it can be traced to its original form. A series of documentation is available for each procedure. The training will include running through each of the procedures, with the relevant documentation explaining how the procedures work. The demonstrating how to access the database and where the files are located for each procedure to be logged in. The administrator will then be allowed to process a set of dummy applications in the presence of a member of senior staff who will question the administrator and perform a series of scenarios for the administrator to perform. The set of procedures are outlined in the CPS and are summarised below

- * Receipt of queries - log client data in database and send information pack.
- * Follow-up queries - if no reply by week 2 contact the applicant
- * Receipt of signed application form and contract - log-in data in database
- * Verification procedures
 - ⇒ send off for trade references and bank reference
 - ⇒ check Companies House registration by visiting select libraries who hold such data (e.g. MBS) or Companies House
 - ⇒ the result of the verification are stated in the documentation initially a senior member of staff will review the verification procedures of the trainee administrator until he/she understand it fully.

4. The Help-Desk/Support Procedures

This will be manned by the technical engineers who have already been trained in customer services and understand the installation and operation procedures of the software. The help-line engineers will have access to a computer with the client software already installed and the manuals so that they can follow the description of the client. All calls will be logged by the engineers and allocated a fault number. If the engineer cannot solve the problem him/herself, then they will forward the query to a senior member of the technical staff who will reply within one working day. If the technical person cannot resolve the query he will contact the software manufacturers and report this to the engineer. The engineer will keep the customer informed of developments and record all outcomes in the log.

Appendix 12 - Training Presentation

SECURE USE OF THE INTERNET

Rana Tassabehji
December 1997

GEMISIS 2000

- A collaboration between:
 - The University of Salford
 - Cable & Wireless
 - The respective Cities of Salford and Manchester
 - Manchester TEC
- Aims & Objectives
 - To develop user driven applications that exploit benefits of the Information Superhighway
 - Assist regeneration of the NW of England

GEMISIS 2000

- Core Areas of research:
 - Education
 - Business
 - Community
 - Health
- Live Projects Include:
 - "TVC" - The Virtual Chamber of Commerce
 - Healthcare project with local hospitals
 - CCTV in Salford

Introduction

- Aims and Objectives
- Security an Overview
- Involvement
- Time Scales
- Security Software Demonstration
- Next Steps

Aims and Objectives

- Best Practice Guide
- Encourage SME use of the Internet securely
- Development of Electronic Commerce
- Achieving competitive advantage
- Doctoral Thesis

SECURITY ISSUES The Apparent

- Physical Security
 - Building access controls
 - Computer bolts and chains
 - Infra-red identification markers
 - Motion sensitive systems
- Network Security
 - Firewalls - (network and application level)
 - Virus Software
 - Password access

SECURITY ISSUES The Over-looked

- Data Security in transition
- Security Policy
- Training and staff co-operation

The Advantages of Data Security

- Privacy
- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

SECURITY

- Data Security
 - Public Key Infrastructure (PKI)
 - Certification Authority (Trusted Third Party TTP)
 - Digital Signatures
 - Encryption

PKI

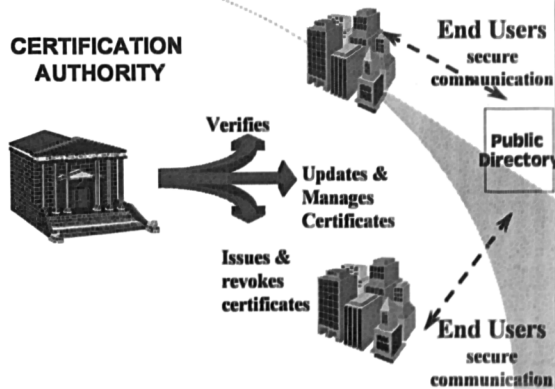
Public Key Infrastructure

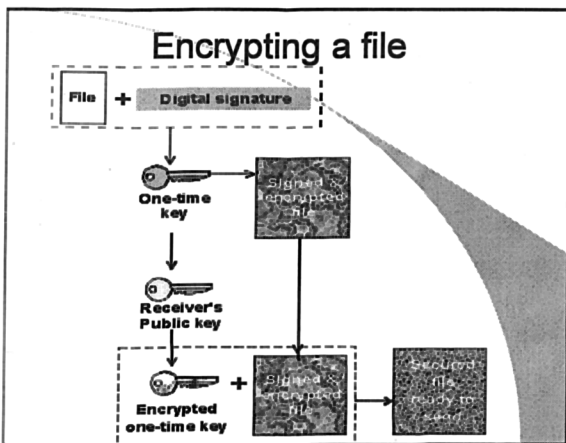
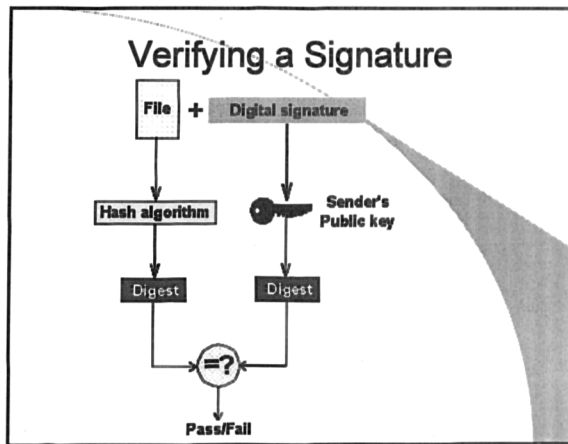
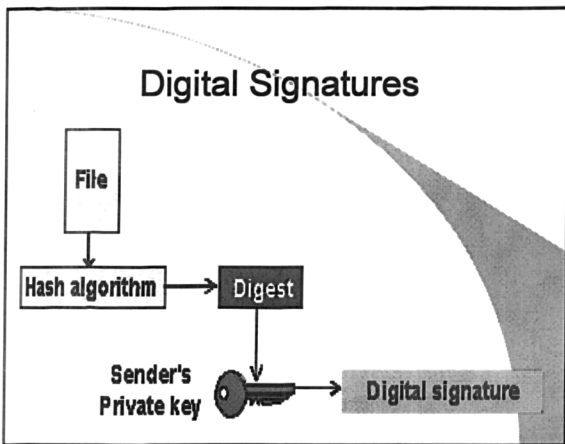
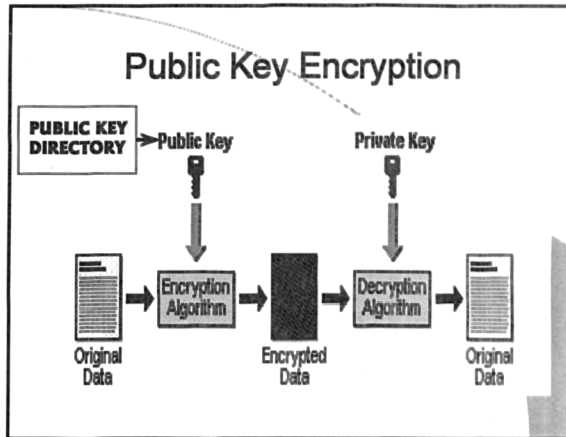
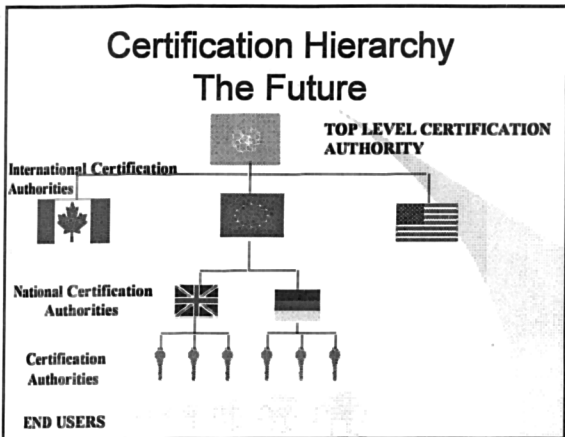
- Cryptographic Keys
 - Manage generation and distribution of public and private key pairs
 - Publish public keys with user's id in a public directory (X.500)
- Certificate delivery system
 - Certification Authorities (CA) or Trusted Third Parties (TTP)

Certification Authority (Trusted Third Party)

- Verifies members
- Manages public key directory (X.509)
- End-user support (back-up and recovery)
- Revokes certificates and publishes revocation lists (CRL's)
- Manages key updates and certificate renewals

CERTIFICATION AUTHORITY

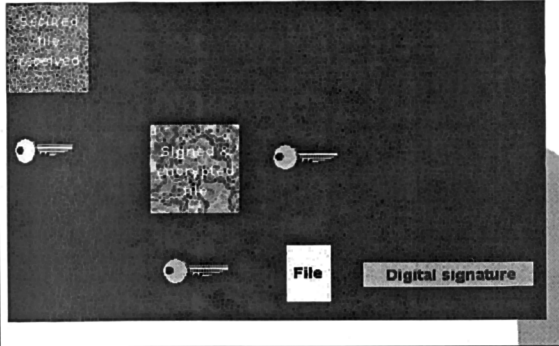




Encrypted Message - An extract

```
[ENTRUST HEADER START]
Proc-Type: 4,ENCRYPTED Content-Domain: RFC822 EntrustFile-Version: 2.0
DEK-Info: CAST1-CBC,S36203A6E1B7F8A0
Originator-Certificate:
+Uskx1B/TXOZNJhA66b11r/ZT1t6+FSbLj/KeyInfo:
RSA,mMe08YdNBDenHn2LaeKsnisgja4f8AVTgSDx5EVOIqhyqYxU9rUlJg==
SMIC-Info: RSA-MD5, RSA,
X3JJaulln4vNM17ofhDBAnVkuTyFKiOGhASH7QWIYICULL2QGspr9VzQCAQ1
QvM49cA6RHxaUBpDGZ+fyb/RfYARWRpBtlyasZJEZWL+9tUd+AF4nFoc16g
zYX18uzhxp8jee90x+TlocYMEPsA==
Recipient-ID-Asymmetric:
MCYxCzAJBgNVBAYTAkdCMRcwFQYDVOQKEw5UenVidHJ1c3QgTHRkLg==36
5002007
Key-Info:
GJafUOpaluHVAvT4HNvup+zCEzSVveyad90k8vocy2/80uzMIm8VjGg==
[ENTRUST HEADER END]
Wk6@9d-HZ6ivE*E8iAmzYVQ 8[]->4bOM_N=>[U0%yp0REM1-μe2m
7%[]?M E8awaa*)J(ε-C8u
```

Decrypting a file



Choice of Certification Methods



Areas of Analysis

- Strategic
 - Formulation
 - Implementation
 - Evaluation
- Technical
 - Software
 - Certification Authority
- End-User

What is involved . . .

- Read and understand Certification Practice Statement (CPS)
- Choice of certification method
- Regular Contact more intensive at first but then once monthly
 - telephone
 - e-mail
 - face-to-face
 - group
 - questionnaires

What you receive . . .

- Security Software - Installation and Training
- Verification of All Certified Members
- Key Management Service
- Advice From Leading Experts in the Field
- An Infrastructure on Which to Build Secure Electronic Commerce Practices Over the Internet
- Access to the Best Practice Guide

Timescales

December 1997	Strategy Review and development
January 1998	Installation Training Initial feedback
February - September 1998	Feedback
October - December 1998	Procedures Audit End of Free licence

**ENTRUST Technology
Security Software
Demonstration**

Next Steps . . .

- Complete application form
- Agree Contracts
- Read Certification Practice Statement
- Agree date for installation and training
- Agree contacts and how to proceed
- Other issues raised

Appendix 13 Entrust Software User Guide

From Pegasus – De-encrypting an attached file

Click on the attached file

Then click on save and view

Save in the directory and name the file as you want it BUT do not change the extension of the document – so the file should always be e.g examquestions.ent

Then carry on the procedure as follows:

A. Log On Procedure

In order to log onto Entrust, locate your personal entrust profile file (yourname.epf)¹ select it and enter. This should automatically be there so just type in your password².

Select the option you require from:

- Encrypt and Sign** – which allows you to encrypt documents³, encrypt and digitally sign documents⁴ or solely digitally sign documents⁵
- Decrypt and Verify** – which allows you to decrypt documents received and verify that they are in the same state that they were sent and the origin of the sender.
- Recipients List** – creates a list of recipients and options for encrypting and signing documents
- Secure Delete** – allows secure deletion of data files

*** NB From within Pegasus the Decrypt and verify option will automatically launch please follow the decrypt and verify instructions (C)**

B. Encrypt and Sign

1. Select the file to be encrypted and/or signed from the directory
2. Click on open
3. If you wish to select more than one file, locate the required files from the directory and “Add” them to the source files list.
4. Select one of the following options from the right hand side of the screen

¹ This will have been generated at the registration and installation stage. This is stored either on a floppy disk or in the PC's directory

² Your password must be made up of a minimum of 8 characters of which there must be letters of the alphabet and numbers. For added password safety, it is advised that you incorporate alphanumeric characters, mix upper and lower case letters and do not use familiar or common words or names.

³ For confidential documents

⁴ For confidential documents and documents where the recipient can be assured that the document originates from the sender

⁵ For documents where the recipient can be assured that the document originates from the sender

- ENCRYPT DOCUMENTS** – this allows users to encrypt a document. Users can encrypt the document for themselves only to decipher or select from the list of recipients able to decipher the document (see point 5.)
 - ENCRYPT AND DIGITALLY SIGN DOCUMENTS** – this allows users to encrypt the document as above and also digitally sign the document to enable the recipient to validate the authenticity of the document’s sender.
 - SIGN DOCUMENTS** – this option allows users to digitally sign non-confidential documents
5. To enable others to decrypt a document, select the **RECIPIENTS LIST** and click on **ADD** recipients.
 6. Select the required name(s) from the authorised and verified members in the TrueTrust Directory. The search criteria is initially by organisation name. Select the required organisation name, this will reveal a list of verified individuals within the organisation. To speed up the search, type in the last name of the individual required in the space indicated. Clicking on the “magnifying glass” icon, will launch the search of the directory.
 7. Once the required individual is located, highlight the name and “**ADD**” to the list of recipients who will be able to decrypt the document(s). Selected individuals can be removed by highlighting them in the recipient list and clicking “**REMOVE ALL**”.
 8. To check the details of the selected individual, highlight the name and click on “**Recipient Information**”.

The **OUTPUT** option offers the following:

- In Place** – This will store the encrypted/signed file(s) in the same place as the original file(s) on the PC’s directory
- To Directory** – This will allow the user to store the encrypted/signed file(s) anywhere on the PC’s directory
- To Mail** – This option is only active with an Entrust e-mail package plug-in.

DELETE SOURCE FILE – This option which should be clicked for selection, allows the user to delete the original file(s) which have been selected for encryption/signing. Once the original file has been deleted it cannot be retrieved.

MORE OPTIONS . . . – This is for more advanced users and users are advised to retain the default options

- Source files** – compress data files this reduces the size of the files encrypted
- Destination files** – this indicates the type of file and the file extension
- Encryption Method** – the most secure is triple DES and CAST 128

Once these have been completed then click on **OK** and the selected files will have encrypted/signed. A screen confirming that the file(s) have been encrypted/signed appears. If you require more detail, click on **Information** which shows the type of encryption that has occurred and whether the process has been successful or not. If the encryption/signing process has been successful (**Verify status: Successful** and **Last error: No error**), then these files can then either be stored on a floppy disk or PC or sent as an e-mail attachment as required by the user.

C. Decrypt and Verify

1. Select the file to be decrypted and/or verified from the directory
2. Click on **Open**
3. If you wish to select more than one file, locate the required files from the directory and “**Add**” them to the source files list.

The **OUTPUT** option offers the following:

- In Place** – This will store the decrypted/signed file(s) in the same place as the original file(s) on the PC’s directory
- To Directory** – This will allow the user to store the decrypted/signed file(s) anywhere on the PC’s directory e.g. if you have created a special exam directory c:\exam\
- No output** – This allows the user to verify a signature and does not save the decrypted/signed file.

DELETE SOURCE FILE – This option allows the user to delete the original encrypted/signed file(s) which have been selected for decryption/signature validation. Once the original file has been deleted it cannot be retrieved.

Once the file has been selected for decryption/verification of a signature, click on **OK** and the selected files will be decrypted/validated. **Signature information** indicates the owner of the signature and thus the sender of the document and the Certification Authority which has verified and issued the signature to the owner.

The **Information** option gives more detail of the signature and the decryption process. This shows the type of decryption that has occurred and whether the process has been successful or not. If the decryption/verification process has been successful (**Verify status: Successful and Last error: No error**), then these files can be trusted as coming from the owner of the signature.

The **Launch** option is available only when you have selected to save the decrypted/signed file **In Place/ To Directory**. This will launch the decrypted/signed document within the relevant file reader programme.

D. Recipients List

This allows the user to create an encrypted/digitally signed distribution/ mailing list. Click on this option, select the people you wish to add to your list by highlighting and selecting. Then call the list something appropriate which will identify the list of users e.g. exam pilot participants.

E. Secure Delete

This option is for the permanent deletion of files. Select the file intended for deletion by browsing for the file. Once the file is selected and the user has confirmed deletion of the file it cannot be retrieved and the file will be retrieved permanently.

Appendix 14 - Help Desk Enquiry

GEMISIS CA Help Desk Enquiry	
Contact Name:	
Company Name:	
Postal Address:	
Telephone Number:	Fax Number:
Date and Time Contacted:	
Details of the enquiry:	
Action taken by Helpdesk	
Date call terminated:	
*Signed	
* Signed and dated by a TrueTrust representative	
FOR INTERNAL USE ONLY	

Appendix 15 - Questionnaires for Company T

A. Pre Implementation Questionnaire for Participants

1. Name:	
2. Job Description:	
3. Age:	<input type="checkbox"/> <18 <input type="checkbox"/> 25-34 <input type="checkbox"/> 45-54 <input type="checkbox"/> 18-24 <input type="checkbox"/> 35-44 <input type="checkbox"/> >55
4. Please state your educational background (please tick all relevant boxes)	
<input type="checkbox"/> O'Levels/ GCSE <input type="checkbox"/> Degree (BA/BSC) <input type="checkbox"/> Post graduate degree (MSc/MA/PhD) <input type="checkbox"/> A'Levels <input type="checkbox"/> BTEC/HND <input type="checkbox"/> Other (Please specify)	
5. How often do you use a computer at work in a typical week?	
<input type="checkbox"/> Every day <input type="checkbox"/> 4 days <input type="checkbox"/> 3 days <input type="checkbox"/> 2 days <input type="checkbox"/> 1 day <input type="checkbox"/> Rarely <input type="checkbox"/> Never	
6. What do you use the computer at work for?	
<input type="checkbox"/> Word processing <input type="checkbox"/> E-mail <input type="checkbox"/> The Internet <input type="checkbox"/> Spreadsheet <input type="checkbox"/> Presentations <input type="checkbox"/> CAD <input type="checkbox"/> Other (please specify)	
7. What software do you use at work?	
<input type="checkbox"/> Microsoft Works <input type="checkbox"/> MS <input type="checkbox"/> Other (please specify) <input type="checkbox"/> Lotus Notes Outlook <input type="checkbox"/> WordPerfect Pegasus <input type="checkbox"/> Microsoft Office CC.mail <input type="checkbox"/> (Word/Excel/Powerpoint) <input type="checkbox"/> Eudora	
8. Do you use a computer at home? <input type="checkbox"/> Yes <input type="checkbox"/> No (please go to Q10)	
If yes do you use the computer at home for	
<input type="checkbox"/> Word processing <input type="checkbox"/> E-mail <input type="checkbox"/> Presentations <input type="checkbox"/> Games <input type="checkbox"/> Special interest software (e.g. landscape/ <input type="checkbox"/> The Internet interior design/learning languages etc.) <input type="checkbox"/> CAD <input type="checkbox"/> Other (please specify) <input type="checkbox"/> Childrens software	
9. Do you have an Internet connection from home? <input type="checkbox"/> Yes <input type="checkbox"/> No	

Please indicate your level of agreement with the following list of statements					
	Agree Strongly	Agree	Neither/ Nor	Disagree	Disagree Strongly
i. Computers can save people a lot of work					
ii. It takes a good maths background to learn to use a computer					
iii. Computers are taking over					
iv. . Computers increase the amount of time we have for other activities					
v. Men are better with computers than women					
vi. In the future there will be jobs that don't require computer skills					
vii. Computers may eventually act independently of people					
viii. When I use a computer I think this will be fun					
ix. When I use a computer I think I am going to make a mistake					
x. When I use a computer I feel stupid					
xi. When I use a computer I am totally confused					
xii. When I use a computer I think this will shorten my workload					
xiii. Getting a computer error message makes me feel anxious					
xiv. Using the automated bank teller machine makes me feel anxious					
xv. I don't like visiting computer shops					

Many thanks for completing this questionnaire. Please return the completed questionnaire to Rana Tassabehji at the address below. Please note that all the Personal information collected will remain confidential to the originator of this questionnaire.

If you have any queries or problems please contact Rana Tassabehji at the IT Institute, University of Salford, M5 4WT Tel: 0161-745 5482 Fax: 0161-745 8169 Tel: 04100 21709 (Mobile) E-mail: R.Tassabehji@iti.salford.ac.uk

B. Post Implementation Questionnaire

Please complete as indicated. Please note that all information given will be kept confidential.

1. Name:

2a. Have you ever used security/encryption software prior to this project?

Yes No

2b. Please state which security/encryption software you have used prior to this project.

3a. How did you rate the training you received – was it -

Very good Good Adequate Poor Very Poor

3b. Please indicate how the training could have been improved

4a. Please tick the Entrust security software features YOU WERE ABLE TO USE after you were given training?

Signing/Encryption Verification/Decryption Secure Delete

4b. Please explain the nature of the difficulty you experienced

5. How often did you use the following features of the Entrust security software ?

Encryption

- Once
- 2-4 times
- >5 times

Decryption

- Once
- 2-4 times
- 5 or More times

Secure Delete

- None
- Once
- 2-4 times
- 5 or More times

6. What did you use the Entrust security software for? (you may tick more than one option)

- Encrypting document for storage on your pc/floppy drive**
- Encrypting documents for sending by e-mail to an Internal colleague**
- Encrypting/signing documents for sending by e-mail to an external partners**
- Decrypting/verifying documents received from internal colleagues**
- Decrypting/verifying documents received from external partners**
- Secure delete documents (please state which documents)**
- Other tasks (please state which)**

7. Please state any difficulties (Network, hardware or software) or other issues you encountered while using the Entrust security software.

8a. Did you use the Entrust security software using an ISP?

Yes

No (please go to Q9)

8b. If yes , Please state your location (home/work/other location) whether you had any problems and explain the nature of the problem(s)

9a. Do you think that the transmission of documents by e-mail, using security/encryption software has improved your business process?

Yes

No

9b. Please explain why.

10a. Do you think that the transmission of documents by e-mail, using security/encryption software should become the standard process for exchanging business orders and communicating with business partners?

Yes

No

10b. Please explain why.

11a. Would you be prepared to use security software in your business processes again?

Yes

No

11b. Please explain why

Many thanks for completing this questionnaire. Please return the completed questionnaire to Rana Tassabehji at the address below. Please note that all the Personal information collected will remain confidential to the originator of this questionnaire.

If you have any queries or problems please contact Rana Tassabehji at the IT Institute, University of Salford, M5 4WT Tel: 0161-745 5482 Fax: 0161-745 8169 Tel: 04100 21709 (Mobile) E-mail: R.Tassabehji@iti.salford.ac.uk

Appendix 16 - University X - Pre-Implementation Questionnaire

a. Exam Participants Questionnaire (Originator)

This section will deal with personal background questions. Please complete as indicated. Please note that all information given will be kept confidential.		
1. Name:		
2. Job Description:		
3. Age: <input type="checkbox"/> <18 <input type="checkbox"/> 25-34 <input type="checkbox"/> 45-54 <input type="checkbox"/> 18-24 <input type="checkbox"/> 35-44 <input type="checkbox"/> >55		
4. Please state your educational background (please tick all relevant boxes) <input type="checkbox"/> O'Levels/ GCSE <input type="checkbox"/> Degree (BA/BSC) <input type="checkbox"/> Post graduate degree (MSc/MA/PhD) <input type="checkbox"/> A'Levels <input type="checkbox"/> BTEC/HND <input type="checkbox"/> Other (Please specify)		
5. How often do you use a computer at work in a typical week? <input type="checkbox"/> Every day <input type="checkbox"/> 4 days <input type="checkbox"/> 3 days <input type="checkbox"/> 2 days <input type="checkbox"/> 1 day <input type="checkbox"/> Rarely <input type="checkbox"/> Never		
6. What do you use the computer at work for? <input type="checkbox"/> Word processing <input type="checkbox"/> E-mail <input type="checkbox"/> The Internet <input type="checkbox"/> Spreadsheet <input type="checkbox"/> Presentations <input type="checkbox"/> CAD Other (please specify)		
7. What software do you use at work? <input type="checkbox"/> Microsoft Works <input type="checkbox"/> MS <input type="checkbox"/> Other (please specify) <input type="checkbox"/> Lotus Notes Outlook <input type="checkbox"/> WordPerfect Pegasus <input type="checkbox"/> Microsoft Office CC.mail (Word/Excel/Powerpoint) <input type="checkbox"/> Eudora		
8. Do you use a computer at home? <input type="checkbox"/> Yes <input type="checkbox"/> No (please go to Q10) If yes do you use the computer at home for <input type="checkbox"/> Word processing <input type="checkbox"/> E-mail <input type="checkbox"/> Presentations <input type="checkbox"/> Games <input type="checkbox"/> Special interest software (e.g. landscape/ <input type="checkbox"/> The Internet interior design/learning languages etc.) <input type="checkbox"/> CAD <input type="checkbox"/> Other (please specify) <input type="checkbox"/> Childrens software		
9. Do you have an Internet connection from home? <input type="checkbox"/> Yes <input type="checkbox"/> No		

The following section will deal with the examination paper preparation process in your department. Please complete all the questions as indicated

10. What do you think of the current paper based method of examination paper preparation and submission?

11. What problems have you encountered using this method?

12. Do you have a problem submitting your examination questions to the exams office on time?

- No
- Yes (please explain why)

13. In what format do you send examination Questions (Q) and Solutions (S) for: (please tick the relevant boxes)

	Moderator /QA		External Examiner		Exams Administrator	
	Q	S	Q	S	Q	S
All Handwritten						
All Wordprocessed						

Please specify the software package(s) you use

Both handwritten and wordprocessed

Please specify what elements of the Q and S are handwritten and what are wordprocessed

14. How do you send examination Questions (Q) and Solutions (S) to: (please tick the relevant boxes)

	Moderator/QA		External Examiner		Exams Administrator	
	Q	S	Q	S	Q	S
Personally by hand						
Internal mail						
E-mail						
Registered Mail						
External Private Courier (e.g. DHL)						

15a. Would you be prepared to submit/receive examination questions and solutions by E-mail ?

Yes No

If No please explain why.

15b. Do you think electronic submission of examination questions would improve the whole examination submission and preparation process?

Yes No

Please explain why

16. Would you be prepared to submit examination questions and solutions electronically using additional software which guarantees the confidentiality of your text?

Yes No

Please indicate your level of agreement with the following list of statements

	Agree Strongly	Agree	Neither/ Nor	Disagree	Disagree Strongly
i. Computers can save people a lot of work					
ii. It takes a good maths background to learn to use a computer					
iii. Computers are taking over					
iv. . Computers increase the amount of time we have for other activities					
v. Men are better with computers than women					
vi. In the future there will be jobs that don't require computer skills					
vii. Computers may eventually act independently of people					
viii. When I use a computer I think this will be fun					
ix. When I use a computer I think I am going to make a mistake					
x. When I use a computer I feel stupid					
xi. When I use a computer I am totally confused					
xii. When I use a computer I think this will shorten my workload					
xiii. Getting a computer error message makes me feel anxious					
xiv. Using the automated bank teller machine makes me feel anxious					
xv. I don't like visiting computer shops					

many thanks for completing this questionnaire. Please return the completed questionnaire to Rana Tassabehji at the address below. Please note that all the Personal Information collected will remain confidential to the originator of this questionnaire.

If you have any queries or problems please contact Rana Tassabehji at the IT Institute, University of Salford, M5 4WT Tel: 0161-745 5482 Fax: 0161-745 8169 Tel: 04100 21709 (Mobile) E-mail: R.Tassabehji@iti.salford.ac.uk

b. Exam Participants Questionnaire (Administrator)

This section will deal with personal background questions. Please complete as indicated. Please note that all information given will be kept confidential.

1. Name:

2. Job Description:

3. Age: <18 25-34 45-54
 18-24 35-44 >55

4. Please state your educational background (please tick all relevant boxes)

O'Levels/ GCSE Degree (BA/BSC) Post graduate degree (MSc/MA/PhD)
 A'Levels BTEC/HND
 Other (Please specify)

5. How often do you use a computer at work in a typical week?

Every day 4 days 3 days 2 days 1 day Rarely Never

6. What do you use the computer at work for?

Word processing E-mail The Internet Spreadsheet Presentations CAD
Other (please specify)

7. What software do you use at work?

Microsoft Works MS Other (please specify)
 Lotus Notes Outlook
 WordPerfect Pegasus
 Microsoft Office CC.mail
(Word/Excel/Powerpoint) Eudora

8. Do you use a computer at home? Yes No (please go to Q10)

If yes do you use the computer at home for

Word processing E-mail Presentations
 Games Special interest software (e.g. landscape/
interior design/learning languages etc.) CAD
 The Internet Childrens software
 Other (please specify)

9. Do you have an Internet connection from home? Yes No

The following section will deal with the examination paper preparation process in your department. Please complete all the questions as indicated

10. What do you think of the current paper based method of examination paper submission?

11. What problems have you encountered using this method?

13. In what format do you receive examination Questions (Q) and Solutions (S) from: (please tick the relevant boxes)

	Exam Originator		External Examiner		Exams Administrator	
	Q	S	Q	S	Q	S
All Handwritten						
All Wordprocessed						

Please specify the software package(s) you receive them as

Both handwritten and wordprocessed

Please specify what elements of the Q and S are handwritten and what are wordprocessed

14. How do you receive examination Questions (Q) and Solutions (S): (please tick the relevant boxes)

	Moderator/QA		External Examiner		Exams Administrator	
	Q	S	Q	S	Q	S
Personally by hand						
Internal mail						
E-mail						
Registered Mail						
External Private Courier (e.g. DHL)						

15a. Would you be prepared to receive examination questions and solutions by E-mail ?

Yes No

If No please explain why.

15b. Do you think electronic submission of examination questions would improve the whole examination submission and preparation process?

Yes No

Please explain why

16. Would you be prepared to submit examination questions and solutions electronically using additional software which guarantees the confidentiality of the text?

Yes No

Please indicate your level of agreement with the following list of statements

	Agree Strongly	Agree	Neither/ Nor	Disagree	Disagree Strongly
i. Computers can save people a lot of work					
ii. It takes a good maths background to learn to use a computer					
iii. Computers are taking over					
iv. . Computers increase the amount of time we have for other activities					
v. Men are better with computers than women					
vi. In the future there will be jobs that don't require computer skills					
vii. Computers may eventually act independently of people					
viii. When I use a computer I think this will be fun					
ix. When I use a computer I think I am going to make a mistake					
x. When I use a computer I feel stupid					
xi. When I use a computer I am totally confused					
xii. When I use a computer I think this will shorten my workload					
xiii. Getting a computer error message makes me feel anxious					
xiv. Using the automated bank teller machine makes me feel anxious					
xv. I don't like visiting computer shops					

many thanks for completing this questionnaire. Please return the completed questionnaire to Rana Tassabehji at the address below. Please note that all the Personal Information collected will remain confidential to the originator of this questionnaire.

If you have any queries or problems please contact Rana Tassabehji at the IT Institute, University of Salford, M5 4WT Tel: 0161-745 5482 Fax: 0161-745 8169 Tel: 04100 21709 (Mobile) E-mail: R.Tassabehji@itl.salford.ac.uk

10. What do you think of the current paper based method of examination paper receipt and submission?

11. What problems have you encountered using this method?

12. Do you have a problem submitting your examination feedback to the exams administrator on time?

- No
- Yes (please explain why)

13. In what format do you prepare feedback on examination Questions (Q) and Solutions (S) for: (please tick the relevant boxes)

	Exam Originator		Exam Administrator	
	Q	S	Q	S
All Handwritten				
All Wordprocessed				

Please specify the software package(s) you use

Both handwritten and wordprocessed						

Please specify what elements of the Q and S are handwritten and what are wordprocessed

14. How do you send feedback on examination Questions (Q) and Solutions (S) to: (please tick the relevant boxes)

	Moderator/QA		External Examiner		Exams Administrator	
	Q	S	Q	S	Q	S
Personally by hand						
Internal mail						
E-mail						
Registered Mail						
External Private Courier (e.g. DHL)						

15a. Would you be prepared to submit examination questions and solutions by E-mail ?

Yes No

If No please explain why.

15b. Do you think electronic submission of examination questions would improve the whole examination submission and preparation process?

Yes No

Please explain why

16. Would you be prepared to submit examination questions and solutions electronically using additional software which guarantees the confidentiality of your text?

Yes No

Please indicate your level of agreement with the following list of statements

	Agree Strongly	Agree	Neither/ Nor	Disagree	Disagree Strongly
i. Computers can save people a lot of work					
ii. It takes a good maths background to learn to use a computer					
iii. Computers are taking over					
iv. . Computers increase the amount of time we have for other activities					
v. Men are better with computers than women					
vi. In the future there will be jobs that don't require computer skills					
vii. Computers may eventually act independently of people					
viii. When I use a computer I think this will be fun					
ix. When I use a computer I think I am going to make a mistake					
x. When I use a computer I feel stupid					
xi. When I use a computer I am totally confused					
xii. When I use a computer I think this will shorten my workload					

xiii. Getting a computer error message makes me feel anxious					
xiv. Using the automated bank teller machine makes me feel anxious					
xv. I don't like visiting computer shops					

many thanks for completing this questionnaire. Please return the completed questionnaire to Rana Tassabehji at the address below. Please note that all the Personal information collected will remain confidential to the originator of this questionnaire.

If you have any queries or problems please contact Rana Tassabehji at the IT Institute, University of Salford, M5 4WT Tel: 0161-745 5482 Fax: 0161-745 8169 Tel: 04100 21709 (Mobile) E-mail: R.Tassabehji@itl.salford.ac.uk

Appendix 17 - University X - Post Implementation Questionnaire

<p>Please complete as indicated. Please note that all information given will be kept confidential.</p>																	
<p>1. Name:</p>																	
<p>2a. Have you ever used security/encryption software prior to this project?</p> <p style="text-align: center;"><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>2b. Please state which security/encryption software you have used prior to this project.</p>																	
<p>3a. How did you rate the training you received – was it -</p> <p><input type="checkbox"/> Very good <input type="checkbox"/> Good <input type="checkbox"/> Adequate <input type="checkbox"/> Poor <input type="checkbox"/> Very Poor</p> <p>3b. Please indicate how the training could have been improved</p>																	
<p>4a. Please tick the Entrust security software features YOU WERE YOU ABLE TO USE after you were given training?</p> <p><input type="checkbox"/> Signing/Encryption <input type="checkbox"/> Verification/Decryption <input type="checkbox"/> Secure Delete</p> <p>4b. Please explain the nature of the difficulty you experienced</p>																	
<p>5. How often did you use the following features of the Entrust security software in the secure exam pilot project?</p> <table style="width: 100%; border: none;"> <thead> <tr> <th style="text-align: left; width: 33%;">Encryption</th> <th style="text-align: left; width: 33%;">Decryption</th> <th style="text-align: left; width: 33%;">Secure Delete</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Once</td> <td><input type="checkbox"/> Once</td> <td><input type="checkbox"/> None</td> </tr> <tr> <td><input type="checkbox"/> 2-4 times</td> <td><input type="checkbox"/> 2-4 times</td> <td><input type="checkbox"/> Once</td> </tr> <tr> <td><input type="checkbox"/> >5 times</td> <td><input type="checkbox"/> 5 or More times</td> <td><input type="checkbox"/> 2-4 times</td> </tr> <tr> <td></td> <td></td> <td><input type="checkbox"/> 5 or More times</td> </tr> </tbody> </table>			Encryption	Decryption	Secure Delete	<input type="checkbox"/> Once	<input type="checkbox"/> Once	<input type="checkbox"/> None	<input type="checkbox"/> 2-4 times	<input type="checkbox"/> 2-4 times	<input type="checkbox"/> Once	<input type="checkbox"/> >5 times	<input type="checkbox"/> 5 or More times	<input type="checkbox"/> 2-4 times			<input type="checkbox"/> 5 or More times
Encryption	Decryption	Secure Delete															
<input type="checkbox"/> Once	<input type="checkbox"/> Once	<input type="checkbox"/> None															
<input type="checkbox"/> 2-4 times	<input type="checkbox"/> 2-4 times	<input type="checkbox"/> Once															
<input type="checkbox"/> >5 times	<input type="checkbox"/> 5 or More times	<input type="checkbox"/> 2-4 times															
		<input type="checkbox"/> 5 or More times															

6. What did you use the Entrust security software for? (you may tick more than one option)

- Encrypting exam papers for storage on your pc/floppy drive**
- Encrypting/signing exam papers for sending by e-mail to an Internal QA**
- Encrypting/signing exam papers for sending by e-mail to the exam administrator**
- Encrypting/signing exam papers for sending by e-mail to the external examiner**
- Decrypting/verifying exam papers from the Internal QA**
- Decrypting/verifying exam papers from the exam administrator**
- Decrypting/verifying exam papers from the external examiner**
- Decrypting/verifying exam papers from the exam author**
- Secure delete documents (please state which documents)**
- Other tasks (please state which)**

7. Please state any difficulties (Network, hardware or software) or other issues you encountered while using the Entrust security software.

8a. Did you use the Entrust security software using an ISP?

Yes

No (please go to Q9)

8b. If yes , Please state your location (home/work/other location) whether you had any problems and explain the nature of the problem(s)

9a. Do you think that the transmission of examination papers by e-mail, using security/encryption software has improved the examination submission process?

Yes

No

9b. Please explain why.

10a. Do you think that the transmission of examination papers by e-mail, using security/encryption software should become the standard process for examination submission throughout the university?

Yes

No

10b. Please explain why.

11a. Would you be prepared to use security software for the examination submissions process again?

Yes

No

11b. Please explain why

Many thanks for completing this questionnaire. Please return the completed questionnaire to Rana Tassabehji at the address below. Please note that all the Personal information collected will remain confidential to the originator of this questionnaire.

If you have any queries or problems please contact Rana Tassabehji at the IT Institute, University of Salford, M5 4WT Tel: 0161-745 5482 Fax: 0161-745 8169 Tel: 04100 21709 (Mobile) E-mail: R.Tassabehji@iti.salford.ac.uk

Please complete the next section and return with the completed questionnaire in order that we can process it.

Please state whether you wish a £25

- book voucher**
- M&S Voucher**

Please indicate the address where you wish us to send these vouchers.

Appendix 18 - Discussion Guide for Depth Interviews

1. BACKGROUND ON THE CURRENT MEANS OF COMMUNICATIONS

This is to understand from what standpoint the organisation is commenting and provides a valuable background in which to base the information we subsequently gather

i) Can I first of all begin by asking you to tell me a little bit about the communications media you have at the moment . Probe :

⇒ how frequently do you use this and what types of communication do you use it for (e.g. sales confirmations, contracts, purchase orders etc). What are the advantages and disadvantages of this medium?

For :

- Fax
- Royal Mail (post/paper mail)
- Courier Services (royal mail and other private couriers)
- Other mail services
- E-mail
- Any other service they mention

2. BACKGROUND ON THE INFRASTRUCTURE

Their existing network and computer systems - the prevalence of computer usage in the organisation. What is the current level of IT usage in the organisation ? Are there common problems that you are experiencing ?

ii) What are the benefits of (the IT mentioned)?

iii) What is the infrastructure (intranet/private networks/ LAN/WAN)

3. E-MAIL USAGE AND DEGREE OF UPTAKE

This will give an indication of how widespread the e-mail system is in the organisation and the extent to which TTP and other electronic mail services can be introduced (i.e. from the starting point of installing the new system or whether they are already using it) And how to approach the organisation with regards to introducing new services related to electronic mail.

iv) Concentrating particularly on e-mail and other electronic messaging services how widespread is this in the organisation? Is it used by the all tiers of employees in the organisation ? Is it used mainly for internal communication?

v) Do you think that this is currently replacing more traditional forms of communication

e.g. fax, traditional post, courier , registered . Why do you say that?

4. PRODUCT POSITIONING AND PRODUCT SUBSTITUTION

We want here to understand the current data transmission service they use and whether this can be translated into a new and modified service for electronic mail.

vi) Can you just tell me what data transmission services (post,courier,e-mail) you currently use ?. Do you think these are in line with your communications strategy for the future? i.e. do you think these will become obsolete services because you are moving to different ways of doing business and different means of communication

vii) How do you see the future of your organisation in terms of changing business needs and requirements ?

The existence of a security policy and the decision-making process in the organisation.

5. THE TRUSTED THIRD PARTY

Their reception to the TTP service, what they would use it for , who they would use it with, their requirements from such a service. What I am also proposing here is that we leave them with some sort of documentation and offer them the opportunity to be a part of the pilot

viii) We have developed a new service to adapt to the changing needs of businesses as technology develops and changes. The Trusted Third Party Service developed means that a third party will provide a service for electronic messages which guarantees :

- ⇒ integrity - ensuring that a message or file has not been altered during storage or transfer
- ⇒ confidentiality - encryption of messages and files where only named recipient can decipher and read them
- ⇒ non-repudiation - where the sender cannot deny having sent the message and the receiver cannot later deny having received the message
- ⇒ authentication - where unique digital signatures prove that a message really came from the originator

Only users authorised by the organisation and certified by the Trusted Third party would be able to use this service, which further ensures security features described above.

ix) How receptive would you be to this service? What type of documents would you use it for ? Is there anything else you feel should be added?

x) What would you be prepared to pay for this service (where on the scale of services you currently receive would you place this)?

Appendix 19 - Internet and E-mail Policies and Guidelines

The following is an example of the kind of E-mail and Internet usage policy which employees should be made aware of and comply with.

Important Guidelines and Warnings for Use of E-mail and Voice-mailⁱ

The guidelines and warnings listed below are of critical importance and non-compliance could in certain circumstances constitute a serious disciplinary matter.

1. Beware what you say in E-mail or voice-mail. Improper statements can give rise to personal or company liability. Work on the assumption that E-mail messages may be read by others.
2. Never send abusive, sexist, racist, or defamatory messages.
3. Never send strictly confidential messages via the Internet.
4. Never import non-text files or unknown messages onto your system without having them scanned for viruses. If you have not been properly trained to scan for viruses never import such items.
5. Always remember that E-mail or voice-mail messages, however confidential or damaging, may have to be disclosed in court proceedings or in investigations by competition authorities/regulatory bodies if relevant to the issues.
6. Do not create E-mail congestion by sending trivial messages or unnecessarily copying E-mails and do not advertise by E-mail or send messages for missing items unless genuinely urgent for business reasons. Use bulletin boards.
7. Always make hard copies of E-mails which you need to retain for record keeping purposes,
8. Ensure that you obtain confirmation of receipt of important messages.
9. Do no download, copy or transmit to third parties the works of others without their permission as this may infringe copyright.
10. Take care and obtain legal advice before entering into contractual commitments by E-mail or voice-mail
11. Do not view or download offensive or pornographic literature on office equipment.

ⁱ M.Hart - Internet Law Computer Law & Security Report Vol.14 No.4 1998.

Appendix 20 - International Certification Authorities

International Certification Authorities as compiled by Juan Alvaran
www.qmw.ac.uk/~t16345/ca.htm March 1999.

Africa

- Thawte Consulting - South Africa
- South African Certification Authority - South Africa (Verisign International Affiliate)

Asia

Japan:

- Initiative for Computer Authentication Technology (ICAT)
- Thawte CA sponsored by MEDIX Inc.
- Verisign Japan KK (Verisign International Affiliate)

Korea:

CrossCert SoftForum

Malaysia:

Digicert MTrust

Singapore:

Controller of Certification Authorities

Taiwan:

Hitrust (Verisign International Affiliate)

[back to the top](#)

Europe

Europe-Wide CAs:

GlobalSign Network of CAs:

European Union Projects:

- AD AEQUITATEM - Spain (Part of the INFOSEC AEQUITAS Project.)
- ICE-TEL Project

<u>Austria</u>	<u>Belgium</u>	<u>France</u>
<u>Germany</u>	<u>Greece</u>	<u>Ireland</u>
<u>Italy</u>	<u>Luxembourg</u>	<u>Spain</u>
<u>Sweden</u>	<u>Switzerland</u>	<u>The Netherlands</u>
	<u>United Kingdom</u>	

Austria:

Globalsign Austria (Globalsign Network)

Belgium

- Belsign (Globalsign Network)
- Isabel (Interbank Standards Association Belgium) In French and Dutch.

France:

Certplus (Verisign International Affiliate) Thawte Francophone

Germany:

- PCA of the German Research Network - Germany (cooperating with the ICE-TEL project but not a part of it).
- DFN - PCA Germany
- IN-CA: Individual Network e.V.: - Germany
 - List of regional IN-CAs of the Individual Network e.V.
- c't - Krypto-Kampagne: - Germany
- TC TrustCenter: - Germany

- IKS Certification Authority: - Germany
- GeFökoM CA - Germany
- Rus Test Certification Authority (RTCA) - Germany (in German)

Greece:

Globalsign Greece (Globalsign Network)

Ireland:

- Eurotrust (Baltimore Technologies)
- Software and Systems Engineering Limited (Certification products) Ireland

Italy:

- Certification Authority Tin (Telecom Italia Net) - in Italian
- Societ` Interbancaria per l'Automazione S.p.A. (SIA) - Italy: "Non-profit company delivering infrastructural services (like e.g. data transportation, cryptographic key management, etc.) to the whole community of Italian banks, including X.509v3 certification services." SIA CA Pilot Project. (In Italian)
- SSB - Societ` a per i Servizi Bancari S.p.A.
- Globalsign Italy (Globalsign Network)

Luxembourg:

Globalsign Luxembourg - Chambre de Commerce du Grand-Duché de Luxembourg
Certification Service Provider (CSP) (Globalsign Network)

Spain:

- Internet Publishing Services (IPS)
- Siscer
- Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE)
- Agencia de Certificación Electrónica (ACE)

Sweden:

- COST

Switzerland:

SwissKey Entrust Europe

The Netherlands:

Rocade (Verisign International Affiliate)

United Kingdom:

- BT Trustwise (Verisign International Affiliate)
- The Global Trust Register
- Inter Clear
- TrueTrust (Salford University)
- Globalsign UK (Globalsign Network)
- Viacode (Royal Mail CA)

[back to the top](#)

Middle East:

- Globalsign Lebanon (Globalsign Network)

South America:

- Argentina Governmental PKI and Licensing Authority
- Certisign - Brazil
- Mandic - Brazil

[back to the top](#)

North America

- **Canada:**
 - Entrust - Certification Products - Canada
 - Keywitness - Canada
 - OnWatch Key Management Centre - Canada
 - XCert - Canada
- **United States of America:**

- ARINC (airlines and aircraft operators)
- Certco (Certification Products).
- Digital Authentication Systems, Inc. (DAS-Inc.)
- Entegriy Solutions Corporation (Certification Products and Services)
- Frontier Technologies (Certification Products)
- GTE Cybertrust (Certification Products)
- IBM World Registry
- MIT Internet PCA Registration Authority
- PenOP - Signature Dynamics Authentication Technology
- Utah Digital Signature Program and Licensed CAs and Repositories:
 - Digital Signature Trust Company
 - Universal Secured Encryption Repository Company (USERFirst)
 - Arcanvus
 - The Usertrust Network
- SET Certificate Authority
- SUN Certification Authorities
- TradeWave Corporation
- Utah Digital Signature Authority
- Verisign
- Verisign SET Certification Authority
- WebVision - Certification Products

[back to the top](#)

Oceania:

- Signet as part of the Australian National Public Key Authentication Framework (PKAF) - Australia
- 128i - New Zealand's Certification Authority - New Zealand

Global

- Bolero Ltd - (TTP for Electronic Bills of Lading)
- Society for Worldwide Interbank Funds Transfers (SWIFT)

E-Club of the International Chamber of Commerce (ICC)

Appendix 21 – Methodology Definitions

One of the most common distinctions of research methodology is qualitative and quantitative.

Quantitative Methodology	Advantages	Disadvantages	Used in the Project
Surveys Software Evaluation	<ul style="list-style-type: none"> ▪ Findings are substantiated by statistics ▪ This can be repeated using the same sample can receive the same responses ▪ This methodology can quantify a phenomenon 	<ul style="list-style-type: none"> ▪ In depth observations cannot be made. ▪ Questionnaires are pre-defined towards an area of investigation 	<ol style="list-style-type: none"> 1. Telephone Survey (96/97) to determine Internet usage and attitudes of SMEs in the Greater Manchester region. Appendix 6 and chapters 5.2.1 2. Time Series Telephone survey (99) to assess change in usage patterns and attitudes of SMEs to Internet and security. Chapter 7.2 3. Software Evaluation Chapter 5

Qualitative Methodology	Advantages	Disadvantages	Used in the Project
Focus Groups Depth Interviews Case Study	<ul style="list-style-type: none"> ▪ This enables the understanding of people, social and cultural contexts ▪ Allows investigation of a phenomenon in a real life context ▪ Allows the preliminary identification of phenomena ▪ Enables the investigation 	<ul style="list-style-type: none"> ▪ Findings are not substantiated by statistics ▪ This cannot be repeated with similar responses ▪ This methodology cannot quantify a phenomenon 	<ol style="list-style-type: none"> 1. Focus Groups (96/97) Appendix 6 and chapter 5.2.1 2. Depth Interviews to understand corporate attitudes to authentication, digital signatures and certification authorities. Chapter 7.1 3. Case study to study the implementation process of security solution in organisations. Chapter 6

REFERENCES

Chapter 1

- 1 Meyer I., "Security Spending Rises", Communications Week, 30/9/96. Published by EMAP.**
- 2 Rash W. Jnr., "Security ", Communications Week, 30/9/96. Published by EMAP.**
- 3 Hornbach K., "Competition by Business Design", Long Range Planning Vol. 29, no.5 pp616-628. 1996. Published by Elsevier Science.**
- 4 Karimi , Gupta and Somers, "IT and Strategic Response to Globalization", Journal of Management Information Systems, Vol. 12 No.4 Spring 1996 p.55-88. ISSN 0742-1222**
- 5 Ross J.W., Beath C.M., Goodhue D.L., "Developing Long-Term Competitiveness Through IT Assets", Sloan Management Review Fall 1996. Published by MIT.
<http://mitsloan.mit.edu/smr/past/1996/smr3813.html> (Correct as at July 2000)**
- 6 Karimi , Gupta and Somers, "IT and Strategic Response to Globalization", Journal of Management Information Systems, Vol. 12 No.4 Spring 1996 p.55-88. ISSN 0742-1222**
- 7 "The Shape of Nets to come", The Economist July 1 1995 V336 n7921 pS17(2)**
- 8 Newing R., "Development in electronic commerce", Financial Times 8/1/97.**
- 9 www.eu.org accessed in May 1997. (Correct as at July 2000).**
- 10 Julian T., " Commerce Site Networks ", 6/4/98
<http://www.forrester.com/ER/Research/Report/Excerpt/0,1338,2500,FF.html> (Correct as at July 2000)**
- 11 Farmer D., "Shall We Dust Moscow? Security Survey of Internet Hosts and Various Semi-relevant Reflections" 18/12/96 <http://www.info-sec.com/internet/Infosecx.html-ssi> (Correct as at July 2000)**
- 12 The Computer Security Institute, "Computer Crime and Security Survey", December 98 <http://gocsi.com> (Correct as at July 2000)**
- 13 Anonymous - Maximum Security - A Hacker's Guide to Protecting Your Internet Site and Network - 2nd edition (September 1998) Sams; ISBN: 0672313413**
- 14 Anonymous - Maximum Security - A Hacker's Guide to Protecting Your Internet Site and Network - 2nd edition (September 1998), p97-99. Sams; ISBN: 0672313413**
- 15 Anonymous - Maximum Security - A Hacker's Guide to Protecting Your Internet Site and Network - 2nd edition (September 1998), p.98.Sams; ISBN: 0672313413**
- 16 Anonymous - Maximum Security - A Hacker's Guide to Protecting Your Internet Site and Network - 2nd edition (September 1998), p.110. Sams; ISBN: 0672313413**
- 17 Nuttall C., "Kosovo Info Warfare Spreads" - 1/1/99**

http://news2.thls.bbc.co.uk/hi/english/sci/tech/newsid_308000/308788.stm (Correct as at July 2000)

18 Trends Business Research - 28/01/99 http://www.tbr.co.uk/smes/tabs_uk/tab_2.htm (Correct as at July 2000)

19 Keegan V., "Internet Users of the World Unite", The Guardian Economics Notebook 30/9/97

Chapter 2 /

20 Development of the Information Society - The Role of Government - The Spectrum Report, January 1999. <http://www.isi.gov.uk/isi/govbenchframe.htm> (Correct as at July 2000)

21 Doyle C., "Wanted: Cyber-sheriff to tame new Wild West", The Guardian 29/3/99 <http://www.guardianunlimited.co.uk/Archive/Article/0,4273,3845777,00.html> (Correct as at July 2000)

22 Edwards L., Waelde C. "Regulating Cyberspace: Is there a role for Law?" , Computers and Law, December 1997/January 1998.

23 Mallon P., "The Legal Implications of Electronic Commerce in International Trade" , Computers and Law, October/November 1997.

24 Mayer-Schonberger V., "Internet Privacy", Computer Law & Security Report, Vol. 14 no.3 1998.

25 Hart M., "Internet Law" , Computer Law & Security Report, Vol 14, no.4 1998.

26 Black G., "Government grapples with electronic trade rules", Financial Times IT Review , 5/11/98.

27 UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT 1996 with additional article 5 bis as adopted in 1998 UNITED NATIONS

<http://www.uncitral.org/english/texts/electcom/ml-ec.htm> (Correct as at July 2000)

28 Kalakota, R. and Winston, A.B. Frontiers of Electronic Commerce. Addison-Wesley Publishing Inc. 1996. ISBN: 0201845202

29 Unattributed report in The Guardian On-line, 9/9/97, p1.

30 Ward C., "Online with Netcom" ,The Times. Quotation by David Garrison chairman of Online Communication Services, 20/11/96. <http://www.thetimes.co.uk/news/pages/tim/1996/11/20/frontpage.html?>(Correct as at July 2000)

31 Saunders W., "Slipping Through the Net", The Guardian, 18/11/96, p.39.

32 Magee M., quotation from Zobel R., EU representative on a project called The

- Global Marketplace for SMEs, Network News, 18/7/97. VNU Business Publishing Limited UK.
- 33** The DTI (1997) "UK Business: Moving into the Information Society" 1997.
www.dti.org.uk (No longer available at July 2000)
- 34** Information Strategy, A Survey of the Top 100 Companies in Europe who are the biggest IT Investors, 22/1/97 www.info-strategy.com/t100_pnl.htm (No longer available)
- 35** Robinson G., "Making the Web Safe for Children", The Daily Express, 3/10/98.
- 36** Hagel, A., and Armstrong, J., 'The Real Value of On-line Communities', *Harvard Business Review* 1/5/96. Publishers Harvard University Press.
- 37** Dellecave T. Jnr., "How do you stack up?", *Sloan Management Review*, December 1996 pp 34-37. Publishers MIT.
- 38** www.ibm.com/e-com.html, October 1997. (No longer available)
- 39** "UK Business and the Internet", Traynor Kitching and Associates Publication 1996.
- 40** Shafe L., "New technologies", *Financial Times*, 7/1/98.
- 41** Quelsch J.A., and Klein L.R., (1996) "The Internet and International Marketing" *Sloan Management Review*, Spring, 1996.
<http://mitsloan.mit.edu/smr/past/1996/smr3735.html> (Correct as at July 2000)
- 42** Spar, D., & Bussgang J.J., 'Ruling the Net', *Harvard Business Review*, 1/5/96. Harvard University Press.
- 43** Sunoo B.P., "Loafing on the Job", *Personnel Journal*, December 1996.
- 44** Jellenick D., "Cyberpower to the people", *Guardian Online*, 2/10/97.
- 45** Meikle J., "Nation divided into IT haves and have nots", *The Guardian*, 23/10/97
- 46** "1996 Internet Report", Continental Research. www.continentalresearch.com (report no longer available as at July 2000)
- 47** "1996 Internet Report" Continental Research. www.continentalresearch.com (report no longer available as at July 2000)
- 48** Unattributed, Internet User Report, *Business Computer World*, January 1997, p.116.
- 49** Gabriel C., "Interneccine Wars", Management Consultancy, January 1997.
- 50** Charlesworth A., "Tesco Pilots EDI net for small suppliers", *Network News*, 18/6/97 p.2. VNU Business Publishing Limited UK.
- 51** Electronic Commerce Report 6/4/98 <http://www.forrester.com/ER/Research/Report>. (report no longer available at July 2000)
- 52** <http://www.whatis.com/email.htm> (Correct as at July 2000)
- 53** Saunders B., "Slipping Through The Net", *The Guardian*, 18/11/96 p.39
- 54** Kalakota R., Whinston B., *Frontiers of Electronic Commerce*, Addison Wesley Publishing Company Inc., 1996. ISBN: 0201845202

- 55** www.su.se/palme.http 1997(No longer available at July 2000)
- 56** Nisse J., "NU to make e-mail libel payout", The Times, 18/7/97.
- 57** Stobie I., "E-mail do's and don'ts", Business Computer World, September 1997.
- 58** Stobie I., "Email slur cost £450K" ,Business Computer World, September 1997.
- 59** Black G., "Information Overload", Financial Times, 8/1/97.
- 60** Nairn G., "Using the Internet", Financial Times, 23/7/97.
- 61** Cavalli A. "Electronic Commerce over the Internet and the Increasing Need for Security" - A White Paper 8/12/95 <http://www.tradewave.com/products/vpiwp.html>
(Correct as at July 2000)
- 62** British Standards for Computing and Technology (BS7799) HMSO Publications 1999.
- 63** Howard J., "An Analysis of Security Incidents on the Internet 1989-1995", 7/4/97
<http://www.cert.org/research/JHThesis/Word6/> (Correct as at July 2000)
- 64** "Security is a low priority in the UK", Network News, 30/10/96 p.2. VNU Business Publishing Limited UK. ISSN: 0954-0636
- 65** Methvin D.W., "Web Insecurity Rampant", Windows Magazine 8/96 v7n8p36(2)
- 66** Methvin D.W., "Safety on the Net", Windows Magazine, 8/96 v7n8p164
- 67** Security Survey 1997. www.iss.net September, 1997 (The report is no longer available)
- 68** No reference

Chapter 3

- 69** Wallace W., The Logic of Science in Sociology. New York Aldine 1971. ISBN: 020230194X
- 70** Burrell G. and Morgan G., Sociological Paradigm and Organisational Analysis. Heinemann, London,1979. ISBN: 1857421140
- 71** Pettigrew A.M., Doing Research That is Useful for Theory and Practice, Jossey Boss, San Fransisco, 1985 p.222
- 72** Martin J., A garbage can model of the research process in McGrath, Martin and Kulka, 1982.
- 73** Kulka R.A., Idiosyncrasies and circumstance: choices and constraints in the research process in McGrath, Martin and Kulka, 1982.
- 74** Gill J., Johnson P., Research Methods for Managers, 1991. Paul Chapman Pub; ISBN: 1853961191
- 75** Gill J., Johnson P., Research Methods for Managers, 1991. P146-7 Paul Chapman Pub; ISBN: 1853961191

- 76** Denzin N.K., *Sociological Methods a Source Book*, McGraw-Hill, New York. 1978
- 77** Campbell D.T., and Fiske D.W., "Convergent and discriminant validation by the multitrait-multimethod matrix", *Psychological Bulletin* Vol. 56 p.81-5
- 78** Jick T.J., "Mixing qualitative and quantitative methods: triangulation in action", *Administrative Science Quarterly*, Vol24 December 1979 p.602-11
- 79** Morris C., *Qualitative Approaches in Business Studies*. Pitman Publishing 1996.
- 80** Yin R.K., *Case Study Research: Design and Methods*, Applied Social Research Series, Vol 5, Beverly Hills, Calif. (1984) ISBN: 0803956630

Chapter 4 :

- 81** "Business Environments Study of Trusted Services" BESTS - Desk research Summary Report - Coopers & Lybrand , March 1998
- 82** Garfinkel,S., and Spafford,G., *Web Security & Commerce.*, 1997.p.188 O'Reilly & Associates; ISBN: 1565922697
- 83** "An Introduction to Information Security" The first in a series of The Elliptic Curve Cryptosystem (ECC) whitepapers Published: March 1997 A Certicom Whitepaper - <http://www.certicom.com/research/white4.html> (Correct as at July 2000)
- 84** Garfinkel,S., and Spafford,G., *Web Security & Commerce.*, 1997. O'Reilly & Associates; ISBN: 1565922697
- 85** Schneier, B., *Applied Cryptography*, John Wiley and Sons 1996. ISBN: 0471128457
- 86** Wiener,M., "Efficient DES Key Search", School of Computer Science, Carleton Ottawa Canada TR244 May 1994.
- 87** "Cryptography FAQ" <http://www.rsasecurity.com/rsalabs/faq/> (Correct as at July 2000)
- 88** Chokhani & Ford Informational [Page 1]_RFC 2527 PKIX March 1999
- 89** Diffie,W and Hellman,M., "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol IT-22 no.6 (1976)
- 90** "The Elliptic Curve Cryptosystem" A White Paper Current Public-key Cryptography System, April 1997. <http://www.certicom.com/research/white2.html> (Correct as at July 2000)
- 91** Koblitz, N. "Elliptic curve cryptosystems", *Mathematics of Computation*, number 48, pages 203-209, 1987.
- 92** Miller, V.S., "Use of elliptic curves in cryptography", *Advances in Cryptology - Proceedings of CRYPTO'85*, Springer Verlag Lecture Notes in Computer Science 218, pages 417-426, 1986.
- 93** Ford, W. and Baum, M., *Secure Electronic Commerce* Prentice Hall, 1997.p.111

ISBN: 0134763424

- 94 Definition obtained from this site <http://burks.bton.ac.uk/burks/foldoc/70/16.htm> is no longer available.
- 95 INFOSEC 93 report Task S.01: Report to the Commission of the EC for the requirements for Trusted Third Services, Reference S2101/01, October 1993.
- 96 Hickson,N., "The Role of Security in Electronic Commerce" - Electronic Commerce Opening up New Opportunities for Business Eds. P.Timmers, B.Stanford-Smith and P.Kidd Cheshire Henbury 1998.
- 97 Definition of TTP and CA at www.dti.gov.uk/e-commerce, June 1997. This is no longer available.
- 98 www.verisign.com 1997 (Correct as at July 2000)
- 99 Eds. R.J.Anderson, B.Crispo, J.Lee, C.Manifavas, V.Matyas Jr., F.A.P. Petitcolas The Global Internet Trust Register 1998
<http://www.cl.cam.ac.uk/Research/Security/Trust-Register/> (Correct as at July 2000)
- 100 www.oecd.org/news_and_events (No longer available)
- 101 "Towards a European Framework for Digital Signatures and Encryption"
www.ipso.cec.be/eif/policy (No longer available)
- 102 "Towards a European Framework for Digital Signatures and Encryption"
www.ipso.cec.be/eif/policy (No longer available)
- 103 "The Cryptography and Liberty 1999 An International Survey of Encryption Policy"
Electronic Privacy Information Centre Washington, DC
<http://www.gilc.org/crypto/> (Correct as at July 2000)
- 104 "The Cryptography and Liberty 1999 An International Survey of Encryption Policy"
Electronic Privacy Information Centre Washington, DC
<http://www.gilc.org/crypto/> (Correct as at July 2000)
- 105 <http://www.wassenaar.org/> (Correct as at July 2000)
- 106 www.ourworld.compuserve.com (No longer available)

Chapter 5

- 107 Surveys:30% of businesses are connected to the Internet {PC World 25/12/96};
A survey of the top 1,000 companies in the UK revealed that 38% are on-line and 42% would have to get linked to the Internet in the foreseeable future {Internet World November, 1996};
The percentage of all business non-users of the Internet fell from 52% in April 1996 to 45% in January 1996 {source: The Internet Black Box Survey - Computer Weekly February 1996}

- 108** DeMillo R.A., McCracken W.H., Martin R.J., Passafiome J.F. , Software Testing and Evaluation, Benjamin Cummings Publishing Company 1987. ASIN: 0805325352
- 109** Basili VR, Perricone, BT "The TAME Project:Towards improvement-orientated software environments", IEEE Trans Soft Eng 14(6), 1988, 758-773.
- 110** Fenton, N.E., Software Metrics- A Rigorous Approach, Chapman & Hall 1991. ISBN: 0534954251
- 111** The information is based on the work carried out by Tattersall,S in an MSc Dissertation at the University of Salford 1998. This is unpublished.
- 112** Tattersall. S, MSc Dissertation - University of Salford 1998
- 113** Boehm BW, Brown JR, Kaspar JR, Lipow M., MacCleod GJ, Merrit MJ, Characteristics of Software Quality, North Holland, 1978. ASIN: 0444851054
- 114** "Standards for software quality metrics methodology" IEEE Computer Society Report P1061/D20, 1989
- 115** <http://www.entrust.com/> correct as at July 2000)
- 116** Chokhani S., Ford W., Certificate Policy and Certification Practice Statement Framework, 3 November, 1996.
- 117** <http://www.ice-tel.org> (No longer available) www.darmstadt.gmd.de/ice-tel, See appendix 9. (Correct as at July 2000)
- 118** <http://www.gemisis.co.uk/> (Correct as at July 2000)
- 119** <http://www.tvc.org> (Correct as at July 2000)

Chapter 6

- 120** <http://www.tvcnet.org.uk/> (No longer available)
- 121** http://www.vaiism.com/roger/Proto2/archived/vol1/columns/weil-rosen0998_1.html (No longer available)
- 122** Rowe et al. Strategic Management - A Methodological Approach – 1994 Addison-Wesley Pub Co; ISBN: 020158638X
- 123** Porter M.E., The Competitive Advantage of Nations,1998. Free Press; ISBN: 0684841479
- 124** <http://www.tvcnet.org.uk/> (No longer available)
- 125** <http://technostress.com> - Technophobia Measurement Instruments, Dr Larry Rosen and Dr Michelle Weil CA <http://technostress.com> Correct as at July 2000)

Chapter 9

- 126** Krcmar,H., Bjorn-Andersen,N., and O'Callaghan R., Eds. EDI in Europe - How it works in practice - 1995. John Wiley & Son Ltd; ISBN: 0471953547

- 127** Brynjolfsson E., Austin Renshaw A., M.Van Alstyne "The Matrix of Change a Tool for Business Process Re-engineering" , MIT Sloan School of Management - 8/98
<http://mitsloan.mit.edu/smr/past/1997/smr3823.html> (Correct as at July 2000)
- 128** Milgrom P., Roberts J., "Complementarities and Fit: Strategy, Structure and Organisational Change in manufacturing", Stanford Department of Economics 1993.
- 129** Runaway Projects 1998. <http://www.kpmg.co.uk/uk/services/manage/run.html>
 (Correct as at July 2000)

Chapter 10

- 130** Dicken P., Global Shift - The Internationalisation of Economic Activity, 1992.
 Guilford Press; ISBN: 0898624886
- 131** Daft R., Organisation Theory and Design, 1992
 South-Western Pub; ISBN: 0538879025

Chapter 13

- 132** Electronic Communications Bill 1999 - <http://www.dti.gov.uk/> (Correct as at July 2000)
- 133** www.dti.gov.org/consumer/whitepaper accessed 1998 (No longer available)
- 134** "Ensuring Security and Trust in Electronic Communications" - EC Report – 1998
<http://www.ispo.cec.be/eif/policy/97503.html> (No longer available)
- 135** <http://www.epic.org> on behalf of GILC www.gilc.org/crypto (Both URLs correct as at July 2000)
- 136** www.premier-ministre.gouv.fr/pm (No longer available)
- 137** www.vn.fi/telecomm/ (No longer available)
- 138** www.vn.fi/telecomm/ (No longer available)
- 139** "The Cryptography and Liberty 1999 An International Survey of Encryption Policy"
 Electronic Privacy Information Centre Washington, DC <http://www.gilc.org/crypto/>
 (Correct as at July 2000)
- 140** <http://www.trustwise.com/welcome.html> (Correct as at July 2000)
- 141** www.viacode.co.uk <http://www.royalmail.com/default.htm>
 (Correct as at July 2000, automatically redirects to above)
- 142** Travis A "On the Net - Guardian/ICM Poll" , The Guardian 11/1/99
- 143** Lawson Rob www.NOP.com (3/3/99) (No longer available)
- 144** Hart M, "Internet Law" - Computer Law & Security Report, Vol 14, no.4 1998.
- 145** Yasin R. "Plugging Holes in FTP, Mail Servers" , InternetWeek, Issue 753, 22/2/99
 Publishers CMP Media Inc.

- 146** Unattributed article in The Guardian Online - 20/5/99
- 147** Van Der Zee B., "Consumer", The Guardian 28/5/98
- 148** "How safe is the net" , www.businessweek.com 22/6/98
- 149** GIS Survey 1998 - Ernst and Young http://www.ey.com/global/gcr.nsf/us/Welcome_-_Library_-_Ernst_&_Young_LLP
(Correct as at July 2000)
- 150** Staunton D "Hackers expose net insecurity", The Guardian, 30/3/1998.
- 151** Youngjohns R - "David Hewson of Sun Microsystems in the UK", The Sunday Times
- Getting wired, 2/11/97 p.3
- 152** McGhie T, "Finance and Economics", The Guardian 18/3/99 pp22
- 153** Amazon.com Case Study - www.iss-awareness.cenorm.be/ecawarept accessed
2/3/99
(No longer available)
- 154** Girishankar S. "Heavy Trading at Schwab Online"
<http://www.internetwk.com/trends/trends122198-2.htm> 21/12/98 (Correct as at July
2000)
- 155** J.Fontana, "Chrysler Keeps SCORE",
<http://www.internetwk.com/trends/trends122198-1.htm> 21/12/98 (Correct as at July
2000)
- 156** Amazon.com Case Study - www.iss-awareness.cenorm.be/ecawarept 2/3/99
(No longer available)
- 157** Chin Leong K. "The Web's No Game For Ailing Toys R US"
<http://www.internetwk.com/trends/trends122198-3.htm> 21/12/98 (Correct as at July
2000)
- 158** Case Study Conclusions - www.iss-awareness.cenorm.be/ecawarerpt 2/3/99
(No longer available)
- 159** Keegan V. , "Web Wars", The Guardian Online, 20/5/99
- 160** Ostergaard S.D. , "Naestved Info-Society 2000", IBM Nordic Published report from
IBM sent on request. September 1998.
- 161** "Naestved and IBM pilot digital signature in Denmark", IBM (UK), 8/9/98
<http://www-5.ibm.com/uk/releases/98285.html> (Correct as at July 2000)
- 162** IBM (UK), July 1998 <http://www-5.ibm.com/uk/releases/> (Correct as at July 2000)
- 163** Flisi C., "Building On-line Marketplaces", International Herald Tribune, 6/10/98
<http://www.iht.com/IHT/SUP/> (Correct as at July 2000)
- 164** Greco,J. "Designing for the 21st Century", Journal of Business Strategy, Nov/Dec 98.
- 165** Herman, R., Gioia,J. Lean and Meaningful, 1998. Oak Hill Press; ISBN: 1886939071

- 166** Herman, R., Gioia, J. *Lean and Meaningful*, 1998. Oak Hill Press; ISBN: 1886939071
- 167** Herman, R., Gioia, J. *Lean and Meaningful*, 1998. Oak Hill Press; ISBN: 1886939071
- 168** Gates, B., C Hemmingway, *Business@ the Speed of Thought: Using a Digital Nervous System*, 1999. Warner Books; ISBN: 0742906760
- 169** Firmage, J., "Retailers face Net Invasion", *The Guardian* 15/12/98
- 170** Firmage, J., "Retailers face Net Invasion", *The Guardian* 15/12/98
- 171** DeCovny S., "Electronic Commerce comes of Age" , *Journal of Business Strategy* November/December 1998.
- 172** The UK Electronic Commerce Market.7 /8/98, IDC. <http://www.idcresearch.com/>
(Report no longer available)
- 173** IBM and Government
<http://houns54.clearlake.ibm.com/solutions/government/govpub.nsf/detailcontacts/Hcme?OpenDocument> (Correct as at July 2000, automatically redirects to above)
- 174** Schofield J. , "Cover Story" , *The Guardian Online* , 20/5/99
- 175** Cottrill K., "Iris recognition", *The Guardian On-line*, 6/11/97
- 176** Foremski T., "US Initiatives", *Financial Times -IT Review*, 5/11/98
- 177** Foremski T. "US Initiatives" *Financial Times -IT Review* 5/11/98
- 178** Shillingford J., "Telecoms Future", *Financial Times*, 18/3/99