TOWARDS A MODEL FOR ENSURING OPTIMAL INTEROPERABILITY BETWEEN THE SECURITY SYSTEMS OF TRADING PARTNERS IN A BUSINESS-TO-BUSINESS E-COMMERCE CONTEXT.

by

MAREE PATHER

Submitted in part fulfilment of the requirements
for the degree of

MASTER OF SCIENCE

in the subject

INFORMATION SYSTEMS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF. L.M. VENTER

JUNE 2002

TOWARDS A MODEL FOR ENSURING OPTIMAL INTEROPERABILITY BETWEEN THE SECURITY SYSTEMS OF TRADING PARTNERS IN A BUSINESS-TO-BUSINESS E-COMMERCE CONTEXT.

by

MAREE PATHER

Towards a Model for Ensuring Optimal Interoperability Between the Security Systems of Trading Partners in a Business-to-Business E-Commerce Context.

TABLE OF CONTENTS

TABLE OF FIGURES

ABBREVIATIONS AND ACRONYMS USED

The following abbreviations and acronyms occur in this document. Explanations are supplied in the text where it is doubtful whether a term is in everyday use.

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
Affine Transformation	A transformation consisting of multiplication by a matrix followed by the addition of a vector.
AH	Authenticating Header (an IPSec protocol)
ANSI	American National Standards Institute
Array	An enumerated collection of identical entities (e.g., an array of bytes).
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode; high-bandwidth packet- switching technology.
ATM	Asynchronous Transfer Mode, a 53-byte fixed-length cell relay
B2B	Business-to-Business E-Commerce
B2C	Business-to-Consumer E-Commerce
CA	Certification Authority (for digital certificates)
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication protocol (also in Microsoft-specific version, MS-CHAP), found in PPTP
CSCW	Computer-based Systems for

	Cooperative Work
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CUG	Closed User Group
DEA	Data Encryption Algorithm (ANSI Standard)
DEA-1	Data Encryption Algorithm (ISO Standard)
DES	Data Encryption Standard
DES-CBC	DES – Cipher Block Chaining mode
DHTML	Dynamic Hypertext Markup Language
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
DSP	Digital signal processor
DSS	Digital Signature Standard (from NIST)
ebXML	Electronic Business XML
EDI	Electronic Data Interchange
EFF	Electronic Frontier Foundation
E-RD	Entity-Relationship Diagram
ESP	Encapsulating Security Payload (an IPSEC protocol)
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GDSS	Group Decision Support Systems
GRE	Generic Routing Encapsulation
GSS	Group Support Systems
HDM	Hypermedia Data Model
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language

HTML	Hypertext Mark-up Language
HTTP	Hypertext Transport Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange, a combination of ISAKMP and OAKLEY; also known as IKMP
IKMP	Internet Key Management Protocol
IOIS	Inter-organizational Information System
IOS	Inter-organizational System
IP	Internet Protocol, a connectionless network layer protocol.
IPSec	Secure Internet Protocol
ISAKMP	Internet Security Association and Key Management Protocol (RFC 2408)
ISDN	Integrated Services Digital Network, digital circuit-switched technology
ISO	International Standards Organisation
ISP	Internet Service Provider
ITSEC	European Information Technology Security Evaluation Criteria
JAD	Joint Application Design
JDK	Java Development Kit
JIT	Just-In-Time (compilation)
KDC	Kerberos Distribution Centre
L2F	Layer 2 Forwarding Protocol, a Cisco VPN encapsulating protocol
L2TP	Layer 2 Tunnelling Protocol, a Cisco-developed VPN protocol
MD5	Message Digest 5, a hashing algorithm from RSA

MIME	Multi-purpose Internet mail extension
MMX	Matrix Math extension
MPLS	Multi-protocol Label Switching
NAT	Network Address Translation
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology(formerly NBS, National Bureau of Standards)
NTD	Network Terminating Device
OAKLEY	Key Establishment protocol (RFC 2412)
ODBC	Open Data Base Connectivity
OS	Operating System
PDU	Protocol Data Unit (in OSI Reference Model)
PGP	Pretty Good Privacy, an e-mail privacy utility that uses public key encryption
PKCS	Public Key Cryptography Standard from RSA Security Laboratories
PKI	Public Key Infrastructure (for digital certificates)
PKIX	Public Key Infrastructure X.509 (IETF)
PPP	Point-to-point protocol, a layer 2 WAN protocol
PPTP	Point-to-point Tunnelling Protocol, a Microsoft VPN encapsulating Layer 3
PSTN	Public Service Telecommunication Network
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory

RAS	Remote Access Service (a Microsoft Server service)
RC2, RC4	Rivest Cryptosystem 2, 4 (symmetric encryption algorithms designed by Ronald Rivest)
ROM	Read-only memory
RMON	Remote network monitoring
RSA	Key agreement protocol developed by **R**ivest, **S**hamir and **A**delman
SA	Security Association (an IPSec protocol)
S/MIME	Secure Multipurpose Internet Mail Extensions, a protocol for securing e-mail attachments
SET	Secure Electronic Transaction, an e-commerce protocol
SHA-1	Secure Hash Algorithm – 1
SOCKS	A session layer proxy security protocol.
SSL	Secure Sockets Layer, a protocol for incorporating encryption into e-commerce transactions, developed by Netscape
TACACS	Terminal Access Controller Access
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TLS	The IETF's Transport Layer Protocol (also called SSL 3.1).
UDP	User Datagram Protocol

URL	Uniform Resource Locator
VHDL	VHSIC Hardware Description Language.
VHSIC	Very High Speed Integrated Circuits.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Mark-up Language
XOR	Exclusive-OR operation.

Chapter 1

THE PROBLEM AND ITS CONTEXT

1.1. Introduction

In recent years, competitive pressures have spawned numerous alliances and partnerships among various organizations. One trading partner (wholesaler, retailer or manufacturer) generally requires certain items and/or services from another trading partner. Interactions between such trading partners include obtaining updated prices, querying availability of required items, placing of orders, making payments, returning faulty/damaged goods (exchange of debit notes and credit notes), lodging complaints, and advertising of goods on offer or of "special offers". Common tools of interaction include telephones, facsimile machines, E-mail, postal/courier services, dedicated inter-organizational networks, electronic data interchange (EDI), and, more recently, the Internet.

Internet technology has limitless potential for improving the quality of this interaction. However, in the context of trading partners, new concerns are also introduced. These include network management issues, such as bandwidth availability and security issues.

Making security implementations compatible and interoperable across the unsecured Internet poses a serious problem for designers of such inter-organizational systems. If two organizations wish to form an alliance, extending connectivity between them in a private network environment would generally require dedicated connections, compatible equipment, separate dial domains (if dial access is used), and network architecture and management policies that must be negotiated and maintained. Fortunately, Internet technology has given rise to

Extranet Virtual Private Networks (VPNs) (explained in *Definition of Key Terms* below), which obviates these problems to a large extent. For this reason, VPNs have become very popular in inter-organizational systems. A Gartner Group survey estimates that by 2003 nearly 100% of enterprises will supplement their wide area network (WAN) infrastructures with VPNs. (Cisco[1], 1999).

The primary challenge in a VPN Extranet set-up revolves around matching security architectures and management. Variations and nuances in security implementations exacerbate the interoperability problem. Each partner may, for example, employ a different combination of possible security protocols: S/MIME, PGP, SSL, SET, IPSec, L2TP, L2F, PPTP, etc. (See *Abbreviations and Acronyms Used*). Further, differences may occur in encryption algorithms, encryption keys, certification authorities, firewall policies, and whether the public Internet or a Frame Relay or ATM backbone is used. (These concepts will also be elaborated later). Variations may be even more granular, e.g. in respect of specific protocol configurations used by each trading partner. (Cisco[1], 1999; Cisco[2], 2000). How does one reconcile these differences across the Internet chasm?

Once trading partners have been discovered and collaboration agreements have been reached, security mechanisms must be integrated to ensure uniform implementation of standard security services such as authentication, privacy, integrity, authorization and non-repudiation. In the context of global VPNs, the diversity of implementation possibilities, and the expected growth rate in VPN connections, a means for ensuring such interoperability is required. This research, therefore, endeavours to address this need.

1.2. Essential Terminology

1.2.1. Definitions and Meanings of Key Terms

1.2.1.1. Electronic Commerce Terms

The key terms are explained below:

- **B2B (E-Commerce)**: A specific electronic commerce scenario comprising two trading partners. Lawrence et al. (2000, p3) summarize the essential perspectives of e-commerce as: (Using Internet technology for)
    - Communications - to deliver information, products/services and payments;
    - Business - to perform transactions and work flows;
    - Service – customer relationship and product delivery logistics management; and
    - Online transactions – the electronic data network aspect (the Internet).
- **Extranet**: An inter-organizational network based on Internet protocols and infrastructure. An Intranet is a corporate network utilizing Internet technology. An extranet is an extended intranet, which links remote intranets or individuals over Virtual Private Networks built on the Internet. (Chung et al, 2000, p.241).
- **Hypermedia**: Elements and processes in an application which include navigation features such as browsing, backtracking, content-based query, and queries based on the hypermedia link structure. A key component of hypermedia is the set of hypertext elements. Other components include sound and graphics files. (Bieber and Isakowitz, 1996).
- **Inter-Organizational Information System (IOIS)**: This refers to automated information systems shared by two or more organizations (Choudury, 1997).
- **Trading Partner:** One member of at least two collaborating organizations. The collaboration is defined by a variable set of organized activities, which includes designing, producing, promoting, marketing, selling, delivering, and

supporting the products or services, undertaken between them. (Sachs et al, 2000).

- **Virtual Private Network (VPN):** A VPN is an enterprise network deployed on a shared infrastructure employing the same security, management, and throughput policies applied in a private network. A VPN may utilize the public Internet or service provider backbones (generally IP, Frame Relay or ATM networks). They are characterized by an encrypted tunnel between clients and servers. (Cisco1, 1999)

1.2.1.2. Common Information Security Terms

In this section, general security concepts will be briefly explained.

Gollmann (1999:5) states that there is often disagreement about precise definitions of security aspects and that most definitions are based on major sources such as the US Trusted Computer System Evaluation Criteria (TCSEC; the "Orange Book"), the European Information Technology Security Evaluation Criteria (ITSEC), the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) and the International Standards Organization's ISO 7498-2.

The following definitions are primarily intended to eliminate any equivocal meanings of security-related terminology used in this dissertation. They are based on the academic textbook by Pfleeger (1997:3-65), except where otherwise indicated. For this reason, references to material from Pfleeger will generally be omitted.

The following are some common terms used in discussing security:

- **Exposure**: a form of possible loss or harm.
- **Vulnerability:** a weakness in the system that might be exploited for loss or harm.
- **Attack:** the exploitation of one or more vulnerabilities.

- **Threats:** circumstances that have the potential to cause loss or harm.
- **Control:** protective measure – action, device, technique or procedure – that reduces vulnerability.
- **Risk Analysis:** the evaluation of the seriousness of a threat, the likelihood of it occurring and the cost of implementing a suitable countermeasure (control) (Hassler, 2001:4).
- **Principals**: human users, computers or computer processed (Hassler, 2001:3).
- The **Goals of Security** are considered to be**:**

    - **Confidentiality** (secrecy and privacy): This ensures that assets are accessible to only authorised parties.
    - **Integrity:** This ensures that assets can only be modified by authorised parties and in authorised ways.
    - **Availability**: This ensures that assets are accessible to authorised parties; it includes, inter alia, deadlock management. The term "denial of service" is often used to depict the effect of an attack on availability.

Gollmann (1999:8) adds the following two to the list:

- **Accountability**: This ensures that actions affecting security may be traced to specific individuals; audit information is required.
- **Reliability and Safety (Dependability)**: This ensures that reliance can justifiably be placed on the service a computer system is intended to deliver.

- The **major assets** to protect in a computing system are:
    - hardware,
    - software and
    - data.

These can be extended to include:

- Storage media;

- Networks;
- Access to computing equipment, e.g. the theft of computer time; and
- Key people.

- **Threats, Security Services and Attacks**

There are essentially four **kinds of threat** to the security of a computer system: **interruption, interception, modification** and **fabrication**. These may be defined as follows:

- **Interception** refers to the capture of data in transit. If this data is meant to be secret, and is viewed by the interceptor, then *confidentiality/privacy* has been breached. If the data is altered, then *integrity* has been compromised. If the data is prevented from being transmitted, then *availability* is being compromised. The first instance is considered **eavesdropping** while the latter two would constitute **message-tampering** (Hassler 2001:3-4).

- **Interruption** implies an incidental break in a process/service. If the interruption is a deliberate break, then *availability* of the process/service has been compromised.

- **Modification** is the altering of assets to cause mischief/harm. If the data is deliberately modified to mislead, then *integrity* has been compromised. Software modification includes using Trojan horses, viruses, trapdoors (programs with secret entry points), and information leaks (deliberately or inadvertently, in a program, to make information accessible to unintended people or programs). This is also referred to as **infiltration** (Hassler, 2001:4).

- **Fabrication** implies falsification. False data is "planted" to pose as the correct form of data. This is an attack on the *integrity* of the data

set. Hassler (2001:3-4) also lists **masquerading** (using another principle's identity) and **replaying** (using a previously sent message to gain another principal's use-privileges) as similar attacks. Masquerading is also known as **spoofing** (e.g. Pabrai and Gurbani, 1996:3).

- **Traffic Analysis** allows an interceptor to obtain information about relationships, types of data, etc, exchanged between parties. Traffic padding is the mechanism used to prevent this form of attack. (Pabrai and Gurbani, 1996:6).

The words in italics in the list above are termed **security services**. On the basis of **risk analysis**, one can define a **security policy** that clearly specifies what must be secured. The functions that enforce a security policy are what are referred to as security services. (Hassler, 2001:5). The International Standards Organization (ISO) (cited in Hassler, 2001:5-6) identifies the following additional basic security services:

- **Authentication**: This ensures the authenticity of the origin of data or of a principle's identity.
- **Access control**: This ensures controlled differential access to protected resources.
- **Data confidentiality:** Also called privacy, this ensures that only authorized principals can understand the protected data.
- **Data integrity:** This ensures that data is not modified by unauthorized principals.
- **Non-repudiation**: This ensures that either the receiver cannot deny having received data or the sender cannot deny having sent the data, or both.

Actual **attacks** (exploiting vulnerabilities) include: viruses, worms, Trojan horses, trap doors, logic bombs, port scanning, IP address spoofing, sequence

number spoofing, session hijacking, DNS spoofing, man-in-the-middle attacks, DNS poisoning, redirects, replay attacks, password cracking, social engineering, sniffing, web site defacement, war dialling, ping of death, SYN flooding, spamming, and smurf attacks (Canavan, 2001: 25-43).

Security controls need to be put in place to prevent such attacks. Some of these are outlined in the next sub-section.

- **Security Controls**

Security services are implemented by means of **security controls/mechanisms,** which may be broadly categorized as:

  - Implemented policies (e.g., frequency of change of passwords),
  - Physical controls (locked doors, labelled data, etc),
  - Encryption,
  - Software controls (e.g., database access controls), and
  - Hardware controls (smart card controls, locks, etc).

Hassler (2001:6-47) prefers to discuss controls in terms of security services, as follows:

  - **Encryption mechanisms:** generally, protect confidentiality.
  - **Digital signature mechanisms:** provide source authentication and integrity services.
  - **Access control mechanisms:** closely connected to authentication.
  - **Data integrity mechanisms:** protect data from unauthorised alteration.
  - **Authentication exchange mechanisms:** authenticate the sender on both sides.
  - **Traffic padding mechanisms:** offer protection against traffic analysis.

- **Routing control mechanisms:** allow a specific path to be chosen for sending data through a network, as well as the acceptance or rejection of incoming traffic; provide authentication and access control.
- **Notarisation mechanisms:** are third parties that ensure integrity, origin, time or destination of data; provide authentication and non-repudiation services.

Greenstein and Feinman (2000: 228) provide the following table (modified) of more specific security controls and their corresponding security services:

SECURITY SERVICE	SECURITY CONTROL
Confidentiality	Encryption
Integrity	Hashing (Digest)
Authentication	Digital Signatures Challenge-response Passwords Biometric devices
Access Control	Firewalls Passwords Biometric devices
Non-repudiation	Bi-directional hashing Digital signatures Transaction certificates Time stamps Confirmation services

- **Basic Encryption Terms:**

Unless otherwise specified, the main source of information in this regard is Pfleeger (1997:21-65).

- **Encryption** may be defined as the process of encoding a message so that its meaning is not obvious. It may be represented as follows (Kaufman et al, 1995:39):
  Plaintext→*encryption*→ciphertext→*decryption*→original plaintext

Other useful definitions include:

- **Enciphering** is the translation of letters or symbols individually, while **encoding** involves entire words or phrases.
- **Cryptography** implies hidden writing or using encryption to conceal text.
- **Cryptanalysis** is the study of encryption and encrypted messages with the goal of finding hidden meanings of messages.
- **Cryptology** is the study of encryption (includes cryptography and cryptanalysis).
- **Cipher** refers to a set of encryption operations.

1.2.2. The B2B IOIS Context

An Extranet implies an inter-organizational wide area network (WAN) based on Internet protocols and infrastructure, comprised of a selected group of participant private networks. The nature of the collaboration need not necessarily include formal business transactions. Barua (1996), e.g., describes an academic "colaboratory", which is an Extranet comprised of different academic institutions. An Extranet comprises, by definition, at least one VPN (e.g., Turban et al, 2000: 243). It is also an Inter-Organizational System (IOS) and, generally, an Inter-Organizational Information System (IOIS) (defined in section 1.2.1.1.).

B2B refers to a specific e-commerce scenario: the conducting of electronic business between two organizations (trading partners), based on Internet

protocols and infrastructure. As such, it is a business-oriented Extranet. B2B and Extranets are therefore subsumed under IOS and IOIS.

Thus,

- "Extranet" implies the Internet and VPN, but not necessarily business;
- "VPN" implies neither the Internet nor business, while
- "B2B" implies business and Extranet, and, therefore, VPN.

In identifying a term with the implicit connotations of: Extranet, E-Commerce (Internet and business), trading partners, VPN, and the various IOIS types (Chapter 2) – in order to describe the context of this investigation, "B2B IOIS" seems the most appropriate. In "B2B IOIS", "Extranet" and "VPN" are implied and are therefore superfluous. "IOIS", although redundant in "B2B IOIS", is retained to denote the various manifestations of IOIS (as described by Choudury's typology in Chapter 2).

In the remainder of this document, "B2B IOIS" will have the connotations as described above.

1.3. The Research Problem

Each trading partner in a B2B IOIS may implement various permutations of security controls. This is a major impediment to ensuring the required level of interoperability between trading partners. Hence, the following question is investigated: Can a framework be formulated to facilitate sufficient congruence between collaborating systems to overcome this problem?

1.4. The Sub-problems

a. What are the risks and corresponding controls currently documented for B2B IOISs?
b. Can a framework be proposed to ensure the interoperability of electronic business security implementations between trading partners in a B2B IOIS context?
c. Can the proposed framework (sub-problem b. above) satisfy existing evaluation criteria in terms of optimal interoperability of security implementations between trading partners, in the B2B IOIS context?

1.5. The Delimitations and Scope of this Research

The proposed solution will focus on integrating security structures from a functional services perspective. The following are considered integral factors in the solution, but in-depth treatment of each is beyond the scope of this dissertation:

- Describing business processes outside of the security context, i.e. the business operational view;
- Broader electronic business issues (such as the contractual qualities of digital signatures); and
- Broader network management and security management issues.

1.6. The Organization of Chapters

The chapters have been organized as follows:

- Chapter 1 is a brief introduction.
- Chapter 2 discusses Inter-organizational Information Systems (IOISs) in terms of benefits, classification and management (e.g., Massetti and Zmud, 1996; Kumar and Dissel, 1996; Choudury, 1997). This is of

fundamental importance, since the sharing or exchange of information between trading partners presupposes some form of IOIS.

- Chapter 3 examines existing security models in a business-to-business (B2B) electronic commerce context, specifically, the UNIFACT/OASIS electronic business XML (ebXML) standard (UN/CEFACT and OASIS[1], 2000; UN/CEFACT and OASIS[2-8], 2001).
- Chapter 4 focuses on exactly what is required in possible security implementations in B2B IOISs for optimal interoperability, and where the strengths and deficits in this regard lay in existing models, standards and implementations. It covers, inter alia, current Virtual Private Network technologies (e.g. King et al 2001: 177-215; Cisco[1], 1999; Cisco[3], 1999 Cisco[4], 2000).
- Chapter 5 attempts a synthesis of ideas extracted from information in the previous chapters. A possible framework for optimum interoperability between trading partners in B2B IOISs is derived.
- Chapter 6 supplies arguments and relevant criteria for evaluating the contentions raised in Chapter 5.
- Chapter 7 reports the outcome of the evaluation in chapter 6. Chapter 7 also concludes with statements regarding the significance and validity of the research and relevant thoughts for the future.

Chapter 2

INTER-ORGANIZATIONAL INFORMATION SYSTEMS

2.1. Introduction

This chapter reviews the related literature on Inter-Organizational Information Systems (IOISs) specifically in relation to trading partners, but not necessarily in relation to the Internet. IOISs constitute the background within which this research finds its point-of-departure. The intention behind this chapter is to provide some insight into the context of B2B IOISs, which will be explored in more detail in later chapters. Chapters 3 and 4 are intended to elaborate on the security aspects of B2B IOISs.

The literature survey for this chapter was directed by the following questions, considered pertinent in this regard:

- Why do organizations become involved in Inter-Organizational Systems (IOSs)? What is the motivation for relatively persistent trading partners?
- What are the benefits provided by the Internet technology (in B2B) over previous private Inter-Organizational Systems (IOSs) network links? What is the nature of Internet-based (B2B) IOISs?
- What are the implementation options available in choosing Inter-Organizational Information Systems (IOISs) as a business strategy?

In subsequent sections the following will be discussed.

- The reasons for the electronic integration – to varying degrees – of trading partner information systems (Section 2.2.).

- The impact on this phenomenon (IOISs) made by the advent of Internet technology (B2B IOISs) (Section 2.3.).
- A taxonomical view of IOISs; the nuances of implementation options which make a singular security solution difficult (Section 2.4.).

2.2. Drivers for IOISs

The following general reasons for cooperation between participants in Inter-Organizational Systems have been identified (Kumar and Dissel, 1996):

- *Globalization*: the trend to trade world-wide;
- *Environmental turbulence*: business process re-engineering driven by dynamic technological factors;
- *Resource pooling*: sharing resources with business partners to lower costs;
- *Risk-sharing*: sharing business processes and resources to reduce risk;
- *Reducing supply-chain uncertainty*: ensuring availability and fulfilment from suppliers, and to customers; and
- *Increasing resource utilization*: ensuring more efficient use of machinery and skills, e.g. through readily available real-time transaction capability.

Additional factors include (Massetti and Zmud, 1996):

- The improved speed and quality of computations;
- Increased availability of data/information; and
- The reduction in required manpower and operations.

The IOIS drivers outlined above serve to illustrate why B2B electronic commerce is rapidly building on the infrastructural capability provided by the Internet and IOIS technologies such as Electronic Digital/Data Interchange. Factors such as globalization, reducing supply-chain uncertainty and real-time transaction-processing have been greatly enhanced by the ubiquitous use of the

Internet. The next section discusses how the Internet extends the benefits of IOISs by virtue of its added hypermedia benefits.

2.3. The implications of hypermedia-based IOISs

2.3.1. Benefits of hypermedia in IOISs

Older Group Decision Support Systems (GDSS) and Computer-Based Systems for Cooperative Work (CSCW) or "groupware" lacked emphasis on media richness, communication bandwidth, geographic scope and real-time communication capability. Internet technology, in the form of B2B E-Commerce, provides these features through a single, open user interface: the Web Browser (Barua et al, 1995). Current systems allow for technologies such as Dynamic HTML and streaming multimedia to provide dynamic, animated audio-visual presentations. Broader-bandwidth technologies (such as: optic fibre, DSL, ISDN, Frame Relay and ATM) have done much to change the quality of groupware.

The more-obvious motivational factors for implementing a B2B E-commerce IOS include:

- Providing a presence on the Internet has corporate-image ramifications; including allowing smaller organizations to compete with larger ones;
- It allows for targeting a broader market segment;
- Brick-and-mortar shop fronts and concomitant staff requirements are obviated;
- Business processes become more streamlined, thereby reducing (essentially, human) errors, and increasing productivity;
- Both hardware and software requirements for client computers are greatly reduced. The only client software required, aside from the operating system, is a browser;
- It involves EDI-like exchange of business documents (orders, invoices, etc);

- The communication infrastructure is cheaper; instead of costly dedicated lines, either dialup (PSTN or ISDN) lines could be leased from telecommunication organizations. Various newer cost-effective options (such as DSL) are now available. All telecommunications utilize the Internet; thus all calls are charged at local-call rates; and
- Processing of transactions and accessing trading partner data (such as prices, availability, etc) can be done in real-time.

2.3.1. Problems introduced by hypermedia in IOISs

Internet technology, unfortunately, also seems to bring with it a few significant disadvantages, including:

- Higher bandwidth and quality-of-service requirements due to hypermedia components. This implies more expensive hardware. As operating systems and supporting applications improve to accommodate hypermedia capabilities, so the platform requirements spiral progressively outwards.
- The public nature of the Internet and the increasing power of desktop computers have additional ramifications for security. This will be elaborated in subsequent chapters.

2.4. Options available in selecting an IOIS

2.4.1. Types of IOIS

Various classifications of IOIS exist. Most notable are those presented by Choudury (1997) and Kumar and Dissel (1996). Within the B2B IOIS context, the subtle differences in classifications are merely of historical significance. Brief descriptions of the classifications are provided to illustrate the overall IOIS context as the precursor for the B2B IOIS context. It will become clear in later

paragraphs that the IOIS type of major significance is the multilateral electronic market type, underpinned by the ebXML standard.

An IOIS may involve two participants or more. The business strategy behind the IOIS may be

- Either *competitive*, e.g., a organization might collaborate with another organization which has already collaborated with a rival of the first organization; or
- *cooperative*; in which case it may be
    - either a *strategic alliance* among a few selected organizations,
    - or a *"public good"* and is open to all organizations. (Choudury, 1997).

Choudury (1997) proposes a typology comprising three different IOIS types:

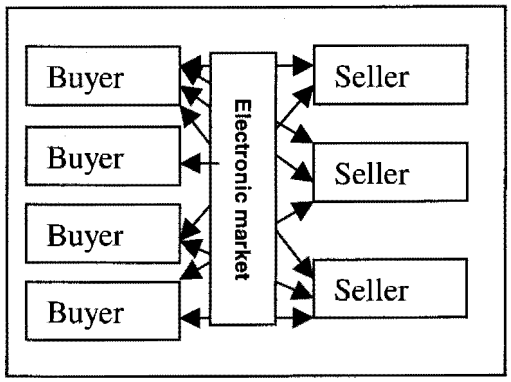
- *Multilateral IOISs*: A buyer/seller interacts with a large, potentially unlimited, number of trading partners over a single logical inter-organizational link. Examples include (cooperative) electronic markets (citing Malone et al. 1987) and (competitive) electronic shopping/broadcast sales systems. Kumar and Dissel (1996) discuss "Pooled Information Resource" IOISs in much the same way: A pooled dependency, where participants share and use common resources e.g., a common data-processing centre used by a number of organizations, common databases, common communication networks, and common applications such as used in airline reservation systems.

- *Electronic Dyads*: These are bilateral IOISs. Each buyer/seller establishes individual logical links with other selected sellers/buyers. Electronic Digital Interchange (EDI) links are a common example. Kumar and Dissel (1996) describe a similar "Networked Resource" IOIS. A reciprocal dependency exists e.g., teams from various organizations working towards designing, developing and delivering a common

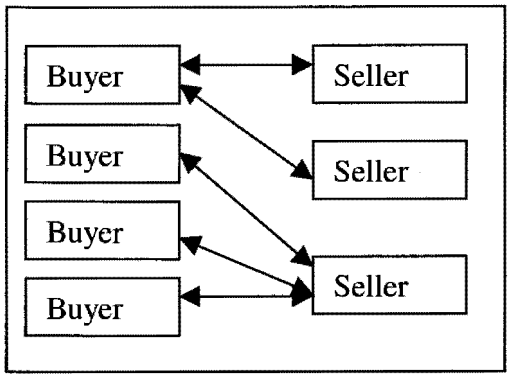
product. They typically represent joint ventures, which may be long-term or short-term. Manifestations include e-mail, fax and voice communication and even the use of desktop/screen-sharing technologies, CAD/CASE data interchange and repositories, discussion databases, synchronous and asynchronous time/place computer-based systems for supporting collaborative work and video-conferencing.

- *Electronic Monopolies*: These IOISs support a sole source relationship for a product (or set of products). They are a special case of electronic dyad - a bilateral IOIS, but only one link is established between a buyer and a seller. These IOISs are similarly depicted by Kumar and Dissel (1996) as "Value/Supply Chain" IOISs. They represent a sequential dependency, where the output of one organization becomes the input for another organization. They are strategic necessities rather than strategic advantages. The primary motives for the collaboration are the reduction of uncertainties in the supply chain, thereby gaining cost, cycle-time, and quality advantages, over competing supply chains in the industry.

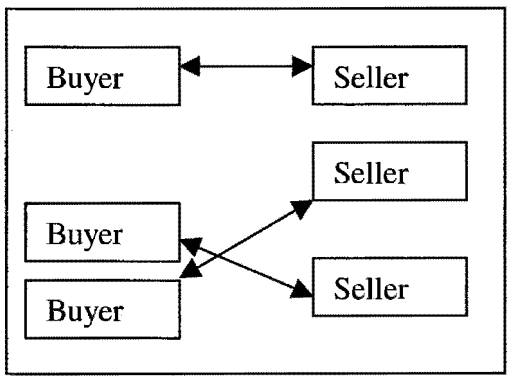
Kumar and Dissel (1996) suggest that there is a trend observed in the literature that organizations are moving (from competitive) towards more collaborative relationships. Choudury's typology is illustrated on the following page (Figure 1).



(a) Multilateral IOIS



(b) Electronic Dyads



(c) Electronic Monopolies

FIGURE 1: TYPES OF IOIS ACCORDING TO CHOUDURY (1997)

2.4.2. Management Aspects of IOISs

An important aspect of IOISs is the management concept: *sustainable collaboration* (Kumar and Dissel, 1996). The typology used by these researchers, corresponds with Choudury's typology, so Choudury's nomenclature will be used instead (for the sake of continuity).

Kumar and Dissel (1996) contend (in relation to sustainable collaboration) that:

- Increased interdependence leads to increased potential for conflict, hence the need for coordination is increased. Choudury (1997) also refers to electronic integration, the degree with which any two organizations are linked electronically. Electronic integration is generally higher in an Electronic Dyad and is highest in an Electronic Monopoly. The potential for conflict thus increases from Multilateral IOISs through Electronic Dyads to Electronic Monopolies.
- The level of structure and coordination in the relationship is of the utmost importance. Lack of structure leads to equivocality, which contributes to the risk of conflict. "Structure" is defined as "the level of specification of roles, obligations, rights, procedures, information flows, data, and analysis and computational methods used in the inter-organizational relationship."
- The greater the level of pre-specification of these coordination aspects, the greater the initial structure in the relationship. Pre-specifications are recommended as follows:
    - Muliteral IOIS - Standards and rules
    - Electronic Dyad - Standards, rules, schedules and plans
    - Electronic Monopoly - Standards, rules, schedules, plans and mutual adjustment.

2.5. Conclusion

The aim of this chapter was to introduce the context of the research problem.

Fundamental to the research problem is the concept of an Inter-Organizational Systems (IOS), which is defined in terms of electronic integration between two or more organizations. When data is exchanged or shared in such a relationship, the IOS qualifies as an Inter-Organizational Information System (IOIS) (Choudury, 1997).

Three fundamental IOIS types were identified:

- Multilateral/Pooled Information Resource,
- Electronic Dyad/Networked Resource and
- Electronic Monopoly/Value Chain. (Choudury, 1997; Kumar and Dissel, 1996).

Reasons for engaging in IOIS relationships, as well as the typical features of each, and factors influencing sustainable collaboration, were discussed. Electronic Monopoly/Value Chain IOISs have the highest potential for conflict and require the highest degree of management pre-specification (structure). Multilateral IOISs are at the opposite end of the scale.

An Extranet represents a hypermedia-based IOIS, which utilizes the public Internet and is therefore a function of the Internet's associated infrastructure, standards and protocols. Business-to-business (B2B) E-Commerce Extranets are aimed at performing electronic business within one of the various IOIS contexts described earlier. An Extranet comprises Virtual Private Network (VPN) architecture, a specialized WAN (security) strategy superimposed onto any IOIS type. The B2B E-Commerce Extranet, which is the focus of this investigation, will simply be referred to as "B2B IOIS" in the rest of this document.

The following explanation is intended to illustrate the underlying security interoperability problem within the B2B IOIS context. The concepts used will be elaborated in subsequent chapters. Suppose that trading partner A (TP_A) uses a Virtual Private Network to communicate with trading partner B (TP_B). TP_A may configure his web server to use PPTP, while TP_B may use IPSec. Thus, client computers attempting to connect to respective web servers will be unable to do so. Even if this problem is resolved, and both trading partners start using IPSec, each might configure IPSec differently. The problem is exacerbated when additional trading partners join the extranet. In a multilateral IOIS/ electronic market, numerous trading partners may collaborate with each other. The interoperability challenge exists for each two trading partners.

Chapter 3 attempts to examine current B2B IOIS models in order to refine the ultimate discussion on the interoperability problem.

Chapter 3

Current Models for B2B IOIS

3.1. Introduction

The previous chapter described the context in which a solution to the problem of security interoperability is to be sought. This chapter examines the status quo in terms of available models to achieve this end.

The focus of this chapter will be on ebXML (explained in detail below) as a reference model upon which to build B2B IOIS solutions. EDI will be described only very briefly as it is envisaged that ebXML will supplant EDI in the near future (see below). The framework architecture proposed in Chapter 5 attempts to incorporate ebXML. However, ebXML forms only part of the proposed framework and is not essential for ensuring interoperability. As a standard for B2B interaction, it provides an open platform, rather than a prescription for how to ensure interoperability. Indeed, it is this need for more comprehensive guidelines that have made this research necessary.

3.2. Electronic Digital Interchange (EDI)

EDI refers to the exchange of electronic business documents, e.g. invoices, debit notes, etc, between trading partner applications. No paper – and minimal human intervention - is involved. The documents are formatted according to published standards. (Greenstein and Feinman 2000:101).

EDI standards from the Accredited Standards Committee X 12 (ASC X12) in the USA and the United Nations' EDI for Administration, Commerce and Transport

(UN/EDIFACT) have in the past provided specifications (transaction sets) for electronic business exchanges between trading partners. A concerted effort is being made towards unifying these standards.
(Schneider and Perry, 2001:331-345, Greenstein and Feinman 2000:109).

EDI typically involves third party network services, called value-added-networks (VANs). These services include EDI translation software, security assurances of data, reliability of service due to multiple alternative telecommunication links, EDI systems development assistance, and employee training sessions. The VAN executes only valid (authorized) transactions between valid trading partners, as prescribed by a signed contract. VANs may be partially or fully integrated. (Greenstein and Feinman 2000:104-107).

However, some of the shortcomings of the EDI model include the following:

- Only large companies have been able to afford to implement EDI and EDI implementations generally involve a dominant partner imposing a specific approach on its other partner(s).
- It also requires specialized technical knowledge, is tightly-coupled, requires expensive dedicated networks and comprises an inflexible architecture.

(UN/CEFACT and OASIS[2], 2001, Greenstein and Feinman, 2000:101-102).

- Extrapolating Choudury's classification (previous chapter), EDI seems to typify the electronic monopoly IOIS, which is predicated by higher electronic integration and increasing conflict. A greater degree of pre-specification would therefore be required for sustainable collaboration (as described in Chapter 2).
- The costs of EDI software, hardware and monthly Value-added network (VAN) connection fees have rendered EDI cost-prohibitive to most small and medium-sized companies (Greenstein and Feinman, 2000: 102).

The previous paragraph outlines some of the disadvantages of EDI, which have probably detracted from its wider use between trading partners. With the advent

of the Internet, a mechanism for using EDI standards on the Internet became possible (without, inter alia, the need for expensive leased lines). *Open EDI* refers to using EDI on the Internet. Extensible Markup Language (XML) is considered an important tool in this context because of its flexibility in creating and manipulating data elements (Schneider and Perry, 2001:331-345).

The Electronic Data Interchange-Internet Integration (EDIINT) standard defines the use of encryption and digital certificates to secure Open EDI (Greenstein and Feinman, 2000: 117).

Thus, a more accessible tool, XML, could be used by developers at each end. Further, since a concomitant standard for ensuring security also became available, security requirements could be addressed.

EDI web browser packages provide client software for connecting to EDI trading partners. Web forms are translated (to ASC X12 format) using software such as IBM's Information Exchange. Typically, a repository of web forms is available through a VAN. The forms may be customised by individual firms. (Greenstein and Feinman, 2000: 123).

It may be deduced from the above that both EDI and Open EDI are open to an endless variety of customisable forms. Further, neither makes any provision for discovering trading partners and establishing trading partner agreements electronically. Also, each two trading partners would have to individually negotiate the means to ensure interoperability at various levels. These deficiencies – and others - are addressed by ebXML, which is discussed in the next section.

3.2. Electronic Business Extensible Markup Language (ebXML)

Unless otherwise referenced, the material in this section comes from UN/CEFACT and OASIS[1,2,5,6,7,9,10,11], 2001.

In May 2001, the technical architecture for a new electronic business de jure standard was released. It is called ebXML[1] (electronic business XML). ebXML is a suite of specifications for electronic business data exchange, developed by the United Nations body for Trade Facilitation and Electronic Business (UN/CEFACT) and the Organization for the Advancement of Structured Information Standards (OASIS), together with international industry groups.

ebXML is built on the following published goals:

- To provide an infrastructure that ensures data communication interoperability;
- To provide a semantics framework – as is the case with EDI specifications - that ensures commercial interoperability; and
- To provide a mechanism that allows prospective trading partners to discover each other, create collaboration agreements and conduct business with each other, over the Internet.

It is envisaged that all of these operations be performed automatically, with minimal, if any, human intervention.

The ultimate goal is to provide an XML-based open framework for creating a "single global electronic market". There are three categories of ebXML task team deliverables (available from the website indicated in footnote 1) from which additional information may be obtained:

- *Technical Specifications*: These specify components of the ebXML System and conform to the ebXML Requirements document.
- *Technical Reports*: These are either guidelines or catalogues.
- *White Papers*: These constitute a "snapshot" of on-going work within a Project Team.

[1] http://www.ebxml.org/

The content of the above literature appears to support Choudury's classification (previous chapter). The "electronic market" concept in ebXML purports to enable collaboration for the common good (as opposed to competitive gain). It goes beyond supporting established value chains, allowing both buyers and sellers to trade in a many-to-many fashion with other buyers and sellers, as depicted in Choudury's "multilateral electronic market" IOIS.

The ebXML specifications utilize XML as a platform for the following reasons:

- XML is an open and freely available document from the World Wide Web Consortium (W3C);
- It allows parties to exchange structured data, as is kept in databases, over the Internet;
- It supports Unicode that enables the display and exchange of various languages in the world; and
- It is supported by prominent information technology companies, such as Microsoft and IBM.

ebXML is also globally supported by standards organizations, e.g. ASC X12, the Data Interchange Standards Association, PeopleSoft Incorporated, XML/EDI Group, GENCOD-EAN France and XMLGlobal. Further, ebXML is based on Internet technologies using open standards such as: HTTP, TCP/IP, MIME, SMTP, FTP, UML, and XML. It is thus vendor-neutral. It can also be implemented and deployed on most computing platforms, using most programming languages. The designers anticipate that businesses of all sizes will adopt ebXML for reasons of lower development cost, flexibility, and ease of use.

From the perspective of interoperability, specifically security interoperability (between trading partners), the actual ebXML architecture is examined in the following section. The subsequent section (3.2.2.) examines relevant aspects in the actual use of ebXML.

3.2.1. Architectural overview

ebXML is an end-to-end solution, but is intended to be modular in nature. It is envisaged by the designers that ebXML compliant "off-the-shelf" software will become available in the near future.

As mentioned in the goals of ebXML, in the previous section, in order for enterprises to conduct electronic business with each other, they must:

- Discover each other and the products and services they have to offer.
- Determine which shared business processes, and associated document exchanges, to use for obtaining products or services from each other.
- Determine the contact points and form of communication for the exchange of information.
- Agree on the contractual terms on the above chosen processes and associated information.

Thereafter, they should be able to exchange information and services (in an automated fashion) in accordance with these agreements.

The design is aimed at providing the infrastructure to ensure data communication interoperability, by way of:

- a standard message transport mechanism with a well defined interface, packaging rules, and a predictable delivery and security model; and
- a business service interface that handles incoming and outgoing messages at either end of the transport

It also provides a semantics framework to ensure commercial interoperability, comprising:

- a metamodel for defining business process and information models;

- a set of re-useable business logic based on core components that reflect common business processes and XML vocabularies; and
- a process for defining actual message structures and definitions as they relate to the activities in the business process model.

The third goal - the mechanism to allow enterprises to find each other, agree to establish business relationships, and conduct business - is provided through:

- a shared repository where enterprises can register and discover each other's business services via partner profile information;
- a process for defining and agreeing to a formal Collaboration Protocol Agreement (CPA), if required; and
- a shared repository for company profiles, business process models and related message structures.

The essential ebXML architecture is depicted in the diagram (Figure 2) below:

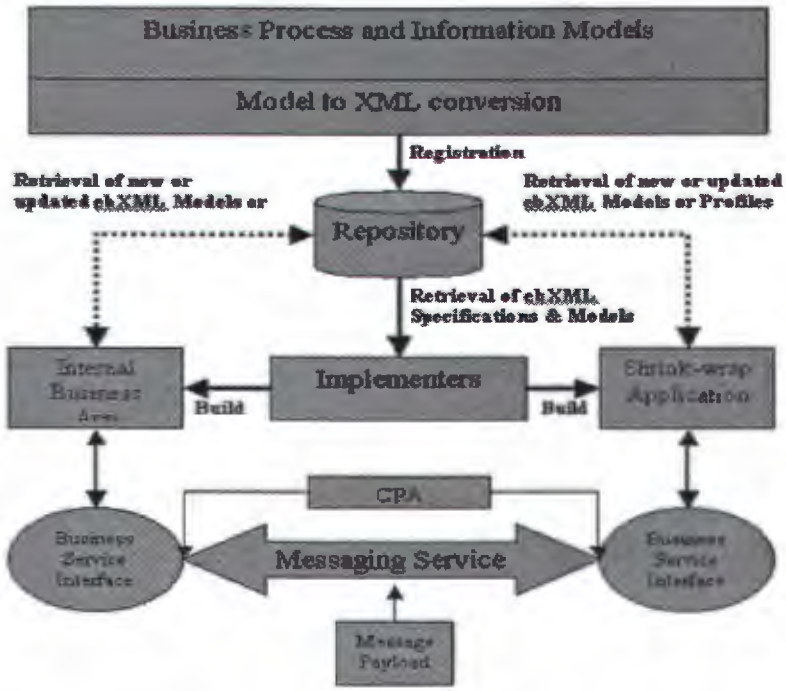


FIGURE 2: ebXML TECHNICAL ARCHITECTURE (UN/CEFACT AND OASIS[1], 2001)

The technical architecture is composed of five main areas of emphasis (see Figure 2):

- Business Process and Information Model;
- Company Profiles;
- Messaging Services;
- Registry & Repository; and
- Collaborative Partner Agreements.

The Business Process models define how business processes are described. Business Processes can be represented using modelling tools. The specification for business process definition enables an organization to express its business processes so that they are understandable by other organizations. This enables the integration of business processes within a single company, or between different companies.

The Information models define reusable components that can be applied in a standard way within a business context. These Core Components are defined using identity items that are common across all businesses. This enables users to define data that is meaningful to their business while maintaining interoperability with other business applications.

The ebXML Messaging Service specification defines the set of services and protocols that enables electronic business applications to exchange data. The specification allows any application-level protocol to be used. These can include common protocols such as SMTP, HTTP, and FTP. Well established cryptographic techniques can be used to implement strong security. For example, secure protocols such as HTTPS can be used to ensure confidentiality. In addition, digital signatures can be applied to individual messages or a group of related messages to ensure authenticity.

The Registry and Repository provides a number of key functions. For the user (application) it stores company profiles and Trading Partner specifications. These give access to specific business processes and information models to allow updates and additions over time. For the application developer it will store not only the final business process definitions, but also a library of core components.

The Collaborative Partner Agreement (CPA) defines the technical parameters of the Collaborative Partner Profiles (CPP). This captures critical information for communications between applications and business processes and also records specific technical parameters for conducting electronic business.

3.2.2. Using ebXML

Using ebXML is essentially a four step process, as illustrated in Figure 3 below. These activities may be performed in slightly different sequences and with different scope and focus, depending on the actual context. The activities considered important are:

1. The design and registration of business processes and information models.
    a. The implementer browses the repository for appropriate business processes, or for the process the intended partner is registered to support.
2. The Implementation of business service interfaces and registering Collaborative Partner Profiles.
    a. The implementer buys, builds, or configures application(s) capable of participating in the selected business process.
    b. The implementer registers his (software's) capability to participate, in the form of a Collaborative Partner Profile (CPP).
3. The negotiation of technical details and/or functional overrides, and the drawing up of the result in the form of a CPA between the two parties .

a. Parties optionally register the CPA on the ebXML Registry.

4. The sending and receiving of ebXML messages containing ebXML business documents, over the ebXML Messaging Service.

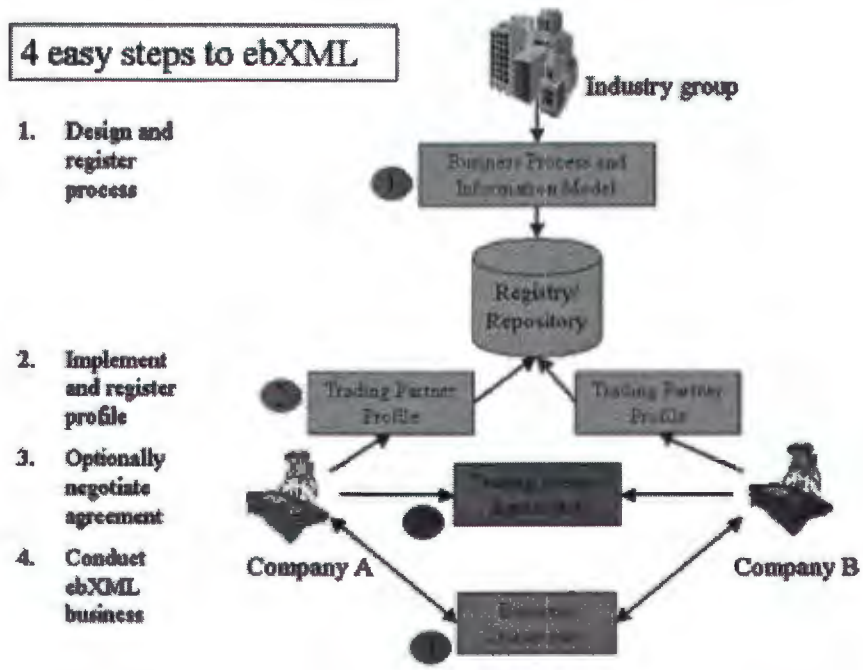


FIGURE 3: USING ebXML (UN/CEFACT AND OASIS[1], 2001)

In this section, the mechanism of how ebXML is expected to function was outlined. The following section examines how ebXML makes provision for security interoperability.

3.2.3. ebXML and Security

eXML messages are specified as Simple Object Access Protocol (SOAP) Objects. While the Messaging Service specification recommends the use of XML digital signatures (still under development by the W3C/IETF) and Secure IP (IPSec), the Message Service Handler in the specification currently supports only persistent XML digital signatures. Secure Multimedia Internet Mail Extensions (S/MIME) is recommended for ebXML payloads (SOAP messages).

The ebXML specifications identify the more obvious risks, but recommend that each trading partner uses BS7799/ISO17799 to complete a thorough risk analysis for security management purposes. A policy-based framework and a layering architecture for security are recommended.

A White Paper on ebXML security concludes that in the current version of the CPP/CPA, the specification of security elements is limited. It recommends that XML schema be utilized for more effectively expressing security attributes. Currently, the security characteristic is a single XML element that contains attributes with Boolean values indicating whether or not a security attribute has been addressed. The paper concedes that it would be more appropriate to indicate the type of the security characteristic with a reference id to include on lower elements (like the transport element), which contain the details, such as the protocol. Thus, actual security control parameters have not yet been addressed effectively to take into account the required granularity.

3.3. Conclusion

This chapter identified and described EDI and its successor, ebXML. ebXML is the standard upon which most future B2B IOISs are likely to be built. However, the standard currently lacks clear specifications on exactly which security implementations may be used to ensure interoperability. It recommends the use of IPSec and XML Digital Signatures, but provides very limited specification detail and no guidance on how this should be implemented, except that the details should be elaborated in lower security elements in the relevant XML schemas.

However, the components which make up the ebXML architecture have been derived from the collaborative efforts of representatives of most major software industry players, and will thus almost certainly become the common modus operandi for setting up B2B IOISs.

Chapter 4

Integrating B2B IOIS Security Implementations: Exactly what is available?

4.1. Introduction

This chapter deals with security mechanisms (controls) to realize information security services, which in turn are required to counter specific information security threats. The intention of this chapter is not to provide an in-depth analysis of the practice of computer security, or of network security. It does not deal with security policies, risk analysis, general security design, monitoring, logging, auditing, applying forensic analyses, or damage control – all part of the process of computer security (Wadlow, 2000: vii-xi). Further, physical security, denial-of-service vulnerabilities (including virus, worm and Trojan attacks), operating system hardening, and network segmentation (using Virtual LANs, VLANs), will also not be considered.

The overall context of this chapter is information security in TCP/IP (Internet-capable) networks, specifically as it relates to B2B IOISs. The main thread of this chapter is intended to be an investigation of which technologies are available for providing interoperable security in B2B IOISs. This information will be used, in Chapter 5, to arrive at a suggested framework based on the most suitable of these technologies.

It will be demonstrated in subsequent sections that encryption is (currently) at the heart of security services on the Internet; thus, its implications for B2B IOISs will be examined first.

4.2. Encryption

As indicated in Chapter 1, encryption is generally used to ensure confidentiality. In a B2B IOIS context, the other security services – integrity, authentication, access control and non-repudiation – are essential, but must also be implemented to ensure interoperability between the connected systems. Encryption and the various ways in which it may be implemented are therefore discussed in terms of achieving this aim.

4.2.1. Symmetric Encryption

Recall from the definition of encryption in Chapter 1 that plaintext (P) is encrypted to yield a ciphertext (C), which in turn is decrypted to yield P. A *symmetric* cryptographic algorithm is used to apply a secret key (K) – known only to the sender and receiver – to both the encryption and decryption transformations. Symmetric encryption may generally be depicted as follows:

- $E_K (P) = C$ for encryption, and
- $E_K (C) = P$ for decryption.

(Inter alia, Hassler, 2001:15-16).

An alternative notation also used in this document is:

- $E (P, K) = C$ for encryption, and
- $E (C, K) = P$ for decryption.

4.2.1.1. Advanced Encryption Standard (AES)

The new de jure standard for symmetric encryption is the Advanced Encryption Standard (AES). The significance and relevance of AES will only be examined in the light of its implications for B2B IOIS security. The following is an attempt to summarize the actual AES formal specification (NIST[1]: 4-50):

AES/Rijndael algorithm is a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. It was designed to accommodate additional block sizes and key lengths, but these were not adopted in the standard. The algorithm variants may therefore be referred to as "AES-128", "AES-192", and "AES-256". The previous standard, Data Encryption Standard (DES), processed 64-bit data blocks with a key length of 56 bits. The number of rounds varies according to the key length; it is therefore 10, 12 or 14, respectively. The basic unit for processing in the AES algorithm is a byte. The input, output and cipher key bit sequences are processed as arrays of bytes.

Rijndael was adjudged to be the best overall algorithm for AES for the following primary reasons (Nechvatal et al, 2000:13-16):
(All the security and algorithmic concepts mentioned in the list are discussed in the reference).

- It appears to be a consistently very good performer in both hardware and software across a wide range of computing environments in both feedback and non-feedback modes.
- Its key set-up time is excellent, and its key agility is good.
- It has very low memory requirements, which make it very well suited to restricted-space environments. It also demonstrates excellent performance in this situation.
- Rijndael's operations are among the easiest to defend against power and timing attacks, without significantly impacting on its performance.

- Rijndael is designed with some flexibility in terms of block and key sizes, and the algorithm can accommodate alterations in the number of rounds used.
- Rijndael's internal round structure appears to have good potential to benefit from instruction-level parallelism.
- Although future computing platforms are unpredictable, to some extent, as is the wide range of environments in which AES will be implemented, "Rijndael's combination of security, performance, efficiency, implementability, and flexibility make it an appropriate selection for AES for use in the technology of today and in the future".

It seems, therefore, quite clear that if symmetric encryption is to be used as part of the overall solution, that the algorithm of choice should be AES.

4.2.1.2. Shortcomings of Symmetric Encryption for B2B IOIS

A central consideration in the use of AES – as it has been for its predecessors – is the distribution of the secret key that is used for generating the key schedule. For decryption, the inverse cipher algorithm must be employed on the receiver's end, using the same secret key. Various key exchange protocols are available, which include key transport protocols and key agreement protocols (Hassler, 2001:51). The intrinsic vulnerabilities associated with key distribution (including frequency of changing keys) are amplified as the number of users increases. For n users, the number of keys is given by $n(n + 1)/2$ (Pfleeger, 1997:129).

Another problem is: deciding how often to change a key. This dilemma exists because of (a) the necessity to change keys regularly to reduce the amount of ciphertext available from one key (to reduce the amount the cryptanalyst has to work with), and (b) the need to keep keys, to resolve disputes years after a contract has been signed (Ibid).

A possible solution to these problems resides in the use of a *central key distribution centre (KDC).*

4.2.1.3. Central Key Distribution Centres (KDCs)

Using a KDC involves the following steps, as described by Pfleeger (1997:131-132):

- User *A* sends to the central key distribution service (repository) a request: (A,B,I_A), where *A* and *B* are the identities of the recipients (of messages), and I_A is the unique identifier for *A*'s requests (if more are possible). This information need not be encrypted.
- The repository generates a secret key K_{AB}, encrypts it with a unique second key K_A (shared by the repository and *A*) and sends it to *A* as $E(I_A,B,K_{AB},E((K_{AB},A),K_B),K_A)$, which is
    - The unique message identifier for this key request (I_A),
    - *B*'s identification (B),
    - A key for communication between *A* and *B* (K_{AB}) and
    - A string containing his identification and the same key, encrypted under the distribution centre's key shared with *B*, (i.e. K_B) thus: $E(K_{AB},A),K_B$.
    - *A* cannot decrypt this, but can send it to *B*.
- *A* sends $E((K_{AB},A), K_B)$, to *B* who is able to decrypt it with K_B (shared by the repository and *B*).

A key (K_{AB}) may thus be successfully distributed to both A and B, without A and B having initially shared a key.

The advantages of this approach include (Ibid):

- The number of keys is reduced. Adding a new user requires only one key shared with the key distribution centre.

- Users can change keys as often as they like, simply lodging the new key request with the distribution centre.
- No prior private exchange between users before key registration is required.

There are, however, disadvantages to this approach. Pfleeger (Ibid) lists the following:

- Flexibility is reduced, since the server has to be used for all changes.
- The key distribution centre must be constantly available.
- The key distribution centre is a potential bottleneck.
- The key distribution centre is a target for attack, disablement or impersonation.

KDCs are similarly discussed by Kaufman et al (1995:189-190, 243). Additional shortcomings of KDCs are discussed in the next section.

4.2.1.4. Shortcomings of KDCs for B2B IOIS

The steps outlined above presuppose that the KDC and A share a secret key (K_A). This is also the case for the KDC and B (where K_B is shared). A glaring problem with this approach is: How are K_A and K_B distributed to A and B without risk?

Asymmetric encryption is an attempt to address this particular problem.

4.2.3. Asymmetric Encryption

In asymmetric encryption algorithms – also called public key algorithms – two algorithmically-related keys are used (Gollmann, 1999:212).

The following information on public-key cryptography is based on the following source: Greenstein and Feinman, 2000:235-240.

The public-key cryptography concept was promulgated by Diffie and Hellman in 1976. It allows a sender and receiver to generate a shared, secret key over an insecure telecommunications line, thereby addressing the problem of distributing secret keys. Their method, as well the RSA method (developed by Rivest, Shamir and Adelman), will be explained below.

4.2.3.1. The Diffie-Hellman Algorithm

This algorithm is based on the following steps:

1. The sender determines a secret value *a*.
2. *a* is used to derive another value *A*, which is made public.
3. Similarly, the receiver determines a secret value *b*, from which another value *B* is derived, and made public.
4. The Diffie-Hellman algorithm is used to calculate a secret key corresponding to the key pairs (*a*, *B*) and (*b*, *A*).

It is computationally infeasible to determine *a* and *b* from simply knowing *A* and *B*, respectively. The secret key is thus shared, without it having been transmitted to A and B.

4.2.3.2. Shortcomings of the Diffie-Hellman Algorithm

The Diffie-Hellman algorithm is vulnerable to man-in-the-middle attacks, where the public values A and B could be replaced by an interceptor's own public value, Z. The sender and the receiver will then generate (a, Z) and (b, Z), respectively. The sender and receiver would be unaware that they do not share a secret key. The interceptor would then generate (z, A) and (z, B) to decrypt messages from A and B. The messages could be altered and then be forwarded to the receiver.

To overcome this problem, a means for ensuring authentication of the sender and message integrity is therefore required.

4.2.3.3. The RSA Algorithm

The RSA algorithm is based on key pairs (a public key and a private key) generated from a one-way function with an intentional "trap-door". It does not rely on anyone else's public values; therefore, it is not vulnerable to man-in-the-middle attacks. The trap-door allows for reverse computation with the use of a precise piece of information. However, for the cryptanalyst, deriving the private key by reverse computation requires the factoring of large prime numbers, which makes the process extremely difficult.

4.2.3.4. Shortcomings of the RSA Algorithm

The following are noted shortcomings (for both RSA and Diffie-Hellman asymmetric cryptography):

- The sender may use her private key to encrypt a message and the receiver would use the sender's public key to decrypt it. However, anyone with the sender's public key may decrypt the message. Thus, message confidentiality may be compromised.
- The sender may use the receiver's public key to encrypt the message and the receiver would use his own private key to decrypt it. Here, the authentication of the sender presents a problem, since the message could have come from anyone who has the receiver's public key.
- Public key cryptography (as exemplified by the RSA algorithm) is not as computationally efficient as symmetric encryption. For example, Digital Encryption Standard (DES) – the previous symmetric encryption standard - is 100 times and 1000 times faster than RSA on software and hardware platforms, respectively.

To overcome the latter problem, Greenstein and Feinman describe replacing RSA with DES. The message is encrypted with DES. The smaller (than the message) DES key, used to encrypt the message, is then encrypted with the receiver's public key. Both the encrypted message and the encrypted key are sent to the receiver. Only the receiver's private key can decrypt the DES key, which is necessary for decryption of the message. Thus, message confidentiality is ensured. (Ibid:238-241).

In the explanation above, it seems evident that DES could be replaced with AES, with the same results. Although AES has larger keys, AES is much faster than DES. However, authentication of the sender remains a problem.

One way in which authentication of the sender can be ensured, is to use digital signatures, which utilize hashing algorithms. (Another way is by using digital certificates which will be discussed in a subsequent section). Digital signatures are discussed in the next section.

4.2.3. Digital signatures

Digital signatures bind the message sender with the exact contents of the message. This provides both integrity and sender authentication. Digital signatures make use of hash algorithms with one-way functions, which transform a message into a message digest or hash. Unlike with other encryption, message digests are not intended to be decrypted. (Ibid:242).

The hashed message is encrypted with the sender's private key (sender authentication). The encrypted message digest together with the original, unencrypted message is sent to the receiver. The receiver's software uses the original, unencrypted message to create the same message digest, by using the same hashing algorithm. The encrypted message digest is then decrypted with the

sender's public key. The two message digests are compared. If they are identical, the digital signature is considered valid and integrity of the message has been preserved. This description, depicted in Figure 4, applies in particular to MD5 (an example of a hash algorithm).

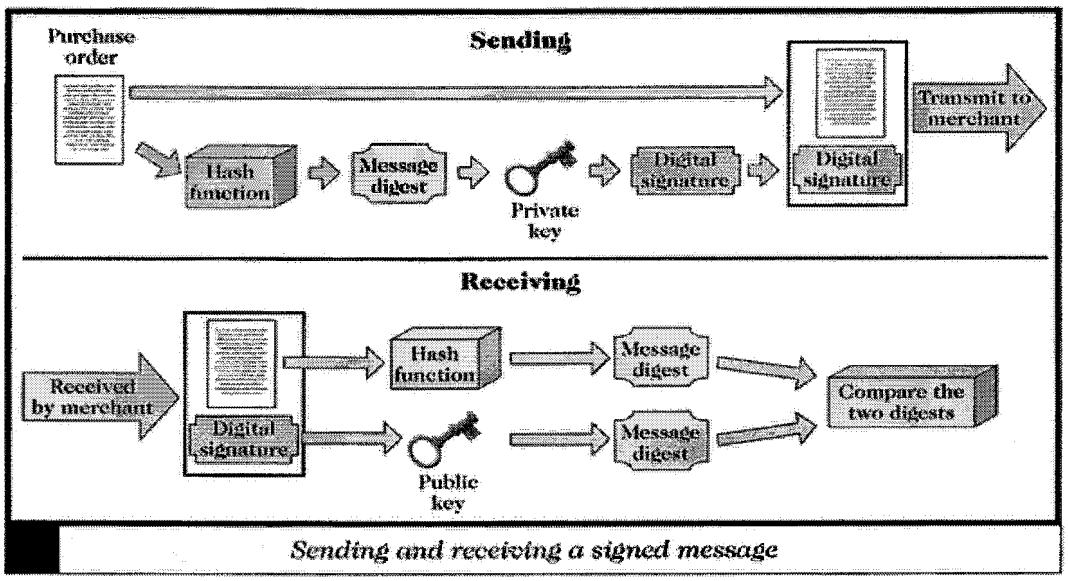


FIGURE 4. USING DIGITAL SIGNATURES (SCHNEIDER AND PERRY, 2001:225).

Examples of hash algorithms are: SHA-1 (developed by NIST for NSA) and MD5 (from RSA), and Digital Signature Algorithm (DSA), which is defined by NIST's Digital Signature Standard (DSS).
(King et al 2001: 354-358).

4.2.3.1. Shortcomings of Digital Signatures

Digital signatures still appear to have a flaw: Unless the receiver has personally taken possession of the sender's public key directly from him/her, simply having

the sender's public key may still not irrevocably attest to the sender's identity. (Ibid).

Digital certificates, while not a panacea, seem to address this problem.

4.2.4. Digital certificates

Digital certificates are managed by trusted third parties, called Certification Authorities (CAs). CAs make public keys available to interested parties, but also bind a public key to a particular name. Further, public key certificates are digitally signed by the CA. These digital certificates are considered legally binding. (Hassler, 2001:41).

The sender's public key is housed in the certificate. The CA acts as a notary public, vouching for the sender as the owner of the public key. The certificate has similar characteristics to a passport:

- It is unique to the individual and carries his/her unique identification details
- It is issued by a trusted third party
- It is universally accepted as a means of identification
- It has a fixed validity period
- It is tamper-proof.

(King et al, 2001: 359).

These characteristics are defined by digital certificate standards. Several such standards have been described, but the "most advanced and widespread specifications" are defined by the X.509 Working Group (PKIX) of the Internet Engineering Task Force (IETF). (Also very influential in this area is the Public Key Cryptography Standard (PKCS) from RSA Security Laboratories). The collection of components and procedures required to support the management of

digital certificates is known as Public Key Infrastructure (PKI). Hence, the PKIX standard (RFC 2459), defines the PKI X.509 version 3 certificate.

An X.509 version 3 certificate contains specific fields such as: Issuer CA name, subject name and validity period; it also contains the subject's public key (as a delimited hexadecimal text field). The CA digitally signs the certificate before sending it to the subject.

The following services are supported by the use of digital certificates:

- *Web authentication and channel privacy*: This is effected using protocols such as Netscape's Secure Sockets Layer (SSL) and the IETF's Transport Layer Security (TSL). These protocols will be examined later.
- *Signed and encrypted messaging*: Certificates and associated keys can be used to encrypt and digitally sign e-mail messages; this is implemented in protocols such as Secure Multi-purpose Internet Mail Extensions (S/MIME).
- *Signed transactions and form signing*: Here digital signatures are used.
- *Network operating system, host and mainframe authentication*: Certificates, such as Kerberos certificates, are used to authenticate users. This will also be examined later.
- *Remote access*: The distributed employee work force can connect to corporate resources and be authenticated using certificates
- *Virtual Private Networks*: This uses an encrypted tunnel to allow secure transmission along the Internet infrastructure.
- *File Encryption*: This is for authenticating users allowed access to sensitive data.
- *Software code signing*: This is to ensure that software (especially updates) are being provided by trusted sources.

(King et al, 2001:347-350).

A tutorial by Hunt (2001:1460-1471) provides a detailed account of the operation of PKI, the issues surrounding its operation and the problems that need to be

addressed to ensure its widespread use. The following section is a brief overview of PKI.

4.2.5. Public Key Infrastructure (PKI)

The following explanation is based mainly on material from Greenstein and Feinman (2000:248-254) and Hunt (2001:1460-1471).
A PKI system consists of three main functional parts:

- Certification authorities (CAs): Trusted entities that issue and revoke public key certificates and certificate revocation lists (CRLs).
- Registration Authorities (RAs): Entities that are trusted by CAs to register or attest to the identities of CA users.
- Certificate Repositories (CRs): Publicly accessible databases that hold information such as certificates and CRLs.

Hunt adds two further components: A security policy and PKI-enabled applications (Hunt 2001:1461).

A distributed hierarchy of CAs and RAs generally exists to ensure scalability and reliability, with the "Root CA" at the apex. Cross certification is the process by which CAs agree to recognize one another's authority. When a certificate has been revoked (due to it having been compromised or lost), it is added to the CRL for the CA. Various levels of certificates exist, based on the level of authentication the owner wishes to convey with his messages.

This protocol uses the concept of one "vouching for" (attesting to the identity of) someone else in a chain-of-authentication hierarchy. Each consecutive authenticator trusts the authenticator immediately above it.

An entity at the top of the hierarchy selects a key pair, publishes the public part and retains the private part. An entity immediately below creates a public key pair, puts the public key in a message together with its identity, and passes the message securely to the top-level entity above it. The top-level entity signs it, by creating a *hash value* of the message and then encrypting the message and the hash with its private key. By signing the message, the top-level entity affirms that the public key and the identity are for the same lower-level entity. The message is the latter's *certificate.*

The next-level entity/entities also create messages with their public keys. The entity at the immediate-higher level hashes each message, signs it with her private key and appends its own certificate, and returns the certificates. Thus, for any entity lower down the hierarchy, a certificate consists of its certificate combined with all the certificates of the entities hierarchically above it.

4.2.5.1. The (Technical) Suitability of PKI for B2B IOISs

At this juncture, it is apparent that PKI provides the most appropriate answers to technical problems in respect of B2B IOIS security. The main (technical) disadvantage is that it relies on trusting the topmost entity in the certificate hierarchy (Pfleeger, 1997:135-140). The major advantage of PKI is that it provides secrecy, authentication, integrity and non-repudiation (Hunt, 2001: 1460).

PKI-enabled applications are used to implement, inter alia, Secure Sockets Layer (SSL), Secure MIME (S/MIME) and Virtual Private Networks (VPNs) (Ibid:1462). Some of these are discussed below in order to identify the most appropriate for B2B IOISs.

4.2.6. Secure Sockets Layer (SSL) and Secure HTTP (SHTTP)

SSL is the predominant protocol for providing security services for HTTP traffic, although it is application-independent. Both Microsoft's Private Communicating Transport protocol (PCT) and SHTTP have been deprecated in favour of SSL in the popular browsers (Oppliger, 2000: 132-133).

Canavan (2001:80-82) states the following in respect of SSL:

- It was developed by Netscape to protect information being transmitted on the Internet, e.g. in the sending of credit card information
- It utilizes both symmetric and asymmetric encryption
- It generally establishes a secure HTTP encrypted tunnel between a client and a server; this is referred to as secure HTTP or HTTPS.
- Confidentiality is maintained by encryption and integrity is established with hashing algorithms.
- To set up SSL, both sides exchange random numbers. The server authenticates itself by sending a CA-signed digital certificate. It also sends a session ID. The browser client creates a pre_master_secret key, which it encrypts with the server's public key and transmits it to the server. Then both sides generate a session key using the pre_master_secret and random numbers. The session key is used to encrypt all messages between the client and the server, for the duration of the session.
- The switch-over to symmetric encryption creates much less overhead.
- SSL is connection-oriented and operates at the transport level.
- An alternative to SSL is secure HTTP (SHTTP) developed by Enterprise Integration Technologies. The latter is transaction-oriented and operates at the application level (of the OSI Reference Model); each individual message is encrypted.

- SSL may be used for other TCP/IP suite protocols, such as FTP and TELNET, while SHTTP is designed only for HTTP. Hence, SHTTP is very rarely used, while all major browsers support HTTPS.
- SSL requires a PKI for optimum efficiency.

SSLv3 (SSL, version 3, also known as Transport Layer Security or TLS) is the current IETF standard (Hunt, 2001:1466).

4.2.6.1. Shortcomings of SSL for B2B IOIS

Greenstein and Feinman (2000: 297), state that SSL with digital certificates are not commonly used.

SSL diminishes network throughput significantly, as cryptographic processing is extremely CPU-intensive. Canavan (2001:80-82) cites a 1999 Sun Week study in which a Sun 450 Server is able to handle 500 connections per second, which drops to 3 transactions per second when SSL is employed.

Further, SSL does not protect against traffic analysis. The source and destination IP addresses and TCP port numbers and volume of transmitted data is unencrypted. This allows an interceptor to determine which parties are interacting, the types of services they are using, and even information about business and personal relationships (Oppliger, 2000:134).

The following section examines the feasibility of using Kerberos in the B2B IOIS context.

4.2.7. Kerberos

The following summarizes the salient points about implementing Kerberos as a cryptographic option (Phaltankar 2000: 149-152):

- It was originally designed at MIT as part of the Athena project; the latest version (5) is documented in RFC 1510.
- It is used for authentication and access control, but avoids using passwords on a clear channel.
- The user data is currently encrypted using DES. (It seems fair to speculate that later implementations could use AES).

The following is a simplified explanation of Kerberos operation (Kanavan, 2001: 72-78):

- Step 1. The client creates a request to send to the Kerberos server. The client, using his/her own private key, digitally signs the request.
- Step2. The digitally signed request is then encrypted using the Kerberos server's public key.
- Step 3. This is sent to the Kerberos server.
- Step 4. The Kerberos server uses its private key to decrypt the message. It then uses the sender's public key to verify the digital signature of the sender. All authorized users have public keys in the database of the trusted server.
- Step 5. If the client has access authorization, then the server sends identical session tickets to both the client and the server providing the services. For this, the respective public keys of the client and the server are used.
- Step 6. Both the client and the server decrypt the session tickets using their respective private keys. The tickets could also be digitally signed by the Kerberos server to verify the source of the tickets.
- Step 7. The client then sends a copy of its ticket to the server (providing the services), encrypted with the server's public key.
- Step 8. When the server receives the encrypted ticket from the client, it decrypts it with its own private key. It matches this ticket

with the one received from the Kerberos server. If they match, the connection is established.

- Step 9. The systems can encrypt the communication using either the session key or the client's public key, or they can use no encryption at all.

These steps are repeated for each new service.

4.2.7.1. The Suitability of Kerberos for B2B IOIS

The following are advantages of Kerberos:

- No password information is sent over the network
- User access to all applications is controlled by the user's profile.

Phaltankar (2000:149-151)

- While PKIs rely on CRLs to remove authorization for an individual or entity, both revocation and authentication can be done immediately with Kerberos.
- Like a PKI, Kerberos key exchange relies upon public key cryptography and digital signature technology. It uses both secret key and public key cryptography. It uses a single central server as the trusted third party, based on the premise that it is impossible to secure all the servers in a distributed computing environment, but that it is possible to truly secure a single server. Hence, it is more secure to control all network access from one single secure server.

(Kanavan, 2000: 77-78).

The following are disadvantages of Kerberos:

- Kerberos is a single sign-on (SSO) authentication scheme. Every Windows 2000 domain controller is a KDC. Thus it seems expedient to simply plan more domains, in order to delegate Kerberos control to each domain controller (for the sake of scalability). However, each application

still has to be "Kerberized". An added problem is the changing of passwords of the centralized application and that of the application itself. For UNIX, The MIT Kerberos distribution includes a standard replacement for the login program.

(King et al, 2001:328).

- There are several extensions to the basic Kerberos authentication system developed by MIT, e.g. Yaksha, SESAME (secure European system for applications in a multi-vendor environment) and DCE (Distributed Computing Environment) developed by the Open Group (the 1996 consolidation of the Open Systems Foundation (OSF) and X/Open Company Ltd., which includes, among others, technology vendors IBM, Microsoft and DEC). In Microsoft's Windows 2000 (NT 5), Kerberos is used as a single sign-on (SSO) system to log into the NT domain (as mentioned above). The domain controller acts as the Kerberos Distribution Centre (KDC), which includes the Authentication Server (AS) and the Ticket Granting Server (TGS). Kerberos may also be used to feed the Security Association (SA) database of a corresponding IPSec implementation. Microsoft enhancements are similar to SESAME and DCE enhancements, but are not compatible with them.

Oppliger (2000:123-124)

- All services have to be "Kerberized" on both the client and server sides. This requires the source code for the applications.
- The Kerberos server represents a single point of failure.If the Kerberos server is compromised, the network is compromised.
- Workstations have to be single-user; multiple users would allow certificates to be stolen.

(Phaltankar (2000:151)

- A major disadvantage is denial-of-service attacks (even simply flooding the server with requests or flooding the network with traffic). Kerberos can be susceptible to replay attacks. This can be avoided by the use of timestamps.

- Also, the server is prone to scalability issues – as the number of workstations and resources increase, so the number of requests will increase. Ultimately, the server capacity would no longer be able to grow. Thus for bigger networks, such as the Internet, PKI with digital certificates is better suited.

(Kanavan, 2000: 77-78).

While Kerberos seems an equitable solution for intra-organizational networks, it seems to present many shortcomings for IOISs.

4.2.8. Virtual Private Networks (VPNs)

In terms of Business-to-Business (B2B) e-commerce (extranets), trading partners generally consider Virtual Private Network (VPN) implementation as a core security option. This option also applies to remote users connecting to a company intranet. (Oppliger, 2000:96-97).

VPNs provide encryption on an untrusted network. The encryption is either node-to-node (or link-to-link) or end-to-end encryption.

Node-to-node encryption involves the data link layer of the OSI Reference Model. A packet has to be decrypted and re-encrypted at each hop along the route, to allow the routing information at layer three to be read. This implies that every node must have compatible devices and key management processes.

End-to-end encryption implies that encryption is done at the sending node and decrypted at the receiving node. It involves encryption at the upper layers of the OSI Model. The drawback here is that the higher up the encryption is on the protocol stack, the more transmission information (e.g. TCP/IP ports) is contained unencrypted in a packet.
(Canavan, 2001:201-203)

In selecting VPN solutions, a major interoperability factor is the VPN protocol. This is considered in the section below.

4.2.8.1. VPN Protocols

Common VPN protocols may be listed as:

- Point-to-point Tunnelling Protocol (PPTP);
- Layer 2 Tunnelling Protocol (L2TP);
- Internet Security Protocol (IPSec); and
- SOCKS.

(Ibid:205)

A brief summary of each protocol is provided in the following sections. Unless otherwise indicated, the material is based on Canavan (2001:205-208).

(a) PPTP

- Supported by Microsoft, it is one of the earliest VPN protocols
- It is used for connecting remote clients to servers; on Windows computers, the underlying services are referred to as Remote Access Services (RAS).
- It works at layer 2 of the OSI model and is an extension of the Point-to-Point protocol (PPP).
- It encapsulates PPP packets using a modified version of the Generic Routing Encapsulation (GRE) protocol; GRE makes it able to encapsulate IP, IPX and NetBEUI. However, firewalls may not permit the GRE service. (King et al, 2001:197).
- The actual encryption is either by means of CHAP (Challenge Handshake Authentication Protocol, which uses RSA's MD4 for

hashing and RC4 for symmetric encryption) or MS-CHAP (Microsoft's version of CHAP, which is the default setting)

- The server sends the client a challenge which is used by the client to encrypt the client's password. The password is returned to the server in order for the client to log in.
- PPTP has been submitted to the IETF for standardization.
- It is available for Linux and Windows (98 and NT).
- It is recommended that PPTP not be used to protect sensitive data, as it is relatively insecure (King et al, 2001:197).

(b) L2TP

- This is an IETF standard that combines features from Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's PPTP.
- It is also an extension to the PPP and operates at layer 2. It therefore, like PPTP, provides node-to-node encryption.
- It does not yet have significant deployment, and is not likely to be favoured over IPSec in the future (King et al, 2001:198).

(c) IPSec

- IPSec is under development by the IETF for Internet and Intranet implementations.
- It operates at layer 3 (the network layer) and supports two modes: transport mode or tunnel mode.
    - In transport mode, it encrypts only the data (payload) of each packet. This provides end-to-end encryption, since the header is unencrypted. Although this is prone to traffic pattern analysis, the payload is protected. Transport mode is always used between two hosts (Phaltankar, 2001:202).
    - Tunnel mode encrypts the entire packet. This results in node-to-node encryption. Each receiving device must be IPSec-compliant,

decrypt the packet, interpret the relevant information, re-encrypt it, and then forward the packet to the next device. Each receiving device has a public key for the sending device's digital certificate; the Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley) is used. Tunnel mode is considered more secure than transport mode. Tunnel mode is used between two security gateways or between a host and a security gateway (Phaltankar, 2001:202).

- IPSec is not a single protocol, but a suite of protocols, which provide privacy, authentication and data integrity to IP packets:
    - *Authentication Header* (AH), for data integrity and packet data-origin authentication (using hashed message authentication code, HMAC with MD5 or SHA-1);
    - *Encapsulating Security Payload* (ESP), for packet encryption and/or authentication (also using HMAC with MD5 or for integrity and DES-CBC for encryption); and
    - *Security Association* (SA), which defines the security policy between two nodes. SAs determine which algorithms will be used, how keys will be exchanged (HMAC uses a secret key), and how often keys will be changed. Automated key management is generally provided by the Internet Key Exchange (IKE) algorithm, which is a combination of the ISAKMP/Oakley protocols, mentioned above. ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete SAs. Oakley uses the Diffie-Hellman key exchange algorithm.

King et al (2001:198-203)

- Although designed primarily for IP version 6 (IPv6), it is being used on IP version 4 (IPv4) systems (Ibid).
- Using IPSec secures both TCP and UDP applications (Oppliger, 2000:116).

(d) SOCKS

- SOCKS is an IETF protocol standard for handling TCP traffic through a proxy server.
- Two versions in use are SOCKS4 and SOCKS5 (versions 4 and 5). Version 5 provides additional security through authentication.
- SOCKS5 provides rudimentary firewall capabilities, by providing authentication of incoming and outgoing packets, as well as network address translation (NAT), whereby the internal network IP addresses are masked from external networks.

4.2.8.2. The Suitability of VPNs for B2B IOIS

Various VPN configurations are possible, e.g. router-to-router, server-to-router, server-to-server, workstation-to-server, or workstation-to-router. (Canavan, 2001:208). This makes it highly suitable for B2B IOISs. Essentially, a VPN creates a virtual pipe between two endpoints. Private (RFC 1918) IP addressing schemes for the endpoint networks can be used, without conflicting with Internet addresses. (Multiprotocol Label Switching (MPLS)[2] is another technology that circumvents this problem and is generally used by ISPs.).
(King et al 2001:177-215).

VPNs provide authentication, access control, confidentiality and data integrity; these services are encryption-based, which is a defining feature of VPNs. VPNs are seen as only part of a complete security solution, protecting data streams in transmission between two endpoints. (Ibid:179-180). Typically, the networks would be simple dial-up using PSTN, ISDN, xDSL, frame relay, ISDN or ATM. (Oppliger, 2000:96-98).

[2] More information on MPLS is available at www.ietf.org/html.charters/mpls-charter.html

The accepted standard in extranets is IPSec. (King et al, 2001:183). In fact, King et (Ibid:195) contend that IPSec has "become the protocol of choice to build the best VPN system because it offers strong security, encryption, authentication, and key management".

4.3. Conclusion

One might therefore conclude that in B2B IOISs,

- AES would provide optimal encryption-based security;
- PKI provides optimal security services, as well as key distribution and key management services; and
- VPNs employing IPSec, with ESP and IKE, seem to be the B2B IOIS deployment of choice.

When suitably implemented, the degree of security provided by these controls ultimately depends on how secure the encryption algorithms are that are used for encrypting data and providing message digests. AES/Rijndael algorithm is demonstrably efficient in this regard. It seems logical that to ensure interoperability, the same algorithm be used for both encryption-decryption and hashing.

Hunt (2001:1467) states that PKI has not enjoyed widespread deployment as a result of cost, complexity, lack of qualified resources and "a critical mass of businesses". PKIs are, however, being implemented to manage VPNs. Further, the author points out that VPNs are standardising on IPSec, using IKE for key exchange.

It seems logical to conclude that AES will begin to play a critical role in both SSL/TLS (B2C networks) and VPNs (remote-user-intranet set-ups and B2B networks). While AES has become the symmetric encryption standard, the use

of PKI to circumvent secret key exchange and to ensure sender authentication, seems to be essential. It is very likely that AES will be used for digital signatures as well.

The next chapter looks at how VPNs, using PKI, may be used to provide a framework for interoperability between security systems of trading partners in a B2B IOIS.

Chapter 5

A Proposed Framework for Optimal Interoperability

5.1 Introduction

Security interoperability implies that the security mechanisms underlying the network activity (e.g. online transactions) taking place between trading partners have sufficient commonality to allow appropriate parts of the information systems of each trading partner (TP) to be electronically integrated, while still providing the required security. The question arises: how does one determine what provides optimal interoperability and what provides optimal security in any given B2B IOIS?

Neither ITSEC, nor TCSEC, nor CC is suitably applicable for evaluating security in networked and distributed systems (Oppliger, 2000:15). The BS7799 (British Standard) Code of Practice (CoP) has as one of its objectives: "to provide confidence in inter-company trading" (Von Solms, 1998). However, the CoP is not a set of specifications and merely provides guidance and recommendations (BSS7799-1-1999:iii). Thus, the degree of interoperability between security systems of TPs is determined by which technology standards are implemented by each TP, as well as how they are implemented. No standard specifications framework appears to exist for ensuring interoperability between TP security systems in a B2B IOIS context.

Therefore, it is contended here that a VPN solution between TPs can be configured such that interoperability between TP security systems in a B2B IOIS

context can be ensured, while still maintaining optimal security. The following are additional features of this solution:

- Each TP may supplement the VPN solution with additional security layers, as dictated by risk-assessment, security policy, performance considerations and budgetary considerations, etc, without affecting interoperability. PGP-encrypted e-mail used over the VPN tunnel will, for instance, not be affected by the VPN configuration.
- The ebXML templates for the Messaging Service and CPA may be used as the basis upon which details of the solution are specified.

5.2. The Proposed Framework

5.2.1. Objectives

The primary objective of this framework is to propose a possible standard set of choices in terms of security controls/countermeasures (technologies) and procedures used, to ensure interoperability between security systems of trading partners.

At a minimum, irrespective of the configurations of OSI Reference Model layers, the framework should allow complete connectivity, while simultaneously providing all five security services. Further, the framework should be flexible enough to allow for additional security measures.

5.2.2. Assumptions Based on Literature Review

The following are assumed antecedents (for which no further provision is made in the proposed framework):

- Both parties in a B2B IOIS would be responsible for using a suitable yardstick (such as the BS 7799) to assess the risks implicit in the IOIS and to select the required controls to be implemented. Some of the possible risks in B2B IOISs include: Unauthorised transactions and fraud, disclosure of sensitive information on the network, errors in processing and communications, potential loss of management and audit data, and potential legal liability. If the parties decide to utilize the software envisaged by the ebXML designers, then presumably this step would eventually be supported by that software. (UN/CEFACT and OASIS[10], 2001: 13).
- Business process agreements would have been established between participants in the B2B IOIS, by a commonly-agreed upon means as an integral part of the trading partner agreement (e.g. an ebXML CPA).
- Each TP would have secured their site with appropriate security tools (as determined by their individual security policies) for prevention, detection and correction of security breaches. This would include staff training, firewalls, network scanners, intrusion detection tools, anti-virus software, data backup and recovery strategies and a business continuity plan. (Phaltankar, 2001:130).
- Web Servers (and related virtual servers, drives and directories) hosting information to be shared would have been secured by appropriate configuration, such as not to allow anonymous access, restricting access to a closed user group (CUG) (based on e.g. IP address or user authentication), and hidden URLs (Oppliger, 2000:22-40). Access control up to application level is an imperative, as is authentication, privacy, integrity and non-repudiation. Access control may be provided by Kerberos, for instance.
- Each TP would have configured their firewall(s) and proxy server(s) to allow internal (corporate) users to communicate with the outside from within the corporate intranet; and remote users to access the inside from the outside.

- Each TP will employ network management tools for fault management, configuration management, accounting (charge) management, performance management and security management for the site (Phaltankar 2000:101-120).

All of the above measures are considered essential to overall security, but are superfluous to maintaining interoperability between TPs.

In formulating the proposed framework, the following trends in B2B IOISs are assumed:

- B2B IOISs are VPNs and will thus utilize PKI as the currently optimal means to provide all five OSI security services (as described in Chapter 1).
- PKI software will tend towards using AES as the encryption algorithm of choice.
- The increasing pervasiveness of digital certificates will make it a more affordable proposition in the near future.
- For the sake of interoperability, the IPSec open standard is the protocol of choice for VPNs (King et al 2001, 183). For B2B, tunnel mode with ESP, and IKE for providing the PKI requirements, would be most appropriate.
- The ebXML Technical Architecture (Chapter 3) will become the B2B platform of choice and become the means by which TP discovery, business process agreements, collaboration protocol profiles (CPPs) and collaboration protocol agreements (CPAs) are achieved. Thus, the framework proposed here would be specified on CPP and CPA templates, from which Message Services would be configured.
- In terms of Choudury's IOIS typology (Chapter 3), a multilateral electronic market IOIS with less electronic integration, and less-detailed policy requirements, is initially preferred. This will evolve, in some cases, to electronic dyads and, ultimately, to electronic monopolies, if the

degree of integration increases. However, it is important to note that most studies undertaken in respect of IOIS involve EDI using private networks. B2B IOISs involve the public Internet, so that the set of vulnerabilities is much greater.

- Transactions involving the transfer of funds would preferably be made by the payer into the payee's bank account. Hence, Internet payment options would not necessarily affect interoperability between TPs (even though it might affect business flows).

5.2.3. Components Required for Interoperability

The B2B IOIS infrastructure would, at a minimum, include the following (see Figure 5):

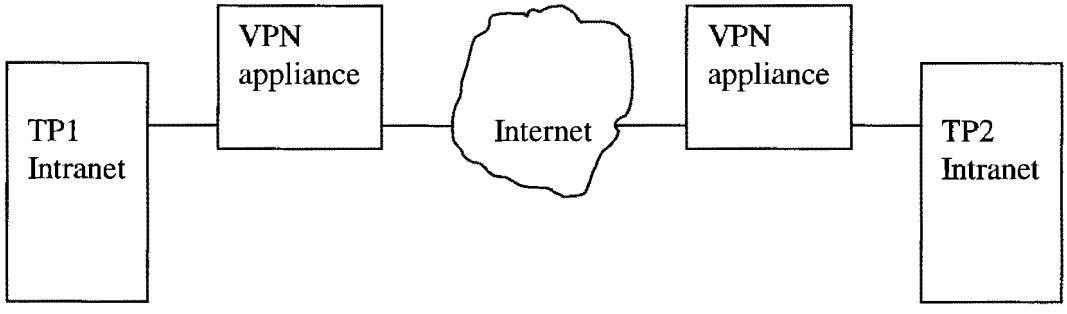


FIGURE 5: MINIMAL B2B IOIS INFRASTRUCTURE

At the heart of the interoperability framework is the actual configuration of the VPN appliances.

5.2.3.1. VPN appliances

As pointed out earlier, the VPN appliances could be either routers configured as firewalls, or multi-homed computers (servers with two or more network cards) configured as firewalls with firewall software (such as Cisco's PIX firewall). Often, more than one firewall could be used on either or both ends. Each VPN

appliance would be further configured to include at least the following (see figure 6):

VPN Appliance

Must be configured with:

1. A Digital Certificate to identify it uniquely
2. IPSec:
   - which uses ESP
     - (using AES)
   - operating in tunnel mode,
   - utilising IKE and SAs

FIGURE 6: MINIMAL INTEROPERABILITY COMPONENTS

(a) Digital Certificates

Each TP hosting a web server for B2B interaction requires a digital certificate (site certificate) supplied by a reputable CA. This is for use with IKE, which uses the Diffie-Hellmann algorithm for key exchange, at each receiving node. The certificate may also be used for other purposes, as in SSL/TLS.

Diffie-Hellmann does not generally use a CA, but in PKI a CA is used to provide digital certificates, from which public keys are installed on the receiving nodes. IKE (using Diffie-Hellmann) can then use the sender's public key, to create a secret key.

(b) IPSec protocol

The IPSec protocol must be configured on both ends, with

- *Tunnel mode, using ESP*. Each VPN node, including ISP gateways, should be configured with the connecting TP's public

key. Tunnel mode encrypts the entire packet and encrypts and decrypts the packet at each node.

- *IKE*. IKE provides:
  - The SA and key parameter negotiating service;
  - The primary authentication for communicating entities at the start of the negotiation;
  - The management of the key exchange;
  - The method for generating other keys for authentication and the encryption service.

  (Ibid).
- Appropriate *security associations* (SAs). SAs comprise, e.g. the source IP addresses of the TPs and the cryptographic algorithm for each TP. Note that each SA has a unique identifier called the security parameter index (SPI), which enables the VPN appliance to select the appropriate SA. (Phaltankar, 2001:204).

(c) Encryption algorithm

For both symmetric encryption and hashing, AES would seem to be more than appropriate. This would optimally support interoperability in an electronic market IOIS. Phaltankar (2001:204) states that any symmetric encryption algorithm is supported by ESP. Thus, AES could be used in ESP encryption.

(d) ebXML CPA Components

VPN appliances would, additionally, be configured in respect of ebXML CPA components (as described in chapter 3). For example: the Telnet protocol might be disallowed.

Configurations beyond the VPN appliance level would provide the necessary standardisation of infrastructure for business processes, semantics, messaging

and the processes (as contained in the CPA). Thus, the required pre-specifications for sustainable collaboration within the IOIS – as discussed in chapter 2 – can be determined before any actual implementation. This is discussed in the next section.

5.2.4. Proposed Procedural Guidelines

The following steps, to be conducted in a recursive fashion, are proposed in the setting up of the B2B IOIS (see Figure 7):

1. Develop an IOIS strategy (see chapter 2)
2. Use BS7799/OSI17799 (Code of Practice) to extend the existing security policy for the TP's internal network to include the IOIS strategy.
3. Use the ebXML Registry (discussed in chapter 3) to obtain the details of a prospective TP.
4. Ascertain the ebXML Collaborative Partner Profile (CPP) (chapter 3) of the prospective TP.
5. Negotiate the terms of the Collaborative Partner Agreement (CPA) with the prospective TP, including security strategies, specifically with regard to the Messaging Service (MS) security parameters (chapter 3).
6. Obtain a digital certificate from a reputable Certification Authority (CA), if one has not already been acquired.
7. Download the semantic specifications for developing an ebXML-compliant application and develop the application, or use a "shrink-wrapped" application (chapter 3), for conducting business with the TP.
8. Implement the IOIS security strategy in a layered fashion (using the OSI Reference Model for networks), using the recommended interoperability components.
9. Use the ebXML application for conducting business with the TP.

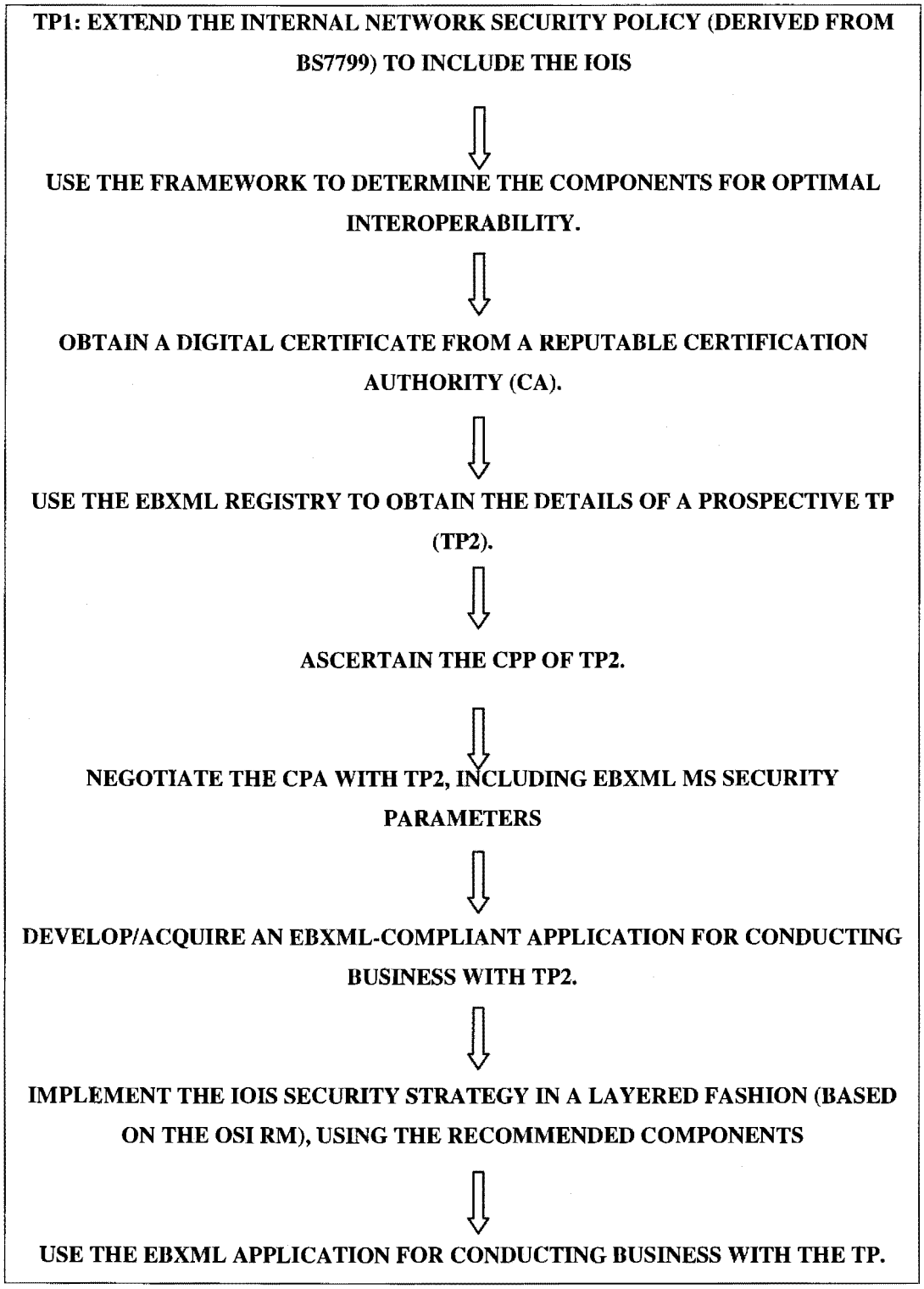


FIGURE 7: PROCEDURAL GUIDELINES FOR INCORPORATING THE FRAMEWORK

5.3. Conclusion

This chapter suggests a reference architecture for security interoperability across IOISs. It is not intended to be a complete framework. From the practitioner's perspective, it eliminates much of the guesswork in selecting specification options.

It proposes a technological framework - underpinned by a policy-based, layered approach (using standards such as ISO 7498 and BSS 7799/ISO 17799) - which simultaneously ensures optimal interoperability and optimal security. The following are important points to note in this regard:

- The IOIS security component is relatively independent of the rest of the TP's internal security structure although it may share the same infrastructure. It simply requires the VPN appliance to be configured such that it is simultaneously compliant with the TP's internal Security Policy and the CPA. The same appliance may be used for other TPs (using different SAs), based on other Security Policy and CPA stipulations. The VPN appliance is the crucial component of this interoperability framework. If the configurations were "standardized", as per the proposed framework, only the minimum (Security Policy and CPA) negotiations between TPs would be necessary.
- It is suggested that, for the sake of interoperability and standardization, that the *simultaneously most secure and most interoperable* implementation of B2B IOIS electronic integration be used by both TPs. While the framework does not provide an all-encompassing set of specifications for security, it uses components which ensure interoperability and which are the most secure of available options. Therefore, the VPN options of IPSec, with ESP, tunnel mode, IKE,

digital certificates, and AES for encryption/hashing, are suggested as being *standard* choices for B2B IOISs.

- The use of AES, for symmetric encryption and /or hashing, is certainly more expedient, as discussed previously.
- Further implementations, such as PGP for e-mail, may be mutually-agreed upon in the CPA. Since B2B IOISs, of necessity, use TCP/IP stacks – or appropriate gateways – and since UNICODE generally facilitates compatibility at the (OSI) presentation layer, application layer incompatibilities may be resolved subsequently (if not anticipated in the CPA).
- The use of the ebXML specification suite is strongly recommended, especially since it facilitates interoperability at a business operational level as well as the functional services level.

The incipient framework proposed in this chapter is evaluated in chapter 6,

Chapter 6

Evaluation of the Framework

6.1. Introduction

In deciding how to implement a B2B IOIS security strategy, one is faced with the challenge of choosing from a host of security controls and procedural options. Some of the options are:

- EDI or ebXML?
- VPN or Private network?
- VPN: leased line, ATM, Frame Relay, or Internet?
- VPN: PPTP, L2TP, or IPSec?
- Network Authentication/Identification: Kerberos, RADIUS, CHAP or digital certificates?
- Privacy protocols: PGP, S/MIME, AES, DES, 3-DES or others (notably, Twofish, MARS, Serpent, and RC6)?
- Integrity protocols: SHA-1, RSA, HMAC, DSA, or AES?
- Authorization/Access control: Passwords, Kerberos, or ACLs?
- Non-repudiation options: digital signatures or digital certificates?
- Remote Access methods: RADIUS, CHAP, Kerberos, or digital certificates

This list is by no means exhaustive, but serves merely to indicate the variety of options available. (The acronyms are explained on p6). Chapter 4 examined the more obvious risks related to B2B IOISs, and the corresponding countermeasures/ controls. In chapter 5, a set of controls and control parameters were chosen to present a recommended configuration for optimal interoperability. An interoperability "baseline" was sought.

From a client-server perspective, additional client and server controls would be required to attain the expected assurance level (EAL) in the envisaged protection profile (PP). Further, additional security controls - such as Layer 2 Tunnelling Protocol at the data link layer, or S/MIME at the application level (in terms of the OSI 7-Layer Reference Model), or the forbidding of Telnet packets with a (packet-filter) firewall – could be added to augment overall security.

The physical implementation of this framework requires that an entire B2B IOIS be set up; such an operation would be beyond the scope of this dissertation. A theoretical evaluation is therefore provided.

In order to evaluate the security of a site in which the equipment of a TP that participates in an IOIS is located, a comprehensive set of criteria such as contained in the Common Criteria, TCSEC or ITSEC, is required. The framework proposed does not purport to provide comprehensive security. Its point of departure is: interoperability of security implementations within the context of B2B IOISs. Hence, the criteria for evaluating the framework should emanate from the overall objective stated in section 5.2.1.

6.2. Criteria for Evaluating the Framework

- Has the problem context been thoroughly examined for security control options?
- Is the set of controls proffered the most expedient for ensuring interoperability between TPs?
- Are all five security services ensured by the framework?
- Is optimal interoperability ensured?
- Can the fundamental controls be augmented/supplemented with additional controls, without detracting from the original configuration?

6.2.1. Has the problem context been thoroughly examined for security control options?

Usage popularity – as reported in the literature - was used as a general yardstick for selecting the available control options. The following information was gleaned from the literature:

- VPNs have become a de facto standard for B2B electronic commerce. The cost-effectiveness of using the Internet in preference to private networks is a powerful driver in this regard. Chapter 2 outlines the business benefits of implementing hypermedia IOISs.
- The choice of IPSec in preference to other VPN protocols is explained in chapter 4. IPSec is being developed by the IETF primarily for IPv6, which is set to replace IPv4. However, in its current IPv4 implementation, it is the protocol of choice for B2B scenarios, as described in chapter 4.
- For scalable electronic markets, digital certificates issued by a noted CA are preferred for providing all five security services. The superiority of digital certificates over Kerberos and Key Distribution Centres, as well as over digital signatures, is described in chapter 4.
- The ebXML initiative – which enjoys far-reaching support – has highlighted the trends favouring XML, UNICODE and multi-lateral electronic markets (in keeping with the open nature of the Internet).
- The establishment of the Rijndael algorithm as the powerful new encryption standard (AES) makes it the automatic choice for symmetric encryption and hashing.

6.2.2. Is the set of controls proffered the most expedient for ensuring interoperability between TPs?

In chapter 4 an attempt was made to indicate how flaws in encryption implementations may be overcome with alternative control options. It was shown that encryption has evolved to the point where keys require to be distributed and managed by means of a PKI for optimal efficiency; secret keys are generated locally and are not exchanged or transported. Public keys embedded in digital certificates - with characteristics equivalent to passports - are issued by a trusted third party (King et al, 2001:359).

In terms of providing optimal security (service) options (including sender authentication) and interoperability, digital certificates present the best current option. The PKIX X.509 v3 (discussed in Chapter 4) defines public extensions, which provide, inter alia, for Certificate Revocation Lists (CRLs). Thus, certificates may be revoked, if necessary, allowing receiving nodes to disallow authorisation. Certificate management protocols support certificate enrolment, certificate revocation, key recovery and automated certificate renewal. (Ibid: 363). Using a VPN with IKE (in tunnel mode) provides this fundamental interoperability.

6.2.3. Are all five security services provided?

The VPN between each two TPs would utilize encryption (AES) for secrecy/privacy, digital certificates for authentication, access control/authorization, and non-repudiation, and hashing algorithms (AES is recommended) for integrity.

A specific SA is set up for each two TPs at each receiving node. ESP provides symmetric encryption (DES-CBC is currently commonly used) and hashing (HMAC with SHA-1 or MD5 are current options). IKE is used for negotiating the SA and setting up of AH and ESP services; the primary authentication at the start of the negotiation; the management of the key and nonce exchange; and determining the method for generating other keys for authentication and the

encryption service (Phaltankar 2000:206). Nonces prevent replay attacks and are used to generate fresh keys (Ibid).

6.2.4. Is optimal interoperability ensured?

The ebXML specifications allow for a Collaboration Protocol Profile (CPP) for each TP, stored in the Registry, which can be further negotiated by TPs. The CPP merely contains XML elements such as

```
<DeliveryChannel >
      <Characteristics
            nonrepudiationOfOrigin=''false''
            nonrepudiationOfReceipt=''false''
            secureTransport=''true''
            confidentiality=''false''
            authenticated=''false''
            authorized=''false''
      />
</DeliveryChannel>
```

Sub-elements of a **`DeliveryChannel`** must be further defined. For example, if the security attribute **`secureTransport`** is indicated in the CPP, then the **`Transport`** element of the CPP might contain details as follows:

```
<Transport transportId="N12">
      <Protocol version="1.1">HTTP</Protocol>
            <Endpointuri=https://www.ebxmlregisterservices.org/as
            ynch type="request"/>
      <TransportSecurity>
            <Protocol version="1.0">TLS</Protocol>
            <CertificateRef certId="N05"/>
      </TransportSecurity>
<Transport>
```

The CPP defines different levels at which security may be implemented. For example, the transport level may use SSL/TLS. TPs negotiate the contents of

the CPPs, which results in a *Collaboration Protocol Agreement* (CPA) document. Currently this is a manual process.
(UN/CEFACT and OASIS[11], 2001: 17-19).

It is proposed in this dissertation that this step could be greatly expedited by the standardization of security implementations between TPs. As with cryptography, knowledge of the mechanics of the implementations should not weaken the security. (The algorithm for AES is popularly known, yet the strength of the algorithm is not unduly compromised by this fact). If all TPs utilized VPNs with IPSec – with ESP and IKE – and AES for encryption (including hashing), optimal interoperability would be ensured. As AES renders other cryptographic algorithms redundant, so such a framework would render other B2B IOIS implementations redundant. CPAs could then be negotiated with greater effectiveness.

6.2.5. Can the fundamental controls be augmented/supplemented with additional controls, without affecting the original configuration?

The policy-based approach to security (as defined in the BSS 7799/ISO17799 CoP) and the layered approach (as defined in ISO 7498-2) seem to represent the common trend in information security. Since the recommended IPSec protocol works at the network layer (OSI layer 3), the receiving node (such as a firewall) would examine the (tunnel mode) SA for its SPI value, after layer 1 and layer 2 information have been stripped off the packet. The ESP (data and IP header both encrypted) is encapsulated by a standard IP packet (hence "tunnel mode") (Phaltankar, 2000:204). Thus, if L2TP – for instance - is properly implemented at layer two by both the sending and receiving nodes, this would not affect the IPSec implementation at layer three. Similarly, after the IPSec layer has been stripped off by the IPSec-compliant receiving node, SSL/TLS can be implemented at the transport layer (layer 4), and /or SOCKS at layer 5, and/or S/MIME (or PGP) at layer seven (Ibid: 207-209). The obvious disadvantages to

implementing additional layers of security would be increased latency and excessive bandwidth utilization.

6.3. Conclusion

This chapter evaluates the proposed framework fundamentals in the light of the objectives for the framework.

The literature indicates that in terms of the criteria listed, the proposed controls would constitute a reasonable basis for a framework to be constructed for the security practitioner. By narrowing down the security options available to those best suited to B2B IOISs, a reference architecture for implementing an optimal interoperability solution has been successfully derived.

Chapter 7

Conclusions and Recommendations

This aim of this dissertation was to propose a set of controls and procedures as a foundation towards a framework for optimising interoperability between the security implementations of trading partners in a B2B IOIS context. The current standard for B2B IOIS interoperability is the ebXML set of specifications, for which software implementations (XML code generators) will soon be available. However, ebXML does not specify actual security controls or control parameters, and the range of permutations for possible implementations (controls) still remains vast. Hence, the objectives for the proposed framework included finding the most expedient controls in terms of optimising interoperability and ensuring that all five of the ISO-defined security services were provided by the chosen controls. Further, the envisaged framework had to provide a scalable foundation upon which additional controls could be added (preferably without having to renegotiate CPAs).

Firstly, the fundamental concepts and terminology of information security were reviewed. This was followed by a review of the IOIS concept. Chapter 3 was used to review ebXML (and its predecessor, EDI) as a set of standard specifications for B2B IOISs, specifically multilateral electronic markets (using the public Internet, rather than dedicated private communication lines). At this point, it appeared that in view of the emerging ebXML standard, that all B2B IOISs should begin as multilateral electronic markets (with collaboration being the primary driver, rather than strategic gain), which may evolve to electronic dyads and ultimately, electronic monopolies, as dictated by required electronic integration and IOIS policies (plans, rules, regulations). The business foundations of IOIS were only superficially considered, merely as a basis for understanding the migration to e-commerce/B2B IOIS/ebXML from EDI.

A review of the available security controls in the context of B2B IOIS was undertaken in chapter 4. This review was intended to cover the breadth of security controls rather than to explore each in depth. Encryption technologies were examined in the light of evolving enhancements to the point of key management facilitation. Various implementations of security controls were considered.

Thereafter, a set of specifications was proposed to ensure optimal interoperability between TPs. The emergent technologies playing a role in B2B IOISs, in general, include VPNs, ebXML and PKI. A review of the related literature reveals that the complexities of each of these technologies – from the perspective of the practitioner - could be reduced by "standardising" on available (and evolving) standards. ebXML CPAs could be arrived at more effectively. For instance, all B2B VPNs should use VPN appliances compatible with IPSec (using tunnel mode SAs and IKE); and IPSec and PKI should standardize/rationalize on AES for encryption (including hashing). ebXML specifications for business processes and semantics (obtained and registered from the ebXML Registry) would provide the (other) necessary business and technical standards.

In chapter 6, the proposed specifications were evaluated in terms of criteria based on the objectives from which the specifications were derived. It was concluded that the literature supported the set of specifications proposed towards a more comprehensive framework (for use by practitioners). A natural progression from this work would be an attempt to synthesise a comprehensive framework, based on ebXML, IPSec and PKI (incorporating the future XML signature standard).

BIBLIOGRAPHY

- Bakos J.K. (1991). Information Links and Electronic Marketplaces: The Role of Inter-organizational Systems in Vertical Markets. *Journal of Management Information Systems. 8(2): 31-52.*
- Barua A., Chellapa R. and Whinston A.B. (1995). Creating a Collaboratory in Cyberspace: TheoreticalFoundation and an Implementation. *Journal of Organizational Computing 5(4): 417-442.*
- Barua A., Ravindran S. and Whinston A.B. (1997). Efficient Selection of Suppliers over the Internet. *Journal of Management Information Systems 13(4): 117-138.*
- Bieber M.P. and Isakowitz T. (1996). Introduction to the Special Issue: Hypermedia in Information Systems and Organizations. *Journal of Organizational Computing and Electronic Commerce 6(3): iii-vi.*
- British Standards Institute (1999), BS 7799: Code of Practice for Information Security.
- Canavan JE (2001). *Fundamentals of Network Security.* Artech House.
- Chen M. (1995). A Model-Driven Approach to Accessing Managerial Information: The Development of a Repository-Based Executive Information System. *Journal of Management Information Systems 11(4): 33-64.*
- Choudury V. (1997). Strategic Choices in the Development of Inter-organizational Information Systems. *Information Systems Research 8(1): 1-24.*
- Cisco[1] Systems (1999). A Primer for Implementing a Cisco Virtual Private Network. [Online]. Available from Internet URL: http://www.cisco.com/warp/public/cc/cisco/mkt/security/vpn, accessed on 12/04/01
- Cisco[2] Systems (2000). White Paper: Cisco IOS Software Feature: Network Layer Encryption. [Online]. Available from Internet URL:

http://www.cisco.com/warp/public/cc/techno/protocol/ipsecur/ipsec/tec/encrp_wp.htm accessed on 17/04/01

- Cisco[3] Systems (1999). Reference Guide: Deploying IPSec. [Online]. Available from Internet URL: http://www.cisco.com/warp/public/cc/cisco/mkt/security/encryp/prodlit/dplip_in.htm, accessed on 20/03/00
- Cisco[4] Systems (2000). White Paper: IPSec. Encryption. [Online]. Available from Internet URL: http://www.cisco.com/warp/public/cc/techno/protocol/ipsecur/ipsec/tec/encrp_wp.htm accessed on 20/03/00
- Clarke T.H. and Stoddard D.B. (1996). Inter-organizational Business Process Redesign: Merging Technological and Process Innovation. *Journal of Management Information Systems 13(2): 9-28.*
- Corcoran E. (1989). Hypermedia Turns Information into a Multisensory Event. *Scientific American 261:72-74.*
- Daemen J and Rijmen V (1999). *AES Proposal: Rijndael*, AES Algorithm Submission, September 3, available at [NIST[3]].
- Dawson E., Clarke A. and Looi M. (2000). Key-Management in a non-trusted distributed environment. *Future Generation Computer Systems 16(14): 319-329*
- Denning D. (1999). *Information Warfare and Security.* Addison-Wesley.
- Diffie W. (1998). E-Commerce and Security. *Standard View 6(3): 116-117*
- Dworkin M. (2000). *Conference Report: Third Advanced Encryption Standard Candidate Conference.* March, available at [NIST[3]].
- Farhoomand A.F. and Drury D.H. (1996). Factors Influencing EDI Success. *Data Base Advances 27(1): 45-57*
- Garzotto F., Paolini P. And Mainetti L. (1995). Hypermedia Design, Analysis and Evaluation Issues", *Communications of the ACM, 38(8):74-86*
- Gollmann D. (1999). *Computer Security.* John Wiley and Sons.

- Gouldsbrough N. (1997). Technical Strategies and VPN. *LANDaba Conference Notes.* AITEC (SA).
- Greenstein M, Feinman TM. (2000). *Electronic Commerce: Security, Risk Management and Control.* McGraw-Hill.
- Hart N. (1997). Securing Your Domain Using VPN. *LANDaba Conference Notes.* AITEC (SA).
- Hassler V. (2001). *Security Fundamentals for E-Commerce.* Artech House.
- Hunt R. (2001). Technological infrastructure for PKI and digital certification. *Computer Communications.* 24:1460-1471.
- International Standards Organisation. (1989). ISO 7498-2.
- Kaufman C, Perlman R and Speciner M. (1995). *Network Security: Private Communication in a PUBLIC World.* Prentice Hall.
- Kent S. and Atkinson R. (1998). Security Architecture for the Internet Architecture. RFC 2401. The Internet Society (Network Working Group).
- King C.M., Dalton C.E. and Osmanoglu T.E. (2001). Security Architecture – Design Deployment and Operations. Osborne/McGraw-Hill.
- King CM, Dalton CE and Osmanoglu TE. (2001). *Security Architecture: Design, Deployment and Operations.* RSA Press.
- Kumar K. and Dissel H.G. (1996). Sustainable Collaboration : Managing Conflict and Cooperation in Interorganizational Systems. *MIS Quarterly September: 279-299*
- Landau S^1. (2000). Standing the Test of Time: The Data Encryption Standard. *Notices of the AMS.* Vol 47(3). March: 341-349.
- Landau S^2. (2000). Communications Security for the Twenty-first Century: The Advanced Encryption Standard. *Notices of the AMS.* Vol 47(4). April: 450-459.
- Lee H.G. and Clark T.H. (1997). Market Processing Reengineering through Electronic Market Systems: Opportunities and Challenges. *Journal of Management Information Systems. 13(3): 113-136.*

- Leedy P. (1993). Practical Research: Planning and Design. 5th ed. New York: Macmillan.
- Massetti B. And Zmud R.W. (1996). Measuring the Extent of EDI Usage in Complex Organizations : Strategies and Illustrative Examples. *MIS Quarterly September: 331-345*
- Nechvatal J. (2000)., *Report on the Development of the Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, October 2, available at [NIST[3]].
- Nickull D. (2001). ebXML Technical Architecture. [Online]. Available from Internet URL: http://www.ebxml.org/documents/documents.htm, accessed on 12/04/01.
- NIST[1] (2001). FIPS: *Announcing the Advanced Encryption Standard.* Available [online] at http://www.nist.gov/aes/publications/drafts/dfips-AES.pdf . Accessed: 12/08/01
- NIST[2] (2001).*Overview of the AES Development Effort.* Available [online] at http://csrc.nist.gov/encryption/aes/index2.html#overview. Accessed: 31/08/01
- NIST[3] 2001. *AES Home Page.* Available [online] at http://www.nist.gov/aes/. Accessed: 31/08/01
- Oppliger R. (2000). *Security Technologies for the World Wide Web.* Artech House.
- Pabray UO and Gurbani VK. (1996). *Internet & TCP/IP Network Security: Securing Protocols an Applications.* McGraw Hill.
- Phaltankar KM. (2000). *Practical Guide for Implementing Secure Intranets and Extranets.* Artech House.
- Phleeger CP. (1997). *Security in Computing (International Edition; 2nd ed.).* Prentice-Hall.
- Portillo E. and Patel A. (1999). Design Methodology for Secure Distributed Transactions in Electronic Commerce. *Computer Standards and Interfaces 21(1):5-18 25 May*

- Riggins F.J. and Mukhopadhyay T. (1994). Interdependent Benefits from Inter-organizational Systems: Opportunities for Business Partner Reengineering. *Journal of Management Information Systems 11(2): 37-58*
- Sachs M., Dan, S., Nguyen T., Kearney R., Shaikh H., Dias D. (2000). Executable Trading Partner Agreements in Electronic Commerce. [Online]. Available from Internet URL: http://www-106.ibm.com/developerworks/library/tpaml.html, accessed on 5/05/01
- Schneider GP and Perry JT. (2001). *Electronic Commerce (2nd ed).* Course Technology Thomson Learning.
- Turban E, Lee J, King D and Chung HM. (2000). Electronic Commerce. A Managerial Perspective. Prentice Hall.
- UN/CEFACT and OASIS[1] (2000). White Paper: Enabling Electronic Business with ebXML. [Online]. Available from Internet URL: http://www.ebxml.org/white_papers/whitepaper.htm. Accessed on 28/05/2001.
- UN/CEFACT and OASIS[2] (2001). ebXML Technical Architecture Specification v1.0.4. [Online]. Available from Internet URL:
- UN/CEFACT and OASIS[3] (2001). Proposed Revisions to ebXML Technical Architecture Specification v1.0.4. [Online]. Available from Internet URL: http://www.ebxml.org/specs/bpTAREV.pdf . Accessed on 28/05/2001.
- UN/CEFACT and OASIS[4] (2001). ebXML Registry Security Proposal. [Online]. Available from Internet URL: http://www.ebxml.org/specs/secREG.pdf . Accessed on 20/05/2001.
- UN/CEFACT and OASIS[5] (2001). ebXML FAQ. [Online]. Available from Internet URL: http://www.ebxml.org/faq.htm . Accessed on 28/05/2001.
- UN/CEFACT and OASIS[6] (2001). ebXML Endorsements. [Online]. Available from Internet URL: http://www.ebxml.org/specs/secREG.pdf . Accessed on 20/05/2001.

- UN/CEFACT and OASIS[7] (2001). ebXML News [Online]. Available from Internet URL: http://www.ebxml.org/news/news.htm . Accessed on 20/05/2001.
- UN/CEFACT and OASIS[8] (2001). ebXML General Information. [Online]. Available from Internet URL: http://www.ebxml.org/geninfo.htm . Accessed on 20/05/2001.
- UN/CEFACT and OASIS[9] (2001). ebXML Requirements Specification Version 1.06 [Online]. Available from Internet URL: www.ebxml.org/specs/ebREQ.pdf. Accessed on 20/05/2001.
- UN/CEFACT and OASIS[10] (2001). Technical Architecture Risk assessment Version 1.0 [Online]. Available from Internet URL: http://www.ebxml.org/specs/secRISK.pdf. Accessed on 20/05/2001.
- UN/CEFACT and OASIS[11] (2001). Message service Specification [Online]. Available from Internet URL: http://www.ebxml.org/specs/ebMS.pdf. Accessed on 20/05/2001.
- Von Solms R. (1998). Information Security Management (3): The Code of Practice for Information Security Management (BS7799). Information Management and Computer Security 6/5:224-225.
- Wadlow TS. (2000). *The Process of Network Security*. Addison Wesley Longman Inc.
- Zhang N., Shi Q., and Merabti NM. (1999). A Flexible Approach to Secure and Fair Document Exchange. *Computer Journal: 42(7):569-581*

I declare that

TOWARDS A MODEL FOR ENSURING OPTIMAL INTEROPERABILITY BETWEEN THE SECURITY SYSTEMS OF TRADING PARTNERS IN A BUSINESS-TO-BUSINESS E-COMMERCE CONTEXT.

is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

.....

Maree Pather

TOWARDS A MODEL FOR ENSURING OPTIMAL INTEROPERABILITY BETWEEN THE SECURITY SYSTEMS OF TRADING PARTNERS IN A BUSINESS-TO-BUSINESS E-COMMERCE CONTEXT.

Abstract

A vast range of controls/countermeasures exists for implementing security on information systems connected to the Internet. For the practitioner attempting to implement an integrated solution between trading partners operating across the Internet, this has serious implications in respect of interoperability between the security systems of the trading partners. The problem is exacerbated by the range of specification options within each control.

This research is an attempt to find a set of relevant controls and specifications towards a framework for ensuring optimal interoperability between trading partners in this context. Since a policy-based, layered approach is advocated, which allows each trading partner to address localized risks independently, no exhaustive risk analysis is attempted. The focus is on infrastructure that is simultaneously optimally secure and provides optimal interoperability. It should also be scalable, allowing for additional security controls to be added whenever deemed necessary.

Key terms:

Security; Business-to-Business e-commerce (B2B); Extranet; Interoperability; Trading Partner