Proposed Model for Outsourcing PKI

Christopher McLaughlin

Technical Report
RHUL-MA-2008-10
15 January 2008

Department of Mathematics
Roal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

Candidate Number: Christopher McLaughlin

MSc Thesis: Proposed Model for Outsourcing PKI

Supervisor: Dr. Geraint Price

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature:  **Date:** 30th August 2007

Table of Contents

List of Figures

List of Tables

Acknowledgements

I would like to acknowledge the assistance given to me by the teaching and support staff of the Information Security Group. Their help and tuition from the very beginning of the MSc has made my time at Royal Holloway enjoyable and rewarding. I would especially like to thank Dr. Geraint Price for the guidance and support through the process of writing this dissertation. I would also like to thank my fellow students for the opportunity to discuss issues surrounding Information Security. These debates have deepened my understanding of Information Security and provided me with invaluable knowledge.

Executive Summary

PKI is often referred to as a pervasive substrate. This terminology is used to describe the technological layer that permeates the entirety of the organisation on which PKI services are established. From the mid 1970s when Whitfield Diffie and Martin Hellman published their paper New Directions in Cryptography the concept of Public Key Cryptography, for the first time, allowed two entities with no previous relationship to communicate secure information over unsecured channels. PKI provides the infrastructure that allows Public Key Cryptography to function within a hierarchical structure, providing between two entities, an acceptable level of trust.

Outsourcing is the process of acquiring sources or services from an external source. With the modular structure of today's organisations it can also mean that goods and services can be procured from one segment of the organisation to another through in-house service-supplier agreements. Outsourcing has evolved from the days of heavy industry and manufacturing in the 1960s to the total solution management of today.

This dissertation brings together the concepts of both PKI and Outsourcing. It details our AB-5C Model for organisations to outsource a PKI system within the scope of the businesses strategic goals and objectives. Our proposed model takes into account the need to use existing models, procedures and practices in support of an outsourced PKI Model. These include a process or processes to ensure that any outsourced solution adds value to the organisation, and that there is a business strategy that allows the alignment of the outsourcing strategy to the organisations strategic plan.

Motivation

Public Key Infrastructure (PKI) is a business enabler. With the advent of a network centric society organisation's have to meet the threats, challenges and opportunities that lie ahead. PKI can provide the services that enable business and meet the demands of the 21st Century. The technology is available but security professionals that have both the technical and business skills are in short supply. I aim to learn about the issues involved in both the business and technical aspects of outsourcing PKI as the next rung on the ladder of my future career.

PKI is an expansive subject providing the core services of Confidentiality, Integrity, Authentication and Authorization. By studying PKI outsourcing I aim to consolidate my technical knowledge gained on the core and elective modules. I also aim to bring in the non-technical aspects of the course by looking at the Business and Management (both Security and Risk Management), legal aspects as well as standards and regulatory bodies that are involved with PKI.

Glossary of Terms

A

ABA	American Bar Association
AC	Attribute Certificate
ANSI	American National Standards Institute
API	Application Programming Interface

C

CA	Certification Authority
CARL	Certification Authority Revocation Lists
CESG	Communication Electronics Security Group
CMP	Certificate Management Protocol
CMS	Cryptographic Message Syntax
CP	Certificate Policies
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format
CRT	Certification Revocation Tree
CSP	Certification Service Provider

D

DN	Distinguished Name
DNS	Domain Name System
DSA	Digital Signature Algorithm
DSA	Directory Service Agent

E

EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EEMA	European Association for e-identity and Security

EPRL	End Entity Public Key Certificate Revocation List

F

FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol

G

GCHQ	Government Communications Headquarters
GSS	Generic Security Service

H

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL

I

ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPRA	Internet Policy Registration Authority
IPSEC	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Standards Organisation
ITIL	IT Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria
ITU-T	International Telecommunications Union – Telecommunication

K

KDC	Key Distribution Centre
KEA	Key Exchange Algorithm
KTC	Key Translation Centre

L

LDAP	Lightweight Directory Access Protocol
LAN	Local Area Network

M

MAC	Message Authentication Code
MIC	Message Integrity Check
MIT	Massachusetts Institute of Technology
MSCHAPv2	Microsoft Challenge-Handshake Authentication Protocol

N

NIST	National Institute of Standards and Technology

O

OASIS	Organisation for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OID	Object Identifier

P

PCA	Policy Certification Authorities
PDCA	Plan, Do, Check, Act
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhancement for internet electronic Mail
PGP	Pretty Good Privacy
PKC	Public Key Cryptography
PKCS	Public key Cryptographic Standard
PKI	Public key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PP	Protection Profile
PPP	Point to Point Protocol

R

RA	Registration Authority
RADIUS	Remote Authentication Dial in User Service

RFC	Request for Comments
ROI	Return on Investment
RSA	Rivest-Shamir-Adleman

S

S/MIME	Secure Multipurpose Internet Mail Extensions
SABSA	Sherwood Applied Business Security Architecture
SAML	Security Assertion Mark-up Language
SCVP	Simple Certificate Validation Protocol
SET	Secure Electronic Transaction
SHS	Secure Hash Standard
SIM	Subject Identification Method
SLA	Service Level Agreement
SPKM	Simple Public Key GSS-API Mechanism
SSE-CM	System Security Engineering – Capability Model
SSL	Secure Socket Layer
ST	Security Target

T

TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
TOE	Target of Evaluation
TSA	Time-stamping Authority
TSP	Time-stamping Protocol

U

URL	Uniform Resource Locator

V

VPN	Virtual Private Network

W

WAN	Wide Area Network
WAP	Wireless Application Protocol
WLAN	Wireless LAN
WTLS	Wireless Transport Layer Security

X

XML	Extensible Mark-up Language

1. Introduction

This dissertation will take the following structure:

- Chapter 1 will provide the reader with the necessary information to understand why outsourcing PKI was chosen by the author as the subject of the dissertation.
- Chapter 2 defines the basic principles of PKI and aims to give the reader a level of understanding of the technologies and principles that are common to PKI.
- Chapter 3 defines the basic principles of outsourcing, ranging from the history, reasons for outsourcing, advantages and disadvantages and details the concept of multi-sourcing that has recently emerged.
- Chapter 4 is our own AB-5C Model for Outsourcing PKI. This brings together various existing models in support of the final model.
- Chapter 5 summarizes the work completed in the dissertation and provides details of how the original outcomes have been met, a critique of the work carried out and a brief description of further work leading from this dissertation.

1.1. Introduction

PKI and Outsourcing are phenomena that gained widespread industry exposure in the 1990s. Both were regarded equally by pundits as a method in which organisations could cut cost and utilise new technologies to gain business advantage. Whilst outsourcing took off, PKI failed to make an impact on organisations due to the cost of setting up the system and the requirement for skilled staff, which at the time were few and far between.

The failure of PKI can be shown by the demise of Baltimore Technologies from a company valued at £7 billion at the height of the dotcom boom, to a company with only £25 million in cash in 2003.[1] At a share meeting in Dublin, Baltimore's PKI technology was sold to beTrusted a PWC subsidiary, with its core software security business sold to UniCert. The downfall of Baltimore Technologies was not entirely of its own making but the failure of PKI to take off. This was due to the difficulty and

cost of implementing PKI and the lack of requirement from businesses of such an expensive overhead.

It now seems that outsourcing in many industries is falling out of favour as complaints about poor service circulate. Many UK Banks, and Building Societies, and Service Providers advertise that they are bringing some of their outsourced activities back into the organisation. PKI on the other hand looks like it has been shown to have solid business applications and cost benefits. According to the European Association for e-identity and Security (EEMA) at their EEMA UK Regional Interest Group meeting titled Management and Application of PKI in Corporate Environments, a consensus was reached by the twenty-six delegates that:

> "*The fact that the benefits of strong PKI across many business applications outweigh the cost of the PKI infrastructure management; and that PKI is not just about securing things, it is also an enabler for new, cost-effective, efficient, business processes which were hitherto not feasible because of security risks, legislation etc*"[2]

This view is supported by Stijn Bijnens, Senior VP Identity Management, CEO Ubizen. In a presentation to the Leuven Security Excellence Consortium, IT Security Congress,[3] Bijnens discussed the implementation problems of PKI during the dotcom boom. He also discussed the resurgence of PKI due to the renewal of interest by Governments keen to pursue ID card schemes, whilst at the same time, applying pressure to commercial organisations to meet compliance requirements.

PKI still has its opponents and one of the most outspoken is Bruce Schneier. In a paper co-written with Carl Ellison, titled, "Ten Risks of PKI: What you're not being told about Public Key Infrastructure."[4] Schneier and Ellison discuss organisation's failure to understand the risks associated with PKI, and accuse computer security industry of "the year of the ….." syndrome. It emphasises that year on year a new technology or product emerges that is hailed as the new fix for an organisations woes and argues that PKI is one such technology. The paper refutes the argument that PKI is required in order for e-commerce to flourish, when, in reality the e-commerce market without PKI was valued at $8.5 Trillion in 2005.[5]

PKI will always have its supporters as well as its critics. Today PKI is more widely accepted within business, it is now seen as an affordable and beneficial business enabler for organisations. As the understanding of the technology improves and the concerns of people such as Bruce Schneier are addressed it is our opinion that the adoption of PKI will surely grow and evolve.

1.2. Background

Historically PKI has been seen as a technical solution in search of a problem to solve, but as the understanding of PKI's advantages and limitations were uncovered it was seen more as a business solution and a tool in the strategic arsenal of an organisation, not just a technology solution that is available and therefore must be implemented. In 1999 David Lacey, at the time Director of Security and Risk Management at the Royal Mail, was quoted as saying that:

> *"The Golden Age of PKI was always going to be 2004-07, unifying companies to use connected, and regulated certificate authorities will be one way to propel PKI forward, while another will be the use of smartcards to make things more manageable."*[6]

Since 1995 Gartner has produced and used Hype Cycles to demonstrate graphically the maturity, adoption and business applications of specific technologies (See Fig.1).[7]

This representation has five distinct phases and can be used to show the approximate journey of PKI since it is a term that has been around since the mid 1990's the actual technology goes back to 1976 when Whitfield Diffie and Martin Hellman published the paper "New Directions in Cryptography."[8] The five phases of Gartner's Hype Cycle are:[9]

- The Technology Trigger
- The Peak of Inflated Expectations
- The Trough of Disillusionment
- The Slope of Enlightenment
- The Plateau of Productivity

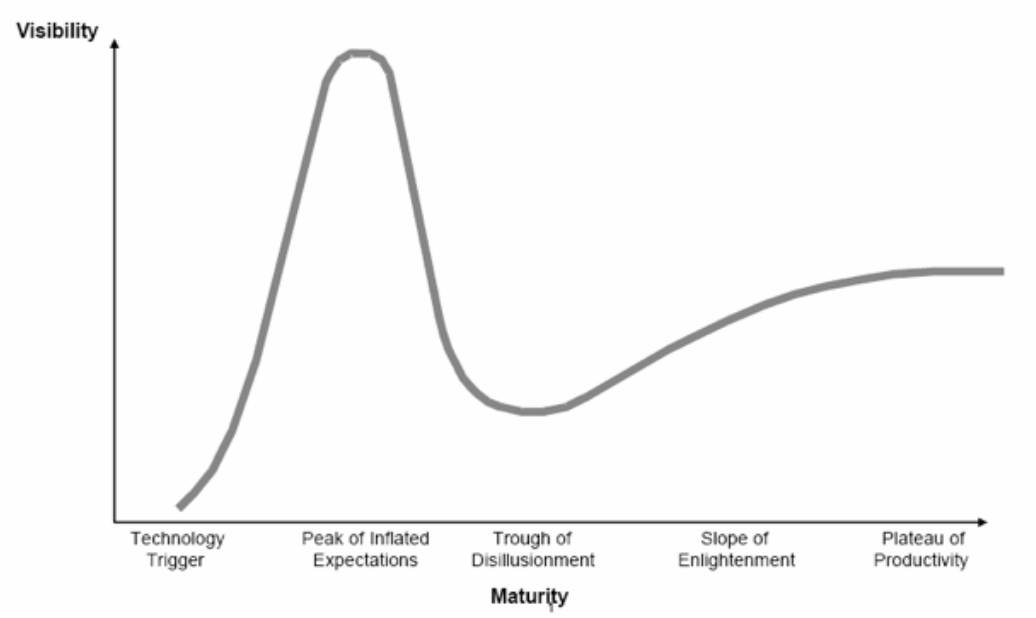


Figure 1: Gartner's Hype Cycle

If we map PKI and its progression to Gartner's Hype Cycle then the technology trigger was the Diffie-Hellman paper written in 1976. It is now known that Clifford Cocks of the UK Government's Communications-Electronic Security Group (CESG) recorded a formula for non-secret encryption in 1973 in a report titled "A Note on Non-Secret Encryption.[10] This of course was kept secret by the Government of the United Kingdom and cannot be taken as the technology trigger.

The peak of expected Inflation is when there is a widespread over expectation of what the technology can do i.e. it can have limited successes in the implementation of the technology but also many failures. David Lacey's comments about the golden age of PKI fall into this phase of the cycle. The trough of disillusionment is where the technology fails to meet the expectations and is abandoned by the mainstream, or this occurred with PKI because of the cost of the implementation of the technology, lack of skilled staff and lack of management understanding led to abandonment of PKI projects.

The slope of enlightenment is the phase where the technology is not used by the mainstream, though some organisations continue to use it in a more experimental way until it supports the business requirements of the organisation. This phase has been

prominent in the last few years where PKI has been used successfully though implementations but has still retained some problems associated with deployment.

The final phase of the cycle is the plateau of productivity whereby the benefits of the technology are firmly shown and accepted by the mainstream, the technology becomes more stable and implementation becomes easier, in the case of PKI this is shown by the comments of the EEMA UK Regional Interest Group and Stijn Bijnens. (Section1.1)

1.3. Statement of Objectives

The objectives I will achieve through this dissertation are to introduce the principles behind PKI and outsourcing. This will give the reader an insight into the history, technology and methodology that lies behind the infrastructure. It will be aimed at a high level audience and will remain at a technical level that a broad audience will be able to understand.

The introduction into the principles of outsourcing will be a management level overview of what outsourcing is, which organisations need to outsource and why it is beneficial for an organisation to outsource part of or the whole infrastructure. This chapter will also cover the managerial aspects of outsourcing PKI including Service Level Agreements (SLAs), trust in Trusted Third Parties (TTPs) and strategic planning behind the decisions to outsource a PKI solution.

1.4. Methods Employed to Achieve Objectives

The methods employed to achieve the stated objects will be the use of standard bodies including the Internet Engineering Task Force (IETF). The International Organisation for Standardization/International Electro-technical Committee (ISO/IEC). The American National Standards Institute (ANSI), and the Institute of Electrical and Electronic Engineers (IEEE), as well as de-facto standards from RSAs Public Key Cryptography Standards (PKCS) range. I will use a wide range of books, lecture notes from modules undertaken during both terms of study, research & white papers and vendor websites. A more complete list of resources that I intend to use to achieve the stated objectives is listed in Appendix A: Project Description Form.

1.5. Summary

In this section I have aimed to give a brief introduction and skeletal overview of PKI and Outsourcing to give the reader a brief understanding of the concepts that will be discussed in this dissertation. As additional background information I have mapped the rise of PKI through Gartner's "Hype Cycle" although this is a basic comparison it gives the reader some perspective of PKI and gives some sense of technological developments as seen by the mainstream organisations. I have explained in this section what my objectives with this dissertation are and how I will meet my objectives, the purpose of this will allow me to set out a format that any reader of this dissertation will be able to follow and understand the validity of any conclusions I make from the material I have researched.

2. Basic Principles of PKI

This chapter will give the reader a level of understanding of the technologies and principles that are common in PKI. The chapter starts with detailing the cryptographic principles that provide PKI core services of Confidentiality, Integrity and Authentication. The reader is taken through the history of PKI, the fundamental concepts behind PKI and a full description of a basic PKI infrastructure as defined in RFC 3280. There are descriptions of the services and applications enabled by PKI including:

- Server Identification, Authentication and Authorization
- E-mail Security Services
- IPSec and VPNs
- Wireless Network Security
- Services Provided by TTPs

The description of key management and models for key distribution have been added, this will allow the reader to understand the importance of correct key management and key distribution within a PKI. One of the fundamental threats to any cryptosystem is to attack the key management. So a strong understanding of this topic is advised for anyone designing or implementing a PKI.

There is a detailed description of certificates concentrating on the X.509v3 certificate, certificate policies, certificate policy statements and certificate revocation including both OCSP and CRLs. Digital signatures are described, allowing the reader to understand not only certificates and certification but also the types of digital signatures that are used and how they are created. The final sections of this chapter deal with legal and regulatory aspects of PKI. This is an overview of E-Signature legislation and directives. It is important for the reader to understand the basic legal concepts in relation to PKI such as the legality of digital signatures and the liability that arises from the use of certificates.

2.1. Introduction

PKI is the basis for a pervasive security infrastructure whose services are implemented and delivered using public key techniques. The primary goal of a security infrastructure is to function as an application enabler providing end-user transparency and comprehensive security. The benefits of having a pervasive security infrastructure can include cost savings, interoperability and uniformity of solutions.

2.2. Public Key Cryptography

PKI is just another tool in an organisation's arsenal which can be used as the basis for strong information protection for systems and services. It utilises Public Key Cryptography (PKC), also known as Asymmetric Cryptography. Each end entity maintains a unique cryptographic key pair, the key used for encryption is the public key and the key used for decryption is the private key. In the case of digital signatures the entity maintains a unique key cryptographic key pair for signing and verification. The private key can be seen as the signing key and the verification key as the public key, though the two definitions are markedly different and should not be confused.

Both cryptographic keys are mathematically related and dependant on each other. A main requirement for the asymmetric algorithm is that while the public key can be computed from the private key it is computationally infeasible to compute the private key from the public key, this allows the public key to be made publicly available although the private key has to be kept secret.

If Alice wants to send a message to Bob over an un-secured channel (Figure 2) she will obviously know the message that she wants to send but will also be in possession of Bob's public key. The cipher-text will be the result of the message and Bob's public key processed through the encryption algorithm. For Bob to retrieve the plain-text Bob processes the cipher-text and his private key through a decryption algorithm to recover the plain-text message.

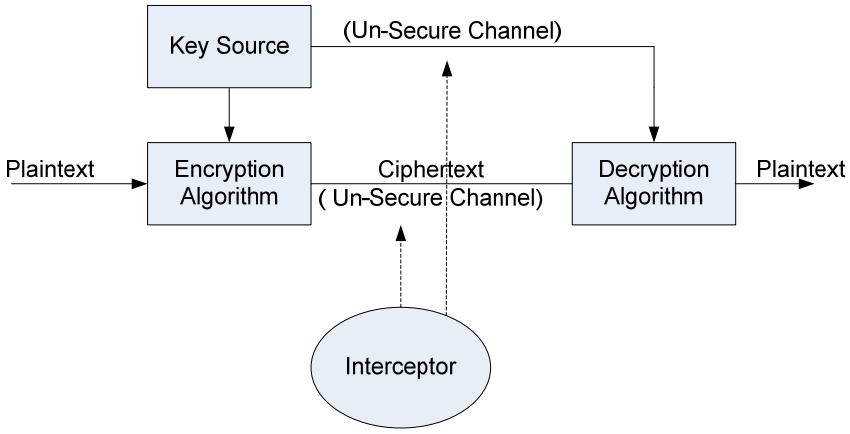


Figure 2: Public Key Cryptosystem

If Alice wants to wants to provide proof that she is the sender of the message to Bob she will sign the message by computing a digital signature and sending that along with the message to Bob, in this case the key pair are known as the signature and verification keys. The signature key is equivalent to the private key and the verification key is equivalent to the public key.

A digital signature is a cryptographic primitive which is fundamental in providing authentication (corroboration of the identity of an entity) and non-repudiation (preventing denial of previous commitments or actions) but also authorization (conveyance to another entity of official sanction to do or be something). The purpose of the digital signature is to provide the means for an entity to bind its identity to a piece of information.

Public Key Cryptography has some problems in that an entity does not know who is using their public key which can lead to certain types of attack, also, the key management requires a functionality trusted TTP. Public Key Cryptography has a significantly lower throughput of data than Symmetric Key Cryptography. Depending on the mode being used keys may not need to be changed too often, though the digital signatures mechanism for Public Key Cryptography is relatively efficient.

2.3. Symmetric Cryptography

In Symmetric Key Cryptography, also known as Secret Key Cryptography, both parties share a key which must remain secret at both ends of the channel. In a Symmetric Cryptosystem (Figure 3), when Alice wants to send a message to Bob then she uses a key that has been previously agreed with Bob. The shared secret key along with the plaintext is put through an encryption algorithm to produce the cipher-text which is then sent over an un-secured channel.

When Bob receives the cipher-text he runs this through a decryption algorithm along with the shared secret key to recover the plaintext. Although symmetric cryptography can be used to send traffic confidentially over an un-secure channel it has various other uses such as secure storage on un-secured media as well as the basis for authentication protocols. If Alice and Bob want to ensure that they are communicating with each other without revealing the secret key to eavesdroppers they can use a challenge/response mechanism.

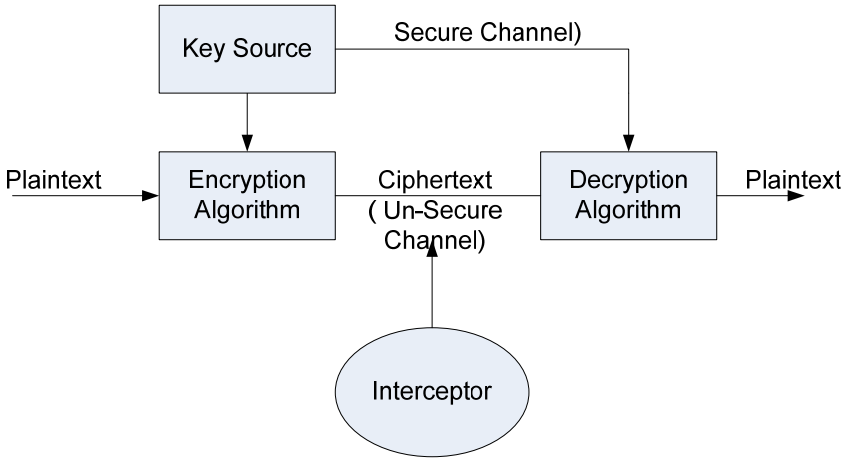


Figure 3: Symmetric Cryptosystem

There are disadvantages with symmetric cryptography, primarily key exchange problems. In large networks many pairs of keys have to be managed and this key management requires an unconditional trust in Trusted Third Parties (TTPs). This trust will have been built, developed and managed through the use of processes, procedures and contracts, more details of which can be found in Section 2.16.2 of this document.

2.4. Cryptographic Algorithms in PKI

The cryptographic algorithms used in PKI need to be selected carefully so that they work together to provide a comprehensive suite of security services. The algorithms that are used are selected on their strengths and weaknesses depending on the requirements of the system and the objectives of the organisation. Symmetric Cryptography algorithms such as DES, 3DES, AES and IDEA which are used to provide confidentiality through encipherment mechanisms, these algorithms can also be used to provide a degree of data integrity, identification and authentication through the use of MACs

2.4.1. Asymmetric Algorithms

Asymmetric algorithms are effective for data integrity mechanisms, authentication mechanisms and for key distribution. Digital signature algorithms such as RSA or Digital Signature Algorithm (DSA) provide relatively efficient digital signature schemes; the key used for the verification process is normally smaller than that of its symmetric cryptography counterpart. With the use of a TTP digital signatures can be used to provide a non repudiation service. Algorithms for Key Transport such as RSA and Key Agreement algorithms such as Diffie-Hellman can be used to securely distribute symmetric keys and by utilizing the TTP it is easier to establish the identity of a private key for an end entity. Table 1[11] is a summary of cryptographic primitives used in PKI and the services provided.

Mechanism		**Data Integrity**	**Confidentiality**	**Identification and authentication**	**Non-Repudiation**	**Key Distribution**
Symmetric Key Cryptography	Encryption	No	Yes	No	No	No
	MACs	Yes	No	Yes	No	No
	Key Transport	No	No	No	No	Yes - requires out-of-band initialization
Secure Hash Function	Message Digest	Yes	No	No	No	No
	HMAC	Yes	No	Yes	No	No
Asymmetric Cryptography	Digital Signatures	Yes	No	Yes	Yes (With TTP)	No
	Key Transport	No	No	No	No	Yes
	Key Agreement	No	No	Yes	No	Yes

Table 1: Summary of Cryptographic Mechanisms

2.4.2. Secure Hash Functions and HMAC

Secure Hash Functions and HMACs provide the basis for integrity within a PKI system. FIPS 180-2 specifies four secure hash algorithms all of which are designed as iterative one-way hash functions that are used to produce a message digest, full details are found in Table 2.[12]

Algorithm	Message Size (Bits)	Block Size (Bits)	Word Size (Bits)	Message Digest Size (Bits)	Security (Bits)
SHA-1	$<2^{64}$	512	32	160	80
SHA-256	$<2^{64}$	512	32	256	128
SHA-384	$<2^{128}$	1024	64	384	192
SHA-512	$<2^{128}$	1024	64	512	256

Table 2: Secure Hash Algorithm Properties

Mechanisms that provide integrity and are based on secret keys are called MACs, HMACs are MAC mechanisms based on cryptographic hash functions, and HMACs can be used in combination with iterative hash functions. The main objectives of HMACs are to use without any modification, an available hash function whose code is freely available and can perform well in software with the ability to handle keys in a simple way.

2.5. Digital Signatures

A digital signature is used by the CA to sign a Certificate which binds the identity of an individual to a public key. It also acts as a function that when applied to a message produces a result which enables the recipient of a message the ability to verity the integrity and origin of a message. It has the property that only the messages originator can produce a valid signature on a message. Digital signatures can be used to provide non-repudiation of message origin, that is, the recipient of the message has the ability to ensure that the sender of the message cannot repudiate that the message originated from them. In digital signature schemes asymmetric cryptography is employed. The private key is used for signing the message and the public key is used by the recipient to verify the original signature.

2.5.1. Probabilistic and Deterministic Schemes

A digital signature scheme consists of three operations, these are the generation of keys the signing of a message by the originator and the verification of the signature by a recipient. There are two types of scheme that are relevant with digital signatures the first is deterministic schemes, these are schemes that do not make use of randomly generated data and secondly probabilistic schemes, these are schemes the do make use of any randomly generated data. There are problems with both types of scheme if a deterministic scheme is used to sign the same message twice then the same signature will result but if a probabilistic scheme is used to sign the same message twice then the resulting signatures will result. Probabilistic schemes are normally more secure than deterministic schemes but it can be very difficult to generate truly random bits that are required for probabilistic schemes.

2.5.2. Digital Signatures Schemes

There are two different types of digital signature Schemes, digital signatures with message recovery where all or part of the message is recovered from the signature, this scheme is standardised in ISO/IEC 9796. Digital signatures with appendix where the message needs to be stored and sent with the signature is standardised in ISO/IEC 14888

2.5.3. Digital Signature with Message Recovery

Digital signatures with message recovery are produced by lengthening the message by the addition of redundancy according to a pre agreed formula, the lengthened message is then subjected to the signing process. The process of verification reveals the message with redundancy which the original message can be recovered from. With this signature scheme the message contained in the signature so the message does not need to be sent of stored independently of the signature, though this has the drawback of only being able to be applied to messages of a certain length. For messages of a longer length that cannot be fully recovered from the signature partial message recovery can be used, in this case the signature will be used to sign the whole message but the verification algorithm will only recover a portion of the message with the redundancy calculated as a function of the whole message.

2.5.4. Digital Signatures with Appendix

Digital signature schemes with appendix generally operate in the same way, the message that is to be signed is input into a collision free one way hash function, the output of the hash function, called a hash code, is subjected to the signing process. The signed hash code will be the signature or in other words the appendix to the message. The verification process needs to take two inputs, the original message and the signature, unlike digital signatures with message recovery the message cannot be recovered from the signature in this scheme. In some digital signature with appendix schemes use the sent message to compute a new hash code which is used as part of the verification algorithm, in this case the old hash code is not explicitly computed but it is implicitly compared to the new has code by some form of computation which should have a predictable result if the two hash codes are equal.

2.5.5. Method of Signing a Message

The method of signing a message is the same regardless of which signature schemes are being employed. The sender first has to prepare a message representative and then apply a signature transformation to the message. The message representative is a publicly known process and is slightly different for the different signature mechanisms but in both cases normally requires the use of a private key. Digital signatures always add some form of redundancy to a system, the redundancy is dependant on the message and the message representative is referred to as having redundancy meaning that the message representative depends on the message itself.

2.5.6. Method of Message Verification

As with signing of message, verification of messages is normally done in the same way for both types of digital signature mechanisms. Message verification works by undoing the signature transformation to recover the message representative, the recipient checks the redundancy of the message representative which will allow the recipient to check whether the signature is correct or not. For digital signatures with message recovery the complete message or portion of the message can be recovered from the message representative. There are exceptions to this method of message verification, the Digital Signature Algorithm (DSA) dictates that the message representative is re-computed and checks are carried out to ensure that certain values are correct.

2.6. History of PKI

The history of PKI begins with the 1976 Whitfield Diffie and Martin Hellman paper "New Directions in Cryptography"[13], in this paper two methods are suggested for transmitting keying information over an insecure channel whilst still maintaining the security of the public key cryptosystem:

> "*In a public key cryptosystem enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible. The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user in the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user encipher in such a way that only the intended receiver is able to decipher it.*"[14]

In 1977 Ron Rivest, Adi Shamir and Leonard Adleman at the Massachusetts Institute of Technology (MIT) publicly described an algorithm for a public key cryptosystem scheme:

> "RSA is the most widely used public-key cryptosystem". *It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization problem,*"[15]

A definition of the integer factoring problem is "given a positive integer n, find its prime factorization; that is, write $n = p_1^{e1}, p_2^{e2} \ldots p_k^{ek}$ where p_i are pair-wise distinct primes and each $e_i > 1$."[16]

In 1978 Loren M. Kohnfelder in his Thesis for his Bachelor of Science at MIT entitled "Towards a Practical Key Cryptosystem"[17] Loren deals with RSA (Len Adleman was his supervising professor) which had been published the previous year. In this paper Loren introduced the concepts of certificates which were "presented to reduce the active role of a public authority administering the public keys,"[18] these concepts were developed by Loren to simplify the implementation of RSA and to overcome some of the related problems.

Public Key Cryptography and Certificates from this point developed in parallel. In 1985 Victor S. Miller and Neal Koblitz independently proposed the use of elliptic curves for cryptography. In 1988 X.509 Version 1 Certificates "began an association with the X.500 standard and assumed a hierarchical system of certification authorities for issuing of certificates." [19]

In 1993 RSA labs published PKCS #1, the RSA cryptography standard and in the same year X.509 Version 2 certificates with two new fields were introduced. From 1993 to 1998 saw the introduction of FIPS PUB 186 the DSA Federal Standard, ANSI X9.30 the DSA Banking Standard, X.509 Version 3 Certificates, the ABA Digital Signature Guidelines, the Internet PKI Certificate and CRL Profile (RFC 2459) and the Internet PKI Certificate Policy and Certification Practices Framework (RFC 2527) and many more standards that contributed to the evolution of PKI.

2.7. Fundamental Principles of PKI

The fundamental principle of PKI is that the public key can be distributed freely allowing scalability, though this has to be backed by integrity mechanisms otherwise the services enabled by PKI can be undermined. A single mechanism is used to assure the user that the public key has integrity and that it has been bound to the claimed owner in a trusted manner. This mechanism is the use of public key certificates, namely, X509.V3 certificates. Briefly an X509 certificate contains the following data:

- Version
- Serial number
- Signature, Issuer
- Validity
- Subject
- Subject Public Key Info
- Issuer Unique ID
- Subject unique ID
- Extensions

The Certification Authority and Certificate revocation has been discussed earlier but an additional point is that certificates can be revoked either on-line by means of the Online Certificate Status Protocol (OCSP) or off-line using Certificate Revocation lists (CRLs).

2.8. Primary Components of PKI

The primary components of a PKI system include:

- Certification Authority (CA), the authority is trusted by a large segment of the user population to provide the function of binding a public key pair to a given identity and allows entities with no prior relationship the ability to communicate securely.
- A Certificate Repository which allows the entities to locate certificates issued by the CA quickly and efficiently.
- Certificate Revocation allows for the revocation of certificates that are either no longer valid or for the compromise of a private key.
- Key Backup and Recovery, in a system it is to be expected that users will lose the use of their public key for various reasons including lost passwords, destruction or replacement of a medium and for organisations the loss of data protected by the key would be unacceptable.
- Cross certification allows for forming relationships between formally unrelated PKI stations.
- Non-repudiation services in providing technical evidence required should the repudiation of an action have to be resolved. Finally time stamping, there has to be a time source that is trusted and securely conveyed to entities that are part of that particular PKI community.

2.9. PKI Primary Services

A PKI is generally considered to provide three primary services:

- Authentication (the assurance that one entity is who he is claimed to be)
- Integrity (the assurance to an entity that data has not been changed)
- Confidentiality (assurance to an entity that no one but the authorized entity can read a particular piece of data)

In addition to these primary services PKI can enable the following additional services:

- Secure Communication which is the transmission of data from one entity to another with one or more of the three primary services.
- Notarization provides notary certification and validation of data.
- Privilege management which is a generic term for authorisation, access control, rights management etc.

To provide PKI primary services, security mechanisms are required and these include digital signatures, Hashes, MACs and ciphers and so on, a full description of security mechanisms can be found in ISO/IEC 7498-2.

2.10. Cryptographic Key and Certificate Management

Cryptographic key and certificate management are crucial to the success of any PKI. There are underlying assumptions regarding a key management and certificate life cycle which have to be noted. These are; the end entity management of key and certificate life cycle are not practical and the key and certificate life cycle management must be as automated as possible. The key and certificate life cycle management must be as unobtrusive to the end user. Comprehensive key and certificate life cycle management requires the secure operation and cooperation of trusted entities such as the Registration Authority (RA), the CA and the client side software which interacts with the PKI components.

2.11. Basic PKI Infrastructure

A typical PKI system has the following components as described in IETF RFC 2459.[20]

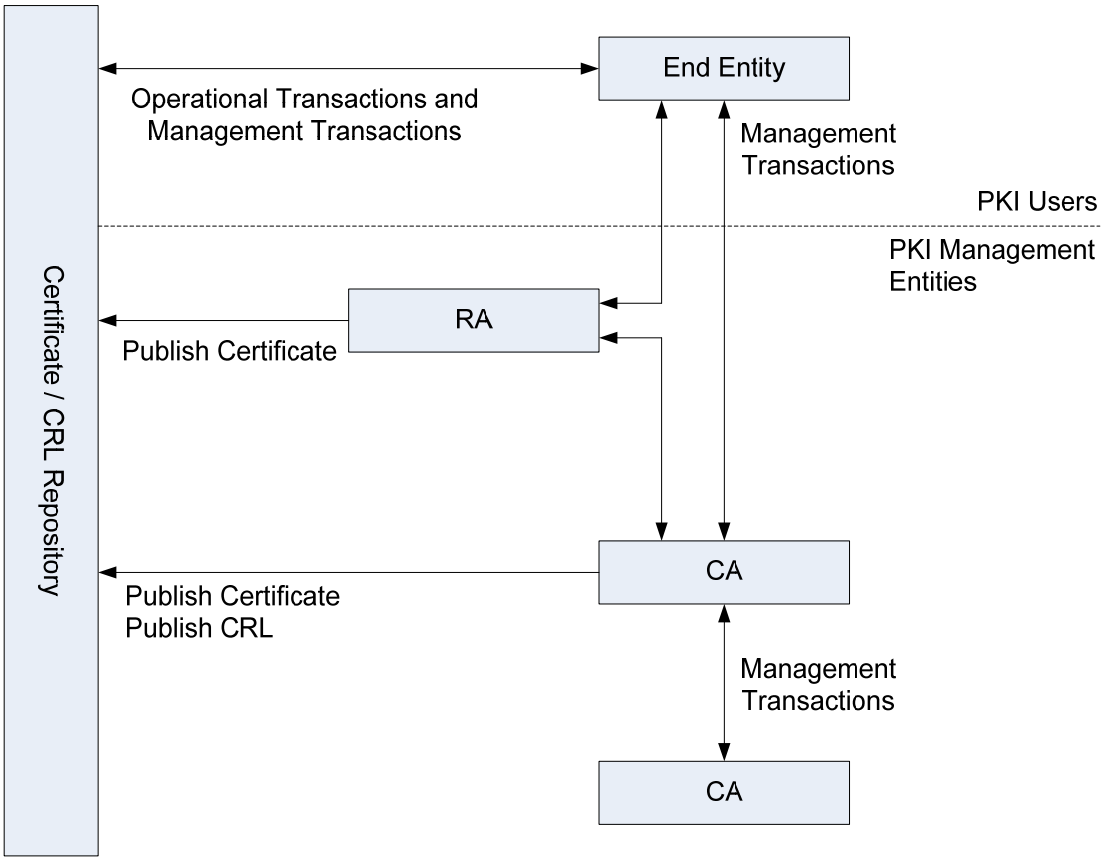


Figure 4: Public Key Infrastructure (RFC 2459)

2.11.1. Certificate Authority (CA)

> "*The CA is responsible for generating public key certificates in accordance with a defined CPS (Certificate Practice Statement), and such that the certificates can be interpreted subject to a defined CP (Certificate Policy).*"[21]

The CA in practice is an entity that carries out the management functions of issuance, certificate management, authentication, signing and revocation of digital signatures, and they are widely standardised within the IETF PKIX RFCs. CAs normally have a hierarchical structure but depending on the organisation and requirements there are other architectures such as Mesh, Loose Hierarchies, Policy Based Hierarchies and

Distributed Trust Architectures. Figure 3[22] shows a Strict Hierarchical Structure for CAs

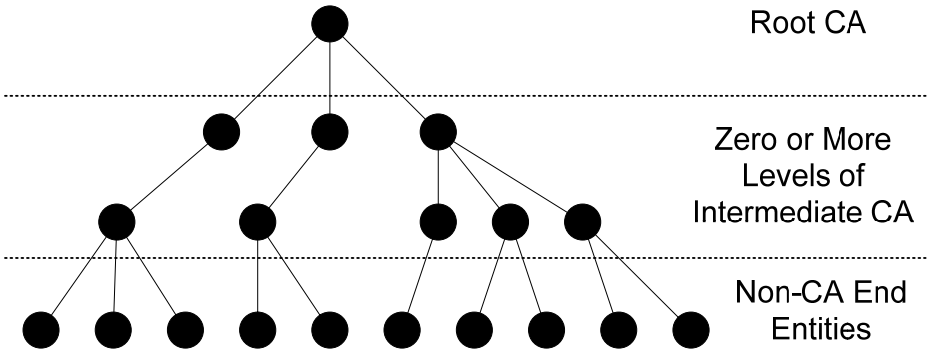


Figure 5: Strict Hierarchy of CAs Trust Model

In a Strict Hierarchical Model all the subordinate entities must trust the Root CA; it is done in a way that provides different levels of security, management and ease of certificate issuance. The Root CA is the highest level of CA and it produces a self-signed root certificate which will act as the foundation for trust of all the other entities in the hierarchal model. The Root CA will sign or certify the certificates in the level below it for the zero or more levels of intermediate CA. In turn this level will sign or certify the certificates for the lower "non-CA end entities" level. Each entity within the hierarchy must be issued with a copy of the Root CA Certificate; this process of hierarchical distribution is the corner stone of public key installation.

2.11.2. Registration Authority (RA)

The Registration Authority (RA) acts in collaboration with the CA. The RA can be used to: [23]

- Register new users.
- Verification of registration information provided by the user.
- Generation of end entity cryptographic keys.
- Certificate revocation.
- Validating that the user posses a valid certificate.

There are two methods of providing communication between the CA and the RA depending on which level of security is required by the organisation, the first is the introduction of a firewall on the private network between the RA and the CA:

> "*Only the RA Officer with an RA Certificate is able to forward certification requests to the CA and wait for the CA to sign the certificate or CRL, this method only provides moderate security as there is still the possibility to attack the CA through the RA Server*."[24]

The second approach which is the standard approach is to ensure that the CA is stand-alone and has no network connections, with certification and CRL requests etc transferred from the CA on removable media. This provides the highest level of security as long as the physical security of the CA is maintained no remote attacks can occur.

2.11.3. Certificate / CRL Repository / Directory

Certificate / CRL Repository / Directory are defined in RFC 2459 as:

> "*A system or collection of distributed systems that store certificates and CRLs and serves as a means of distributing these certificates and CRLs to end users*."[25]

A repository is a system that has two main constituent parts, the address protocol and the access protocol. The access control protocol is one of the most important considerations when designing a PKI system as it will determine the responsibilities that are assigned to each of the parties involved i.e. the CA, the Repository and the end entity. "Different repository protocols have different attributes"[26] such as:

- Location transparency: This is the ability of a system to hide from the client the actions it undertakes in locating the information required, when a client searches for information the process should appear seamless.
- Performance and availability: The requirement from the relying parties to access information grows the repository has to have the ability to cope with

the demand. If the relying party is unable to retrieve the information then the system fails.

- Anonymous versus authenticated access is the attribute where end entities can remain anonymous or can be authenticated.

There are advantages and disadvantages of both methods. It is purely an organisational decision, if the end entities are authenticated it means that, within the scope of the organisational business model, those entities can be billed for the services provided by the repository.

The last attribute which will be discussed is interoperability, as all parties involved in the system interact with the repository it is of the up most importance that they are able to communicate with one another seamlessly, if they are unable to inter-operate then the parties will be unable to exchange information.

2.11.4. Directories and Directory Access

Traditionally a typical PKI repository is called a Directory; this is an online database of arbitrary information, this information is referred to as a Directory Entry. Each entry is associated with an object class; this class defines the attributes which the Directory Entry is expected to contain. If a client requires information from the directory it is necessary for the client to know where the request has to be sent and the attributes they want from that entry. In addition to the entry being associated with an object class the entry is also identified by a distinguished name and this is used as the subject and issuer names in the certificate.

Depending on the information required the client will request different attributes, these attributes are defined in several standards. The preferred access method for repository attributes for PKI is the IETF RFC 2587 – PKIX LDAPv2 Schema. Although repositories are most commonly based on the X.500 directory the definition of a repository can “apply to a database or other form of information storage and distribution, such as on-line revocation and status responder.”[27] If this definition of a repository is used then there are various technologies that can be encompassed by this definition LDAP Servers, X.500 Directory System Agents (DSAs), OCSP Responders, Domain Name Servers (DNS), Hypertext Transport Protocol (HTTP) and

File Transfer Protocol (FTP) Servers. These access protocols allow the clients to access information for the repositories about certificates and certificate revocation on demand allowing flexibility and scalability though the most common method remains LDAPv2.

2.11.5. End Entities

The End Entity is a user of PKI certificates and/or end user system that is the subject of a certificate:

> *"End entities may be human users, or other types of entities to which certificates may be issued. In some cases, the entry for the end entity may already exist and the PKI-specific information is added to the existing entry. In other cases the entities may not exist prior to the issuance of a certificate, in which case the entity adding the certificate may also need to create the entry."*[28]

2.11.6. Operational and Management Protocols

Operational Protocols are required to deliver certificates, CRLs or certificate status information to client systems that utilise certificates. There is a requirement for various methods of certificate and CRL delivery and distribution including LDAP, HTTP, FTP, DNS and X.500 DSAs all of these specifications are defined in the IETF PKIX Standards. Management Protocols are needed to support on-line interactions between the end user and management entities, for example:

> "*A management protocol might be used between a CA and a client system with which a key pair is associated, or between two CAs which cross certify each other*."[29]

There is set of functions for which a management protocol is required these include registration, where the end entity makes itself known to the CA either directly or through an RA before the CA issues a certificate, and Initialization, which happens before the end entity can securely operate and the keying materials are installed and where the relationship between cryptographic key pairs has been established with the CA.

Certification is the process where the CA issues a certificate for the end entities public key and then posts the certificate in the repository or returns it to the end entities system. Key pair recovery where the end entities private key can be backed up by the CA or a dedicated key backup system, if there is a requirement for the end entity to recover keying material then a dedicated protocol is required.

Key pair updates is another management protocol where there is a requirement to update the key pair regularly and replaced with new keys and corresponding certificate. Finally cross certification, where two CAs exchange the information required for cross certification, to cross certify one CA issues a certificate to another CA which contains a CA signature key used for issuing certificates.

2.12. PKI Security Services

There are three core services that PKI provide these services are defined in the standard ISO/IEC 7498-2:1989, Interconnection - Basic Reference Model - Part 2: Security Architecture Information processing systems - Open Systems.

2.12.1. Authentication

Authentication can be split into two main broad categories the first is entity authentication. This is the process whereby one entity is assured of the identity of a second entity in a protocol exchange, this is normally achieved through gathering corroborative evidence. [30] Entity authentication has to ensure that the identity is claimed at a certain point of time, normally through time stamps or Nonce's. Entity authentication is typically required at the start of connections as it can protect against masquerade and replay attacks.

The second category is Data Origin Authentication this is the corroboration to an entity that the source of the data received is as claimed. [31] This does not provide any integrity protection and therefore cannot protect against the duplication or modification of the data. Data Origin Authentication protocols if not designed correctly can lead to replay and delay attacks, to that end, most data origin authentication and data integrity are provided by the same mechanisms.

•

2.12.2. Data Integrity

Data Integrity provides protection of active threats to data. It has is the property whereby data has not been altered since its time of creation, transmission or storage by unauthorized or malicious users.[32]

ISO/IEC 7498-2 defines five types of data integrity service all of these threats are designed to address specific types of threats to integrity. The first service is connection integrity with recovery, this service gives integrity protection to all the data transferred over an active connection and detects any form of modification or deletion of any data, if either occurs then the system tries to recover the data normally by requesting the data be resent.

The second service is connection integrity without recovery, which is the same as the previous service but it has no message recovery. The third service is selective field connection integrity; this service provides integrity for selective fields within the data stream transmitted over a connection. The fourth service is connectionless Integrity, this service provides assurance of the integrity of the data by the recipient and it gives the recipient of the data the ability to determine whether the data has been changed or not. The final service is selective field connectionless integrity; this service provides integrity protection for selective fields within a connectionless data unit.

2.12.3. Data Confidentiality

Data confidentiality is the protection of data from unauthorized exposure. Confidentiality, secrecy and privacy are synonymous with each other, some of the methods to protect the confidentiality of data range from mathematical algorithms to “scramble” data to physical security measures.[33]

ISO/IEC 7498-2 defines four types of Data Confidentiality service. The first service is connection confidentiality which provides data confidentiality for all data that is transmitted over a connection. The second service is connectionless confidentiality which provides data confidentiality for a single data unit that is transmitted over a connectionless circuit. The third service is selective field confidentiality which provides for the data confidentiality of a selective field data unit irrespective of whether it is connection orientated or connectionless. Finally, traffic flow

confidentiality is the protection of information through obscuring the traffic flow from analysis.

2.13. Services and Applications enabled by PKI

The Security Services of Authentication, Data Integrity and Data Confidentiality are offered by PKI, but there are also services that are enabled by having a robust PKI in place within the organisation. There are various services available that allow secure communications for server identification, authentication and authorization of web applications, email security in the form of Secure Multipurpose Internet Mail Extensions (S/MIME), authentication for Virtual Private Networks (VPN's) and Internet Protocol Security (IPSEC), wireless network security and secure instant messaging.

2.13.1. Server Identification, Authentication and Authorization

Server identification, authentication and authorization of web applications can be realised by using Secure Socket Layer (SSL) / Transport Layer Security (TLS) and Hypertext Transport Protocol over SSL (HTTPS) both of which require certificates to provide the stated security services.

> "*SSL is a protocol that provides secure channel between two machines. It has facilities for protecting data in transit and identifying the machine with which you are communicating. The secure channel is transparent, which means that it passes the data through unchanged. The data is encrypted between client and server.*"[34]

SSL/TLS protocol is defined in the IETF RFC 2246, "The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS handshake protocol. At the lowest level, layered on top of the reliable transport protocol (i.e. TCP), is the TLS Record Protocol. "The TLS Record Protocol provides connection security that has two basic properties, that is the connection is private and that the connection is reliable." [35]

There are four cryptographic primitives that are attributed to TLS:

- Digital Signatures.
- Stream Ciphers.
- Block Ciphers
- Public Key Cryptography.

A PKI can be put in place to provide the cryptographic requirements of SSL/TLS and ensure that the security services that are provided meet the confidentiality, integrity and authentication requirements of PKI.

The first application layer protocol to be secured by SSL was HTTPS the first implantation of which was in 1995 by Netscape. HTTPS is standardised by the IETF in RFC 2616, as the requirement for secure applications using HTTP, SSL/TLS was designed to provide channel orientated security and is used in the same way HTTP over TCP is used:

> "*The HTPPS approach is very simple: The client makes a connection to the server, negotiates an SSL connection, and then transmits its HTTP data over the SSL application data channel*."[36]

2.13.2. E-mail Security Services

E-mail security service in PKI can be provided by S/MIME and is standardised by the IETF S/MIME working group in a series of RFC's. SMIME provides a method of sending and receiving secure MIME data, it provides the following security services:[37]

- Authentication.
- Message Integrity.
- Non Repudiation of Origin. (*When using digital signatures*).
- Privacy & Data Security using encryption.

S/MIME provides the following functions, enveloped data, which is the encrypted content of any type encryption keys for one or more end entities. Signed data, a digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key for the signer. The content plus signature are then encoded using base64 encoding, signed data message can only be viewed by an end entity with an S/MIME capability.

Clear-signed data, as with signed data, a digital signature of the content is formed. However in this case, only the digital signature is encoded using base64, end entities without S/MIME can view the message but cannot verify the signature. Signed and enveloped data, singed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

Function	**Requirement**
Create a Message Digest (MD) to be used in forming a digital signature	Must support SHA-1 Receiver Should support MD5 for backward compatibility
Encrypt message digest to from a digital signature	Sending and receiving agents Must support DSS Sending agents Should support RSA encryption Receiving agents Should support verification of RSA signatures with key sizes 512 bits to 1024 bits
Encrypt session key for transmission with message	Sending and receiving agents Must support Diffie-Hellman Sending agents Should support RSA encryption with key sizes 512 bits to 1024 bits Receiving agent Should support RSA decryption
Encrypt message for transmission with one-time session key	Sending agents Should support encryption with 3DES and RC2/40 Receiving agents Must support decryption using 3DES and Should support decryption with RC2/40

Table 3: S/MIME Cryptographic Algorithms

Table 3 lists the cryptographic requirements for S/MIME, the definitions used in the table are taken from IETF RFC 2119.[38]

2.13.3. IPSec and VPNs

IPSec is the basis for Virtual Private Networks (VPNs):

> *"IPSec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, and data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption) and limited traffic flow confidentiality."*[39]

IPSec meets it objectives through the use of two security protocols. The first is the Authentication Header (AH), this protects the IP header by computing a cryptographic checksum and hashing the IP header with a secure hashing algorithm. The second is the Encapsulating Security Payload (ESP), this protects the packet data by symmetric cryptographic algorithms and also through key management protocols.

The protocols and procedures utilised by IPSEC are determined by the security requirements of the organisation, systems or users. When the implementation of the protocols and procedures are complete it should be such that there is no adverse effect on the users or operation of internet applications. IPSec can be used in one of two modes, transport mode, which is used between end entities supporting IPSec or between an end entity and a gateway if the gateway is treated as a host.

The second mode is the tunnel mode which is commonly used to encrypt traffic between IPSec gateways, and it is used to build a virtual network between two separate subnets which is called a VPN. The protocol that is used to authenticate each point of the encrypted tunnel is the Internet Key Exchange (IKE) Protocol:

> "*Configuring VPN devices to authenticate via a CA is actually requires more work up front. However, it provides a scalable, centrally managed solution for revoking and reassigning the certificates used to create a trusted connection."*[40]

To configure a VPN to authenticate via a CA there are several steps that have to be completed. The first is the implementation of the PKI, the next step is to generate the key pairs for the VPN devices and then follow the standard method or registration, creation of certificate and entry of the certificate into the repository. After these steps have been completed then the IPsec access control lists can be configured

2.13.4. Wireless Network Security

Wireless network security can benefit from having a PKI in place to support its security services:

> *"WLAN's using Remote Authentication Dial in User Service (RADIUS) bolted on to existing servers or using self-signing digital certificates can be used in medium to large enterprise WLAN's to enhance security."*[41]

For increase security in authentication normal Protected Extensible Authentication Protocol-Extensible Authentication Protocol-Microsoft Challenge-Handshake Authentication Protocol (PEAP-EAP-MSCHAPv2) is not allowed because it is dependant on a password which is a method of single factor authentication. Instead digital signatures stored on the end entities hard drive are recommended as a method for providing a higher security protection.

To implement PEAP-EAP-MSCHAPv2 a CA is required to provide dedicated digital certificates and not just certificates that are stored on end entities hard drives, it should also include a multi-tier hierarchy with an off line Root CA and an on-line directory. "Wireless Application Protocol (WAP) has introduced a number of innovations to cater for a wireless environment,"[42] The WAP Forum has adapted the protocol to all different certificate formats including X.509v3 and the certificates for the new Wireless Transport Layer Security (WTLS) protocol. Other adaptations of the protocol allow for certificate request protocols, WAP profiles within X.509v3 certificates and the use of certificate Uniform Resource Locators (URLs) to limit the amount of bandwidth used by end entities when making requests and receiving replies.

2.13.5. Services provided by Trusted Third Parties

A series of services can be provided by PKI with the use of Trusted Third Parties (TTPs) these include Time Stamping Authorities (TSAs), notarization and non-repudiation services. These are described briefly in the following section:

> *"A time-stamping service supports assertions of proof that a datum existed before a particular time. A TSA may be operated as a (TTP) service, though other operational models may be appropriate, e.g., an organisation might require a TSA for internal time-stamping purposes."*[43]

The TSA is a TTP that is trusted to have a valid and accurate time source that will accept validated requests and produce an accurate timestamp token. These tokens have a series of caveats associated with them including identifiers of requesting parties and security policies under which the timestamp token was issued. There are a number of security considerations that have to be taken into account when using a TSA. This will include procedures for revoking the TSAs certificate when the private key has been compromised.

The length of keys used by the TSA has to be considered to allow sufficient cover time for the timestamp tokens and procedures put in place to re-stamp documents when the cover time of the key expires:

> "*Notarization offers the registration of data under the authority or in the care of a TTP, thus making it possible to provide subsequent assurance of the accuracy of characteristics claimed for the data, such as content, origin, time and delivery."*[44]

Finally non-repudiation, "*Non-repudiation blocks the sender's false denial that the sender performed, or failed to perform a particular action.*"[45] Non repudiation services are standardised in ISO/IEC 13888 which provides mechanisms for the provision of non-repudiation services. Non repudiation services produce non repudiation tokens that can be used to prove that an entity did "something" they later deny.

2.14. Key Management

A solid key management framework is a requirement for PKI and there are various standards that can be utilised to provide this. The first standardised key management procedures came out of ANSI banking standards and have resulted in a series of key management standards that are used within the industry, including the X9.xx series of standards.

Out of the work of NIST the ISO started to develop a series of key management standards and developed ISO/IEC 11770 which is a multipart key management standard, Part 1 is the key management framework and Part 2 is the key distribution mechanisms based on symmetric cryptography. Part 3 contains key distribution and agreements mechanisms based on asymmetric cryptography. ISO/IEC 17799 provides controls for cryptographic management of keys in Section 12.3.2 and states that:

> *"All cryptographic keys should be protected against modification, loss and destruction. Equipment used generate, store and archive keys should be physically protected."*[46]

There are three types of cryptographic keys that have to be protected; the public key which is the part of the asymmetric key pair that is distributed, the private key with is the part of the asymmetric key that has to be kept secret and the secret key with is a symmetric key which also has to be kept secret. Keys are organised in key hierarchies with higher level keys used to protect keys in the lower levels of the hierarchy, each of the keys in the hierarchy have limited use, thus providing some protection against attacks on the keys. The key at the highest level of the hierarchy is referred to as the Master Key; if this key is compromised it means that all of the keys at lower levels of the hierarchy can be compromised.

2.14.1. ISO/IEC 11770-1: Model for Key Lifecycle

ISO/IEC 11770-1 describes a general model for key lifecycle that has three key states and five transition states. The three key states are pending active when a key is not used for normal operations, the active state where the key is used cryptographically to process information, and the post active state when the key is taken out of service and should only be allowed to be used for limited decipherment and verification of any data that had been generated by using the keys before revocation occurred.

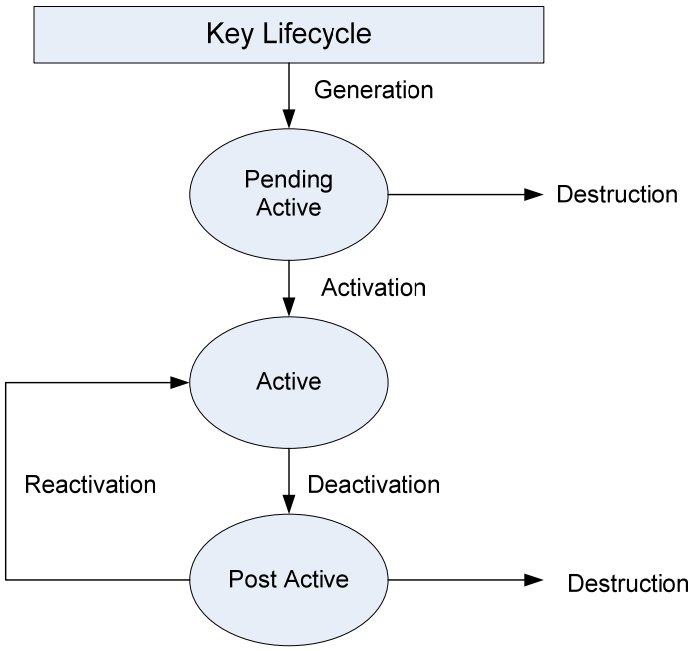


Figure 6: Key Lifecycle Model

The transition states described in ISO/IEC 11770-1 is a movement of a key from one state to another. The first state is generation which is the process of generating the key and must be carried out according to the policy and procedures determined by the organisation. The second state is activation which makes the key valid for use. The third state is deactivation which limits the keys use; this can be for various reasons including expiration or revocation of the key. The fourth state is reactivation which makes a deactivated key active again. Finally destruction is when the key's lifecycle is ending, this can occur at the pending active stage if a key has been generated and is not required for any reason, or after the post active stage when the key has been compromised, ended its lifetime or been revoked for any other reason.

2.14.2. Key Management Services

The key lifecycle on its own doesn't provide a key management service. For this, key management services are required. ISO/IEC 11770-1 lists eleven possible key management services some of which are mandatory and some optional, these are shown in Table 4. The first service is key generation - this should be a random and unpredictable process and should not be able to be tampered with.

Key registration is typically used with symmetric cryptography when an RA is used to register the end entities details and provide the CA with proof of the end entities identity. Creating the key certificate is used primarily with asymmetric cryptography and involves the CA creating public key certificates and distribution of those certificates both to the end entity and to the repository/directory.

Distribution of the key involves making the keys available to end entities that are required to have access to the material - the keying material can be either distributed cryptographically or by physical means. Installation and storage of the keys make the keying material available for use and to provide short to mid term storage for the key. Key derivation allows for the higher levels in the key hierarchy to derive keys for the level below it.

Key archiving is the provision of long term storage for the keying material, the principle behind this is that the key should only be archived once it has become post active and will no longer be used for decipherment or verification but is kept to provide evidence if required in later disputes. The final services deal with the revocation of the key which removes the key from use, the deregistering of the key which deletes the entry in the RAs table that associates the end entity with the keying material, and the destruction of the key which simply deletes all of the copies of the keying material other than the copies that have been marked for archiving.

	Generation	Activation	Deactivation	Reactivation	Destruction
Generate Key	Mandatory	N/A	N/A	N/A	N/A
Register	Optional	Optional	N/A	Optional	N/A
Create Key Certificate	Optional	Optional	N/A	Optional	N/A
Distribute Key	Optional	Optional	N/A	Mandatory	N/A
Install Key	N/A	Mandatory	N/A	Optional	N/A
Store Key	Optional	Optional	Optional	Optional	N/A
Derive Key	N/A	Optional	N/A	N/A	N/A
Archive Key	N/A	N/A	Optional	N/A	Optional
Revoke Key	N/A	N/A	Optional	N/A	N/A
Deregister Key	N/A	N/A	N/A	N/A	Mandatory
Destroy Key	N/A	N/A	N/A	N/A	Mandatory

Table 4: Key Management Services

ISO/ICE 11770 identifies various models for communications between end entities for which key management is required, the end entities that require the support may be in the same security domain or may be from different security domains.

2.15. Models for Key Distribution

There are three models that have to be considered which provide the best possible option for modelling key distribution. These are key distribution between directly communicating parties, key distribution within one security domain and key distribution between security domains. Before describing these models there are numerous definitions that have explained. The first is key establishment which is a general term for making keys available to end entities, key control is the end entity that has control of the keying material and this can be either a desirable or undesirable property depending upon the operating environment. Key transport is a service when one of the end entities has complete authority over the key control process. Finally, key confirmation gives an end entity the assurance that another end entity is using recently established keying material.

Key distribution within a single security domain is defined by a domain security policy which is defined by the security authority; the security authority also acts as a trusted intermediary providing assistance in the key establishment process. There are two methods of key establishment that have to be considered, these are, asymmetric techniques and symmetric techniques. With asymmetric techniques certificates need to be distributed and the security authority has to be contacted by both parties in order

to get each others public key certificates and with symmetric techniques Key Distribution Centres (KDC) or Key Translation Centres (KTC) have to be employed.

2.15.1. Key Distribution Centre (KDC)

A KDC is an entity that is trusted to generate and distribute keys to end entities that share keys with it.

.

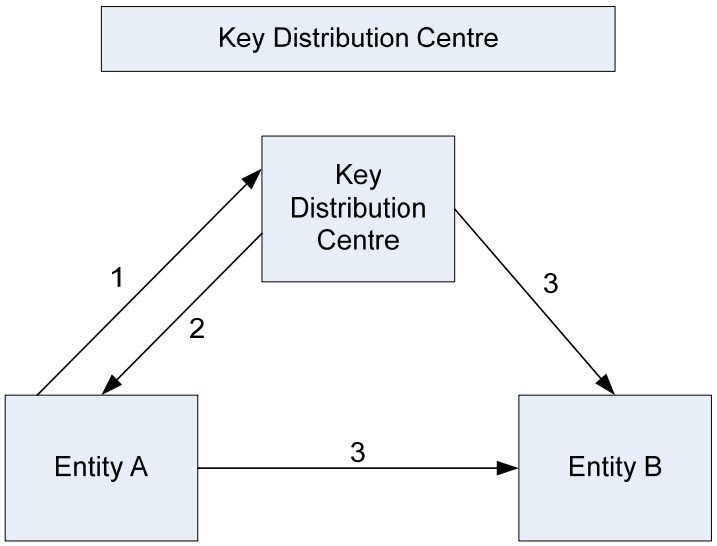


Figure 7: Key Distribution Centre

Figure 7 shows the use of a KDC within a single security domain. We have to assume that the KDC has a shared secret key with both entity A and entity B. Entity A will request the KDC to generate and distribute a secret key that can be shared between entity A and entity B. After the KDC generates the key it either enciphers it will with the key shared between itself and entity A. With entity A then forwarding it to entity B enciphered with their shared key (of entity A and entity B). Another way for entity B to get the keying material is for the KDC to encipher the generated secret key with the key it shares with entity B, and send the shared key for communication with entity A directly to entity B, after the key has been generated and distributed. Then entity A and entity B will have the shared key and will be able to communicate effectively with each other.

2.15.2. Key Translation Centre (KTC)

A KTC as the name suggests, transports keys between entities that share a secret key with the KTC.

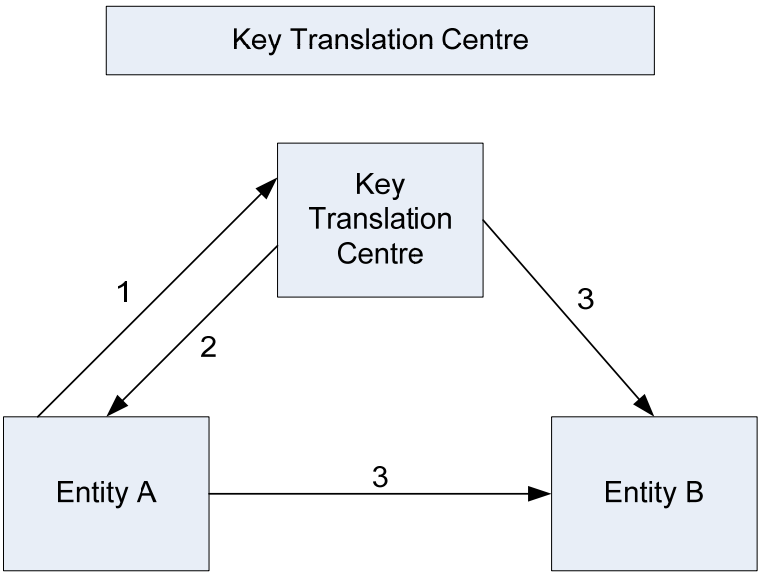


Figure 8: Key Transport Centre

Figure 8 shows the use of a KTC within a single security domain. We have to assume that the KTC has a shared secret key with both entity A and entity B. Entity A sends a key encipher with the shared key between itself and the KTC to the KTC. The KTC deciphers and re-enciphers it using the key it shares with entity B. Two methods that the KTC can employ to carry out this task is to firstly re-encipher and send it to entity A who will then forward it to entity B or the KTC can forward the key directly to entity B, this is also known as call forwarding.

2.15.3. Key Distribution between Domains

Distribution of keying material between domains deals with entities who wish to communicate directly with each other but reside within separate security domains and they only trust the security authority within their own domain. There are two cases which have to be considered, firstly entity A or entity B wish to obtain the public key certificate for the other entity or entity A and B wish to share a secret key.

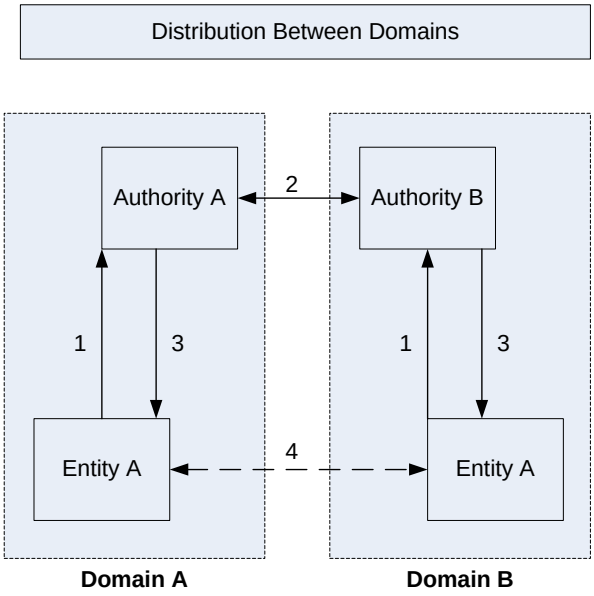


Figure 9: Key Distribution between Domains

Asymmetric or symmetric techniques can be used to provide the key establishment service. In Figure 9 symmetric key distribution is the preferred technique. The first step is for both entities to ask their own security authority to establish a key on their behalf, the security authorities then agree on secret material for both entities and this is distributed to the entities using a pre-existing shared key between the two security authorities. After the key has been generated and distributed then entity A and entity B will have the shared key and will be able to communicate effectively with each other.

2.16. Certificates

> *"A public-key certificate (hereinafter "certificate") binds a public-key value to a set of information that identifies the entity (such as person, organisation, account, or site) associated with use of the corresponding private key (this entity is known as the "subject" of the certificate)."*[47]

Users of a PKI system require assurance that the private key belongs to the correct end entity with which the associated security mechanisms will be used i.e. digital signatures or encipherment. User assurance is given by the use of public key certificates which bind the user with the associated public key. The CA digitally signs the certificate after it is assured that the identity of the user matches the associated public key. This assurance can come from either challenge/response

mechanisms or having the RA providing confirmation of a user's identity to the CA. In 1988 X.509v1 was published as part of the X.500 directory recommendations and defines a standard for the X.509 certificate format, this was revised in 1993 where two more fields were added resulting in X.509v2. In 1996 the ISO/IEC, ITU-T and ANSI X.9 developed the X.509v3 certificate standard to provide for interoperability, and adaptation of X.509v2, which added extension fields that could be either specified through the standards or defined by the requirements of organisations

2.16.1. X.509v3 Certificate Syntax

"The X.509v3 syntax is encoded using American Standard Notation 1 (ASN.1), this is a tag, length, value encoding systems for each element."[48] ASN.1 provides a platform independent language to specify data structures and rules to encode data structures and enables two applications on different platforms that have been encoded differently to exchange data. The top level ASN.1 specification is shown in Figure 10.

```
Certificate         ::=     Sequence {
        tbsCertificate              TBSCertificate
        signatureAlgorithm                  AlgorithmIdentifier
        signatureValue              Bit String          }
```

Figure 10: Top Level ASN.1 Specification

The signatureValue field contains a digital signature computed upon the ASN.1 encoded tbsCertificate this is used as the input to the signature function, this signature value is then ASN.1 encoded as the bit string and included in the certificates signature field. The X.509 signatureAlgorithm field shown in Figure 10 contains the identifier for the cryptographic algorithm used by the CA to sign the certificate.

```
AlgortithmIdentifier        ::=     Sequence        {
        Algorithm                   object identifier
        Parameters                  any defined by algorithm optional  }
```

Figure 11: X.509 Signature Algorithm Field

The algorithm identifier is used to identify a cryptographic algorithm and the object identifier component identifies the algorithm (such as DSA with SHA-1). The contents of the optional parameters field will vary according to the algorithm

identified. This field must contain the same algorithm identifier as the signature field in the sequence tbsCertificate. AlgorithmIdentifiers are defined for the following signature/hash combinations RSA with MD2, RSA with MD5, RSA with SHA-1 and DSA with SHA-1

The X.509 tbsCertificate field contains the names of the subject and issuer, a public key associated with the subject, a validity period etc as shown in Figure 12.

```
Version ::=          integer {v.1 (0), v2(1), v3(2) }
CertificateSerialNumber   ::=      integer
Signature            ::=      algorithmIdentifier
Validity ::=         sequence          {
        NotBefore    Time
        NotAfter     Time     }
        Time    ::=  Choice   {
        utcTime utcTime
        generaltime  generalizedtime
UniqueIdnetifier ::=  bitstring
SubjectPublicKeyInfo      ::=      sequence          {
Algorithm                 algorithmidentifier
subjectPublicKeybit string          }
Extensions           ::=      sequence size     (1…..max) of extension
        Extension    ::=      sequence          {
        ExtnID       object identifier
        Critical     Boolean default false
        xtnVlaue     octet string        }
```

Figure 12: tbsCertificate Fields

The version field describes the version of the encoded certificate. The default version is Version.1 .The serial number is an integer assigned by the CA to each certificate. It must be unique for each certificate issued by a CA - this is especially useful when constructing CRLs where the serial number can be used to identify the certificate being revoked. The signature algorithm identifier is also used to specify which algorithm was used to sign the certificate.

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a sequence of two dates, the date on which the certificate validity period begins and the date on which the certificate validity period ends. The unique identifier fields may only appear in the X.509 certificate version 2 or 3, the subject and issuer

UniqueIdentifiers are present in the certificate to handle the possibility of reuse of subject and / or issuer names over time. The SubjectPublicKeyInfo field is used to carry the public key and identify the algorithm with which the key is used. The algorithm is identified using the AlgorithmIdentifier structure. The Extensions field is only applicable for X.509v3 certificates, if present, this field can be used to hold policy information, information on key usage, subject alternative names, basic certificate constraints or certificate naming constraints.

2.16.2. Certificate Policy (CP)

When a CA issues a certificate it is giving assurance that a public key is bound to a user. Different certificates are issued depending on the process, procedures and policies depending on the organisation, application or use of the certificate. “The X.509 standard defines a certificate policy as:

> "*A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose*.”[49]

The certificate policy has to be recognized by all parties involved in the use of the certificate. The policy is represented in the certificate by a unique registered object identifier and the entity that registers the object identifier publishes a specification that can be scrutinised by end entities. A certificate policy can form the basis for accreditation of a CA.

Accreditation can be gained against the implementation of one or more policies by the CA, when cross certification occurs the CAs must assess the others certificate policies to determine the level of trust that can be attached to the certificate within the scope of the defined trust model. In order to support certificate policies there are several X.509 certificate policy fields including the certificate policies extension, policy mapping extension and the policy constraints extension field.

2.16.3. Certification Practice Statements (CPS)

A Certification Practice Statement (CPS) is defined by the American Bar Association (ABA) as "A statement of the practices which a CA employs in issuing certificates."[50] In 1995, the ABA in its guidelines expanded the definition to include a declaration by the CA of the trustworthiness of the system and the practices that it employs in the support of certificate issuance, the CPS could also be part of the contract between the CA and the end entity.

The CA also has to lay down its responsibilities to any relying party including the legal relationships that exist between the parties and the CAs duty of care towards the relying parties, the CA also has to ensure that the relying party is made aware of the CPS and that any associated documents are accessible to the relying party. The CPS should define any standards that the CAs practices and procedures conform to; these references should indicate the suitability of the CAs practices and procedures to the relying entities purposes.

2.16.4. Certificate Revocation

When certificates are issued it is not for a finite period. At some point the certificate has to be revoked, this can be for numerous reasons including expiration of the certificate after a certain period. Changes to the name of the end entity, association between the subject and the CA or compromise of a private key are all reasons why a CA would need to revoke a certificate.[51] Certificates can either be revoked online or offline. Off line revocation takes the form of CRLs, on line revocation takes the form of OCSP, both concepts are explained in detail in the following sections.

2.16.5. Certificate Revocation Lists (CRLs)

X.509 defines Certificate Revocation Lists (CRLs) as the method for certificate revocation; this involves the CA issuing a CRL which is a time stamped list that identifies the certificates that have been revoked, this occurs periodically as is described as off-line certificate revocation. The CRL is published in the repository with the certificates that have been revoked are identified by their serial number, when an end entity wishes to use a certificate it not only checks the signature and the validity but will also check to see if the certificate is on the CAs CRL, this is an obvious disadvantage of this method as there could be long periods between CRLs

being issued. An advantage of this system is that the CRLs can be issued in the same way as the certificates in that they are entered into the register for relying parties to check.

2.16.6. Online Certificate Status Protocol (OCSP)

Another method of certificate revocation is to use an online service, namely, Online Certificate Status Protocol (OCSP). “OCSP enables applications to determine the revocation state of an identified certificate,”[52] it has the advantage over CRLs that in fulfils a requirement of being able to carry out revocation in a more timely manner. OCSP clients issue requests to an OCSP responder and in the time between the request and response, suspends acceptance of the certificate.

An OCSP request contains the protocol version, service request, target certificate identifier and any optional extensions that the OCSP responder may or may not process. When a request is made the OCSP responder determines if the message is well formed, the responder is configured to provide the service requested and that the request contains the information required by the OCSP responder. If any of the conditions are not met then the OCSP responder sends the requester an error message otherwise a response is sent to the requester with the required information.

The response from the OCSP responder can conform to various types, the basic type of response that must be supported by all OCSP servers and clients is that all definitive response messages must be digitally signed and that the key used to sign must belong to either the CA who issued the certificate, a trusted responder whose public key is trusted by the requester or a CA designated responder who holds a specially marked certificate issued directly by the CA, this indicates that the CA can issue OSCP responses for that CA.

A definitive response message contains the version of the response syntax, name of responder, responses for each of the certificates in a request, optional extensions, signature algorithm OID and the signature computed across hash of the response. The response for each of the certificates in a request consists of a target certificate identifier, certificate status value, response validity interval and any optional extensions. There are three types of definitive responses that the OCSP specification

defines; the first is a good response this states that the certificate is not revoked though it does not determine if the certificate was ever issued or that the response was within the validity period of the certificates lifetime. The next definitive response is revoked which defines that the certificate has been revoked either permanently or temporarily and the last definitive response is unknown, this response is issued when the OCSP responder does not know about the certificate being requested.

2.17. Building Trust in PKI

> *"The degree to which a certificate user can trust the binding embodied in a certificate depends on several factors. These factors include the practices followed by the CA in authenticating the subject; the CAs operating policy procedures, security controls, the subject's obligations and the stated undertakings and legal obligations of the CA."*[53]

A relying party that requires a certificate to provide assurance that an entity is bound to a specific public key will require the validation of a certificate this may necessitate the use of certificate chains called certificate paths these are required because a relying party is only ever initialized with a limited number of assured CA public keys.

2.17.1. Hierarchical Modelling of CAs

There are different ways that CAs can be configured to provide the user with verifiable certificate paths that they can trust, the most widely used is the hierarchical model described in IETF RFC 1422.[54] The first level in the hierarchical model is the Internet Policy Registration Authority (IPRA) acts as the root for Privacy Enhancement for Internet Electronic Mail (PEM) certification hierarchy at level 1 and it issues certifications for the next lower level in the hierarchy, all certification paths start with IPRA. Policy Certification Authorities (PCAs) are at level 2 of the hierarchy with each of the PCAs being certified by the IPRA.

The PCA has to publish its own policy and CPS with respect to the certification of subordinate authorities in the CA hierarchy. Level 3 and lower of the hierarchy is the CA; these are certified by the PCA above it in the hierarchy. The CA can only issue certificates for entities whose names are subordinate to itself in the X.500 naming tree with the trust implied by the PCA name. The rules associated with the hierarchical

model ensure that the CAs below the PCA in the hierarchy are constrained to the entities that they can certify with user systems being able to automatically check the naming conventions and ensure that the subordination rule has been followed.
Using X.509v3 certificates:

> "*The requirements of RFC 1422 can be addressed using certificate extensions, without the need to restrict the CA structures used. In particular, the certificate extensions relating to certificate policies obviate the need for PCAs and the constraint extensions obviate the need for the name subordination rule. As a result a more flexible architecture is supported*."[55]

The more flexible approach to the architecture allows the certification paths start with the CA in the relying entities domain with the CAs public key the top level of the hierarchy, this local domain tends to have the advantage of being the most trusted. Name constraints can be imposed by using the extension filed in the X.509v3 certificate and the policy extension fields and policy mappings can replace the concept of the PCA, this approach allows a greater degree of automation with automated determination of certification paths.

2.17.2. Building Trust in TTPs through Standardization

ISO/IEC 14516:2002[56] standardises the guidelines for the use of management of TTPs and as a CA is essentially a CA we can use the guidelines laid down in this standard to ensure that organisations can build and manage trusted relationships with the TTPs that they select to carry out the selected services. The first point to note is that a security authority has to have the ability to chose the TTP that best suites its needs and the TTP should have the ability to choose its clients this ensures that a TTP cannot be forced on an organisation by, for example, regulation or government interference. Trust cannot be established by the use of technical means it has to be established using sound business principles this means that a contract has to be put in place between the TTP and the organisation using its services:

> "*Agreements with third parties involving accessing, processing, communicating or managing the organisation's information should be covered by all security requirements.*"[57]

Table 5 lists some of the terms that should be considered for inclusion in agreements with TTPs these are defined in ISO/IEC 17799:2005.

Control	Description
Information Security Policy	The policy statement should be a high level documents explaining the services offered by the TTP
Controls to ensure asset protection	This includes procedures, process for logical and physical protection of assets and restrictions of use
User and administrator training methods, procedure and security	All staff should be trained to a satisfactory standard; this should be a continual process.
Ensure User awareness for Information Security responsibilities and issues	User have to be made aware of the rules and regulations surrounding their responsibilities
A clear reporting structure and agreed reporting formats	This is important to ensure correct and timely passage of information between TTP and clients
Access control policies	Access required by the TTP to client information and the processes that cover access requests.
Incident Handling	Arrangements for reporting, notification and investigation of information security incidents.
Product/service description	A description of the product or service being provided and details of the security levels of the information being handled.
Service Level Agreements	The target level of service as well as unacceptable levels of service
Monitoring of TTP	The right of the client to monitor the activities of the TTP in relation to the organisations assets.
Audit of TTP	The right of the client to audit the TTP as defined by agreement
Legal Liabilities	Ensuring that legal requirements are met by both parties
Business Continuity	Availability and reliability requirements are met
Termination of Agreements	Contingency plans should be in place in case of either party terminating the contract.
TTPs and subcontractors	Ensuring adequate security controls are put in place

Table 5: IS0/IEC 17799: 2005 TTP Management Requirements

2.18. Legal and Regulatory Aspects of PKI

Any organisation that issues qualified certificates i.e. digital certificates is known as a Certification Service Provider (CSP), the CSP vouches for the authenticity of the binding of an end entities identity to their public key. In May of 2000 the Alliance for Electronic Business set up an industry led approval process called tScheme, this is "the independent, industry-led, self-regulatory scheme set up to create strict assessment criteria, against which it will approve Trust Services**."**[58] tScheme touts itself as an essential element in organisations and consumer's ability to trust when dealing with e-business transactions though it can be argued that self regulation is not a true form of regulation and is only put in place to correct market failure.

Self regulation is normally delegated by Government to industry to manage and regulate the industry in the case of CAs tScheme which aims to meet the requirements of Part I of the UK Communications Act 2000[59] lays out the following; the register of approved providers, this lays out the duty of the Secretary of State to establish and maintain a register of approved providers of cryptographic support services. Arrangements for the grant of approvals, for anyone providing cryptographic support services approval has to be granted by the Secretary of State with the approvals being granted within the limits of certain conditions laid out within the law. Delegation of approval functions outlines the regulation is respect to the Secretary of State delegating responsibility for carrying out the provisions of the Act.

Restrictions on disclosure of information describes the restrictions and caveats in place in dealing with the disclosure of information, pen ultimately regulations under Part I of the Act gives the Secretary of State the right to amend the regulations though any changes have to put in front of Parliament before they would become law. The final section on Part I is the provision of cryptographic support services, this is a broad definition of the term, the definition just means the service and does not refer to the supply of use of computer hardware or software unless integral to the provision of the service. There is little requirement to use a self regulated, fee charging organisation when there is Governmental regulation is in place for the protection of all parties involved in the use of cryptographic support services.

2.18.1. Electronic Signature Legislation

Worldwide adoption of Electronic Signature Law was aimed at allowing countries to facilitate the use of electronic signatures and to contribute to their legal recognition. Countries adopted various forms of electronic signature law to provide both confidence and trust to the consumer and to business. Electronic signature laws allow for the equal treatment of signature technologies (i.e. handwritten signature equal to an electronic signature equal to an advanced electronic signature) and accept that as technology advances then authentication methods will also change.

Electronic signature law also allow for compliance with a set of rules for the Certification Authority, Signatory and any relying third parties and lays out any liability that may arise for each of the parties involved. In international terms Electronic signature laws allow for the provision of recognizing foreign certificates through cross border treaties to allow interoperability at a global level.

2.18.2. EU Directive 1999/93/EC

One such law comes from the EU Directive 1999/93/EC.[60] The main aim of this directive is the promotion of interoperability of electronic signature products because interoperability is the key to expansion and uptake both in business and government circles. It also builds trust in electronic signatures by recognising rapid technological advances will allow authentication of electronic data thus allowing for freer movement of goods and services within the internal market. As the directive sets a balance between consumer and business needs and sets out the liability of those involved trust is created which is increasingly important in dealing with cross border activities with a view to increasing competitiveness and that the directive also facilitates a voluntary accreditation scheme that again will increase trust and confidence in electronic signatures.

The EU directive 1999/93/EC has some fundamental weaknesses, primarily it does not seek to harmonize contract law and is unconcerned with procedural requirements this can lead to “misunderstandings” in contract negotiations as an organisation from one country may not be fully aware of laws regulating the use of Electronic Signatures in another, although the Rome Convention goes some way in alleviating these concerns they are still prevalent. There is also concerns on the interpretation of

the directive within each member state, although there is a voluntary accreditation scheme is available many organisations may see this as another overhead to be avoid and may or may not be more useful if it was made compulsory. The UK Electronic Communications act 2000 says that accreditation is not compulsory; however CAs should register them and provide assurance that they have been independently assessed against standards of quality which could be a good measure to be introduced into the EU Directive to give further assurance of trust.

2.19. Summary

In summary, PKI's offer the ability to offer a foundation for a large organisation to build a comprehensive security architecture. PKI can enable applications to add security to their own interactions with other data, resources or entities and it can provide the core services of Confidentiality, Integrity and Authentication as well as enabling further security services.

To meet the stated objectives this section covers the basic principles of PKI including the history of PKI, fundamental principles and primary components and services. A basic PKI infrastructure is defined along with the terminology relating to it with detailed descriptions of each component. There is a description of the cryptographic algorithms, both asymmetric and symmetric involved in a functioning PKI along with the security services that can be provided by these algorithms. There is a comprehensive key management section detailing with standardised models for key management and various methods of key distribution.

X.509v3 certificates are described in detail including the certificate policy, certificate practice statements and various methods of certificate revocation, digital signatures are described in a low level of detail to support the certificate section. The section aims to allow the reader an understanding of the technical issues surrounding PKI and the ability to determine the drivers for delivering an outsourced PKI and how, ultimately, how to determine the core and enabled services that are offered by PKI and the methods employed by an organisation to ensure trust in their outsource partner ensuring that they are treated as a TTP.

3. Basic Principles of Outsourcing

There are many ways in which a PKI can be successfully outsourced. This chapter will introduce outsourcing in general but more specifically outsourcing a PKI:

- The History of Outsourcing
- Business Reasons for Outsourcing
- Reasons for Outsourcing Security Services
- A Methodology of Security Engineering for Outsourcing
- Governing and Managing Outsourcing
- Advantages and Disadvantages of Outsourcing
- Multi-sourcing Strategies

Each topic in this chapter introduces different aspects of outsourcing PKI. A section of this chapter is dedicated to multi-sourcing, a new concept in outsourcing whereby organisations blend information security services from internal and external providers for optimal results. This is an important concept for the reader to understand as multi-sourcing strategies are becoming more prevalent in the business world.

3.1. Introduction

The term Outsourcing entered the business lexicon in the early 1980s and described the process of acquiring sources or services from external sources. A dictionary definition of Outsourcing is "to procure (as some goods or services needed by a business or organisation) under contract with an outside supplier."[61]

Today's modular organisational structure means that the acquisition of goods or services needed by the business does not have to come from an outside supplier, goods or services can now be procured from one part of the business to another through "in-house" service and supply agreements.

Outsourcing is not always the best option for an organisation. There may be cases where it is impossible for an organisation to outsource, such as Governments, Military or organisations dealing with Critical National Infrastructure. For those who can

outsource it has to be a strategic decision as it contracts out important functions of the organisation to a specialized provider.

These providers have to become more than just a solution provider but they have to become an extension of the organisation itself.

> *"The difference between simply supplementing resources by subcontracting and actual outsourcing, is that the latter involves substantial restructuring of particular business activities including, often, the transfer of staff from a host company to a specialist, usually smaller, company with the required core competencies."*[62]

3.2. History of Outsourcing

Industry has always looked at ways of gaining competitive edge over rivals, from the days of large locally owned companies organisations have looked at ways to increase profitability, reduce costs and maximize production. Historically, outsourcing is not a new concept in the United States from the mid 1920s textile mills moved their operations from the expensive towns in New England to the Southern States where costs were substantially cheaper. After the Second World War components and assembled products were sourced to offshore factories, this approach was particularly prevalent in the United States as it had one of the only post war economies that hadn't been destroyed by five years of conflict reaped the benefits from cheaper overseas labour.

Year	Focus	Approach
1960s	Hardware	Service and Facility Management
1970s	Software	Facility and Operation Management
1980s	Hardware and Software Standardization	Customization Management
1990s	Total Solution	Asset Management

Table 6: Timeline of IT Outsourcing Trends

The introduction of mainframes by IBM in the 1960s ensured that the IT-Business begun in earnest. "IT outsourcing started with time-sharing and processing services,

as computers were very expensive.[63] In the 1970s standard application packages were introduced and the contracting of programming started a new trend in outsourcing.

The timeline of IT outsourcing trends (Table 6) shows that the evolution of outsourcing changed along with technological advances, from the early days of outsourcing in manufacturing through the 1970s and 1980s which were service orientated until today when the emphasis is on total solution outsourcing.

3.2.1. 1960s and 1970s

The 1960s and 70s saw the beginning of the process of globalization, no longer were organisations satisfied with operating single industry companies they wanted to diversify to protect organisations from a downturn in profits in any one sector. This diversity caused many organisations to overstretch themselves and the management structures became complicated and over bearing, this proved to stifle the flexibility of organisations to deal with changes in the modern world.

At this point organisations started to realise that they had to concentrate on their core businesses, that's where they were making profits. This realization brought about the modern term of outsourcing, functions that were not directly connected to the core business or that the organisation was unqualified to carry out were outsourced. As each stage of the process became more successful for organisations then they looked at ways to lower costs and managers embraced it with vigour outsourcing nearly all of the activities not relating to the core business, including Human Resources, Distribution, Accounting etc.

3.2.2. 1980s and 1990s

As technology boomed in the 1980s and 90s American and Japanese firms started to outsource more of their electronics manufacturing to cheaper locations in South East Asia to meet the demand of western consumers. Computing power was increasing and prices were dropping and to keep those prices down organisations had to find cheaper ways of producing their products and the push to outsourcing to even cheaper locations began. By the 1990s the term Global Production Networks (GPN's) was common this was defined as:

> *"Interconnected functions and operations through which goods and services are produced and distributed - have become both organisationally more complex and also increasingly global in their geographical extent.."*[64]

The concept of GPN allowed organisations to be competitive, for the price of one technician in the UK, Europe or the USA organisations could have ten technicians for the same price in the developing world.

3.2.3. 2000 to Present Day

By the end of the 1990s and the beginning of 2000 outsourcing became incredibly profitable, the strategic objectives of organisations changed and only a portion of the core business was carried out by organisations with all other business functions being carried out by outsourced providers. The main driver for this change was the distribution of computer networks and the ease of carrying out e-business, as technology allowed organisations to more easily achieve their business objectives it also allowed for more and more of the organisations business processes to be outsourced.

> *"In 2003, outsourcing accumulated $298.5 billion in global revenues, Gartner Inc. data shows. At least 3.3 million US jobs and $136 billion in wages will be outsourced to India, China, Russia, Ukraine, Pakistan, and Vietnam by 2015."*[65]

Outsourcing is and will continue to be a strategy employed by organisations to meet its business objectives though as the decade progresses. Outsourcing contracts with a value of £27.06 million (€40 million) bracket was up by 78% in 2006, this equates to £8.23 billion (€12.3 billion) of new business.[66]

3.3. Business Reasons for Outsourcing

Outsourcing is driven by the tactical and strategic objectives of an organisation in order to improve its operational and financial effectiveness in a competitive marketplace. Outsourcing has evolved to a point where it is the preferred method of

many organisations as if fulfils the needs of the organisation, investors as well as helping the business position itself better in the marketplace. [67]

Reasons	Sought Benefits
Organisationally Driven Reasons	Enhancing effectiveness by focussing on core skills
	Increase flexibility to meet changing business conditions, demand for products, services and technologies
	Increase product and service value, customer satisfaction and share holder value
Improvement Driven Reasons	Improve operating performance
	Obtain expertise, skills and technologies that would not otherwise be available
	Improved management and control
	Improve risk management
	Acquire innovative ideas
	Improve credibility and image by associating with superior providers
Financially Driven Reasons	Reduce investments in assets and free up these resources for other purposes
	Generate cash by transferring assets to the provider
Revenue Driven Reasons	Gain market access and business opportunities through the provider's network
	Accelerate expansion by tapping into the providers developed capacity, processes and systems
	Expand sales and production capacity during periods when such expansion could not be financed
	Commercially exploit the existing skills
Cost Driven Reasons	Reduce costs through superior provider performance and the providers lower cost structure
	Turn fixed costs into variable costs
Employee Driven Reasons	Give employees a stronger career path
	Increase commitment and energy in non core areas

Table 7: Reasons to Outsource and Benefits Sought

Table 7[68] details the most common business reasons for organisations to outsource and the benefits that they aim to achieve.

Outsourcing allows organisations to concentrate on their core business whilst operational necessities are carried out by their partners that are experts in their respective fields. One of the greatest burdens for an organisation is the day to day running of systems in that cost valuable resources, both in terms of money and time,

when the answer could simply be to outsource allowing assets to be used to make the core business more effective.

> *"On average IT departments spend over 70% of their time and effort in basic operational tasks with less than 30% available for research, development and improvement."*[68]

3.4. Reasons for Outsourcing Security Services

As there is a continual change in the organisation's threat landscape it is critical that the organisation maintains reliable and effective information security. Any decision on outsourcing security solutions has to be based on the considerations in the context of managing business risks.[69] Risks can be identified and treated as part of a risk treatment plan, this includes acceptance, mitigation and transference of risks.[70] Forming strategic partnerships with security service providers is an acceptable treatment option for the transferral of the risks associated with information security. Specific reasons for outsourcing managed security services, including PKI, can be summarised in by using "Ten Reasons to Outsource Managed Security Services" by Veritas. These are shown in Table 8 below.[71]

Reason	Description
Device management and monitoring can be mundane and tedious.	As skilled staff are in short supply having the system monitored by a security provider frees up those individuals to focus on more pressing tasks.
The best in-house information misses the big picture.	Concentrating on only the internal PKI system and not focussing on the wider trends and threats to the organisation means that the threat landscape can change quicker than the organisation can.
Threats don't go on vacation or take holidays.	As with device management skilled staff are in short supply. The infrastructure has to be continually monitored and relying on one or two individuals presents a business risk.
Information Security is patchy and contradictory, a moving target.	It has become increasingly difficult for just one organisation to understand the impact of evolving threats. A security provider is in a stronger position to understand and combat these threats.
Security tools come in a box: security solutions don't.	PKI is a complex system and the configuration, management and monitoring of it is difficult,

	time consuming and expensive.
Your operational costs may escalate with each new security initiative.	Outsourcing security solutions can lower operating costs by using a vendor neutral provider. It will also help with lowering costs for recruiting, training and retaining staff.
You worry about every threat, hack, virus, or worm that may attack.	When the organisation outsource to a security provider that provider takes on the responsibility for the overall effectiveness of the system leaving the organisation's staff to concentrate on its core business.
Non compliance is a business risk.	Whether or not the organisation is aware of its regulatory obligations, the business can be liable for security breaches and non compliance when working within certain industries.
Find out how well your security initiatives are doing.	Organisations invest heavily in its technology and people. With the evolving threats and increase regulation and outsource provider may be better placed to look after the organisation's systems and take the burden of the time consuming activities associated with keeping up to date with threats and regulation.
Strategic outsourcing keeps you focussed on your business.	Outsourcing can help the organisation maximise its technology investment and ensure that the focus remains on creating a more secure environment for the enterprise and making the business more profitable.

Table 8: Veritas: Top 10 Reasons to Outsource Managed Security Services

Trust is the key with outsourcing, it is essential that the organisation and it's outsource partner have the necessary framework in place such as the existence of contracts, non-disclosure agreements and service level agreements.[72] With any outsource agreement there will always be situations that arise that will require the revision of agreements, this is an area that requires the trust between the two parties. When outsourcing security services it is also important to note that an organisation can quickly become dependant on its partner.

In our opinion then advantages of outsourcing PKI both in terms of the business and as an outsourced security solution far outweigh the disadvantages. Though the organisation has to ensure that the outsource partner that is selected is right for its business, that is the aim of our AB-5C model for outsourcing PKI.

3.5. A Methodology of Security Engineering for outsourcing PKI

An organisations outsourcing methodology usually involves in the engagement of processes that are designed to be mutually beneficial to both the organisation and the outsource partner, although every partnership will be decidedly different there are certain steps that should be undertaken.

We propose the methodology used for a security of engineering of PKI outsourcing is System Security Engineering – Capability Model as defined in ISO/IEC 21827.[73]
This Model was selected as it was designed to be used by a variety of organisations who are involved in product development, system integration, administration and the provision of security services.

The SSE-CM model was developed to be used as:

- A tool for engineering organisations to evaluate security engineering practices and improve systems.
- A method for security engineering evaluation organisations can establish confidence in an organisation's systems and as an input into the assurance programme.
- A mechanism for customers to evaluate a provider's security engineering capability.

As such it is well suited as the preferred methodology for security engineering of PKI Outsourcing. The benefits of this model include:

- Continuity
    - Using knowledge from previous efforts can be used in future efforts.
- Repeatability
    - Ensuring projects can be completed with repeated successful effort.
- Efficiency
    - Allowing developers and the evaluators to work more efficiently.
- Assurance

- Giving all parties involved the assurance that security needs of the organisation are being addressed.

The model will describe the characteristics of the methodology and security engineering processes that must exist in order to ensure good security engineering on part of the organisation and the outsource supplier. The model provides a standard metric for security engineering practices and covers:

- The entire security engineering life cycle.
- The entirety of the organisation.
- Interactions with concurrent engineering activities.
- Interactions with other organisations.

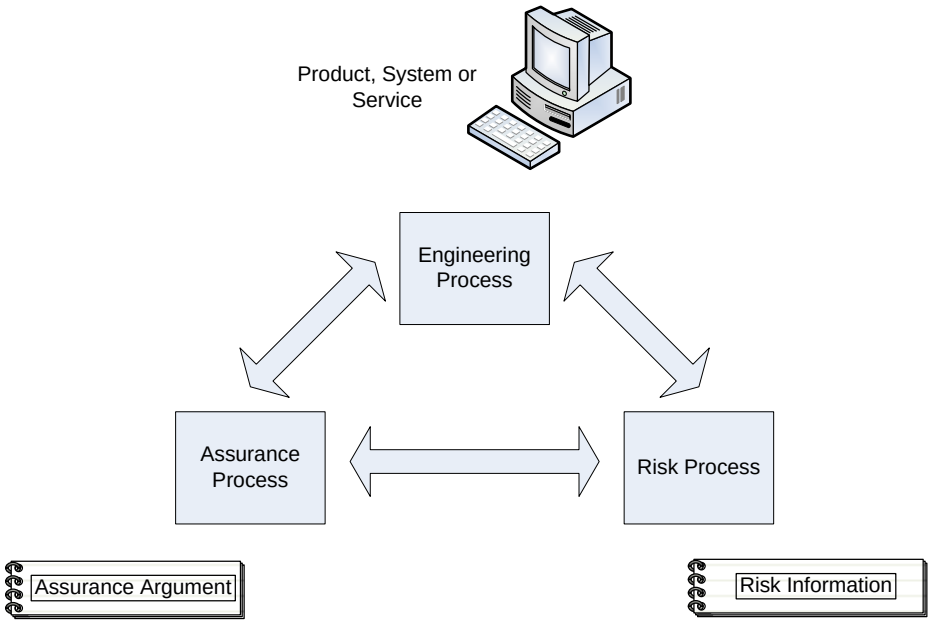


Figure 13: Security Engineering Process Overview

Figure 13 shows the ISO/IEC 21827 Security Engineering Process Overview.[74] The three areas defined, engineering process, assurance process and risk process work together to ensure that the security engineering process meets the goals and the objectives of the organisation.

3.5.1. Risk Process

Security Engineering is concerned with the managing of risks to business information. It should reduce the likelihood of information security incidents occurring leading to breaches of Confidentiality, Integrity and Availability. Security Engineering aims to prevent incidents occurring, reduce the negative effects of incidents which do occur, improve recovery from these incidents and learn lessons to help with future prevention.

The Risk Management process is made up of several dependant processes and procedures within itself. These being The Organisations Security Requirements, Risk assessment, Risk Treatment, Risk Acceptance, Risk Communication and Risk monitoring and Reviewing. Risk assessment can be further divided into risk analysis and risk evaluation. The security requirements of an organisation can be categorised into the overall business strategy of the organisation and the loss impact to these requirements dependant upon incidents.

The Risk assessment process is a process defined by the Risk analysis and Risk evaluation. Risk analysis is the process of identifying risks, describing risks and the estimating and quantifying the impact of these risks. The two main types of risk analysis are quantitative and qualitative. Quantitative assigns an annual impact figure to the impact of an incident upon an asset whilst qualitative measures the impacts based upon tuition and experience. The result of either process is to provide information to management in an understandable format for consideration and budgeting. Once the risk analysis process has been completed risk evaluation is necessary to compare the estimated risks against the risk criteria or objectives of the organisation. The evaluation process defines whether or not the risk should be accepted or treated.

The Risk treatment process begins with the organisation’s objectives and criteria for determining whether or not risks should be accepted. In general terms risks are accepted if it is surmised that the risk is low or the cost of treatment is in excessive of the organisations budgetary acceptance of that risk. There are several options open to the treatment of identified risks:[75]

- Accept the risk
- Avoid the risk
- Manage the risk
- Transfer the risk

By accepting the risk the organisation has knowingly and objectively accepted the risks provided they are within the organisation's policy and criteria for risk acceptance. The managing of risk involves the applying of appropriate controls to meet the requirements of the risk assessment process. Controls should bring the level of risk exposure to an acceptable level, without reducing the effectiveness of other controls, within the requirements of the organisation's objectives. Controls will very rarely eliminate risk totally so therefore the residual risk must be within the organisations risk appetite and acknowledged as so. The transfer or risk is normally handled by transferring the risk to a third party in the form of insurance against the identified risk.

3.5.2. Engineering Process

Security engineering is a process of concept, design, deployment, operation, maintenance and decommission.[76] This process is not solely in the realms of security engineering but has to take into account other engineering activities such as systems and communications engineering. This model puts the emphasis on security engineers working as part of larger teams with co-ordinated activities with other engineering disciplines to ensure that security is not left as a stand alone activity but is part of the full design.

Information gathered from the risk process along with full system requirements, organisational policy, procedures and a whole host of other information is brought together to identify the security requirements of the organisation. After this process is complete the security engineers can identify specific requirements and begin the process of creating solutions. In the case of the model we are suggesting for the outsourcing of PKI the results from the modelling of organisational outsourcing based on the requirements of the PKI (Section 4.7) will be taken into account when specifying the requirements.

In specifying the requirements for an organisations PKI part of the security engineering process will be to determine whether there is a requirement to outsource or can the security requirements be met “in-house.” There is one major problem with determining these requirements, that is, the decision cannot be made on the basis of security alone. A range of considerations have to be taken into account, this can vary from cost, risk and ease of use through to more problematic areas such as: [77]

- Difficulty retrieving keys and certificates
- Questionable value of certified key representations
- Certificate processing complexity
- Costly certificates
- Problematic cross domain trust management
- Naming semantics
- Use with insecure clients
- Privacy compromises

It is the responsibility of the security engineer to ensure that to ensure that these areas are addressed to ensure that during the security engineering process that these issues to not re-appear and introduce new risks into the system later in the lifecycle.

3.5.3. Assurance Process

A failing of the SSE-CMM model is that it only contributes one aspect of the assurance process and that is in the confidence gained by organisations due to the repeatability of results in the security engineering process. It is aimed primarily at mature organisations as those are more likely to be able to produce positive repeat results. For immature organisations it may not possible to provide positive repeatable results, in our opinion this is a major failing of the SSE-CMM assurance process. A better option for the assurance process would be the Common Criteria which was standardised in ISO/IEC 15408.[78]

The Common Criteria is a harmonisation between ITSEC [79] and the US Federal Criteria [80] and is split into three parts:

- Part 1: Introduction
- Part 2: Security Functionality Requirements
- Part 3: Security Assurance Requirements

The Common Criteria allows for the evaluation of both products and systems with product evaluation is done against an approved protection profile which is an independent statement of the security needs of the system in a particular situation. The flexibility of the Common Criteria is provided by the use of a Target of Evaluation (TOE), a Security Target (ST) and a Protection Profile (PP).

A Target of Evaluation is either a product or a system. The standard uses the term product to refer to either a single product or a system of products. It is important to note that a single product may be used in a variety of different circumstances operational environments and produce different results in each on of these. Hence, we define a Target of Evaluation (TOE) to be any product or system that is being used in one particular way.

A security target is a product-dependant statement about the security that a TOE aims to give. It is roughly equivalent to the information provided by the sponsor in an ITSEC evaluation. However, an ST can mandate that a TOE match the levels of security demanded by a protection profile. This allows for the classification of products in the same way as in the US Federal Criteria

ISO/IEC 15408 part 3 [81] describes a set of Evaluation Assurance Levels (EALs) from EAL0 to EAL7. The defined evaluation assurance levels (EALs), i.e. the levels defining how rigorous an evaluation should be, are mostly aligned with ITSEC and TCSEC (Orange Book). The only EAL that is not aligned with earlier evaluation criteria as EAL1. This corresponds to simple functional testing using the interface and security functionality defined in the protection profile. This analysis should be performed by an independent body.

Whichever method is used to provide assurance certain levels of evidence have to be produced to support the stated claims, evidence is normally in the form of documentation produced during the course of the engineering process.

3.6. Governing and Managing Outsourcing

When the organisation has selected it's outsource partner and the solution is being provided then the relationship has to be managed effectively and good governance procedures put in place. A good governance structure can provide:

> *"A framework for the leadership, organisational structures and business processes, standards and compliance with theses standards, which ensures that the organisations information systems support and enable the achievement of its strategies and objectives."*[82]

It is important that the governance and management procedures include what steps the outsource partner will undertake to meet its own legal and liability obligations, having clear escalation procedures, ensuring that there are training and awareness programmes in place so that all staff are aware of their responsibilities and that disaster recovery and business continuity plans are in place.

Relationship Management is an aspect of outsourcing that is often overlooked; it is up to the organisation doing the outsourcing to manage the relationships effectively as this is something that is not always factored into the planning phase. A hidden cost that can occur is the provision of a relationship manager and a technical support team to manage the relationship and the technical aspects of the outsourced service, these are full time positions that are required in order to ensure that transactions are carried out according the pre-agreed timescales, standards and quality.

> "*To build the relationship effectively, the relationship manager and the organisation should be active in monitoring and evaluating performance and in addressing issues. If this does not occur, the provider's performance is likely to suffer. This might happen because the provider takes shortcuts that are not caught and corrected.*"[83]

It is common sense that something as important as outsourcing should be managed properly, the organisation although not trusting an outsource partner to provide for its core business. It would not be able to operate if its support functions were to fail, not only leading in loss of income but it could prove catastrophic if the organisations reputation was fundamentally damaged.

3.7. Advantages of Outsourcing PKI

The advantages of outsourcing PKI include:

- Saving's on setup and operating costs
- Provision of all in one services
- Quick Implementation
- Scalable solutions
- Reliability of solutions
- Organisationally Driven

Building and operating an in-house PKI can be extremely expensive, the average PKI installation is in the region of $1 million.[84] These costs include the technical expertise to configure the software, setting up the system policies, and the registration, issuance and revocation of digital certificates. Outsourcing can provide a method of allowing organisation's to set up a PKI through outsourcing as there is no up front investment in infrastructure, and no requirement for the recruiting and training of new staff. There is a downside too, although initial set up and operating costs can be low in the long term because the organisation will have to pay year on year for the issuance and revocation of certificates as long as the contract lasts.

Outsource partners can provide a "one stop shop" for PKI solutions, making available a bespoke solution to meet the organisations requirements. Fees are levied against the services that are provided by the outsource partner, such as:

- Certificate Authority functions.
- Registration Authority processes.
- Certificate Repositories.
- Key Backup and Recovery Systems.

- Non-repudiation services.
- Time Stamping Services.
- Directory Services.

These services can be quickly implemented as outsourcers are geared towards providing primary critical components such as the RA, CA etc. Secondary services can also be provided such as policies, procedures, guidelines etc.

Outsourcing PKI can offer the flexibility, scalability and reliability that an in house solution can't.[85] Outsource providers are well placed to meet those demands. PKI requirements grow from the initial pilot scheme of small numbers of user accessing secure applications to a fully rolled out, high volume PKI system. Providers have strategic plans in place for growth of PKI systems, and are well versed the requirements to scale the system according to the customers needs.

Having an outsource provider sign the certificates that the organisation issues with its own root certificate ensures that the certificates are seen as reliable, but more importantly they have a high level of trust associated with them.

3.8. Disadvantages of Outsourcing PKI

It has been suggested in studies that between 20% to 35% of all IT Outsourcing contracts are not renew after expiration.[86] There are some serious disadvantages to outsourcing a PKI solution [87], a selection of these are listed below:

- Building Trust Relationships
- Defining Multiple Legal Relationships
- Roaming and Usability of the PKI System
- Private Key Management
- Certificate Distribution and Revocation
- Legacy System Migration

PKI doesn't provide the answer to creating trust. Building trust requires more that just the issuance of certificates, there has to be guarantees put in place. Methods for building trust in a PKI have already been discussed in Section 2.17 of this document.

Even with risk assessments, contracts, audits and other "business methods" trust has to be won. It is only through a long standing relationship and stringent processes that an organisation will trust it's outsource partner. It may be the case through business necessity that there will be various levels of trust associated with certification, the amount of trust placed in an outsource partner normally hinges on judgement.

"An impediment to the adoption of PKI has been the legal complexity and novelty traditionally associated with PKI."[88] There are many legal ambiguities associated with PKI. For instance, In 2000 Australia's National Office for the Information Economy (NEAC) published a report the "Legal Liability in E-Transactions" [89] found that, in general, Australian law provided an adequate level of guidance on the apportion of liability.

There is however an exception in that there is no legal basis for liability in the relationship between the CA and the Relying Party (RP). This is compounded by the lack of provisions under private law to allocate liability between the CA and the RP. The Australian case is relevant as along with the US, and much of Europe the laws are technologically neutral and require more research and refinement in terms of the apportion of liability.

Some of the problems with roaming and usability of PKI systems emerge from the use of soft certificates. These allow users to have their private keys stored on a central server and uploaded to their terminal when required. [90] This technology allows a roaming capability by allowing the user to move from one terminal to another without the need to manually export their private keys. This also enhances usability of the system.

However, the roaming of soft certificates provides an attacker with the option of eaves-dropping the central server in order to recover cryptographic keying material. It can be a costly in terms of money and manpower to ensure that the risks soft certificates present to the business are managed effectively.

Key Management problems, certificate issuance and revocation, and legacy system migration are all well known problems in PKI. Outsourcing PKI does not get rid of these problems, it can make the system easy to manage but the organisation has to ensure good governance and management of the outsource provider and the selected solution in order to overcome these problems.

3.9. Multi-sourcing Strategies

> "*Multi-sourcing: the disciplined provisioning and blending of business and IT services from the optimal set of internal and external providers in the pursuit of business goals*."[91]

A multi-sourced PKI solution is optimized to meet the needs of the organisation. Outsourcing can mean that sometimes the organisation has to relinquish sole control of its outsourced functionality. In terms the importance of and organisations information assets the best option may not be an outsourced solution but a multi-sourced solution. This ensures that the organisation's information assets that it wants to retain control off can be kept "in house".

Multi-sourcing is seen as a step beyond outsourcing as it provides more agility and capability by using various providers to enable the addition of new and versatile frameworks for managing functionality from providers both inside and outside of the organisations core disciplines. For Multi-sourcing to be successful organisations have to look beyond the quick-fix options of traditional outsourcing and look the "creation of a sourcing strategy that is tightly linked to the overall business strategy and constantly monitored by an effective enterprise-wide governance system."[92]

When building a multi-sourcing strategy it is important that the business objectives are clearly defined, it is often clear that organisations from the very start of the process are not clear on the objectives that they wish to achieve. The objectives are normally either over-specified leading to micro management or an unworkable solution to under-specified leaving the provider to have carte blanche when designing the solution which normally fails to meet the organisations original objectives. The next stage in the strategy is to ensure that the organisation gets maximum value for their investment either from an internal or external provider, to do this the

organisation has to factor in including how much is the solution going to cost and are there going to be efficiency gains that make the sourcing of the functionality worth while.

The organisation has to deal with issues of integration if the functionality is sourced internally will it be easier to integrate the required systems and services than it would if the functionality was sourced from an external provider. Finally, how does the organisation govern and manage relationships in a multi-sourced environment it appears that it would be easier to implement internally sourced functionality as the policies, procedures, guidelines etc are already in place for existing staff but it could prove more difficult for externally sourced functionality, it has already been mentioned that there is a need for an effective enterprise-wide governance system which could prove costly.

Multi-sourcing as well as outsourcing can have many advantages and disadvantages for an organisation, cost, competitive edge and external expertise all combine to provide the organisation with the tool to concentrate on core business and remain competitive in the market place. Multi-sourcing takes this one stage further and promotes sourcing of functionality both internally and externally to provide the best possible solution to meet the business objectives of the organisation.

In terms of PKI, this approach if adopted could prove to be the optimum model for a sourced solution allowing the organisation to source internally the functionality that will retain the confidentiality, integrity and availability of its core assets whilst externally sourcing the functionality that it is not capable of providing internally either due to cost restrictions or lack of skilled personnel.

3.10. Summary

To meet the stated objectives I have defined the basic principles of Outsourcing, the history of outsourcing is explored to determine why organisations outsource and the various reasons that are used to measure the benefits of outsourcing such as organisationally driven, improvement driven and financially driven reasons. There is a brief introduction to the methodology of security engineering in outsourcing. The

SSE-CMM model outlines the risk, engineering and assurance processes required when dealing with the outsourcing of PKI.

There is a section that looks at governing and managing outsourcing - this is a brief description of governance and how it applies to outsourcing and the relationship management aspect of outsourcing along with the advantages and disadvantages of outsourcing. The final section deals with multi-sourcing - this is the new thinking of outsourcing which provides a more flexible solution by combining internal and external processes in an apparent seamless match which are closely managed and governed to provide the optimum degree of efficiency.

4. Proposed Model for Outsourcing PKI

This chapter describes our own model for Outsourcing PKI, various models, both of the authors own designs and existing models, to provide a modeled solution to outsourcing PKI. The models detailed in this chapter are:

- The Enterprise Security Architecture will be based on the Sherwood Applied Business Security Architecture (SABSA).[93]
- Our AB-5C model based on organisational checklists, which will determine core service requirements, enabled services requirements, deployment considerations, operational considerations, information dissemination requirements and trust model deployment and considerations.
- Aligning outsourcing with the organisation's strategic plan, the "Seven-S Model" [94] developed by McKinsey & Company in the 1970s is used to analyze the organisation's effectiveness and help the organisation plan for and cope with the change of outsourcing PKI.
- Continuity management will be based on ITIL Service Continuity Model [95] which is designed to support the business continuity management functions of an organisation and ensure that the services disrupted can be recovered within an agreed timeframe. Following on from the continuity management are our own incident management flowcharts both for incident handling and post incident review.
- Change management modeling is done through a PA Consulting framework for outsourcing and outsourced enabled change.[96] This model is only briefly explained and added to show the importance of having an effective and efficient change management scheme as part of the overall outsourcing activity.
- The final section brings together these models into the author's own model (AB-5C Model), detailing a common operating environment where organisation's cultures and strategic aims are aligned based on the results of the activities explained in this chapter.

4.1. Introduction

Organisation's have their own methods of selecting which processes and services have to be retained in-house and which have to be outsourced, this is no different for PKI. This process normally involves alignment of the strategy and the wider business goals and objectives to that of the outsource partner. Modelling PKI outsourcing is a complex task and in this section we propose our model (AB-5C Model) that will give organisation's a tool to outsource PKI in a structured way relevant to the organisations business needs.

4.2. Proposed Model

The model we are proposing deals with both business requirements and the technology of outsourcing PKI. The AB-5C Model of Outsourcing PKI is a qualitative approach to helping the organisation make the right decisions when choosing to outsource PKI. This in turn can achieve a reduction in costs, access to resources and services that it cannot provide for internally, but at the same time retain flexibility and innovation through outsourcing functional elements of the organisation's PKI.

4.3. The AB-5C Model of PKI Outsourcing

Our AB5C Model is designed to assist organisations in its PKI outsourcing activities. It is a method of analyzing aspects of selecting and defining an outsourced PKI solution. The parts of the AB-5C Model are:

- (A) - Adding Value to the Organisation
- (B) - Business Strategy
- (5C) - Competencies, Conditions, Culture, Continuity and Change

The model we propose defines the importance of adding value to the organisation, details the strategy that the organisation uses when planning an outsourced PKI, and defines a set of variables that have to be met by any outsource provider. All of these concepts are explained clearly in this section.

4.4. Adding Value to the Organisation –Business Goals and Objectives

Outsourcing has to add value to the organisation, it has to meet the business goals and objectives laid out by senior management and it has to ensure that it is the best decision for the organisation, not purely a cost cutting exercise. In adding value to the organisation the CEO and board have to ensure that the correct level of investment is set to meet the business goals and objectives.

If a full PKI rollout is required then the management have to be sure that the correct level of management buy-in is available. This buy-in is required, not just during the implementation of the system, but also in its running, maintenance and as the system adapts when functionality requirements change. The executive have to understand that the level of expertise required for a PKI system covers many disciplines and as such it they must have all of the secondary processes in place to meet the business goals and objectives, such as audit and training and awareness programmes.

To ensure that the goals and objectives of the organisation are met there has to be policies that are followed; these have to be specific so that there is no confusion about the requirements of the system in meeting strategic objectives of the organisation. The key aim is to be precise in the requirement and not deviate from the original goal. There have to be procedures put in place to continually measure the effectiveness of the system in meeting the goals and objectives of the organisation. As new goals and objectives are added then the system has to be measured to ensure that it is still adding value to the organisation.

The organisation has to be realistic in what a PKI system can do in meeting its business goals and objectives. PKI is a technology solution in support of the business but can also be seen as a business tool. What it is not is a quick fix that is implemented just because the technology is available. It has to be implemented in support of the organisation and relevant to the organisation. Finally, the timeframe in which the goals and objectives have to be achieved by the utilisation of a PKI system has to be realistic, there has to be adequate time for the design lifecycle to be completed with the associated testing and re-adjustments to take place. As with any new system this can take a significant amount of time and thus the expectations in

terms of meeting the goals and objectives of an organisation within a given timeframe have to be realistic.

4.5. Business Strategy – Aligning Outsourcing with Strategic Planning

Strategic planning is not a solitary discipline and has to be looked at from different views in order to understand the processes and consequences of long term decision making for the organisation. There are four common views to look at: "the futurity of current decisions, process, philosophy and structure."[97]

Firstly, the futurity of current decisions looks at the cause and effect of decisions over a pre-agreed period of time, allowing management to adjust the planning considerations accordingly and factor in any alternatives that may need to be considered. In terms of outsourcing the futurity of current decisions has to take into account the changing needs of the organisation and ensure that the management of the outsource agreement can be flexible enough that if the initial planning is flawed then alternatives can be put in place to correct initial planning decisions and the organisation doesn't suffer as a consequence.

Secondly, the process view starts with the setting of the organisations aims and objectives and defines the processes, policies, guidelines, strategies etc to support the achievement of those aims and objectives. The process view takes into account the time period of the strategic plan, how it is to be implemented and what results will be achieved. This will result in a set of strategic plans that will form the basis of a continual planning processing phase which will enable the organisation to meet the continually changing and demanding requirements of their core business. As with any technological solution, PKI has to have a strict set of project plans and guidelines that allow for the implementation processes to be followed, measured and changed when and if required.

The third, philosophical view is not a strict process driven view but a thought driven process that guides decision making. In the case of PKI the organisation, both management and staff, have to believe that it is the right decision for the future of the organisation or the implementation will fail to be fully accepted within the organisation and thus fail. The final view is the structure view is a more formalized

strategic planning system and takes into account the main types of organisational strategic planning, these being, operational planning, short-term budgetary planning and medium range program planning as well as the organisations overall strategic planning processes.

The final view is the structural view. Strategic planning can follow various models such as centralized, de-centralized and devolved structures with each of the organisational strategic planning streams coming together to form the overall organisation's strategic plan. The strategic planning structure can have a huge impact on the adoption of a PKI as each constituent part, if following the organisational models, needs stakeholders from each of the work streams to ensure that any implementation is managed correctly and provides each of the management streams with the system that meets all of their own and the organisation's goals and objectives in line with both tactical and strategic plans.

4.6. Competencies - Defining an Enterprise Security Architecture

A model for measuring competencies can be based on the Sherwood Applied Business Security Architecture (SABSA) which itself is based on the Zachman Framework.[98] "SABSA is a model and a methodology for developing risk-driven enterprise information security architectures."[99] SABSA is characterised by the fact that all decisions are derived by analysing the business requirements for security of an organisation This methodology makes the SABSA model very desirable when defining an Enterprise Security Architecture for Outsourcing PKI both for the organisation, its outsource partner and the alignment of the organisations competencies.

4.6.1. SABSA Operational Security Architecture

The SABSA Operational Security Architecture is based on a six layer model which is the basis of a process led methodology for creating security architectures. In Figure 14 the model is shown with the operational security architecture spanning the other five architectures. The reason for this is that operational security issues occur at each of these five layers and have to be addressed throughout. Figure 14,[100] shows the SABSA Model for Security Architecture Development with Table 8, [101] a brief overview of each layer.

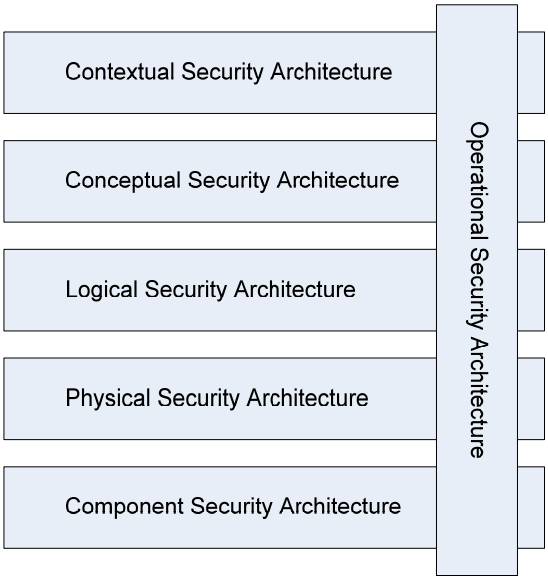


Figure 14: SABSA Model for Security Architecture Development

Layer	Description
At the Contextual Layer	Business policymaking, business risk assessment process, business requirements collection and specification, organisational and cultural development, etc.
At the Conceptual Layer	Major programmes for training and awareness, business continuity management, audit and review, process development for registration, authorisation, administration and incident handling, development of standards and procedures, etc.
At the Logical Layer	Security policymaking, information and classification, systems classification, management of security services, security of service management, negotiation and interoperability standards for security services, audit trail and monitoring and innovation of actions, etc.
At the Physical Layer	Development and execution of security rules, practices and procedures, including: cryptographic key management, communication of security parameters between parties, synchronisation between parties; ACL's (Access Control List) maintenance and distribution of ACEs (Access Control Entry), backup management (storing, labelling, indexing, etc), virus pattern search maintenance, event log management and archiving, etc.
At the Component Layer	Products, technology, evaluation and selection of standards and tools, project management, implementation management, operation and administration of individual components, etc.

Table 9: SABSA Operational Security Architecture

4.6.2. Contextual Layer - Security Architecture

The contextual layer which is considered the be the layer that expresses the business view in which there is analysis of the context in which the system will be used, the business has to know how the system will meet the business goals and objectives and it is the businesses responsibility to answer these questions and provide the best solution to meet the business goals and objectives.

In the case of PKI the type questions that the business will have to ask itself are how, when, where, why and by whom will the system be used and how will it meet the strategic goals and objectives of the organisation. The contextual layer will also include the creation of the organisations policies, procedures, guidelines along with the risk assessment process. The system requirements will be developed at this layer along with the specifications and any other business orientated process that will ensure that the developed system will meet the business requirements of the organisation.

4.6.3. Conceptual Layer - Security Architecture

The Conceptual layer is the architect's view of the system is the architect's concept of how the organisations goals and objectives will be met by the security architecture. It is also a strategic view of how all the work streams involved in the system will come together to provide the final solution along with the high level requirements and design decisions.

In terms of PKI the conceptual layer will provide the high level strategies that will allow the system to meet the organisations objectives by ensuring that the system as a concept is clearly and suitably defined and is relevant to the organisation. Additional strategies that can be defined at this layer are training and awareness, business continuity planning with incident handling, internal and external audit procedures along with the further development of standards, policies, procedures and guidelines.

4.6.4. Logical Layer - Security Architecture

The logical layer which is considered to be the designer's view where the designer takes the higher level conceptual ideas and converts them into realistic structures that can be implemented in a real world environment. In this layer the designer carries out the systems engineering activities and details the overall system, the sub systems and constituent parts into a logical framework.

> *"The logical security architecture should reflect and represent all of the major security strategies in the conceptual security architecture. At this logical level, everything from the higher layers is transformed into a series of logical abstractions."*[102]

In terms of PKI this layer is concerned with securing the logical representation of the real world business information and specifying all of the policy requirements to protect this information. It is the layer where the security services that PKI provide fit together to establish the logical services that enable the implementation of the PKI system.

4.6.5. Physical Layer - Security Architecture

The Physical Layer, known as the builders' view where the conceptual views of the architect that have been translated into logical design by the designer are interpreted by the builder who turns the logical designs into a physical security architecture and technology model. This layer concerns itself with the:

> *"Development and execution of security rules, practices and procedures, including: cryptographic key management, communication of security parameters between parties, synchronisation between parties; ACLs (Access Control List) maintenance and distribution of ACEs (Access Control Entry), backup management (storing, labelling, indexing, etc), virus pattern search maintenance, event log management and archiving, etc."*[103]

In terms of PKI this is where the security services and mechanisms as described in Section 2 are defined and turned from logical plans into physical assets, this layer

deals with the actual details of the specifications of how the system will be put together and ultimately operate.

4.6.6. Component Layer - Security Architecture

The component layer is the tradesman's view, after the designer has finalised all of the specifications of the system it is necessary to assemble a team of "tradesmen" i.e. all the individuals necessary to build, implement and manage the process, in other words the project team.

Each member of the team will be responsible for their own speciality and are required to ensure that the system is build in accordance with higher layer instructions from the builders and the architects. They are also responsible for compliance with the specifications and any policies, procedures or guidelines to produce the system that complies with the overall plan to build and implement a secure system.

In PKI this could mean that the system is built from scratch or that the designer has decided that architecture that is already in place can be used to implement the system, with the tradesmen customizing the hardware and software that is currently installed within the organisation

4.6.7. Operational Security Architecture

The operational security layer, also known as the facilities management view, encompasses all of the five layers in the security architecture. The facilities manager is the person who is responsible for the day to day operation of the system - one method of managing the system is through an Information Security Management System (ISMS), as defined in ISO/IEC 27001,[104] by using the Plan, Do, Check, Act Cycle (PDCA). The facilities manager can ensure that there is continuity of operations whilst managing the risks and adapting the controls that are put in place that affect the security of the system.

4.7. Conditions – Modelling Outsourcing based on PKI Requirements

This section will look at modelling organisational outsourcing based on the requirements of the PKI within the organisation, it will take a qualitative approach and it will form the basis of the model by being an integral part of the common operating environment between the organisation and the outsource partner.

The specifications are developed by a composite project team consisting of members of both the organisation and the outsource partner but there will also be a strict governance hierarchy in place to oversee the work of the project team both to ensure that the outsource partner can provide the PKI requirements of the organisation, and also that the organisation is meeting its strategic goals and objectives by having the correct implementation of the PKI for their business needs.

4.7.1. Methodology for Qualitative Analysis of Conditions

This section will describe the overall methodological approach used in determining the conditions for outsourcing PKI. Qualitative analysis will be carried out on the following conditions for modelling organisational outsourcing based on the organisation's PKI requirements.

- PKI Core Services
- PKI Enabled Services
- PKI Application Enablers
- PKI Business Drivers
- PKI Supplier Provisions
- PKI Deployment Considerations
- PKI Operational Considerations
- PKI Information Dissemination
- PKI Trust Models

We propose a theoretical model (Figure 15) which will provide organisation's with criteria in order to qualitatively assess each of the above conditions. This model will allow the composite project team from the organisation and outsource provider to determine the ability of the business to meet their goals and objectives with regard to PKI.

Each condition is graded Low, Medium or High with a base score attached to each:

- Low (Base Score 0.0-3.9) – The condition is not required to meet the business goals and objectives.
- Medium (Base Score 4.0-6.9) – The condition is not required but may assist in meeting the business goals and objectives.
- High (Base Score 7.0-10) – The condition is a mandatory requirement in meeting the business goals and objectives.

The composite project team assign the qualitative value for each of the conditions depending on the extent to which:

- The condition adds value to the organisation
- The condition is aligned with the organisations business strategy.
- The condition meets the competencies required by the organisation.
- The condition meets other requirements laid out by the organisation.
- The condition is in cultural alignment with the organisation and the outsource provider.
- The condition provides for continuity of operations
- The condition allows for the organisation to retain management control during periods of change.

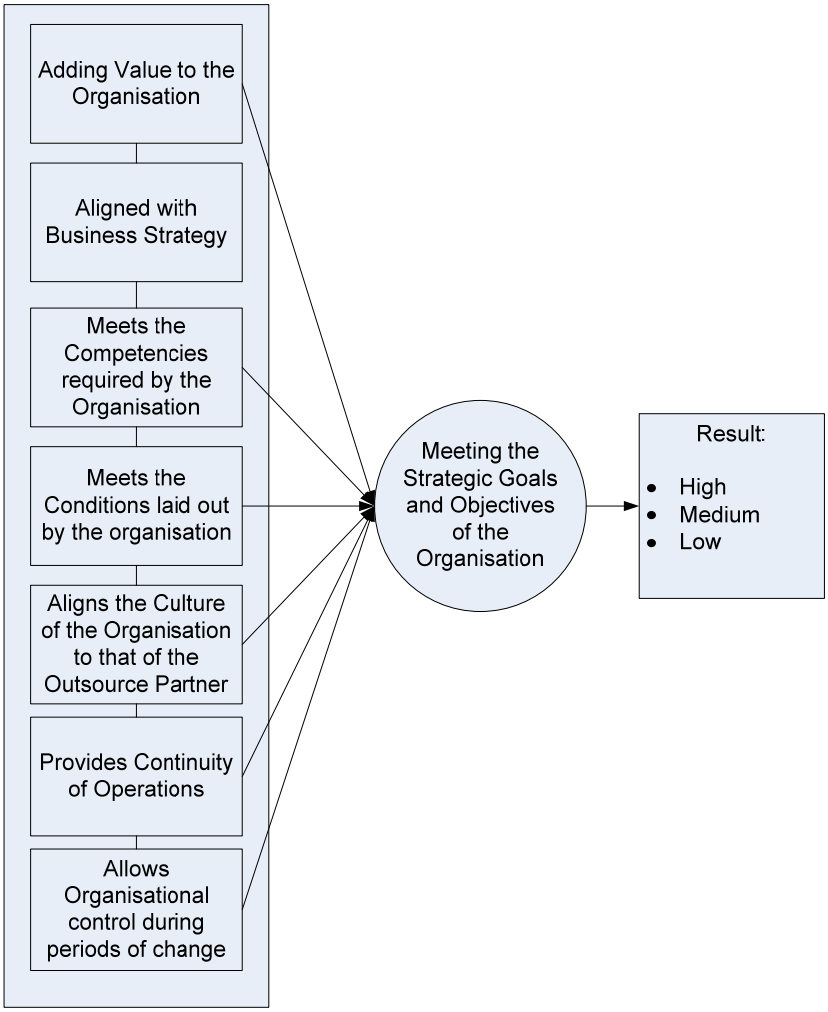


Figure 15: Theoretical Model for Qualitative Assessment

After the initial Low, Medium or High grade has been assigned the capability for each condition is then assigned a base score and the conditions are plotted on a graph (See Figure 16).

This process gives the composite project further detail in which to support the analysis of the most suitable condition in meeting the organisations goals and objectives. Section 4.72 will be used as an example of how the tables are completed. It is beyond the scope of this dissertation to go into the details of the decision making process, it will however, provide the reader with an idea how to complete the tables..

4.7.2. PKI Core Services

PKI is normally associated with three core services: [105]

- Confidentiality
- Integrity
- Authentication

Each of these core services have been defined in Section 2.12 of this document. As mentioned Privacy and Confidentiality are synonymous with each other, confidentiality is the assurance of data privacy. In this case the assurance of data and privacy are methods other than symmetric cryptography such as physical protection etc.

In terms of this model Integrity mechanisms that will give assurance of non-alteration for data considered to be either in transit or storage will encompass cyclic redundancy checks. For integrity mechanisms that utilise public key cryptography, digital signature mechanisms will be used.

Authentication mechanisms previously been explained. In terms of grading entity authentication will be treated as either, mutual and unilateral authentication and the grades awarded in those terms. Data origin, remote, local and single factor authentication are self explanatory and will be treated as single, though bearing in mind that one or more of the authentication mechanisms may be provided within other protocol runs. Multi-factor authentication will take into account that there are many ways in which to prove ones identity, in considering the grading the reader must determine which dual authentication methods they wish to use, for example: [106]

- Something you have. (Smart token)
- Something you know. (Password)
- Something you are. (Biometric)

PKI Core Services	Low	Medium	High
Confidentiality			
Assurance of data Privacy	☐	☐	☒
Symmetric Cryptography	☐	☐	☒
Integrity			
Assurance of Non-Alteration	☐	☐	☒
Digital Signatures	☐	☐	☒
Authentication			
Entity Authentication	☐	☒	☐
Data Origin Authentication	☐	☒	☐
Remote Authentication	☒	☐	☐
Local Authentication	☐	☐	☒
Single Factor Authentication	☒	☐	☐
Multi-Factor Authentication	☐	☐	☒

Table 10: PKI Core Services

Table 10 provides a List of PKI Core Services which provides a score card for the general qualitative value of Low, Medium or High. This is the first step in the modelling process; the grading gives the composite project team the high level overview to assist in the modelling of organisational outsourcing based on the requirements of the PKI. In this example:

- Assurance of data privacy was rated high:
  - The key requirement of the organisation is to maintain the confidentiality of key business information.
- Symmetric cryptography was rated high:
  - It was decided that symmetric cryptography should be used to encrypt the organisations data backups.
- Assurance of Non Alteration was rated high:
  - Integrity Mechanisms such as MAC and HMAC used to ensure integrity of stored data.
- Digital Signatures was rated high:
  - Selected as high to provide the organisation not only with integrity mechanisms but also the provision of non repudiation.
- Entity Authentication was rated medium
  - The organisation operates in a closed environment, with few staff.

- Data Origin Authentication was rated medium
    - The use of digital signatures will provide for most of the data origin authentication requirements.
- Remote Authentication was rated Low
    - As mentioned, the organisation is within a closed environment and there is no requirement for remote authentication.
- Local Authentication was rated high
    - Local authentication is a high requirement as the user has to present his credentials to the local terminal in order to gain access to the system.
- Single Factor Authentication was rated low.
    - The organisation considers this a weak notion of authentication..
- Multi Factor Authentication was rated high
    - The business requires a multi factor authentication to include smart token and password to gain access to the system.

	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change
Confidentiality							
Assurance of Data Privacy	High	High	High	High	High	High	High
Symmetric Cryptography	High	High	High	High	High	High	High
Integrity							
Assurance of Non-Alteration	High	High	High	High	High	High	High
Digital Signatures	Medium	High	High	High	High	Low	Low
Authentication							
Entity Authentication	High	High	High	High	High	High	High
Data Origin Authentication	Medium	Medium	High	High	Medium	High	High
Remote Authentication	Low	Low	Low	Low	Low	High	High
Local Authentication	Medium	Medium	Medium	Medium	Low	Low	High
Single Factor Authentication	Low	Low	Low	Low	Low	Low	Low
Multifactor Authentication	High	High	High	High	High	High	High

Table 11: PKI Core Services - Capability Matrix

The next step is to complete the PKI Core Services Capability Matrix. This is carried out by to assign the qualitative value of Low, Medium or High, to each of the conditions depending on the extent to which they meet the requirements. The grading system is:

- Low – The condition is not required to meet the business goals and objectives.
- Medium – The condition is not required but may assist in meeting the business goals and objectives.
- High – The condition is required to meet the business goals and objectives.

Assurance of Data Privacy	7.5	8.3	7.1	9.3	8.4	7.7	7.7
Symmetric Cryptography	6.6	8.1	9.1	6.3	9.1	8.7	6.3
Assurance of Non-Alteration	7.1	9.8	8.7	7.8	7.2	7.78	8.1
Digital Signatures	6.6	8.1	9.1	8.3	8.6	3.2	2.7
Entity Authentication	7.5	8.3	7.1	9.3	8.4	7.7	7.7
Data Origin Authentication	5.8	6.3	9.1	8.7	6.2	7.1	9.3
Remote Authentication	3.8	2.1	2.7	1.9	3.4	9	8.7
Local Authentication	4.7	6.1	5.3	5.7	0.7	1.1	7.1
Single Factor Authentication	0.3	0.9	1.3	0.8	2.1	3.3	2.7
Multifactor Authentication	7.9	8.4	7.6	9.3	9.4	7.8	8.1
	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change

Table 12: PKI Core Services - Base Score Matrix

Table 12 shows the Base Score Matrix for PKI Core Services. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

Each condition is graded with a Base Score, these are defined as:

- Base Score 0.0-3.9 (Low) – The condition is not required to meet the business goals and objectives.
- Base Score 4.0-6.9 (Medium) – The condition is not required but may assist in meeting the business goals and objectives.
- Base Score 7.0-10 (High) – The condition is required to meet the business goals and objectives.

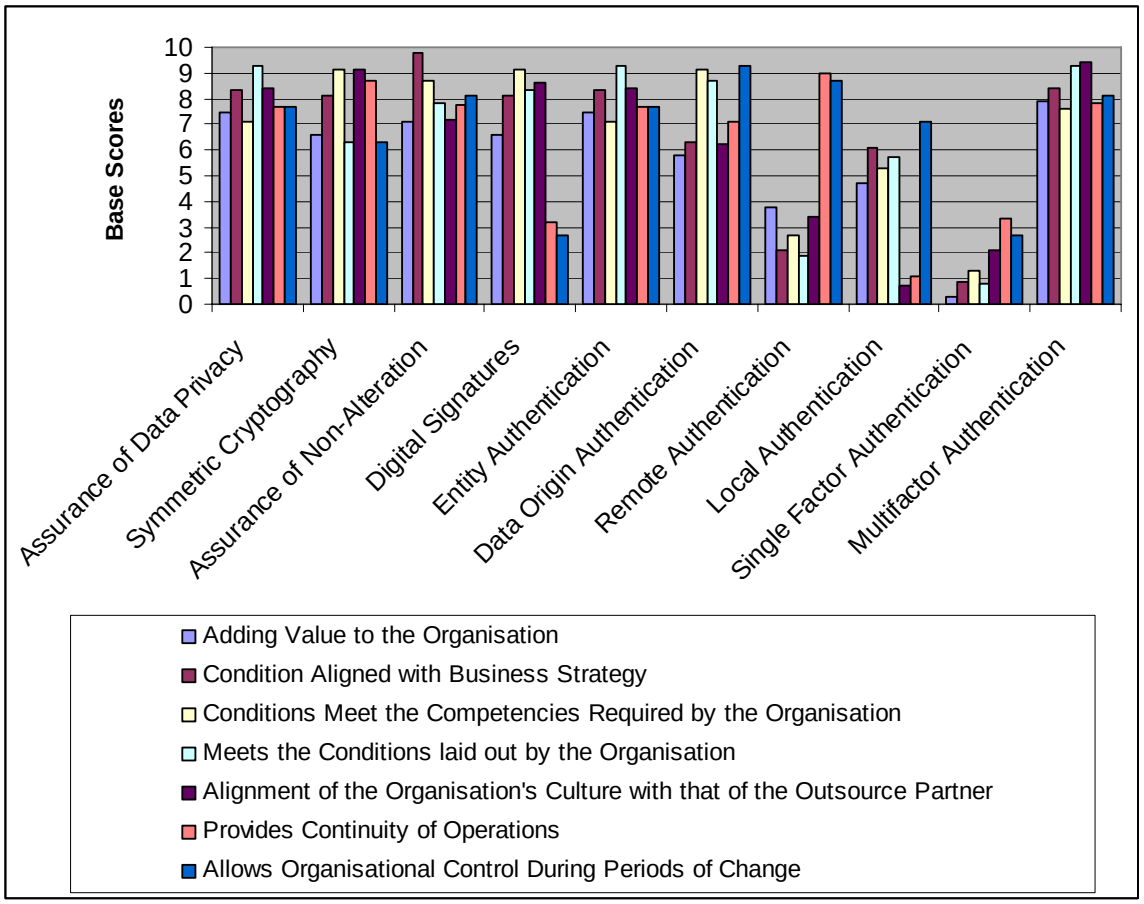


Figure 16: Graphical Representation of Base Scores

Figure 16 is a graphical representation of the base scores assigned by the composite project team. This chart displays the Base Score of each condition in relation to the requirements of the qualitative assessment model (See Figure 15).

4.7.3. PKI Enabled Services

There are ten PKI Enabled Services which are looked at in this section, this is by no means all of the services enabled by PKI but it does provide a broad view of the services available in order to grade each of the conditions. This section will briefly discuss each of the enabled services in turn and give an overview of the security services they provide. (See Table 13)

PKI Enabled Services	Low	Medium	High
Secure E-Mail	☐	☐	☐
Secure Web Servers	☐	☐	☐
IPSec/IKE	☐	☐	☐
Non-Repudiation	☐	☐	☐
Authentication/Authorization	☐	☐	☐
Authorization Authorities	☐	☐	☐
Policy Servers	☐	☐	☐
Attributed Certificates	☐	☐	☐
Trusted Delivery Mechanisms	☐	☐	☐
Secure Protocols	☐	☐	☐

Table 13: PKI Enabled Services

Secure E-Mail within PKI can be provided by S/MIME (Section 2.13.2) which is standardised in the IETF S/MIME working group through a series of RFCs. S/MIME provides the following security services:[107]

- Authentication.
- Message Integrity.
- Non Repudiation of Origin (*When using digital signatures.*)
- Privacy & Data Security using encryption.

The provision of Secure Web Services (Section 2.13.1) in PKI is realised by using SSL/TLS and HTTPS, both protocols require digital signatures to provide the following security services:

- Data Privacy (Confidentiality)
- Data Integrity

IPSec/IKE was designed to provide interoperable and cryptographically based security services for IPv4 and IPv6. IPSec either uses or provides the following security services:

- Data Confidentiality
- Data Integrity
- Data Origin Authentication
- Access Control

Non Repudiation (Section 2.13.5) enabled services provided by PKI include:

- Non repudiation of origin.
- Non repudiation of receipt.
- Non repudiation of creation.
- Non repudiation of delivery.

Policy Servers, Attributed Certificates, Trust Delivery Mechanisms and Secure Protocols are all enabled by a PKI infrastructure those mechanisms provide the support for the security services offered by the PKI enabled services.

Table 15 shows the Base Score Matrix for PKI Enabled Services. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

Secure E-Mail							
Secure Web Servers							
IPSec/IKE							
Non-Repudiation							
Authentication / Authorization							
Authorization Authorities							
Policy Servers							
Attributed Certificates							
Trust Delivery Mechanisms							
Secure Protocols							
	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change

Table 14: PKI Enabled Services - Capability Matrix

4.7.4. PKI Application Enablers

Application enablers provide a user friendly interface to the organisation's information infrastructure. This section details a selection of PKI application enablers and gives brief descriptions of each along with some advantages and disadvantages to assist in the grading of these conditions.

Application Enabler	Low	Medium	High
Secure Sign-On	☐	☐	☐
End User Transparency	☐	☐	☐
Comprehensive Security	☐	☐	☐
Application Layer Proxies	☐	☐	☐

Table 15: PKI Application Enablers

A secure sign on system provides an organisation with a scalable enterprise authentication solution. Authentication information is securely passed between systems that the user has permission to access. The obvious benefit to this is that the user doesn't have to remember numerous passwords for different systems. This takes away the temptation for the employee to put the sticky with the password under their keyboard.

The other benefit is that eavesdroppers on the network will be limited to sniffing the user's LAN. After the initial authentication, secure protocols are used to pass the authentication information to other systems. The main disadvantage is that if an attacker has access to the authentication credentials then they will have access to all of the systems the user is privy to.

End User Transparency means that the user requires no knowledge of the underlying infrastructure. In terms of a PKI solution all of the security services should be hidden from the user. The system should be seen to function seamlessly without the need for the user to interact with the security functionality of the system. There are obvious exceptions to this rule, one being that if the user is required to be presented with any special security information when logging into a system.

Comprehensive Security is the provision of a "pervasive substrate" on which security applications can work together to provide a seamless security solution. This can prove to be difficult to integrate and manage but if successful a comprehensive security infrastructure supported by PKI would be very effective.

Application Layer Proxies are used to protect against malicious attacks, and are widely seen as the best choice when the organisation has allowed access to the internet for its users. The reason it is popular is because application layer proxies are normally used on a limited set of internet protocols such as HTTP, FTP and SMTP.[180] The application layer proxy acts as a relay for application level traffic, when the user wants to access a service, the proxy is alerted and opens a pseudo application for the request. The request is then passed to the gateway and it is either authorized or rejected based on the protocol and policy. The advantage of this proxy is that it can limit the internet activities of users by only allowing a strict set of

protocols which are closely monitored. The disadvantages of the proxies is that it can put a large processing overhead on the system, like all security activities it is a balancing act between security and usability.

Table 16 shows the Base Score Matrix for PKI Application Enablers. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

Secure Sign-On							
End User Transparency							
Comprehensive Security							
Application Layer Proxies							
	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change

Table 16: PKI Application Enablers - Capability Matrix

4.7.5. Outsourced PKI Business Drivers

There are many drivers that have the attributes to be able to describe them as PKI Business Drivers. The analysis of business drivers for PKI is far beyond the scope of this dissertation, though, some common drivers are listed in Table 17. These have been selected as in our view provide a high level overview of the business drivers behind PKI.

Cost savings are described in more detail in Section 3.3. Cost driven reasons for outsourcing PKI include reducing operational costs through superior outsource partner performance and the ability of the partner to provide a lower cost structure. This in turn will turn the fixed costs to the organisation of operating its own PKI, into variable costs, allowing the business to save on the initial start up costs and save on the management of the system.

The interoperability of a PKI system into an organisation is a multi faceted problem comprises of both technical and non-management issues. For PKI systems, sub systems and applications to work together its interfaces must conform to technical standards. As businesses deploy PKI to support their core business processes the organisation has to take into account interoperability with external partners.

Business to business (B2B) applications will require interoperability of PKIs, these may have been implemented on different architectures, work to different policies or use varying cryptographic protocols. Interoperability is an important issue that has to be addressed early in the process of defining the PKI architecture. A strong driver for a business to adopt a PKI is to provide a comprehensive security system. This is the provision of a "pervasive substrate" on which security applications can work together to provide a seamless security solution.

PKI can assist an organisation with emerging business opportunities. As organisations become more security aware the expectation that their business partners provide solid security practices, assurance of good governance and compliance is ever more important. Having a solid PKI in place, either in house or outsourced, can provide an organisation with a sound basis for the pursuit of a comprehensive security solution. This gives prospective clients or business partners the confidence that the organisation takes the security of their information seriously.

Offering Identity Driven Management solutions is becoming more all-encompassing as organisations face the challenge of providing secure user access to systems and applications.[109] Identity Management solutions help in the provision of business issues such as:

- Remote Access
- Secure Sign-on
- Photo ID Card Solutions

A complete Identity Management solution that is trusted by business partners can deliver increased security, reduction in cost and user convenience.

Business Drivers	Low	Medium	High
Cost Savings	☐	☐	☐
Interoperability	☐	☐	☐
Inter-Enterprise	☐	☐	☐
Uniform Solution	☐	☐	☐
Comprehensive Security	☐	☐	☐
Internal Business Transformation	☐	☐	☐
Efficiency	☐	☐	☐
Technology Innovations	☐	☐	☐
Emerging Business Opportunities	☐	☐	☐
Identity Driven Management	☐	☐	☐

Table 17: PKI Business Drivers

Table 18 shows the Base Score Matrix for PKI Business Drivers. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

Cost Savings							
Interoperability							
Inter-Enterprise							
Uniform Solution							
Possibility of achieving full security							
Internal Business Transformation							
Efficiency							
Technology Innovations							
Emerging Business Opportunities							
Identity Management							
	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change

Table 18: PKI Business Drivers - Capability Matrix

4.7.6. PKI Supplier Provisions

The requirement of supplier provisions is a decision that has to be agreed by both the organisation and the outsource partner. Table 19 lists twenty two supplier provisions that the organisation may require the outsource partner to provide, describing in detail all of these provisions is beyond the scope of this dissertation. This list is based on our own opinion and experience, and it is by no means comprehensive.

The outsource partner may well be able to fulfil all of the supplier provisions, but it may not be in the best interest of the organisation to source all of their needs from one supplier. There are other factors to take into account when dealing with suppliers and these will require other areas of the business to get involved such as procurement and legal to ensure that the organisation's governance structure is not compromised and, in the case of cryptographic hardware for example, that all of the legal matters regarding liability etc. are covered before entering into any agreement.

Supplier Provisions	Low	Medium	High
Cryptographic Hardware for Certificate signing	☐	☐	☐
Root Key Protection	☐	☐	☐
User Key Management	☐	☐	☐
Dual Key Support	☐	☐	☐
Key/Certificate Revocation	☐	☐	☐
Ease of Integration	☐	☐	☐
Use of Standard or Proprietary PKI	☐	☐	☐
Directory Technology Used	☐	☐	☐
Database Technology Used	☐	☐	☐
Availability and Scalability	☐	☐	☐
Built in Redundancy	☐	☐	☐
Disaster Recovery	☐	☐	☐
Security Management	☐	☐	☐
Risk Management	☐	☐	☐
Facility Security	☐	☐	☐
Personnel Security	☐	☐	☐
Independent Audit	☐	☐	☐
Non-Repudiation	☐	☐	☐
Dedicated Staff	☐	☐	☐
State of the art skill set	☐	☐	☐
Cross Certification	☐	☐	☐

Table 19: PKI Supplier Provisions

Table 20 shows the Base Score Matrix for PKI Supplier Provisions. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

Cyptographic Hardware for Certificate signing							
Root Key Protection							
User Key Management							
Dual Key Support							
Key/Certificate Revocation							
Ease of Integration							
Use of Standard or Proprietary PKI							
Directory Technology Used							
Database Technology Used							
Availability and Scalability							
Built in Redundancy							
Disaster Recovery							
Security Management							
Risk Management							
Facility Security							
Personnel Security							
Independent Audit							
Non-Repudiation							
Dedicated Staff							
State of the art skill set							
Cross Certification							
	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change

Table 20: PKI Supplier Provisions - Capability Matrix

4.7.7. PKI Deployment Considerations

There are twenty six deployment considerations list in Table 21. As with PKI business drivers this is not a comprehensive list and is solely based on our own opinions and experience. It may be the case that the outsource partner has more experience and is able to provide the expertise required to ensure that the organisation meets it strategic goals and objectives. Table 14 is a sample of some of the deployment considerations, and, as with all of the conditions in this section, it is a qualitative approach that is taken by the composite project team to ensure the correct decisions are made.

Deployment Considerations	Low	Medium	High
Selection of Trust Model	☐	☐	☐
In-House or Outsource	☐	☐	☐
Build or Buy	☐	☐	☐
Closed Vs Open Environment	☐	☐	☐
X.509 Vs Alternative Certificate	☐	☐	☐
Targeted Applications	☐	☐	☐
Comprehensive Solutions	☐	☐	☐
Standard Solutions	☐	☐	☐
Proprietary Solutions	☐	☐	☐
Interoperability Considerations	☐	☐	☐
Peripheral Support	☐	☐	☐
Facility Requirements	☐	☐	☐
Personnel Requirements	☐	☐	☐
Certificate Revocation	☐	☐	☐
End Entity Roaming	☐	☐	☐
Key Recovery	☐	☐	☐
Repository Issues	☐	☐	☐
Disaster Planning and Recovery	☐	☐	☐
Security Assurance	☐	☐	☐
Mitigating Risk	☐	☐	☐
Lack of Industry Accepted Standard	☐	☐	☐
Multi-Vendor Operability	☐	☐	☐
Scalability and Performance	☐	☐	☐
Knowledgeable Personnel	☐	☐	☐
PKI Enabled Applications	☐	☐	☐
Corporate Level Acceptance	☐	☐	☐

Table 21: PKI Deployment Considerations

Table 22 shows the Base Score Matrix for PKI Deployment Considerations. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

Selection of Trust Model							
In-House or Outsource							
Build or Buy							
Closed Vs Open Environment							
X.509 Vs Alternative Certificate							
Targeted Applications							
Comprehensive Solutions							
Standard Solutions							
Proprietary Solutions							
Interoperability Considerations							
Peripheral Support							
Facility Requirements							
Personnel Requirements							
Certificate Revocation							
End Entity Roaming							
Key Recovery							
Repository Issues							
Disaster Planning and Recovery							
Security Assurance							
Mitigating Risk							
Lack of Industry Accepted Standard							
Multi-Vendor Operability							
Scalability and Performance							
	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change

Table 22: PKI Deployment Considerations - Capability Matrix

4.7.8. PKI Operational Considerations

Table 23 lists sixteen PKI operational considerations, as with the previous two sections these considerations are our own opinion, based on our experience and by no means a comprehensive list. Operational considerations map to the physical layer of the SABSA model as the operational considerations are the components of a PKI system that allow it to function. As with all of the conditions it is a qualitative process decided by the composite project team to provide the organisation with the means to support its strategic goals and objectives whilst maintaining the management capability of the system by the organisation.

Operational Considerations	Low	Medium	High
Time Stamp Servers	☐	☐	☐
Notarization Services	☐	☐	☐
Non-Repudiation Services	☐	☐	☐
Revocation Checking	☐	☐	☐
Key Life Cycle Management	☐	☐	☐
Certificate Policy Enforcement	☐	☐	☐
Restricting Network Access	☐	☐	☐
Secure Reinforced Rooms	☐	☐	☐
Installing Proper Access Control	☐	☐	☐
Hardware Security Modules	☐	☐	☐
Smart Cards and Tokens	☐	☐	☐
Biometric Authentication	☐	☐	☐
Multifactor Authentication	☐	☐	☐
Authentication	☐	☐	☐
Compromise of User Key	☐	☐	☐
Disaster Preparation and Recovery	☐	☐	☐

Table 23: PKI Operational Considerations

Table 24 shows the Base Score Matrix for PKI Operational Considerations. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

Time Stamp Servers							
Notarization Services							
Non-Repudiation Services							
Revocation Checking							
Key Life Cycle Management							
Certificate Policy Enforcement							
Restricting Network Access							
Secure Reinforced Rooms							
Installing Proper Access Control							
Hardware Security Modules							
Smart Cards and Tokens							
Biometric Authentication							
Multifactor Authentication							
Authentication							
Compromise of User Key							
Disaster Preparation and Recovery							
	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change

Table 24: PKI Operational Considerations - Capability Matrix

4.7.9. PKI Information Dissemination

PKI Information Dissemination deals with key distribution, directories and directory access. Section 2.7.4 of this document has a detailed description of publication and repository technologies. This section can be seen as a continuation of operational considerations as these are the components that allow PKI to function and the same rules for operational considerations should apply with information dissemination techniques.

Information Dissemination	Low	Medium	High
Hand Delivery	☐	☐	☐
Attached to E-mail	☐	☐	☐
LDAP	☐	☐	☐
X.500 DSA	☐	☐	☐
OCSP Responders	☐	☐	☐
DNS	☐	☐	☐
Web Servers	☐	☐	☐
FTP	☐	☐	☐
Corporate Database	☐	☐	☐
Direct Access Repository	☐	☐	☐
Border Repository	☐	☐	☐
Shared Repository	☐	☐	☐
Inter-domain replication	☐	☐	☐

Table 25: PKI Information Dissemination

Table 26 shows the Base Score Matrix for PKI Information Dissemination. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

Hand Delivery							
Attached to E-mail							
LDAP							
X.500 DSA							
OCSP Responders							
DNS							
Web Servers							
FTP							
Corporate Database							
Direct Access Repository							
Border Repository							
Shared Repository							
Inter-domain replication							
	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change

Table 26: PKI Information Dissemination - Capability Matrix

4.7.10. PKI Trust Models

Employing the correct PKI Trust Models, Section 2.17 provides a detailed description of trust models. Implementing the correct trust model for the organisation and its core business is the key to a successful PKI. Trust models are required in order to build a large scale infrastructure, as it is practically impossible to carry out authentication of an entity without having trust - these models allow trust relationships to be formed between entities that may have had no previous relationship.

The decision of which trust model is selected has to do with the size of the implementation, whether or not the implementation is inter or intra organisational and a whole host of other reasons, but most importantly it has to support the strategic goals and objectives of the organisation.

PKI Trust Models	Low	Medium	High
Strict Hierarchy of Certification	☐	☐	☐
Authorities	☐	☐	☐
Loose Hierarchy of Certification	☐	☐	☐
Certificate Authorities	☐	☐	☐
Policy Based Hierarchies	☐	☐	☐
Distributed Trust Architecture	☐	☐	☐
Four Corner Trust Model	☐	☐	☐
Web Model	☐	☐	☐
User Centric Trust	☐	☐	☐

Table 27: PKI Trust Models

Table 28 shows the Base Score Matrix for PKI Trust Models. This provides a more detailed analysis of the conditions depending on the extent to which they meet the requirements.

	Adding Value to the Organisation	Condition Aligned with Business Strategy	Conditions Meet the Competencies Required by the Organisation	Meets the Conditions laid out by the Organisation	Alignment of the Organisation's Culture with that of the Outsource Partner	Provides Continuity of Operations	Allows Organisational Control During Periods of Change
Strict Hierarchy of Certification							
Authorities							
Loose Hierarchy of Certification							
Certificate Authorities							
Policy Based Hierarchies							
Distributed Trust Architecture							
Four Corner Trust Model							
Web Model							
User Centric Trust							

Table 28: PKI Trust Models - Capability Matrix

4.8. Culture – Aligning Organisations for Strategic Partnership

One of the most important aspects for an organisation in selecting an outsource partner is the culture of both of the organisations which have to be aligned. A corporate culture that is able to adapt encourages employees to work effectively to ensuring the ease transition during periods of change which is necessary for long term growth.

4.8.1. The Seven-S Mode

The Seven-S Model developed by McKinsey & Company in the 1970s was originally developed for comprehensively analyzing the culture and behaviour of organisations. The model is split into two parts the hard S's which are strategy, structure and systems, which are the core business functions of the organisation and are "hard-wired" into the organisation. The second part of the model is the soft S's, the skills, shared values, style and staff, that are more concepts that deal with people in the organisation, how they interact with one another, the skills they posses and the style in which they carry out their tasks. The Seven-S Model is shown in Figure 15.[110]

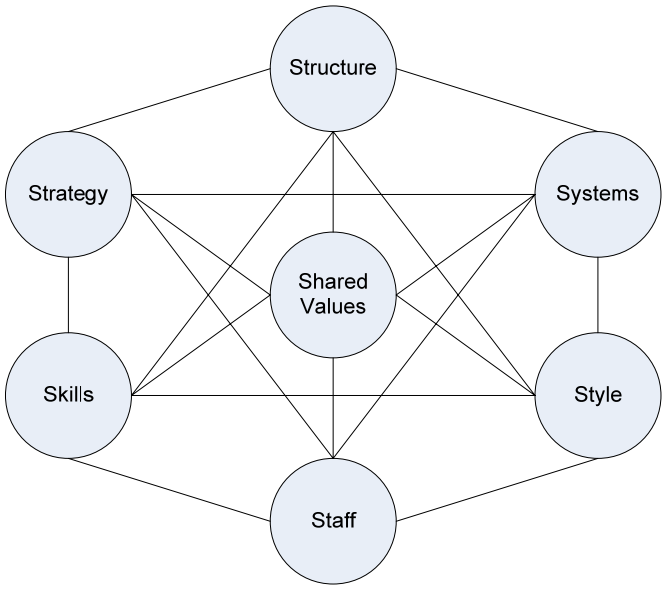


Figure 17: The Seven S Model

4.8.2. Structure

The organisation's structure is normally one of three main models: centralised; decentralised; or, devolved management. The centralized model has a central top down structure where the responsibility lies within the central body of the organisation with activities being centrally controlled to avoid duplication of effort, to provide mutual support and to ensure efficient and economic use of all resources. The devolved model takes away a lot of the control from the central authority and gives the decision making capability to department managers who then report to a senior person in the organisation. This approach gives the managers more control over the management framework and can enable a close alignment of the business needs of the organisation.

The decentralized model takes away the decision making from the central authority completely allowing individual managers to make decisions that effect the organisation directly; this allows the managers to develop their own strategies, policies etc depending on the area of the business, geographic location and any unique circumstances in which they may operate. All of the models have their pros and cons and each effect how the management framework is designed and delivered to the organisation but one of the most important things that all of these models have is they offer is the ability to apply strategic, tactical and operational initiatives depending on the size, culture and operational area of any given organisation when and where it is required.

4.8.3. Strategy

The organisation's strategy is defined as:

> "*The direction and scope of an organisation over the long term: which achieves advantage for the organisation through its configuration of resources within a challenging environment, to meet the needs of the markets and to fulfil stakeholder expectations.*"[111]

Different areas within the organisation will have developed their own strategies. There will be a corporate strategy that governs how the organisation will meet its goals and objectives, which may be driven by stakeholder expectations and, not

necessarily, what is best for the organisation. There is also a business work flow strategy which deals directly, in which the specific business unit operates and defines how the organisation interacts with its customers and providing its customers with the products which will maintain their competitive edge, thus, ensuring the organisations success.

Finally there is the operational strategy, which is the strategy that will ensure that all of the business work flow strategies come together to meet the overall corporate strategy and deals with all of the resource and management issues within the wider organisation.

4.8.4. System

The organisation's system defines the "procedures both formal and informal, by which an organisation operates and gathers information."[112] the system also accounts for existing innovation within the organisation to create a culture of innovation. It is important that the whole system supports it, and this may mean that the culture of the organisation has to change to allow for individual innovation in support of the organisations growth.

4.8.5. Shared Values

The organisation's shared values are the guiding concepts that normally are not part of the goals and objectives of the organisation but are the core ideas on which the organisation was founded. Shared values are fundamental in forming the principles that allow everyone in the organisation to feel as if they are working towards the greater good, gives them a sense of belonging to an organisation which projects from them the ideals of the organisation. Shared values are the foundation blocks of the organisations culture.

4.8.6. Skills

The skills that are present in the organisation's staff are crucial to the success in meeting the goals and objectives of the organisation. Having the right people, with the right skills working on the right projects will provide successful results and having the wrong people will mean failure. Each organisation should focus on its core business as the skills of their staff lie in these areas. This is an important point for outsourcing PKI - one of the main reasons that organisations have to look elsewhere when

designing and implementing a PKI system is that internal staff does not have the specialized skill set required.

4.8.7. Style

The organisation's style is:

> "*The leadership approach of top management and the organisations overall operating approach; also the way in which the organisations employees present themselves to the outside world, to suppliers and customers."*[113]

Every organisation has a different style and to some extent this defines an organisation to its customers and it can be instrumental in gaining new business but more importantly retaining already existing contracts.

4.8.8. Staff

The people who work in an organisation are its single most important asset, without dedicated, intelligent and skilled staff the business will fail. 'Staff' in this context also deals with all of the human resources issues such as recruitment, integration, training and continual career development which will allow the organisation to recruit, train and retain the best people possible to ensure the success of the organisation.

4.9. Continuity – Ensuring Effective Continuity of Operations

> "*Continuity management is the process by which plans are put in place and managed to ensure that IT Services can recover and continues should a serious incident occur. It is not just about reactive measures, but also about proactive measures – reducing the risk of disaster in the first instance."*[114]

Ensuring that the organisation can recover quickly and effectively from any incident is paramount to its continued success - as customers want a continued service without interruptions every minute systems are down money is lost and reputation damaged.

4.9.1. ITIL Service Continuity

The IT Infrastructure Library (ITIL) mission statement for IT Service continuity is to:

> "*Support business continuity management functions by ensuring that IT services can be recovered in the event of a major business disruption within required timescales.*"[115]

The most critical aspect of the mission statement is that the IT services affected are recovered within the agreed timescales. This will have been defined in any contract between the organisation and the outsource provider. ITIL aims to achieve this by covering all of the major business functions of the organisation with IT service continuity plans and ensuring that these plans are thoroughly audited and tested - from this it is possible to determine realistic timescales for recovery. ITIL lists key activities which are described in Table 29 below.[116]

Key Activity	Description
Define the scope of IT Service Continuity Management.	As with ISO/IEC 27001 the scope is defined in terms of the characteristics of the business, the organisation, the location, assets, technology with justifications.
Conduct Business Impact Analysis.	The business impact analysis will show how each part of the business will be affected by an incident and will cover both internal and external events.
Conduct IT Risk Assessment.	The IT Risk assessment will identify the assets within the scope of IT Service Continuity and identify the owners of the assets. It will identify the threats to the assets and the vulnerabilities that may be exploited by those threats, finally it will identify the impact on the assets if an incident occurs.
Define IT Service Continuity Strategy in Line with Business Continuity Strategy	This will involve aligning the IT service continuity which looks at the threats and analysis of the associated vulnerabilities to the Business Continuity Strategy which looks at the impact on the organisations business functions.
Perform IT Service Continuity Organisation and Implementation Planning Activities.	This must be a multi-disciplined approach with both technical and business managers involved to ensure that the all the stakeholders involved are aware of how IT Service Continuity is plan and implemented
Implement Standby Arrangements and Risk Reduction Measures.	The organisation has to have in place standby arrangements this will normally be done by having a contract in place with a standby provider
Develop IT Recovery Plans and	The organisation has to have the plans and

Procedures	procedures in place to ensure that any incident does not result in the organisation not being able to recover within the timescales required.
Perform Testing of IT Recovery Plans and Procedures.	The disaster recovery team must test the continuity plan at regular intervals and use the results of the exercise to improve the existing plans and procedures.
Review and Audit IT Recovery Plans and Procedures.	The organisation has to undertake regular audits and reviews of the IT Recovery plans to ensure that the scope of the IT service continuity management remains adequate and that improvements are identified.
Perform IT Service Continuity Educational Training and Awareness Activities.	It is essential that the organisation has a training and awareness package in place to ensure that all of the staff in the organisation knows their roles and responsibilities in the event of an incident.
Assess Impact of IT Changes on IT Service Continuity Plans and Processes.	Any continuity plan or process has to be compatible with the existing IT infrastructure if the existing structure has to be changed then an impact analysis will have to take place with a change management process following.
Validate Ongoing ability of IT Service Continuity Strategies to Meet Business Requirements.	IT continuity is put in place primarily to ensure that the business meets its strategic goals and objectives. IT continuity management has to be continually reviewed to ensure that it always meets the business requirements of the organisation.
Provide Management Information about IT Service Continuity Management Quality and Operations.	Management have to be kept informed of the activities of the IT Service Continuity team but also have to provide the necessary resources to ensure that the plans and quality of operations are sufficient to overcome any incident that has been planned for.

Table 29: ITIL Key Activities

4.9.2. Incident Management

We have designed two flowcharts for incident management processes. The first is the initial incident management flow process. This deals with the response of the organisation from the initial incident to the resumption of the system back to its normal state.

The second process we have developed in the post incident review procedure. This deals with the review of the procedures taken during the incident and analyses the processes to ensure that they were carried out effectively and that any lessons learnt for the incident can be incorporated into the initial incident flow process.

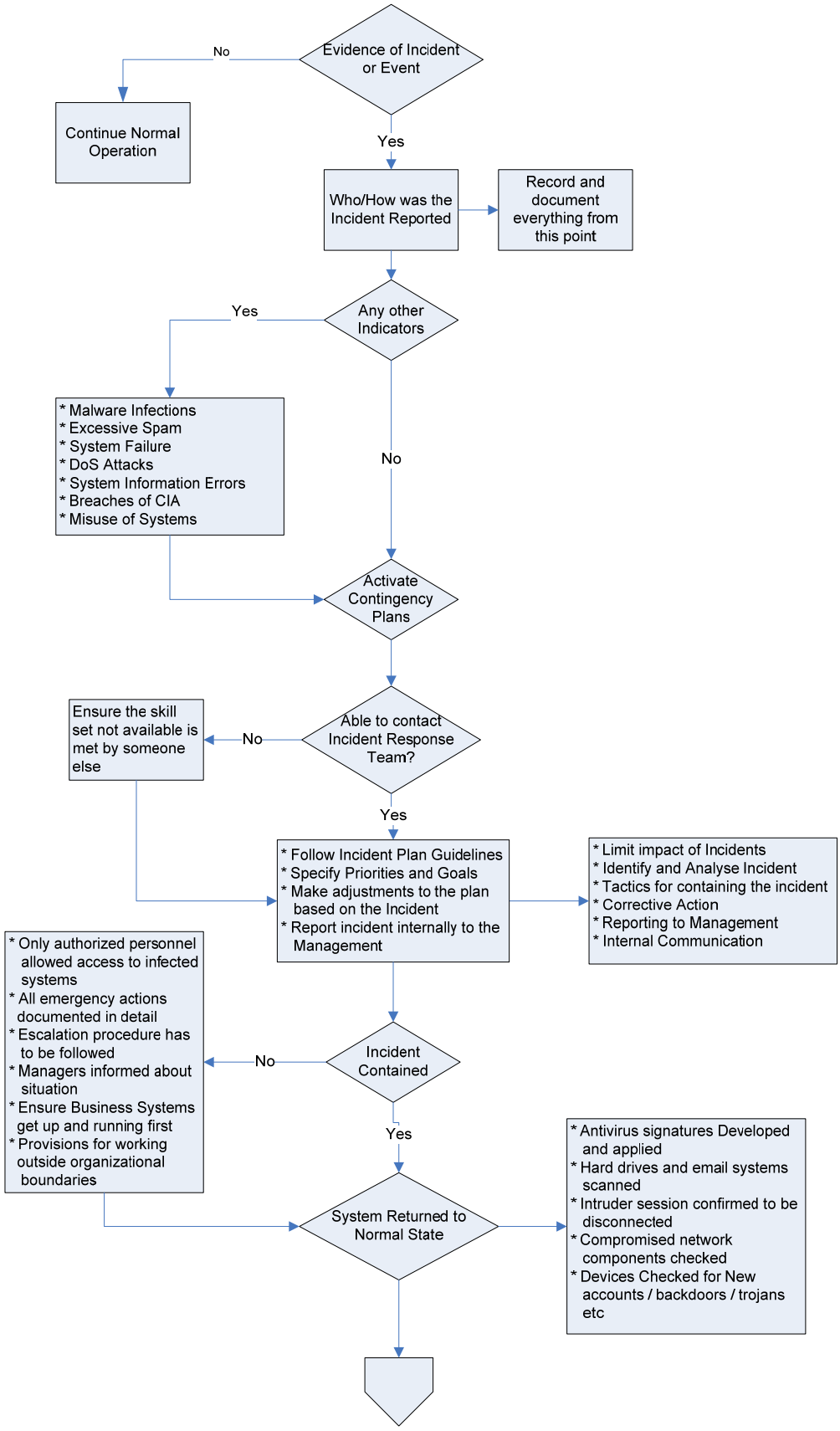


Figure 18: Incident Management - Process Flow

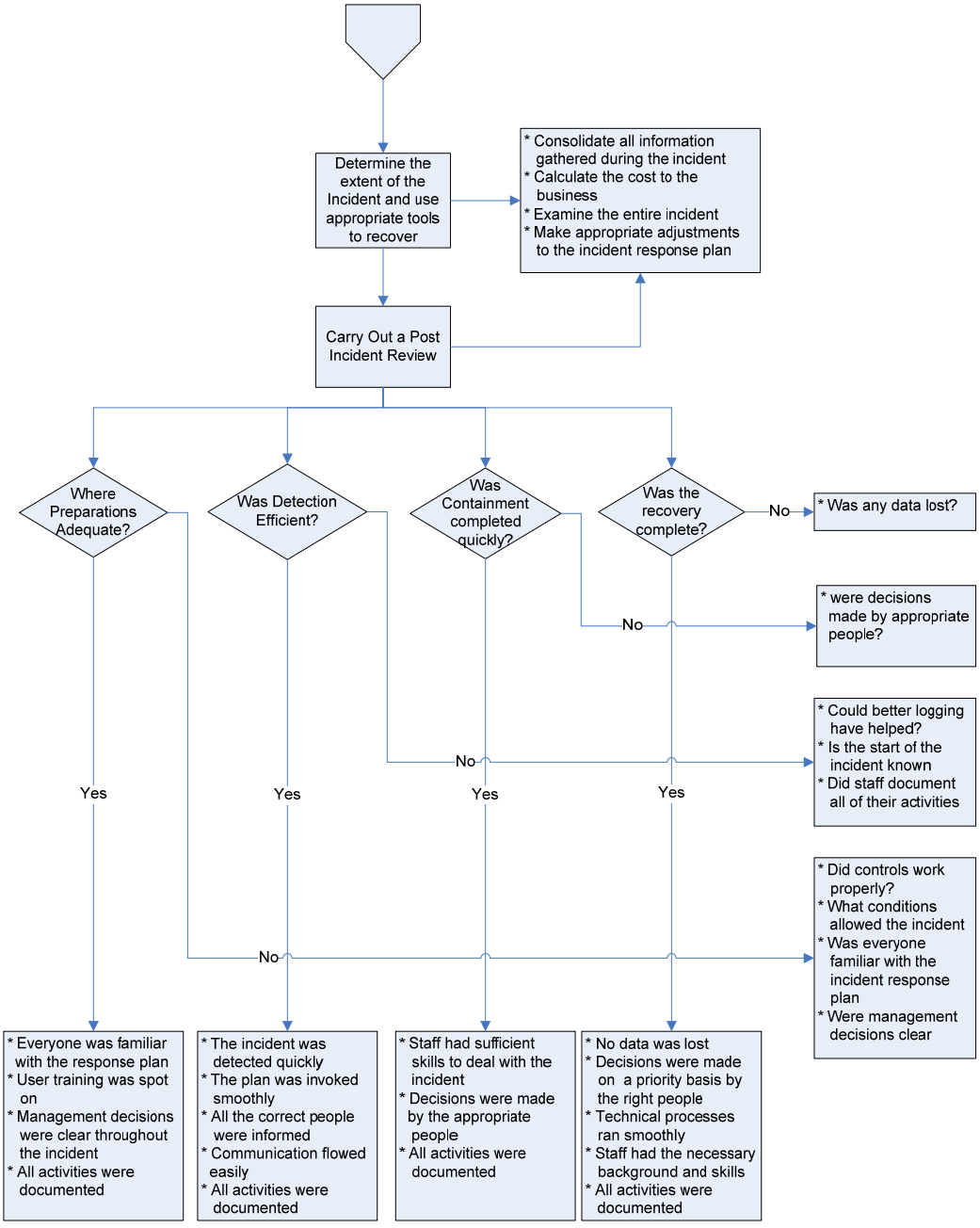


Figure 19: Incident Management - Post Incident Review

4.10. Change Management – Strategy for Technological Change in Outsourcing

Change management activities are an important aspect to outsourcing, too often organisations have entered outsource partnerships and found that they have lost management control this often hinders the organisations ability to adapt to technological change and allow the organisation to continually meet its strategic goals and objectives. Having a change management specialist as part of the project team is essential in:

> "*Recognizing the risks associated with studying and implementing a transformation tool such as outsourcing and in assisting in creating an environment in which such an initiative can be successful.*"[117]

In a PA Consulting Sourcing Interest Groups New York Regional Meeting a framework for outsourcing and outsourced enabled changed was introduced, in the presentation one of the topics discussed was how often change occurs within an organisation.

> "*The statistics are as follow: 89% of organisations make changes to their organisations with 65% changing their business processes, 78% implementing new IT Systems and 14% carrying out other change initiatives, if an organisation outsource key systems and then are unable to manage these systems then the core business of the organisation will suffer, affecting not only profitability but also the organisations reputation.*"[118]

Change Management is a key area where the organisation has to ensure that their selection of a strategic outsource partner allows for change to takes place seamlessly in order to continually meet the organisations goals and objectives. The model the PA Consulting proposed is shown in Figure 18.[119]

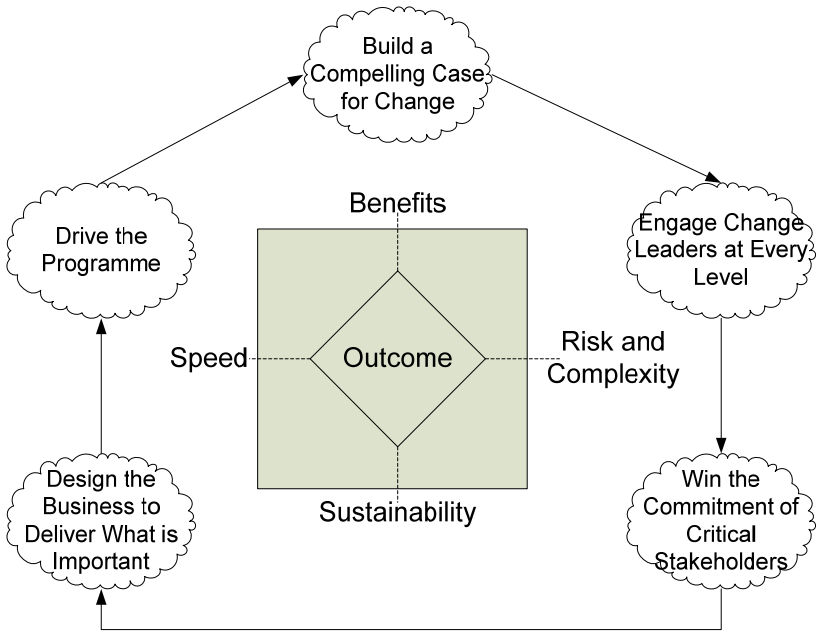


Figure 20: Structured Change Framework

4.11. PKI Outsourced Model – Bringing the Pieces Together

This section aims to bring each aspect of the model together to show the decision making process in a common operating environment shown in Figure 19, and describing how all aspects of this dissertation to combine and form the proposed PKI Outsourcing Model.

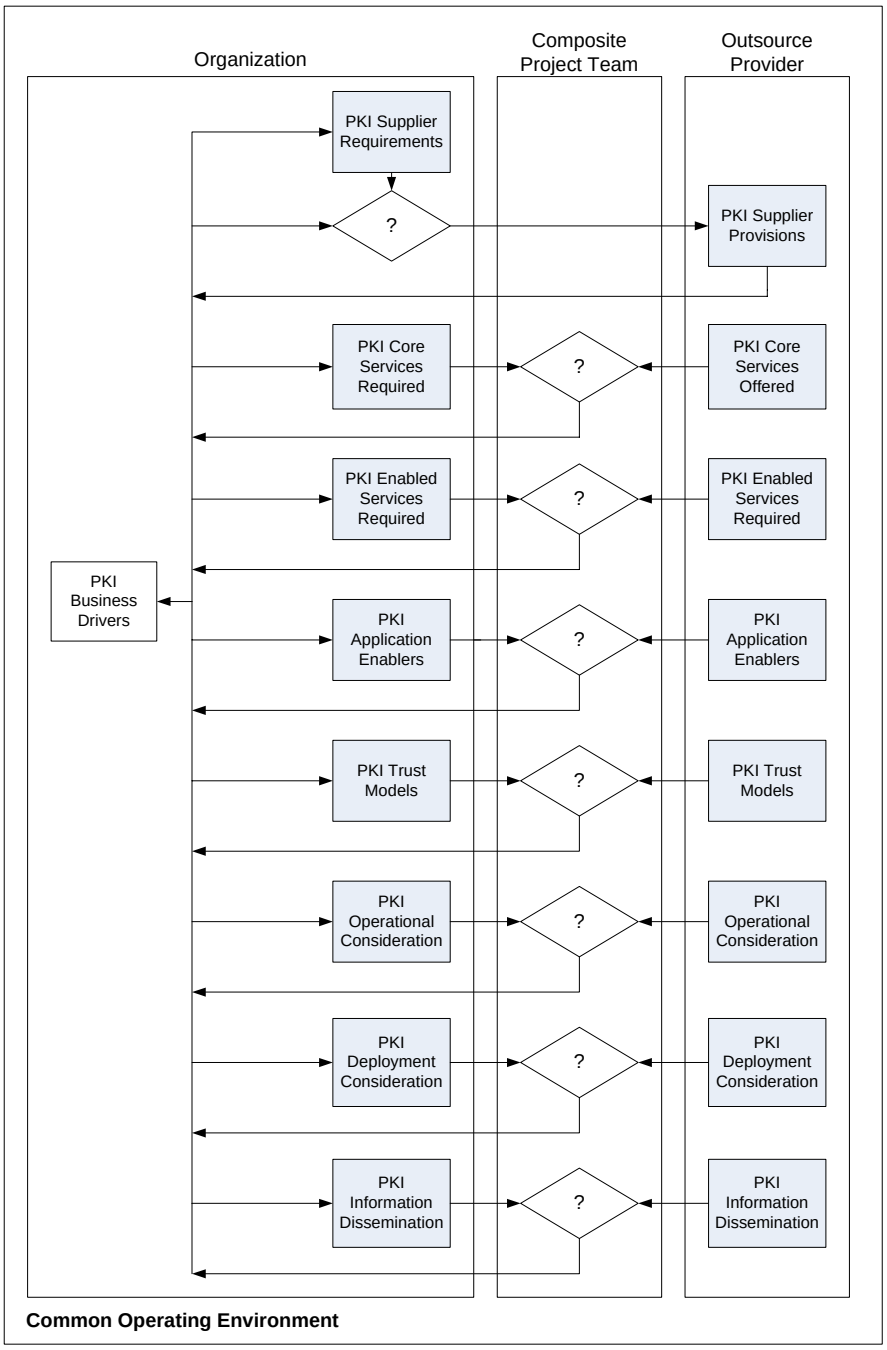


Figure 21: Modelling Organisational Outsourcing: Operating Environment

The common operating environment is built through aligning the organisation's strategic goals and objectives with that of the outsource partner. It has been explained in the dissertation how an outsource partner has to be treated like a TTP. The rules and regulations that surround allowing a TTP access to the organisation's most sensitive information are laid out both in ISO/IEC 17799[120] and ISO/IEC 14516.[121] The trust that is formed between the entities during this process is the basis for the common operating environment. Further to this, the alignment of the culture of both organisations is also extremely important and McKinsey & Companies Seven S Model is an extremely good tool for gauging an organisation's culture and ensuring that both the outsource partner and the organisation have a cultural alignment.

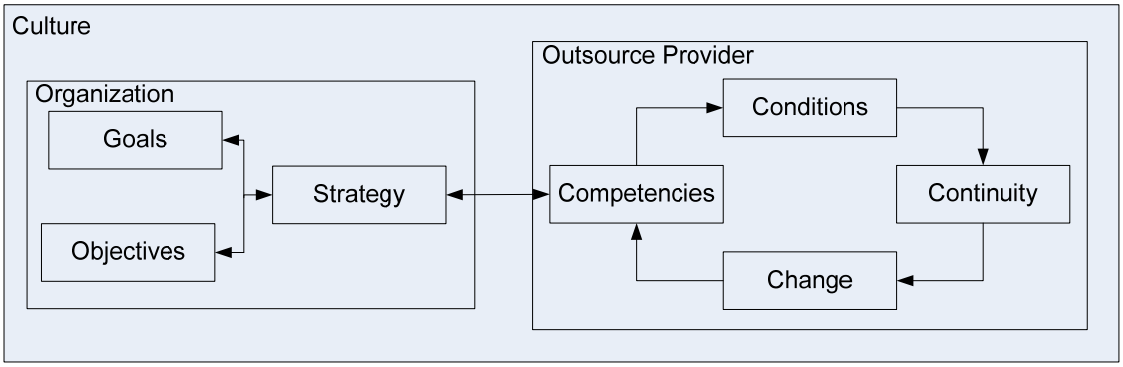


Figure 22: Proposed AB-5C PKI Outsourcing Model

The proposed model brings all of the pieces of the jigsaw together to provide a model that fulfils the strategic goals and objectives of the organisation. The basis of the outsource relationship, as already discussed, is trust and an alignment of cultures between the organisation and the outsource partner. These are long term strategic partnerships and as such it is imperative that there is culture alignment and a solid base of trust between the two parties.

In terms of the organisation the implementation of a PKI has to add value to the organisation, and, as discussed in Section 4.4 of this document, the business goals and objectives that will be supported by a PKI have to be laid out by senior management and using the technology solely because it is available will not support the organisations goals and objectives. The organisation's business strategy and the alignment of any outsourcing activities with the strategic plan have to be thought out carefully. Section 4.5 of this document details the most common views associated

with strategic planning and outlines the importance of having a structure in place that can support the long term plans of the organisation.

It has been mentioned in the previous section about the importance of the common operating environment to ensure an alignment of strategy and culture between the two organisations. The competencies of the outsource provider have to enable the organisation to meet its strategic goals and objectives - in this model the outsource provider has to have a cyclical process of competencies, conditions, continuity and change. A very effective model for measuring the competencies of an outsource provider is to use the SABSA Information Security Architecture to map the requirements of the organisation to the competencies of the outsource provider.

With the SABSA Model the analysis of the business requirements to provide the security architecture are paramount and the operational security architecture provides a process led methodology for the creation of the security architecture. The five main layers of the SABSA model detail the roles and responsibilities within the organisational hierarchy from the business perspective to the facilities management, this model allows the organisation to map competencies against a recognized and widely used model to ensure the outsource provider has the correct competencies to allow the organisation to meet its strategic business goals and objectives.

The conditions that are laid down for successful strategic partnership between the organisation and the outsource partner come from the decisions made by the composite project team. Representatives from both the organisation and the outsource provider make decisions concerning all of the aspects of a PKI design, and its implementation and management. These decisions are based on a qualitative approach with the experience of both parties taken into consideration when developing a system that is feasible, cost effective, what the client wants, what the outsource partner can provide but most importantly that it meets the goals and the objectives of the organisation.

It is imperative that any outsource arrangement has effective continuity management which ensures that plans are put in place to recover services should an incident occur. It would be wise to use an existing, standardised method for doing this as it has been thoroughly tried and tested. ITIL provides a good system to enable organisations to

recover within an acceptable timescale either by countering the incident or using a standby partner to run the services, in the case of PKI this could include backup CAs, TA's or any of the components associated with a PKI system. In association with continuity management is incident management, Figure 16 (Incident Management – Process Flow) and Figure 17 (Incident Management – Post Incident Review) need little explanation as they detail the decision trees for both incident handling and post incident review. Change management is critical in the success of an outsourced PKI implementation, management control is often lost when outsource agreements are signed and this limits the organisations ability meets its strategic goals and objectives in a rapidly changing technological, legal and regulatory environment.

4.12. Summary

In summary, this section introduced the concepts surrounding our new model (AB-5C) for an organisation to outsource PKI. The model looks at ensuring that the organisation adds value to the business and meets the existing goals and objectives of the organisation's long term strategy whilst at the same time aligning outsourcing with the organisation's strategic plan. The competencies for defining enterprise security architecture for an outsourced PKI is discussed and the model chosen was SABSA, essentially a five layer model covering all aspects of a business focussed methodology for operational security architectures.

The conditions for outsourcing PKI are discussed and a qualitative approach taken when looking at all of the different aspects of a PKI implementation, these are fully discussed in Section 4.7 of this document. To define the cultural aspects of selecting an outsource provider the McKinsey Seven S-Model was selected as it was originally developed for the purpose of comprehensively analyzing the culture and behaviour of organisations.

Continuity is explained in terms of the ITIL continuity service management model, this is a widely adopted and accepted method and this section also outlines an incident management process flow along with a post incident review flow. Finally each of the disciplines that have been explained in this section is brought together and the relevance to the model explained.

5. Conclusion

5.1. Introduction

The aim of this section is to provide the reader with a summary of results achieved from this dissertation, an analysis of the relationship of the realistic results, the expected results and how well this dissertation met the stated objectives laid out in the dissertation proposal. To finish off there will be a section detailing further work form\ this dissertation both on the technical, managerial and outsourcing activities associated with PKI.

5.2. Summary of Outcomes

In Section Two a basic PKI infrastructure is defined along with the terminology relating to it with detailed descriptions of each component. There is a description of the cryptographic algorithms, both asymmetric and symmetric involved in a functioning PKI along with the security services that can be provided by these algorithms. There is a comprehensive key management section detailing with standardised models for key management and various methods of key distribution. X.509v3 certificates are described in detail including the certificate policy, certificate practice statements and various methods of certificate revocation, digital signatures are described in a low level of detail to support the certificate section.

In Section Three I have defined the basic principles of Outsourcing. The history of outsourcing is explored to determine why organisations outsource and the various reasons that are used to measure the benefits of outsourcing such as organisationally driven, improvement driven and financially driven reasons. This section looks at governance and management of outsourcing and provides a brief description of both and how they apply to outsourcing.

In Section Four the concepts surrounding the model where introduced and each of the separate disciplines explained individually before being put into context of the model. The key concepts looked at in this section were how does the organisation, by the introduction of an outsourced PKI, add value to the organisation and how does it help the organisation meet their long term strategic aims and objectives. The C’s of the model, culture, competencies, conditions, continuity and change are described in

terms of existing practices and processes that can be easily adopted within organisations if they are not already standard practices. The section finishes with taking the concepts that have been discussed and putting them in the context of the model.

5.3. Relating Outcomes to Original Objectives

The original objectives detailed in the project proposal are listed in Table 19 below.

Main Objective	Sub-Objective
Introduce the Principles Behind PKI	Define the Basic Principles of PKI
	Define the Terms Associated with PKI
Introduce the Principles Behind Outsourcing	Define the Basic Principles of Outsourcing
	Define the Terms Associated with Outsourcing
Managerial Aspects of Outsourcing PKI	Determine the Business Drivers for Outsourcing PKI
	Trusting PKI Outsource Partners
	Address the Managerial PKI Deployment Considerations Respect to Outsourcing
	Address Associated Management Problems in terms of an Outsourced PKI Infrastructure
Technical Aspects of Outsourcing PKI	Understanding the Technical Issues and Complexities of Outsourcing PKI
	Determine the Technical Drivers for Outsourcing PKI
	Determine the Core Services PKI offer and which can be Outsourced
	Address the Technical PKI Deployment Considerations in Respect to Outsourcing
	Determine the Enabled Services PKI Offer and which can be Outsourced

Table 30: Project Proposal Statement of Objectives

The dissertation has clearly met all of the outcomes of the original objectives set out in the project proposal there is a comprehensive introductory section to PKI with detailed descriptions from the history and the fundamental principles to the terminology, technologies, technical and managerial aspects of PKI. In Section 3 there is an introduction to the principles behind outsourcing which details the history of

outsourcing to the modern day theory of multi-sourcing as well as defining basic principles of outsourcing and the definition of the terms associated with outsourcing. Section 4 is the proposed model for outsourcing PKI this section brought together all of the disciplines described in the previous sections of the dissertation and focused on the managerial and technical aspects of PKI.

For the managerial aspects of PKI the outcomes met the objectives because the dissertation covers the objectives mentioned in the project proposal such as determining the business drivers for outsourcing PKI, building trust in outsource partners, addressing deployment considerations and outlining potential management problems associated with PKI. The outcomes for the technical aspects mentioned met the objectives be detailing technical issues that can arise, determining technical drivers, and deployment considerations along with determining core and enabled PKI services.

5.4. Critique - Where the Outcomes as Expected?

The outcomes were as expected I had planned for the descriptions of PKI and Outsourcing would provide the reader with an insight into both disciplines though I thought there would be less detail than was actually presented. I expected the PKI section to be comprehensive but had to limit the depth of the technical information in this section. I expected the Outsourcing section to provide me with the most difficulty because of my relative inexperience in this area but the outcome of this section in meeting the objectives I have laid down in the project proposal was as I had anticipated and from this the reader gains enough information to understand this section and how it fits in with the overall theme of the dissertation.

The final model wasn’t as anticipated, initially I aimed to produce a unique model but as my research progressed it became obvious that for the model to be accepted existing processes and procedures had to be incorporated that is why I looked at the SABSA Operational Architecture Model, the Seven S-Model, ITIL Service Continuity and the PA Consulting Change Management Model, all of these models are already being used and can provide strong support for an Outsourced PKI Model.

5.5. Future Work from this Dissertation

There is an enormous amount of future work to come out of this dissertation, as PKI becomes more accepted as people become more aware of the technology and the business benefits it can bring to an organisation the fear of the unknown will evaporate and PKI will be seen as a business enabler. To that end future work can involve looking at ways in which PKI technology will be used, it can already be found supporting identity and access management systems the question has to be asked is how far organisations will want to go in allowing an outsource provider access to even more sensitive corporate information.

For each of the sections, Introduction to PKI, Introduction to Outsourcing and the Proposed Model there is a vast amount of work that can be pursued, the model can be refined and the management processes investigated in greater detail, every aspect of the technology can be refined to meet the organisations strategic aims and objectives. Most importantly the model can be applied to theoretical or even existing case studies to see if its implementation would be effective.

Bibliography

[1] M. Loney. Baltimore's death spells gloom for PKI. ZDNet UK. 2003. Found at. http://news.zdnet.co.uk/security/0,1000000189,39118180,00.htm

[2] EEMA UK Regional Interest Group meeting 2007: The management and application of PKI in corporate environments. Found at http://www.eema.org/index.cfm?fuseaction=events.content&cmid=337

[3] S. Bijnens. Why PKI is getting a second chance. Leuven Security Excellence Consortium. IT Security Congress. Found at. http://www.l-sec.be/calit.htm

[4] B. Schneir & C. Ellison. Computer Security Journal, v 16, n 1, 2000, pp. 1-7 Ten Risks of PKI: What you're not being told about Public Key Infrastructure. Found at. http://www.schneier.com/paper-pki.html

[5] OUT-LAW News. B2B e-commerce to reach $8.5 trillion in 2005. Found at. http://www.out-law.com/page-1470

[6] D. Bradbury 2004: ID fraud preys on technology's immaturity. Found at http://www.vnunet.com/computing/features/2072364/id-fraud-preys-technology-immaturity

[7] J. Fenn & A. Linden 2005: Gartner's Hype Cycle Special Report for 2005. Found at http://www.gartner.com/DisplayDocument?doc_cd=130115

[8] Whittfield Diffie & Martie E. Hellman, 1976: New Directions in Cryptography. Found at http://crypto.csail.mit.edu/classes/6.857/papers/diffie-hellman.pdf

[9] Understanding Hype Cycles. Found at http://www.gartner.com/pages/story.php.id.8795.s.8.jsp

[10] Public key Cryptography (PKC) History. Found at http://www.livinginternet.com/i/is_crypt_pkc_inv.htm

[11] D. R Khun, V. C. Hu, W.T Polk & S Chang: NIST SP800-32 – Introduction to Public Key Technology and Federal PKI Infrastructure. 2001. (p. 9). Found at http://csrc.nist.gov/pki/publickey.html

[12] Federal Information Processing Standards Publication 180-2 - Secure Hash Standard. 2002. Found at http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[13] Whittfield Diffie & Martie E. Hellman, 1976: New Directions in Cryptography. Found at http://crypto.csail.mit.edu/classes/6.857/papers/diffie-hellman.pdf

[14] A. J. Menezes, P.C. Van Oorschot & S. A. Vanstone. Handbook of Applied Cryptography. CRC: CRC Press LLC. 1997 (p. 285-286)

[15] A. J. Menezes, P.C. Van Oorschot & S. A. Vanstone. Handbook of Applied Cryptography. CRC: CRC Press LLC. 1997 (p. 89)

[16] Loren M. Kohnfelder: Bachelor of Science Thesis at MIT entitled “Towards a Practical Key Cryptosystem: 1978. Found at http://theory.csail.mit.edu/~cis/theses/kohnfelder-bs.pdf

[17] Loren M. Kohnfelder: Bachelor of Science Thesis at MIT entitled “Towards a Practical Key Cryptosystem: 1978. Found at http://theory.csail.mit.edu/~cis/theses/kohnfelder-bs.pdf

[18] What is X.509? Found at http://www.tech-faq.com/x.509.shtml

[19] R. Housley, W. Ford, W. Polk & D. Solo. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999. Found at http://www.ietf.org/rfc/rfc2459.txt

[20] R. Housley, W. Ford, W. Polk & D. Solo. RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999. Found at http://www.ietf.org/rfc/rfc2459.txt

[21] A. Dent & C. J. Mitchell. Users Guide to Cryptography and Standards. Artech House. 2004. (p. 268)

[22] C. Adams & S. Lloyd. Understanding PKI (Concepts, Standards and Deployment Considerations, Second Edition. Addison-Wesley. 2005. (p. 133)

[23] M. E. Whitman & H. J. Mattord. Principles of Information Security. Second Edition. Thomson Course Technology. 2005. (p. 369)

[24] PKI Model, Hong Kong University of Science and Technology. 2004. Found at http://www.ust.hk/itsc/pki/model/index.html

[25] R. Housley, W. Ford, W. Polk & D. Solo. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999. Found at http://www.ietf.org/rfc/rfc2459.txt

[26] R. Housley & T. Polk. Planning for PKI, Best Practices Guide for Deploying Public Key Infrastructure. Wiley Computer Publishing. John Wiley & Sons Inc. 2001 (p. 126)

[27] C. Adams & S. Lloyd. Understanding PKI (Concepts, Standards and Deployment Considerations, Second Edition. Addison-Wesley. 2005. (p. 162)

[28] S. Boeyen, T. Howes & P. Richard. IETF RFC 2587: Internet X.509 Public Key Infrastructure LDAPv2 Schema. 1999. Found at http://www.ietf.org/rfc/rfc2587.txt

[29] R. Housley, W. Ford, W. Polk & D. Solo. RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999. Found at http://www.ietf.org/rfc/rfc2459.txt

[30] A. J. Menezes, P.C. Van Oorschot & S. A. Vanstone. Handbook of Applied Cryptography. CRC: CRC Press LLC. 1997 (p. 386)

[31] A. Dent & C. J. Mitchell. Users Guide to Cryptography and Standards. Artech House. 2004. (p. 23)

[32] A. J. Menezes, P.C. Van Oorschot & S. A. Vanstone. Handbook of Applied Cryptography. CRC: CRC Press LLC. 1997 (p. 361)

[33] A. J. Menezes, P.C. Van Oorschot & S. A. Vanstone. Handbook of Applied Cryptography. CRC: CRC Press LLC. 1997 (p. 4)

[34] E. Rescorla. SSL and TLS, Designing and Building Secure Systems. Addison-Wesley. 2005. (p. 44)

[35] T. Dierks & C. Allen. RFC 2246. The TLS Protocol, Version 1.0. 1999. Found at http://www.faqs.org/rfcs/rfc2246.html

[36] E. Rescorla. SSL and TLS, Designing and Building Secure Systems. Addison-Wesley. 2005. (p. 305)

[37] C. Ramsdell (ed.). RFC 2633. S/MIME Version 3 Message Specification. 1999. Found at http://www.ietf.org/rfc/rfc2633.txt

[38] S. Bradner. RFC 2119: Key words for use in RFC's to indicate requirement levels. 1999. Found at http://www.ietf.org/rfc/rfc2119.txt

[39] S. Kent & R. Atkinson. RFC 2401: Security Architecture for the Internet Protocol. 1998. Found at http://tools.ietf.org/html/rfc2401

[40] J. Reavis. Is VPN the killer application for PKI. Network World on Security. 1999. Found at http://www.networkworld.com/newsletters/sec/0920sec2.html

[41] G. Ou. Wireless LAN Security Guide. 2005. Found at http://www.lanarchitect.net/Articles/Wireless/SecurityRating/

[42] Certicom. Complete WAP Security. 2000.Found at www.comms.scitech.susx.ac.uk/fft/networking/WAPsec.pdf

[43] C. Adams, P Cain, D Pinka & R. Zuccherato. RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). 2001. Found at http://www.ietf.org/rfc/rfc3161.txt

[44] R. Shirey. RFC 2828: Internet Security Glossary. 2000. Found at http://www.faqs.org/rfcs/rfc2828.html

[45] C. R. Merill, McCartner & English. What PKI Does, The Killer Apps. 2000. Found at http://www.pkilaw.com/nonrepud_2.htm

[46] ISO/IEC 17799:2005. Information technology Security techniques: Code of practice for information security management. 2005.

[47] S. Chokhani & W. Ford. RFC 2527: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework. 1999. Found at http://www.faqs.org/rfcs/rfc2527.html

[48] R. Housley, W. Ford, W. Polk & D. Solo. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999. Found at http://www.ietf.org/rfc/rfc2459.txt

[49] S. Chokhani & W. Ford. RFC 2527: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework. 1999. Found at http://www.faqs.org/rfcs/rfc2527.html

[50] S. Chokhani & W. Ford. RFC 2527: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework. 1999. Found at http://www.faqs.org/rfcs/rfc2527.html

[51] R. Housley, W. Ford, W. Polk & D. Solo. RFC 2459: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile. 1999. Found at http://www.faqs.org/rfcs/rfc2459.html

[52] M. Myers, R. Ankney, A. Malpani, S. Galperin & C. Adams. RFC 2560: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol (OCSP). 1999. Found at http://www.faqs.org/rfcs/rfc2560.html

[53] S. Chokhani & W.Ford: RFC 2527 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. 1999. Found at http://www.ietf.org/rfc/rfc2527.txt

[54] S. Kent. RFC 1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate Based Key Management. 1993. Found at http://www.faqs.org/rfcs/rfc1422.html

[55] R. Housley, W. Ford, W. Polk & D. Solo. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999. Found at http://www.ietf.org/rfc/rfc2459.txt

[56] ISO/IEC 14516:2002. Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services

[57] ISO/IEC 17799:2005. Information technology Security techniques: Code of practice for information security management. 2005.

[58] About tScheme. 2005. Found at http://www.tscheme.org/about/index.html

[59] Electronic Communications Act 2000. Found at http://www.opsi.gov.uk/Acts/acts2000/20000007.htm#1

[60] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Found at. http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=en

[61] Merriam-Webster Dictionary. Found at http://mw1.merriamwebster.com/dictionary/outsourcing

[62] Dr. R. Handfield. Current Trends in Production Labour Sourcing. Supply Chain Resource Co-operative. 2006. Found at http://scm.ncsu.edu/public/facts/facs060531.html

[63] K. Tinselboer. University of Twente. The present and future of outsourcing: theory meets practice. Found at. http://referaat.ewi.utwente.nl/documents/2005_03_D-INFORMATION_SYSTEMS_MANAGEMENT/2005_03_D_Tinselboer,K.J.-The_present_and_future_of_outsourcing_theory_meets_practice.pdf

[64] Manchester University. School of Environmental Management. Making the connections: Global Production Networks in Europe and East Asia. Found at http://www.sed.manchester.ac.uk/geography/research/gpn/

[65] Logicaster. E-business and Outsourcing: How This Happened and Growth Period. Found at http://www.logicaster.com/growth_period.html

[66] M. Burke. Europe sees a 78% increase in new outsourcing deals. Found at. http://www.cio.co.uk/concern/budgets/news/index.cfm?articleid=1651

[67] Quoquam Technologies Inc. Outsourcing: A Business Perspective. (p. 4) Found at www.quoquam.com/onsite.pdf

[68] M. F. Greaver II. Strategic Outsourcing: A structured Approach to Outsourcing Decisions and Initiatives. AMACOM. 1998. (p. 4-5)

[68] Business Systems Group. Managed Services Breakfast Briefing – transform your IT department into a strategic asset. Found at http://www.bsg.co.uk/newsevents/events/managed_services_briefings/default.aspx

[69] J. Allen, D.Gabbard, C. May. Outsourcing Managed Security Services. Software Engineering Institute. 2003. Found at. http://www.sei.cmu.edu/publications/documents/sims/sim012.html

[70] ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems – Requirements.

[71] Verisign. 10 Reasons to Outsource MSS. Found at. http://www.verisign.co.uk/managed-security-services/enterprise-security-info/why-security-consulting/index.html

[72] F. Seindeldin. Openware. Managed Security Services - A New Trend. 2007. Found at. http://www.openware.biz/news.cgi?accion=imprimir&agrp=A&skin=Casos_en&id=194

[73] ISO/IEC 21827: Information Technology – System Security Engineering – Capability Model.

[74] ISO/IEC 21827: Information Technology – System Security Engineering – Capability Model.

[75] ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management System – Requirements.

[76] ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management System – Requirements.

[77] J. Linn & M. Branchaud. An Examination of Asserted PKI Issues and Proposed Alternatives. 2004. Found at. http://middleware.internet2.edu/pki04/proceedings/issues_alternatives.pdf

[78] ISO/IEC 15408. Information Technology – Security Techniques – Evaluation for IT Security

[79] ITSEC. Found at. http://www.iwar.org.uk/comsec/resources/standards/itsec.htm

[80] US Federal Criteria. Found at. http://csrc.nist.gov/nistgen/fcscope.txt

[81] ISO/IEC 15408. Information Technology – Security Techniques – Evaluation for IT Security – Part 3 – Assurance Requirements.

[82] A. Calder & S. Watkins. IT Governance: A Managers Guide to Data Security and BS7799 / ISO17799.3rd Ed. Kogan Page. 2005. (p. 3)

[83] M. F. Geaver II. Strategic Outsourcing: A structured Approach to Outsourcing Decisions and Initiatives. AMACOM. 1998. (p. 269)

[84] K. J. Higgins. Outsourcing PKI is an Option to Building One. Information Week. Found at. http://www.informationweek.com/811/pki.htm

[85] Globalsign. Enterprise Solutions. Found at. http://uk.globalsign.com/pki/corporatera.htm

[86] B. Tesler. Outsourcing IT Development: Advantages and Disadvantages. Found at www.webspacestation.com

[87] The DST View of PKI. Discussion of the outsourcing of PKI to Digital Signature Trust Co. Found at. http://connect.educause.edu/library/abstract/TheDSTviewofPKI/42839

[88] S. Wilson. Rethinking PKI. SC Magazine. 2003. Found at. http://www.scmagazine.com/asia/news/article/419737/rethinking-pki/

[89] Australian Government, NEAC, Legal Liability in E-Transactions. 2000. Found at. www.claytonutz.com/downloads/tip0008_7.pdf

[90] S. Wilson. A Vulnerability Assessment of Roaming Soft Certificate PKI Solutions. 2002. Found at. www.sans.org/reading_room/whitepapers/vpns/763.php

[91] L. Cohen & A. Young. Multisourcing: Moving beyond Outsourcing to Achieve Growth and Agility. Harvard Business School Press. 2006. (p. 1)

[92] Gartner. Stop Outsourcing, Start Multi-sourcing. 2005. Found at www.out-law.com

[93] SABSA Overview. Found at www.sabsa-institute.org/the-sabsa-method/sabsa-overview.aspx

[94] The Seven S's: Framework for Analyzing and Improving Organisations. Found at http://www.1000ventures.com/business_guide/mgmt_inex_7s.html

[95] Continuity Management. ITIL & ITSM World. Found at http://www.itil-itsm-world.com/itil-8.htm

[96] PA Consulting. Sourcing Interest Groups New York Regional Meeting. 2005. Found at http://sourcinginterests.org/regional%20presentations/2005newyork/delivering%change%20%through%20%sourcing%20%by%20pa%20consulting%20-%20ny%20v2.pdf

[97] G. A. Steiner. Strategic Planning – What Every Manager Must Know. Free Press Paperbacks. Simon & Schuster. 1997. (p. 13-15)

[98] The Zachman Framework. Found at www.zifa.com

[99] SABSA Overview. Found at www.sabsa-institute.org/the-sabsa-method/sabsa-overview.aspx

[100] J. Sherwood, A. Clark & D. Lynas. Enterprise Security Architecture: A Business Driven Approach. CMP Books. 2005. (p. 34)

[101] J. Sherwood, A. Clark & D. Lynas. Enterprise Security Architecture: A Business Driven Approach. CMP Books. 2005. (p. 41)

[102] J. Sherwood, A. Clark & D. Lynas. Enterprise Security Architecture: A Business Driven Approach. CMP Books. 2005. (p. 38)

[103] J. Sherwood, A. Clark & D. Lynas. Enterprise Security Architecture: A Business Driven Approach. CMP Books. 2005. (p. 38-39)

[104] ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems – Requirements.

[105] C. Adams & S. Lloyd. Understanding PKI (Concepts, Standards and Deployment Considerations, Second Edition. Addison-Wesley. 2005. (p. 37-43)

[106] J. Conroy-McNelley. Multi-Factor Authentication: The Next Generation Solution. Found at. http://www.bankersonline.com/vendor_guru/pps/pps_multi.html

[107] P. Hoffman. RFC 2634. Enhanced Security Services for S/MIME. 1999. Found at. http://www.ietf.org/rfc/rfc2634.txt

[108] Application Level Proxies. Found at. http://winwww.rutgers.edu/~pravin/presentations/splice-talk/Splice-Talkl4.htm

[109] Identity Management, Verisign, Found at http://www.verisign.com.au/idmanagement/

[110] The Seven S's: Framework for Analyzing and Improving Organisations. Found at http://www.1000ventures.com/business_guide/mgmt_inex_7s.html

[111] The Seven S's: Framework for Analyzing and Improving Organisations. Found at http://www.1000ventures.com/business_guide/mgmt_inex_7s.html

[112] Strategy – What is Strategy? Found at http://www.tutor2u.net/business/strategy/what_is_strategy.htm

[113] S. Silbiger. The 10-Day MBA: A Step by Step Guide to Mastering the Skills Taught in the Top Business Schools. Piatkus. 2006. (p. 326-329)

[114] The Seven S Model: A Managerial Tool for Analyzing and Improving Organisations. Found at. http://www.1000ventures.com/business_guide/mgmt_inex_7s.html

[115] Continuity Management. ITIL & ITSM World. Found at http://www.itil-itsm-world.com/itil-8.htm

[116] Continuity Management. ITIL & ITSM World. Found at http://www.itil-itsm-world.com/itil-8.htm

[117] Open Guide. IT Service Continuity Management: Continuity Management / Disaster Recovery / Business Continuity. Found at http://www.itlibrary.org/index.php?page=IT_Service_Continuity Management

[118] PA Consulting. Sourcing Interest Groups New York Regional Meeting. 2005. Found at http://sourcinginterests.org/regional%20presentations/2005newyork/delivering%change%20%through%20%sourcing%20%by%20pa%20consulting%20-%20ny%20v2.pdf

[119] PA Consulting. Sourcing Interest Groups New York Regional Meeting. 2005. Found at http://sourcinginterests.org/regional%20presentations/2005newyork/delivering%change%20%through%20%sourcing%20%by%20pa%20consulting%20-%20ny%20v2.pdf

[120] ISO/IEC 17799:2005. Information technology - Security technique - Code of practice for information security management

[121] ISO/IEC 14516:2002. Information technology - Security techniques. Guidelines for the use and management of trusted third party services

Appendices

Appendix A: Critique of Existing Models used in Section 4

System Security Engineering – Capability Model - ISO/IEC 21827		
Advantages	International Standard	• Established by consensus • Approved by a recognized body • Provides for common and repeated use of rules, guidance or characteristics of activities and their results. • Aimed at the achievement of the optimum degree of order in a given context
	Cost effective and time efficient ensuring commercial viability	The use of this standard can be used to cut out trial and error in development and best practices.
	Credible	This standard is developed by an independent body to find best practices for system security engineering.
	Core Competencies	The model deals with the core competencies required for outsourcing PKI, namely: • Risk • Engineering • Assurance
Disadvantages	Inherent problems with International Standards.	• Standards implicitly require compromise. • Compromise can lead to loss of interoperability and financial and/or commercial viability.
	Partial Implementation due to commercial pressure	Partial compliance with the standard can lead to interoperability issues.
	Standards can be aggressively undermined	An organisation can set out to change the standard by adapting / extending it beyond all recognition, effectively killing the standard.
	Specific threats to this standard.	A specific threat to this standard model is that if many organisations adopt it, and it is subsequently found to have a vulnerability then all of organisations will be affected by the vulnerability
	Lack of Scope in Assurance process.	The assurance process in this model deals only with repeatability and not security functionality or other security assurance requirements.

SABSA Model		
Advantages	Usability	The model provides an appropriate and usable infrastructure for effective operational and management processes.
	Inter-Operability	The model provides long term requirements for interoperability.
	Integration	The model allows for integration with multiple platforms and applications for future growth.
	Supportability	The solution the model provides is capable of being supported in the environment it was designed for.
	Low Cost Development	The model supports modular design which is capable of being easily integrated into a development programme at minimal cost.
	Fast Time to Market	The model supports modular design which is capable of being easily integrated into a development programme with minimal delay.
	Scalability of Platforms	The model supports the use of a range of platforms.
	Scalability of Security Level	The model supports the solution to provide a range of cryptographic techniques which will be required for the security level of the system.
	Re-Usability	The model supports the re-use of the system in similar situations.
	Lower Operation and Administration Costs	The model allows for the cost impact on system operations to be minimised, allowing efficient administration.
Disadvantages	Purely a Risk Driven Approach	The model is based on decisions derived solely on the analysis of business requirements for security. In our opinion this scope should be widened to include other approaches such as: • Data driven approach • Scenario driven approach • Business goal driven approach • Architecture driven approach
	User Expectations	Users may expect applications to be available at all times due to the high confidence instilled in an organisation that adopts an enterprise security architecture
	Complex Design and Development	Not only is the design and development complex but this model requires architects and designers to be able to work together to create the system. If there is poor project management then this will be an almost impossible task.

Seven-S Model - McKinsey & Company		
Advantages	Adopts a holistic perspective	The inter relationships between key components are used to determine the overall systems performance
	Adopts organisational software	Organisational software such as mapping human behaviour and ergonomics are used as part of the systematic approach to organisational assessment..
	The Seven S Model is simple and easy to remember	The seven S's were designed so that the headings and contents were easy to remember.
	User Friendly.	The model has a user friendly framework and can be used from the earliest stages of organisational analysis
Disadvantages	Focuses on internal activities	This model only focuses in activities that happen within the organisation and misses the opportunity to take into account additional activities such as the context in which the analysis takes place.
	High level of abstraction	There is very little guidance on the actual operation of each of the S's, there is a high level description but that's about it.
	Doesn't deal with a variety of organisational issues	As with the focus on internal activities there are a whole host of other organisational issues that this model should take into account but are omitted.

ITIL Service continuity		
Advantages	Aligned with organisational strategy	This model allows for the delivery of managed services to meet the business requirements of any organisation that adopts ITIL.
	Improved quality of service	This model is industry best practice, this in itself does not provide quality of services but if the principles and procedures in ITIL are followed then there will be improvements in the quality of service.
	Service costs can be justified	As ITIL is widely known and has been proven to provide better quality of service then justifying the cost of implementation should be fairly straight forward.
	Known and common procedures.	The ITIL framework is well known and accepted within the business community and as such has a level of credibility within industry
	Efficient reporting and management	ITIL is focused on continual process improvement to optimise service quality
	Supported by International Standards Organisations	BS15000 and ISO 2000 support the concepts of ITIL, both were developed after ITIL and are now widely deployed IT Service Management Standards.
Disadvantages	ITIL is not a comprehensive service management system	Ignoring or being unaware of additional requirements can
	Management and staff unable to understand the principles of ITIL	ITIL should be used alongside existing management systems and not be implemented as the sole system. Management effort can be distracted which results in the additional costs and workloads in implementing an ITIL framework and may not produce the required results.
	ITIL requires careful maintenance and monitoring	ITIL doesn't provide very much detail on information requirements for its process. A lot of time and effort will have to be spent on developing an information architecture that can support and ITIL installation.

PA Consulting - Framework for Outsourcing and Outsourced Enabled Change		
Advantages	Use of Business Driver Analysis	Emotional and financial cases for change are required if change is to be accepted. The used of business driver analysis can be used to build an emotional case for change, thus, supporting the financial case for change.
	Engages changes leaders	Identifies and manages relationships between the individuals at various levels of the business who are responsible for change. The model defines how change leaders should be approached and managed in order to gain a successful result.
	Winning the commitment of critical stakeholders	The model defines how stakeholders are identified and managed through robust communications planning to build trust and understanding.
	Driving the change management program	This model advocates that the program is driven "ruthlessly" through the organisation as part of a thorough change management programme.
	Business outcomes are gauged	This model describes the use of rigorous controls to achieve and demonstrate business outcomes. This ensures that the stakeholders and change leaders are aware of milestones in the programme.
Disadvantages	Takes the view of a management consultancy	This model is designed for consultants who undertake change management programmes for clients, this model may not be well suited to all organisations. It will largely be down to the culture of the organisation if this model is adopted.
	Lack of credibility	There are numerous change management models, some of these include: • Beer's Model • Shaw's Model These two models are already well known and have credibility.

Appendix B: Project Description Form

Project Description Form

Royal Holloway, University of London

MSc Information Security

TO BE COMPLETED BY THE PROJECT CANDIDATE

Name: Christopher McLaughlin

Contact Email Address(es): christopher.mclaughlin@rhul.ac.uk

Provisional Title of Project: Outsourcing PKI

1. Statement of Objectives

1a. I intend to achieve the following objectives:

1. Introduce the principles behind PKI
    a. Define the basic principles of PKI
    b. Define the terms associated with PKI
2. Introduce the principles behind Outsourcing
    a. Define the basic principles of Outsourcing
    b. Define the terms associated with Outsourcing
3. Managerial Aspects of Outsourcing PKI
    a. Determine the Business drivers for Outsourcing PKI
    b. Trusting PKI Outsource Partners
        i. HMG PKI Initiative
        ii. tScheme
    c. Address the Managerial PKI deployment considerations in respect to Outsourcing
    d. Address associated management problems in terms of an Outsourced PKI Infrastructure.
4. Technical Aspects of Outsourcing PKI
    a. Understand the technical issues and complexities of outsourcing PKI
    b. Determine the technical drivers for Outsourcing PKI
    c. Determine the Core Services PKI offer and which can be outsourced
    d. Address the technical PKI deployment considerations in respect to Outsourcing
    e. Determine the Enabled Services PKI offer and which can be outsourced
5. Future work leading on from this dissertation
    a. Define trends in Outsourcing of PKI services
    b. Define changing environments where PKI will become more relevant
    c. Review technological advances that will encourage more widespread use of PKI

1.b I have chosen this project for the following reasons:

PKI is a business enabler and with the advent of a network centric society organisations have to meet the threats, challenges and opportunities that lay ahead. PKI can provide the services that enable business to meet the demands of the 21st Century; the technology is available but security professionals that have both the technical and business skills are in short demand. I aim to learn about the issues involved in both the business and technical aspects of outsourcing PKI as the next step on the ladder of my future career.

PKI is an expansive subject providing the core services of Confidentiality, Integrity, Authentication and Authorization. By studying PKI outsourcing I aim to consolidate my technical knowledge gained on the core and elective modules. I also aim to bring in the non-technical aspects of the course into play with looking at the Business and Management (both Security and Risk Management), legal aspects as well as standards and regulatory bodies that are involved with PKI.

2. Methods to be used

2a. I aim to use the following methods to achieve the objectives listed in Section 1, this list is not inclusive of all of the resources that will be used:

- Standards bodies
    - Objectives to be met by using these standards: Introduction to PKI, Technical Aspects of PKI & Future Work:
        - ISO / ITU-T (www.itu.int)
            - X.500 series of standards
        - IETF PKIX (www.ietf.org)
            - Certificate and CRL Profile (RFC 3279, RFC 3280)
                - LDAP V.2 Profile (RFC 2559)
                - LDAP V.2 Schema (RFC 2587)
                - FTP / HTTP Operational Protocols (RFC 2585

- OCSP - Online certificate status protocol (RFC 2560)
- CMP – Certificate Management Protocol (RFC 2510)
- CRMF – Certificate Request Management Format (RFC 2511)
- CP – Certificate Policy (RFC 2527)
- CPS – Certificate Practice Statement Framework (RFC 2527)
- CMS – Certificate Management messages over CMS (RFC 2797)
- Qualified Certificate Profile (RFC 3039)
- TSP – Time Stamp Protocol (RFC 3161)
- S/MIME (RFC 2311 / 2312 / 2630-2634 / 2459)
- ISO TC68
- IPSEC (RFC 2246)
- TLS (RFC 2246)
- SPKI (RFC 2692 / 2693)
- OpenPGP (RFC 2440)

  - ANSI (www.ansi.org)
    - X9 Committee
  - IEEE (www.ieee.ogrg)
    - IEEE P1363

- Websites
  - Objectives to be met by using these websites: Introduction to PKI, Technical Aspects of PKI & Future Work:
    - Understanding X.500: http://sec.cs.kent.ac.uk/x500book/
    - The PKI Page: http://www.the-pki-page.net/
    - Open Source PKI Book: http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI-html/ospki-book.htm
    - PKI Forum: www.pkiforum.com

        - PKI Forum Hong Kong: www.hkpkiforum.org.hk
        - OASIS: www.oasis-open.org/committees/pki/
        - Federal PKI Steering Committee: http://www.cio.gov/fpkisc/
        - NIST PKI Project: http://csrc.nist.gov/pki/
    - Objectives to be met by using these websites: Introduction to principles behind Outsourcing & Managerial aspects of Outsourcing.
        - HMG PKI: www.hmgpki.gov.uk/
        - tScheme: www.tscheme.org
        - Webtrust: www.webtrust.org
        - PKI Law: http://www.pkilaw.com/
- Books
    - Objectives to be met by using these books: Introduction to PKI, Technical Aspects of PKI & Future Work:
        - Alex .W Dent & Chris .J Mitchell, 2005. Users guide to Cryptography and Standards. Artec House Inc.
        - Michael .E Whitman & Herbert .J Mattord, 2005. Principles of Information Security. Thomsom course Technology of Thomson Learning Inc.
        - Ed. Lorrie Faith Cranor & Simson Garfinkel, 2005. Security and Usability. Orielly Media Inc.
        - Carlisle Adams & Steve Lloyd, 2005. Understanding PKI. Addison Wiley of Pearson Education Inc.
        - Dieter Gollman, 2004. Computer Security. John Wiley & Sons
        - William Stallings, 2003, Network Security Essentials. Prentice Hall of Pearson Education Inc.
        - Bruce Schneier, 1996, Applied Cryptography. John Wiley & Sons
        - Alfred .J Menezes, Paul .C van Oorschot & Scott .A Vanstone, 1997. Handbook of Applied Cryptography. CRC Press

- Objectives to be met by using these books: Introduction to principles behind Outsourcing & Managerial aspects of Outsourcing.
  - Ian .J Lloyd, 2004. Information Technology Law. Oxford University Press
  - Chris Reed, 2004. Internet Law, Cambridge University Press
  - Steve Hedley & Tanya Aplin, 2006. Statutes on IT and E-commerce. Oxford University Press
  - Maurice .F Greaver II, 1998. Strategic Outsourcing. AMA Publications of American Management Association International
  - Linda Cohen & Allie Young, 2006. Multi-sourcing. Harvard Business School Press
  - Carlisle Adams & Steve Lloyd, 2005. Understanding PKI. Addison Wiley of Pearson Education Inc.

- Research and White Papers (Selection of Research and White Papers when found)
  - Objectives to be met by using Research and White Papers: Introduction to PKI, Technical Aspects of PKI, Introduction to principles behind Outsourcing, Managerial aspects of Outsourcing. & Future Work:
- Vendor Websites
  - Objectives to be met by using these Vendor Websites: Introduction to PKI, Technical Aspects of PKI, Introduction to principles behind Outsourcing, Managerial aspects of Outsourcing. & Future Work:
    - Verisign: www.verisign.com
    - Globalsign: www.globalsign.com
    - Entrust: www.entrust.com
- Questionnaire (depending on level of response)
  - Objectives to be met by using the Questionnaire: Introduction to PKI, Technical Aspects of PKI, Introduction to principles behind Outsourcing, Managerial aspects of Outsourcing. & Future Work:

2b. Getting Started

My plan for starting this project is to plan my argument carefully and to break this argument down into relevant sections as chapter outlines, the purpose of this will allow me to set out a format that any reader of this project will be able to follow and understand the validity of any conclusions I make from the material I have researched.

The project will start with a comprehensive introduction into the project and will serve the purpose of outlining the general topic of the project, introduction into the research I have carried out in the line of preparing the project and to provide a preview of what the project will cover and the arguments that I will lay before the reader.
Successive chapters will cover the main headings that I have decided on, namely:

1. Introduction to the principles behind PKI
2. Introduction to the principles behind Outsourcing
3. Managerial Aspects of Outsourcing PKI
4. Technical Aspects of Outsourcing PKI
5. Future work leading on from this dissertation

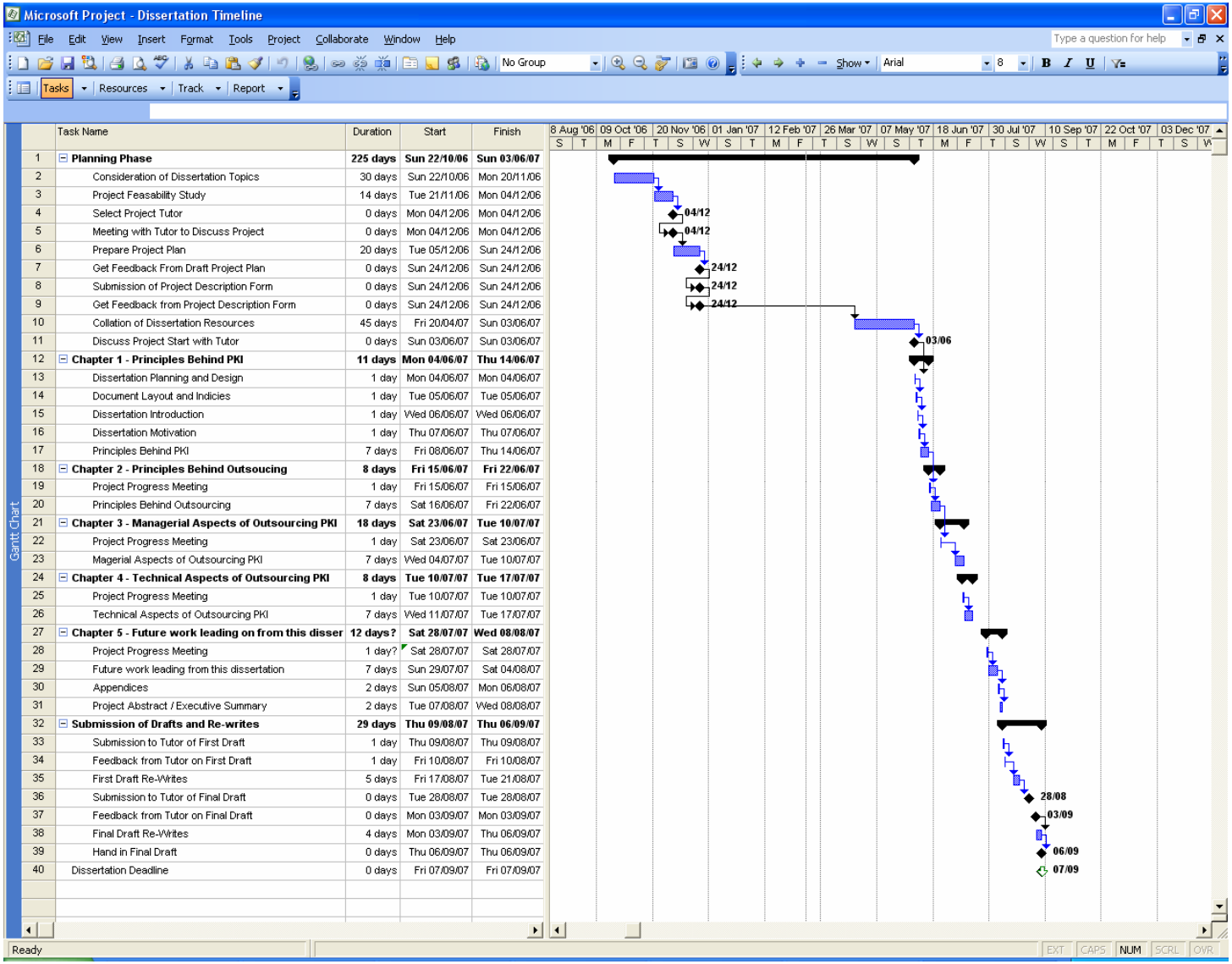
I will start each of the chapters by pre-reading material relevant to the chapter and analyzing the information obtained from the resources that I have listed. From there I will produce draft copies of each of the chapters which I will aim to show my arguments for or against any agreeable or conflicting information obtained from the resources listed.

I aim to gather as many resources as possible within the months January to July. My preparation will include pre-reading of any relevant material including Standards, White Papers, Research Papers and Management Reports. I will also try to cultivate contacts within Industry that I can use primarily as up to date sources of information about the state of PKI in industry and the opportunities for outsourcing services but, if possible, use them to review the draft copies of the project as to give an objective view on my ongoing efforts.

I also aim to utilize the existing faculty members of the ISG to gain as much knowledge from them as possible on the different technical, theoretical and practical aspects of the technology behind PKI services and the methods of obtaining trust in Outsourcing these services.

After the chapters have been satisfactorily completed then my aim is to tie my arguments together with a strong conclusion showing the reader that I have fully understood and researched the material and pointing him/her in the direction of further work that can be followed on from this project.

3a. The work plan



	Task Name	Duration	Start	Finish
1	**Planning Phase**	**225 days**	**Sun 22/10/06**	**Sun 03/06/07**
2	Consideration of Dissertation Topics	30 days	Sun 22/10/06	Mon 20/11/06
3	Project Feasability Study	14 days	Tue 21/11/06	Mon 04/12/06
4	Select Project Tutor	0 days	Mon 04/12/06	Mon 04/12/06
5	Meeting with Tutor to Discuss Project	0 days	Mon 04/12/06	Mon 04/12/06
6	Prepare Project Plan	20 days	Tue 05/12/06	Sun 24/12/06
7	Get Feedback From Draft Project Plan	0 days	Sun 24/12/06	Sun 24/12/06
8	Submission of Project Description Form	0 days	Sun 24/12/06	Sun 24/12/06
9	Get Feedback from Project Description Form	0 days	Sun 24/12/06	Sun 24/12/06
10	Collation of Dissertation Resources	45 days	Fri 20/04/07	Sun 03/06/07
11	Discuss Project Start with Tutor	0 days	Sun 03/06/07	Sun 03/06/07
12	**Chapter 1 - Principles Behind PKI**	**11 days**	**Mon 04/06/07**	**Thu 14/06/07**
13	Dissertation Planning and Design	1 day	Mon 04/06/07	Mon 04/06/07
14	Document Layout and Indicies	1 day	Tue 05/06/07	Tue 05/06/07
15	Dissertation Introduction	1 day	Wed 06/06/07	Wed 06/06/07
16	Dissertation Motivation	1 day	Thu 07/06/07	Thu 07/06/07
17	Principles Behind PKI	7 days	Fri 08/06/07	Thu 14/06/07
18	**Chapter 2 - Principles Behind Outsoucing**	**8 days**	**Fri 15/06/07**	**Fri 22/06/07**
19	Project Progress Meeting	1 day	Fri 15/06/07	Fri 15/06/07
20	Principles Behind Outsourcing	7 days	Sat 16/06/07	Fri 22/06/07
21	**Chapter 3 - Managerial Aspects of Outsourcing PKI**	**18 days**	**Sat 23/06/07**	**Tue 10/07/07**
22	Project Progress Meeting	1 day	Sat 23/06/07	Sat 23/06/07
23	Magerial Aspects of Outsourcing PKI	7 days	Wed 04/07/07	Tue 10/07/07
24	**Chapter 4 - Technical Aspects of Outsourcing PKI**	**8 days**	**Tue 10/07/07**	**Tue 17/07/07**
25	Project Progress Meeting	1 day	Tue 10/07/07	Tue 10/07/07
26	Technical Aspects of Outsourcing PKI	7 days	Wed 11/07/07	Tue 17/07/07
27	**Chapter 5 - Future work leading on from this disser**	**12 days?**	**Sat 28/07/07**	**Wed 08/08/07**
28	Project Progress Meeting	1 day?	Sat 28/07/07	Sat 28/07/07
29	Future work leading from this dissertation	7 days	Sun 29/07/07	Sat 04/08/07
30	Appendices	2 days	Sun 05/08/07	Mon 06/08/07
31	Project Abstract / Executive Summary	2 days	Tue 07/08/07	Wed 08/08/07
32	**Submission of Drafts and Re-writes**	**29 days**	**Thu 09/08/07**	**Thu 06/09/07**
33	Submission to Tutor of First Draft	1 day	Thu 09/08/07	Thu 09/08/07
34	Feedback from Tutor on First Draft	1 day	Fri 10/08/07	Fri 10/08/07
35	First Draft Re-Writes	5 days	Fri 17/08/07	Tue 21/08/07
36	Submission to Tutor of Final Draft	0 days	Tue 28/08/07	Tue 28/08/07
37	Feedback from Tutor on Final Draft	0 days	Mon 03/09/07	Mon 03/09/07
38	Final Draft Re-Writes	4 days	Mon 03/09/07	Thu 06/09/07
39	Hand in Final Draft	0 days	Thu 06/09/07	Thu 06/09/07
40	Dissertation Deadline	0 days	Fri 07/09/07	Fri 07/09/07

3b. Project Plan

My Project Plan (Provided in more detail on the Gantt Chart):

- Write Project Description Form
- Get supervisor approval
- Follow the work plan schedule in terms of milestones
- Semester Two (January to July)
    - Pre-reading
    - Research
    - Dispatch Questionnaire
    - Cultivate Industry contacts
- Summer Term (June to September)
    - Start Write-up
    - Regular meetings with supervisor
    - Final Draft
    - Re-writes if necessary
    - Hand in Dissertation

4. Additional comments

The main objectives of this dissertation may change as the project progresses it may not be possible to use any information gained through the responses to questionnaires as it is difficult to estimate the level of interest that will be achieved.

I aim to cultivate industry contacts as the project progresses to gain a full and varied understanding of the issues and complexities surrounding, not only the Outsourcing of PKI but also the challenges faced by organisations who maintain an in-house capability

TO BE COMPLETED BY THE PROJECT SUPERVISOR
I approve the attached project plan.

Signed:

Name:

Date:

Appendix C: PKI Related Standards

ANSI X9.24	Retail Financial Services Symmetric Key Management - Part 1: Using Symmetric Techniques
ANSI X9.30	Digital Siganture Algorithm (Based on FIPS 186)
ANSI X9.31	Reversible DSA (RSA and Rabin-Williams)
ANSI X9.62	Elliptic Curve Digital Signature Algorithm
FIPS 180-2:2002	SHS (Secure Hash Standard)
IEEE 1363	Standard Specifications for Public Key Cryptography
IEEE 1363a	Standard Specifications For Public Key Cryptography-Amendment 1: Additional Techniques
IETF RFC 4809	Requirements for and IPSec Certificate Management Profile
IETF RFC 1510	The Kerberos Network Authentication Service
IETF RFC 2025	Simple Public Key GSS-API Mechanism
IETF RFC 2246	The Transport Layer Security Protocol Version 1.0
IETF RFC 2311	S/MIME Version 2 Message Specification
IETF RFC 2312	S/MIME Version 2 Certificate Handling
IETF RFC 2401	Security Architecture for the Internet Protocol
IETF RFC 2411	IP Security Document Roadmanp
IETF RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
IETF RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols
IETF RFC 2511	Internet X.509 Certificate Request Message Format
IETF RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
IETF RFC 2528	Internet X.509 Public Key Infrastructure Representation of Key Excahange Algorithm keys in Internets X.509 Public Key Infrastructure Certificates
IETF RFC 2559	Internet X.509 Public Key Infrastructure Operation Protocols LDAPv2
IETF RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol
IETF RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols FTP and HTTP

IETF RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema
IETF RFC 2632	S/MIME Version 3 Certificate Handling
IETF RFC 2633	S/MIME Version 3 Message Specification
IETF RFC 2797	Certificate Management Messages over CMS
IETF RFC 2875	Diffie-Hellman Proof of Possession Algorithms
IETF RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols
IETF RFC 3039	Internet X.509 Public Key Infrastructure Qualified Certificate Profile
IETF RFC 3161	Internet X.509 Public Key Infrastructure Time Stamping Protocol
IETF RFC 3174	SHA-1 Hash Function
IETF RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
IETF RFC 3280	Internet X.509 Public Key Infrastructure Certificate and CRL profile
IETF RFC 3281	An Internet Attribute Certificate Profile for Authorization
IETF RFC 3628	Policy Requierements for Timestamping Authorities
IETF RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
IETF RFC 3709	Internet X.509 Public Key Infrastructure Logotypes in X.509 certificates
IETF RFC 3739	Internet X.509 Public Key Infrastructure Qualified Certificate profile
IETF RFC 3770	Certificate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN
IETF RFC 3779	X.509 Extensions for IP Addresses and AS Identifiers
IETF RFC 3820	Internet X.509 Public Key Infrastructure Proxy Certificate Profile
IETF RFC 3874	A 224-bit One-way Hash Function SHA-224
IETF RFC 4043	Internet X.509 Public Key Infrastructure Permanent Identifier

IETF RFC 4055	Additional Algorithms and Identifiers for RSA cryptography for use in Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List
IETF RFC 4059	Internet X.509 Public Key Infrastructure Warranty Certificate Extension
IETF RFC 4158	Internet X.509 Public Key Infrastructure Certification Path Building
IETF RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocols
IETF RFC 4211	Internet X.509 Public Key Infrastructure Certificate Request Message Format
IETF RFC 4306	Internet Key Exchange Version 2
IETF RFC 4308	Cryptographic Suites for IPSec
IETF RFC 4325	Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List Extensions
IETF RFC 4334	Certificate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN
IETF RFC 4346	The Transport Layer Security Protocol Version 1.1
IETF RFC 4366	The Transport Layer Security Protocol Extensions
IETF RFC 4386	Internet X.509 Public Key Infrastructure Repository Locator Service
IETF RFC 4387	Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP
IETF RFC 4476	Attribute Certificate Policies Extensions
IETF RFC 4491	Using GOST R 34.10-94, GOST R 34.10-2001 and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
IETF RFC 4492	Elliptic Curve Cryptography Cipher Suites for TLS
IETF RFC 4630	Update to Directory String Processing in the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
IETF RFC 4683	Internet X.509 Public Key Infrastructure Subject Identification Method
IETF RFC 4806	Online Certificate Status Protocol Extensions to IKEv2

ISO/IEC 7498-2:1989	Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture
ISO/IEC 10118-1:2000	Information technology -- Security techniques -- Hash-functions -- Part 1: General
ISO/IEC 10118-2:2000	Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher
ISO/IEC 10118-3:2004	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 10118-4:1998	Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic
ISO/IEC 10181-1:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview
ISO/IEC 10181-2:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework
ISO/IEC 10181-3:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework
ISO/IEC 10181-4:1997	Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework - Part 4:
ISO/IEC 10181-5:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework
ISO/IEC 10181-6:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework
ISO/IEC 10181-7:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework
ISO/IEC 11770-1:1996	Information technology -- Security techniques -- Key management -- Part 1: Framework
ISO/IEC 11770-2:1996	Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric

	techniques
ISO/IEC 11770-3:199	Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques
ISO/IEC 11770-4:2006	Information technology -- Security techniques -- Key management -- Part 4: Mechanisms based on weak secrets
ISO/IEC 14516:2002	Information technology. Security techniques. Guidelines for the use and management of trusted third party services
ISO/IEC 14888-1:1999	Information technology. Security techniques. Digital signatures with appendix, General
ISO/IEC 14888-2:1999	Information technology. Security techniques. Digital signatures with appendix, Identity-based mechanisms
ISO/IEC 14888-3:2006	Information technology. Security techniques. Digital signatures with appendix, Discrete logarithm based mechanisms
ISO/IEC 15946-1:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General
ISO/IEC 15946-2:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures
ISO/IEC 15946-3:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 3: Key establishment
ISO/IEC 15946-4:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 4: Digital signatures giving message recovery
ISO/IEC 17799:2005	Information technology. Security techniques. Code of practice for information security management
ISO/IEC 18014-1:2002	Information Technology: Security Techniques: Time Stamping Services Frameworks
ISO/IEC 18014-2:2002	Information Technology: Security Techniques: Time Stamping Services: Part 2: Mechanisms producing independent tokens
ISO/IEC 18014-3:2004	Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens
ISO/IEC 18033-1:2005	Information technology - Security techniques - Encryption

	algorithms - Part 1: General
ISO/IEC 18033-2:2005	Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers
ISO/IEC 18033-3:2005	Information technology - Security techniques - Modes of operation for an n-bit block cipher
ISO/IEC 18033-4:2005	Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers
ISO/IEC 9796-2:2000	Information technology. Security techniques. Digital signature scheme giving message recovery. Integer factorisation based mechanisms
PKCS #1:	RSA Cryptography Standard
PKCS #10:	Certification Request Syntax Standard
PKCS #11	Cryptographic Token Interface Standard
PKCS #12	Personal Information Exchange Syntax Standard
PKCS #13	Elliptic Curve Cryptographic Standard
PKCS #15	Cryptographic Token Information Format Standard
PKCS #3:	Diffie-Hellman Key Agreement Standard
PKCS #5	Password Based Cryptographic Standard
PKCS #6:	Extended Certificate Syntax Standard
PKCS #7:	Cryptographic Message Syntax Standard
PKCS #8:	Private Key Information Syntax Standard
PKCS #9:	Selected Attribute Types