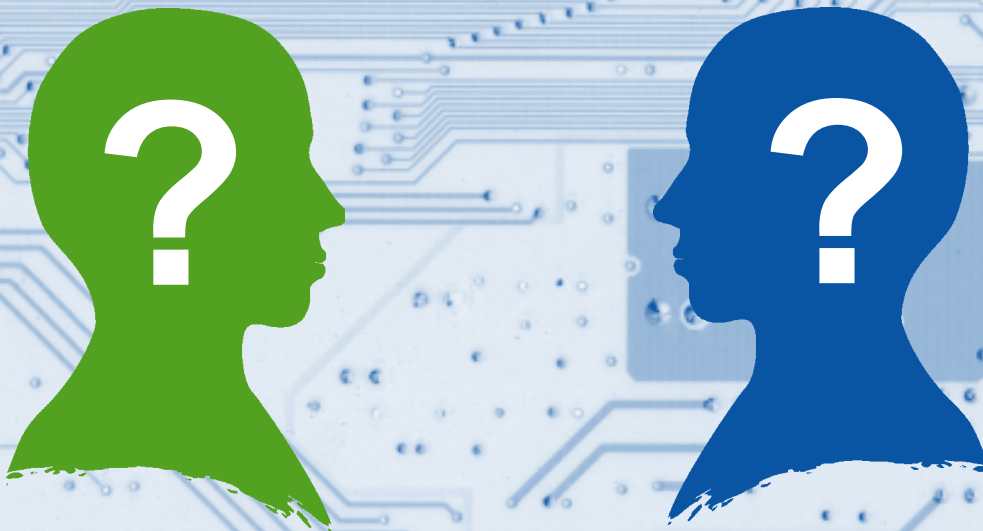




Asia-Pacific Economic Cooperation

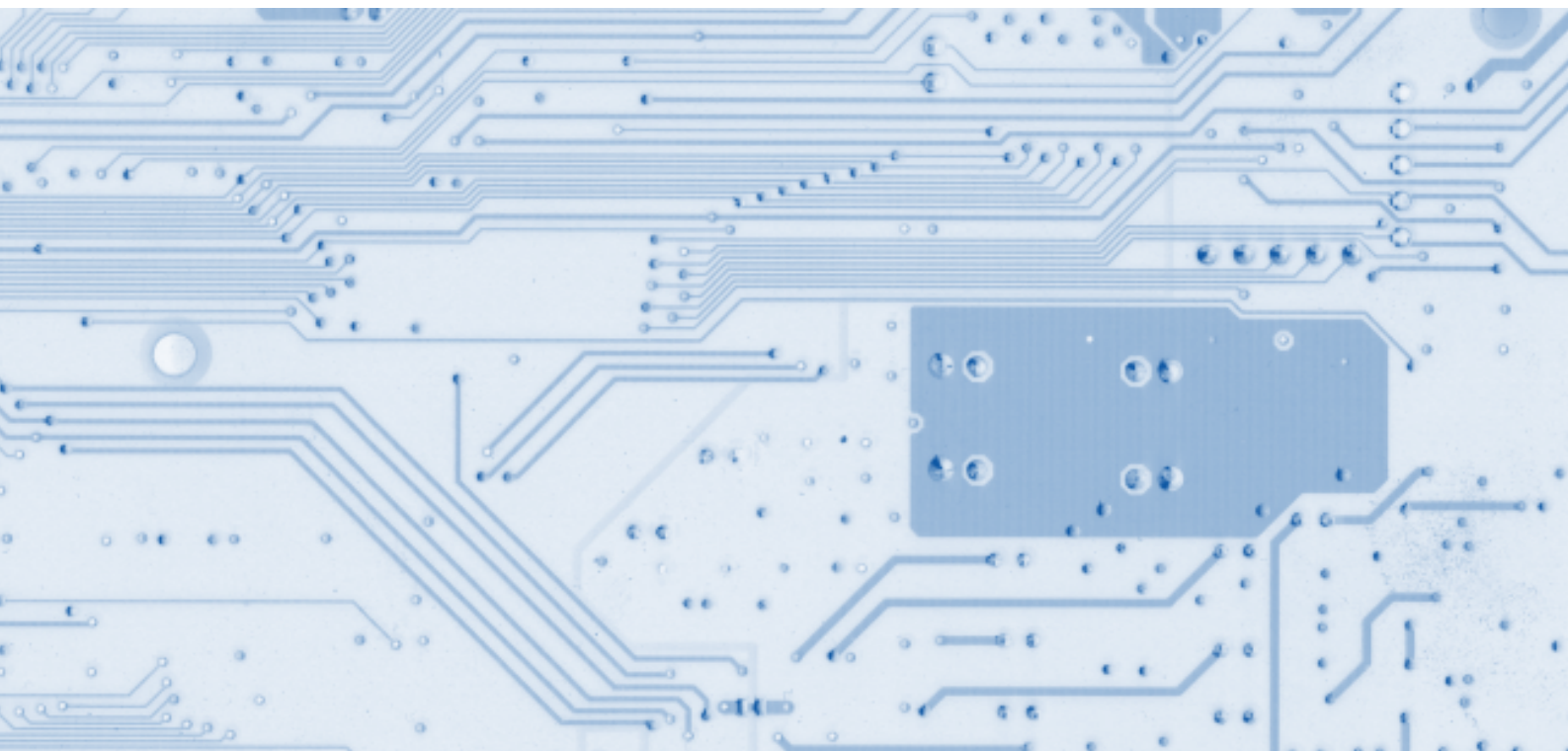
# Electronic Authentication

Issues relating to its selection and use



**eSecurity Task Group**  
Business Facilitation Steering Group  
APEC Telecommunications and Information Working Group

**2002**



Asia-Pacific Economic Cooperation

APEC Secretariat

35 Heng Mui Keng Terrace Singapore 119616

Tel: (65) 6775 6012 Fax: (65) 6775 6013 Email: [info@mail.apecsec.org.sg](mailto:info@mail.apecsec.org.sg)

APEC#202-TC-01.2

ISBN: 981-04-7690-6



# **Electronic Authentication**

Issues relating to its selection and use

**eSecurity Task Group**

Business Facilitation Steering Group

APEC Telecommunications and Information Working Group

**2002**

2002

Publication numbers: APEC#202-TC-01.2

ISBN: 981-04-7690-6.

Copyright © 2002 APEC Secretariat

Requests and inquiries concerning reproduction  
and rights should be addressed to:

Asia-Pacific Economic Cooperation Secretariat  
35 Heng Mui Keng Terrace  
Singapore 119616

telephone: +65 6775 6012

facsimile: +65 6775 6013

email: [info@mail.apecsec.org.sg](mailto:info@mail.apecsec.org.sg)

# Foreword

This report was prepared at the request of the APEC Telecommunications and Information Working Group (TEL). It is built on a number of papers prepared for the eSecurity Task Group and its predecessor the Electronic Authentication Task Group, both subgroups of the Business Facilitation Steering Group of the Telecommunications and Information Working Group. Some material was developed by the PKI Interoperability Expert Group which is a subgroup of the eSecurity Task Group.

In accordance with a decision taken at the 18<sup>th</sup> meeting of the TEL the report addresses all forms of electronic authentication and identifies issues relating to their selection and use. It has been structured around a series of points identified at that meeting with a separate chapter devoted to each group of authentication technologies also identified at that meeting.

While the report has been primarily prepared for government policy makers, much of the information contained in the report can assist businesses considering the use of electronic authentication, lawyers practicing in the field of electronic commerce and students of the subject. It is recommended that those not familiar with cryptography read the cryptography tutorial in Chapter 8 before reading this report.

The report is published using funds allocated from the APEC Central Fund.

When naming economies, the report uses the APEC convention of separating individual economies by a semi colon. This allows readers to distinguish between Hong Kong, China; and China where individual economies are listed.

A number of economies provided information for input into this report particularly through their response to questionnaires. I would particularly like to thank Chris Charnes, Josef Pieprzyk, Jennifer Seberry, Standards Australia and Stephen Wilson from Australia; Peter Ferguson, Jane Hamilton, Laurie Mack and Bob Stevens from Canada; John Daly from Hong Kong, China; and Er Chiang Kai, Francis Goh, Goh Seow Hiong, Leonard Lee and Pebble Teo from Singapore for their contributions to chapters of this report.

I would also like to thank György Endersz of the European Telecommunications Standards Initiative; Riccardo Genghini of the Comité Européen de Normalisation, Information Society Standardization System; and Richard Wilsher of the European Electronic Signatures Standardization Initiative for their input on PKI interoperability activities in Europe and Stephen Lloyd, Andrew Nash and Lisa Pretty of the PKI Forum for their input on PKI interoperability in general.

I would especially like to thank Michael Baum, co author of *Secure Electronic Commerce*, for his input and his invaluable comments on draft chapters of this report.

Finally I would like to thank the Australian Attorney-General's Department for allowing me the time to prepare some parts of this report while working for them and the Australian National Office for the Information Economy which funded my completion of this report.



Steve Orłowski  
Chair  
eSecurity Task Group  
Business Facilitation Steering Group  
APEC Telecommunications and Information Working Group

Electronic Authentication—issues relating to its selection and use

# Table of contents

Foreword	3
Table of contents	5
Table of figures	9
Table of acronyms	11
<b>Executive summary</b>	<b>17</b>
Definitions	17
Electronic business models	17
User requirements	18
Electronic authentication technology	18
Certification models	18
Trust	18
Liability	18
Roles of participants	19
Interoperability	19
Accreditation	19
Cultural differences	19
Awareness	19
Leadership	20
Legal Issues	20
Conclusion	20
<b>Chapter 1. General issues relating to the selection and use of electronic authentication</b>	<b>23</b>
Introduction	23
Background	25
Definitions	26
Electronic business models	26
User requirements	30
Electronic authentication technologies	32

Electronic Authentication—issues relating to its selection and use

Certification models	35
Trust	37
Liability	37
Roles of participants	38
Interoperability	39
Accreditation	42
Cultural differences	44
Awareness	45
Leadership	47
Conclusion	49
<b>Chapter 2. Asymmetric (public key) cryptography</b>	<b>51</b>
Definitions	52
Technology	54
Infrastructure	59
Use in electronic business models	66
User requirements	70
Certification models	70
Trust	70
Liability	74
Roles of participants	76
Accreditation	78
Interoperability	81
Cultural differences	81
Awareness	82
Leadership	83
Combination with other technologies (hybrids)	86
<b>Appendix 1. Electronic authentication in a multi-format multi-protocol environment</b>	<b>87</b>
Terminology	87
Methods of achieving authentication	88
Types of authentication	89
Basic issues	89
Possible solutions	90
<b>Chapter 3. Public key infrastructure interoperability</b>	<b>93</b>
Achieving PKI interoperability	94
Mapping of certification authorities accreditation schemes	104
Initial mapping of certification authorities accreditation schemes	110
Second mapping of certification authorities accreditation schemes	114
Detailed mapping of PKI schemes	120



## Table of contents

Appendix 1. Terminology mapping	121
Appendix 2. Selected definitions of cross-certification	123
<b>Chapter 4. Shared secret technologies</b>	<b>125</b>
Definitions	125
Technology	127
Use in electronic business models	129
User requirements	130
Certification models	130
Trust	131
Liability	133
Roles of participants	133
Interoperability	133
Accreditation	134
Cultural differences	134
Awareness	134
Leadership	135
Combination with other technologies (hybrids)	137
Appendix 1. Secret sharing	139
Terminology	141
Models for secret sharing	142
Some known schemes	142
The problem of cheaters	145
Non-perfect schemes	145
<b>Chapter 5. Biometric technologies</b>	<b>147</b>
Definitions	147
Technology	148
Use in electronic business models	149
User requirements	150
Certification models	151
Trust	151
Liability	152
Roles of participants	152
Interoperability	153
Accreditation	153
Cultural differences	153
Awareness	154
Leadership	155
Combination with other technologies (hybrids)	156

<b>Chapter 6. Other technologies</b>	<b>157</b>
Characteristics	157
Use in electronic business models	159
User requirements	159
Certification models	160
Trust	160
Liability	160
Roles of participants	161
Interoperability	161
Accreditation	161
Cultural differences	161
Awareness	161
Leadership	162
Combination with other technologies (hybrids)	162
<b>Chapter 7. Hybrid technologies</b>	<b>163</b>
Technology	163
Use in electronic business models	167
User requirements	168
Certification models	168
Trust	169
Liability	170
Roles of participants	170
Interoperability	171
Accreditation	172
Cultural differences	172
Awareness	172
Leadership	173
<b>Chapter 8. A brief tutorial on cryptography for the novice</b>	<b>175</b>
The electronic world	176
Security services	176
Cryptography fundamentals	177
Asymmetric cryptographic technique	180
Digital signature	182
Certificates	184
<b>Chapter 9. Legal issues</b>	<b>187</b>
International legal framework	187
Assurance and evidence of legal effect in cross-border transactions	191
Liability	199
Privacy	201

# Table of figures

Figure 1: Open Model .....	27
Figure 2(a): Closed Model Example 1 .....	28
Figure 2(b): Closed Model Example 2 .....	28
Figure 3(a): Open-but-bounded Model Example 1 .....	29
Figure 3(b): Open-But-Bounded Model Example 2 .....	29
Figure 3(c): Open-But-Bounded Model Example 3 .....	29
Figure 4: Asymmetric Cryptography .....	33
Figure 5: Shared Secret .....	33
Figure 6: Biometrics .....	34
Figure 7: Other Email Address Example .....	34
Figure 8: Hybrid Using Three Technologies .....	35
Figure 9: Formal Certification (PKI) .....	36
Figure 10: Informal Certification .....	36
Figure 11: No Certification .....	37
Figure 12: Registration and Certificate Issue .....	54
Figure 13: Certificate Revocation .....	55
Figure 14: Certificate Validation .....	55
Figure 15: Root Certification Authority .....	61
Figure 16: Message Translation .....	89
Figure 17: Secure Proxy Agent .....	90
Figure 18: Bypass Technique .....	91
Figure 19: A Framework for Analysing PKI Interoperability Schemes .....	96
Figure 20: Cross-certification Between Two CAs : CA-A and CA-B .....	97
Figure 21: Illustration of the Concept of Cross-recognition (How User A trusts User B) .....	100
Figure 22: Certificate Authority Accreditation Model .....	109
Figure 23: Shared Secret .....	128
Figure 24: Biometrics .....	149
Figure 25: Other Email Address Example .....	159
Figure 26: Two-Element Chained Technology .....	164
Figure 27: Three-Element Chained Technology .....	164
Figure 28: Two-ASP-Chained Technology .....	164
Figure 29: Secured Technology .....	165

## Electronic Authentication—issues relating to its selection and use

Figure 30: Multiple Layered Secured Technology .....	166
Figure 31: Combined Technology .....	166
Figure 32: Cryptographic Key .....	178
Figure 33: Symmetric Cryptography .....	178
Figure 34: Symmetric Cryptography Key Management (One-to-many) .....	179
Figure 35: Symmetric Cryptography Key Management (Many-to-many) .....	179
Figure 36: Asymmetric Cryptography (encryption) .....	181
Figure 37: Digital Signature .....	182
Figure 38: Example of Hash Function .....	183
Figure 39: Digital Signature Using Hash Function .....	184
Figure 40: X.509 Version 3 Certificate Format .....	184
Figure 41: Certification Authority (CA) .....	185
Figure 42: Cross-certification .....	193
Figure 43: Bridge Certification Authority .....	194
Figure 44: Cross-recognition .....	195
Figure 45: Certificate Trust List .....	195
Figure 46: Accreditation Certificate .....	196
Figure 47: Strict Hierarchy .....	197
Figure 48: Delegated Path Discovery .....	198
Figure 49: Provision of Trust Status Information .....	199

# Table of acronyms

AJP	M. Abrams, S. Jajodia, and H. Podell, eds, 'Information Security —An Integrated Collection of Essays'
AOEMA	Australia Oceania Electronic Marketplace Association
APEC	Asia Pacific Economic Cooperation
API	Application Programming Interface
AS	Australian Standard
ASP	Authentication Service Provider (NB. not 'Application Service Provider')
ATM	Automatic Teller Machine
B2B	Business to Business
B2G	Business to Government
CA	Certification Authority
CEN/ISSS	Comité Européen de Normalisation, Information Society Standardization System
CESG	Communication Electronic Security Group (United Kingdom Government)
CFD	Common Fill Device
CIMC	Certificate Issuing and Management Components (a family of protection profiles developed by NIST)
CMA	Certificate Manufacturing Authority
CP	Certificate Policy. The plural is CPs to avoid confusion with CPS below.
CPS	Certification Practice Statement
CRL	Certificate Revocation List

## Electronic Authentication—issues relating to its selection and use

CSP	Certification Service Provider
DAP	Directory Access Protocol
DBMS	Data Base Management System
DNA	Deoxyribonucleic Acid (a genetic material)
DNS	Domain Name System
DSA	Digital Signature Algorithm
DSP	Directory Service Provider
DSVP	Digital Signature Verification Processor
EC	European Community
ECC	Elliptic Curve Cryptography
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration Commerce and Transport (standards developed by the United Nations Economic Commission)
EEMA	European Forum for Electronic Business (formerly the European Electronic Messaging Association)
EFTPOS	Electronic Funds Transfer-Point of Sale
EOI	Evidence of Identity
EESSI	European Electronic Signatures Standardization Initiative
eSTG	APEC TEL eSecurity Task Group
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	Federal Information Processing Standards (developed by NIST)
HA	High Availability
HTTP	HyperText Transfer Protocol
ICA	Intermediate Certification Authority
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force
I/O	Input-output

## Table of acronyms

IP	Internet Protocol
IS	Information System
ISO	International Organisation for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunications Union
JTC	Joint Technical Committee (of ISO and IEC)
KDC	Key Distribution Centre
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest Version 5 (a hashing algorithm)
NEAC	National Electronic Authentication Council (Australia)
NIST	National Institute of Standards and Technology (United States of America)
NSTISSI	National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, National Information Systems Security (INFOSEC) Glossary (US National Computer Security Center)
OCSP	Online Certificate Status Protocol
OECD	Organisation for Economic Cooperation and Development
PC	Personal Computer
PEM	Privacy Enhanced Mail
PCA	Policy Creating Authority (It may also be a certification authority.)
PGP	Pretty Good Privacy (a product)
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PKAF	Public Key Authentication Framework (Australia)
PKCS	Public Key Cryptography Standards (developed by RSA Security Inc)
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 (an IETF working group)
PKD	Public Key Directory

## Electronic Authentication—issues relating to its selection and use

PKT	Public Key Technology
RA	Registration Authority. The plural is RAs to avoid confusion with RAS below.
RAS	Reliability, Availability and Scalability
RCA	Root Certification Authority
RFC	Request for Comments (an Internet standards-related specification published by the IETF)
RSA	An asymmetric cryptography algorithm named after its inventors Rivest, Shamir and Adelman
SAS	Statement of Auditing Standards (developed by the American Institute of Certified Public Accountants)
SC	Sub-Committee (of JTC1 of ISO and IEC)
SCVP	Simple Certificate Validation Protocol
SDSI	Simple Distributed Security Infrastructure
SET	Secure Electronic Transactions (a protocol developed by Visa and MasterCard)
SHA	Secure Hash Algorithm
SIS	Syntax Independent Signatures
SITA	Originally the Société Internationale de Télécommunications Aéronautiques (a provider of information and network services for the aviation industry)
SME	Small and Medium Enterprise
S/MIME	Security Multipurpose Internet Mail Extension
SMTP	Simple Mail Transfer Protocol
SPAM	Common use term for unsolicited e-mail
SPKI	Simple Public Key Infrastructure
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunications (a network for interbank financial transfers)
TEL	APEC Telecommunications and Information Working Group
TELMIN	APEC Ministerial meeting of the telecommunications and information industry



## Table of acronyms

TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
U...	User
UK	United Kingdom
UNCITRAL	United Nations Commission on International Trade Law
URI	Universal Resource Indicator
URL	Universal Resource Locator
US, USA	United States of America
USB	Universal Serial Bus
VA	Validation Authority
VAN	Value Added Network
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WEMA	World Electronic Messaging Association
WWW	World Wide Web
X.....	Standards developed by the ITU
XML	eXtensible Markup Language

Electronic Authentication—issues relating to its selection and use

# Executive summary

In their 1998 Blueprint for Action<sup>1</sup>, APEC Ministers recognised the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce. A cornerstone in achieving that potential is providing the tools that will allow parties to transactions to know with certainty the degree of reliance they can place on that transaction. Electronic authentication provides such tools through technologies that can ensure the authenticity of transactions. Some of the technologies also provide integrity, non-repudiation and confidentiality functions.

Electronic authentication is a developing field. As it evolves new technologies and new issues emerge. Addressing these issues is a problem for both users and government policy makers. For this reason it was agreed at TEL 18 that the then Public Key Authentication Task Group address all authentication technologies. This report identifies the major issues involved in selecting and using electronic authentication to provide APEC member economies with guidance when developing policy and legal frameworks to support electronic authentication. The report addresses the issues in general, examines five different groups of technologies, and documents how these relate to the issues raised. It also addresses some of the legal issues involved with the use of electronic authentication.

## DEFINITIONS

There is a great degree of variation in definitions associated with both electronic commerce in general and electronic authentication in particular. There is a role for member economies to contribute to and stimulate international organisations' work in attempting to achieve the maximum degree of consistency.

## ELECTRONIC BUSINESS MODELS

The Report examines a number of models of the environment in which electronic business might be conducted. These are provided to indicate the variety of different relationships that might exist between parties to an electronic transaction.

It also notes a trend towards requiring authentication in electronic transaction where signatures are not required in equivalent paper processes<sup>2</sup>. It notes the potentially greater demands on and or costs to businesses and users that can arise from this trend.

---

1 APEC Blueprint for Action, [http://www.dfat.gov.au/apec/ecom/ecom\\_blueprint.html](http://www.dfat.gov.au/apec/ecom/ecom_blueprint.html)

2 In some cases a letterhead can also provide a degree of authentication in the paper world.

## **USER REQUIREMENTS**

User requirements cover technical, business process and legal requirements. It is recognised that these requirements need to be met in a consistent or interoperable manner and a manner that is simple to operate and easy to understand. There is a role for both governments and business representative groups to ensure the requirements are met.

## **ELECTRONIC AUTHENTICATION TECHNOLOGY**

The report discusses in broad terms the advantages and disadvantages of a number of technologies including processes that involve the use of several technologies, or several uses of the same technology<sup>3</sup>, in a single transaction.

It is recognised that different technologies can meet different requirements. In part the choice is one for the parties to a transaction based on a risk assessment. In other instances particular technologies may be mandated by legislation or by the requirements of another party. There is, therefore, a need for governments to develop legal and policy frameworks to support all appropriate technologies.

## **CERTIFICATION MODELS**

The report examines the different ways through which a recipient of a transaction can establish whether the claimed sender is the actual sender of an electronic transaction. As with electronic business models, different relationships that might exist when trying to establish the authenticity of a transaction are examined.

## **TRUST**

Trust<sup>4</sup> is the belief that a person, process or machine will act in the manner claimed or expected. In electronic authentication it can be achieved through the development of appropriate technology, development of appropriate legal and policy frameworks and development of appropriate business practices. Accreditation processes are designed to enable users to trust the technologies while legal frameworks are designed to enable users to trust that they can rely on the legal validity of a transaction. Awareness raising programs are designed to build the level of required trust once the appropriate frameworks are in place.

## **LIABILITY**

Liability has been raised as one of the major issues facing users and authentication service providers. This issue is under active consideration in a number of international forums. Central to the discussion is whether governments should legislate in respect of liability, permit a contractual approach or both. The issue is complicated by the fact that a number of economies are federations and jurisdiction for liability may rest with state or provincial governments. In federal approaches a further complication can be a conflict of laws at the federal and state or provincial level.

Different jurisdictions have adopted different approaches to liability. It will be important to ensure that adopting one approach does not prevent transactions with jurisdictions that adopt alternative approaches.

---

3 For example a password can be used to trigger another password as is the case with password ‘wallets’.

4 Trust is discussed by the Authorization, Authentication and Accounting ARCHitecture research group at <http://www.aaaarch.org/dublin/salowe/aaatrust.htm>

## **ROLES OF PARTICIPANTS**

As an essential part of electronic commerce, electronic authentication cuts across both the public and private sectors and extends down to individual users. For the electronic authentication schemes to function effectively, each of these groups needs to undertake defined roles in respect of developing, supporting, promoting or using the technologies or their supporting frameworks. Examples of these roles are discussed in the report.

## **INTEROPERABILITY**

The issue of interoperability means different things to different people. It has been argued in some quarters that we should be aiming for a single globally interoperable scheme. Others support the concept of a number of globally interoperable schemes. Different technologies will meet different requirements based on risk, cost and integration with other technologies. It is unlikely that the differing requirements can be met by a single scheme without compromising security and increasing risk at one end, or cost at the other. However too many schemes will confuse users, possibly increase costs as users need to implement an excessive number of schemes and leave users with a bewildering array of technologies attached to their systems. The objective should be to minimise the burden on users in order to encourage them to adopt electronic authentication and electronic commerce methods. Government and industry need to pursue an appropriate balance in consultation.

Technical standards and legal and policy frameworks will all impact on interoperability and cross border recognition of electronic transactions.

## **ACCREDITATION**

One of the main issues to be addressed by governments is whether they should license or regulate authentication technology or authentication service providers. Approaches could include government licensing, government endorsed accreditation schemes, standards based accreditation schemes and industry endorsed accreditation and audit schemes. Implementation of these schemes can be mandatory or voluntary. The type of approach adopted will vary from jurisdiction to jurisdiction determined largely by domestic policy on issues such as industry regulation and consumer protection. Problems will emerge if jurisdictions insist that authentication technologies or service providers satisfy their licensing or accreditation processes and requirements even where the service provider or user of the technology is located outside their immediate jurisdiction. This needs to be balanced against the need to ensure the reliability of the technology being used.

## **CULTTEURAL DIFFERENCES**

The task group discovered several examples of cultural differences that have the potential to impact on electronic authentication. The principal difference related to the concept of community rather than individual ownership of property as discussed in Chapter 1. This will impact on the general approach of using individual based authenticators in the electronic world. The differences highlight the need for governments to be sensitive to the existence of cultural differences between economies. Cultural differences have the potential to impact on technical, legal and policy aspects of electronic authentication. Often cultural differences are not addressed in these aspects through ignorance rather than intent. There is a need to raise awareness of both cultural differences and their possible impact.

## **AWARENESS**

Electronic commerce and electronic authentication are still emerging disciplines. The level of awareness of both the technologies and their use is patchy and in many cases fraught with

misconceptions. This is particularly the case in respect of the security and reliability of the technologies and their implementation. There is a need to raise awareness among government policy makers, business managers and individual users. In many cases it will be difficult to focus attention on just electronic authentication as a large proportion of the target audience will have wider ranging responsibilities or interests. Strategies for raising awareness of electronic authentication technologies and associated issues will often need to be integrated with broader electronic commerce awareness raising strategies. Specific electronic authentication awareness raising programs can be developed and targeted at selected audiences.

## LEADERSHIP

Governments, international organisations, business, academia, users and user groups and the IT industry all have to assume leadership roles if electronic commerce in general and electronic authentication in particular are to flourish. Adoption of clear legal and policy frameworks, standards and business practices as well as use of the technologies themselves will provide the leadership required to ensure the widespread uptake of electronic commerce.

## LEGAL ISSUES

There are a number of legal issues associated with the use of electronic authentication. These include legal effect of electronic transactions and electronic signatures, liability and privacy.

## CONCLUSION

It was not the objective of the task group to make specific recommendations in this report. Rather the report has been prepared to identify relevant issues for APEC member economies and the various working groups of APEC that will need to consider these issues and develop options in consultation with the wider international community. However a number of points raised by the task group have been adopted by the TEL or Ministers.

At APEC TEL 18 the following points were adopted<sup>5</sup>:

*APEC supports the concept of market driven development of business models and authentication technologies.*

*Governments can, through their use of various business models and authentication technologies, lead by example in the use of these models and technologies.*

*Member economies should adopt policy and regulatory approaches which ensure a neutral approach to both business models and authentication technologies used in electronic commerce.*

The fourth APEC ministerial meeting of the telecommunications and information industry adopted a Programme of Action<sup>6</sup> that included the following points proposed by the then Electronic Authentication Task Group (now the eSecurity Task Group):

*There is a variety of business models, authentication technologies, and implementations of electronic commerce. There should be free choice of these models, technologies and implementations.*

*It should be recognised that in authenticating an electronic transaction multiple technologies may be used.*

---

<sup>5</sup> <http://www.apectelwg.org/apecdata/telwg/18tel/report/18file-2.html>

<sup>6</sup> <http://www.apectelwg.org/apec/are/telminsub02.html>

## Executive summary

*When developing legal and policy frameworks, consideration should be given to the role of multiple technologies.*

*Legal and policy frameworks that focus on specific technologies can impede the use of multiple technologies.*

At TEL 23 the following point was adopted<sup>7</sup>:

*When framing laws, policies and standards, economies should be aware that formatting and protocol requirements of electronic messaging systems may invalidate digital signatures attached to original messages.*

---

<sup>7</sup> [http://www.apectelwg.org/apecdata/telwg/23tel/plenary/plen\\_33.doc](http://www.apectelwg.org/apecdata/telwg/23tel/plenary/plen_33.doc)

Electronic Authentication—issues relating to its selection and use



## Chapter 1

# General issues relating to the selection and use of electronic authentication

### INTRODUCTION

What is Electronic Authentication?

*It is the means by which the recipient of a transaction or message can make an assessment as to whether to accept or reject that transaction.<sup>1</sup>*

The opening quotation, then relating to digital signatures, was part of the preliminary report of the then Public Key Authentication Task Group. The quotation is, however, equally relevant to all types of electronic authentication. There are a number of factors that will be taken into consideration when making the assessment including value of the transaction, assurance of the identity, security of the technology and the legal status of the authenticator.

Electronic authentication is a developing field. As it evolves new technologies and new issues emerge. Addressing these issues is a problem for both users and government policy makers. For this reason it was agreed at TEL 18 that the then Public Key Authentication Task Group address all authentication technologies. This report identifies the major issues involved in selecting and using electronic authentication to provide APEC member economies with guidance when developing policy and legal frameworks to support electronic authentication. The report addresses the issues in general, examines five different groups of technologies and documents how these relate to the issues raised. It also addresses some of the legal issues involved with the use of electronic authentication.

For the purposes of both the eSecurity Task Group and this report, the term ‘electronic authentication’ covers the authentication of individual, organisational and machine identity, roles and attributes. Electronic authentication schemes and technologies may also cover message integrity and non-repudiation in addition to authentication.

---

<sup>1</sup> Asia Pacific Economic Cooperation, Telecommunications Working Group, Business Facilitation Steering Group, *Public Key Authentication Task Group Preliminary Report*, September 1997, <http://www.apectelwg.org/apecdata/telwg/eaTG/eaTG-1.html>

## Electronic Authentication—issues relating to its selection and use

As part of the technology neutral approach<sup>2</sup>, the following terms are used throughout the report, with or without the prefix ‘electronic’:

Authenticator	A parameter, either process or data, for the authentication of individual, organisational or machine identity, roles or attributes that can be applied by a natural person or machine.
Authentication Technology	The technology used to generate, issue or interpret an authenticator.
Authentication Service Provider	A body that generates, issues, receives or stores all or part of an authenticator and might add some further service (for example a certification authority in public key cryptography terms or the holder of a biometric template).
Authentication Scheme	A scheme that involves authenticators and authentication service providers.
Certificate	An electronic document generally issued by a third party that binds an authenticator to a specified user.
Cross-Certification	The practice of recognition of another authentication service provider’s authenticator to an agreed level of confidence and is normally evidenced in a contract or agreement (an extension of the concept used in public key infrastructures).
Cross-Recognition	The practice of recognition of an authentication service provider’s authenticator based on assurance resulting from some form of assessment scheme (an approach developed by this group and discussed in Chapter 3).
High Level Authentication Authority	A body with responsibilities relating to the activities of a number of subordinate authentication service providers (for example a root authority in a public key infrastructure or a government licensing body).

It was also recognised that a number of economies are federations with a number of state or provincial governments that, in some cases may have, or share, legal jurisdiction over all or part of commerce. For that reason the term jurisdiction has been used rather than economy.

A number of alternative approaches are identified, and in some cases detailed, throughout this report. These are only put forward as possible solutions and the eSecurity Task Group does not recommend that member economies adopt these particular approaches. In some cases they will form the basis for further discussion within APEC.

---

<sup>2</sup> The term ‘technology neutral’ means that no particular technology is excluded or given preferential treatment. In the context of this report this means that any technology capable of providing some form of electronic authentication is considered.

## BACKGROUND

Electronic commerce transactions including financial, human resources, registrations, on-line shopping and document exchanges, are invoked through a number of on-line applications such as e-mail, web browsers and electronic data interchange (EDI). As the transition from a paper-based legal framework to electronic means continues, there is an increased urgency to ensure that these transactions are secure and, where appropriate, legally binding and auditable.

Authentication schemes provide the authenticity and, in some cases, integrity of transactions. As governments and private institutions continue to expand their electronic networks to serve the public directly and conduct business with organisations external to their own, the requirement to certify and otherwise establish a level of trust between the organisations becomes more important.

At the 15th meeting of the then Asia Pacific Economic Cooperation (APEC) Telecommunications Working Group (TEL) in March 1997, it was agreed to establish a task group to review and assemble information about international trends in public administration with respect to public key authentication. The then Public Key Authentication Task Group presented its preliminary report to TEL 16 in September 1997.

In September 1998, a workshop on public key authentication and a meeting of the APEC Public Key Authentication Task Group were held in conjunction with APEC TEL 18 in Port Moresby, Papua New Guinea. As a result it was agreed that the task group (renamed the Electronic Authentication Task Group) develop a report expanding on a number of issues identified as being critical to the implementation of electronic authentication. The report would also need to identify any unique needs, either in business models or electronic authentication requirements, in APEC member economies and focus on ensuring cross-border recognition of electronic authentication techniques within the APEC region.

The task group and workshop identified the following issues to be addressed in this report:

- definitions,
- business models,
- user requirements,
- technology,
- trust,
- liability,
- roles of participants,
- interoperability,
- accreditation,
- cultural differences,
- awareness, and
- leadership.

The task group agreed to the preparation of a technology neutral report addressing the main issues relating to the use of electronic authentication. It also agreed to the production of four technology specific chapters addressing the following groupings of technologies:

- asymmetric cryptography,
- shared secrets,
- biometrics, and
- other.

A further two chapters were subsequently requested:

- hybrid technologies, and
- an explanation of cryptography.

The chapters cover how the specific technologies address the issues raised in the main body of the report.

Given the complexity of issues relating to public key infrastructure (PKI) interoperability and the legal issues relating to electronic authentication, these are the subject of separate chapters.

The chapters were presented as a series of papers from TEL 19 to TEL 26.

## DEFINITIONS

The first problem encountered in examining this subject was the question of definitions and terminology. As electronic commerce has evolved certain terms have become synonymous with specific technologies. For example the term digital signatures is generally related to the use of public key cryptography and the term electronic signature is now used to cover all electronic signing processes. Similar problems emerge where a term has different meanings depending on where it is used. The problem became apparent in the preparation of this report as the term ‘certification’ had one meaning in respect of public key infrastructures and another in respect of standards accreditation processes.

In addition as noted in an Organisation for Economic Cooperation and Development (OECD) paper<sup>3</sup> prepared for the 1998 OECD Ministerial Conference in Ottawa, certain terms have come to be used in very specific ways in technical communities but are often used inconsistently in policy discussions.

The International Organization for Standardization and the International Electro-technical Commission Joint Technical Committee on Information Technology, Sub Committee 1, Vocabulary (ISO/IEC JTC1 SC1) has the formal task of standardising the vocabulary for information technology and has produced the ISO/IEC 2382 series of standards.

In many cases a term can have a different meaning depending on its context. It is therefore unlikely that complete consistency can be achieved. There is a role for member economies to contribute to and stimulate work in attempting to achieve the maximum degree of consistency. However, member economies also have a role in encouraging the inclusion of definitions in particular documents. Governments can play a leadership role by adopting this practice for their documents.

## ELECTRONIC BUSINESS MODELS

Electronic business can be categorised on the basis of the environment in which it operates. There are several definitions under discussion in various communities to categorise certification authorities by business model, and this work can be extended to describe business models in general. Some of these definitions are discussed below:

### Open Model

An open model involves the use of electronic authenticators between users who do not have a pre-arranged or organisational relationship covering reliance on the particular authenticator. It assumes there are many parties who may rely on an authenticator but who may not have been known to each other at the time the authenticator was issued.

---

<sup>3</sup> Organisation for Economic Cooperation and Development, *Inventory of Approaches to Authentication and Certification in a Global Networked Society*, Paris, October 1998, [http://www.oecd.org/dsti/sti/it/ec/prod/reg\\_3e.pdf](http://www.oecd.org/dsti/sti/it/ec/prod/reg_3e.pdf)

In typical open models, a user enters into a business contract with a third party based on the exchange of electronic authenticators validated where necessary by reference to a service offered by an authentication service provider (ASP<sup>4</sup>). In this case the parties are independent legal entities although there may be a legal relationship between one of the parties and the authentication service provider.

The classic example of an open model is Internet based business where two parties may enter into a transaction without any prior contact or formal arrangement.

The main advantage of this model is that it allows a business to have an almost unlimited field of potential clients. However establishment of a business relationship typically goes beyond simply authentication of identity and other aspects, such as financial viability and ability to deliver goods, are often established and taken into consideration. These could reduce the 'openness' in many cases.

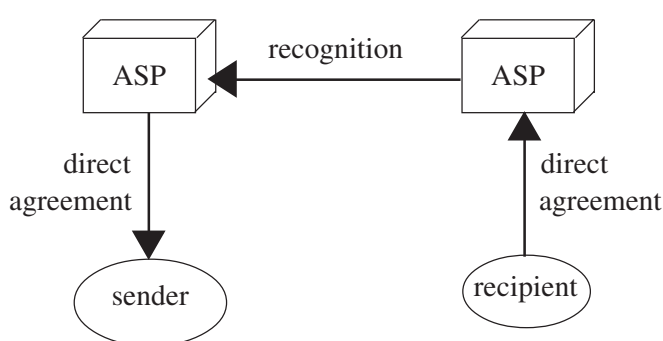


Figure 1: Open Model

## Closed Model

A closed model is one in which authenticators are exchanged between users who have a pre-arranged contractual or organisational relationship that extends to the issue and use of authenticators.

Typical of closed models would be authenticators exchanged internally between employees of a corporation or government (organisational relationship) or authenticators exchanged between users and a hub organisation such as between a business and its customers or suppliers where an agreement on the use of authenticators exists (contractual relationship).

Examples of closed models would be value added networks such as EDI where formal agreements exist; or online merchants who request that a client establish an account. A number of banks have also established closed systems for dealing with their customers.

The main advantages of this model are its simplicity, the fact that the business can retain its relationship with its client, and greater certainty in dealing within established relationships rather than introducing an intermediary.

Within a closed model the absence of a central hub can lead to a complex web of relationships.

---

<sup>4</sup> The acronym ASP is often used to refer to an Application Service Provider. In this report, however, it is used for Authentication Service Provider.

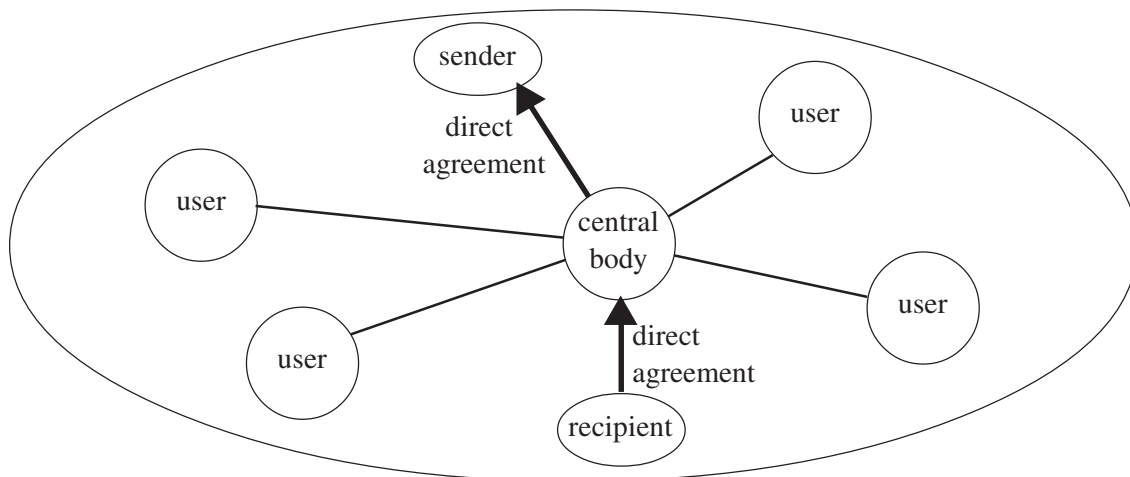


Figure 2(a): Closed Model Example 1

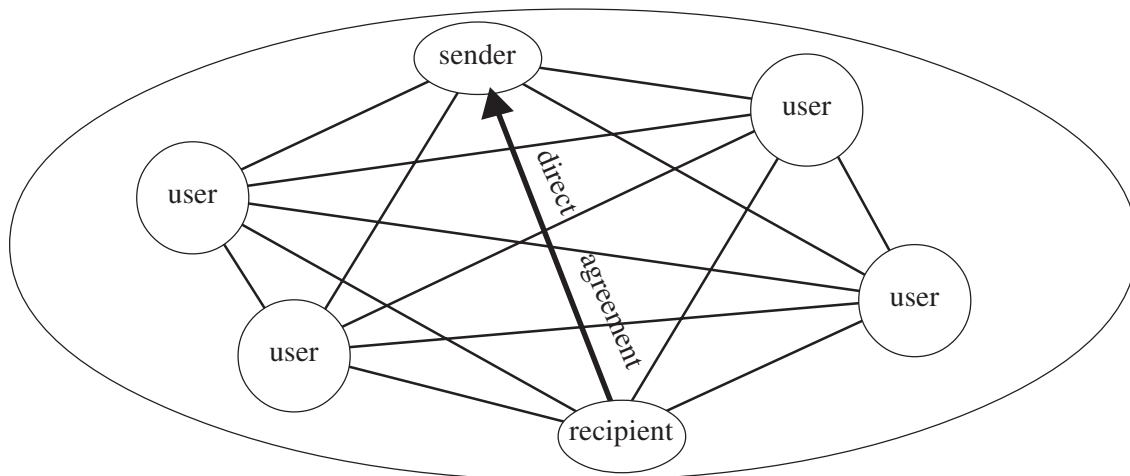


Figure 2(b): Closed Model Example 2

### Open-But-Bounded Model

There is a third model sometimes referred to as open-but-bounded. In this model multiple parties within a bounded community could rely upon an authenticator issued by any one of a number of ASPs within the boundary. The boundary limits the possible number of relying parties. Trust would be gained through an advance agreement by known parties.

In typical open-but-bounded models, a number of relying parties agree to accept an authenticator issued by one or more ASPs.

An example of an open-but-bounded model would be one where a government decides that its clients can use a single authenticator issued by any one of a number of authentication service providers. The authenticator would be recognised by a number of agencies without there being formal agreements in place. This is the model adopted by the Australian Government in its Project Gatekeeper.<sup>5</sup>

A draft paper by Michael Baum, of Verisign (Emeritus), observes<sup>6</sup>:

*A closer look at “open” PKIs in actual commercial practice demonstrates a very different reality. Open PKIs often become constrained, or bounded, just prior to use by relying parties.*

<sup>5</sup> Office of Government Information Technology, *Government Online GATEKEEPER A strategy for public key technology use in the government*; <http://www.ogit.gov.au/gatekeeper/pub/GATEKEEPER.pdf>

<sup>6</sup> Michael S Baum, *Technology Neutrality and Secure Electronic Commerce: Rule Making in the Age of “Equivalence”*, [http://www.verisign.com/repository/pubs/tech\\_neutral/](http://www.verisign.com/repository/pubs/tech_neutral/)

In this case the boundary could be imposed by an ASP by limiting the community that can rely on its certificates.

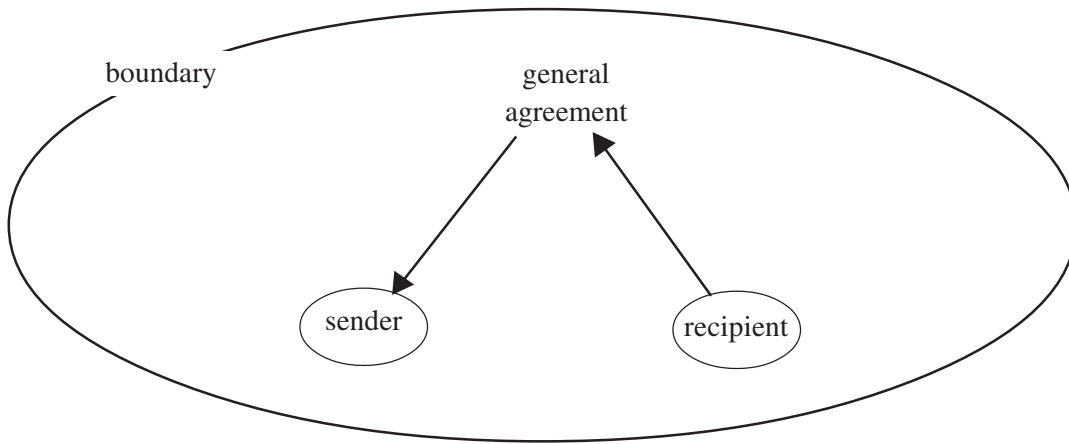


Figure 3(a): Open-but-bounded Model Example 1

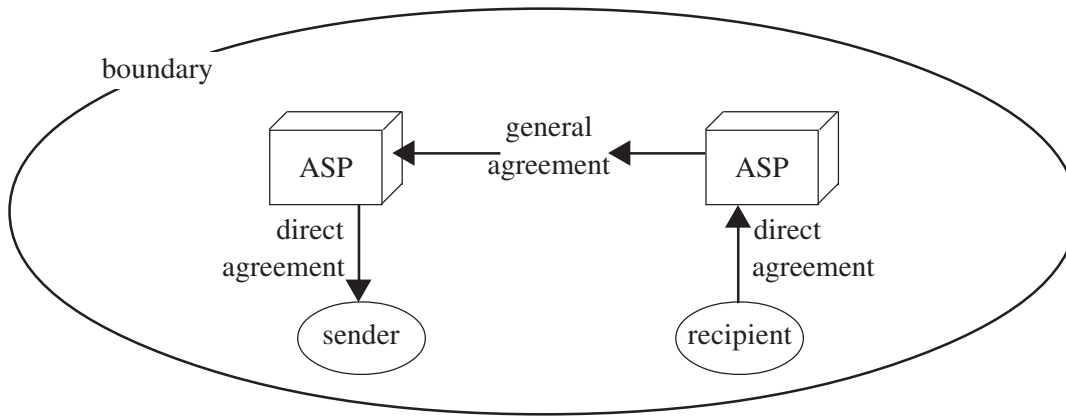


Figure 3(b): Open-But-Bounded Model Example 2

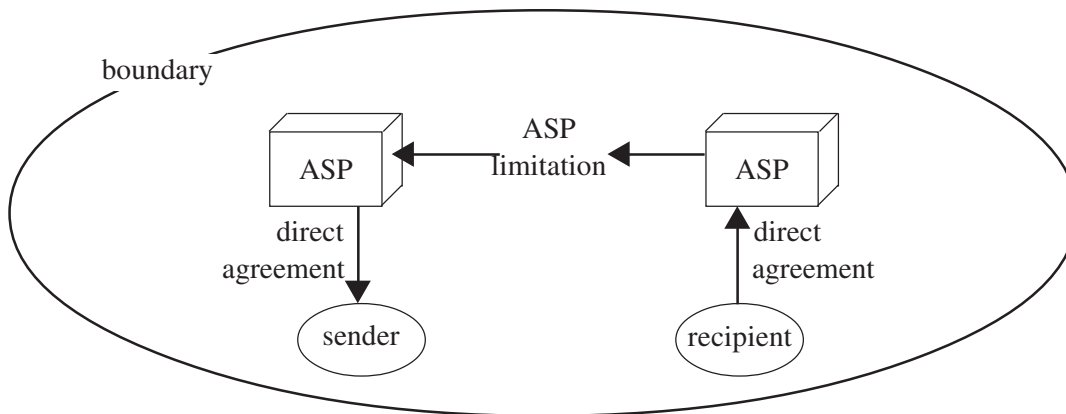


Figure 3(c): Open-But-Bounded Model Example 3

One problem that is becoming apparent, irrespective of the business model, is that in the move to electronic transactions, a number of implementors are assuming that some form of electronic authentication is required. In some cases electronic authentication is being used in transactions where signatures are not used in the equivalent paper process. This can place electronic transactions at a disadvantage, in terms of cost and bandwidth associated with the authenticator and in public acceptance of electronic transactions. While business process re-engineering is an important element in the development of electronic commerce, it is important to ensure that some of these processes do not inadvertently place greater demands on and or costs to businesses and users.

## USER REQUIREMENTS

Most users of electronic commerce do not and will not understand the complexities of the security and authentication services that they require in order to conduct business safely over telecommunications infrastructures.

The one thing that they do realise is that they need confidence in the system that they are using and confidence in the surrounding infrastructure. Further users also need relatively simple and foolproof methods of engaging the security and authentication services that they require.

### Requirements Identified by User Groups

The following is a list of user requirements that has been formulated by the World Electronic Messaging Association (WEMA<sup>7</sup>). This is a grouping of the individual messaging associations from around the world.

- (a) Encryption—it shall be possible to send encrypted messages and attachments though any/multiple service providers.*
- (b) Encryption algorithms—the messaging system shall be capable of en(de)crypting messages using different algorithms and the algorithm shall be transparent to the user.*
- (c) En-route encryption options—there shall be different options for en-route encryption: end to end (User Agent to User Agent) , Link (Message Transfer Agent to Message Transfer Agent) and Network (local user Message Transfer Agent to remote user Message Transfer Agent).*
- (d) Authentication—there shall be bi-directional recognition of authentication. The sender shall be able to authenticate the recipient and the recipient the sender.*
- (e) Repudiation—proof of delivery shall be such that a receiver cannot deny having received a message. Likewise the same sort of proof shall be available such that the sender cannot deny having sent the message.*
- (f) Encryption key lengths—there shall be no restriction on encryption key lengths.*
- (g) Confidentiality—users shall be able to specify that a message is confidential and the service provider shall ensure that the message is encrypted in such a fashion that no access to the message can be made while it is in transport.*
- (h) Traffic patterns—service providers shall not observe user traffic patterns and therefore shall not be able to deduce abnormal activity levels (eg. increased traffic prior to a merger or acquisition).*
- (i) Virus detection—mechanisms shall be provided to protect against and detect viruses contained in message attachments. If a virus is detected the originator and recipient shall be warned.*

---

<sup>7</sup> <http://www.opengroup.org/messaging/wema>



## Chapter 1. General issues relating to the selection and use of electronic authentication

*(j) Mandatory routing—there may be times when it is desirable that a message does not transit through certain countries, or transit through certain service providers. There shall be a mechanism for a user to specify a mandatory route.*

The WEMA group is also working towards making the above requirements a reality.

The Internet Law and Policy Forum developed the following consensus principles<sup>8</sup>:

*Governments should identify and remove legal barriers that hinder the recognition of electronic authentication.*

*An electronic authentication should not be denied legal effect solely because of its electronic form.*

*To the fullest extent possible, national laws and jurisdictions should recognize and give full legal effect to contractual agreements concerning the use and recognition of electronic authentication techniques.*

*Legal rules relating to electronic authentication should be made to operate collaboratively and provide consistent results across jurisdictions to promote the growth of electronic transactions and establish a predictable legal environment for the use and recognition of electronic authentication methods.*

*Governments should recognize that their actions with respect to electronic authentication can create barriers to trade. Governments should not unreasonably discriminate against electronic authentication methods or providers from other jurisdictions or erect improper non-tariff barriers to trade.*

*Governments should not require or unduly promote the use of particular electronic authentication means or technologies.*

*Standards for use of electronic authentication methods or technologies should be market-driven to meet user needs.*

Other business groups are working on defining their own requirements. This gives rise to two potential conflicts. The first is that inconsistencies will develop between perceived needs of the various business groups. The second is that governments will introduce policies and legislation that do not adequately meet the user needs. The need for continued dialogue between the different interests is obvious.

### **Technical Requirements**

More specifically than those items mentioned above, security procedures and authentication should be as transparent as possible for users. A user should be able to readily verify an authenticator incorporated in a message or transaction. Unless this procedure is simple or transparent, most users will not bother.

### **Business Process Requirements**

Users need to be educated in the procedures required to verify information in the electronic world. There needs to be discussion on why and when security procedures are required.

It is incumbent upon business groupings, industry associations and the accounting bodies to ensure consistency in the procedures for the electronic environment just as they have been built up for paper based procedures.

---

<sup>8</sup> <http://www.ilpf.org/events/intlprin.htm>

## Legal requirements

Users need to feel confident that any transactions or messages acted upon which have used correct security procedures will be supported within the legal environment.

## Government Endorsement

Governments need to back the establishment of a global electronic community in which the citizens of each economy can feel that they have the rights and responsibilities they are accustomed to in the normal paper based environment.

## ELECTRONIC AUTHENTICATION TECHNOLOGIES

In examining authentication technologies, the task group identified four groupings as follows:

- asymmetric cryptography,
- shared secrets,
- biometrics, and
- other.

In addition the task group noted there was a trend towards using a combination of several authentication technologies or several uses of the same technology<sup>9</sup>, in a single transaction. The name ‘hybrid’ was attached to this group.

## Asymmetric Cryptography

This group covers public key cryptography that many people see as synonymous with strong electronic authentication. It is also known as digital signature technology. Products in this group provide functions of authentication, integrity, non-repudiation and support confidentiality. Asymmetric cryptography can be used to authenticate identities and attributes and can be used in open, closed or open-but-bounded environments. It can also be used as a tool to ensure the integrity documents without using the authentication capability. Again this can occur in open, closed or open-but-bounded environments. An important element is the existence of public and private components (known as keys) and for access to the secret component to be controlled by the owner. One of the policy issues is the question of control over private keys particularly in respect of key generation which is discussed in the asymmetric cryptography chapter (Chapter 2). This technology is the only one that provides a message integrity capability.

While the concept and some technical implementations are very mature, it is only in recent years that the infrastructures required to support widescale deployment of this technology have started to emerge.

The cryptography tutorial chapter (Chapter 8) contains a tutorial on cryptography, including asymmetric cryptography while the asymmetric cryptography chapter (Chapter 2) contains more detailed discussion on this group of technologies.

---

<sup>9</sup> For example a password can be used to trigger another password as is the case with password ‘wallets’.

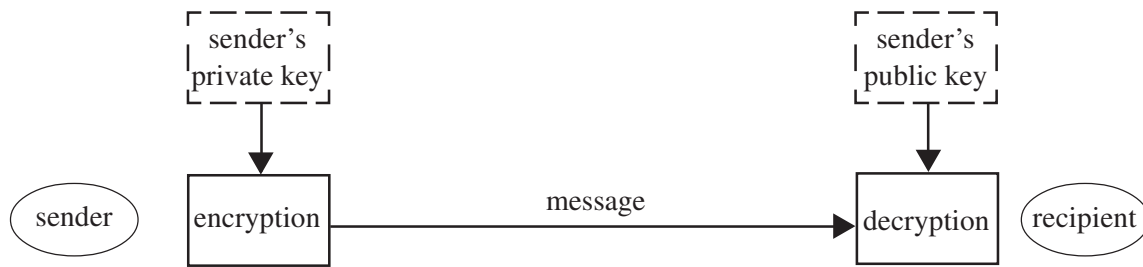


Figure 4: Asymmetric Cryptography

### Shared Secrets

This group covers implementations such as symmetric cryptography, passwords and PINs, and challenge-response. Technologies in this group provide for authentication. However, only symmetric cryptography can provide confidentiality and integrity capabilities in some implementations. Depending on whether the secret is unique to each pair of parties, a degree of non-repudiation may be possible. This group mainly supports closed business models as the secret has to be shared between both parties and there is likely to be some form of associated arrangement. It can, however, support open-but-bounded models through a chaining arrangement where an authenticator in one closed system could generate an authenticator for another closed system. For example Kerberos could be used in this way.

A number of the technologies in this group have been in use for many years. Some businesses have indicated a preference for operating on shared secret technologies at this stage as they are more familiar with the associated business risks.

The shared secrets chapter (Chapter 4) contains more detailed discussion on this group of technologies.

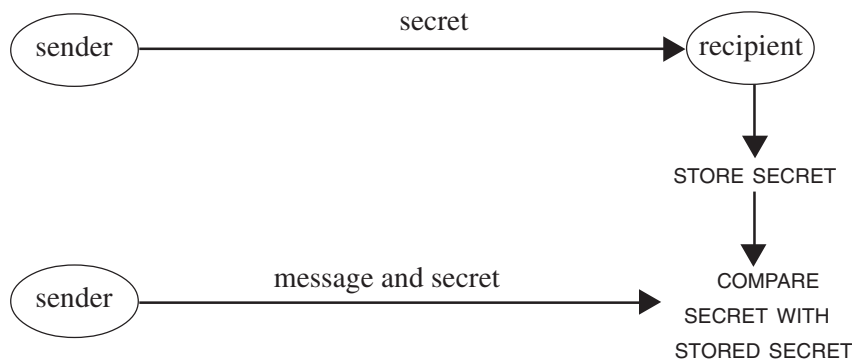


Figure 5: Shared Secret

### Biometrics

This group covers a range of technologies that use personal characteristics as authentication data. It includes fingerprints, hand geometry, retina and iris patterns, signature or keyboard dynamics and voice verification. Other characteristics may be used in the future. Technologies in this group can provide authentication and non-repudiation. Biometrics rely on the recipient being able to compare a biometric with some form of template or the original of the characteristic. However, it is possible for templates to be certified and stored for comparison in the same way as public keys are in asymmetric cryptography. This group could, therefore, support open, closed and open-but-bounded models.

Biometrics have been used for physical access control for many years. However these implementations were closed systems. Heightened problems emerge in the protection of templates in the non-closed electronic environments. A number of implementations are using cryptographic techniques to protect templates and communication of biometric characteristics. For this reason many implementations of the technologies will fall under the hybrid heading.

The biometrics chapter (Chapter 5) contains more detailed discussion on this group of technologies.

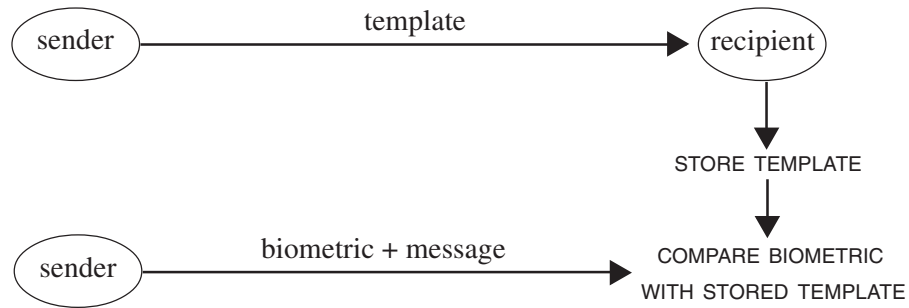


Figure 6: Biometrics

## Other

This group of approaches covers a number of characteristics of a message or transaction rather than specific technologies. These include email address, domain name, IP address, and the signature block on a message. This group only covers authentication but the technologies can be used in open, closed and open-but-bounded models.

Use of authenticators from this group is actually very widespread. It is one of the most common means of authentication currently used, particularly in respect of email. Generally it is used in association with other collateral evidence such as expectation of the communication, shared knowledge of events or introduction by a third party. This results in an aggregation of trust. Its use for high risk and high value transactions can be expected to diminish as the technologies discussed above become more widely available. It will, however, continue to play a part in both low value transactions and in closed systems such as organisational email for the foreseeable future.

The other technologies chapter (Chapter 6) contains more detailed discussion on this group of technologies.

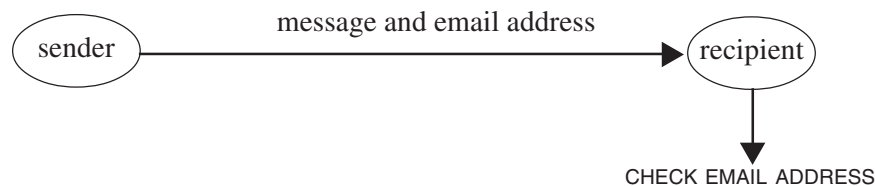


Figure 7: Other Email Address Example

## Hybrid

It is becoming apparent that in a number of instances, several technologies or several uses of a single technology are being utilised in a single transaction. An example is the use of signature dynamics for authentication combined with cryptography for message integrity. Passwords are passed over the Internet using cryptography (eg SSL in browsers) to protect them. Biometrics are being used to trigger a digital signature (asymmetric cryptography) which on receipt generates a Kerberos ticket (symmetric cryptography) to access a particular file. The question is to determine at what point to separate the authentication process from the associated security process. Ultimately that will be a matter for courts to decide and will probably vary from case to case. However the legal and policy frameworks for electronic authentication need to be flexible enough to cover these hybrid technology approaches.

The hybrid technologies chapter (Chapter 7) contains more detailed discussion of these approaches.

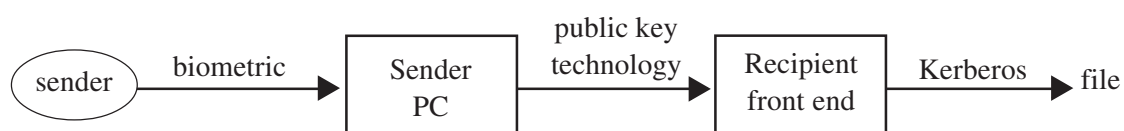


Figure 8: Hybrid Using Three Technologies

## Selection

The selection of the appropriate electronic authentication technology is primarily one of risk management and will vary over time as technologies in the different groups emerge and are superseded. Users will need to examine the assets they are trying to protect and the risk to those assets before selecting the most appropriate technical solution. Other issues would include requirements mandated in legislation or contracts, cost-benefit and integration with other technologies. The decision is one for users and not for government other than where government is in the role of a user. Legal and policy frameworks need to be flexible enough to allow users to make the choice of the most appropriate technology for their purpose. Governments may, however, have a role in ensuring that technologies and their implementations meet their stated objectives and that users are able to make informed choices. These issues are discussed elsewhere in this report.

## CERTIFICATION MODELS

Several of the technologies outlined in the previous section require a third party to certify the identity of the holder of a particular electronic authenticator. As early as 1996<sup>10</sup> distinctions were being made between formal and informal certification approaches. For the purposes of this report three basic certification approaches are considered.

### Formal Certification

This approach generally involves an authentication service provider formally taking on the role of binding a party to a particular electronic authenticator. A number of approaches involve hierarchical structures with each level being certified by a higher element until a trust anchor is reached. For this reason it is also referred to as a chain of trust. These bodies may be established within an organisation

<sup>10</sup> See for example abstract to paper *Let A Thousand (Ten Thousand?) CAs Reign* Stephen Kent, BBN Corporation, <http://jya.com/dimacs.txt>

or may be provided on a commercial basis. The Public Key Infrastructure (PKI) approach is an example of a formal certification approach. PKI approaches can range from small implementations within an organisation to elaborate hierarchical models that can cover millions of key holders. PKI approaches are addressed in more detail in the asymmetric cryptography chapter (Chapter 2). A series of IETF standards, Public-Key Infrastructure (X.509) (pkix)<sup>11</sup>, describe this approach.

It is also possible for biometric templates to be bound to an individual party. This approach is not yet in common use and standards are only now starting to become available.

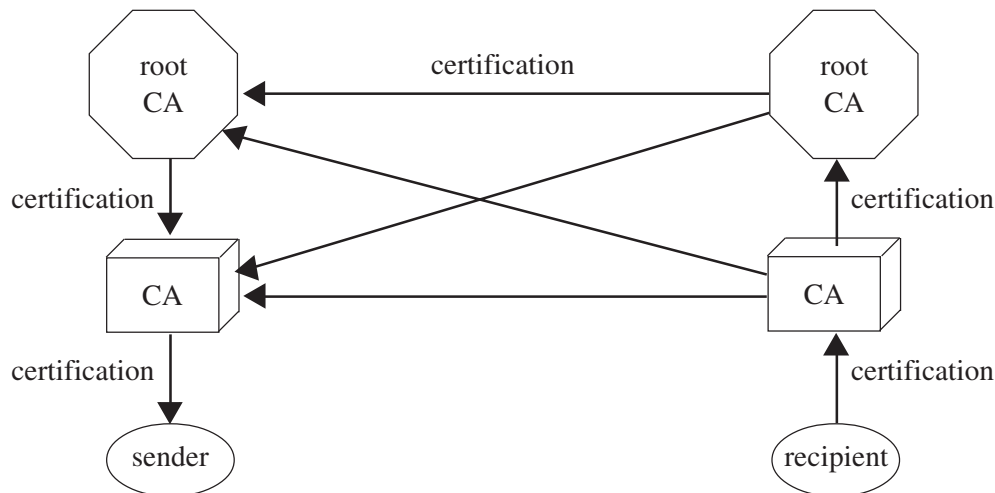


Figure 9: Formal Certification (PKI)

### Informal Certification

This approach generally involves a third party or a number of third parties certifying that an electronic authenticator belongs to a particular party. A relying party checks to see if it trusts one of the certifiers. This technique is used for public keys in approaches such as Simple Distributed Security Infrastructure (SDSI), Simple Public Key Infrastructure (SPKI) and in the PGP suite of products. It does not necessarily rely on the formal hierarchical structure that is common to formal certification and is often referred to as a web of trust. A number of IETF standards, Simple Public Key Infrastructure (SPKI)<sup>12</sup> and PGP<sup>13</sup>, exist for this approach. These approaches are addressed in more detail in the asymmetric cryptography chapter (Chapter 2).

In theory it may be possible to informally certify biometric templates but no examples of such approaches could be found.

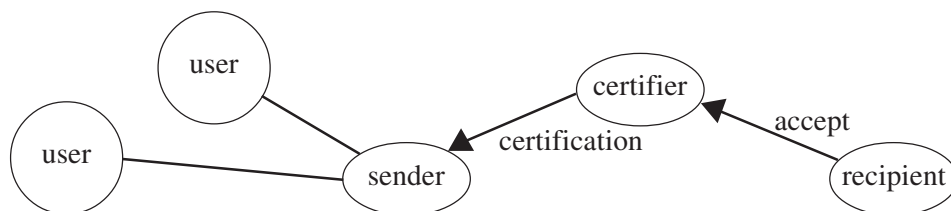


Figure 10: Informal Certification

11 <http://www.ietf.org/html.charters/pkix-charter.html>

12 <http://www.ietf.org/html.charters/spki-charter.html>

13 <http://www.ietf.org/html.charters/openpgp-charter.html>

## No Certification

A number of electronic authentication technologies do not require, or can exist without, any form of certification. Shared secret implementations require the parties to know each other before the secret is shared. Therefore there is no need for certification where this technology is used.

The 'other' group of technologies does not lend itself to the use of either formal or informal certification although it may be argued that some of the 'introductory' aspects such as a party advising a third party's email address does add some element of increased trust when dealing with the third party. As no 'certificate' is created or utilised, this approach has been included in the 'no certification' model.

All authentication technologies can be used without certification.



Figure 11: No Certification

## TRUST

Much has been written about the need to develop user trust or confidence in the new technologies including electronic authentication<sup>14</sup>. This includes trust that the technology can deliver the benefits (economic, productivity) and trust that the user will not be disadvantaged by using it (fraud, privacy, consumer issues).

Trust can be achieved through the deployment of appropriate technology, development of appropriate legal and policy frameworks and development of appropriate business practices. In all cases not only do these elements need to be provided but users need to be aware of them and the issues involved. However in most cases the implementations need to be transparent to users.

Many of the sections of this report are ultimately directed at developing frameworks that will generate user trust. For example, accreditation processes are designed to enable users to trust the technologies while legal frameworks are designed to enable users to trust that they can rely on the legal validity of a transaction or have appropriate redress. Awareness raising programs are designed to build the level of required trust once the appropriate frameworks are in place.

As these elements are discussed in more detail in this report those discussions will not be duplicated here.

## LIABILITY

Liability has been raised as one of the major issues facing users and authentication service providers. This issue is under active consideration in a number of international forums. Central to the discussion is whether governments should legislate in respect of liability, adopt a contractual approach or a combination of both. The issue is complicated by the fact that a number of economies are federations and jurisdiction for liability may rest with state or provincial governments.

---

14 See for example  
Asia Pacific Economic Cooperation, *APEC Economic Leaders Declaration: Connecting the APEC Community*, Vancouver, Canada, November 25, 1997 <http://www.apecsec.org.sg/econlead/vancouver.html>  
Organisation for Economic Cooperation and Development, *Dismantling the barriers to global electronic commerce*, Paris, November 1997, <http://www.oecd.org/dsti/sti/ec/prod/dismantl.htm>



It is likely that different jurisdictions will, at least initially, adopt different approaches. It will be important to ensure that adopting one approach does not prevent transactions with jurisdictions that adopt an alternative approach.

Liability is discussed in more detail in the legal issues chapter (Chapter 9).

## **ROLES OF PARTICIPANTS**

The community of interest applicable to electronic authentication includes:

- governments,
- high level authentication authorities (optional),
- authentication service providers, and
- users.

The term ‘users’ includes end-entities, users and subscribers depending on the terminology used in a particular architecture. They may be independent or associated with a sponsor recognised by an authentication service provider. A sponsor is an organisation with which an end-entity, subscriber, user is affiliated (for example an employee of a firm).

The term ‘relying party’ is used in some system documentation to define the recipient of an authenticator who acts in reliance on that authenticator. By that definition ASPs and users are all relying parties during specific processes and exchanges in a PKI supported system.

All elements of a community of interest have roles particularly in respect of ensuring the assurance of the authentication technology and framework.

### **Governments**

It is the role of government to provide the legal, regulatory and policy frameworks to support electronic authentication. The balance of legal and self-regulatory approaches will vary from jurisdiction to jurisdiction. In some implementations, the activities listed below may be performed by government, in which case it would need to take on the additional roles.

### **High Level Authentication Authorities**

In some cases or for some authentication technologies it may be decided to establish one or more high level authentication authorities. These may be established by government, industry groups or even individual organisations managing one or more authentication service provider. In some cases high level authentication authorities may be involved in the accreditation or licensing of their subsidiary authentication service providers.

Roles of high level authentication authorities could include:

- providing or approving policy and practice statements for subsidiary authentication service providers;
- ensuring compliance with applicable legal provisions, policy and practice statements, and technical standards;
- warranting or guaranteeing the scheme; and
- facilitating cross-certification or cross-recognition as discussed in the next section.



## **Authentication Service Providers**

It is the role of authentication service providers to:

- advise users of the authentication service provider's policy and practice statements;
- make copies of documented cross-certification agreements including relevant policy and practice statements available to subscribers of all certified and cross-certified authentication service providers;
- revoke authenticators and publish revocation lists as required under the relevant policy statement;
- perform the identification and authentication procedures stipulated in the applicable policy statement;
- provide authentication and repository services consistent with the policy statement;
- provide the operational, security and technical controls stipulated in the policy and practice statements;
- comply with all applicable policy and legal provisions; and
- accept liability for damages arising from or in connection with its services to the extent warranted in the relevant agreements or in accordance with relevant laws and regulations.

## **Users**

Users may have roles in ensuring that:

- no unauthorised party has had access to any secret component of an authenticator held by the user;
- all representations made to an authentication service provider in the course of obtaining an authenticator are true and or updated in accordance with agreements; and
- revocations are requested in accordance with agreements.

## **INTEROPERABILITY**

The issue of interoperability means different things to different people. It has been argued in some quarters that we should be aiming for a single globally interoperable scheme. Others support the concept of a number of globally interoperable schemes. As mentioned earlier different technologies will meet different requirements based on risk, cost and integration with other technologies. It is unlikely that the differing requirements can be met by a single scheme without compromising risk at one end or cost at the other. However too many schemes will confuse users, possibly increase costs as users need to implement an excessive number of schemes and leave users with a bewildering array of technologies attached to their systems. The objective should be to minimise the burden on users in order to encourage them to adopt electronic authentication and electronic commerce while maintaining the appropriate level of security. Government and industry need to pursue an appropriate balance in consultation.

Interoperability covers technical interoperability, cross border recognition of legal and policy frameworks supporting transactions and, more specifically, cross-certification within authentication schemes.

A number of these issues were canvassed in the task group's preliminary report and are included here in an updated form.

## **Technical Standards**

International technical standards will be essential for ensuring interoperability of electronic authentication. A number of national and international standards bodies are addressing these issues.

There is the potential for the development of inconsistent standards in these different arenas. In addition, a number of industry sectors are also developing their own systems or products based on proprietary or industry group standards. Clearly there is the potential for short-term problems of interoperability with the various approaches. To be too dogmatic about particular standards, however, has the potential to stifle developments in both the authentication technology and the interoperability processes.

Standards need to be examined at two levels—detailed standards for particular technologies and their use, and standards for interoperability between the different technologies. The former can be developed in isolation to a certain extent, although it is important that interoperability be considered even at that level. The latter must be developed at a full international level. Even regional approaches have the potential for inconsistencies that can cause problems for inter-region interoperability. If this emerges as a significant problem, APEC member economies may need to take a pro-active role in international standards making bodies to ensure full interoperability is achieved.

A number of APEC economies are active in the international standards arena and can assist in progressing these issues in those forums.

### **Cross Border recognition of Legal and Policy Frameworks**

Some see the ideal situation as having consistent legislation across all jurisdictions. However, inconsistencies are already starting to emerge in legislative approaches in different jurisdictions. This problem may be exacerbated in some federal structures where state or provincial governments may adopt legislative approaches inconsistent both between each other and with that of the federal government. In some cases these inconsistencies can be quite significant, for example mandatory use of particular authentication technologies or government licensing of authentication service providers versus a completely free market approach. Other problems may arise from legislation containing inflexible specifications of the technology and procedures that need to be adopted.

Another difficulty which arises is that, whilst particular legislation might be seen to be highly desirable and may be strongly advocated by the technical or business sectors in one economy, such proposed legislation might in practice be unlawful or unenforceable when reviewed against provisions of the constitutions of, or the common laws in, other economies. It is likely that some fundamental legal rights provisions are in fact included in all civil and common law jurisdictions and any proposals to introduce procedures which are not consistent with such fundamental legal rights, however desirable they may be from the technical or business viewpoint, are doomed to failure. For international trade it is essential to consider the legal frameworks of other jurisdictions when developing a legal framework for electronic authentication within individual jurisdictions.

The United Nations Commission on International Trade Law (UNCITRAL) has developed the *Model Law on Electronic Commerce* and the *Model Law on Electronic Signatures*<sup>15</sup> and is undertaking work on electronic contracts. Any significant APEC work on model legislation would be an unnecessary duplication of the work being carried out by UNCITRAL.

A number of APEC economies are active in the UNCITRAL arena and can assist in progressing these issues in that forum.

As highlighted in a number of areas throughout this report, a significant danger to the interoperability of electronic authentication schemes is overly specific or inflexible legislation or regulation. Schemes that mandate particular approaches to the exclusion of all others, be they technical, legal or

---

<sup>15</sup> United Nations Commission on International Trade Law, *Model Law on Electronic Commerce*, New York, June 1996, [http://www.uncitral.org/english/sessions/wg\\_ec/index.htm#TOP](http://www.uncitral.org/english/sessions/wg_ec/index.htm#TOP)

procedural, will not be able to accept authenticators from schemes that do not adopt the same approach. However, schemes that adopt more flexible approaches will be able to accept authenticators from schemes that mandate approaches. This will disadvantage schemes that adopt the mandatory approach in terms of electronic commerce. From the broader perspective, it will establish non-tariff barriers to international interoperability. Having said that, it is still possible to ensure an appropriate level of security while allowing some flexibility in implementation.

In some cases it may be possible to introduce schemes of a particular model for internal use within an economy or within particular industry sectors. The problems emerge when the scheme mandates that particular type of scheme for all transactions regardless of where they originate. This can be overcome by technology neutral legislation which does not specify that a particular technology or process must be used for transactions to be acceptable.

While this somewhat oversimplifies the problem, there will be a need for governments to consider how to achieve national objectives in some of these areas without formulating legislation which would have the effect of precluding varying schemes.

In its preliminary report, the task group recommended further work be carried out with other international organisations. This work can be approached in a number of ways:

- the establishment of a formal liaison mechanism between the secretariats of the various organisations,
- the exchange of official observers for relevant meetings,
- the exchange of draft documents between members of various groups,
- nominating representatives already members of the other bodies to act as liaison points, and
- the conduct of joint meetings, seminars and the like.

In fact a combination of these approaches may be the most appropriate. The important thing is to establish a dialogue with these other bodies to ensure that work is not duplicated, or worse, develops in different directions.

APEC Ministers and senior officials have endorsed international cooperation on e-commerce and electronic authentication. The eSTG has established liaison with the OECD, the European Electronic Signatures Standardization Initiative (EESSI), the Asia PKI Forum and the PKI Forum and regularly shares information with these bodies.

## **Cross-Certification and Cross-Recognition**

There is a requirement to establish a consistent and auditable level of trust between authentication schemes. Formal methods for recognition of authenticators from other schemes known as ‘cross-certification’ are being developed<sup>16</sup>. These schemes are currently being developed for public key infrastructures but the same principles can be used for other authentication service providers that use the same basic authentication technology (such as biometrics).

The process of cross-certification includes legal, technical and policy review of each other’s authentication scheme policies and authentication scheme practice statements, their implementation and operational management. This is to ensure that the authentication service provider of each respective domain agrees and meets the standards as set out in its authentication scheme policy and authentication scheme practice statement and that these are of ‘substantially equivalent level of reliability’<sup>17</sup>. If there is agreement on their equivalence, a formal process leading to a mutual

---

<sup>16</sup> See for example: Electronic Commerce Promotion Council of Japan, Certification Authority Working Group, *Publication of “Exposition of Cross-Certification Technology and Proposed Basic Specification”*, [http://ecom.ecom.or.jp/eng/output/97report\\_summary/wg08-2.htm](http://ecom.ecom.or.jp/eng/output/97report_summary/wg08-2.htm)

<sup>17</sup> This is a test noted in Article 12 of the UNCITRAL Model Law on Electronic Signatures.

agreement in the form of a contract allows the authentication service providers to cross-certify with each other. The process must allow for changes and coordinate these in a timely fashion to prevent interference with organisational programs and business transactions. Cross-certification agreements should have a fixed term and allow for renewal, termination and amendments.

Cross-certification can take place at single or multiple levels of assurance. Programmed site inspection of the cross-certified authentication service provider facilities must occur in order to verify the integrity of the agreements.

The eSTG has developed the concept of cross-recognition. This approach allows users to rely on assessment data for a particular authentication scheme rather than relying on cross-certification at the ASP level or high level authentication authority level. A similar approach, provision of trust status information, is being developed by EESSI. eSTG and EESSI are cooperating on these approaches. Alternative approaches such as ‘bridges’ are also being considered. . The cross-recognition approach is discussed in detail in the PKI interoperability chapter (Chapter 3). Other approaches are discussed in the legal issues chapter (Chapter 9).

A further issue that is starting to emerge is interoperability between authentication technologies and other technologies used in the process of generating, transmitting or receiving secure transactions. We are already starting to see instances where authentication technologies can be rendered ineffective by other technologies. For example firewalls and gateways can reject digital signatures or encrypted messages as they could possibly be maleficent code or contain viruses. There is a need to encourage cooperation between IT and security product developers and implementors to ensure that unnecessary barriers are not erected.

## **ACCREDITATION<sup>18</sup>**

One of the main issues to be addressed is whether government should license or regulate authentication technology or authentication service providers and if so, how. A number of possible scenarios emerge:

- government licensing,
- government endorsed accreditation scheme,
- standards-based accreditation scheme<sup>19</sup>, and
- industry endorsed accreditation, assessment or audit scheme<sup>20</sup>.

Implementation of these schemes can be mandatory or voluntary. The type of approach adopted will vary from jurisdiction to jurisdiction determined largely by domestic policy on issues such as security, industry regulation and consumer protection. Problems will emerge if jurisdictions insist that authentication technologies or service providers satisfy their licensing or accreditation processes and requirements even where the service provider or user of the technology is located outside or has been accredited outside their immediate jurisdiction.

As mentioned at the outset, the key requirement of authentication schemes is to allow the recipient of a message or transaction to make an informed assessment as to whether to accept that transaction or not. To be able to make that judgement, the recipient needs to be aware of the type of accreditation the authentication scheme or technology has received as well as any relevant cross-certification

---

18 For a detailed discussion of the assessment and accreditation process see: Ford and Baum, *Secure Electronic Commerce, 2nd Edition*, Prentice-Hall Publisher, 2002 (Chapter 11). Also published in Chinese and Japanese.

19 Standards based schemes can include industry based standards groups as well as those developed by domestic or international standards making bodies.

20 For example the American Institute of Certified Practicing Accountants SAS 70 and WebTrust for CAs schemes <http://www.aicpa.org> and the American Bar Association PKI Assessment Guidelines <http://www.abanet.org/scitech/ec/isc/home.html> .

information. The means by which accreditation and cross-certification information is conveyed to a recipient needs to be standardised with respect to structure, format and terminology. This is the focus of work in both APEC and EESSI.

### **Authentication Service Providers Accreditation Process**

In both mandatory and voluntary schemes, the chain of confidence in authentication services can be established on a sound footing by developing an effective accreditation and certification system. This system relies on independent judgement being made at each level of the system. In the first instance, the certification bodies make a judgement as to whether the service provider's operations (authentication services for example) complies with a relevant standard. The certification body is judged to be competent to carry out the relevant certification by an accredited body. The certification and accreditation processes are generally both carried out by independent bodies. With such a process in place in two economies, the chain of confidence can then be completed by the accreditation bodies making judgement in the competence of each other's programs.

The criteria against which the service of an applicant is assessed are those outlined in an international or domestic standard, or in a normative document nominated by an accreditation scheme regulatory body.

Depending on the development of standards and other normative documents internationally (or domestically) a service provider could apply for certification in one of the following methods:

- If there is an international or domestic standard available, the applicant can approach an international or domestic certification body to obtain certification in its authentication operations. The evaluation (and the certification) work is carried out by the certification body (or a subcontracted body on behalf of the certification body). Following satisfactory compliance of the relevant criteria or standard, the service provider receives certification to operate within a defined infrastructure as a certified authentication service provider.
- If there are other normative documents available, the applicant can approach the relevant regulatory body for guidance on achieving certification in its authentication operations. The evaluation (and the certification) work is carried out by nominated evaluators on behalf of the regulatory body. Following satisfactory compliance of the relevant criteria or standard the service provider receives certification to operate within a defined infrastructure as a certified authentication service provider.

The following is a step by step guide to the accreditation process used in the standards environment<sup>21</sup>:

- **Identify what goals are required to be achieved.** The typical objectives and goals in applying for certification will be to be more efficient and profitable, produce better services, achieve customer confidence and satisfaction, increase market share, improve communication within the service provider's organisation and reduce costs and liabilities. Identification of what the customers and end users, suppliers, shareholders, community and employees expect of the services will also be beneficial in assessing the need to apply for certification.
- **Service provider registers with the appropriate certification body.** The service provider should contact several certification bodies to find out what is offered, what the likely costs are, the period for which the certification will apply and how frequently they will want to audit the system. Some certification bodies may include an initial pre-assessment in their offer. This can be of major benefit in finding out the current status and what needs to be done. When the service provider

---

<sup>21</sup> The approach detailed here is that used for accreditation against ISO standards.

registers with the certification body, a project coordinator may be appointed by the certification body for liaison, and the relevant documentation detailing certification requirements will also be forwarded.

- **Service provider prepares required documentation for certification.** The service provider should obtain information about the certification criteria and prepare all required documentation and apply the certification criteria to the authentication operations to ensure and demonstrate conformance.
- **Service provider forwards relevant documentation to the certification body for evaluation.** The certification body may carry out the certification work itself or subcontract this work to a recognised evaluator. It may be necessary for certification bodies (or evaluators) to make a number of site visits or reviews of documentation, dependent on the need for further evaluation. For example, a physical security review may recommend changes to locks, doors etc. The service provider will need to carry out any work recommended and be re-evaluated to ensure compliance.
- **The service provider obtains certification from the certification body.** When all criteria has been reviewed to the satisfaction of the certification body, a certificate of certification will be presented to the service provider confirming that it may now advertise, market and operate as a certified service provider within a defined infrastructure. A list of certified service providers may also be published either by the accreditation or the certification body.
- **Certification maintenance.** The service provider will be required to maintain the certification by notifying the certification body of any changes in its services and carrying out a periodic audit as required by the certification body.

### **Authentication Product Accreditation Process**

While accreditation of specific authentication technologies and software packages is part of the process of accrediting an authentication service provider, it can also be applied to the technology software package alone. This may assist in generating user confidence in the products that they, rather than the service provider would be using.

The steps involved are similar to those set out in the section above but would be limited to the product itself.

### **Audit of Policies and Practices**

An alternative or integrated complement to formal accreditation against standardised criteria is an independent audit of the assertions made in a service provider's policies and practices. Such audits and compliance statements can assist users in assessing the reliability of the service being provided. A number of guidelines have been developed to facilitate such audits.

Regardless of whether formal accreditation or another auditor assessment process is used, there is a requirement for ongoing audit or assessment to ensure the ongoing compliance with the criteria or statements.

### **CULTURAL DIFFERENCES**

During the course of its workshop in Port Moresby, and subsequent discussions, the task group has become aware of a number of cultural differences within the APEC region that can affect the way electronic authentication is implemented. The first difference noted involves various concepts of community property rather than identifiable individual or joint ownership of property. The



community property concept can cover extended families or clan, village or tribal groupings. In many cases no single individual is given authority to act on behalf of the community. Many electronic authentication techniques have as central themes the concepts of binding an electronic authenticator to an individual and for the authenticator to be under the control of that individual. It is difficult to translate electronic authentication techniques that rely on the concept of individuals to cultures whose basic concepts are communal. These community property concepts are present in a number of APEC member economies.

The second difference involved the signing process and the means by which agents sign on behalf of the principal. In a number of Asian member economies, chops or seals are used rather than written signatures. A principal can assign an agent signing privileges by providing the chop or seal. In economies where written signatures are used, agents are provided with a written power of attorney by the principal and the agent applies his or her own written signature on behalf of the principal. Similar processes apply in respect of delegated authorities. Again the electronic authentication concept of individual control over an authenticator does not translate to an environment where the cultural approach is the transfer of the signing instrument.

In both the above examples, legal frameworks may be based on the cultural concepts.

These are only examples of cultural differences and have been presented to highlight the need for governments to be sensitive to the existence of cultural differences between economies. These cultural differences have the potential to impact on technical, legal and policy aspects of electronic authentication. Often cultural differences are not addressed in these aspects through ignorance rather than intent. There is a need to raise awareness of both cultural differences and their possible impact.

## **AWARENESS**

Electronic commerce and electronic authentication are still emerging disciplines. The level of awareness of both the technologies and their use is patchy and in many cases fraught with misconceptions. This is particularly the case in respect of the security and reliability of the technologies and their implementation. There is a need to raise awareness among government policy makers, business managers and individual users. In many cases it will be difficult to focus attention on just electronic authentication as a large proportion of the target audience will have wider ranging responsibilities or interests. Strategies for raising awareness of electronic authentication technologies and associated issues will often need to be integrated with broader electronic commerce awareness raising strategies. Specific electronic authentication awareness raising programs can be developed and targeted at selected audiences.

### **Government Awareness**

Government policy makers shape the framework within which electronic authentication will operate. In doing so they need to be aware of the international as well as national environment in which the technologies will be used. In most governments there are a large number of policy makers, very few of whom participate in international discussion of electronic authentication issues. This is particularly true in federal structures where the state or provincial governments are rarely directly involved in the international policy development process. There is a need to give all relevant government policy makers access to information on both national and international issues relating to electronic authentication. An awareness raising strategy could include newsletters, seminars, workshops and information resources.

Seminars and workshops need to be conducted at both the national and international level with the aim of meeting national objectives while ensuring cross border recognition of laws and policies. As

mentioned earlier some of these activities need to address electronic commerce in general with electronic authentication as a component, while others need to be specifically designed to address electronic authentication issues in some detail. Part of the strategy would be to identify a high level champion to encourage attendance at these seminars and workshops.

In keeping with the electronic nature of the subject, electronic media can be used for awareness raising. There are already numerous electronic resources, newsletters and list servers dealing with electronic commerce and electronic authentication. The main problem is finding them. One project this task group has been asked to carry out is to establish a website that provides links to resources on electronic authentication. This website could be developed in cooperation with other international bodies.

Governments will not be able to carry out the leadership role nor develop user confidence unless they are able to convince their constituents that they have the necessary awareness of the issues and have developed appropriate responses.

### **Business Awareness**

Governments have an interest in encouraging the uptake of electronic commerce to obtain the associated economic advantages for the economy. Industry bodies have an interest through their role of maximising the efficiency and profitability of their members. These outcomes can only be achieved if business recognises the advantages of the new technologies and has the confidence to use them.

To achieve these outcomes, there are a number of areas where business awareness needs to be raised. These include awareness of the role of electronic authentication in supporting the business advantages of electronic commerce, awareness of the available electronic authentication technologies and their implementation, and awareness of the government and industry group frameworks to support electronic authentication.

As mentioned earlier both governments and industry have an interest in promoting the new technologies. It would be appropriate for awareness raising strategies to be developed as a cooperative activity between the two. The identification of champions within industry sectors to carry the message to their colleagues is another important element.

One example of the broad role that governments can play is the former Australian National Electronic Authentication Council (NEAC) which involved government, industry and users. Its role was described as<sup>22</sup>:

*In particular, NEAC will provide a national focal point on authentication matters, encourage interoperability between different systems and the development of relevant technical standards and provide information and advice to industry, government and consumers.*

The small business seminars on electronic commerce conducted by Australia Oceania Electronic Marketplace Association (AOEMA) in a number of economies under the auspices of APEC TEL are a good example of the type of business awareness raising programs that can be implemented.

In addition to the information resources and seminars and workshop approaches discussed in the previous section, another awareness raising activity is pilot projects. Business may be more prepared to participate in a pilot activity than to commit to something in isolation. Experiences from a pilot would increase their awareness and also that of their peers and clients and can contribute significantly

---

<sup>22</sup> Minister for Communications, Information Technology and the Arts, *New e-commerce authentication council members announced*, Press Release, 17 September, 1999, [http://www.dcita.gov.au/nsapi-text/?Mlval=dca\\_dispdoc&ID=4330&template+Newsroom](http://www.dcita.gov.au/nsapi-text/?Mlval=dca_dispdoc&ID=4330&template+Newsroom)



to awareness raising on a sectoral or industry group basis. A number of pilots are being conducted in and between APEC economies and some are reported to APEC TEL. These reports can provide a valuable awareness raising resource.

As with government, awareness raising is part of the leadership role of business.

### **Individual User Awareness**

There is still considerable apprehension and misconception among individual users on the subject of both electronic commerce and electronic authentication. Much of this relates to the security of their transactions and payments. Unless this is overcome they will not utilise the new technologies.

While there are a number of focal points for government and business through which awareness raising campaigns can be directed, this is not the case for individuals. Any strategy for this group needs to have two elements. First, there is a need to raise the awareness of and obtain support from key representative associations, such as user groups and consumer groups. Second, there is a need for broadcast campaigns through various media channels, building on support from representative groups where appropriate. Representative groups should be included in any awareness raising strategy group.

Word of mouth is still an important tool in awareness raising, both in a positive and negative sense. An individual's experience in use of electronic authentication can influence the decisions of a number of associates. A negative impression will spread faster than a positive. It is important for business to recognise that failures, even in pilot projects, have an awareness raising impact.

The importance of information on the level of security offered in respect of payment systems, which would include the authentication technique, is raised by the OECD in its Guidelines for Consumer Protection in the Context of Electronic Commerce<sup>23</sup> which include the following guideline:

*Consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms provide.*

Inclusion of such information can raise awareness of the technologies and confidence in their use.

For a comprehensive comparison of the relative strengths and weaknesses of several forms of PKI alongside other forms of electronic authentication, see the article *Comparison of authentication technologies in e-business* in the Asia Business Law Review, number 22, July 2001.

## **LEADERSHIP**

The leadership required to encourage the practical usage of electronic authentication clearly will vary according to the circumstance within each economy. The following suggests some of the initiatives that may be appropriate. Broadly, leadership is required from:

- governments,
- international organisations,
- business corporations,
- users and user groups, and
- IT industry.

### **Governments**

The first critical requirement is that governments should publish as early as possible their overall policies with regard to the establishment of authentication schemes. Such policies need not initially

---

<sup>23</sup> Organisation for Economic Cooperation and Development, *Guidelines for Consumer Protection in the Context of Electronic Commerce*, 9 December 1999, <http://www1.oecd.org/publications/e-book/9300023E.PDF>

be too detailed, but their complete absence will seriously impede many related developments. The private sector, and indeed government departments, cannot make their own plans with any certainty, and surely will be reluctant to invest scarce capital resources without the reasonable probability that their own authentication scheme will integrate smoothly into whatever it is that the government proposes.

Possible government policy models can be very different.

- Government may decide to leave the authentication arena wide open. Government may or may not establish one or more authentication schemes within its own departments and related organisations, the private sector being free to set up authentication schemes, commercial or otherwise, as it sees fit. There would be no mandatory high-level authentication authority and authentication service providers would be responsible for ensuring interoperability with other service providers, domestically and internationally, depending upon the objectives in establishing that authentication scheme. No licensing or technology approvals of authentication service providers would be required, save for the usual consumer protection regulations.
- Government may decide to establish either a voluntary or mandatory high level authentication authority. In this case other authentication service providers may find the necessity to interoperate with the high level authentication authority if they wish to have their authenticator accepted outside their own systems. In this case, the technical and management specifications of the authentication service providers must be published as quickly as possible so that both government departments and the private sector may plan accordingly. Licensing and technology approvals for each authentication service provider could be required.
- Government may decide to establish one central and national authentication service provider to the exclusion of any others within the economy, except perhaps for some special purpose authentication service providers established with government approval.

## **International Organisations**

Appropriate international organisations try to monitor developments in various economies and should regularly issue policy advice papers to all governments setting out the advantages and disadvantages of adopting particular policies, based on actual experience of successes and failures.

Such international organisations need to play a coordinating role to assist economies to establish authentication schemes under such economies' control to interoperate with authentication schemes that are not under their control.

Some international bodies are standards making bodies, and where required they should reach an early consensus on authentication standards and publish them as soon as possible. Given the rapid evolution of technology in the electronic authentication field, the standards making process will be a continuous and iterative process.

## **Business Corporations**

Business corporations, being major users of authentication schemes, generally have a particular responsibility to adopt schemes that are compatible, where appropriate, with the authentication schemes being adopted internationally. Exceptions occur where the business case indicates that a closed system using non-standardised techniques is a better approach.

In particular, business corporations should seek not to impose their authentication schemes on their trading partners, unless such schemes are compatible with the internationally accepted schemes.

## Users and User Groups

Individual users and their representative groups have a role to play in encouraging the uptake of electronic commerce and electronic authentication. Personal recommendations by individual users carry significant weight. These views can be built on by user groups who can make appropriate recommendations. On the other hand any adverse experiences and associated publicity can have a devastating effect on development.

Governments and industry need to work with users and user groups to ensure that proposals meet user requirements and users will take an appropriate leadership role in encouraging user uptake.

## IT Industry

The IT industry has a leadership role through the development of innovative and competitive authentication products. The IT industry, especially the developers of authentication products, must also strive towards, and take active steps to try to achieve, international interoperability.

It should be a guiding development principle that if a developer introduces an authentication technology that is, of itself, not interoperable with internationally accepted schemes, then that developer should ensure that its product is equipped with effective gateways to ensure international interoperability. It should not be necessary for the user of an internationally accepted authentication scheme to have to modify its international scheme in order to accommodate the non-international scheme.

## CONCLUSION

It was not the objective of the task group to make specific recommendations in this report. Rather the report has been prepared to identify relevant issues for APEC member economies and the various working groups of APEC that will need to consider these issues and develop options in consultation with the wider international community. However a number of points raised by the Task Group have been adopted by the TEL or ministers.

At APEC TEL 18 the following points were adopted<sup>24</sup>:

*APEC supports the concept of market driven development of business models and authentication technologies.*

*Governments can, through their use of various business models and authentication technologies, lead by example in the use of these models and technologies.*

*Member economies should adopt policy and regulatory approaches which ensure a neutral approach to both business models and authentication technologies used in electronic commerce.*

The fourth APEC ministerial meeting of the telecommunications and information industry adopted a Programme of Action<sup>25</sup> that included the following points proposed by the then Electronic Authentication Task Group (now the eSecurity Task Group):

*There is a variety of business models, authentication technologies, and implementations of electronic commerce. There should be free choice of these models, technologies and implementations.*

*It should be recognised that in authenticating an electronic transaction multiple technologies may be used.*

---

<sup>24</sup> <http://www.apectelwg.org/apecdata/telwg/18tel/report/18file-2.html>

<sup>25</sup> <http://www.apectelwg.org/apec/are/telminsub02.html>

## Electronic Authentication—issues relating to its selection and use

*When developing legal and policy frameworks, consideration should be given to the role of multiple technologies.*

*Legal and policy frameworks that focus on specific technologies can impede the use of multiple technologies.*

At TEL 23 the following point was adopted<sup>26</sup>:

*When framing laws, policies and standards, economies should be aware that formatting and protocol requirements of electronic messaging systems may invalidate digital signatures attached to original messages.*

---

<sup>26</sup> [http://www.apectelwg.org/apecdata/telwg/23tel/plenary/plen\\_33.doc](http://www.apectelwg.org/apecdata/telwg/23tel/plenary/plen_33.doc)

## Chapter 2

# Asymmetric (public key) cryptography

Asymmetric cryptography is one of the most widespread and mature types of electronic authentication used in electronic commerce today. This chapter deals with three concepts:

- Public key technology (PKT) which is the technical implementation of asymmetric cryptography;
- digital signatures which are a specific implementation of PKT providing authentication, integrity and non-repudiation; and
- Public key infrastructure (PKI) which is the framework established to support some implementations of PKT.

Two separate approaches are possible with a PKI:

- certification of public keys to allow users to authenticate themselves, sometimes through the use of digital signatures, and
- certification of public keys to facilitate secure symmetric key exchange to protect the confidentiality of information.

The OECD in its Cryptography Policy Guidelines<sup>1</sup> recognised

*that the use of cryptography to ensure integrity of data, including authentication and non-repudiation mechanisms, is distinct from its use to ensure confidentiality of data, and that each of these uses presents different issues.*

This chapter only addresses the first approach. The second approach can be used to protect the confidentiality of another authenticator. This use is discussed in the hybrid technology chapter (Chapter 7).

PKT forms the basis of most standard Internet security techniques, including:

- Secure Sockets Layer (SSL) for securing transactions between browsers and web sites,
- S/MIME for securing e-mail,
- PGP also for securing e-mail,
- Virtual private networks (VPNs),
- Wireless Application Protocol (WAP) for web-like services to mobile phones,
- Secure Electronic Transactions (SET), an out-dated protocol for credit cards on-line, and
- Visa 3D, a new replacement for SET.

---

<sup>1</sup> <http://www.oecd.org/EN/document/0,,EN-document-43-nodirectorate-no-24-10242-13,00.html>

This chapter canvasses the major issues in the use of PKT for authentication, in the interests of helping economies make informed decisions about the potential application of PKT in their electronic commerce applications. These issues include certification authority models, the responsibilities of all players, types of asymmetric key pair generation, security of private and public keys, and liability of certification authorities (CAs).

While PKT is mature and widespread in commercial Internet applications, PKI schemes around the world are still in their infancy. One reason for this is that PKT implementations have tended to be application or market specific, which limits the scope and extent of the associated PKI. For example, different relatively small scale PKIs might be dedicated to securing B2B banking applications, or healthcare transactions, or B2G tax reporting.

Another reason is that a number of major debates are still taking place, especially concerning liability of CAs, cross domain recognition of certificates, and methods for establishing the reliability of CAs. Many users including business people find these debates confusing, and some have decided not to commit to PKT until the debates have been resolved. For anyone evaluating large-scale deployment of PKT, it is important to understand these debates.

This chapter is for the most part non-technical, although a working knowledge of the principles and operation of asymmetric cryptography is assumed. For technical background on cryptography, please refer to the cryptography tutorial in Chapter 8.

Given the complexity of the issues involved with PKI interoperability, and the extensive work that has been done on it, PKI interoperability is discussed in a separate chapter (Chapter 3). Interoperability issues relating to PKT are discussed in this chapter.

## DEFINITIONS

The following plain language definitions have been derived from practical business experience, and are intended to give economies a better understanding of how the concepts apply in business. In some cases, technical definitions from international standards are also provided, where noted.

- |                         |   |
|-------------------------|---|
| Certificate             | A mechanism for publicising public keys in such a way that vouchsafes either their owners' identities, credentials or both; an electronic document issued by a certification authority (CA), that includes the owner's name, their public key, an indication of the certificate policy (CP) under which it was issued, and the name of the CA. The certificate is digitally signed by the CA, making it tamper resistant and providing non-repudiation of its issuance. In most open PKI systems, certificate format is governed by the X.509 standard. Proprietary vendor standards for digital identities may also apply.       |
| Certificate Policy (CP) | <i>A named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements (X.509); a document which specifies the rules and conditions under which a certificate is issued and intended to be used.</i><br><br>The CP forms the basis of any legal relationship between the CA and its subjects and relying parties. It broadly states what a CA does and is typically published by the CA. The CP should include the intended purpose of the certificates, the conditions for their use, and the identification requirements for recipients. |

## Chapter 2. Asymmetric (public key) cryptography

Certification Authority (CA)	<p>An entity responsible for the overall process of vouchsafing the identity, credentials of users or both and issuing them with digital certificates that bind their public key to their identity.</p> <p><i>A party trusted to vouch for the binding between names or identities and public keys. [The Object Management Group, 'CORBA services', OMG Publications, 1997, Chapter 15.]</i></p>
Certification Practice Statement (CPS)	<p>A document that defines the procedures under which a given CA will operate.</p> <p>The CPS broadly states how a CA performs its duties (whereas the certificate policy states what it does). The CPS may remain confidential to the CA. It should include the technical specifications of the CA systems, and all personnel and physical security measures undertaken at the CA.</p> <p><i>A statement of the practices which a certification authority employs in issuing certificates. [American Bar Association; Internet Engineering Task Force RFC2527]</i></p>
Intermediate Certification Authority (ICA)	<p>A 'higher level' certification authority which in some PKIs is responsible for certifying the compliance of lower CAs with their respective policies and practices, and other standards. An ICA does not necessarily create policies; c.f. PCA).</p>
Policy Creating Authority (PCA)	<p>A 'higher level' certification authority which in some PKIs is responsible for writing certificate policies for the benefit of 'lower' CAs.</p>
Public Key Infrastructure	<p>A system of processes, trained personnel, cryptographic technologies and controls, for managing the large-scale deployment of digital certificates.</p>
Public Key	<p>The part of an asymmetric key pair that is revealed by the owner.</p>
Private Key	<p>The part of an asymmetric key pair that is not revealed by the owner. Note that strictly speaking the term secret key is different, in that it refers to a symmetric key.</p>
Trust Anchor	<p>Any given CA in a certificate chain which a relying party elects to trust, such that certificates issued by any CA below the trust anchor are trusted. Thus, a certificate chain need not be parsed beyond the trust anchor.</p> <p>Trust anchor is a more accurate term than root CA in many cases, since technically there should only ever be one root, yet many web applications support a database of multiple roots.</p>



## TECHNOLOGY

There are a number of proprietary implementations of public key technology. For that reason this section address the functionality which the technology is designed to achieve rather than the individual approaches.

### Major algorithms

The various implementations use asymmetric cryptography and hash functions as described in Chapter 8. Two major asymmetric cryptography algorithms are in use today.

- **RSA** (named for its three inventors, the cryptographers Rivest, Shamir and Adelman) is by far the dominant algorithm, used in all commercial SSL, S/MIME and PGP-related applications (that is, all WWW website authentication and secure e-mail products). The algorithm is based upon the mathematics of large prime numbers and uses relatively long keys. The most common commercial key lengths are 512 and 768 bits, but 1024 and 2048 bit keys are increasingly becoming available.
- **DSA** (Digital Signature Algorithm)<sup>2</sup> is a newer technique specially designed for digital signatures, as opposed to general asymmetric cryptography. DSA is based on the mathematics of discrete logarithms. It is preferred for technical reasons by many governments, because it is said that DSA cannot be used for practical message encryption. DSA is not yet widely supported commercially.

The newest public key technique of any significance is so-called elliptic curve cryptography (ECC). Little or no commercial use has yet been made of ECC but it has the promise of much reduced signature key lengths and therefore faster performance and better token storage capacity.

There are two major hash functions or algorithms.

- **MD5** (Message Digest 5) produces a 128-bit message digest or hash of the message.
- **SHA** (Secure Hash Algorithm) produces a 160-bit hash of the message. It is designed to be used with DSA.

Regardless of the algorithm used, a party (Alice, for example) must generate or obtain a key pair and register the public key of that key pair with a certification authority. The CA then manufactures a certificate containing the public key and provides a copy to Alice and also places a copy in a certificate database known as a directory or repository. Alice keeps the private key securely.

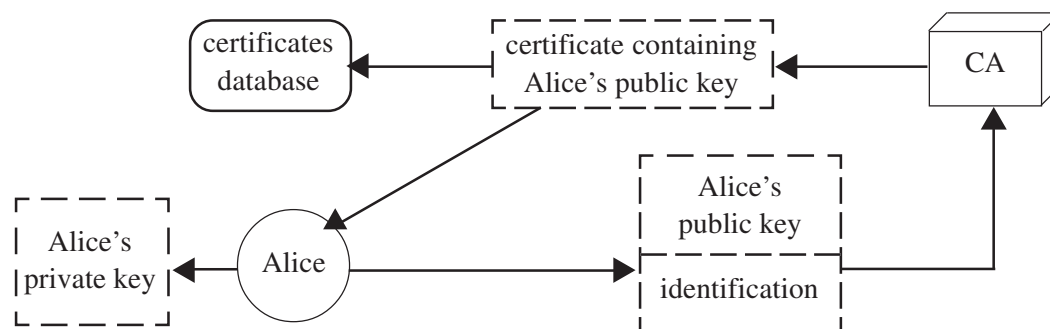


Figure 12: Registration and Certificate Issue

In web of trust implementations discussed below, the certification process may be carried out by an 'introducer' instead of a CA. In that case there may not be a formal certificate or certificate database.

<sup>2</sup> <http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf>



If Alice has reason to believe her private key has been compromised she can ask the CA to revoke the certificate associated with the public key. The CA notifies revocation by including it in a directory known as a certificate revocation list. In some cases Alice may need to provide identification to prevent spurious revocation. In some implementations an interim step which suspends the certificate may also be involved.

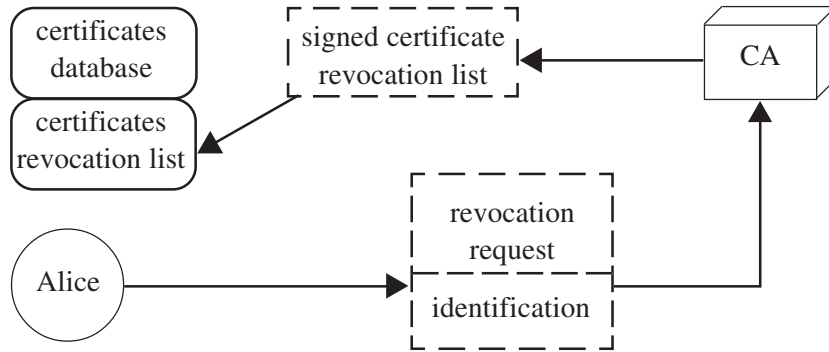


Figure 13: Certificate Revocation

When a relying party, Bob, receives a transaction from Alice, Bob validates the certificate by checking the directory and certificate revocation list in addition to checking the integrity of the message by comparing the message hash with the decrypted version of the encrypted message hash signed by Alice.

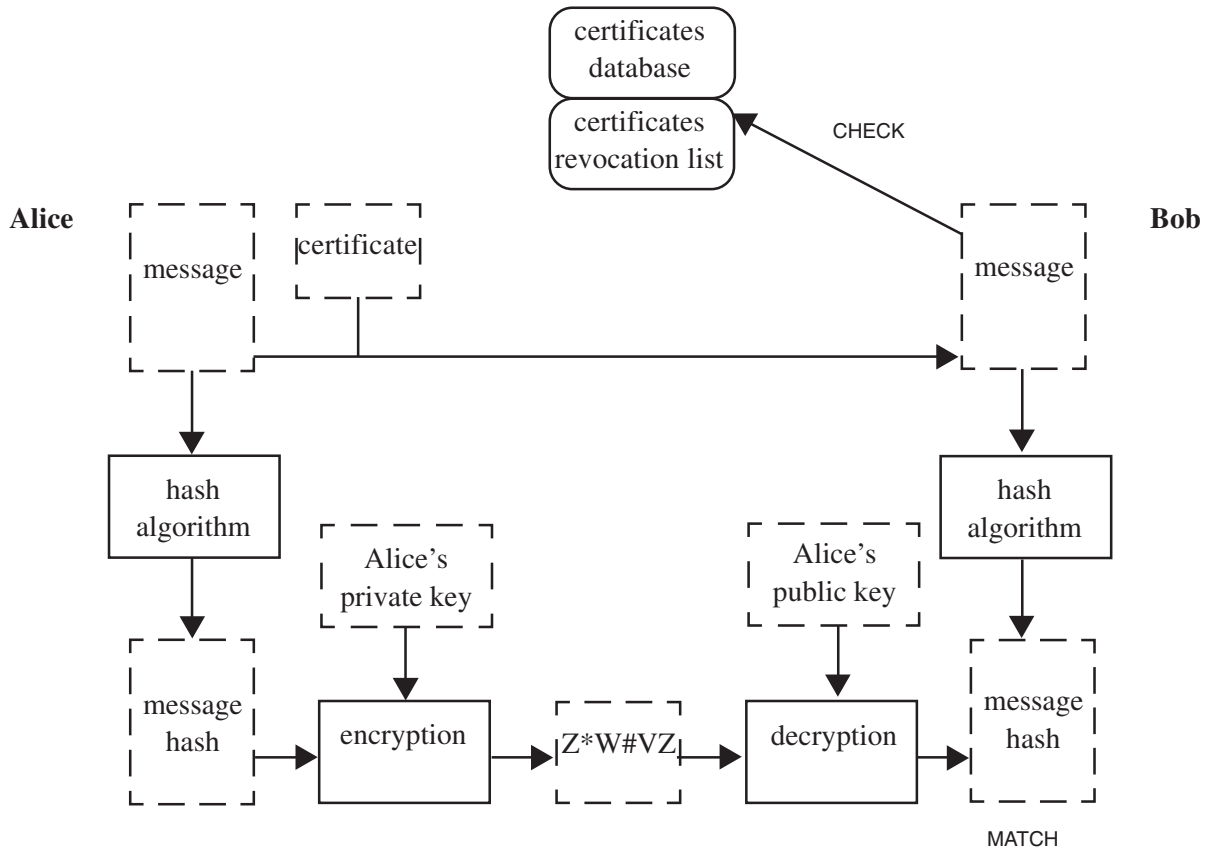


Figure 14: Certificate Validation

The elements of this process are key generation, identification (registration), certificate manufacture, certificate revocation, directory services and message validation.

## Key Generation

The style of key pair generation is a fundamental issue in PKT schemes, for the strength of non-repudiation depends upon assurance that nobody other than its owner has access to a private key. There are two basic modes of key generation: central generation (where the CA or similar entity generates a key pair on behalf of the subject) and user generation (where the subject generates their key pair for themselves). A third mode has recently become available in the form of crypto tokens. This mode shares many of the properties of user generation but will be treated separately below.

### Central Key Generation

For the purposes of discussion, in the centralised generation model, the example of the CA generating the user's key pair is used. However, it is possible for the CA to have a further entity actually create the key pair and forward it securely to the CA or the user (an RA could generate and issue at the time of registration). The principles of central key generation are the same whether the CA generates the keys or whether a specialised entity does it.

Historically CAs have performed key generation because it has been regarded as a specialist function, beyond the capabilities of the users themselves. The advent of SSL-capable browsers has made key generation software widely available at the desktop. There is an argument that commercial key generation software is generally of uncertain quality and that it is still better for the CA to generate the user's keys. However, this argument in practice is flawed as discussed in the Trust Section below.

When the CA generates the user's key pair, the CA must transport the private key using a secure method of transmission, separate from the public key certificate. Transport may be by encrypted e-mail or other electronic transmission, a PIN- or password-secured diskette, or may involve the use of a token. Thereafter, the user is responsible for the safe keeping of their private key.

The advantages of central key generation are as follows:

- assurance that the key pairs, being generated in the sophisticated environment of a central trusted authority, have been properly generated and are of a certain quality;
- simple from the user's point of view;
- better administrative control over the generation and distribution of the keys, and over revocation and replacement when necessary.

The main disadvantage of central key generation is that because their private keys originated in an environment outside their own control, the users may be able to repudiate digital signatures. The argument could be:

*I do not dispute that the digital signature in question was created using my private key, since it validates using my public key. But I myself did not use my private key to create that signature—somebody else using my private key must have created the signature. From the moment it came into my possession, I have carefully safeguarded my private key, so whoever used my private key to create the signature must have copied it before I received it. Since I have no control over the systems and staff used by the CA to create the key pair and to transmit the private key to me, my contention is that sometime during the generation or distribution procedures my private key was illicitly copied and was subsequently used to create the signature in dispute.*

### User Key Generation

In the user generation model, users generate the key pair for themselves, using software and hardware tools under their control. Users subsequently store their private key securely, so that it never leaves their possession or control. The users have to provide the matching public key to an RA or CA, along with the required proof of identity or credentials.

The main advantage of user key generation is that since the key pair has been generated under their own control, the user can be held entirely responsible for the process and for the subsequent security of the private key. The user is therefore less able to repudiate their digital signature on the basis that someone else may be presumed to have a copy of the private key.

The disadvantages of user key generation are as follows:

- Historically the key generation procedure and the subsequent transmission of the public key to the RA or CA may be excessively complex for the average user.
- There is the possibility that key generation software becomes corrupted or that non-standard or inferior software is used, and thus the key pair may not be properly generated and may not be secure. Note however that trusted key generation packages are available which sign the keys they create, thus providing assurance of quality.

### Token Key Generation

The main advantage of user key generation is that, in principle, it ensures that nobody other than the user ever has access to their private key. This property can also be achieved by the use of newly available cryptographic tokens. Cryptographic devices with the same functionality as smartcards (that is, private key storage and ideally private-public key pair generation) are now available in different 'form factors' which allow them to be used in existing input-output ports rather than requiring specialist readers. Most common is the USB token or 'dongle' which can be used with the standard universal serial bus connection. These tokens may not be as robust as smartcards over the long term at present, but are far more portable, and offer the same information security features. Some tokens have the ability to securely generate a public-private key pair within the token chip and to subsequently perform all private key operations also within the chip. This means that the private key never leaves the secure environment of the token. A CA's operations can be designed so that personalisation of the token, including key generation, can be linked to user registration and token delivery, so that only the user ever has control over the private key held within.

Key generation has only recently become practical in tokens because it requires substantial processing power and memory capacity. Even now, few tokens feature secure key generation performed entirely within the chip. Scheme operators and users need to take care evaluating device specifications if they intend to use cryptographic tokens.

The advantages of token key generation are as follows:

- Key generation is, in effect, entirely under the control of the user and so strong non-repudiation of the user's digital signature is achieved.
- If the private key never leaves the token, then unapprehended theft of the key is much less likely than in the case of disk storage (see Private Key Hygiene in the Trust Section below).

The disadvantages of token key generation are as follows:

- Tokens with secure key generation are still relatively expensive, though prices will fall.
- Smartcard readers have yet to become widely available and in most cases scheme operators or users must pay for readers over and above their normal computer hardware. This is not an issue with USB tokens.

- Despite their theoretical advantages, tokens are still vulnerable to several types of attack, ranging from sophisticated hacking of token reader firmware, to mundane theft of tokens and PINs. At face value, tokens are a compelling solution to the key generation and key hygiene problems but users and scheme operators must take care not to take the advantages for granted. As with any security system, care must be taken to achieve the full benefits tokens have to offer.

### Summary of Key Generation Issues

In evaluating key generation options, it is suggested that parties:

- pay careful attention to the issues surrounding central and user generation of key pairs;
- give preference to schemes that give users a choice of generation modes;
- encourage CAs to include information in their certificates, CP or CPS on how the related key pair was generated and the software, hardware and security environment of such generation (CP may be better unless it becomes a standardised extension.);
- encourage the development of user generation systems that are easy and friendly to use, and that will generate acceptable quality key pairs.

### Private Key Storage Media

Private keys are basically data and may theoretically be held on any storage media. In practice, end user keys are held on either diskette or hard disk drive, or on hardware tokens. Many electronic commerce systems also use embedded keys, installed within dedicated hardware such as automatic teller machines.

The latest model tokens have the ability to generate a public key pair entirely within the token, such that the private key never leaves the token. Thus the token may be more than merely a key storage medium; ideally it should also perform all of the user's important cryptographic processing, especially signature generation. Non-repudiation is greatly enhanced by this type of token. Users and PKT scheme operators are advised to carefully study token performance specifications and claims with respect to key generation and signature generation on the token.

Smartcard standards for mechanical and electrical performance have been stable for many years (see for example ISO 7816) but smartcard cryptographic processing standards are undergoing rapid development at present. Some guidance may be found in *ISO 10202 Security Architecture of Financial Transactions Using Integrated Circuit Cards*. Some aspects of these standards may also be applicable to other forms of tokens.

### Hybridisation

The area of key storage media is beginning to show some examples of combining PKT with biometric authentication. The commonest case is where access to a token is controlled by a biometric instead of just a PIN or passphrase. Smartcard readers are available now where a fingerprint must be presented before using the card and the private key contained within. Ideally, the biometric template should be stored within the card as well as the private key. This approach is discussed in more detail in the hybrid technologies chapter (Chapter 7).

## INFRASTRUCTURE

This section describes the main functions in Public Key Infrastructures.

### Public Key Certificates

In public key authentication, a digital signature or similar piece of unique identifying data is generated using one's private key, and is verified using the corresponding public key as discussed in the cryptography tutorial in Chapter 8. Evidence of the true identity of the private key holder is usually provided via a public key certificate (or 'digital certificate'), a formalised data structure which binds the name of the holder to a copy of their public key. The public key certificate is itself digitally signed by the entity which issues it. This can be another PKT user (as is the case in the informal 'web of trust' used in PGP) or else a more elaborate entity serving the needs of large numbers of users; that is, a 'certification authority'.

The web of trust and the CA models are discussed in more detail below.

### Basic Players

Not including regulators, the major players in any public key authentication scheme are as follows:

**Certificate subjects** (also known as certificate 'subscribers') possess at least one asymmetric key pair with which they create digital signatures to authenticate their actions in an electronic transaction. Their identities, credentials—especially their capacity to act— or both are carried in the form of a digital certificate and are thereby bound to their key pair. The digital certificate carries the public key and is used by relying parties and others to securely obtain the subject's public key for signature verification.

**Certificate holders** can hold and use a certificate containing the public key of the issuing authority but not containing a certificate subject or a certificate subject public key. An emerging field is the use of such certificates to evidence entitlements or attributes.

Note 'certificate user' is not a good term for certificate subjects or holders, because in an important sense, relying parties (see below) **use** certificates without being subjects or holders.

**Certificate issuers** vouch for the identities and credentials of subjects, and create and sign their public key certificates. They can also issue and sign entitlement certificates. Certificate issuers may be individual users or formal entities known as certification authorities. Depending on the model, CAs may be third parties, independent from the subject and their subsequent transactions, or else they may be related to the subject, as an employer for example. In some cases entitlement certificates are issued by another body known as an attribute authority or by an automated process, sometimes known as an attribute server, which uses an identity or credential certificate to issue the entitlement certificate that can be used by the certificate holder anonymously.

Certificate issuers also typically undertake the certification revocation process by issuing certificate revocation lists.

There has been a general shift in the last few years from the independent third party CA model towards more use of internal CAs serving the special needs of communities of interest. Both the independent model and the internal model are valid, as well as hybrids of the two.

Architecturally, the operation of most CAs is broken down into front-end registration functions, backend certificate manufacturing and directory service functions, as discussed in more detail below.

**Relying parties** are the counter parties to transactions authenticated by a subject's certificate. They receive transactions signed by certificate subjects and will rely upon undertakings, commitments, representations and the like contained within those messages and authenticated via the digital certificate. They may also receive entitlement certificates and action those entitlements.

The principle issue for relying parties is how to gain sufficient information to help them decide whether or not to accept the certificate and therefore accept the transaction or action the entitlement. In electronic commerce, the relying party may have never met the subject before and therefore has no basis to directly trust the subject. Thus the question for the relying party is how do they trust the CA?

## Public Key Infrastructure

It has been stated elsewhere that a PKI is not involved in all implementations of PKT. Perhaps most notable is the secure e-mail product PGP which does not require a PKI, but instead involves its users managing the distribution of digital certificates. Nevertheless, PKI is prominent in most important PKT systems, and so will be covered in detail in this report.

The term PKI is used in many different ways, often for commercial marketing reasons. Some companies choose to use the term to encompass application software and hardware, as well as certificate issuance and management functions. Such a broad definition can be problematic however when it comes to deciding how to manage and regulate PKI.

All meaningful definitions of PKI however acknowledge the importance of processes as well as technology. Because a PKI is supposed to deliver assurances about identities and other information, there are significant risks, liabilities and compliance issues associated with it. The processes for operating all elements of the PKI must be rigorously understood and documented.

PKI is probably most effectively used to refer to systems—both technologies and documented processes—of inter-working certification authorities.

The fundamental purpose of a PKI is to provide the means for relying parties to establish trust in CAs, rather than having to be familiar with each CA directly before they can be trusted. PKIs generally involve CAs being certified by other higher level authorities, assuring the fitness for purpose of the certificates issued by the CAs. In an orthodox PKI, a chain of certificates is created that extends from an end user back to the most central CA in the infrastructure.

A **root certification authority** (RCA) is the most central CA in a PKI. The term 'root CA' can be confusing because it would seem to imply that there is only one such entity. But multiple PKIs are emerging around the world, on commercial bases or for local jurisdictional reasons, and thus we are faced with multiple root CAs. If this seems paradoxical, then perhaps a better term for root CA is **trust anchor**. (See figure 15.)

Relying parties can keep lists of all trust anchors they choose to recognise within their software system, signifying that all CAs chained back to each trust anchor will by extension also be trusted. The list of trusted root CAs or trust anchors is termed a **trust list**. Trust lists have been subject to extensive study by the APEC e-Security Task Group and are reported on in Chapter 3.



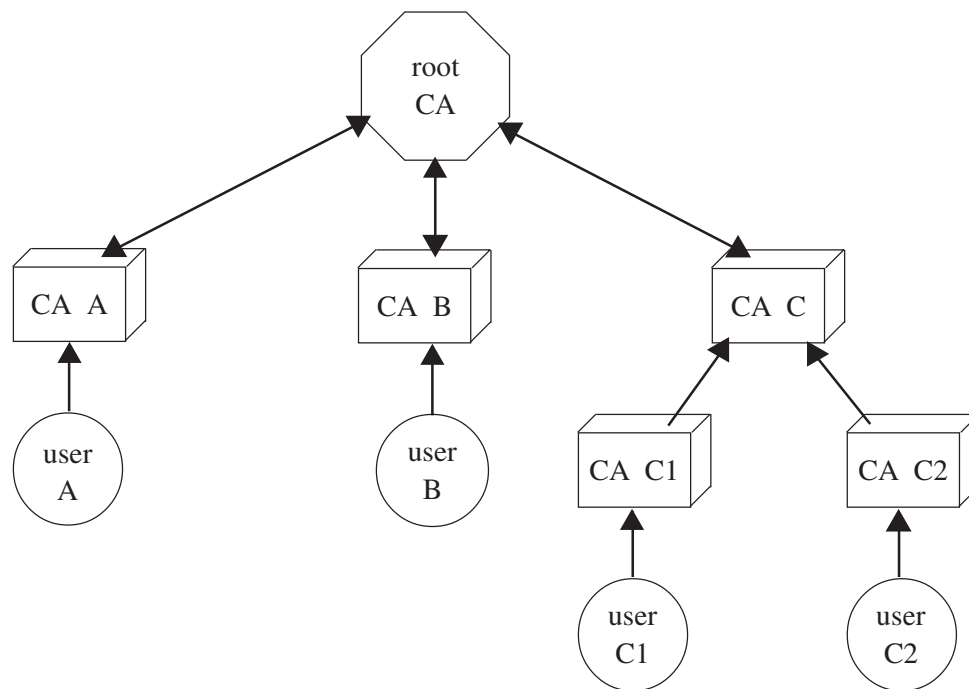


Figure 15: Root Certification Authority

### Typical CA Architecture

The operation of a certification authority can be divided into two or more parts, for the more effective management of the functions. The typical roles are for registration authorities and certificate manufacturing authorities. There are widely understood and are not discussed in detail. Two emerging components are directory service providers and validation authorities. Consequently these are discussed in more detail.

**Registration authority (RA)** is the front-end function where subjects are vetted against the CA's identification rules. The RA is typically also responsible for revocation. The RA may be located at a convenient location such as customer service desk or personnel department.

If the CA's identification rules are standardised (for example, a nationally recognised photo identification check) then the CA may outsource the RA function to a bureau. In some cases, post offices have established RA functions, based on their recognised ability to check the identification of individual people and their extensive network of physical locations.

**Certificate manufacturing authority (CMA)** is the back-of-house function responsible for creating digital certificates in standard format and signing them before distribution. The CMA is usually located in a physically secure facility where proper care can be taken of the CA signing key. However if the RA is remote from the CMA, special security will be needed for the RA-to-CMA link, especially with respect to authenticating certificate requests. It is relatively common for a CA to outsource its CMA function to a specialty bureau.

The backend function of certificate manufacture is sometimes called the CA. This can be confusing, as it blurs the distinction between the overall business of issuing certificates, and the specific backend role of manufacturing them. As discussed below, one legal entity usually has to take responsibility for the end-to-end process of registering certificate holders and distributing the certificates. Even if these functions are operated separately by different entities, there is usually one overall certification authority or CA. Therefore care must be taken when using the term CA to refer solely to the backend.

**Directory service providers (DSPs)** may host directories and CRLs on behalf of CAs. In some cases a CA may provide directory services for subordinate CAs. The function may be outsourced by a CA for reasons of availability or accessibility. The role of directories has been relatively neglected compared with registration and certificate manufacture.

Directories and repositories are typically used by CAs to publish the certificates and CRLs. These directories may or may not be publicly available depending on the model adopted. Relying parties who need to verify a digital signature can retrieve a copy of the signer's certificate from such a directory. If the relying party has the certificate but wishes to know more about the signer, they can usually also retrieve information about them and the CA, including copies of the CP and other relevant documents.

A directory is a flexible, database-like store of information 'objects', which may include certificates, documents, hypertext, software and so on. The X.500 series of standards govern directories, the ways to name objects, and protocols for accessing them. Note that X.500 describes the directory access protocol (DAP) whereas the more common method for interfacing directories is the alternative lightweight directory access protocol (LDAP). LDAP originated as free-of-charge shareware from the University of Michigan in the US and has now been integrated with many commercial e-commerce applications.

Directories are not restricted to PKI and are becoming an important part of many e-commerce applications, including catalogues. Note also that directories are not in fact essential to the operation of a CA. Certificates are commonly distributed together with signed messages, so relying parties do not necessarily need to retrieve them from directories. Furthermore CRLs may be hosted as ordinary hypertext or on conventional databases. When designing a PKI scheme, it is therefore important to consider the costs and benefits of the directory function, separate from the CA function.

All PKIs require one or more repositories to store public key certificates and CRLs.

Such repositories must usually be easily and quickly accessible on-line by a large number of individual digital signature verification processors (DSVP).

There may be some small or closed PKIs where on-line access to the repository is not required, where public key certificates are distributed individually on disc or tokens for example and where CRLs are not required on-line by individual users, but such PKIs can be classified as special purpose applications.

Other special purpose applications are those PKIs where there may be only a single DSVP, such as in applications where a central facility verifies digital signatures on behalf one or more users, as is sometimes the case in public or private sector e-business gateways.

More usually there will be a need for the repository to be accessed by DSVPs as in the typical situation where, in a public or a private PKI, users themselves verify digital signatures on their own individual computer systems. In this case, depending upon the nature of the particular PKI application, the number of users needing to access the repository simultaneously may be very large.

A repository is, in the simplest terms, a database. However, there are many different types of database and in respect of PKIs the two most relevant types are the relational DBMS and the directory and it is important to recognise the difference between these two special purpose databases.

The primary purpose of a relational DBMS is to allow items of data to be related to each other. The primary purpose of a directory is to be able to quickly find a particular item of data, known as an object in directory terms, by use of a hierarchical tree-like structure.



A relational DBMS may be employed as a PKI repository but, due to its relatively slow speed (as compared with a directory) to find and export a particular item of data, its use may be limited to those PKIs in which there are only a small number of separate DSVPs or where speed is not of paramount importance.

In PKIs where there are multiple DSVPs, for example where there are many individual users making a large number of simultaneous access attempts, and where speed is essential, then a directory is a much better choice for the repository.

Until recently, consideration of a PKI usually concentrated on two primary components: the RA and the CA. The repository was often given scant attention and was viewed as a sort of off-the-shelf bolt-on component with no great attention being paid to its specification.

Practical experience has now shown the importance of the repository, and this can best be illustrated by comparing the results of a failure of each of the primary components of a PKI:

- Failure of an RA is largely a temporary inconvenience. New users cannot be registered, or may have to go to another RA.
- Failure of the CA is much more serious. New public key certificates cannot be issued and, far more critically, updated CRLs cannot be issued putting many transactions at risk.
- Failure of the repository is very serious, verging on catastrophic. All those DSVPs relying on the repository (and in a big PKI there may be many thousands of DSVPs) will be unable to verify digital signatures. In a PKI serving the business community, the resultant disruption of commerce might cost the community untold millions of dollars.

Given its importance to the PKI as illustrated above, it is clear that the repository must be run in a high availability (HA) environment, the primary criteria being reliability, availability and scalability (RAS). Fortunately servers and operating systems are ever growing more reliable and prices are steadily falling. Today it is not unrealistic to attain very high levels of RAS at affordable cost. Moreover, directory replication technology provides another means of maintaining high availability for a repository.

The aim should be to run a PKI repository at an availability level at which a fail-over will be unnoticeable and transparent to the user, with no interruption of service and no degradation in performance.

**Validation authorities** (or VAs) are a new type of third party service, typically independent from any CA, which provides relying parties with information about the validity of certificates they receive. In some cases a CA may outsource its directory services to a VA.

Historically, the primary source of information about the validity of certificates has been CRLs posted in a publicly accessible directory by the associated CA. Traditionally, the CA that issues a certificate is also responsible for providing the means for the user to revoke it, and for maintaining and publishing the CRL.

The VA concept was originally based on the experience of many relying parties that CRLs could be hard to find. Either it was not obvious where to locate the directory that held the relevant CRL, or else that directory might not be available when it was needed.

CRLs suffer from a more fundamental problem, concerning the latency of update. CRLs are only updated periodically and consequentially there is a risk of relying unwittingly upon a certificate that has very recently been revoked without yet making it onto the CRL. In practice, the CRL update period cannot be made too small, because of storage and communications cost tradeoffs. In practice, 24 hours is a typical update period. Traditionally, if the relying party estimates that the risk is too high

to accept the CRL on face value, then they have to wait and re-check the CRL a day later, or they can try to check the sender out-of-band, perhaps via a phone call.

Yet transactions are becoming more and more automated and the processing cycle is shrinking. It is plainly unacceptable to wait 24 hours before accepting a stock market transaction, and rapid automated processing precludes out-of-band verification. Thus it doesn't matter how quickly a CRL is updated; there will always be a window within which a certificate is potentially of unknown validity.

Downloading a CRL can be time-consuming, resource-hungry, and inconvenient in the event that revocation information might be needed for just one specific certificate. A more convenient service is nowadays available from some CAs in the form of the online certificate status protocol (OCSP). This service returns a signed, time stamped message asserting a given certificate's validity at the time an inquiry is made. CAs typically charge relying parties a fee per OCSP inquiry.

The value proposition of the VA model is to offer a one-stop-shop where for any given certificate, relying parties can find:

- the applicable CRL,
- potentially, additional information about the validity or credentials of the certificate holder, and
- potentially, additional access to third party data about the certificate holder.

The value of the VA model is sometimes premised on the claim that relying parties can increasingly expect to receive certificates from unknown parties, which are issued by unknown CAs. In this scenario, relying parties would have little or no knowledge of the CAs and might therefore lack access to the revocation data published by those CAs, or else they might lack confidence in the data. VAs claim that relying parties can instead retrieve aggregated revocation data from a single trusted source.

The classic VA operates by aggregating CRLs from a large number of CAs. A VA must encourage as many CAs as possible to send them their CRLs.

VA models are still new, but at this stage, it appears that VAs do not charge CAs for this service. Instead, a VA will claim to add value to each of the CAs by making their CRLs easier to use, increasing the attractiveness and accessibility of each CA's overall service. VAs make their money instead from charging access fees to relying parties.

With e-business spreading, especially B2B commerce, we are finding that parties transacting with one another are seeking more and more information with which to verify one another's trustworthiness or dependability. For example, to help decide whether or not to accept a high value financial transaction on-line, a relying party might like access to real time up-to-date information about the sender's credit history. It is possible that VAs might bundle such additional information with the basic certificate status data, to enhance the value of their services. This merging of data has privacy implications. These aspects are discussed in the legal issues chapter (Chapter 9).

There is a related scenario where a certificate subscriber might seek to use their certificate in transactions that somehow go beyond the original scope of their certification.

VAs are faced with alternative means for relying parties to gain access to revocation information. Chief among these is the 'CRL Distribution Point', a URI (Universal Resource Indicator) where the CRL can be found on line. The X.509 Version 3 standard specifies the CRL distribution point as a standard extension. Many CAs now routinely populate this extension in the certificates they issue. Further, client-side software such as web browsers and development toolkits increasingly feature automatic checking of the CRL distribution point as part of their certificate processing functions.

The CRL distribution point means that the CRL for a given certificate's issuer is physically accessible by relying parties even if they have no prior knowledge about the CA.

CRLs are typically considered part of the intellectual and commercial property of a CA and many CAs claim copyright protection. While a CRL is usually publicly available, a CA might assert its rights and so prevent VAs from collating and republishing the CRLs.

As discussed, one of the reasons for using VAs is the expectation that relying parties will receive certificates from unknown parties, which are issued by unknown CAs. On the other hand, at least in B2B transactions, it may be rare to receive certificates from a totally unexpected CA. A B2B messaging system is typically a sophisticated set-up involving closely allied solutions providers, service operators, commercial or government sponsors, and certification authorities. There is usually tight control over the certificate policy and the accreditation or approval of certificate issuers. Even in an open B2B system, there will be a limited number of CAs actually involved, and it will be rare for a previously unknown CA to unexpectedly start offering certificates into the system. Therefore it may not be the case that revocation data is difficult to access or trust in e-commerce.

The future role of VAs will depend on the business models they develop and the value they add for CAs and relying parties. The establishment of VAs is not expected to significantly impact on cross border recognition of certificates. Assessment processes relate to the publication, liability, security and privacy of directories and CRLs regardless of whether a CA, a VA or both carry out the functions.

VAs are in a good position going forward to enhance the ability of relying parties to validate transactions on a case-by-case basis. Without modifying the scope of the intended use of a certificate, a VA can make additional instantaneous business information available—such as credit risk ratings, warranty protection, and business status which may help users make better use of digital certificates. A digital certificate only provides information about the holder at the time the certificate was issued, but a VA may be able to provide current information over and above the revocation status.

### **Relationship Between PKI Elements**

In some implementations, it is possible for the various elements to be carried out by different entities. Care needs to be taken in these cases. The overall effectiveness of a CA operation depends critically on all elements. The CA's compliance with standards and regulations will be determined by the elements operating in concert. The CA has to take overall end-to-end responsibility for the process of issuing and supporting certificates. Certification of a CA by a higher authority will require tight, auditable controls of all the elements. Therefore, close attention must be given to contracts between the CA, the RA, CMA, DSP and VA where these are separate sub-entities.

### **Identity and Role**

Because of the close association in business between someone's signature and their level of authority to sign something, digital certificates were quickly applied to create electronic credentials. It is important to separate the notions of identity and role.

Some commercial CAs offer general-purpose digital certificates that establish the personal identity of the subject, to some agreed level of assurance. Such CAs will conform to broadly accepted, transparent identification protocols, such as photo identification checks. Most economies have a standard (either official or de facto) for personal identification for everyday business purposes, such as a passport, a national identity card or drivers licence, or a combination of these. CAs often pragmatically utilise the same standard for general identification. Indeed, the earliest bureau CA business models were based on simply replicating such recognised local standards, and digital certificates to this day are commonly likened to digital passports.

In business transactions, it is often necessary to assert your credentials or role in addition to your identity, or indeed instead of your identity; in many jobs, such as the judiciary and the police, anonymity may be a prime objective. Hence the concept arose of the role-based certificate, for asserting role instead of personal identity.

Conveying role and credentials in a PKT system may be accomplished in several ways.

**Certificate extensions**, supported by the X.509 Version 3 standard, are essentially pieces of customised plain text or data inserted into the public key certificate, which can provide explicit indications about role. Care must be taken however to maintain interoperability when using custom extensions. Often the very presence of an extension will cause commercial software systems to fail.

**Special purpose membership certificates** issued by recognised organisations can form implicit credentials associated with the certificate issuer. For example, a recognised medical registration board might issue certificates only to doctors, representing their qualifications. Such certificates would substantiate the qualifications by reference in the certificate policy and practice statements.

**Attribute certificates** can be used to manage the authentication of identity and credentials separately. These are created and signed by a trusted entity, but unlike public key certificates, they contain no public key for the holder. Therefore, the holder still needs a conventional public key certificate if they are to generate a digital signature of any kind.

Attribute certificates would usually be issued independently from the subject's public key certificate(s) and can explicitly cross-reference a public key certificate. The latter may be a widely recognised identity certificate.

Attribute certificates are relatively new and as of mid 2002, few commercial attribute authority systems had been released. When used in conjunction with digital signatures, attribute certificate systems inevitably introduce even greater complexity than PKI alone, because public key certificates and CAs are still required. Attribute certificates can be used on their own however—with no digital signature function—in pure access control applications. At this time, access control, especially for temporary privileges, is probably the major application for this technology.

## Hybrid Approaches to Role and Entitlement Authentication

Role can be managed separately from identity in e-business by hybridising a PKT system used for digital signatures, with conventional access control lists or directories used for mapping users' identities to their roles. It is important from a business point of view to consider such hybrid approaches, rather than pure PKT solutions, because they can help to re-use existing security infrastructure, and so reduce the risk of introducing an all-new system like PKI.

## USE IN ELECTRONIC BUSINESS MODELS

There are a number of PKT implementation models.

### Hierarchical Public Key Infrastructure

If a relying party is not familiar with the CA that issued a given user's certificate, then the relying party is no closer to being able to depend on that user's transactions. In a hierarchical PKI, CAs may be certified by other, higher level CAs, to improve the chances that an unknown user's certificate can be traced back to a known and trusted CA or trust anchor.

Within this hierarchical category, there are several ways to run a CA. The subsections below summarise the main implementation models for certification authorities today. For each, one key issue is listed relating to the selection of the appropriate CA model.

### **Bureau User CA**

The earliest commercial CA model was the bureau user CA, where a true third party issues personal certificates on a fee-for-service basis. Such certificates may be used to identify parties to personal or retail transactions. The bureau business depends on the CA having accessible service outlets and a reputable, trusted brand.

Service outlets may be bricks-and-mortar sales counters or may be web-based. Obviously the CAs' ability to vet identity details is limited when application is made over the web. Bureau CAs typically implement a range of certificate policies at different price points. Relatively more stringent certificate policies are available via physical, in-person service outlets.

**Key selection issues.** Is personal identity sufficient to authenticate the transactions? Alternatively are special purpose certificates representing role and credentials necessary?

### **Bureau Certificate Service**

Many bureau CA businesses now offer their corporate clients an on-site RA, with which users may be more conveniently registered. In the simplest model, the CA offers its standard certificate policies, delegating responsibility for vetting identity details to the corporation. The certificate issuer is formally the bureau CA.

**Key selection issues.** Is the CA more strongly recognised than the corporate organisation? If the CA has better brand recognition than the corporation, then certificates issued by the CA may be more widely recognisable and therefore more useful, than certificates issued directly by the corporation. On the other hand, if the corporation has an existing trusted role, then it may dilute its reputation by outsourcing the certificate issuance process.

### **Private Label CA**

If a customised certificate policy is required (usually because of a desire to vary the identification rules) or if a corporation wishes to brand its own certificates, then they can buy a 'private label' service from some CAs. Typically the CA and the corporate customer will together design a certificate profile (i.e. customised contents) and certificate policy. Certificates are physically generated by the CA, based on identity data provided by the corporation (either from on-site RAs or from batch data). The certificates however are issued under the name of the corporation. The CA may additionally certify the corporation's signing key, in order to improve the recognition of the private label certificates.

**Key selection issue.** The security and protection of member information exported from the corporation.

### **Organisational CA**

Some organisations prefer not to have their certificates generated by a third party and so choose to operate the entire CA function (RA and CMA) for themselves. They may be reluctant to release their customer or member data to an outsider, or, if the certificate population is large, it may be more economical to in-source the CA function. There are now at least a dozen commercial products with



which organisations can build their own CAs. A range of price points exist, depending on scale and performance characteristics, and on degree of cryptographic security.

**Key selection issue.** Does the organisation have the skills and resources to run its own CA?

### **Certified Organisational CA**

If an organisation runs its CA in isolation, then it will have to take responsibility for distribution of its own public key and it will have to satisfy its users that the CA is being correctly operated, fit for the purpose of its certificates. Both problems can be solved if an external high level CA certifies the organisational CA. Higher level certification involves initial review and ongoing audit of the organisation's CA procedures, especially with reference to the documented certificate policy and certification practice statement. See also the Accreditation Section.

**Key selection issue.** As with any audit, does the higher level CA provide good value with respect to process improvement, total cost of compliance, and recognition?

### **Web of Trust**

Fundamentally, the problem addressed by CAs is the distribution of users' public keys, so that all parties can determine the true ownership of a given key. An alternative to hierarchical PKI with its third party CAs is for users to take responsibility for identifying key holders for themselves. This approach is known as the web of trust. Classically, two parties that know and trust each other personally hand over (or exchange) their respective public keys, without the agency of any third party.

In relatively small, closed communities of users, a web of trust approach can work well. It has the advantages of simplicity and low cost. And it appeals to many people involved in highly private communications founded on personal trust. But for larger groups, or in cases where parties do not know one another, the web of trust has limitations. These are explained in more detail below.

The best known problem with the web of trust is that by itself it does not scale efficiently. That is, the work needed to maintain the web increases per user as the total user population grows. In the worst case, if everyone wants to trust everyone else in a web of trust, then for  $n$  users, the number of key exchanges equals  $\frac{1}{2} (n(n-1))$ . Thus the scale of the web of trust is proportional to the square of the population.

The scaling problem has long been recognised, and is often addressed through introducers. If for example Alice wishes to trust some stranger Steve, and she knows that her friend Bob already trusts him, then she can have Bob introduce Steve to her. Bob passes a copy of Steve's public key onto Alice. By allowing introductions, the number of first-hand key exchanges needed to complete a web of trust can be made much smaller than  $\frac{1}{2} (n(n-1))$  (depending on just who does the introductions). An emerging trend in webs of trust is for introducers to maintain a directory of the keys of the users that are trusted within a particular community of interest. These directories are not generally subject to the same controls as those applied by CAs.

Introductions bring significant control issues, for they depend on users trusting more than just each other's identity. In the previous example, for Alice to trust Steve, she must trust that Bob knows Steve as well as she thinks she knows Bob. That is, she must trust Bob's processes for identifying people. This is a radical jump from needing to trust Bob's identity alone. Without independent standards and controls (usually considered too costly in a web of trust) uniform identification of users is difficult.

Regardless of the PKT model, there are several general business considerations.

### **Geopolitical Considerations**

Increasingly, regulators are taking an interest in certification authorities around the world, in the interests of providing appropriate assurances to consumers and businesses in electronic commerce. Different jurisdictions are imposing different degrees of control over CAs, and prescription of technologies, generally in accordance with their local legal code and conditions. Operators of CAs (be they bureaus or organisations) need to be aware of emerging geopolitical conditions. In particular, some jurisdictions require local auditability of CAs in order to recognise their certificates.

**Key selection issue.** What local laws and regulations apply to CAs in the jurisdiction where you plan to issue certificates?

CAs are sometimes categorised on the basis of the community or electronic business model they are deployed in or support.

### **Open Model**

In this model there are many parties who may rely on a certificate and who may not be known to the CA at the time of certificate issuance. Open model CAs are generally independent legal entities with respect to their subscribers and to relying parties. Certificates issued by an open model CA are intended for use by other distinct legal entities. The bureau and private labels CA models described above are generally examples of open model CAs.

### **Closed Model**

In this model the CA, its subscribers and all relying parties are all part of one legal entity. The CA may be treated simply as one sub-component of the entity's total business operation.

### **Open-But-Bounded Model**

In this model the types of relying parties can usually be defined (in terms of other communities) but individual relying parties cannot be identified in advance. For example, certificates issued to a community of medical doctors are likely to be relied upon by many groups, such as pharmacists, hospitals, insurance companies, specialists and so on. There may be existing understandings between these parties, based on laws, regulations, charters, conventions and so on. The need for additional contracts to enforce or recognise digital certificates needs to be examined.

One of the main differences between the types of business models concerns liability or risk faced by the CA. Open model CAs assume risk and liability for the business applications they serve. Closed model CAs are part of an overall business operation where the liability and risk are distributed throughout the infrastructure. The business operation includes the applications being run or used, the computers and their associated telecommunications systems, business procedures, and the employees or users.

Liability in the case of open-but-bounded model CAs is harder to assess at this point because there is relatively little experience of this type of model. But given the basic principle of referring to existing laws, regulations, charters and the like, liability can be expected to be discernible from existing frameworks.

## **USER REQUIREMENTS**

The principal user requirements in public key systems are the same as for any electronic authentication system.

Public key solutions are particularly suited to the following specific requirements:

- where the relying party has no prior relationship with the authenticated party, and therefore cannot depend on pre-registered authenticators like shared secrets or pure biometrics;
- where an auditable electronic signature must be bound to such long-lived electronic transactions as contracts;
- where the credentials of the authenticated party must be authenticated as well as (or instead of) their personal identity;
- where integrity of authenticated transactions is required (integrity is provided automatically through digital signatures, see the cryptography tutorial in Chapter 8);
- where non-repudiation of authenticated transactions is required (because non-repudiation is also provided automatically through asymmetric digital signature algorithms, see the cryptography tutorial in Chapter 8).

There are a number of specific user requirements that CAs must support:

- availability of directories and certificate revocation processes consistent with user business requirements;
- availability of expired certificates and CA keys (archives) to ensure previously validated certificates can be re-validated if necessary;
- transition arrangements to ensure business continuity for users in the event of a CA ceasing operations.

## **CERTIFICATION MODELS**

The concept of certification of authenticators has largely developed in respect of the use of PKT.

### **Formal Certification**

By their very nature, public key infrastructures using certification authorities are formal certification models. The approach has been discussed in some detail above.

### **Informal Certification**

The web of trust approach provides an informal certification process and again is discussed in some detail above.

### **No Certification**

It is possible for the holder of a key pair to provide their public key to a relying party direct for example in a face to face situation or by a reliable electronic process. In this case there is no certification involved.

## **TRUST**

The level of trust in PKT is directly related to the algorithms and key lengths being used. However basing trust simply on algorithms and key length can lead to a false sense of trust as poor implementations in PKT and PKI are the main source of vulnerability. For this reason a number of key implementation factors are discussed below. Most users do not have the technical expertise to



assess the efficacy of implementations in both PKT and PKI. Accordingly formal assessment of implementations as discussed in the Accreditation Section below is critical to generating trust in PKT and PKI.

### Algorithms

Most commonly used algorithms are in the public arena and have been subject to cryptanalysis to test the efficacy. This process can increase trust in the algorithms.

### Key Length

In mathematical terms the probability of determining a private key is  $2^n$  where  $n$  is the key length. However as some implementations require particular characteristics for a key (prime numbers for example), the actual number of potential keys can be reduced. The longer the key the less likely it is to be determined by cryptanalysis. In PKT implementations key lengths are set at a length that makes it computationally infeasible for a private key to be determined knowing the corresponding public key.

The probability of two messages producing the same message digest or hash is  $2^n$  where  $n$  is the size of the message digest or hash. Again present implementations use hash functions that make this probability computationally infeasible.

Increases in computing power periodically result in the time required to break a key being reduced to the extent of such an event becoming feasible. For this reason key lengths are periodically increased to retain an appropriate level of trust. This raises issues in respect of re-validation of older transactions signed with shorter, now vulnerable, keys. Solutions such as resigning archived transactions are being investigated as means of addressing this problem.

### The Root CA

One of the key issues in building trust in public key systems has been the custodianship of the root CA.

Only a few economies have so far decided to build central root CAs (whereas quite a high number of private sector root CAs have been established by commercial CAs). Several governments (typically those in a 'light touch' mode) have felt that a government owned or operated public sector root CA is not critical to the success of electronic commerce, while others have argued the opposite, seeing a role for the public good. On the other hand, the expected roles and responsibilities of root CAs have not been clearly described. It is fair to say that the role of PKI in e-commerce is still not totally clear, and there is therefore no right or wrong government policy regarding root CAs.

A root CA obviously carries great responsibility for custody of the root private key, for compromise of the root key can lead to the creation of false CAs and, in turn, great numbers of false certificates. Compromise of a root CA is perhaps the worst case failure scenario in any PKT scheme. The root CA must therefore have the highest standards of physical, procedural and personnel security. It is for this reason that most advocates of central root CAs have guessed that it should be the responsibility of government.

On the other hand, under an accreditation-based PKI model, the peak authority in the PKI may have responsibility for accrediting or licensing high level CAs, who in turn independently certify low level CAs. In this case, the root CA function might be better taken on by national or trans-national accreditation bodies. The criticality of the root private key is not reduced in this model but the technological functions of creating, signing and revoking high level certificates can probably be outsourced to a specialist.

Remember that high level CA certificates will be infrequently issued and revoked, and neither issuance nor revocation in these cases is needed at short notice. This means the root private key does not need to be on-line or accessible by very many people, making it easier to protect.

### **Recovery From Root CA Compromise**

Compromise of the root CA can in theory lead to large scale counterfeiting of CAs and certificates. In practice, a PKI can be made relatively robust against this scenario through the presence of high level CAs intermediate between the root CA and other end-user CAs. In much of the literature, these are known as Policy Creating Authorities (PCAs) or, in the case of the Australian Public Key Authentication Framework model (PKAF) they are simply called Intermediate CAs (ICAs).

The role of a PCA or ICA is basically to oversee the operation of lower level CAs and to certify the public keys of those CAs. ICAs and PCAs typically play a major role in either the creation or oversight of certificate policies and certification practice statements or both, and therefore usually perform some sort of audit of CAs. These responsibilities are critical and relatively onerous; it follows that ICAs and PCAs will tend to be large, stable, well-known organisations. Furthermore, the process of becoming an ICA or PCA tends to be meticulous and tightly managed. Therefore, ICA and PCAs are generally highly trusted organisations, in their own right.

As a consequence, in the event of root CA compromise, ICA and PCAs can arguably continue to operate in their own right. If they were well-trusted organisations before the compromise, then they surely remain so afterwards. Given the types of stringent physical protection discussed above, it is safe to assume that a root CA will never be covertly compromised. That is, the compromise will be readily detected. In that case, an alert can be issued to all users to look out for unexpected new ICA or PCAs appearing in the system, and to only trust certificates that chain back to an existing ICA or PCA.

### **Technical Security Issues**

An important element in establishing trust is ensuring that appropriate security measures have been implemented. In any PKT scheme, the following specific security issues must be addressed, either through protective measures, risk mitigation, or both.

Note that the term key hygiene refers to the protection of a key against theft (or copying—theft implies it is gone; it could be either), corruption or substitution.

### **User Private Key Hygiene**

Authentication and non-repudiation in PKT are based on the assumption that only one person or entity has access to a particular private key. It is critical therefore that access is appropriately controlled. The proper degree of control will depend to the effective value of the transactions enabled by the private key. Guidance should be taken from related business security scenarios, such as PIN-protected bank cards, building access control, company safes and so on. Note that cultural factors may have an impact as well.

Different private key media as described above provide different inherent levels of protection. If private keys are held on disk, users and scheme operators need to pay attention to the possibility of keys being stolen without detection. Of special note is recent viruses which appear to be capable of exporting private keys for the purposes of impersonating users. It is recommended that all electronic commerce transactions secured using private keys held on disk be carefully risk limited. For example,

such transactions can have their value capped, or they can be made subject to additional, out-of-band authentication, such as written or telephoned confirmation.

The principle advantage of token storage of private keys is that it should prevent undetected theft of a key. Token security features need to be carefully studied however. Some tokens allow the private key to be exported or otherwise detected under varying conditions. Some tokens can automatically detect certain attempts to extract the key and may destroy the keys instead. In all cases, token access should be controlled by a PIN or biometric, and the same user behaviours should be encouraged as for the use of bankcards.

### **Private Key Transport**

In the case of central key generation discussed above, special attention must be paid to the transport of the private key from the CA to the end user, to prevent theft or substitution. The advantage of known good quality key generation can be lost if the key is not transported securely or indeed if the key, once received by the user, is stored insecurely, for example on disk. This scenario has been likened to the use of an armoured car to transport money from a bank to a shop, only to have the money left out on the counter.

### **Root Public Key Hygiene**

Root keys (or trust anchors) are commonly held in databases within end user applications such as web browsers. Commercial software applications are often shipped with a number of root keys pre-loaded; CAs can contract application vendors for their root keys to be so shipped. Alternatively, a root key can usually be imported into the end user application environment.

No matter how root keys are installed in the user application environment, if they are held in disk storage, then there are significant security issues to be noted.

Protection of root public keys in end user PKT systems generally receives less attention than does protection of their own private keys. There have been few if any reported cases of an attack on a root public key but as the total value of electronic commerce increases, the motivation to substitute a root public key will increase. If an attacker successfully substituted a false key for the trusted root public key in a large number of end user systems, then the attacker could in effect masquerade as any service provider (including a CA) certified under that root. Root public keys held on disk, as is the case in all browsers today, are vulnerable to substitution, although a large number of systems would have to be targeted within a short time to mount a significant attack.

In the longer term we can expect to see root public keys housed in tamper resistant media like tokens. The capacity of tokens to carry useful numbers of root keys will be a limitation. In the meantime, users are advised to regularly check the state of their installed root public keys, by comparing them with known proper values. Most CAs should publish their root public key value in an inherently trusted (probably non-electronic) medium.

### **Root Private Key Security**

Theft of the root private key is one of the worst cases of compromise of a public key security system. In principle, if the root private key (or indeed the private key of any high level CA in a PKI) falls into unauthorised hands, counterfeit CAs can be created and consequentially, large numbers of bogus user certificates released. Therefore the protection of the root private key is of major concern.

It is commonplace for root private keys to be housed (and generated) in secure, tamper resistant crypto modules. Access to the key must be carefully managed, both from technological and procedural points of view. Root key modules should be protected by additional user authentication, by PIN or biometric, and auditable personnel controls are essential.

Further protection may be afforded by split key systems, where the root private key, when not in use, is stored in a number of independent components. The components are brought together only when the key must be used. Each can be separately secured by PINs known only to the custodian of the particular component. In so-called m out of n systems, it is not necessary to bring all components of a key together, just some minimum number. This approach protects the system against loss of a component or unexpected belligerence on the part of one of the custodians. This approach is discussed in more detail in Appendix 1 to Chapter 4.

## **LIABILITY**

In the event that a party is damaged in an electronic commerce transaction as a result of a fraudulent or falsely obtained certificate, a key issue is to establish the liability of the CA that issued the certificate. The liability of any higher level CAs in the PKI, including the root CA must also be determined. Until recently there has been no clear framework in which to analyse the liability questions.

The liability question has been compounded by several problems:

- Widespread electronic commerce is relatively new and there is little experience of the types of damages that may be suffered.
- Digital certificates are even newer and few people rely upon them as yet, so there appears to be no legal precedents at all.
- It is unclear whether digital certificates constitute a product or a service, and therefore whether they fall under existing consumer protection laws and regulations which apply broadly to products in many jurisdictions.
- The criticality of a CA's operation increases exponentially the higher up the chain the CA is, because exponentially more users may be affected when the CA is compromised. This fact has led many to conclude that the liability of higher level CAs, especially the root CA, is prohibitive.

A clearer view of liability may result from formal accreditation and standards-certification of CAs (see also Accreditation). If a PKI is constructed along the lines of a standards certification scheme, then audit standards and principles would appear to limit the liability of higher level CAs and the root CA in the event that a lower level CA falsely issues a certificate.

Guidance may be taken from ISO 9000 and other certification schemes. For instance, liability in the event of product malfunction is rarely transferred to an ISO 9000 auditor, because of the rigorous and transparent guidelines under which auditors operate. In practice, liability in standards certification schemes in fact decreases further up the certification or accreditation chain.

### **Types of Liability**

If an accreditation process is modelled on ISO 9000, different types of liability may be carried by different levels of a PKI. CAs operating at each level make characteristically different types of assertions about the entities they certify, as follows.

PKI level	Subordinate	Assertion by CA of its subordinate	Liability carried by CA
Root CA	ICA or PCA	That the ICA or PCA is independent and competent.	Failure to comply with international generic accreditation standards (such as ISO/IEC Guide 65).
ICA or PCA	User CA	That the CA is complying with standards and agreed policies and practices.	Failure to responsibly audit the CA against standards, policies and practices.
User CA	Users or other certified entities	That the user has been identified according to the requirements stated in the certification policy.	Failure to carry out agreed identification protocols.

In summary, economies will have to seek their own balance between systemic trust and liability, in accordance with their local regulatory and commercial frameworks. Some may choose to enshrine different levels or classes of trust, with corresponding reliance limits or other mechanisms to control liability. The availability of commercial insurance policies may also affect the degree of intervention required by regulators.

### Validation Authorities

It is not yet clear who would ultimately be liable in the event that a relying party suffers loss arising from inaccurate or untimely validation information: the VA, the CA, or both. However, where the VA model involves a payment by the relying party this could address the contract privity problem that exists where relying parties have no relationship with the issuing CA. The VA may be liable to the relying party, subject to any contractual conditions imposed at the time of verification.

It may be difficult to draw general conclusions at this stage, and we can expect that CAs and VAs will endeavour to limit their own liabilities by way of contract. As a result of interposing an additional entity between the CA and other players, liability may become more complex, and users will have to take care to examine how to best protect their interests.

Another liability issue relates to the possible usage of a certificate in transactions that go beyond the scope of the original transaction, where a VA may provide relying parties with additional information to support new types of transactions. All CAs carefully circumscribe the intended purpose of their certificates and disclaim any usage beyond the original scope. While it may be tempting for a subscriber to try to use their certificate for new purposes without having to go through the inconvenience and cost of obtaining a new one, the original CA cannot be expected to be comfortable with changes to the scope of their certificates.

## ROLES OF PARTICIPANTS

Indicative or typical responsibilities for various actors in a PKI are set out below. Consideration should be given to documenting and agreeing upon such responsibilities in contracts, policies and practice statements in any new PKI. The lists are not exhaustive or exclusive.

### Competent Authority

Where PKI schemes are accredited or otherwise assessed a competent authority is established to administer the scheme. The competent authority would undertake the following roles:

- establish accreditation or assessment criteria,
- certify evaluators or assessors,
- manage the accreditation or assessment scheme, and
- accredit CAs and components.

### Certification Authorities

The CA may delegate specific roles and responsibilities to RAs and CMAs, as discussed above. The CA usually retains certain overall responsibilities, as follows:

- conform to the stipulations in a given CP;
- publish the CP for all subscribers and potential relying parties;
- document a CPS that maps explicitly to the CP;
- review and inspect policies and operational procedures of peer or subordinate CAs and negotiate enhancements and assurances of the operational procedures and restrictions on usage of cross-certificates, their validity period and any liability issues affecting CAs and subscribers;
- make copies of documented cross-certification agreements including relevant CPs and CPSs (optional as we say elsewhere that CPS might not be public) available to subscribers of all certified and cross-certified CAs;
- provide certification and repository services consistent with the CP;
- provide the operational, security and technical controls stipulated in the CP and CPS;
- revoke certificates and publish CRLs as required under the relevant CP;
- provide for timely renewal of certificates on expiration;
- issue certificates in accordance with the relevant CP and honour representations to subscribers and relying parties contained in the published CPS;
- comply with all applicable policy and legal provisions;
- publish certificates in a repository accessible to the user community;
- support the rights of the subscribers and relying parties who use certificates in accordance with applicable policy, law or regulations;
- perform the identification and authentication procedures stipulated in the applicable CP; and
- accept liability for elements of damage and financial loss arising from, or in connection with, its services as warranted in the relevant CP.



## Registration Authorities

RAs may or may not be a distinct entity from the CA. Because a CP is realised by both the registration and certificate manufacturing processes, an RA must be intimately related to the CMA.

The following list of roles and responsibilities is very general. Items in the list may not apply if the RA is an agent of the CA.

- Register with a CA and obtain approval for its operational procedures.
- Conform to all relevant CP and CPS definitions in force.
- Be accountable for its procedures in accordance with the requirements of the relevant CP.
- Perform the obligations of an RA and support the right of subscribers and relying parties who use certificates in accordance with the applicable laws and regulations.
- Provide the operational, security and technical controls stipulated in the relevant CP and CPS.
- Perform the identification and authentication procedures set out in the CP.
- Comply with all applicable policy and legal provisions.
- Accept liability for elements of damage and financial loss arising from or in connection with its services as warranted in the relevant CP.

## Certificate Manufacturing Authorities

Where established separately, CMAs will perform the following functions:

- conform to all relevant CP and CPS definitions in force;
- safeguard the CA signing key, by implementing physical and security controls as specified in the CP, CPS and any applicable laws and regulations;
- only use the CA signing key to sign certificates issued on behalf of the CA, in accordance with the CP and CPS;
- create certificates in accordance with the CP and CPS, on request from valid registered RAs;
- revoke certificates on request from valid registered RAs;
- maintain a directory or database of current certificates; and
- maintain and distribute CRLs.

## Directory Service Providers

Where a CA outsources directory services to a directory service provider, the DSP will undertake the following functions:

- conform to all relevant CP and CPS definitions in force;
- maintain a directory or database of current certificates; and
- maintain and distribute CRLs.

## Validation Authorities

Where established a VA would undertake the following functions:

- maintain a directory or database of current certificates;

## Electronic Authentication—issues relating to its selection and use

- maintain and distribute CRLs; and
- notify relying parties of the status of certificates.

### Subjects

Subjects (also known as certificate subscribers) must ensure that at the time of certificate acceptance and throughout the its operational life:

- no unauthorised party has had access to the end user's private key;
- all representations made to the CA or RA regarding the information published in the certificate are true; and
- the certificate is being used for authorised and legal purposes, consistent with the relevant CP.

End users may have to enter into a contract with the CA or make other legally binding assertions of the above conditions.

### Relying Parties

A relying party has a responsibility to undertake the following functions:

- check the CP or CA accreditation to ensure the certificate is appropriate for the transaction; and
- check the validity of any certificates received.

## ACCREDITATION

Accreditation can apply to both public key technology and to the implementation of the technology or the infrastructure supporting the technology. In general technology is accredited against standards while implementations and infrastructure are assessed against accreditation criteria. There are however exceptions discussed below.

### Accreditation Criteria

Accreditation criteria can be developed in both the public and private sectors. In a number of APEC economies accreditation schemes and criteria are established by regulation or administrative order issued in accordance with legislation. In most cases the accreditation schemes adopt standards as the criteria for elements of the scheme. In some cases the accreditation criteria form the basis for recognition of certificates from other jurisdictions. However, in some economies different certificates are issued against different criteria. In these cases it is important to understand against which criteria certificates have been assessed.

**Regulated criteria** may be mandatory or voluntary, and may also impact on the legal status of electronic authentication. In some cases the process is licensing rather than accreditation. This approach has been adopted by Hong Kong, China; Korea and Singapore<sup>1</sup>; as well as by the European Union.

**Public sector criteria** are typically developed by governments for their own government schemes. They can be formal criteria (Australia Gatekeeper<sup>2</sup>), or documented certificate policies and

---

1 <http://www.cca.gov.sg/>

2 <http://www.govonline.gov.au/projects/publickey/GatekeeperAccreditation.htm>



certification practice statements that must be complied with (Government of Canada PKI<sup>3</sup> and US Federal Bridge<sup>4</sup>).

**Private sector criteria** are typically developed by private sector organisations as a basis for independent accreditation or audit of implementations. The American Bar Association<sup>5</sup> has developed PKI assessment guidelines. These do not, in themselves, form part of a formal accreditation scheme but facilitate an assessment of reliability of certificates issued by an assessed CA. Similarly the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants have jointly developed WebTrust for Certification Authorities<sup>6</sup> which provides a ‘seal’ following an audit of the CA. The scheme has been adopted by auditors in other countries

The fact that accreditation criteria differ, and may refer to different standards, has been identified as a major impediment to cross-border recognition in the CA mapping exercise conducted by the PKI Interoperability Expert Group. This is discussed in detail in Chapter 3. The legal implications are discussed in the legal issues chapter (Chapter 9).

### Standards

There are a number of standards that relate to PKT. Some of these are absolute while others may involve differing levels of compliance. As with accreditation criteria it is important that users are aware of the level at which compliance has been established. Key standards include:

**The International Telecommunications Union (ITU)** has published the X.500<sup>7</sup> series of recommendations relating to the use of directories in Open Systems Interconnection. The most important of these recommendations for PKI is X.509 *Public Key and Attribute Certificate Frameworks*. Version 3 of this recommendation is the most commonly used although some implementations use earlier versions.

**The International Organization for Standardization/International Electro-technical Commission (ISO/IEC)** have jointly developed a number of standards<sup>8</sup> relevant to accreditation of PKT and CAs. These fall into two groups: IT security and electronic authentication. These standards can assist in accrediting a CA’s operations and the technology being used. Of significance is the ISO/IEC 15408 series *Information technology—Security techniques—Evaluation criteria for IT security* which is used for the evaluation of the technology used in a PKI and ISO/IEC 17799 *Information technology—Code of practice for information security management* which can be used for the evaluation of PKI implementations.

**The Internet Engineering Task Force (IETF) Public-Key Infrastructure (X.509) (pkix) Working Group<sup>9</sup>** has issued a number of *Request for Comments*. The most significant of these are *RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile* and *RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework*. While the IETF does not have the traditional authority of national and international standards bodies, it has proven to be the most important force for standardisation in Internet technologies, and many of the RFCs are adopted or referenced by more formal standards making bodies.

---

3 [http://www.cio-dpi.gc.ca/pki-icp/index\\_e.asp](http://www.cio-dpi.gc.ca/pki-icp/index_e.asp)

4 <http://csrc.nist.gov/pki/fbca/welcome.html>

5 <http://www.abanet.org/scitech/ec/isc/pagv30.pdf>

6 <http://www.cpawebtrust.org/certauth.htm>

7 <http://www.itu.int/rec/recommendation.asp?type=products&lang=e&parent=T-REC-X>

8 <http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeStandardsListPage.TechnicalCommitteeStandardsList?COMMID=143>

9 <http://www.ietf.org/html.charters/pkix-charter.html>

**Federal Information Processing Standards (FIPS)**<sup>10</sup> are developed by the US National Institute of Standards and Technology (NIST). The most significant for PKI is *FIPS 140 Security requirements for Cryptographic Modules*. This standard is widely used for evaluation of cryptographic modules as part of the accreditation process.

**The Certificate Issuing and Management Components (CIMC)**<sup>11</sup> is a family of protection profiles developed by NIST that defines requirements for components that issue, revoke, and manage public key certificates. A CIMC consists of the hardware, software, and firmware components but not the facility, staff or operational procedures. A CIMC in conjunction with ISO/IEC 15480 can be used to accredit elements of a PKI.

**Public Key Cryptography Standards (PKCS)**<sup>12</sup> developed by RSA Security Incorporated working with a number of product developers, are a series of commercial yet widely respected interface standards for keys, certificates and cryptographic devices.

**The European Electronic Signature Standardization Initiative (EESSI)** was launched in 1999, in response to the EU Electronic Signature Directive, by industry, business and the European standards organisations ETSI (European Telecommunications Standards Institute) and CEN/ISSS (Comité Européen de Normalisation, Information Standardization System). The program is defined and coordinated by the EESSI Steering Group. The standards<sup>13</sup> are developed and maintained by ETSI and CEN/ISSS. The program operates under mandate of the European Commission. While these standards are primarily directed towards Europe, they also impact on the accreditation process for PKI schemes that wish to be recognised in Europe. APEC is working with EESSI to facilitate European recognition of schemes accredited in APEC economies.

**Domestic standards bodies** are also involved in the development of standards for the use of PKI and operation of PKIs. Standards Australia has developed a series of standards *AS 4539: Information technology—Public Key Authentication Framework (PKAF) related Standards*<sup>14</sup>. In Australia and other economies standards have been developed for the use of PKT in specific industry sector, particularly the health and banking sectors.

## Quality Management and Quality Assurance Certification

Like any organisation, CAs may be certified under general standards like *ISO 9000: Quality Management and Quality Assurance Standards*. In many economies, mature accreditation schemes are in place for establishing the authority of independent certification bodies. Interoperability of CAs and PKIs may be enhanced by independent certification and accreditation. There is one proposal that involves certification and accreditation certificates for CAs being issued in X.509 format and those being used to create the certificate chain from user to root CA.

Similarly assurance can be assessed using the Statement on Auditing Standards (SAS) No. 70 *Service Organizations*<sup>15</sup> developed by American Institute of Certified Public Accountants. This approach has been used by a number of CAs.

---

<sup>10</sup> <http://csrc.nist.gov/publications/fips>

<sup>11</sup> [http://csrc.nist.gov/pki/documents/CIMC\\_PP\\_20011031.pdf](http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf)

<sup>12</sup> <http://www.rsasecurity.com/rsalabs/pkcs>

<sup>13</sup> <http://portal.etsi.org/sec/el-sign.asp>

<sup>14</sup> <https://committees.standards.com.au/COMMITTEES/IT-012/PRODUCTS>

<sup>15</sup> <http://www.sas70.com/index2.htm>

## INTEROPERABILITY

Interoperability in public key authentication can be a confusing topic. Care must be taken not to confuse levels of interoperability.

At the lowest level, note that certificates themselves do not interoperate. If two users exchange digitally signed messages, then in order to validate the messages, they require one another's digital certificates. The validity of the certificates is assessed independently, perhaps with reference to the respective PKIs and root CAs. At a minimum, all that is required is for each user's system to hold the trusted root key or trust anchor of the other user's PKI. The certificates remain independent at all times.

### Technological issues

There is a range of low-level issues which affect the ability to distribute, install and use certificates. These issues may need attention from software developers and other technical staff.

- **Algorithm support** for both cryptographic and hashing processes are necessary if digital signatures are to be recognised. The use of proprietary algorithms can prevent interoperability.
- **Application Programming Interfaces (APIs)** exist which specify the interchange of data including certificates between computers and CAs and other entities. One important set of APIs is the PKCS series from RSA Data Securities Incorporated in the USA.
- **Smartcard interface standards** have been stable for some time at the electrical and mechanical engineering levels. Standards for the interchange of keys and certificates are relatively new however.
- **Certificate syntax** is specified by standards such as X.509 Version 3. Most World Wide Web and many secure e-mail applications use X.509 Version 3. Note that while X.509 Version 3 allows for customised extensions, not all commercial applications fully or properly implement the standard. It is always possible for applications to crash when faced with non-standard certificate extensions.
- **Directory access protocols** are used to validate certificates. While standards exist for several protocols, the relying party and the CA or DSP must be able to use or accept the same protocol to validate a certificate.

A recently identified interoperability problem unique to digital signatures is the impact of message reformatting to meet protocol requirements of particular message transport schemes. These proprietary protocols are quite common in the business world. The reformatting of a message will automatically invalidate the digital signature associated with that message. This problem and possible solutions is discussed in Appendix 1 to this chapter.

### Infrastructure Issues

Due to their complexity PKI interoperability issues are discussed separately in Chapter 3.

## CULTURAL DIFFERENCES

The rollout of PKI has been beset by confusion and misapprehension in different parts of the world, much of which has, in part, a cultural angle.

In some economies, there is a historical suspicion of hierarchies and this has made it hard to accept orthodox PKI structures, regardless of whether they involve top-down or bottom-up policy distribution. In places this has inhibited the construction of central root CAs, with the result that PKI

rollout can become fragmented. Note that in itself this might not be a bad thing, since there can be other reasons for PKI to be de-centralised. There is little evidence that the absence of centralised root CAs has had negative effects on e-business overall.

An associated issue in some economies is that the concept of a single national identifier does not have community support. Governments in these economies have generally adopted decentralised approaches to minimise any community perceptions of the creation of electronic single national identifiers.

In some economies, there has been greater enthusiasm for strongly hierarchical PKIs, often based on a recognised national photo identity system. By the same token, commercial uptake of national CAs has generally been slow, and so it cannot be argued convincingly that the presence of centralised PKI ensures success in e-business.

## **AWARENESS**

There is a bewildering amount of information available on PKT and PKI. Much of it is available on the web. In some cases the information relates to specific implementations and can be confusing if considered out of context.

Key concerns for business and individual users include:

- selection of technology,
- roles and responsibilities,
- legal effect of transactions,
- security of transactions,
- interoperability,
- privacy, and
- consumer protection and dispute resolution.

There is also a need for PKT product developers and vendors and PKI implementors to be aware of the legal, policy and technical standards frameworks of economies and jurisdictions in which their products might be used.

These issues need to be addressed in any awareness-raising activities. It is in this context that this report has been produced.

### **Government Awareness**

While there is general awareness of the concepts of PKT and PKI in government, there is less understanding of the detail of the issues involved. Furthermore the focus up until recently has been on domestic issues without considering the international interoperability aspects of implementations. In recent years a number of resources on the use of PKT and PKI and the international interoperability aspects have emerged. However in many cases the international activities have yet to be reflected in domestic approaches. In other cases domestic interpretations of international approaches continue to cause problems. This is discussed in more detail in Chapters 3 and 9.

A number of economies have produced awareness raising documents on both PKI and other security and authentication aspects of electronic commerce. The eSecurity Task Group is in the process of establishing a website to facilitate access to these resources.

One of the principal problems has been a lack of a common understanding of the concepts and terminology associated with the implementation of PKI. This is an issue that needs to be addressed by international groups including vendor and standards making groups.

### **Business Awareness**

Awareness among business is patchy and often riddled with confusion and misunderstanding. This continues to be a major impediment to the uptake of both PKI and electronic commerce. This is particularly the case for small and medium enterprises (SMEs) which often don't have the technical skills to understand both the technology and the debate surrounding it. Within APEC a number of electronic commerce awareness seminars for small business have been conducted by Asia Oceania Electronic Marketplace Association (AOEMA)<sup>16</sup> that include elements on the role and use of PKI.

An important development in PKT awareness is the establishment of domestic, regional and international 'PKI Forum' organisations. Many of these have established web-based resources to improve awareness of the technology and its use. These resources can be used by both product developers and vendors as well as the general public.

The original PKI Forum<sup>17</sup> is an international US-based vendor association formed to promote the development of the PKI industry. It has several technical working groups and has published white papers on interoperability and small business issues. Regional forums have been established in Asia (Asia PKI Forum)<sup>18</sup> and Europe (European Certification Authority Forum)<sup>19</sup>.

While most economies provide information on their legal and policy regimes, these often do not assist business in understanding the approaches in other economies with whom they might wish to transact. Instead, the best legal and regulatory information is perhaps available from several international law firms, which link to authoritative government sources. A wide ranging survey of e-signature legislation has been published by the Internet Law and Policy Forum<sup>20</sup>. This work covers a number of APEC economies but not all. Another international source of information on PKI law and policy is the Digital Signature Law Survey<sup>21</sup>.

### **Individual User Awareness**

Awareness among individual users is even lower than among business. Many are using products such as browsers that incorporate PKT but are often not aware of its presence or its use. Information from vendors on the PKT capabilities of their products and how they might be used is often difficult to find on their websites. While some user groups may provide information on PKT and PKI to their members, most users are not members of such groups. There is a role for both governments and vendors in making information resources on PKI and PKT more widely available to individual users.

## **LEADERSHIP**

The leadership required to encourage the practical usage of electronic authentication clearly will vary according to the circumstance within each economy. Most if not all economies will find public key authentication increasing in importance as a function of its deep integration with all commercial

---

16 <http://www.aoema.org/projects/awareness.htm>

17 <http://www.pkiforum.org>

18 <http://www.asia-pkiforum.org>

19 <https://www.eema.org/ecaf>

20 <http://www.ilpf.org/groups/index.htm#authentication>

21 <http://rechten.kub.nl/simone/ds-lawsu.htm>

Internet commerce applications. Economies need to find their own balance between technology neutrality and support infrastructures for what has become a commercially critical technology.

The following suggests some of the initiatives that may be appropriate. Broadly, leadership is required from governments, international organisations, business corporations, the IT Industry and academic institutions.

## Governments

Governments can provide significant leadership by establishing the appropriate legal and policy frameworks for PKT. The possible absence of policies in this important area may impede many related developments or confuse users and developers in need of guidance. Policy helps the private sector, and indeed government departments, to make their own plans, with reasonable confidence as to how their own authentication systems will integrate smoothly into whatever it is that the government proposes, or else sit alongside government initiatives. Government policies initially need not be too detailed.

There are several possible government policy models.

**Minimal regulation model.** Government may decide to leave the authentication arena wide open. It might establish CAs within its own agencies on a case by case basis but leave the private sector free to set up CAs, commercial or otherwise, as it sees fit. There is no jurisdictional root CA or other higher level authority in this model. Each CA would be responsible for ensuring interoperability with other CAs, domestically and internationally. No licensing of CAs would be required, save for the usual consumer protection regulations.

**Optional root accreditation model.** Government may decide to establish a non-mandatory root CA or similar high level authority, as a resource to facilitate the interoperability of other CAs. By opting into a central recognised authority, CAs can enhance the acceptance of their certificates outside their own systems. Mutual recognition would be mediated with other economies by the central authority. Non-mandatory licensing or technology accreditation for each CA would be required. Special legal protection may or may not be granted to transactions covered by certificates from accredited CAs.

**Mandatory licensing model.** Government may decide to establish one central jurisdictional root CA and PKI, to the exclusion of all others within the economy. Licensing and approval exemptions would be controlled by a central agency, with the objective of ensuring uniformity and high levels of dependability of all certificates issued within the economy.

The interoperability and legal implications of adopting different policy approaches are discussed in Chapters 3 and 9.

Governments can also provide leadership by becoming early adopters of the technology and encouraging its use by both business and individuals in their transactions with government. While the general principle of market lead development of electronic authentication is important, experience to date is that the market is looking to governments to provide leadership in this area. This does not resile from the general principle that product development should be market-driven.

Another key leadership activity is in the establishment or sponsoring of advisory groups to assist in the development of policies relating to the use of PKT and implementation of PKI. Similar leadership can be shown in respect of the development of standards for PKT and PKI.



## International Organisations

International organisations can provide leadership through the development of the necessary frameworks to facilitate the use of PKT in cross-jurisdictional transactions. They can monitor developments in various economies and regularly issue policy advice papers to all governments setting out the advantages and disadvantages of particular approaches, based on actual experience of successes and failures. Such international organisations can also play a coordinating role to assist economies to establish systems in their control to interoperate with other systems that are not under their control.

A number of international business associations such as the International Chamber of Commerce<sup>22</sup> have provided leadership to their members by participation in debates on electronic commerce and the use PKI and PKT.

There is also a leadership role for standards making bodies, both formal and informal in development of the necessary standards and protocols to support PKT.

## Business Corporations

Business corporations can play a leadership role by the adoption of PKT where appropriate to their electronic business requirements. They can also provide leadership by encouraging governments to develop legal and policy frameworks to support their business requirements in respect of the technology. A number of domestic business groupings have established working groups to address issues relating to the use of PKT and to lobby governments. In some cases, business corporations or associations are represented on government advisory bodies which deal with the development of PKI legal and policy frameworks.

## Users and User Groups

A number of user groups are providing leadership by participation in debate on PKT and PKI. In some cases they are involved in government advisory bodies developing legal and policy frameworks. They also have a role in advising governments and product developers on their requirements and concerns regarding the technology and its implementation.

A number of broader interest groups such as those dealing with privacy and consumer interests are also engaged in debate highlighting their specific concerns and requirements.

User groups also have a role in ensuring that their membership and the general public are aware of the technology and their activities in protecting their constituency's interests.

## IT Industry

The IT industry is already providing leadership through the establishment of domestic, regional and international PKI forums and industry bodies that are developing standards and protocols. They are also participating in interoperability experiments and pilots to facilitate the use of PKT. The PKI forums are liaising with users and governments to facilitate the adoption on PKT and development of PKI frameworks.

They can provide further leadership at the individual corporate level by showcasing their products and providing information on the technology and its use.

---

<sup>22</sup> [http://www.iccwbo.org/home/menu\\_electronic\\_commerce.asp](http://www.iccwbo.org/home/menu_electronic_commerce.asp)

### **Academic Institutes**

Academic institutes have played a significant role in the development of asymmetric cryptography algorithms and key generation packages as well as the testing of public offerings. In addition they have also been actively involved in debates on legal frameworks and individual rights. In many cases, however, their work is not widely known outside the academic community.

They can provide further leadership by wider dissemination of their work and by incorporating that work in IT, business and law courses.

### **COMBINATION WITH OTHER TECHNOLOGIES (HYBRIDS)**

Asymmetric cryptography and public key technology can be either chained with other authentication technologies or used to protect other forms of authenticators through the confidentiality functionality. These hybrid approaches are discussed in detail in the hybrid technologies chapter (Chapter 7).



# Electronic authentication in a multi-format multi-protocol environment

Electronic authentication is not always easy to achieve even in an environment that utilises a single format and a single protocol over the whole end-to-end transmission path, for example a plain text message transmitted over TCP/IP. In an environment where more than one format or more than one protocol are utilised at various stages of the end-to-end transmission path, electronic authentication becomes even more complex.

An example of a multi-format or multi-protocol environment might be the transmission of data from a shipping company's system (which might use the CARGO.IMP EDI standard over SMTP) to a customs authority that requires the data in a UN/EDIFACT format transmitted by X.400.

Despite the decades long efforts of many public and private bodies towards the goal of standardisation, in practice there are a great many different standard and proprietary formats and protocols in use today and this situation is unlikely to change in the foreseeable future.

The following discussion tries to summarise some of the issues associated with electronic authentication in a multi-format or multi-protocol environment.

### TERMINOLOGY

Translator	The term translator is used in this appendix as a generic expression to describe any computer program (be it an end user module or a large EDI clearing-house system) that accepts messages in one or more formats or in one or more communications protocols, and then translates the messages as required into different formats acceptable to the recipients and routes them to their destinations using the appropriate, and again possibly different, communications protocols.
Message	For the purposes of this appendix the term message encompasses both free text unstructured messages and structured messages, including the many different formats used in EDI systems.
Authentication	Authentication means any one of the several processes that assure the recipient that a message did in fact originate from the claimed computer or individual sender. Authentication technologies also often provide confirmation that the received message is exactly the same as the message originally transmitted by the sender.

Digital Signature	A digital signature is an authentication technology providing confirmation of origin, assurance of the integrity of the content, and non-repudiation. Digital signatures rely on a mathematical digest of all or part of the original message, and if any change is made to such message during transmission, the signature will not validate (see Figure 16 below).
-------------------	--

**NOTE:** In the context of this appendix, the sender and the recipient may be individual persons at each end of a communications link or may be computer systems.

## **METHODS OF ACHIEVING AUTHENTICATION**

### **Message Security**

Message security is a technology in which the security elements are attached to the message itself, allowing it to travel across as many different communication media as may be needed without affecting the security of the message. EDIFACT ISO 9735-5/7 and X12.58 define security of this type.

PKCS#7 (also RFC 2315) may be regarded as another example of message security since it is independent of any communication protocol and is applicable to any data format. However, it wraps the original message into an envelope that hides the sender and the recipient IDs in the original message, unlike the EDIFACT or X12 security standards. Note: such an envelope is not a 'communication envelope' to which envelope security elements are attached (see below); hence PKCS#7 should be viewed as a message security standard.

### **Envelope Security**

Envelope security is a technology in which the security elements are attached to a 'communication envelope' but not to the message itself. Such envelope security elements are lost if the same protocol is not used end-to-end. S/MIME (in combination with RFC-822 or HTTP), PEM and X.400 security standards are examples of envelope security.

### **Transport Security**

Transport security is also dependent on a particular protocol, but operates at a lower level. It is the continuous flow of messages secured between the two entities at each end of the protocol link. SSL, and its newer version TLS, are examples of transport security standards.

### **Network Security**

Network security operates at yet a lower level, and consists of the protection of the physical communication lines as well as access to the network. SWIFT, the worldwide inter-bank network, is an example of a secured network.

Network or transport level security are often better alternatives than envelope or message level security, as they relieve both senders and recipients of all security burdens, and yet they provide a level of authentication and confidence adequate for the conduct of many business transactions.

However, where a community becomes very large or where it expands across multiple third party networks, the maintenance of an adequate level of security within the network or transport layers may become increasingly difficult, and then envelope or message level security techniques become more attractive.

## Access Control

Access control is a form of authentication used only to confirm the identity of an entity seeking access to a resource. Once the access is granted, no further security controls are applied. Access control is a necessary feature of network or transport level security.

## TYPES OF AUTHENTICATION

### End-to-End Authentication

End-to-end authentication occurs when A sends a signed message to B, and B itself is able to validate the signature of A. This is the standard simple case in which A is called the principal because A has said “this message comes from A” and B has been able to validate this statement.

### Delegated Authentication

Delegated authentication occurs when an entity C tells B that the message in question comes from A. In other words, C verifies A’s signature and then reports the result to B (and C may use another signature to sign the report). In this circumstance C is said to ‘speak for A’ and C becomes the principal because C has said “this message comes from A” and B has been able to validate this statement.

When C speaks for A, then C is called a security proxy agent. Such a system is widely used in both SWIFT and SITA, two examples of closed and secured networks.

## BASIC ISSUES

### Invalidation of a Digital Signature

Where a digital signature is based on a digest of the whole or a major part of the original message, which is the standard procedure, then if the translator makes any changes in the format of that message or makes any alterations to the content of the message, the signature will no longer validate.

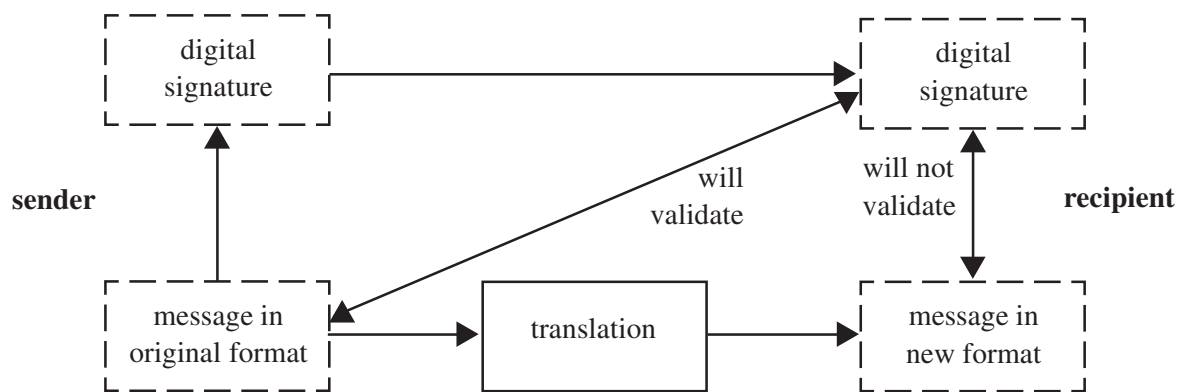


Figure 16: Message Translation

To clarify this most critical issue, consider that the original message is, for example, the phrase ‘The cat drank the cream’. This phrase is inserted by the sender, together with the sender’s private key, into the mathematical algorithms that produce the digital signature. The digital signature is sent to the

recipient accompanied by the original message ‘The cat drank the cream’. When the original message plus the sender’s public key is inserted into the appropriate mathematical algorithms, the digital signature will verify.

But let us suppose that somewhere along the transmission path there is a link that requires that the message must be formatted into fields containing subject, verb and object. Thus the received message now reads ‘subject: The cat — verb: drank — object: the cream’. The content of the message is essentially the same. But when the received formatted message is inserted together with the sender’s public key into the mathematical algorithms, the digital signature will not verify as the specific wording of the original message has been changed. This is what happens when a translator has to make any change, for formatting or other reasons, to the original message.

### Preservation of End-to-End Authentication

Should the format of the original message be one that offers inherent end-to-end authentication (S/MIME for example) it may be difficult, if not impossible, to preserve such end-to-end authentication if the message needs to be forwarded by the translator using a different communications protocol which does not support the original format.

Note: Any combination of these circumstances multiplies the difficulties.

### POSSIBLE SOLUTIONS

There are several possible solutions based on an appropriate selection of message handling and authentication techniques:

#### Proxy Agent

A commonly used technique is for the translator itself to validate the original digital signature and then to create a new digital signature based on the new format and the translator’s private key.

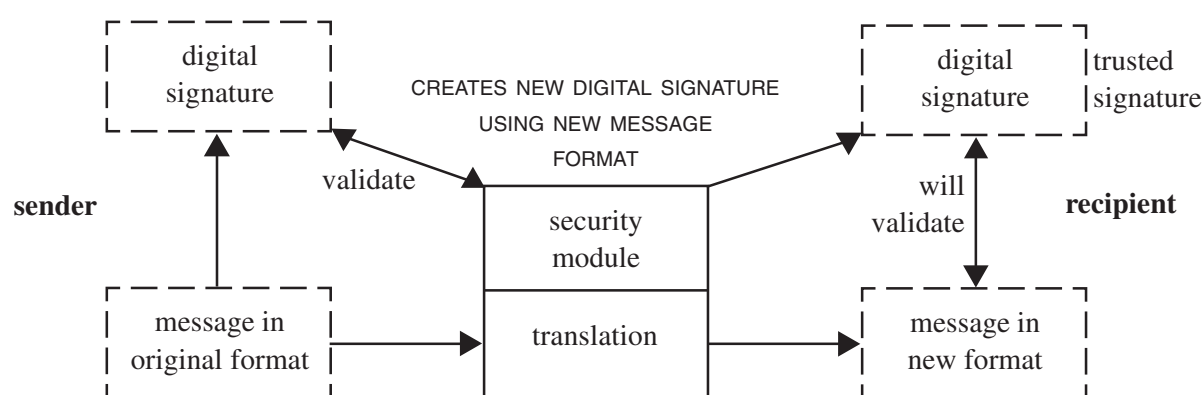


Figure 17: Secure Proxy Agent

In this case the translator assumes the role of a security proxy agent (see above).

## Bypass Technique

Another technique would be for a translated message to be passed by the translator to the recipient accompanied by both the original digital signature and the original message in its original format. The recipient may not be able to read the original message, but would be able to use it to verify the signature. This process requires the recipient to trust the translator to accurately re-format the original message.

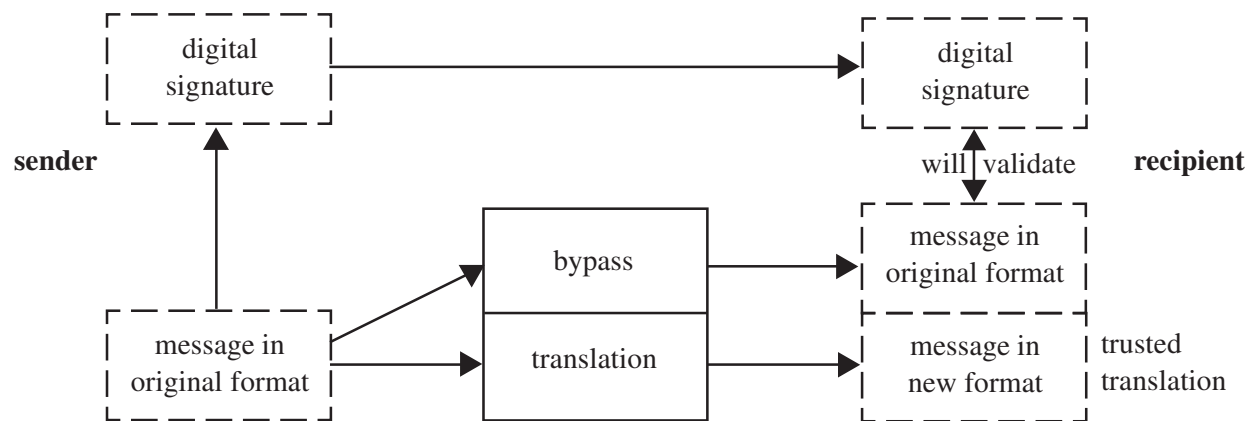


Figure 18: Bypass Technique

## Selective Translation

Certain circumstances (a legal requirement, for example) require that messages should be passed through the translator without any action on the part of the translator that would invalidate end-to-end authentication or validation of a digital signature. This may be accomplished by the careful selection of message formats, communications protocols and authentication techniques.

As an example, one of the techniques that could be used to achieve this objective may be the authentication of only selected sensitive words or fields in the message, possibly by means of Syntax Independent Signatures (SIS) using XML technology.

## Secured Community

End-users may be grouped into a secured community. Communications between each member of the community is effected through a secure clearing-house that incorporates a translator, using any of a number of different cryptographic techniques including that of a security proxy agent. All messages both incoming to and outgoing from the secure clearing-house can be authenticated in a manner appropriate to the requirements of each member of the community.

Such solutions give very great flexibility, but impose on the secure clearing-house the role of a trusted third party and all the participants must agree to this.

## Secure Gateway

To permit members of a secured community to exchange messages with a party who is not a member of that community, the secure clearing-house may provide a secure gateway between the external party and the community using an appropriate authentication technique.

## Electronic Authentication—issues relating to its selection and use

The security of the community is not compromised and the secure clearing-house acts as the secure interface with the external party, using appropriate formats and protocols.

Once again, the translator assumes the role of a trusted third party and all participants including the external party must agree to this.

## Chapter 3

# Public key infrastructure interoperability

As public key infrastructures (PKIs) are being established domestically and in industry sectors, attention is turning to interoperability between those PKIs. Because of the complex nature of PKIs there is a need to consider interoperability at three levels: legal, policy and technical. Initially the task group decided to only address the policy level issues relating to interoperability however as work progressed it became clear that the two other levels needed to be at least partially addressed. Differing implementations of UNCITRAL model laws and identified lack of standards have been addressed in an effort to bridge the differences and identify technical standards requirements.

The objective of the task group is to ensure that business and individuals in each APEC economy have access to a certificate that will allow them to undertake electronic transactions across jurisdictions. This involves ensuring that the certificates meet assurance requirements and have legal effect as required. This is discussed in more detail in the legal issues chapter (Chapter 9).

The basic issues relating to technical interoperability are discussed in the previous chapter. In addition there are now a number of international initiatives addressing technical interoperability such as the UK Communications-Electronic Security Group (CESG) *Secure Messaging and PKI Interoperability Trial*<sup>1</sup> and the European Forum for Electronic Business (EEMA) *PKI Challenge*<sup>2</sup>. Domestic and regional PKI forums have also established interoperability working groups. Within the framework of the Asia PKI Forum, a number of APEC economies are addressing interoperability<sup>3</sup>.

Early approaches to interoperability were premised on one of two basic assumptions:

- large hierarchical structures that would allow interoperability under a common root CA; or
- the existence of a cross-certification agreement between the sender and recipient's CAs or their respective root CAs.

As PKIs began to be established, different models emerged. For commercial and political reasons large hierarchical structures with national root CAs were not established in many economies. Rather national accreditation or licensing schemes for a number of commercially independent PKIs with their own root CAs started to emerge. With these smaller, flatter schemes it is less likely that there will be a cross-certification agreement between the sender and recipient's CAs, particularly in the case of cross border transactions.

---

1 <http://www.cesg.gov.uk/technology/pki/cloud-cover/Final%20Report%20v1-2.pdf>

2 <http://www.eema.org/pki-challenge>

3 <http://www.apectelwg.org/apecdata/telwg/25tel/estg/estg05.htm>

Another emerging trend is for CAs to be accredited under several schemes. As discussed in the legal issues chapter (Chapter 9), legal effect for cross border transactions may require accreditation in the sender's, recipient's or a third jurisdiction. It is therefore necessary for trust paths to be established to the appropriate trust anchor or accreditation process.

For these reasons the then APEC Electronic Authentication Task Group (now the eSecurity Task Group) looked for alternative approaches to achieving PKI Interoperability.

The PKI Forum has also examined a number of different models for interoperability in its *CA-CA Interoperability White Paper*<sup>4</sup>. Most of these models are specific implementations of either cross-certification or cross-recognition. In view of the legal implications of these models they are discussed in more detail in the legal issues chapter (Chapter 9).

A fundamental problem for APEC was to achieve interoperability between economies that used the single economy root CA approach and those that accredited or assessed multiple independent CAs. Another problem encountered was that in some schemes multiple levels of certificates were supported. For that reason part of the APEC approach has been to establish functional equivalence of certificates issued under schemes rather than trying to establish equivalence of the individual CAs operating under those schemes. While a CA's CP and CPS are still an important element of the process, such an approach allows more flexibility for CAs to operate within their own business models.

Furthermore focussing on the accreditation scheme can reduce the demands on users, be they senders or recipients. If they trust the scheme, then they can trust certificates accredited under the scheme without needing to consider the individual CA's CP and CPS. This is particularly the case for schemes where accreditation is required for legal effect or for certain legislated liability aspects.

The accreditation scheme approach also allows the task group to focus on its objective of ensuring the availability of a certificate that can be used for global electronic commerce. It does not need to address all the levels of certificates that might be issued by a particular CA.

While the term 'accreditation' is used in this chapter, a number of the arguments equally apply to other assessment or audit of a CA's compliance with either established criteria or standards or its CP and CPS.

## **ACHIEVING PKI INTEROPERABILITY**

For global electronic commerce (e-commerce) to flourish in a trusted, secure and predictable environment, the interoperability of existing and future electronic authentication schemes is a key issue.

A public key infrastructure offers a mature and integrated electronic security scheme, offering authentication, non-repudiation, confidentiality and integrity. A PKI is defined<sup>5</sup> as the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke certificates based on public-key cryptography.

This section examines in detail two PKI interoperability schemes: cross-certification and cross-recognition. It compares and contrasts the two schemes in terms of their technical implementation, legal and policy implications, and operational requirements. It also proposes a list of actions that can be undertaken to facilitate work leading towards greater interoperability among electronic authentication schemes.

---

4 [http://www.pkiforum.org/pdfs/ca-ca\\_interop.pdf](http://www.pkiforum.org/pdfs/ca-ca_interop.pdf)

5 <http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-08.txt>



Although these two schemes have their roots in PKI, and discussion focuses primarily on PKI, the concepts discussed are potentially extendible and applicable to other electronic authentication schemes.

The study of ‘*cross-certification and the use of a root certification authority, to promote interoperability and trust and to facilitate cross-border electronic commerce*’ was included in the work programme of the *APEC Blueprint for Action on E-Commerce*<sup>6</sup>. The Blueprint was endorsed at the APEC Economic Leaders’ Meeting in Kuala Lumpur, Malaysia on 17–18 November 1998.

At the 19<sup>th</sup> TEL meeting in Miyazaki, Japan, Canada and Singapore presented the joint paper *Cross-Certification Within APEC*<sup>7</sup> and proposed the formation of a cross-certification expert group under the auspices of the then Electronic Authentication Task Group. The proposal was supported by six other economies, including Australia; Hong Kong, China; Japan; Korea; Chinese Taipei and Thailand. Malaysia, who did not attend the meeting, also expressed its support subsequently.

A number of reasons necessitated the expansion of the scope of work of the Cross-Certification Expert Group which subsequently became the PKI Interoperability Expert Group. These included:

- rapid developments in related technologies e.g. validation authorities (VAs);
- complexity of cross-certification, mainly because of the elaborate procedure involved;
- emergence of other interoperability schemes e.g. cross-recognition, that are less elaborate and easier to implement.

These new developments accentuated the need for the expert group to consider the whole spectrum of interoperability issues from a more holistic perspective.

### Terminology

For the purpose of this section whose discussion centres primarily on the PKI, the following terms as defined by the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) Working Group<sup>8,9</sup> are used:

<i>Public-Key Certificate (Certificate)</i>	<i>A record that 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).</i>
<i>Certification Authority (CA)</i>	<i>An authority trusted by one or more users to create and assign certificates. Optionally the CA may create the user’s keys.</i>
<i>Registration Authority (RA)</i>	<i>An optional entity given responsibility for performing some of the administrative tasks necessary in the registration of subjects, such as</i> <ul style="list-style-type: none"><li>• <i>confirming the subject’s identity,</i></li><li>• <i>validating that the subject is entitled to have the attributes requested in a certificate, and</i></li><li>• <i>verifying that the subject has possession of the private key associated with the public key requested for a certificate.</i></li></ul>

6 APEC Electronic Commerce Task Force, Nov 1998, *APEC Blueprint for Action on E-Commerce*, [http://www.dfat.gov.au/apec/ecom/ecom\\_blueprint.html](http://www.dfat.gov.au/apec/ecom/ecom_blueprint.html)

7 Communications Security Establishment, Canada and National Computer Board, Singapore, Mar 1999, *Cross-Certification Within APEC*

8 IETF-PKIX Working Group, Jun 1999, *Internet X.509 Public Key Infrastructure PKIX Roadmap*. <http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-08.txt>

9 IETF-PKIX Working Group, Mar 1999, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. <ftp://ftp.isi.edu/in-notes/rfc2527.txt>

## Electronic Authentication—issues relating to its selection and use

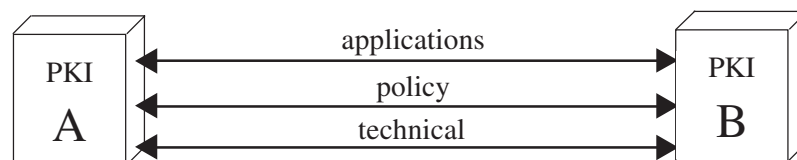
<i>Relying Party</i>	<i>A user or agent (such as a client or server) who relies on the data in a certificate to make decisions.</i>
<i>Subject (Subscriber)</i>	<i>A subject is the entity (CA or end-entity) named in a certificate. Subjects can be human users, computers (as represented by DNS names or IP addresses), or even software agents.</i>
<i>CA-Certificate</i>	<i>A certificate for one CA's public key issued by another CA.</i>
<i>Certificate Policy (CP)</i>	<i>A named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.</i>
<i>Certification Practice Statement (CPS)</i>	<i>A statement of the practices which a CA employs in issuing certificates.</i>

To maintain consistency in the use of terminology in the area of electronic authentication in general within the task group, these PKI-centric terms are mapped to their corresponding technology-neutral terms as defined in the Chapter 1 of this report in Appendix 1.

### Analysing PKI Interoperability Schemes

In this section, the following three-tier framework (Figure 19) is used to examine and analyse the two PKI interoperability schemes: cross-certification and cross-recognition.

- **Technical.** Can the two PKI domains interoperate with each other ('talk to each other') from a technical perspective? Specifically, can the directory system in one of the PKI domains access the directory system of the other PKI domain? In addition, can one of the PKI systems process certificates generated by the other PKI system?
- **Policy.** Are the certification policies (CP) and certificate practice statements (CPS) associated with both PKI domains compatible for the application or service at hand to operate?
- **Applications and Services.** What kind of PKI-enabled applications and services can most ideally be supported by the PKI interoperability scheme?



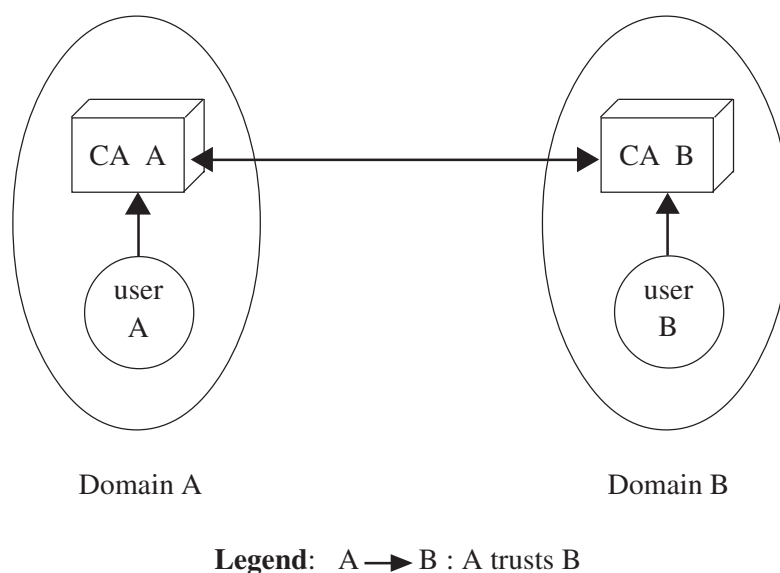
**Figure 19: A Framework for Analysing PKI Interoperability Schemes**

## Cross-Certification

There is a myriad of definitions for cross-certification from various sources. (See Appendix 2 for a selection of these definitions.) For the purpose of this section, the following definition adapted from the general issues chapter (Chapter 1) is used: *the practice of cross-recognition of another CA's public key to an agreed level of confidence and is normally evidenced in a contract or agreement.*

Essentially, cross-certification results in two PKI domains (in whole or in part) being merged into one larger domain through an elaborate process carried out by two representative CAs. For hierarchical PKIs, the representative CA is usually the root CA. However, cross-certification can also be implemented between any two CAs. In the latter case, each PKI domain constitutes only one CA and its subscribers.

In Figure 20, after CA-A and CA-B cross-certify with each other, User A and User B would be able to transact with each other. The cross-certification process between CA-A and CA-B is transparent to both User A and User B. To User A, User B is simply another subscriber within the extended PKI. The same applies to User B for User A.



**Figure 20: Cross-certification Between Two CAs : CA-A and CA-B**

Cross-certification entails an elaborate process that involves technical interoperability and harmonisation of CPs and CPSs . All these take place within the context of the cross-domain applications and services that the merged PKI is meant to support.

As discussed in the introduction to the PKI interoperability framework the cross-certified PKI domains must communicate at a technical level. This involves first a sharing of their two respective directories of certificates such that each PKI domain can access the directory and hence the certificates generated by the opposite PKI domain. Both representing CAs exchange certificates with each other, generating a new pair of certificates called the cross-certificates. This has the similar effect of mutually extending each PKI domain to include the cross-certified PKI domain.

International technical standards are instrumental in ensuring technical interoperability across different PKI systems. Both the IETF-PKIX Working Group and RSA (in their PKCS Standards) are leading the work in this area. However, at the point of writing this report, technical interoperability standards for PKI are still rather fluid and have yet to reach a maturity stage. Moreover, the PKI technology market is traditionally characterised by a number of proprietary players that adopt technologies that do not interoperate with one another<sup>10</sup>.

Fortunately, there has been growing general awareness of the need for greater technical interoperability. This is also fast becoming a key agenda for most PKI technologies today. For example at the RSA'99 Data Security Conference in California, USA in January 1999, the participating technical vendors vouched to adopt open standards and improve technical interoperability with the products of their competitors<sup>11</sup>. Concrete steps such as participation in standards bodies by technology vendors, incorporation of PKI open standards into products, and organisation of talks and seminars to promote interoperability will pave the way for greater technical interoperability in the near future.

Traditionally, cross-certification has incorrectly been equated with only technical interoperability. As aptly clarified in the general issues chapter (Chapter 1), the process of cross-certification includes *legal, technical and policy review of each others authentication scheme policies* (CPs in the PKI context) *and authentication scheme practice statements*, (CPSs in the PKI context) *implementation and operational management*.

The harmonisation of CPs and CPSs is necessary to ensure that both PKI domains are compatible in terms of their certificate management operations (i.e. certificate issuance, certificate suspension and revocation) and adhere to similar operational and management conditions and environments. Other issues such as operational and security requirements, and the amount of liability coverage are also taken into consideration.

The complexity of this policy harmonisation step is easy to comprehend, considering the scope of issues covered in the documents. Moreover, the general trend of an increase in size in these documents further complicates the process. Furthermore, one CP typically corresponds to one specific level of assurance in terms of the type of certificates the CP supports. Hence, depending on the nature of the cross-certification arrangement, multiple CPs may need to be harmonised. It is for this reason that the task group's work is focussing on specific types of certificates.

No doubt, it seems that there is no panacea to ease the harmonisation of CPs and CPSs. Nevertheless, this process can potentially be facilitated if the CPs are authored in adherence to the standards defined by IETF-PKIX in *RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*<sup>12</sup>. In the event that both CPs and CPSs are too diverse to be harmonised, a new common CP or CPS can be jointly developed and adopted by both parties.

In general, cross-certification is relevant for relatively closed business models, and at best, open-but-bounded systems as defined in the general issues chapter of this report. It is most suitable if the two PKI domains belong to two work contexts that share a close working relationship with each other. For example, both work domains may share the set of applications and services, such as email and financial applications. In addition, cross-certification can certainly be simplified if the two PKI

---

10 The Burton Group, Jul 1997, *Network Strategy Report – Public Key Infrastructure Architecture*. <http://www.tbg.com/samples/netsvcs/pkiarc.htm>

11 Rutrell Yasin, 25 Jan 1999, Internet Week Issue 749, Section: News & Analysis, *Vendors Adding to PKI Interoperability*. <http://www.techweb.com/se/directlink.cgi?INW19990125S0025>

Rutrell Yasin, 18 Jan 1999, Internet Week Issue 748, Section: News & Analysis, *PKI Heads for Mainstream*. <http://www.techweb.com/se/directlink.cgi?INW19990118S0003>

12 <http://www.ietf.org/rfc/rfc2527.txt?number=2527>

domains employ technically compatible or interoperable systems, have congruent policies and reside in economies with the same legal structures in this area.

In summary, a number of advantages and disadvantages of cross-certification can be inferred.

The two primary advantages of cross-certification are as follows:

- **Transaction Flow.** Cross-border transactions can be carried out seamlessly, as cross-certification essentially marries two PKI domains into a single larger domain.
- **User Transparency.** The cross-certification arrangement is transparent to the user.

The disadvantages of cross-certification are as follows:

- **Process.** The process of cross-certification is complex. Apart from technical interoperability, relatively detailed mapping of PKI policies and practices is required.
- **Scalability.** In terms of scalability, the effort required for cross-certification increases exponentially with the inclusion of every new PKI domain as discussed in the asymmetric cryptography chapter (Chapter 2).
- **Business Case.** This is strictly speaking, an implication of the above two disadvantages. As a result of the complexity and poor scalability of cross-certification, it is relatively more difficult to justify the need for cross-certification in a business sense. Furthermore, a PKI may demand cross-certification to mutually exchange certificates—this will drive the business case.
- **Third Jurisdiction.** Cross-certification may not address recognition in a third jurisdiction unless there are appropriate cross-certificates with that jurisdiction.

### Bridge Certification Authorities

One approach to the scalability problem has been the establishment of bridge certification authorities. In this approach a number of CAs can cross-certify with the bridge rather than having to establish individual cross-certification agreements between each other. It is a ‘hub and spokes’ approach rather than a ‘mesh’ approach. Such arrangements have been established by the US Government<sup>13</sup> and are being considered by other economies.

### Unilateral Cross-Certification

This is a special case of cross-certification whereby one PKI domain trusts another PKI domain but not vice versa. In a way, the term unilateral cross-certification is a misnomer as the words ‘unilateral’ and ‘cross’ are paradoxical to each other. Technically, this is an atypical scenario, but this is discussed briefly to ensure the completeness of this report.

Generally, the above discussion pertaining to bilateral cross-certification applies to a unilateral cross-certification arrangement as well. However, in such a one-way trust relationship, the PKI domain that chooses to exercise the trust relationship (the ‘truster’) is at the complete mercy of the trusted PKI domain. Hence, apart from technical interoperability, there is no harmonisation process whatsoever in the areas of PKI policy. The truster has to unilaterally ensure that its policies are compatible with those of the trusted PKI domain.

Comparatively, there are also seemingly fewer applications and services that warrant such an unbalanced arrangement. These applications and services conceivably share the common trait that the trust required in the transactions involved is unilateral. An example of such an application is a

---

<sup>13</sup> <http://csrc.nist.gov/pki/fbca/welcome.html>

shopping-like application in which the merchant has to prove to the customer his or her identify before the latter submits a private piece of information.

One use of unilateral cross-certificates is starting to emerge in the form of electronic accreditation certificates. Such an approach has been proposed for the Australian Government PKI Gatekeeper<sup>14</sup> and is being considered for other accreditation schemes. This approach could involve the issue of a unilateral certificate from the accreditation body to CAs accredited under the scheme. In this case the term ‘unidirectional’ may be more appropriate than ‘unilateral’ as there is an agreement between the parties. The use of accreditation certificates can facilitate the cross-recognition approach discussed below.

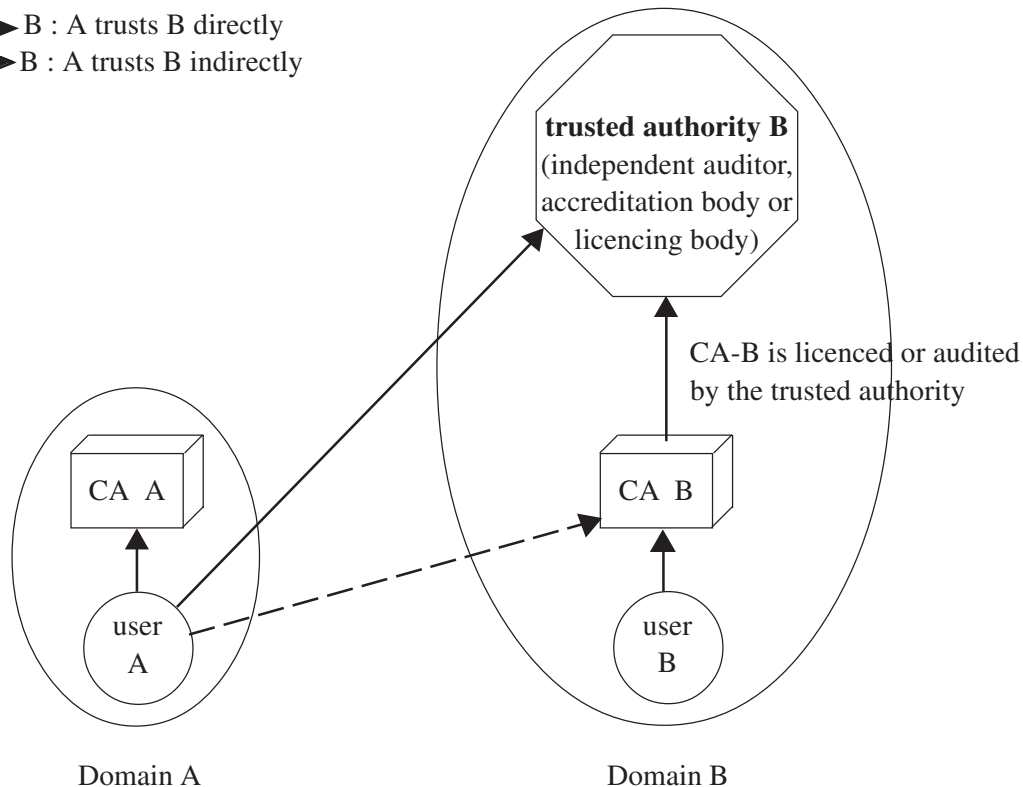
### Cross-Recognition

First coined by the then Electronic Authentication Task Group, cross-recognition can be defined as *an interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a subject in the other PKI domain, and vice-versa.*

Such authority information is typically the result of either a formal licensing or accreditation process in the economy of the other PKI domain, or a formal audit process performed on the representative CA of the PKI domain. Technically, the information can be stored as the value of a certificate field accessible by the relying party or can be evidenced by an electronic accreditation certificate.

Compared to cross-certification, the onus of whether to trust a foreign PKI domain lies with the relying party or the owner of the application or service, rather than a CA that the relying party directly trusts. Also, cross-recognition can be seen as constituting one or two unilateral trusts relationships, unlike cross-certification which is, in most cases, bi-directional (except in a unilateral cross-certification arrangement as above).

**Legend:** A → B : A trusts B directly  
 A ···→ B : A trusts B indirectly



**Figure 21: Illustration of the Concept of Cross-recognition (How User A trusts User B)**

<sup>14</sup> <http://www.govonline.gov.au/projects/publickey/gac.htm>



Consider Figure 21. CA-A and CA-B are not cross-certified with each other. User A trusts User B because CA-B, which issues User B's certificate, has either been licensed by a CA licensing body in Domain B or has been formally audited by an independent auditor. The trust relationship can be represented symbolically as follows:

User A  $\rightarrow$  Trusted Authority B  $\rightarrow$  CA-B  $\rightarrow$  User B

Hence, User A  $\rightarrow$  User B.

Similarly (vice-versa),

User B  $\rightarrow$  Trusted Authority A (not shown)  $\rightarrow$  CA-A  $\rightarrow$  User A

Hence, User B  $\rightarrow$  User A

Collectively, User A cross-recognises User B.

Like cross-certification, a cross-recognition arrangement entails issues pertaining to technical interoperability and policy compatibility. However, in cross-recognition, the decision of whether to trust a foreign certificate lies with the relying party and not its CA. It does not necessarily involve a contract or an agreement between two PKI domains. Hence, the process is comparatively less complicated.

Unlike cross-certification which requires almost full technical interoperability between two PKI systems, the necessity for technical interoperability in a cross-recognition arrangement is brought

down to the application level. There still needs to be interoperability in all aspects such as algorithms, protocols, key lengths. The application must be able to process the information in the foreign certificate. Moreover, it must be able to access the directory system of the foreign PKI domain to validate the status of the foreign certificate.

If the application is developed to accept certificates issued by many different foreign CAs, it must then be able to process all these different certificates. Compared to a cross-certification arrangement, this is perhaps the most difficult issue. Although most digital certificates today are compliant with the X.509 Version 3 standard, the interpretation of certificate fields and the use of certificate extensions can vary across PKIs<sup>15</sup>.

With the event of VAs, technical interoperability can potentially cease to be an issue in a cross-recognition arrangement. As VAs are established specifically to manage certificates from a wide variety of certification revocation systems and directory systems, it is arguably much more applicable in the cross-recognition scheme than the cross-certification scheme.

In a cross-recognition arrangement, detailed mapping of CPs and CPSs is not necessary. Instead, the relying party (via the application at hand) decides whether to accept a foreign certificate for the purpose depending on whether the certificate has been issued by a trustworthy foreign CA. The CA is regarded as trustworthy if it has been licensed or accredited by a formal licensing or accreditation body or has been audited by a trusted independent party. Also, the relying party must be able to unilaterally make an informed judgement based on the policies stipulated in the CP or CPS in the foreign PKI domain.

In contrast with cross-certification which is most suitably implemented in a closed or open-but-bounded business model, cross-recognition is ideal for open systems as discussed in the general issues chapter (Chapter 1) of this report.

---

<sup>15</sup> IETF-PKIX Working Group, Jan 1999, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. <ftp://ftp.isi.edu/in-notes/rfc2459.txt>

In addition, congruent with the less elaborate interoperability process required, cross-recognition is suitable for applications that require a relatively lower level of trust.

Similarly, a number of advantages and disadvantages of cross-recognition can be inferred from the discussion above.

The advantages of cross-recognition are as follows:

- **Implementation.** Cross-recognition involves a relatively less complex process than cross-certification, especially in terms of policy and legal harmonisation.
- **Scalability.** Cross-recognition supports potentially an unlimited scope of interoperable PKI domains, subject to technical interoperability.

The disadvantages of cross-recognition are as follows:

- **User Transparency.** The need to be an informed relying party is a potential burden to the user. An uninformed user might not be aware of the full consequences of choosing to trust a foreign user that it should not.
- **Assurance.** Cross-recognition can be procedurally less rigorous than cross-certification. This may impact on whether the level of trust is fit for purpose.

### **Liability Implications of Cross-Certification and Cross-Recognition**

Liability is a key issue in any e-commerce transaction. In a cross-border context, the question of who should bear liability when a fraud occurs is made even more complex.

In a cross-certification arrangement, one would generally expect the local CAs to bear the bulk of the liabilities (depending on which domain is proven to be at fault, and any prior agreement between the two cross-certified CAs). On the other hand, one would assume the relying parties in a cross-recognition arrangement to cover most of the liabilities as it is their responsibility to decide whether or not to trust the foreign subjects.

Most of digital signature laws are deliberately crafted to limit the liabilities of CAs so as to provide them with the necessary legal support to enable trusted e-commerce to flourish. Moreover, there is a general propensity for CAs to protect themselves. Hence, apart from the legal support from the digital signature laws, CAs would generally tend to shift as much of the liabilities to the subscribers and relying parties by stipulating liability caps in the CA service contractual agreement and CPS/CP.

The amount of liabilities that the relying parties in both arrangements would have to bear is arguably not significantly different. In the long run, CAs might choose to take on greater liabilities to be more competitive than competing CAs, or to leverage on the risk management schemes and services offered by insurance companies.

### **Legal Implications of Cross-Certification and Cross-Recognition**

The essence in the legal implications of our discussion of PKI interoperability lies in the validity of an electronic transaction that is performed by virtue of a cross-certification or cross-recognition arrangement, especially within a cross-border context. For such a transaction that spans across two different PKI domains in different economies and hence jurisdictions, is the transaction legally recognised? If not, what is the necessary supporting legislation, if legislation is required at all?



This legal issue has been singled out as a separate topic in this section (instead of being included as an element of PKI interoperability) as it is an element that is generally beyond the direct control of the two interoperable PKI domains. Nevertheless, it is a factor that can adversely affect the effective implementation of cross-certification and cross-recognition.

For global e-commerce to happen at the exponential rate predicted by most people, some formal recognition needs to be given to electronic transactions conducted within a cross-certification or cross-recognition arrangement. This would entail the harmonisation of laws pertaining to the electronic transactions and digital signature between different jurisdictions. However, it is arguable whether direct legal support for cross-certification or cross-recognition is needed. (If necessary, this can take the form of legislation that stipulates the requirements of a valid cross-certification arrangement, or laws that allow local CAs to recognise digital certificates issued by foreign CAs.)

Increasingly countries have implemented laws related to digital signatures, electronic transactions and the use of electronic authentication schemes. These laws vary in focus and approach (e.g. different CA licensing or assessment schemes, different degrees of technology neutrality) and may be difficult to harmonise. Also, few of these existing laws or regulations however have specific clauses supporting cross-certification or cross-recognition. This is addressed in more detail in the legal issues chapter (Chapter 9).

### **Certificate Trust Lists**

Certificate trust lists are in effect directories, either online or offline, containing information that can establish trust in a certificate issued under a particular scheme. The most common implementation is in browsers where root certificates of a number of schemes are included when shipped and updated as part of the update process. However, the browsers include a capability to allow users to import other root certificates as required. This has the potential to be exploited by malicious code that could add false root certificates. Some proprietary applications have addressed this problem by digitally signing the trust list.

Certificate trust lists can also be used to support both cross-certification and cross-recognition. Directories of cross-certificates maintained by CAs, including bridge CAs, are a form of certificate trust list. In cross-recognition the accreditation or licensing body will typically need to advise the CAs it has accredited. While this can be done through an accreditation certificate as discussed earlier, it could also be done by publishing a list of those CAs possibly also including the public keys of those CAs. In both cases the trust lists can be digitally signed. Users can either regularly download the lists or access them as required. Where cross-certificates or the public keys of accredited CAs are stored in the trust lists, applications can establish the appropriate trust paths.

The European Electronic Signature Standardization Initiative has been examining a similar approach in its *Provision of harmonized Trust Service Provider status information*<sup>16</sup> project. This project is developing a methodology to provide information about the trust scheme, and a list of approved trust service providers.

Where trust lists are created by accreditation or licensing bodies established under legislation that requires such accreditation to give legal effect or specific legal presumptions, such lists can evidence that legal effect particularly in cross-jurisdictional transactions. This is discussed in more detail in the legal issues chapter (Chapter 9).

---

<sup>16</sup> [http://portal.etsi.org/sec/el-sign.asp#TR\\_102\\_030](http://portal.etsi.org/sec/el-sign.asp#TR_102_030)

## Possible Areas of Work

To increase adoption of global e-commerce in a trusted and conducive environment, the task group can work with other international organisations and technical standard bodies to facilitate cross-certification and cross-recognition arrangement.

The following areas of work are recommended:

- **Promote greater awareness of the importance of interoperability for cross-border e-commerce.** Through a combination of both formal and informal means (such as seminars, conferences, and email exchange), the task group can facilitate the exchange of information about the different laws, policies and technical developments related to PKI. This can help to foster greater understanding of the different PKI regimes within the APEC economies, and greater awareness of the importance of interoperability for cross-border e-commerce to flourish. One concrete step is to design and implement a PKI information bank that can serve as a one-stop, non-stop online resource of such information.
- **Promote cross-border pilot trials and feedback.** The lack of truly compelling applications and services (or ‘killer applications’) to make cross-certification and cross-recognition realise their full potential has often been named as a key concern. By working with APEC members from other economic sectors, the task group can help to identify potential cross-border applications and services and facilitate cross-border trials and pilot projects among the economies.
- **Examine the need for a generic framework of technical and policy procedures.** By working with the private sector, as well as other international organisations and technical standard bodies that have ongoing work in interoperability, the task group can evaluate the need for a generic framework of technical and policy procedures that will facilitate cross-certification and cross-recognition between any two PKI domains.
- **Develop a program of action for interoperability within APEC.** Through collective studying of the various interoperability schemes, and monitoring developments in electronic authentication technologies, the task group can develop what will eventually result in a network of interoperable PKIs among member economies. This can begin with a number of pilot trials and constant feedback as discussed earlier.

## MAPPING OF CERTIFICATION AUTHORITIES ACCREDITATION SCHEMES<sup>17</sup>

The Telecommunications and Information (TEL) Working Group is leading the development of many aspects of electronic commerce in APEC. This is in response to instructions from leaders and from trade ministers who agreed that electronic commerce is a potential catalyst for economic growth in the region. Within the TEL, the Business Facilitation Steering Group, the eSecurity Task Group and the PKI Interoperability Expert Group are continuing their efforts to work with the private sector to build trust and confidence in electronic business processes. The focus continues to be on developing an understanding of approaches to authentication and certification that can serve as policy models for member economies, and that will eventually facilitate electronic commerce among businesses in the region.

In this regard, the PKI Interoperability Expert Group has been carrying out a project that will assist member economies in identifying and mapping the certification authority and accreditation linkages that are necessary for organisations to securely interact and to transact with each other electronically across jurisdictional boundaries.

---

<sup>17</sup> This section is based upon a study performed by DOMUS IT Security Laboratory for the Canadian Department of Industry (Industry Canada).

It is recognised that there are differences in some of the approaches being taken. The value in the project is that it facilitates a pulling together of the different approaches and provides an analysis of how the variances might be adapted to meet the same objectives. This could lead to interoperable e-commerce across the region. It is already becoming apparent that different business models have emerged and the criteria critical to an assessment of a certificate's trust may appear in different locations. This mapping exercise will help to encourage and facilitate real marketplace interoperability by highlighting commonalities and moreover recognising where differences need to be addressed.

The project has the potential to speed up the development of policies and processes that will enable interoperability across the region.

While the following discussion refers to accreditation, the same process can be applied to other formally structured assessment and audit schemes.

### Terminology

For the purposes of this section, the following terminology is used:

Certificate Authority (CA)	A certificate authority includes the elements involved in managing certificates, such as directory services and registration services, as applicable. The use of this term in this section covers all these elements regardless of whether they are carried out by a single or several parties.
Certificate Policies (CP)	Certificate policies state the security and other policy requirements ('what') the CA must satisfy. This is also referred to as 'policy'.
Certificate Practice Statements (CPS)	Certificate practice statements document 'how' the requirements are to be satisfied within a particular CA policy domain. This is also referred to as 'practices'.

### Implementation Policies and Practices

There are three primary dimensions to the business environments within which CAs must operate:

- different legal jurisdictions,
- different business models' and
- a broad spectrum of security policies.

The global electronic commerce environment is evolving toward the use of electronic signatures that will be generated within a mix of legal jurisdictions. Some jurisdictions could require regulated or licensed CAs, while others will allow for certification accreditation in non-regulated regimes.

Different business models are emerging in which third parties may carry out the processes generally associated with CAs. Further, it is becoming evident that different applications will likely require a broad range of security policies to support differing levels of trust in a variety of business environments. A common understanding of security policies and related criteria could help facilitate cross border authentication between different jurisdictions. Such norms are required to:

- define the multiple security policy and business model environments;
- define the legal jurisdiction requirements;

- establish the management practices suitable for the multiple security policy and business model environments; and
- facilitate recognition of the level of trustworthiness of digital signatures and their level of trustworthiness across different policy domains. This process of formally evaluating and certifying the trustworthiness is often referred to as ‘accreditation’.

## Accreditation Approach

A common approach to accreditation can form the basis for recognition of CAs between different jurisdictions with different licensing or regulatory requirements. Common accreditation standards and processes can be used to facilitate sound and consistent legal and technical practices across different legal jurisdictions. The Internet Engineering Task Force (IETF) *Internet X509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527)*<sup>18</sup> could serve as guidance for a common CA accreditation approach.

## Accreditation Roles and Interaction

While terminology and processes may vary across the international jurisdictions, there is an evolving recognition that accreditation would somehow involve interaction of players, legal entities, parties, or agents having the following roles:

**Competent Authority.** An agent of the legal jurisdiction or community of interest. It is responsible, within the jurisdiction or community, for a number of actions that could include some or all of the following:

- defining the policy and legal environment within which the accreditation scheme must operate,
- negotiating with other competent authorities to ensure harmonisation across differing legal jurisdictions,
- issuing licenses, authorisations, regulations or other government or legal recognition to various CAs,
- setting minimum policy requirements for advancing CA accreditation schemes across differing legal jurisdictions and communities of interest,
- giving formal recognition to standards, criteria and frameworks for advancing the compatibility of accreditation approaches across differing legal jurisdictions,
- approving and giving formal recognition to the accreditation approach, and
- giving formal recognition to an evaluator accreditation body, which is chartered to carry out the accreditation of evaluators.

**Evaluator Accreditation Body.** An independent body, industry association or other agency which could be recognised by the competent authority or could function on the basis of trust relationships with evaluators or policy authorities. It is responsible for:

- approving and giving formal recognition that evaluators are professionally competent to perform evaluations of compliance to appropriate policies or other requirements which may be provided by the competent authority’, and
- sanctioning, selecting and developing policy compliance, evaluation guidance, criteria and standards.

**Evaluator.** An independent agent, member of an accounting body, financial institution or other qualified professional that is trusted by the policy authority. The evaluator accreditation body could

---

<sup>18</sup> <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-01.txt>

formally recognise evaluators, if such entities existed in that jurisdiction or community of interest. It is responsible for:

- evaluating the operational authority's compliance to the CA policy;
- using specific evaluation guidance, criteria and standards sanctioned by the evaluator accreditation body, to determine that:
  - there are adequate controls in place, and
  - these controls are operating effectively, such that reliance can be placed on transactions that are recorded, processed, executed or maintained by the operational authority in question;
- evaluating other evidence of compliance with the certificate policy, where the parties have effected obligations through mechanisms such as contracts and membership agreements and through the implementation of related operational safeguards or business methods (For specific policy requirements, an external reference may be sufficient to convey an understanding to the evaluator, of the relevant material practices of the domain.);
- producing a CA policy compliance evaluation report. The potential users of an evaluation report include:
  - relying parties who have a significant interest in knowing that a scheme's practices operate with sufficient effectiveness to achieve the requirements within the certificate policy;
  - subscribers who have an interest in knowing that the CA is meeting the requirements of the certificate policy;
  - competent authorities, recognising that an audit is an important component of any authorisation, regulation, licensing or other recognition process, would utilise the evaluation report as part of the initial and on-going recognition process; and
  - policy authorities, who are a primary user of the evaluation report, recognise that the audit is one of the requirements of the certificate policy, that it demonstrates CA compliance with that policy, and utilise it in any cross-certification negotiations; and
  - operational authorities. While the evaluation report is not intended to provide recommendations for improvement in the internal controls of a CA, a value-added benefit of the CA compliance evaluation would often include observations of the auditor for improvements in operations.

**Security Accreditation Authority.** An agent of the CA domain or enterprise. The security accreditation authority is responsible for:

- approving the operation of the CA in a particular mode using particular safeguards, and
- accepting residual security risks on behalf of the CA domain or enterprise.

**Policy Authority.** An agent of the CA domain or enterprise. The policy authority is responsible for:

- selecting or defining documentation for use in the CA domain or organisational enterprise,
- approving any cross-certification or interoperability agreements with external domains,
- approving practices which the CA must follow, by reviewing the CPS to ensure consistency with the CP; and
- providing policy direction to the operational authority.

**Operational Authority.** An agent of the CA domain or enterprise. It should be noted that in some business models, there might be several operational authorities involved in the process of generating a certificate. In most cases, all elements of the CA domain or enterprise must be accredited to establish

the required level of trust for a particular certificate. The operational authority is responsible to the policy authority for:

- interpreting the certificate policies that were selected or defined by the policy authority;
- developing the practices documenting compliance to the policies and other requirements;
- ensuring that the practice statements are updated as required; and
- operating the CA or scheme in accordance with the practice statements.

**Subscriber.** A member of the CA domain or enterprise. The subscriber is a party who is the subject of a certificate and who is capable of using, and is authorised to use, the private key, that corresponds to the public key in the certificate. Responsibilities and obligations of the subscriber would be as required by the CA's policy.

**Relying Party.** May or may not be a subscriber of the same domain. The relying party is a recipient of a certificate who acts in reliance on those certificates or digital signatures verified using that certificate.

### Accreditation Framework

Figure 22 illustrates the relationships between the various roles. To accommodate either the needs of the legal jurisdiction or closed and open business models, unique CA accreditation models can be postulated by combining roles.

Using the approach in Figure 22, it may be possible to reach a common terminology and to facilitate analysis and comparison of accreditation approaches of various economies. Through this proposal it is expected that the PKI Interoperability Expert Group will be able to:

- identify the key elements for establishing trust in certification processes;
- map existing schemes against these key elements; and
- identify potential obstacles to cross border authentication.

The following questions could be considered by economies in undertaking mappings.

- Have governments, agencies, or private sector entities developed policies that correspond to aspects of the model?
- In relation to the model, where do policy gaps exist domestically?
- Will the current model facilitate interoperability across jurisdictions or in what ways should it be modified?

By using the above approach, APEC will be able to provide guidance for member economies when developing their national approach in such a manner that interoperability can be achieved. For successful rollout of secure electronic commerce, it is essential that a common understanding be achieved across such diverse stakeholders, such as the product vendors, service providers and regulatory authorities.

It has been noted that a number of APEC economies are attempting to achieve interoperability of public key schemes through other initiatives. Those exercises are a potential source of information for this project.

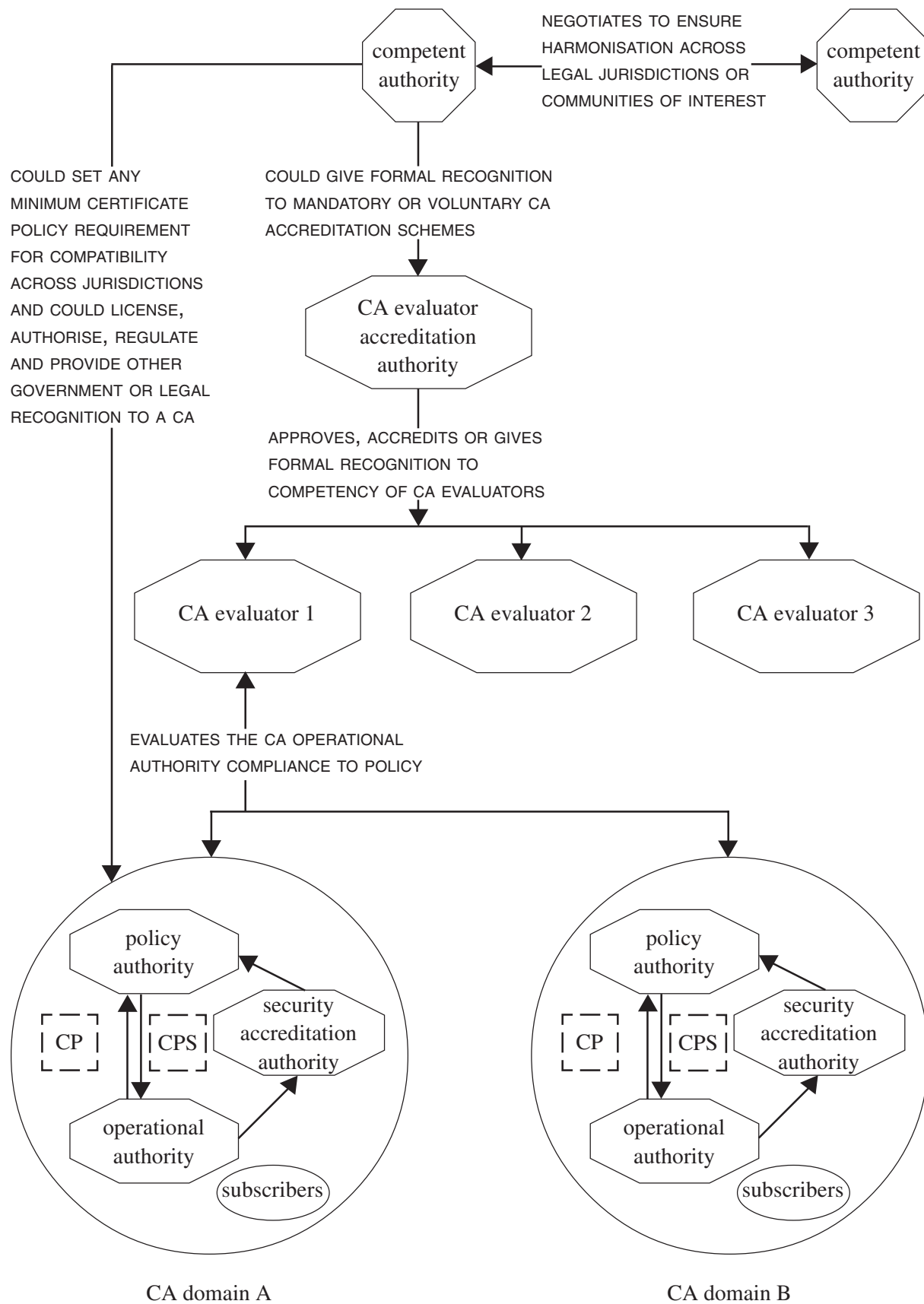


Figure 22: Certificate Authority Accreditation Model



## INITIAL MAPPING OF CERTIFICATION AUTHORITIES ACCREDITATION SCHEMES

Using the methodology set out above, the PKI Interoperability Expert Group undertook two surveys of APEC economies to identify and map the key elements for establishing trust in certification processes and to map the approaches being taken in the various member economies against these elements. The purpose of the surveys was to highlight commonalities, identify policy gaps and provide a framework for analysis of how the variances could be addressed.

### Process

The first survey involved two rounds. The following questions or requests, which related to the building blocks for establishing certification authority linkages, were circulated to all economies and were used for the first round:

1. *Is there implemented or planned implementation of a government PKI scheme?*
2. *Describe how PKIs work or would work together within the economy and internationally.*
3. *If PKI is not used or planned, how will e-commerce be implemented?*
4. *What legislation is used to govern electronic or digital signatures?*
5. *Provide a brief description of the legislation.*
6. *Is industry embracing e-commerce? In what way – via internet browsers, PKI or none?*
7. *What major CA services are available and used?*
8. *What secure services are used, SSL, PIN or Password, PKI or other?*
9. *Is there a Competent Authority function. Who is responsible, how does it work?*
10. *Is there an ‘CA Evaluator Accreditation Authority’? Who is responsible, how does it work?*
11. *Are there ‘CA Evaluators’ or equivalent? Who is responsible, how does it work?*
12. *Is there a ‘Security Accreditation Authority’ function? Who is responsible, how does it work?*
13. *Is there a ‘Policy Authority’ function? Who is responsible, how does it work?*
14. *Is there an ‘Operational Authority’ function? Who is responsible, how does it work?*
15. *Have policies been developed that correspond to the model? Describe the policies.*
16. *What work, if any, is being done to enable e-commerce across different jurisdictions?*
17. *What work, if any, is being done to enable e-commerce between government and industry?*
18. *Provide any comments or remarks to assist the project in determining barriers to interoperability.*

Initial responses were received from eight member economies (Australia; Canada; Hong Kong, China; Japan; Korea; Singapore; Chinese Taipei and Thailand). A document that consolidated the responses from each economy and presented preliminary findings was discussed at TEL 23 in March 2001<sup>19</sup>.

During discussion of the exercise at TEL 23, it was agreed that updated input should be sought. It was also agreed that the questions should be refined to remove certain ambiguities and be refocused to

---

<sup>19</sup> [http://www.apectelwg.org/apecdata/telwg/23tel/estg/estg\\_03.doc](http://www.apectelwg.org/apecdata/telwg/23tel/estg/estg_03.doc)

make a distinction between the public and private sector in the responses. A revised set of questions was developed and provided to member economies for responses. The questions were:

**Legislative and Legal Framework:**

1. *What legislation is used to govern electronic or digital signatures? (Please, provide a brief description of the legislation).*
2. *Is accreditation or licensing of trusted agents (i.e. CAs) required for legal effect within the economy? If yes, please provide details of the competent authority and scheme in Questions 10–16 below.*
3. *Is accreditation or licensing of trusted agents (i.e. CAs) required to give legal effect from foreign jurisdictions? Please provide details of the process in Question 17.*

**Current Private Sector Environment:**

4. *Is industry embracing e-commerce? In what way: via Internet browsers, PKI or none?*
5. *What secure services are used, SSL, PIN or Password, PKI or other?*
6. *What major CA services are available and used?*

**E-Government Initiatives:**

7. *Is there implemented or planned implementation of a government PKI scheme? Please describe.*
8. *If PKI is not used or planned, how will e-commerce be implemented?*
9. *What work, if any, is being done to enable e-commerce between government and industry?*

**Roles and Responsibilities:**

*For each of the following questions, please report separately on public sector and private sector implementations. Please refer to the schematic to see how the roles have been generically broken down:*

10. *Is there a 'Competent Authority' function? Who is responsible, how does it work?*
11. *Is there an 'CA Evaluator Accreditation Authority'? Who is responsible, how does it work?*
12. *Are there 'CA Evaluators' or equivalent? Who is responsible, how does it work?*
13. *Is there a 'Security Accreditation Authority' function? Who is responsible, how does it work?*
14. *Is there a 'Policy Authority' function? Who is responsible, how does it work?*
15. *Is there an 'Operational Authority' function? Who is responsible, how does it work?*
16. *Have policies been developed that correspond to the model? Describe the policies.*

**Interoperability and International Dimensions:**

17. *Describe how PKIs work, or would work together, within the economy and internationally.*
18. *What work, if any, is being done to enable e-commerce across different jurisdictions?*
19. *Provide any comments or remarks to assist the project in determining barriers to interoperability.*

In the second round, six of the original eight member economies updated their input in accordance with the revised set of questions. Responses were received from two additional member economies (Malaysia and the United States). At TEL 24 in September 2001 a matrix of the consolidated input received from both rounds was presented<sup>20</sup>.

---

<sup>20</sup> [http://www.apectelwg.org/apecdata/telwg/24tel/estg/ESTG\\_16.doc](http://www.apectelwg.org/apecdata/telwg/24tel/estg/ESTG_16.doc)

## General Comments

The initial round of the mapping exercise identified areas where there was a high degree of consistency and others where there were inconsistencies. The updated information obtained from the second round confirmed the preliminary findings. However, the expanded, refined data sample afforded by the second round provides a stronger basis for analysis and therefore a better indication of where future work should be focussed.

This mapping exercise made it possible to identify the commonalities and variances in approaches to authentication and certification services. These are identified in the following list.

## Legal and Legislative Framework

### Commonalities

All member economies that responded either already have, or are planning to have, legislation to establish a legal framework for electronic signatures. Virtually all these legislative frameworks establish that a signature may not be denied legal effect simply because it is electronic. For most, if not all economies, the legislation goes on to establish additional provisions relating to government transactions.

### Variances

The legislative framework varies considerably in the degree to which the legislation (or regulations) prescribe the technology and processes that establish the legal effect for the electronic signatures. While the spectrum appears to be narrow in the context of the public sector environment with governments, in most cases, establishing clear criteria that must be met for their operations, it is considerably broader in the context of the private sector. Specifically, the spectrum for the private sector ranges from granting legal effect only to signatures certified by licensed CAs on the one hand, to essentially leaving it up to the parties involved to determine what technology and process they will use to establish legal effect for the signatures associated with their particular transactions, on the other hand.

It follows, therefore, that the legislation also varies considerably in scope. Some set out an administrative framework for licensing CAs and establishing duties and responsibilities for the various players. Others take a very minimalist, technology neutral approach leaving the market to sort out issues such as allocation of duties and liabilities.

## E-Government Initiatives

### Commonalities

Virtually all member economies have identified e-government as a strategic priority. The solutions are predominantly PKI-based and are being deployed by government for government. A small number are partnering with the private sector and using their services for government requirements.

### Variances

Most government initiatives are being developed to eventually provide for linkages to the private sector. For some, the path for such linkages is straightforward (licensed CAs will be recognised), but the vast majority are relying on CAs meeting the requirements of their cross-certification or cross-recognition policies to be the test.

## **Current Private Sector Environment**

### **Commonalities**

The consistency in this area is that a wide range of e-commerce solutions is currently being deployed by the private sector in all member economies (such as SSL, PKI and Internet browsers). In all cases, the solution chosen depends on the security requirements of the environment and the particular transaction.

### **Variances**

The variances in this environment relate not so much to the technology being deployed, but rather to the legislative environment within which the private sector functions (that is whether licensing of CAs is required). As such, the variances will seemingly be discussed and further analysed in that context.

## **Roles and Responsibilities**

### **Commonalities**

The responses indicate that virtually all the functions and responsibilities delineated in the model are recognised and present in all approaches. There is therefore a common understanding of the necessary components of schemes. Areas of most consistency relate to competent authorities, with most indicating that it was a role performed by some form of governmental agency or representative. A second area of high consistency relates to the requirement that there be some form of independent evaluation of entities providing CA services.

### **Variances**

There is, however, a marked difference in how the functions and responsibilities are allocated across the players. In many cases, single entities are performing multiple roles depicted in the model. There are also obvious differences arising from the fact that the roles and duties are prescribed in legislation in some instances, and left to the market to determine in other cases.

## **Interoperability and International Dimensions**

### **Commonalities**

The responses confirm that member economies view interoperability and cross-certification as important to this environment. All recognise the need to work cooperatively in this area to minimise the potential for trade barriers. It is understood that the work needs to be at the policy level but that aspects related to 'bridging' legal frameworks and technical compatibility (such as compatibility of directories) may also need to be addressed.

### **Variances**

There appears to be little consistency in the approaches being pursued to achieve the desired interoperability. Some are pursuing cross-certification while others are providing for alternative solutions involving cross-recognition or mutual recognition arrangements. In the absence of further analysis, this variety of approaches has the potential to create impediments and potentially barriers to interoperability, as it is unclear to what degree they meet similar objectives.

## Conclusions and Areas for Future Work:

An analysis of the above variances is required to see how they can be adapted to meet the same objectives, so that organisations can interact and transact electronically across jurisdictional boundaries securely. The following paragraphs identify the areas where future work could be focussed.

**Legislative Frameworks.** There is a need to discuss the policy gaps that exist in the legislative frameworks. In particular, there is a need to understand the process by which the signatures certified by foreign CAs from jurisdictions without licensing regimes can be given legal effect by those jurisdictions with licensing regimes. A related question would be to understand the process by which a member economy with a licensing regime will provide for a CA from a non-licensed regime to operate in its jurisdiction (that is will member economies ‘license’ foreign CAs, and if so, how? Would this need to be accomplished via a government to government process? If so, there would be implications for those member economies pursuing a private-sector led approach to certification services.)

**Accreditation Schemes.** It would be useful to define basic common elements or parameters for accreditation schemes. A common approach to accreditation can form the basis for mutual recognition of CAs between different jurisdictions. Common accreditation standards and processes can be used to facilitate consistent legal and technical practices. It could also be a building block to establishing common criteria for CAs to be on trust lists. While the model of roles and responsibilities used in the mapping approach has been useful in terms of setting out the areas of responsibility in any scheme, it may not necessarily be as important to know who is performing the function as to know simply that it is being performed. As long as there is a requirement in schemes for independent evaluation that adhere to similar guidelines and criteria, a common level of trust or reliability should be there.

**Interoperability.** The mapping exercise has demonstrated the need to analyse more closely how interoperability across member economies can be achieved. A first step would be to develop a common understanding of the various means of achieving interoperability such as cross-certification, cross-recognition, or mutual recognition agreements. A common understanding and articulation of the general processes involved and component requirements of each approach would be helpful. Information from the various pilots and trials within and between economies would increase understanding of the issues involved.

## SECOND MAPPING OF CERTIFICATION AUTHORITIES ACCREDITATION SCHEMES

At TEL 25 in March 2002 it was agreed to undertake a further survey. The purpose of this survey was to compile updated information on the legislative and legal framework for electronic authentication and gather findings on the security guidelines and regulations required of certification authorities in the respective APEC member economies. The purpose of this exercise was to allow the PKI Interoperability Expert Group to assess cross-jurisdictional challenges and impediments and identify any gaps in the security standards, guidelines or practices between the APEC economies for certification authorities. The results obtained will help determine how varying legislative and legal frameworks can be ‘bridged’ to provide for cross-jurisdictional acceptance of authentication services and provide for legal effect of electronic signatures. They also highlight the need to devise international standards to address the gaps in technical and operational approaches.

## Process

A number of the questions used in this survey were based on key elements of IETF RFC 2527 which is the widely adopted framework for constructing CPs and CPSs. Many of the accreditation schemes use this framework for accrediting CAs within their schemes. The questions were as follows:

### **I. LEGISLATIVE AND LEGAL FRAMEWORK**

*For each of the following questions, please provide information in the following contexts:*

- *public sector only,*
  - *public and private sector,*
  - *separate public and private sector.*
1. *Please name and provide the URL for any legislation you have that sets parameters for the establishment and operation of authentication service providers. Is there a licensing requirement? If no legislation exists and there is no licensing requirement, please describe any framework that has been established for the operation of these services.*
  2. *If there is legislation, describe any aspects that limit or set parameters for the operation or use of foreign authentication services in your economy.*
  3. *What is the framework in which electronic signatures operate? Is their legal effect established in legislation and, if yes, how does it function?*
  4. *How do electronic signatures that have been created outside your economy have legal effect within your economy?*

### **II. REGULATION STANDARDS**

*Financial Responsibility for Recognized, Licensed or Accredited Certification Authorities*

1. *What are the financial requirements for licensed certification authorities?*

*Fees for Recognized, Licensed or Accredited Certification Authorities (for statistics purposes)*

2. *Is there an application fee for the license, recognition or accreditation and what is the renewal fee for it on a yearly basis?*

*Recognition of Foreign Certification Authorities*

3. *What are the requirements for recognition of foreign certification authorities and their certificates?*

### **III. CERTIFICATE POLICY STANDARDS**

1. *Are technical standards mandated through legislation or through any other formal arrangements?*
2. *Is the Certification Practice Statement and Certificate Policies of recognized, accredited or licensed certification authorities prescribed by legislation or regulations to be based on the Internet X.509 framework (RFC 2527) adopted by the Internet Engineering Task Force? If so, are there indispensable items in the CPS?*
3. *Are directory standards clearly prescribed towards the use of X.500 Directory Service produced by ITU and ISO?*

### **IV. TECHNICAL STANDARDS**

*Registration and Initial Identity Validation*

1. *What are the identification and authentication requirements for the CA or RA to validate the identity of a subscriber (organization or individual)? What are the types of documentation and/or identification credentials required?*



*Private Key Protection and Cryptographic Module Engineering Controls*

2. *What standards, if any, are required for the cryptographic module used to generate the keys for CA operations, RA operations, subscriber operations?*
3. *Is the private key under m out of n multi-person control?*
4. *Is the private key escrowed, backed up or archived? If so, who is the escrow, backup or archive agent? What form is the key escrowed, backed up or archived in (examples include plaintext, encrypted, split key), and what are the security controls on the escrow, backup or archive system?*

*Key Pair Generation, Installation and distribution*

5. *Are there security guidelines to determine if the key generation is performed in hardware or software and how are the keys handed over securely?*  
*In the case of CA key generation, how is the private key provided securely to the entity? How is the entity's public key provided securely to the certification authority? How is the CA's public key provided securely to potential relying parties?*  
*In the case where CAs provide a generation package for subscribers, what are the security safeguards for secure generation of keys?*
6. *Are there provisions for separate confidentiality and signature key pairs?*

*Choice of Algorithms*

7. *What cryptographic algorithms if any are prescribed for the electronic signature system? What are the key sizes?*

*Naming Conventions*

8. *Are there any guidelines to standardise the contents of Distinguished Names Components in the certificate fields? For example the use of non-standard or legacy values within distinguished names, assumptions made about the ordering of distinguished names attributes (such as assuming common name is always encoded last or that only one organisational unit attribute is allowed).*

*Personnel Security Control*

9. *What are the controls for trusted personnel and are there security screening procedures in place for them (for example police record screening and financial checks of key personnel)?*

*Physical Security Controls*

10. *Are there physical security requirements for the protection of the CA,RA or both, including the protection of the private key, protection of personal information in registration records?*

*Systems and Software Integrity and Control*

11. *What standards if any are required for systems and software integrity and control?*

*Term of validity of electronic certificates*

12. *What is the duration for the term of validity (or maximum certificate revocation period) of electronic certificates?*

*Archival of Certificates, Logs and Customer Records*

13. *What is the period of retention of archives?*



*Availability of General Purpose Repository and Certificate Revocation List (CRL)*

14. *What are the availability status of the general-purpose repository, certificate revocation list (CRL) issuance frequency, revocation request grace period and time limits for certificate suspension period?*

*Processing of certificate suspension or revocation*

15. *What is the availability of facilities for processing certificate suspension and revocation?*

*Business Continuity Planning*

16. *Are there provisions for business continuity planning and for disaster recovery planning in the guidelines?*
17. *In the event that a CA discontinues its operations, what are the relevant provisions and how can both past and present transactions be validated?*

*Compliance Audits*

18. *What is the frequency of compliance audits for licensed certification authorities, what are the requirements for audit and who are qualified to undertake such audits?*

Responses to the questions were received from six member economies: Canada; Hong Kong, China; Japan; Korea; Singapore; Chinese Taipei; Thailand and the United States. A table summarising the responses has been developed<sup>21</sup>.

## **General Comments**

A number of commonalities and variances were observed as discussed below.

### **Part I: Legislative and Legal Framework**

#### **Commonalities**

Legislation regarding the legal status and framework for electronic signatures exists in all six member economies that submitted responses to the questionnaire. Although the scope of the legislation in each economy differs, all establish the legal validity of electronic signatures.

Although in some cases the legislation is silent on the acceptability of foreign electronic signatures, the majority provides for them to be given legal effect so long as they are created under the same conditions as electronic signatures created domestically.

#### **Variances**

The legislative approach to CAs varies considerably across the responding member economies. Hong Kong, China; Korea; Japan; Chinese Taipei and Singapore have enacted legislation that specifically addresses the licensing or accreditation of CAs. Thailand covers the licensing indirectly through regulations in its Electronic Transactions Act. The United States and Canada have no licensing requirements or accreditation schemes for CAs but both are developing policies and guidelines for interactions among trust domains where at least one of the participants is a federal government entity.

With respect to foreign CAs, the parameters vary significantly again. Korea has no legislation limits for foreign CAs. In Hong Kong, China; Japan and Chinese Taipei, foreign CAs can receive

---

21 <http://www.nvk2000.ru/apec/documents/estg/estg13.doc> . Note that this document does not include responses from Hong Kong, China and Chinese Taipei which were received after TEL 26. Also the entry for Thailand was subsequently updated. An updated document will be presented to TEL 27.

accreditation from the relevant ministries. In Singapore, foreign CAs are recognised on a case-by-case basis by the minister. Thailand imposes some restrictions for alien businesses. In the United States and Canada there are no parameters for foreign authentication services although there are regulations or administrative arrangements governing federal organisation purchases of foreign CA authentication services and products.

## **Part II: Regulation Standards**

### Commonalities

No commonalities were readily evident from responses received.

### Variances

Fee structures differ between schemes in responding member economies. Hong Kong, China; Japan and Singapore charge a fee for licensing, recognition or accreditation of CAs but Canada; Korea; Chinese Taipei; Thailand; and the United States do not.

Approaches vary considerably on financial requirements for CAs with some member economies having specific capital requirements and insurance criteria and others having none.

Mechanisms for recognising foreign CAs are not very developed and member economies are adopting divergent approaches. For example Japan has formal guidelines and regulations for foreign CAs. Hong Kong, China; Korea and Chinese Taipei set requirements according to foreign scheme recognition. Singapore is developing regulations for foreign recognition. Canada and the United States currently act through their government schemes to assess foreign CAs, while Thailand does not have any law or established policy.

## **Part III: Certificate Policy Standards**

### Commonalities

The majority of respondents indicated that they applied IETF RFC 2527 in the development and assessment of Certificate Policies and Certification Practice Statements.

### Variances

Some variances were evident in respect of whether the standards are mandated or not. For example Hong Kong, China; Japan; Korea; Singapore; and Chinese Taipei mandate policy standards. Thailand will mandate policy standards but the details are still under consideration. The United States and Canada do not mandate policy standards by legislation but do utilise internationally accepted standards.

## **Part IV: Technical Standards**

### Commonalities

All economies have established detailed technical standards with the majority having them enshrined in law; Canada; Chinese Taipei and the US being the exceptions. Chinese Taipei does not establish any technical standards in its regulations while Thailand is still considering the details of its standards.

Member economies are deriving their technical standards from internationally recognised sources such as the IETF although individual implementations differ.

While the precise parameters differ, the identification and authentication requirements for the issuance of certificates are, in most cases, a function of the level of assurance involved. The requirements are set out either in regulations or policy.

Most member economies have sophisticated security guidelines governing key generation and management.

Most member economies have similar controls in place for trusted personnel and procedures for security screening.

Most member economies have similar comprehensive policies in place for the physical security requirements for the protection of the CA and RA.

Where specified, the period of retention of archives was fairly consistent across all responding member economies, about seven years, although the US had higher minimum retention periods in some instances based on the assurance level of the certificate supporting the electronic signature.

Generally responding member economies do not support escrow of the private signature key of subscribers.

All member economies have some form of auditing requirement although there are differences with respect to whether it is mandated in legislation and who is eligible to perform the audits. Hong Kong, China; Korea and Singapore require an audit for licensed CAs. Japan states that it is the responsibility of the investigating organisation to investigate whether a standard is satisfied. Chinese Taipei and Thailand are still considering the details for CA auditing. The United States and Canada do not require compliance audits since they do not regulate CAs. However, both require audits prior to cross-certification with the federal government entities and systems.

### Variations

Variations arise in respect of certificate revocation lists with some economies having formal procedures and availability requirements and others not.

Approaches to cryptographic algorithms differ with some economies offering general guidelines and others mandating the use of specific algorithms.

### Summary of Key Findings

Legislation regarding the legal status and framework for electronic signatures exists in all seven responding member economies with all acknowledging the validity of electronic signatures, both foreign and domestic.

All responding member economies have established detailed technical standards for authentication in either policy or regulations although the precise parameters and scope of applicability differ. For example in some economies standards are applicable only when a federal government entity is involved.

A consistent, formal recognition mechanism for foreign certificate authorities does not exist across member economies. Member economies are adopting different approaches with the criteria for foreign recognition either contained in regulations in some instances whereas in other instances there are no formal criteria.

## Forward Plan

At TEL 26 it was agreed to prepare high level principles derived from the results of the two mapping exercises. The purpose of the principles will be to:

- provide guidance to member economies in establishing comprehensive authentication policies;
- assist member economies in addressing any legislative, regulatory, or technical deficiencies with their existing approach to authentication; and
- facilitate the inter-jurisdictional acceptance of foreign certificate authorities by creating recognised and accepted guidelines that can be used as a basis for reciprocal agreements.

## DETAILED MAPPING OF PKI SCHEMES

A number of individual economies have been examining bilateral or multilateral approaches to cross-certification or cross-recognition. These activities have been regularly reported to the eSecurity Task Group meetings. Some of these are sector specific such as the Pan Asian e-Commerce Alliance<sup>22</sup>, while others are examining economy to economy interoperability such as a current pilot project between Japan; Korea and Singapore under the auspices of the Asia PKI Forum<sup>23</sup>.

Several other economies are undertaking a more detailed mapping of the accreditation or cross-certification criteria for their government or economy wide schemes. The methodology involves comparison of procedures or standards used for each element of RFC 2527. It is a more detailed mapping than the broader APEC study discussed above. At TEL 26 it was agreed to consolidate these detailed mappings and extend the mapping to other schemes both in APEC and in Europe through liaison links with the European Electronic Signatures Standardization Initiative. The resultant mappings will be used to develop best practice guidelines for the establishment of schemes that will be capable of being recognised within both communities. They could also provide the basis for cross-certification or cross-recognition agreements between the schemes rather than individual CAs under those schemes.

---

22 [http://www.apectelwg.org/apecdata/telwg/24tel/estg/ESTG\\_21.ppt](http://www.apectelwg.org/apecdata/telwg/24tel/estg/ESTG_21.ppt)

23 <http://www.apectelwg.org/apecdata/telwg/25tel/estg/estg05.ppt>

## Terminology mapping

Number	Technology-neutral term	Definition	PKI-centric term
1.	<b>Authenticator</b>	A parameter for the authentication of individual or organisational identity, roles or attributes.	<b>Public Key</b>
2.	<b>Authentication Technology</b>	The technology used to generate, issue or interpret an authenticator.	<b>Public-Key Cryptography</b>
3.	<b>Authentication Service Provider</b>	A body that generates, issues, receives or stores all or part of an authenticator and might add some further service.	<b>CA</b>
4.	<b>Authentication Scheme</b>	A scheme that involves authenticators and authentication service providers.	<b>PKI</b>
5.	<b>Certificate</b>	An electronic document generally issued by a third party that binds an authenticator to a specified user.	<b>Certificate</b>
6.	<b>Cross-Certification</b>	The practice of cross-recognition of another authentication service provider's authenticator to an agreed level of confidence and is normally evidenced in a contract or agreement. (An extension of the concept used in PKI)	<b>Cross-Certification</b>
7.	<b>High Level Authentication Authority</b>	A body with responsibility relating to the activities of a number of subordinate authentication service providers.	<b>Root CA, Controller of Certification Authorities</b>

Electronic Authentication—issues relating to its selection and use

### Selected definitions of cross-certification

#### Internet X.509 PKI — PKIX Roadmap<sup>24</sup>

*A CA certificate is a certificate in a hierarchy that is neither a self-signed certificate, nor an end-entity certificate. [2459bis] does not make a difference between a CA certificate and a cross certificate since it defines a cross-certificate as “a certificate issued by one CA to another CA”. Some people in the WG believe that a cross certificate is a special kind of CA certificate. A cross-certificate is issued by a CA under one Top CA for another CA under a different Top CA. CAs in the same hierarchy have part of their names imposed by the Top CA or by the CAs under that Top CAS. When a cross certificate is issued, there is no relationship between the names of the CAs.*

*Typically, a cross-certificate is used to allow client systems or end entities in one administrative domain to communicate securely with client systems or end users in another administrative domain. Use of a cross-certificate issued from CA\_1 to CA\_2 allows user Alice, who trusts CA\_1, to accept a PKC used by Bob, which was issued by CA\_2. Cross-certificates can also be issued from one CA to another CA in the same administrative domain, if required. Cross-certificates can be issued in only one direction, or in both directions, between two CA's. That is, just because CA\_1 issues a cross-certificate for CA\_2, CA\_2 does not have to issue a cross-certificate for CA\_1.*

#### Electronic Commerce Promotion Council of Japan (ECOM) Certification Authority Working Group, Cross-Certification Guidelines

*... the reciprocal certification process of two certification authorities. Cross certification enables the reciprocal use of the certificates issued by two certification authorities, increasing the usage range of users' certificates.*

#### VeriSign CPS (Version 1.2)

*A condition in which either or both a VeriSign PCA and a non-VeriSign certificate issuing entity (representing another certification domain) issues a certificate having the other as the subject of that certificate.*

#### A Matter Of Trust — Deploying A Public-Key Encryption System Extends Trust Across Boundaries<sup>25</sup>, by Amy K. Larsen

*... a process in which two certificate authorities in different domains securely pass key information between them. Those certificate authorities basically create cross-certificates that*

---

<sup>24</sup> <http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-08.txt>

<sup>25</sup> <http://www.techweb.com/se/directlink.cgi?IWK19990315S0040>



*guarantee to the user that one certificate authority trusts the other and that all the documents validated by it are unchanged.*

### **Issues Relating to the Use of Electronic Authentication, APEC Electronic Authentication Task Group**

*The practice of cross recognition of another authentication service provider's authenticator to an agreed level of confidence and is normally evidenced in a contract or agreement. (An extension of the concept used in public key infrastructures)... The process of cross-certification includes legal, technical and policy review of each other's authentication scheme policies and authentication scheme practice statements, their implementation and operational management...*

### **Entrust Technologies White Paper — The Concept of Trust in Network Security**

*Cross-certification is a process in which two CAs securely exchange keying information so that each can effectively certify the trustworthiness of the other's keys. Essentially, cross-certification is simply an extended form of third-party trust in which network users in one CA domain implicitly trust users in all other CA domains which are cross-certified with their own CA.*

### **The Burton Group Network Strategy Report — Public Key Infrastructure Architecture**

*In either a hierarchical or a peer relationship, two CAs can exchange the information necessary to establish cross-certificates between them, thus creating a trust relationship.*

## Chapter 4

# Shared secret technologies

The use of shared secrets as an authentication tool dates back as far as, if not further than, the use of signatures. Passwords were a common means of authentication of entitlements to pass or membership of a community to guard posts in historic times. Shared secrets have also been used for a number of years as electronic access control techniques. Most readers would still use a password, for example, when logging on to their systems. In addition, passwords or PINs have been used for a number of years, in conjunction with magnetic swipe cards, for access to automatic teller machines (ATMs) and electronic funds transfer- point of sale (EFTPOS). As a result, many businesses are familiar with the business risks associated with passwords and PINs.

The shared secret group covers implementations such as symmetric cryptography, passwords, PINs, and challenge-response. Technologies in this group generally only provide for authentication. However, symmetric cryptography can provide confidentiality and integrity capabilities in some implementations. Depending on whether the secret is unique to each pair of parties, non-repudiation is possible. This group mainly supports closed business models as the secret has to be shared between both parties and there is likely to be some form of prior arrangement. It can, however, support open-but-bounded models through a chaining arrangement where an authenticator in one closed system could generate authenticator for another closed system. For example Kerberos<sup>1</sup> could be used in this way.

### DEFINITIONS

The following definitions are taken from:

- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, *National Information Systems Security (INFOSEC) Glossary*<sup>2</sup> [NSTISSI],
- M. Abrams, S. Jajodia, and H. Podell, eds, *Information Security—An Integrated Collection of Essays*<sup>3</sup> [AJP].

---

<sup>1</sup> <http://web.mit.edu/kerberos/www/>

<sup>2</sup> National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, *National Information Systems Security (INFOSEC) Glossary*, <http://constitution.ncsc.mil/www/nstissc/assets/pdf/4009.pdf> January 1999

<sup>3</sup> M. Abrams, S. Jajodia, and H. Podell, eds, *Information Security - An Integrated Collection of Essays*, IEEE Computer Society Press, January 1995 referenced at [http://www.isse.gmu.edu:80/~csis/glossary/merged\\_glossary.html](http://www.isse.gmu.edu:80/~csis/glossary/merged_glossary.html).

## Electronic Authentication—issues relating to its selection and use

<i>Challenge and Reply</i>	<i>Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply. [NSTISSI]</i> Note: More commonly called challenge-response.
<i>Computer Cryptography</i>	<i>Use of a crypto-algorithm program by a computer to authenticate or encrypt-decrypt information. [NSTISSI]</i>
<i>Credentials</i>	<i>Information, passed from one entity to another, used to establish the sending entity's access rights. [NSTISSI]</i>
<i>Crypto-algorithm</i>	<i>Well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc. [NSTISSI]</i>
<i>Key</i>	<i>Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter-countermeasures patterns (e.g., frequency hopping or spread spectrum), or for producing other key. [NSTISSI]</i>
<i>List-oriented</i>	<i>Computer protection in which each protected object has a list of all subjects authorized to access it. See also ticket-oriented. [NSTISSI]</i>
<i>Passphrase</i>	<i>Sequence of characters, longer than the acceptable length (C.F.D.)* of a password, that is transformed by a password system into a virtual password of acceptable length. [NSTISSI]</i>
<i>Password</i>	<i>Protected or private alphanumeric string used to authenticate an identity or to authorize access to data. [NSTISSI]</i>
<i>PIN</i>	<i>Personal identification number. Similar to a password but using only numeric characters</i>
<i>Secret Key Cryptography</i>	<i>Cryptography based on a single key (or symmetric cryptography). It uses the same secret key for encryption and decryption. Messages are encrypted using a secret key and a secret key cryptographic algorithm, such as Skipjack, DES (Data Encryption Standard), RC2 (Rivest Cipher 2), or RC4 (Rivest Cipher 4). [AJP]</i>
<i>Secret Key</i>	<i>The key that two parties share and keep secret for secret key cryptography. Given secret key algorithms of equal strength, the approximate difficulty of decrypting encrypted messages by brute force search can be measured by the number of possible keys. For example, a key length of 56 bits is over 65,000 times stronger or more resistant to attack than a key length of 40 bits. [AJP]</i> Note: In some implementations the same secret key may be shared between all parties in a closed group.

---

\* CFD: common fill device

<i>Seed Key</i>	<i>Initial key used to start an updating or key generation process. [NSTISSI]</i>
Session Key	A secret key generated for a particular session between two parties and then discarded.
Symmetric Cryptography	See <i>secret key cryptography</i> above.
<i>Ticket-oriented</i>	<i>Computer protection system in which each subject maintains a list of unforgeable bit patterns called tickets, one for each object a subject is authorized to access. See list-oriented. [NSTISSI]</i>
<i>User</i>	<i>Person or process authorized to access an IS**.</i> [NSTISSI]
<i>User ID</i>	<i>Unique symbol or character string used by an IS** to identify a specific user.</i> [NSTISSI]
<i>Virtual Password</i>	<i>IS** password computed from a passphrase meeting the requirements of password storage (e.g., 64 bits).</i> [NSTISSI]

\* *CFD: common fill device*

\*\* *IS: information system*

## TECHNOLOGY

The principal forms of shared secrets are

- symmetric cryptography (secret key cryptography),
- passwords,
- passphrases,
- personal identification numbers (PINs), and
- challenge-response (challenge and reply).

## Symmetric Cryptography

Symmetric cryptography is generally considered an encryption tool. However, the possession of the secret, in this case a key, can also fulfil an authentication function. If only X and Y share a key and Y receives a message encrypted with that key then Y can assume that the message has come from X. Furthermore a secret key can also be used to encrypt a hash total providing message integrity. As the use of symmetric cryptography is quite mature, a number of IETF standards<sup>4</sup> exist. Special implementations such as Kerberos have achieved widespread use. In some implementations of symmetric cryptography the secret key is reused while in others it is used as a seed key to generate a session key. A further implementation involves the sharing of a session key produced by one user and transferred to another using asymmetric, or public key, cryptography to protect its confidentiality. This last case is technically not a hybrid approach as the asymmetric cryptography is a security device and is not directly involved in the authentication process. However the level of security can impact on the reliability of the authenticator. This issue is discussed in more detail in the hybrid technologies chapter (Chapter 7).

---

\*\* IS: information system

<sup>4</sup> See 'Security Area' at <http://www.ietf.org/html.charters/wg-dir.html>

## Password, Passphrases and PINs

These are also well established technologies for electronic authentication having been used as access control techniques for computers and ATMs for several decades. In some implementations encryption is used to protect the password and PIN during transmission. As with symmetric cryptography above, this issue is discussed in more detail in the hybrid technologies chapter (Chapter 7). A further implementation is the use of one-time passwords. As this approach is more closely related to challenge-response implementations, it has been included in that section. Authentication is achieved by verifying the credential supplied against the credential included in a list held by the recipient.

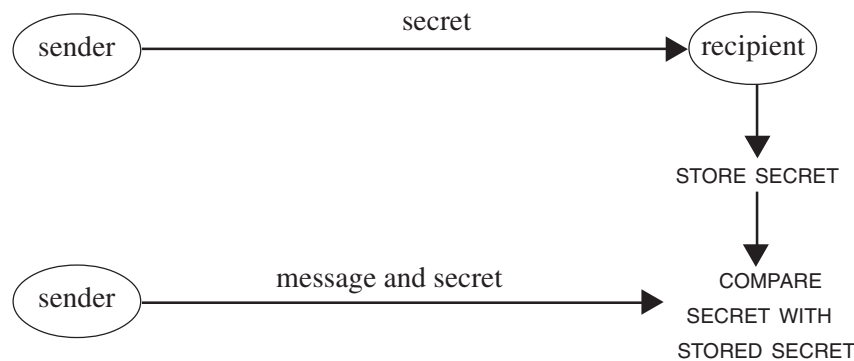
## Challenge-response

In these technologies the user requests access, for example, to a server; the server issues a challenge; the user provides a response based on a generation process; and finally the server verifies the response and grants access. The approach involves synchronisation of processes carried out by both the user and the server. These can depend on factors such as time where a one-time password is changing at regular intervals (for example every minute) for both the user and server. At the same point in time both should have the same password. Another approach is for both parties to use the same algorithm so that if the challenge is entered into the process it will provide a response to match that generated by the server. There are other challenge-response approaches under development.

While it is possible for the processing to occur on a user's computer, it is more common for the users to have a token under their control to undertake the appropriate process. In some cases the token itself may be protected by a PIN to control access. Challenge-response approaches are most commonly used for authentication in access control rather than individual transactions.

It is not intended that this chapter address technical aspects of particular shared secret techniques. Rather it will identify the aspects that are common to all techniques and relevant to the general discussion of electronic authentication.

Shared secrets involve the generation and distribution of the secret so that all parties to the scheme have a copy of the secret. For subsequent authentication the user sends the secret and this is compared with the recipient's stored copy of the secret.



**Figure 23: Shared Secret**

As mentioned in the general issues chapter (Chapter 1), many implementations of shared secrets use cryptographic techniques to prevent capture of the secret for subsequent replaying or generate a new secret for each transaction, again to prevent capture and replay. Other implementations store the

secret on tokens under the control of the individual and the token confirms the secret and then generates an authentication message using another technology such as asymmetric cryptography. The issues associated with these approaches are discussed further in the hybrid technologies chapter (Chapter 7).

### USE IN ELECTRONIC BUSINESS MODELS

Shared secret approaches rely heavily on the secret being restricted to authorised parties. The binding between an individual and the authenticator (secret) is achieved through this limit on sharing of the secret although in some instances a secret may be shared among a group rather than between two parties. It is possible to input a secret into a machine to allow machine to machine authentication. The main factor in determining the degree of trust that can be placed on the authenticator is the security of the secret itself. This is discussed further under the Trust Section of this chapter.

While shared secret authenticators can provide a strong binding with an individual or machine, they do not provide the same facility for corporate, role or attribute authentication. However this has also been the case in the paper world where, for example, written delegations have been used to link an identity to a particular role, attribute or corporate identity. More commonly individuals would have different passwords or PINs in respect of different attributes or roles.

#### Open Model

Shared secrets are not generally useful in this model as there needs to be a prior arrangement to distribute the secret or secret generation process. While asymmetric cryptography could be used to distribute the secret, even this approach generally relies on some form of authentication occurring before the secret is shared. You need to know you are sharing the secret with the right person.

The type of open network systems for which Kerberos was designed do not equate to the open business model described in the general issues chapter (Chapter 1). While Kerberos can carry out cross realm certification<sup>5</sup> the requirement to be a member of a Kerberos realm places a boundary around the model.

Shared secret technologies do not lend themselves to open business models.

#### Closed Model

This model requires some form of prior relationship between the parties and this relationship could involve the distribution of the shared secret or secret generation process. It could also involve establishment of schemes to protect the exchange of the secret. Within an organisation this could be simply reliance on security of the internal network. In external networks it could involve the use of encryption to protect the secret. The use of PINs and passwords for ATMs, EFTPOS and online banking and the use of passwords as access controls for computer systems are classic examples of a closed models.

Shared secret technologies lend themselves to closed business models.

#### Open-But-Bounded Model

It is possible for a chain of trust to be established using a series of shared secrets. This would allow authentication to move outside of a purely closed group and allow parties with no direct relationship

---

<sup>5</sup> Descriptions of Kerberos realms and cross realm authentication can be found in J.G. Steiner, C. Neuman, J.I. Schiller; *Kerberos: An Authentication Sever for Open Network Systems*; <ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS>

to authenticate themselves either unidirectionally or bidirectionally. This is the principle employed by some implementations of Kerberos. This process involves a chain of secrets, implemented through tickets, rather than extended sharing of the original secret. Other implementations involving chains of secrets are possible. However, such chains involve a series of agreements between each link in the chain which place a boundary on the process.

Shared secret technologies can lend themselves to open-but-bounded business models.

## **USER REQUIREMENTS**

Shared secret approaches are widely accepted among both the business and user communities largely as a result of the use of PINs with ATMs, EFTPOS terminals and the use of passwords in the computer environment. The main disadvantage has been the cost and security requirements of the infrastructure required to distribute the secrets. However, in many cases cost effective solutions have been developed, have wide user acceptance and have been integrated into business models. The same can be said for symmetric cryptography where key distribution is a long established technique.

A further disadvantage is that, typically, secrets are shared between discrete parties. Therefore to transact with a number of parties will require the use of the same number of secrets. This will require users to be able to store that number of secrets.

Cost associated with this approach will vary according to the type of secret, the implementation and the parties. For an individual user, the cost can be nil if the person chooses to remember the secret. This is commonly the case with PINs and passwords at present. Alternatively applications are now available at relatively low cost that allow users to store a number of PINs and passwords on their systems protected by a single access control. The security of such applications would need to be considered in the light of the aggregate exposure in the case of compromise of the single access control. In other implementations users may use a token such as a smart card to store one or more secrets. This is a slightly higher cost option.

The cost to business will vary depending on its role and client base. A business with a small client base will probably be able to adopt similar implementations to those of individual users. However businesses with large client bases will need to implement secure facilities to store, distribute and process shared secret authenticators. As mentioned earlier a number of businesses have been using this approach for ATM and EFTPOS networks and the business models are well established. The impact is more likely to be on new Internet businesses who will need to implement new systems. However, it should be noted that this technology does not require the type of infrastructure required for asymmetric cryptography nor the readers associated with biometrics, and may therefore incur a lower implementation and support cost.

The use of shared secret technologies is more familiar to most users than other technologies. However there can be some inconvenience arising from the number of secrets that may be required to be stored, particularly for newly establishing businesses with potentially large client bases.

## **CERTIFICATION MODELS**

As the process of sharing a secret requires some form of prior contact between the parties shared secrets are generally used in a no-certification model. While some might argue that the chaining process previously outlined could be considered an informal certification model, the fact is that a different authenticator is used in each link of the chain. The ultimate recipient does not receive the user's secret, only that of the previous link in the chain. This approach is therefore a chain of non-certification models.



## TRUST

The level of trust in a shared secret depends on a number of factors including the strength of the secret, the security of the secret and the implementation of technology for the distribution and use of the secret.

### Strength of the Secret

In purely mathematical terms the strength of a secret can be calculated as follows.

- Password and passphrase:  $26^n$  where  $n$  is the number of letters in the word or phrase. This can be increased to  $52^n$  if upper and lower case are used and  $72^n$  if numbers and characters are included.
- PINs:  $10^n$  where  $n$  is the number of digits in the PIN.
- Symmetric cryptography:  $2^n$  where  $n$  is the number of bits in the key.

Determination of the strength of symmetric cryptography will also depend on the strength of the algorithm to which the key is applied. Standards have been developed for both symmetric algorithms and their implementation. In a number of cases algorithms are placed in the public arena to allow experts to test their strength. Certain algorithms are known to have weak keys which should be avoided.

In addition the strength of passwords, passphrases and PINs can be reduced by use of words, phrases and numbers that can be readily associated with the user such as family names, favourite car or sporting team. Passwords are further susceptible to ‘dictionary attacks’ where an attacker uses a dictionary to determine a password. These weaknesses can be overcome through good selection techniques and controls on the number of attempts to submit a password.

### Secret Security

The security of a secret can be impacted by secret generation, secret distribution, secret storage and management, and secret transmission processes.

#### Secret Generation and Selection

Secrets can either be generated, or selected, by an individual user and then shared with the other party, or a central authority may generate secrets for use by its clients and distribute the secret to them. There are advantages and disadvantages of both approaches. The centralised approach can be used to ensure the generation of a truly random secret. This can avoid the tendency for an individual to generate a secret, specifically a password, passphrase or PIN, which can be easily remembered but can also be easily guessed or is vulnerable to a dictionary attack. However, if a secret is not easily remembered there may be a tendency for individuals to record it to ensure it is not forgotten. The situation for the generation of a symmetric key is more complex. The topic of key generation is discussed in detail in Chapter 2 and applies equally for generation of symmetric keys. There are a number of guides to assist users select good passwords issued by bodies such as the US National Security Institute<sup>6</sup>.

#### Secret Distribution

Where secrets are generated centrally they need to be distributed to the users by secure means. The level of security for the distribution of the secret needs to be commensurate with the loss that could

---

<sup>6</sup> National Security Institute, *Selecting Good Passwords*, <http://nsi.org/Library/Compsec/goodpass.html>

occur if the secret were compromised. There are well established processes for the distribution of PINs and passwords particularly in respect of credit and debit cards. In some cases symmetric keys are distributed using asymmetric cryptography although this is more commonly used in the encryption context. There are also examples of asymmetric cryptography being used to protect distribution of PINs and passwords, particularly in terms of online registration processes using browsers.

### Secret Storage and Management

As with distribution, secret storage must be secured to a level commensurate with the loss that could occur to either the user or a person transacting with the user if the secret were compromised. As mentioned above, there are a number of measures for protecting a secret ranging from committing to memory, to storage on computers, to use of tokens. One-way encryption can also be used to prevent retrieval of a clear text version of a secret. Another important measure is to regularly change the secret to reduce the risk and consequences of an undetected compromise. There are a number of standards and similar documentation<sup>7</sup> which outline good practice in storing and managing secrets.

### Secret Transmission

Secrets are vulnerable to eavesdropping when they are transmitted between the user and recipient. Techniques such as encryption can be used to protect a secret while it is in transit. The use of encryption in these circumstances is to protect the secret and as such is not performing an authentication function. Similarly one way encryption can be used to prevent a secret being retrieved. Again the level of security for the transmission of the secret needs to be commensurate with the loss that could occur if the secret were compromised.

### Secret Sharing

Some computer systems and transactions require sophisticated security, best attained when a key or password is shared between several people in such a way that it can only be reconstructed by a sufficiently large and responsible group acting in agreement. Secret sharing security systems are used in banks, in other financial institutions, in communications networks and computing systems serving educational or commercial institutions, though the best known examples are military: for instance, in the activation of nuclear weapons or missiles, several officers must concur before the necessary password can be reconstructed. Conversely, if the weapon becomes activated, each of the shareholders knows the other officers who entered their passwords were authorised. They have been mutually authenticated.

Schemes for determining the distribution of the partial information to the people involved are known as secret sharing schemes or access schemes and lead to shared control. These pieces of partial information are known as shares and may be of equal value (as in the military examples mentioned above) or more often of unequal value, probably arranged according to a hierarchy of some kind. For example in a university computing system, shares which lead to the reconstruction of the system manager's or super-user's key are far more valuable than those that lead only to a student's key.

---

<sup>7</sup> National Institute of Standards and Technology, *FIPS 112, Password Usage*, <http://csrc.nist.gov/fips/>  
National Institute of Standards and Technology, *Internet Security Policy: A Technical Guide [Draft]*, <http://csrc.nist.gov/isptg/html/ISPTG-5.html#Heading40>  
Defence Signals Directorate, *Password Management*, Australian Communications-Electronic Security Instructions (ACSI) 33, Section 15, Annex B, <http://www.dsd.gov.au/infosec/acsi33/15annexa.html>  
Siemens Communications Limited, *Fraud Management Guide*, [http://www.siemenscomms.co.uk/useful\\_information/telecom\\_guides/fraud/part22.htm](http://www.siemenscomms.co.uk/useful_information/telecom_guides/fraud/part22.htm)

## Chapter 4. Shared secret technologies

In its simplest form, taking a three digit secret and sharing it between three people in such a way that any two can recreate it can be achieved as follows:

Secret	1 2 3
A's share	1 _ 3
B's share	1 2 _
C's share	_ 2 3

While no one party knows the whole secret any two can recreate it knowing their share and the positions of that share.

Secret sharing is discussed in more detail in Appendix 1 to this chapter.

### **LIABILITY**

As shared secrets involve only the parties between whom the secret is shared, issues of liability only arise between those parties. There is generally no authentication service provider involved with this technology. In some cases there may be liability issues involving the suppliers of the technology used to generate, store or share the secret but these are normal commercial matters and will not be covered here.

It is possible for liability issues to be addressed by contract at the time the secret is shared. This is already the case in respect of debit and credit cards where liability is addressed in the terms and conditions of use. While the potential for loss, theft and misuse is higher than with for example, biometrics, many users are more aware of their responsibilities and exposures in this area due to the established use of this approach both in banking and finance and in computer access control.

Issues of liability are discussed in more detail in the legal issues chapter (Chapter 9)

### **ROLES OF PARTICIPANTS**

The main participants in shared secret schemes are the parties between whom the secrets are shared. Generally one party generates the secret and shares it with the other or others depending on the scope of the scheme. It is the role of all parties to ensure that an appropriate technology is selected and implemented, that the secret selected or generated is appropriate for the types of transactions and that the secret is appropriately secured. There may be a role for governments, standards organisations and industry bodies for advising on appropriate types of secret technologies. There is also a role in developing user confidence particularly with this technology where stories of captured passwords and PINs are quite common. This is discussed further in the Awareness Section.

### **INTEROPERABILITY**

Shared secrets depend on the parties not only sharing the secret but also the technologies to utilise that secret. Those technologies can range from a simple browser used by an individual user to transmit a secret to sophisticated applications used by business to receive and process large numbers of secrets. If the business's application meets all its authentication requirements then interoperability is not an issue for that business. Similarly if the browser meets all the individual user's requirements interoperability is again not an issue. Interoperability does become a problem where a user, either business or individual, is required to maintain a number of authentication technologies.

However, if a number of authentication technologies can be stored on a user's IT system and are readily available, interoperability may not be an issue. This is particularly the case with shared secrets, where a user may be able to store a number of secrets and the technology to use them on a system, and call them up at will.

In general, as shared secrets are generally used in closed systems, interoperability is not an issue for each system. The issue is the number of systems the user needs to communicate with, and the degree of inconvenience this might cause. However as the technologies themselves can use quite different approaches, they do not lend themselves to interoperability in the broader sense.

## **ACCREDITATION**

Secrets themselves cannot be accredited, as providing the secret for examination immediately compromises it. However the secret generation process, and the secret sharing technology and its implementation, can be accredited where standards or other normative documents exist. There are a number of standards in existence relating to symmetric cryptography algorithms and their implementation. Similarly there are a number of reputable guidelines for passwords, passphrases and PINs as mentioned earlier that could also be used as a basis for accreditation.

While the secrets themselves cannot be accredited, there are a number of implementations that prevent the use of less secure passwords, PINs and keys. Consideration of this aspect in the broader accreditation of implementations can provide a greater level of assurance as to the quality of the particular secret being used.

## **CULTURAL DIFFERENCES**

In a number of cultures the concept of an individual is subsumed by that of the tribe, clan or extended family. Property is owned by, and transactions are undertaken on behalf of, the community not the individual. PINs and passwords for credit and debit cards are commonly shared in such communities. Shared secret technologies lend themselves to these cultures. Similarly in cultures where the power to sign is transferred by passing on the signing instrument such as a chop or seal, the same result can be achieved by passing on the secret.

Shared secrets are less likely to be impacted by cultural differences than other more technological approaches to authentication.

## **AWARENESS**

As mentioned earlier, shared secrets is the most commonly used authentication technology today due to its widespread use for ATMs, EFTPOS and computer access. People are generally familiar with the use of secrets such as PINs and passwords, and the need to protect them. A smaller, but still significant, number are aware of their obligations to protect the secret. Even the use of the term secret generally produces an image of something that is not to be shared with others. Experience has shown that users are generally comfortable with a secret as an authenticator in the electronic environment. Their concerns are more about the security of the secret in the online environment. It is in the area of secret security that awareness and confidence has to be raised both for users and system implementors.

### **Government Awareness**

Governments have been using shared secrets as an electronic access control technique for many years. Passwords have been used in computer security since it first became an issue forty years ago. To some extent shared secret use has been overtaken by biometrics and asymmetric cryptography which are seen as being more secure. However, shared secrets continue to enjoy widespread use. The main concern with governments is their potential vulnerability to the exposure of information. This is the reason for high security authentication techniques, particularly in the area of national security and

the protection of personal data. However, there is other information that does not require this level of security. It is in this area that shared secrets continue to be used. As risk management techniques are commonly used in government security circles, governments are aware of the benefits of using authentication techniques that match the risk to the data. In this context they are generally aware of the strengths and weaknesses of shared secret technologies.

### **Business Awareness**

Awareness of shared secrets in the business sector is patchy. While most have some awareness of the role of shared secrets in their personal business dealings, only larger organisations that have operated computing facilities are familiar with the strengths and weaknesses in the business environment. It is important that business be aware of the security requirements when implementing this technology. Poorly implemented systems will be exposed, with consequent loss of confidence both in the technology and in the business. For many, concerns about the security of shared secrets in the electronic environment have led to a reluctance to use this approach. A major part of business awareness will be to raise the confidence of business in the use of this technology. This will include provision of accurate information of the various techniques and their strengths and weaknesses to allow business to adopt a risk management approach in deciding whether the technology is suitable for their business model. This is particularly the case for small and medium enterprises which would not normally be aware of this information.

### **Individual User Awareness**

While individuals are generally familiar with the use of shared secrets, confidence in their use in the electronic environment has been undermined by stories about capture of credit card numbers. While the capture of the number has no direct relationship with authentication, the link between a credit card number and its PIN or password has resulted in a perception that shared secrets themselves are not secure. As discussed earlier, shared secrets can be protected in storage and transit. Users need to be made aware of this and be provided with information that will allow them to judge whether a particular implementation provides adequate security for both their authenticator and their transaction.

Awareness of this technology and its associated security can be raised through industry providing information on their use of the technology and how it is implemented. For example, browsers already incorporate the ability to secure secrets transmitted to websites through the incorporation of SSL in the browsers. This can only be activated with websites that provide the capability. Both business and individual users need to be aware of this capability and how it can be implemented. Many users are not aware of the significance of the closed padlock icon on their browsers. There is a role for browser manufacturers in raising this awareness.

## **LEADERSHIP**

Unlike some of the other technologies mentioned in the general issues chapter (Chapter 1), governments, businesses and individuals have been using this technology for several decades. In the case of this technology, leadership is not so much about leading in use of the technology, but rather about making people aware that the technology is being used.

### **Governments**

The prime leadership role for governments is in establishing the necessary legal and policy frameworks to support electronic authentication including shared secrets. As the technology has been

used for years in EFTPOS and ATM transactions, much of the framework will already be in place. In most cases the use of the technology is in closed systems that are governed by terms and conditions of use agreed by the parties. These are supported under existing contract law. However problems may occur where technology specific approaches do not address, or preclude the use of, shared secret technology. More recently the trend has been towards the establishment of technology neutral frameworks that will support a range of electronic authentication technologies. This form of leadership is required if shared secret technologies are to continue to play a significant role in electronic authentication and electronic commerce.

The other leadership role for governments is through generating confidence in the use of the shared secrets by highlighting their own use of the technology. As governments adopt risk management approaches, they are in a position to provide advice or guidance on circumstances where the use of the technology is appropriate and how it might be implemented.

### **International Organisations**

Much of the discussions on electronic authentication in international organisation to date has focused on the use of asymmetric cryptography in public key infrastructures. The exceptions have been APEC and the OECD which have specifically addressed the wider range of technologies available. Discussions in other organisations will need to be extended if the full range of electronic authentication technologies are to be allowed to develop. Already other international organisations are adopting technology neutral approaches in their considerations. This will provide the necessary leadership for shared secrets to be recognised as a viable electronic authentication technology.

### **Business Corporations**

Many users including businesses use shared secrets in their day to day activities without focussing on the fact that they are using them as an authentication technique. The main leadership role for business is to provide information on how they are using the technology. This can be achieved through providing information on the way in which they are authenticating transactions both in the business-to-business and business-to-consumer context. The provision of business-to-consumer information would be consistent with the OECD consumer protection guidelines mentioned in Chapter 1.

### **Users and User Groups**

Users are already using this technology. However there is still a great deal of concern regarding the security surrounding the transmission and storage of shared secrets. User groups have a leadership role in informing themselves about the security of this group of technologies and their implementation, and passing this information on to their membership. Users and user groups also have a role in informing manufacturers and suppliers of their concerns to ensure that implementations are developed that meet those concerns.

### **IT Industry**

The IT industry is already providing leadership through the incorporation of services in their products such as browsers and email packages to protect secrets during transmission. Applications have or are being developed to protect secrets when stored on systems. Specialist applications are also being developed that incorporate shared secret technologies. The industry can continue to provide leadership through the development of products that meet user requirements and the development of innovative implementations of shared secret technologies.

## **COMBINATION WITH OTHER TECHNOLOGIES (HYBRIDS)**

A number of references have been made in this chapter to the use of shared secrets in combination with other technologies as part of a hybrid approach or to shared secrets being protected by other technologies. Similarly, other chapters have referred to symmetric cryptography, a shared secret technology, being used to protect other authentication approaches such as biometrics. The distinction between the use of several technologies as part of the authentication process and the use of one technology as a security measure for another technology is rather fine. In the chained approach several technologies form part of an authentication chain such as a password triggering a private key and therefore a digital signature. In this case the authentication, or signing process, begins at the point at which the password is entered.

In the secured approach one technology is used to protect an authenticator that uses a different technology such as a password being used to protect a private key. Entering the password releases the private key which is then used to apply a digital signature. In this case the authentication, or signing process, begins at the point at which the private key is applied. These distinctions and their implications will be discussed in more detail in the hybrid technologies chapter (Chapter 7).



Electronic Authentication—issues relating to its selection and use

### Secret sharing<sup>1</sup>

Public key technology is mature and widespread in commercial Internet applications. Currently it is suggested that keys of length 2048 bits length are safe. However, suppose an electronic signature, for example on an electronic will or electronic trade agreement, must remain secure for fifty years. Will its signature still be authentic then, given future changes in technology?

Longer and longer keys have two main disadvantages:

- it is difficult for a legitimate user to store them safely and reproduce them exactly when required; and
- often material that has been authenticated using encryption techniques needs to be accessed after all the legitimate owners or users of the key have left the organisation.

The only method known to protect against these drawbacks is to use secret sharing. Secret sharing also allows mutual authentication of shareholders.

This appendix aims to allow the reader to make an informed decision regarding the kind of shared secret to use and its security while safeguarding against human frailties and the passage of time.

Computer systems require sophisticated security, best attained when a key or password is shared between several people in such a way that it can only be reconstructed by a sufficiently large and responsible group acting in agreement. Shared security systems are used in banks, in other financial institutions, in communications networks and computing systems serving educational or commercial institutions, though the best known examples are military: for instance, in the activation of nuclear weapons or missiles, several officers must concur before the necessary password can be reconstructed. Conversely, if the weapon becomes activated, each of the shareholders knows the other officers who entered their passwords were authorised. They have been mutually authenticated.

Schemes for determining the distribution of the partial information to the people involved are known as secret sharing schemes or access schemes and lead to shared control. These pieces of partial information are known as shares and may be of equal value (as in the military examples mentioned above) or more often of unequal value, probably arranged according to a hierarchy of some kind. For example in a university computing system, shares which lead to the reconstruction of the system manager's or superuser's key are far more valuable than those that lead only to a student's key.

---

<sup>1</sup> The Task Group would like to express its appreciation to Jennifer Seberry, Centre for Computer Security Research, University of Wollongong; Chris Charnes, Department of Computer Science, University of Melbourne and Josef Pieprzyk, Centre for Computer Security Research, University of Wollongong for their work in drafting this appendix.

The best known secret sharing schemes presently available are not hierarchical and may be very unwieldy to implement. Other secret sharing questions may need more complicated combining rules: for example, in Australia, for a referendum to pass, it must be approved both by a majority of the electors nationally, and by a majority of electors in a majority of the states. This can lead to compartmentalised and more specialised schemes. None of those known at present are really adequate and limit flexibility

Secret sharing is concerned with the problems of distributing a secret among a group of individuals or entities, so that only pre-designated collections of individuals are able to recreate the secret collectively by combining their shares of the secret.

The earliest and most widely studied type of secret sharing schemes are called  $(t,n)$ -threshold schemes. In these schemes the access structure—a specification of which of the participants are authorised to recreate the secret—comprises all the possible  $t$ -element subsets selected from an  $n$ -element set.

The problem of realising or implementing secret sharing schemes for threshold schemes was solved independently by Blakley and Shamir in 1979. Shamir's solution is based on the property of polynomial interpolation in finite fields. Blakley's solution is formulated and solved using finite geometries. For practical key management, the scheme based on polynomials is simpler.

In a  $(t,n)$ -threshold scheme, each of the  $n$  participants holds some shares (also called shadows) of the secret. The parameter ' $t$  less than or equal to  $n$ ' is called the threshold value. A fundamental property of the  $(t,n)$ -threshold scheme is that the secret can only be recreated if at least  $t$  shareholders combine their shares, but fewer than  $t$  shareholders cannot recreate the secret. The fact that the key can be recovered from the combined shares of any  $t$ -sized subset is a property which makes threshold schemes very useful in key management. Threshold schemes tolerate the invalidation of up to  $n-t$  shares—the secret can still be recreated from the remaining intact shares.

Secret sharing schemes are also used to control the authority to perform critical actions. For example, a bank vault can be opened only if say, any two out of three trusted employees agree to do so by combining their partial knowledge of the vault combination. In this case, even if one of the three employees is not present at any given time the vault can still be opened, and no single employee has sufficient information about the combination to open the vault.

Secret sharing schemes which do not reveal any information about the shared secret to unauthorised individuals are called perfect. This notion will be formally defined later. We discuss both perfect and non-perfect schemes as the latter are proving useful in various secret sharing applications.

Besides the  $(t,n)$ -threshold structures, more general access structures are encountered in the theory of secret sharing. General access structures apply to situations where the trust-status of the participants is not uniform. For example, in the bank scenario described earlier, it might be considered more secure to authorise either the bank manager, or any two out of three senior employees to open the vault.

Since 1979 the study of secret sharing has developed into an active area of research in cryptography. The fundamental problem of the theory and practice of secret sharing deals with the issue of how to implement secret sharing for arbitrary access structures. We shall later describe some solutions to this problem.

We assume there exists a key distribution centre (KDC) which is trusted unconditionally.

**TERMINOLOGY**

Access Structure	A formal specification of the participants in a secret sharing scheme which are able to recreate a shared key from their portions of the key.
Authentication	One of the two main goals of cryptography (the other is secrecy). An authentication system ensures that messages which are transmitted over a communication channel are authentic.
Cheaters	The participants in a secret sharing scheme which tender corrupt or modified shares to the combiner with the aim of deceiving the other participants as to the nature of the reconstructed secret.
Combiner	The combination phase in a secret sharing system. The participants tender their shares of a secret to the combiner (usually considered to be an algorithm within a computing machine) whose task is to faithfully reconstruct the secret if sufficient shares of the required type have been received.
Computationally difficult problems	The security of many cryptosystems depends on the unproven assertion that certain computational problems are inherently difficult. The accepted instances of such problems are: the discrete logarithm problem in various groups, factorisation of RSA moduli, the RSA inversion problem, finding the square roots modulo $n$ .
Conditionally secure	The security of this type of cryptosystem depends on the unproven assumption that instances computational problems, such as the discrete logarithm problem, are difficult to solve.
Dealer	The initial phase in secret sharing. The secret is selected by the dealer (also usually considered to be an algorithm within a computing machine). Shares of the secret are distributed by the dealer to each participant in the secret sharing scheme.
Discrete logarithm problems	The problem of finding the index, such that raising a fixed generator of cyclic group to this index yields a given element in the group.
Geometric secret sharing	A realisation of a secret sharing scheme using finite geometry. Usually either affine or projective geometries are used.
Key	An input provided by the user of a cryptographic system. This piece of information is kept secret and is the source of security in a cryptographic system. Although some times a part of the key information is made public, in which case the secret part is the source of security.
Key authentication	Identification of a party which possibly shares a key.
Key confirmation	Evidence that a key is held by some party.

Perfect secret sharing	In such a scheme it is impossible to deduce any partial information about a shared key from less than the critical number of shares of the key.
Secret sharing	Protecting a secret key by distributing it in such a way that only the authorised individuals can recreate the key.
Threshold scheme	A secret sharing scheme with a uniform access structure in which any collection of shareholders greater than a given threshold can recreate the secret.

## MODELS FOR SECRET SHARING

A common model of secret sharing has two phases. In the initialisation phase, a trusted entity—the dealer—distributes shares of a secret to the participants via secure means. In the reconstruction phase the authorised participants submit their shares to a combiner, who reconstructs the secret on their behalf. It is assumed that the combiner is an algorithm which only performs the task of reconstructing the secret. We denote the sets of all possible secrets and shares by  $K$  and  $S$  respectively; the set of participants in a scheme is denoted by  $P$ . Secret sharing schemes can be modelled using the information theory concept of entropy. This captures the idea of how much information is in each of the shares and the secret. A perfect secret sharing scheme ensures that no information is leaked about the secret until a required set of authorized shareholders combine their shares in the combiner algorithm. A necessary condition for a perfect threshold scheme is that the entropy of each share is greater than or equal to the entropy of the secret. Most of the secret sharing schemes which we discuss satisfy this condition, but we will also consider briefly schemes, which do not satisfy it; they are called non perfect schemes.

The information rate of secret sharing scheme is a measure of the amount of information that the participants need to keep secret in a secret sharing scheme.

It is desirable to have secret sharing schemes in which the size of the secret information and the size of the information in each share is roughly the same.

This minimises the amount of information that needs to be kept secret by the participants, which means that there is a greater chance of the scheme remaining secure. For example, a  $(t,n)$ -threshold scheme implemented by polynomials is ideal, but when the scheme is modified to prevent cheating it is no longer ideal.

## SOME KNOWN SCHEMES

We now describe several well-known threshold secret sharing schemes.

### A Simplified Version of Blakley's Scheme

A geometric solution is easy to visualise. Suppose that the secret is the combination of a safe, and that it consists of three digits,  $xyz$ . We could share the secret between a group of people by giving each of them the equation of a plane through the point  $(x,y,z)$ .

If we choose the planes so their pairwise intersections give distinct lines through  $(x,y,z)$ , then any two people can together determine a line through the point and any three can determine the point itself, and hence the combination of the lock. This is an example of a threshold scheme with threshold three, meaning that any three shares determine the secret, but no two shares determine it.

Suppose on the other hand, we choose the planes so that all but one of them have a line,  $l$ , say, in common, and the remaining plane,  $P$ , intersects  $l$  in the point  $(x,y,z)$ . Then finding the point requires knowledge of the plane  $P$  and any two other planes. This means that the agreement of the person who knows  $P$  is essential for the determination of the secret, and it is not just a threshold scheme.

Situations where shares of unequal value are used arise often in practice. For example, consider the authorisation of electronic transfer of large amounts of money between financial institutions. One might expect, say, that two vice-presidents could jointly authorise the transfer of amounts over \$10 000 000, two junior vice-presidents amounts between \$1 000 000 and \$10 000 000, two senior tellers amounts between \$100 000 and \$1 000 000 and two tellers lesser amounts. This is in a situation where the appropriate password is never revealed outside the electronic facility (in the bank's head office) which reconstructs the password from the information shares fed into it. What if a vice-president and a junior vice-president are delayed in another city by airport fog?

An obvious solution is to share the authorisation code for transfer of larger amounts of money between larger numbers of more junior staff, but doing this efficiently presents a problem. At present, many access schemes are known and some of them, based on combinatorial designs and finite geometries, have been proved to be the best possible (in a theoretical sense).

### Shamir's Scheme

Shamir's scheme realises  $(t,n)$ -access structures based on polynomial interpolation over finite fields. In his scheme the secrets  $S$  belong to a prime power finite field  $GF(q)$ , in which  $q$  is greater than or equal to  $n+1$ . In the initialisation phase, the dealer  $D$  chooses  $n$  distinct nonzero elements from  $GF(q)$  and allocates these to the participants. This correspondence is publicly known, and creates undesirable side effects if any of the participants are dishonest. However for now, we will assume that all the participants obey faithfully the protocol for reconstructing the secret. Fix a random element of  $GF(q)$  as the secret  $K$ . The shares of  $K$  are created using the following protocol.

The dealer chooses the coefficients of the polynomial, randomly, uniformly and independently and uses them to form a polynomial of degree at most  $t-1$ . The shares of the secret are the  $y$  values evaluated at  $t$  or more points.

With the above data, if any  $t$  out of the  $n$  participants combine their shares then using Lagrangian interpolation, there is a unique polynomial of degree at most  $t-1$  passing through the points. So the combined shares of the  $t$  participants can be used to recreate the polynomial and hence the secret, which is the polynomial evaluated at zero. The relation between the secret and the shares is obtained from Lagrange's interpolation formula.

Shamir's scheme is computationally efficient in terms of the computational effort required to create the shares and to recover the secret. Also the share size is optimal in an information theoretic sense. The reconstruction phase in Shamir's scheme can also be considered as a system of linear equations, which are defined by the shares. If  $t$  shares are submitted to the combiner, the system of linear equations can be solved. However, if  $t-1$  participants try to reconstruct the secret, they face the problem of solving  $t-1$  linear equations in  $t$  unknowns. This system of equations has one degree of freedom. Consequently,  $t-1$  participants do not obtain any information about the secret, as  $K$  was selected uniformly and randomly from  $GF(q)$ . Shamir's system is perfect.

### A $(t,t)$ Threshold Scheme

Karnin, Greene and Hellman describe a secret sharing scheme which realises  $(t,t)$ -access structures. The interest in such schemes is that they can be used as the basis for other cryptographic

constructions. In their scheme, the set of secrets  $S$  is the ring of residue classes  $Z_m$ , where  $m$  is any integer. (In applications  $m$  is large.) The secret  $K$  is shared using the following algorithm:

The dealer,  $D$ , randomly, uniformly and independently chooses  $t-1$  elements  $y_1, y_2, \dots, y_{t-1}$  from  $Z_m$ ;  $y_t$  is defined as  $K$  minus the sum of the  $t-1$  shares modulo  $m$ .

Participant  $P_i$  receives share  $y_i$  from  $D$ .

The Karnin-Greene-Hellman system is perfect, as the following argument shows. The set of shares of  $k < t$  participants attempting to reconstruct the secret either contains the share  $y_t$  (formed from  $K$  minus the sum of all the other shares) or not. In both cases the (unauthorised) participants lack the necessary information to determine  $K$ . Shamir's scheme with  $t=n$  provides an alternative construction of  $(t,t)$ -threshold schemes, using the fields  $GF(q)$  instead of  $Z_m$ .

### Threshold Schemes and Discrete Logarithms

The discrete logarithm in groups has been widely employed in the literature to transform threshold schemes into conditionally secure schemes with extra properties.

It is a consequence of the linearity of equation used to solve for the secret that Shamir's scheme can be modified to obtain schemes having enhanced properties such as disenrollment capability, in which shares from one or more participants can be made incapable of forming an updated secret.

The modified  $(t,n)$ -threshold schemes are capable of disenrolling participants whose shares have been compromised either through loss or theft, and still maintain the original threshold level. In the event that some of the original shares are compromised, the KDC can issue using a public authenticated channel a new group generator which will allow all the shareholders to calculate their new shares from the initial secret data. A similar setting can be used to obtain dynamic threshold schemes. Threshold schemes with disenrollment capability, without the assumption of the intractability of the discrete logarithm problem, can be based on families of threshold schemes.

The discrete logarithm can be used to transform Shamir's scheme into a conditionally secure scheme which does not require a trusted KDC. The discrete logarithm problem is used to encode the secret and the shares so that they can be publicly announced for verification purposes.

Blakley, Blakley, Chan and Massey established a lower bound on the number of bits required to encode the shares in schemes with disenrollment showing that this number grows linearly with the number of disenrollments.

The discrete logarithm can also be used to transform Shamir's scheme, to meet a very different purpose. One of the properties of the discrete logarithm is that the sum of the discrete logarithms of the shares of a secret is equal to the discrete logarithm of the product of the shares of the secret. This property has an application in secret-ballot elections where, in contrast with schemes mentioned above, the discrete logarithm problem is required to be tractable.

### Combinatorial Structures and Secret Sharing

Various connections between combinatorial structures and secret sharing are known. For example, threshold schemes can be based on combinatorial designs. Recently defining sets for  $t$ -designs and critical sets for Latin squares, have been used to design multilevel secret sharing schemes, in which a hierarchical structure can be imposed on the shares. In recent work critical sets in Room squares have also been used to realise multilevel secret sharing schemes. The schemes based on Latin and Room squares are examples of non-perfect schemes.



## THE PROBLEM OF CHEATERS

So far we have assumed that the participants in a secret sharing scheme are honest and faithfully obey the reconstruction protocol. However, there are conceivable situations where dishonest participants (assuming an honest KDC) may attempt to defraud the honest participants by altering the shares they were issued.

In the McEliece and Sarwate formulation of Shamir's scheme, invalid shares can be identified. Schemes with this capability are said to have the cheater identification property.

Tompa and Woll showed that public knowledge of the ordinates in Shamir's scheme allows dishonest participants to modify their shares resulting in an invalid secret  $K'$  being recreated. The cheater tricks the honest participant by submitting a perturbed share which results in a perturbed secret from which only the cheaters can recreate the correct secret, leaving the honest participants to believe that the perturbed secret is the correct secret.

This type of cheating can be prevented by disguising the publicly known ordinates with a randomly and uniformly chosen permutation known only to the dealer. This doubles the amount of information in each share but gives resistance against up to  $t-1$  cheaters.

The problem of secret sharing without the usual assumptions about the honesty of the participants, or even of the KDC, has been considered in the literature. For example, in verifiable secret sharing it is not assumed that the dealer is honest. This problem is studied by Chor, Goldwasser, Micali and Awerbuch. The problem is how to convince the participants in a  $(t,n)$ -threshold scheme, that every subset of  $t$  shares of a share set defines the same secret. This property is called  $t$ -consistency. Shamir's scheme is  $t$ -consistent.

## Realising Schemes Efficiently

There are secret sharing schemes which attain the known upper bounds on the information rate. Stinson also gave a general method, called decomposition to obtain a lower bound on the information rate.

## NON-PERFECT SCHEMES

It is known that in non-perfect schemes the size of the shares is less than the size of the secret. Because of this inequality, a non perfect scheme can be used to disperse a computer file to  $n$  sites, in such a way that the file can be recovered from its images which are held at any  $t$  of the sites ( $n > t$ ). Moreover, this can be done so that the size of the images is less than the size of the original file, resulting in an obvious saving of disk space. Making backups of computer files using this method provides insurance against the loss or destruction of valuable data.

A formal analysis of non-perfect secret sharing schemes is given by Ogata, Kurosawa and Tsujii. Their analysis, using information theory, characterises secret sharing schemes in which the participants not belonging to an access structure do gain some information about the secret. This condition is precluded in perfect secret sharing schemes.

The ramp schemes of Blakley and Meadows are examples of non-perfect schemes where the access structure consists of semi-access subsets. Another way of viewing ramp schemes is that the collective uncertainty about a secret gradually decreases as more participants join the collective.

## Electronic Authentication—issues relating to its selection and use

Ogata et al prove a lower bound on the size of the shares in non-perfect schemes. They also characterise non-perfect schemes for which the size of the shares is one half of the information contained in the secret. Ogata and Kurosawa established a general lower bound for the sizes of shares in non-perfect schemes. They showed that there is an access hierarchy for which the size of the shares is strictly larger than this bound. It is in general a difficult problem to realise non-perfect secret sharing schemes with the optimum share size, as in the case of perfect schemes.

## Chapter 5

# Biometric technologies

Biometrics is the process whereby physiological or behavioural characteristics are used to identify or verify the identity of an individual. It is the verification process that is synonymous with authentication, both in physical and electronic environments and it is this process that will be discussed in this chapter.

Biometrics have been used in some cases (particularly fingerprints and passport photos) for over a hundred years. In more recent years electronic implementations have been used for physical access control, initially in areas with high security requirements although with reductions in costs its use has become more widespread.

### DEFINITIONS

The following definitions have been taken from the 1999 Glossary of Biometric Terms<sup>1</sup>: compiled by the Association for Biometrics and the International Computer Security Association.

<i>Biometric System</i>	<i>An automated system capable of:</i> <ul style="list-style-type: none"><li>• <i>capturing a biometric sample from an end user,</i></li><li>• <i>extracting biometric data from that sample,</i></li><li>• <i>comparing the biometric data with that contained in one or more reference templates,</i></li><li>• <i>deciding how well they match, and</i></li><li>• <i>indicating whether or not an identification or verification of identity has been achieved.</i></li></ul>
<i>Capture</i>	<i>The method of taking a biometric sample from the end user.</i>
<i>Claimant</i>	<i>A person submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity.</i>
<i>Enrolee</i>	<i>A person who has a biometric reference template on file.</i>

---

<sup>1</sup> Association for Biometrics website <http://www.afb.org.uk/downloads/glossuk2.pdf>

<i>Enrolment</i>	<i>The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.</i>
<i>Identification/Identify</i>	<i>The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with 'Verification'.</i>
<i>Match/Matching</i>	<i>The process of comparing a biometric sample against a previously stored reference template and scoring the level of similarity. An accept-or-reject decision is then based upon whether this score exceeds the given threshold.</i>
<i>Template/ Reference Template</i>	<i>Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.</i>
<i>Verification/Verify</i>	<i>The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with 'Identification'.</i>

## TECHNOLOGY

A number of the biometric techniques currently in use or under development. Some of these are listed below.

### Physiological:

- fingerprint
- finger geometry
- hand geometry
- iris recognition
- retina pattern
- face recognition (geometry and thermal imaging)
- palm pattern
- voice verification
- vein pattern
- body odour
- DNA

### Behavioural:

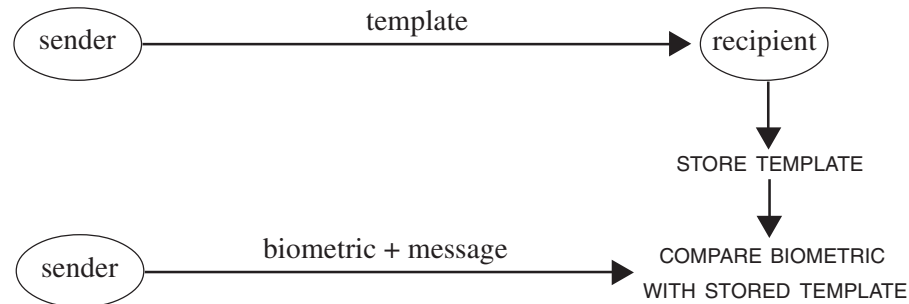
- signature verification
- keystroke dynamics

This chapter does not address particular biometric technologies<sup>2</sup>. Rather it identifies the aspects of the technology that are common to all technologies and relevant to the general discussion of electronic authentication.

---

2. A number of the technologies and terminologies are discussed at <http://www.afb.org.uk/downloads/glossuk2.pdf>

Biometric techniques involve the capture of a sample of the individual's biometric characteristic to produce a template that is then linked to the individual through an enrolment process and stored. For subsequent authentication a new sample is captured and compared with the stored template.



**Figure 24: Biometrics**

As mentioned in the general issues chapter (Chapter 1), many implementations use cryptographic techniques to prevent capture of samples for subsequent replaying. Other implementations use templates stored on tokens under the control of the individual and the token generates an authentication message using another technology such as asymmetric cryptography or shared secret. The issues associated with these approaches are discussed further in the hybrid technologies chapter (Chapter 7).

## USE IN ELECTRONIC BUSINESS MODELS

As a biometric is a characteristic of an individual there is a strong binding between that individual and the authenticator. The strength of the binding may vary in terms of the particular characteristic and the technology being used. As with any authentication technology, both the authentication service provider and user will need to be aware of the degree of reliance that can be placed on the authenticator.

While biometric authenticators provide a strong binding with an individual, they do not provide the same facility for authentication of corporate or machine identity nor for role or attribute authentication. However this has also been the case in the paper world where, for example, written delegations have been used to link an identity to a particular role, attribute or corporate identity. Machine identity authentication is a requirement unique to the electronic environment and does not have a paper based equivalent.

### Open Model

Biometric technologies do not lend themselves readily to the open business model as they rely on comparison between a sample captured at the time of the transaction and a template captured as part of an earlier enrolment process. This implies that there was an earlier relationship between the parties. Unless some form of independent authentication service provider is used, current biometric approaches cannot operate without a prior relationship between the parties.

Furthermore, in an open system the transmission of a sample or template would be unprotected unless encryption were used. If symmetric encryption were used it again would require a prior relationship to exchange the symmetric key. If asymmetric cryptography were used, some form of authentication would be required to validate the public key and the approach would then be one of hybrid electronic

authentication. Another measure is the use of one-way encryption which prevents the biometric from being recovered from the template. Furthermore as the encryption is applied in the validation process this would prevent an encrypted template being directly compared.

It is feasible for an authentication service provider to provide a certified biometric template or validate a biometric authenticator forwarded by the recipient of a transaction. However, again the process is likely to use some form of encryption to protect the biometric information being exchanged and the arguments in the previous paragraph would equally apply.

### **Closed Model**

In this model there is some form of prior relationship between the parties and this relationship could involve the enrolment of the parties biometric data. It could also involve establishment of schemes to protect the exchange of biometric information. Within an organisation this could be simply reliance on security of the internal network. In external networks it could involve the use of encryption to protect the biometric information. Within a closed system, exchange of symmetric keys would be practical. The use of a biometric authenticator as an access control tool is a classic example of a closed model.

Biometric technologies lend themselves to closed business models.

### **Open-But-Bounded Model**

In the open-but-bounded model the type of general agreement envisaged in the general issues chapter (Chapter 1) need not exist until immediately prior to the transaction occurring. In such cases it is unlikely that a biometric authenticator would have been enrolled by a recipient prior to a transaction. In this model it may be possible for a recipient to obtain a certified copy of a template from an authentication service provider. As discussed under open models, such processes are likely to involve other authentication processes and would fall into the hybrid category.

Biometrics alone do not readily lend themselves to open-but-bounded business models.

## **USER REQUIREMENTS**

Biometrics lend themselves more towards business rather than individual user requirements. The two main factors are the need for hardware capture devices and storage capacity for templates. In addition the need to enrol parties is more of a problem for individual and small business users.

The cost of capture devices will vary with the technology adopted. More common devices such as fingerprint capture devices can be expected to become more affordable as they are more widely deployed. Other technologies may be able to be implemented through software using other devices already being used. For example it may be possible to develop facial recognition software that relies on cameras used for video conferencing as the capture device. Voice verification could be performed using existing microphone equipment attached to PCs.

Storage capacity for templates will vary depending on the number of biometric authenticators which a user is likely to receive. In addition, as the template and comparison software is critical to the authentication process these elements must be secured to a level appropriate to the degree of reliance that is to be placed on the authenticator. Uptake of this technology will depend on the costs of storage and security.

Finally there is the enrolment process. Typically this would require the enrolee to physically provide a sample. In open and open-but-bounded models it is unlikely that this would occur. Even in the

closed model this may not always be practical. It is, however, possible for an authentication service provider to enrol authenticators and certify templates. Distribution of certified templates or validation of biometric authenticators against a certified template does involve some security problems as discussed earlier. However, a recipient could have a secure link to an authentication service provider under some agreed scheme, or hybrid technologies—using asymmetric cryptography—could be used.

Whether biometric authentication, alone or as part of a hybrid approach, will meet a user's requirements will depend very much on the business model and the degree of trust required.

### **CERTIFICATION MODELS**

For the purposes of this discussion certification is, based on the definition of certificate in the general issues chapter (Chapter 1): *the process of generating an electronic document, generally issued by a third party, that binds an authenticator to a specified user*. Enrolment is, as defined earlier, the process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. As such, certification of a biometric authenticator involves issuing an electronic document that binds a specified user to a template obtained through an enrolment process.

#### **Formal Certification**

In this case an authentication service provider would enrol a user and issue a certificate binding the user to the template. The template could be incorporated in the certificate and sent with the message or stored in a publicly accessible directory.

#### **Informal Certification**

In this case a third party or a number of third parties other than an authentication service provider would enrol and certify the user. The recipient would accept the certificate from a certifier that they trust.

#### **No Certification**

In this case the relying party directly enrolls the user and dispenses with the requirement for a certificate. This scenario would typically occur in closed models. Biometrics lend themselves to this approach.

While it would be technically feasible for a person to accept a biometric without a template and store it in case of a dispute, it is difficult to imagine a scenario in which this would be a preferred approach.

### **TRUST**

While the level of trust in a biometric itself is high, it should be born in mind that biometric authenticators are based on samples. For example a finger print may be assessed on whether there is or isn't a ridge at a particular point. Therefore if 20 points are sampled the probability of two persons providing the same sample is one in  $2^{20}$ . The more the points of sample, the lower the probability of two persons returning the same sample. Other issues such as assurance of the process used to establish identity, assurance of the binding process between identity and the template, and the operational integrity of the biometric system will all impact on the quality of assurance. The way in which the biometric is implemented can therefore determine the level of trust that can be placed in the technology.



A further factor determined by the implementation and technology is the probability of false acceptance (Type II error)<sup>3</sup> and false rejection (Type I error)<sup>4</sup>. Some technologies can be adapted to lower a particular error rate at the expense of increasing the other error rate.

For these reason biometrics can be implemented with a technology and configuration that produces a level of trust that meets an organisations business risk model. The disadvantage of these technologies is that, as with other authentication technologies discussed in the other chapters, for the most part the means of establishing the level of trust that can be placed on a particular implementation is very dependent on technical issues beyond the understanding of the average user. The development of standards and accreditation processes for biometrics will assist users in determining the product that best suits their needs.

The other major trust issue is the security of the sample in transmission and the template in storage. Techniques such as encryption can be used to protect a sample while it is in transit. The use of encryption in these circumstances is to protect the sample and as such is not performing an authentication function. This is not, therefore, a hybrid authentication approach. Similarly one-way encryption can be used to prevent a template being used to reconstruct a biometric and this, again, is not a hybrid authentication approach. There are a number of other security measures that can be taken to protect biometric samples and templates.

The security of samples and templates is of greater significance in biometric authentication due to the unique nature of the various characteristics and the inability to change or replace them. If a sample or template of a characteristic is captured in a form that allows it to be replayed, the compromised characteristic may not be able to be used again. There are however some avenues for reuse. If several technologies use the same characteristic, such as a fingerprint, but sample the characteristic in different ways, it may be possible to change technologies. Alternatively an individual may start to use a different characteristic. However, alternative approaches are limited and would be more costly to effect than the revocation and reissue of encryption keys, PINs or passwords.

### **LIABILITY**

As a biometric is a physical characteristic of an individual, liability issues arising from failure to protect a secret component of an authentication technology do not arise. However, the vulnerability of biometrics lie in the samples and templates. It is possible that an individual's equipment does not adequately protect a sample, that a sample is not adequately protected in transit and can be captured and replayed, or that the holder of a template has not adequately protected that template. Adequate security measures are needed to reduce these risks.

As with other technologies, if the certification and, in the case of biometrics, the enrolment process has not been correctly performed, liability issues may arise. Also as with other technologies there are liability issues relating to revocation and failure to provide service.

From the user perspective, however, the reduced probability of liability arising from loss of an adequately secured authenticator makes this technology more attractive from a liability perspective.

### **ROLES OF PARTICIPANTS**

The communities of interest for this technology are the same as those outlined in the general issues chapter (Chapter 1). However, as mentioned earlier the main strength lies within closed systems. For

---

3 This term is defined on the Association for Biometrics website <http://www.afb.org.uk/public/glossuk1.html>

4 This term is defined on the Association for Biometrics website <http://www.afb.org.uk/public/glossuk1.html>

this reason the roles of government, high level authentication authorities and authentication service providers are not as significant. However, there is a role for enrolment and storage of templates that would equate to some elements of an authentication service provider; particularly in respect of identification, revocation and security of templates and liability arising from failure of the authentication service provider to adequately provide these services.

### **INTEROPERABILITY**

There is a wide variety of biometric approaches under development and it is not possible to achieve interoperability between them as each can relate to a different characteristic. Even technologies using the same biometric characteristic can have a variety of implementations. Typically the reader and template comparison require the same approach in terms of the characteristic being used, the sampling rate and other special features. The Biometrics Consortium<sup>5</sup> is developing standards for the use and interoperability of biometrics.

However, in the short term, biometrics, as a stand-alone authenticator, are unlikely to be widely adopted outside discrete closed business models. It is the linking of biometrics with other technologies to produce a hybrid technology that is likely to produce widespread interoperable authentication schemes. This issue is further discussed in the hybrid technologies chapter (Chapter 7).

### **ACCREDITATION**

Accreditation processes generally rely on the existence of standards or other normative documents. While individual devices can be tested, and their performance against their own targets can be verified, this is not a formal accreditation process.

The UK Government's Biometrics Working Group<sup>6</sup> has developed best practice standards for testing and reporting on biometric device performance, a common criteria protection profile for biometrics and advice on the selection of biometric products. This work is being undertaken in consultation with product developers and other governments and should lead to the availability of accredited biometric products.

### **CULTURAL DIFFERENCES**

Because biometrics rely on human characteristics, it is the technology most likely to be impacted by cultural differences. For example a face recognition approach is not practical in countries where items of clothing traditionally obscure the face.

In other countries there are civil liberties objections, still a cultural problem, to widespread recording of biometric characteristics such as fingerprints and DNA. These objections are generally based on a fear of possible misuse of the biometric. Developments such as one way encryption of samples to generate templates or storage of templates on tokens under the control of the individual can reduce these problems. The latter case, however, would then need the token to generate another form of authentication and would therefore be a hybrid approach.

A further issue arises where a person is signing on behalf of another person. In some cultures this involves the transfer of the signing instrument, or authenticator from one individual to the other. The concept of power of attorney does not exist. Biometrics are unique to individuals and cannot be transferred. As such they could not be used in such circumstances.

---

<sup>5</sup> <http://www.biometrics.org/html/standards.html>

<sup>6</sup> <http://www.cesg.gov.uk/technology/biometrics>

However, the main cultural problem associated with biometrics is that it is based on a characteristic unique to an individual. In a number of cultures the concept of an individual is subsumed by that of the tribe, clan or extended family. Property is owned by, and transactions are undertaken on behalf of, the community not the individual. Often numerous members of the community can transact on behalf of the community so authority is not attached to a single individual. Other authentication technologies allow the secret component of that technology to be shared. For example PINs and passwords for credit and debit cards are commonly shared in such communities. Even private keys could feasibly be shared. Biometric authenticators would not be effective in these communities without cultural change.

When developing biometric authentication schemes, consideration needs to be given to potential cultural differences in communities with which those schemes are likely to interact.

## **AWARENESS**

There are a number of misconceptions about biometrics and their use. People have a natural fear of injury to their bodies and are reluctant to use capture devices about which they are uncertain. There are also concerns that biometrics, particularly fingerprints and DNA, can be misused by governments and law enforcement agencies. As mentioned earlier, a number of implementations do not allow reconstitution of the biometric. However the fear remains.

While a broad section of society accepts that at least some biometrics are unique, this acceptance is less than universal. In addition many are not confident that the capture techniques will retain the uniqueness. Extensive awareness campaigns will need to be undertaken to overcome these misconceptions and develop user confidence before there is widespread acceptance of the technology.

### **Government Awareness**

Awareness and understanding of biometric authentication within government is still limited. While there is a growing awareness of the role of biometrics, this does not approach the level of awareness of asymmetric, or public key, cryptography. Consequently its potential role as an electronic authentication technology is not generally understood. Until this level of awareness is increased, governments will have difficulty in raising awareness in the community. Biometric technologies continue to be underrated as a tool for electronic commerce. There is a need for governments to better inform themselves of this technology and the contributions it can make to electronic authentication and electronic commerce.

### **Business Awareness**

Unlike governments, who at least have a need to be aware of emerging technologies, business tends to be driven by what is marketed to them. As with governments the electronic authentication technology to which they are most exposed is public key. As businesses tend to be driven by risk management approaches, they are less likely to risk what is to them is an unknown technology. Furthermore, unlike governments, many businesses are unlikely to have an internal capability to assess the technology and the risk implications. Raising business awareness of biometric authentication and the trust that can be placed in it will be crucial if this technology is to be widely deployed.

### **Individual User Awareness**

The greatest apprehension and misconceptions will be with individual users. Even if governments and business were to adopt biometric technologies, its uptake by individual users, in many cases their

largest group of clients, will be slow and patchy unless positive steps are taken to increase their awareness of the benefits for them. There is also a need to consider the ease of the enrolment and registration process that would minimise the real or perceived intrusiveness in capturing the biometric information during this process.

A further factor for individual users is the uptake of these technologies by the suppliers of the equipment to them. If that equipment comes with inbuilt features that facilitate biometric authentication they are more likely to accept the technology. This is particularly the case if reviews of the equipment highlights the inbuilt features and outlines the benefits of its use.

In general the greatest understanding of the technology is in academia and with the product manufacturers. Any awareness raising campaign without their involvement and commitment will be futile. In addition widely reported pilot projects can significantly raise the level of awareness.

### **LEADERSHIP**

While raising awareness is important for the uptake of biometric authentication, leadership is even more important. Leadership by example through the use of the technology is one of the main elements. However, establishing the necessary policy frameworks and business models is also important.

#### **Governments**

A number of governments have established their legal and policy frameworks to support public key approaches to electronic authentication. More recently the trend has been towards the establishment of technology neutral frameworks that will support a range of electronic authentication technologies. Without government leadership through the establishment of frameworks that support biometric as well as other authentication techniques, biometric technology will not be used to its full potential.

The other area where governments can provide leadership is through the use of biometric authentication in its own activities and the publication of that fact. Already governments use biometric authenticators extensively as access control tools. The extension of the technology to electronic commerce applications both within organisations and with client groups will provide significant leadership to the community in general.

#### **International Organisations**

Much of the focus of discussions on electronic authentication to date in international organisations has been on the use of asymmetric cryptography in public key infrastructures. These discussions will need to be extended if the full range of electronic authentication technologies are to be allowed to develop. Already some international organisations are adopting technology neutral approaches in their considerations. This will provide the necessary leadership for biometrics to be recognised as a viable electronic authentication technology.

#### **Business Corporations**

As with Government, a number of businesses use biometric technologies for internal access control. The use of biometrics alone or in combination with other technologies, both internally, and with their clients, will provide leadership in the use of the technology. Furthermore, the identification of the business models to which the technology is suited is best carried out by the business community.

## **Users and User Groups**

The role of users and user groups is more by way of acceptance of the technology and raising awareness of the issues surrounding its use. One of the principle misconceptions about this technology is that it can be misused by authorities. There is a role, particularly for user groups, in obtaining a better understanding of the technology in order to counter the misconceptions. However, there is equally a role for governments and biometric manufacturers in ensuring that user groups obtain sufficient accurate information on which to make their judgements.

## **IT Industry**

The IT industry can provide leadership through incorporating biometric technologies alone or in conjunction with other electronic authentication technologies in their products. This is already occurring with the development of biometric techniques such as fingerprint readers that can interface with computers or smart cards. The biometric sector of the IT industry can facilitate the use of the technology by ensuring users are aware of the benefits and risks associated with the technology. The development of biometric industry associations is facilitating this process.

## **COMBINATION WITH OTHER TECHNOLOGIES (HYBRIDS)**

While this chapter covers the use of biometric authentication technologies, it would not be complete without some reference to the use of biometrics in combination with other electronic authentication technologies. This aspect is covered in more detail in the hybrid technologies chapter (Chapter 7). Biometrics add an extra layer of security to the use of authentication technologies by linking the use of a stored authenticator to a physiological or behavioural characteristic of the owner of that authenticator. At present the main application is to link the biometric to the stored private key component of an asymmetric cryptographic, or public key, authenticator. Conceivably it could also apply to a secret key in authentication systems using symmetric cryptography. Additionally it can add weight to some of the other approaches to electronic authentication such as IP address or email address where access to that address is controlled by a biometric. For example where a user cannot log on to a particular machine or as a particular user without a biometric authentication process this adds weight to the reliance that can be placed on that other authenticator.

While it is likely that the main role of biometric authentication technologies is likely to be in hybrid applications, the issues involved cannot be addressed without an understanding of the issues involved with each of the technologies in the hybrid. This chapter is designed to outline the main issues associated with the use of biometric authentication technologies.

## Chapter 6

# Other technologies

At the present point of development of electronic messaging, particularly email, the most common forms of authentication do not fall into the categories discussed in the previous chapters on asymmetric cryptography, shared secrets and biometrics. These other forms are also most closely related to the paper environment as they involve authentication by either a name or a location, in this case an electronic location. These are characteristics of the message or machine rather than a specific authentication technology. In some cases authentication can occur at the time of the transaction, such as in reading an email address, while in other cases it may occur after the event, such as in using audit trail information.

Most users will have responded to instructions from a superior, sometimes with financial implications, based on the name on the bottom of an email or the displayed email address of the sender. The reliance on simply a name at the bottom of an email can extend to parties who have never met. The then Public Key Authentication Task Group conducted a workshop at TEL 18 in Port Moresby. A number of speakers attended that workshop on the basis of an email from the task group chair with no technology used to authenticate the message. Their organisations were prepared to commit a not inconsiderable sum of money for them to attend the workshop without a formally authenticated invitation to attend.

This group of characteristics can only provide a limited form of authentication and do not provide confidentiality or integrity services.

### **CHARACTERISTICS**

The main message or machine characteristics that can be used to authenticate a message are:

- email address,
- IP address,
- domain name,
- signature block,
- message properties such as those in the message header,
- terminal identifier,
- trace route information, and
- audit logs containing any of the above information.

### **Email Address**

This information is supplied with an email and shows a user name and an associated domain name in the format 'user name@domain name'. The two in combination must be unique to allow the email



system to operate. While in most cases an email address is linked to an individual, it is quite common for an email address to be linked simply to an organisation. There is also a more secure email platform X.400 which includes more detail in the address. An address is usually in the format C = country name, A = administration management domain, P = private management domain, O = organization name, OU = organizational unit name, S = surname, G = given name.

## **IP Address**

The Internet Protocol (IP) address is used primarily as the means by which packets are directed to their destination. It consists of four numbers of up to three digits separated by dots (nnn.nnn.nnn.nnn). Machines with permanent connections have a static IP address while those connected through connections to an Internet Service Provider (ISP) may be assigned an IP address from a bank of addresses for that ISP server. The server assigned IP address may vary each time a connection is made. Similarly a local area network may be connected through a server with a single IP address.

While IP addresses were originally designed to direct messages to a recipient they also are used to identify the source of a message to allow error messages to be returned. It is this source information that can be used to authenticate the machine or server which sent a message. Where more than one person may be connected to a server there is no way of using the IP address to identify the individual who sent a message. IP addresses do have a role in machine to machine authentication.

## **Domain Name**

The Domain Name System (DNS) is a hierarchical system that translates IP addresses into easily recognised names. The domain names are structured in a hierarchy of country code, such as sg (Singapore), au (Australia); domain, such as com (commercial), org (organisation) gov (government) edu (education); and distinguished name expressed in reverse order. It is possible for the country code to be absent as is usually the case for US domain names. For example the APEC Secretariat domain is apcsec.org.sg . The domain name is converted to an IP address through a network of domain name servers. As the domain name is essentially the same as an IP address the comments in the previous paragraphs also apply here.

## **Message Properties**

Information such as email address, IP address and domain name, including routing information, is stored in message headers accessible from email packages. This information may be used as the means of implementing one of the above approaches to authentication.

## **Signature Block**

In many cases email messages have replaced signed letters or internal memoranda. Most people sending e-mails use some form of signature typed at the end of the message. This is probably the most commonly used means of authentication of electronic messages. Generally the signature block identifies an individual although in some cases it may identify a particular group or organisation. It cannot be used to authenticate machines.

## **Terminal Identifier**

Most terminals attached to internal networks have terminal identifiers which may or may not involve an IP address. Where an IP address is not involved, the terminal identifier can often perform the same function as an IP address but limited to the internal network. It can perform machine authentication.

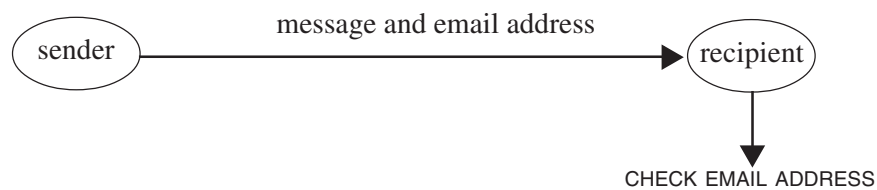


## Trace Route Information

Some toolkits allow you to trace the route of a message while the message is being sent or received. This is of limited use in authenticating messages due to its 'real time' nature. It may have some role in authenticating a recipient machine before a message is sent.

## Audit Logs

Audit logs can be set up to record information such as email address, IP address, domain name and terminal identifier. Information recorded in the logs may be used to authenticate individuals or machines as appropriate.



**Figure 25: Other Email Address Example**

## USE IN ELECTRONIC BUSINESS MODELS

There is no formal binding between an individual or organisation and the above characteristics. Even in the case of email, while there is a distinguished name and a process for the domain issuing that name, generally the only check is that the name has not already been issued. Even domain names are issued without a reliable formal binding at this stage as is evidenced by the current problem of 'cybersquatting'. In the case of IP address there is some minimal binding between the IP address and the machine as this is required to allow connections to be made.

The characteristics, other than terminal identifier, can be associated with messages in open, closed and open-but-bounded models. Terminal identifier can only be used in closed models as they relate to terminals on a particular network. The level of trust can vary depending on the model and this is discussed further in the Trust Section below.

## USER REQUIREMENTS

Most users are familiar with the basic concept of an email address and domain name, and where to find them as they are fundamental aspects of Internet usage. The use of signature blocks is the same as exists in the paper world and would also be familiar to all users. The remaining characteristics require a slightly more detailed technical knowledge.

Most of the characteristics are integral parts of the appropriate applications. For example email packages display the sender's email address either directly or behind a display name. Most browsers display the domain name of the site to which they are connected. Other characteristics such as message headers and IP address can be displayed using standard applications. The additional costs of using these characteristics is generally limited to the time taken to show a user how to find the characteristic.

The main problem is whether the characteristics are trustworthy enough to meet the users requirements. This is discussed in the Trust Section below.

## CERTIFICATION MODELS

Certification was defined in the general issues chapter (Chapter 1) as: *the process of generating an electronic document, generally issued by a third party, that binds an authenticator to a specific user.* As mentioned above, there is no formal process of binding these characteristics to a specific user. However, it may be possible for a person to informally advise that another person has a particular name, or an organisation has a particular domain name. This may form an informal certification process. However in most cases no certification is used.

## TRUST

Many of these characteristics were originally developed as a means of identifying individuals or machines and were not developed as a means of authenticating that identity. They were simply developed to ensure delivery of data to and from particular individuals and machines. The emphasis was more on ensuring the uniqueness of the identity rather than binding the identity to a particular individual. The exception is X.400 which was designed as a secure messaging scheme including message origin authentication. However, X.400 uses asymmetric cryptography as part of its message origin authentication and this approach is included in the hybrid technologies chapter (Chapter 7).

Instances of IP spoofing, identity theft and cyber squatting underline the weaknesses of the characteristics. Tutorials on IP spoofing are readily available on the Internet. Most people will have experienced SPAM mail from a spoofed email address.

The main value of these characteristics as authenticators lies not so much in the characteristic as in supporting information. This can include an expectation of receiving a message or the content of the message itself. This collateral information combined with the message characteristics can form an aggregation of trust sufficient for a party to rely on the message.

The level of trust can be influenced by the nature of the business model. The characteristics when used in a closed system can result in a high level of trust, the level of trust being inversely proportional to the number of participants in the closed model. It is quite common to hear of people using another person's terminal to send a message even in a closed system. Once you move into an open or open-but-bounded model the potential for misuse such as IP spoofing or email address spoofing increases significantly.

Ultimately, as with all authentication technologies, it comes down to the user to decide whether an authenticator, in this case the characteristics, is suitable for the purpose for which it was provided. This is a risk management approach. However, it should be noted that these characteristics are more widely used than generally acknowledged and should not be ignored at this stage.

## LIABILITY

While some characteristics such as email address and domain name are allocated by third parties this is done to facilitate message delivery. Similarly some of the characteristics are generated by machines or Internet elements again to facilitate message delivery. As none of the characteristics are actually developed for authentication, users would carry all liability for their use as authenticators unless they could establish that someone had deliberately interfered with the process for the purpose of misleading them. This may result in criminal rather than civil proceedings as such interference can, in some circumstances, involve unauthorised access to a machine or data.

## **ROLES OF PARTICIPANTS**

The main participant in the use of these characteristics is the recipient. In some cases the characteristics are attached in a manner transparent to the user. Application developers and standards making bodies have a role in supplying the means by which the characteristics are generated and displayed.

## **INTEROPERABILITY**

Most of the characteristics are generated as part of protocols designed to ensure interoperability. There may, however, be some differences in how they are accessed or displayed between different applications. In general interoperability is not a problem with these characteristics.

## **ACCREDITATION**

As these characteristics were not developed for authentication purposes it is not possible to accredit them for that purpose. However, it may be possible to gauge the degree of reliance that can be placed on them. This is more a risk management approach than an accreditation process.

## **CULTURAL DIFFERENCES**

Cultural differences relate primarily to persons. The characteristics covered in this annex relate to messages and machines. It is unlikely that there will be any impact of cultural differences in those cultures based on the concept of community rather than individual. For example an email signature block could be used to identify extended families or clan, village or tribal groupings. Similarly a machine can be linked back to the community in which it is located as easily, if not more easily, as it can be linked to an individual.

These other characteristics cannot, in general, be transferred from individual to individual in the same way as a signing device such as a chop or seal. However, it is possible for a person to use another person's machine and thereby send a message on their behalf, achieving the same result.

## **AWARENESS**

As mentioned earlier, most people already use these characteristics as an authenticator often without realising it. However, the strength of the authentication is more often related to collateral information rather than the characteristic itself. Any awareness needs to focus on that aspect rather than on the characteristics themselves. The main issue however, is the circumstances in which the use of these characteristics is appropriate.

### **Government Awareness**

Governments have a traditionally adopted relatively high levels of security for their information. However, as they have moved towards information technology for their internal communications, the characteristics covered in this chapter are often used for low level authentication of messages. As governments generally use risk management models for their security they should be aware of the circumstances where use of these technologies is appropriate.

### **Business Awareness**

Business, particularly smaller business, is less aware of the risks surrounding these characteristics. The result can range from complete avoidance to inappropriate use of the characteristics. There is a need for raising industry awareness of the role of these characteristics and the circumstances in which their use might be appropriate.

### **Individual User Awareness**

Most individuals currently use the Internet for ordering and paying for goods and services and for personal messages. For the most part authentication of the merchant or other individual is restricted to DNS or email services although there is some reliance on webserver certificates. While there is a lot of hype about security on the Internet, the fact is that so far this approach is operating effectively for those who have sufficient confidence in the system. The problem is more one of generating the necessary confidence. While this will eventually lead to more secure authentication and payment systems, there is a need to ensure that negative publicity does not prevent people using the characteristics until stronger techniques are widely deployed.

### **LEADERSHIP**

These characteristics are already well used as a low level authentication approach. There is little that governments, international organisations, business corporations, users and user groups, and the IT industry can do by way of leadership other than promoting awareness of the role of the characteristics and the appropriate circumstances for their use. There is a role for governments in ensuring that these characteristics are not denied legal effect in line with the technology neutrality provisions of the UNCITRAL Model Law.

### **COMBINATION WITH OTHER TECHNOLOGIES (HYBRIDS)**

These characteristics do not lend themselves to combination with other authentication technologies.

## Chapter 7

# Hybrid technologies

A number of technologies can be combined in the authentication process. These combinations can take two basic forms:

- a number of authentication technologies that are used sequentially in a single transaction—called **chained technologies** in this chapter—and
- a technology or several technologies, generally different, are used to secure an authenticator in a single transaction—called **secured technologies** in this chapter.

In some cases the use of an authentication technology may involve the use of an authentication service provider. Also, in some cases secured and chained technologies can be combined.

### TECHNOLOGY

#### Chained Technologies

In this approach an authentication technology is used to trigger another authentication technology. The most common example at present is the use of a password (shared secret) to release the private key for a digital signature (asymmetric cryptography). In this case the shared secret is between the user and his or her PC or token on which the private key is stored.

One of the most common implementations of two-element chained technology is better known as two-factor authentication<sup>1</sup>. This uses two of three factors:

- something you have,
- something you know, or
- something you are.

Tokens such as smart cards or USB devices (something you have) activated by either a PIN (something you know) or a biometric (something you are) are examples of two-factor authentication using chained technology.

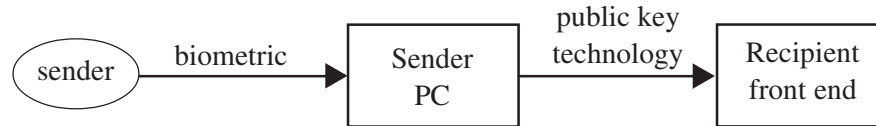
The technique is more commonly used in authentication for access control purposes rather than electronic transactions. However the requirement for secure signature creation devices in the European Union Directive on Electronic Signatures<sup>2</sup> and in other legislation is likely to result in more

---

1 In some cases all three factors may be used. This is known as multi factor authentication. This is not to be confused with the three element technology example below which still only uses two factors.

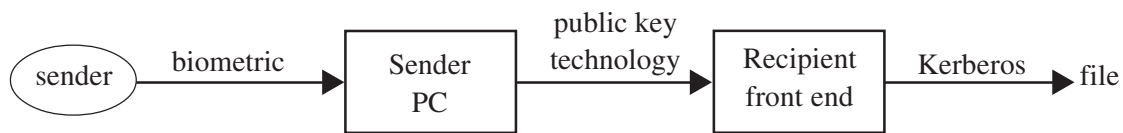
2 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures OJ No L 13 p.12 19/1/2000, <http://www.qlinks.net/comdocs/elsig/en.pdf>

common use of this approach in authenticating electronic transactions. An example is the use of a biometric to trigger the private key for public key technology (asymmetric cryptography).



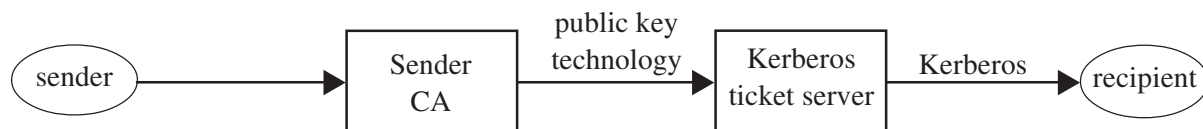
**Figure 26: Two-Element Chained Technology**

In some cases it is possible that three different technologies can be used in a single transaction. An example would be a biometric used to trigger the private-key–public-key technology (asymmetric cryptography) which, on receipt, generates a Kerberos ticket (symmetric cryptography) to access a particular file.



**Figure 27: Three-Element Chained Technology**

Extending the above example, it is possible for more than one application service provider to be involved in the course of a single transaction. An independent certification authority may be involved in the provision of the certificate, and possibly of keys used in the public key technology, while a separate authentication service provider may operate the Kerberos ticket server. In this example the authenticator relied on by the recipient is not the same as that sent from the sender. Furthermore there may not be a direct relationship between the recipient and the sender's certification authority. Some legislative approaches presume that the holder of a private key is the originator of any document signed with that private key. Any presumption in respect of a digital signature would benefit the operator of the Kerberos ticket server (who received the digital signature) but not the recipient (who only received a Kerberos ticket).

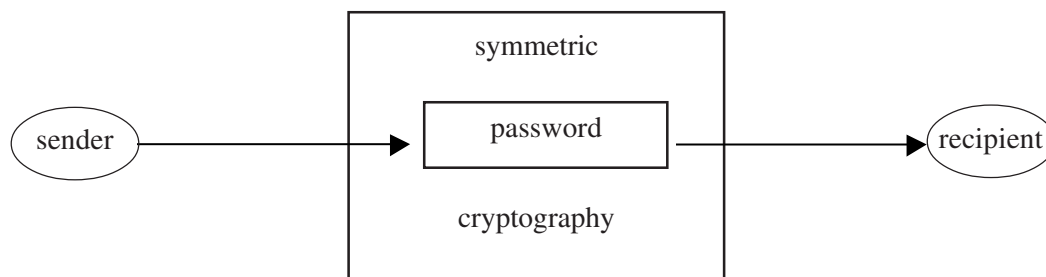


**Figure 28: Two-ASP-Chained Technology**

There has been some discussion that the use of a shared secret or biometric in conjunction with a private key is a security process rather than an authentication process. This will depend on the approach used. If the shared secret or biometric simply provides access to the private key which is then independently used as an authenticator, possibly for multiple transactions, then the shared secret or biometric is simply part of a security process. However, if the process is automated and the action of providing the shared secret or biometric triggers the authentication process for each individual transactions then it can be argued that this is a chained authentication process. Ultimately it may be a matter for courts to decide whether the approach used was a security process or a chained technology process. Overly prescriptive legislation that does not recognise the possibility of chained authenticators can only complicate the legal process.

### Secured Technologies

In this approach another technology is used to protect an authenticator in storage or transit. A common implementation is the use of symmetric cryptography to protect a shared secret. Another common implementation is the use of symmetric cryptography (shared secret) to protect a biometric between the reader and the template storage.



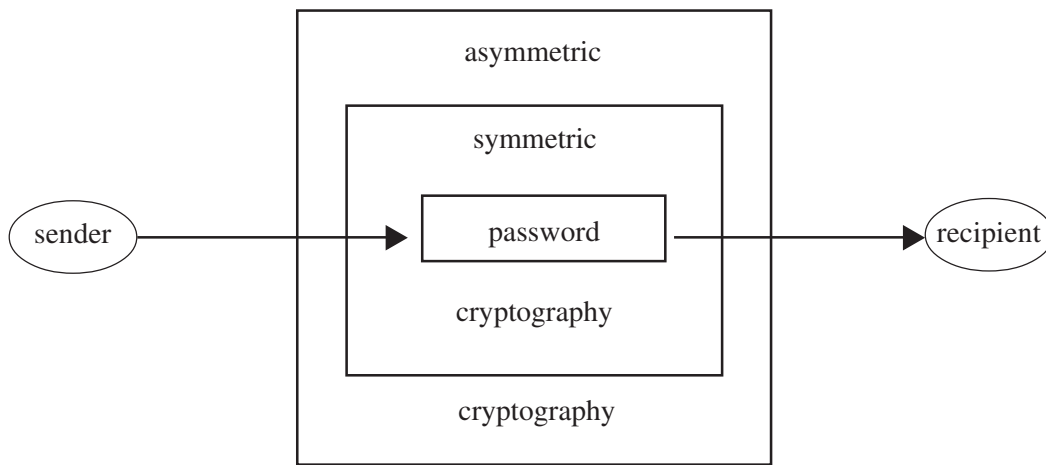
**Figure 29: Secured Technology**

In some cases secured technologies are used to protect an authenticator without playing a part in authentication of individual transactions. In other cases the protective technology is an authentication technology and may be used to authenticate the recipient to the sender. The most common example of this is the use of public key technology (asymmetric cryptography) such as secure sockets layer (SSL) to exchange a key for symmetric cryptography (shared secret) to protect a PIN or password (again shared secrets) during transit. This is still the most common approach in electronic commerce.

Another example is a token used to store a private key for asymmetric cryptography protected by a password (shared secret). The token may be used to sign multiple transactions once unlocked. While the shared secret does not play a direct role in the authentication of an individual transaction, it is a factor to be taken into consideration when determining the level of trust in the authenticator.

In some cases several layers can be involved in a secured technology implementation. For example asymmetric cryptography can be used to transfer symmetric cryptography session keys to protect a shared secret or biometric used for authentication. This is the process often used for automatic teller machines (ATM) and electronic funds transfer point of sale (EFTPOS) machines. Similar approaches are used with SSL and virtual private networks (VPN).



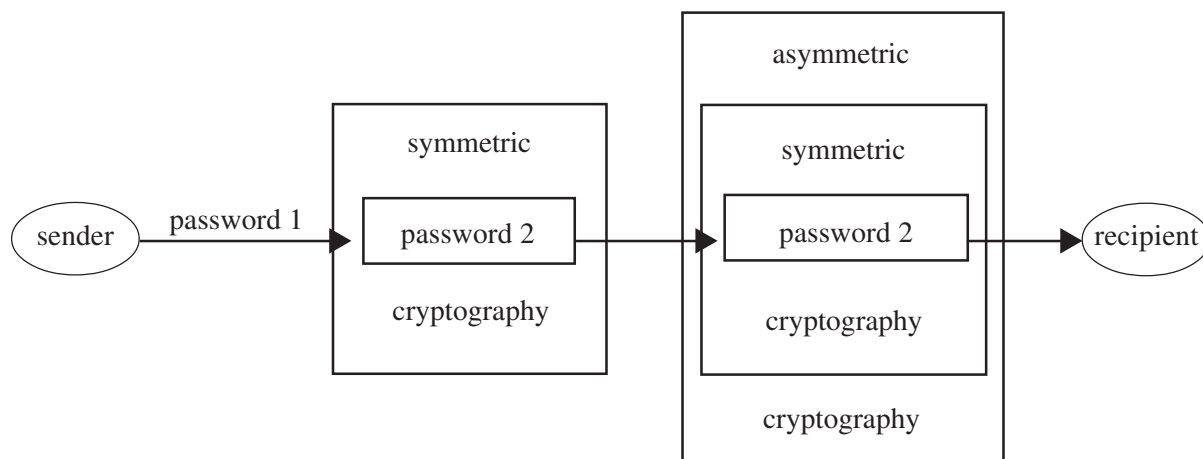


**Figure 30: Multiple Layered Secured Technology**

In the example of SSL protecting a password, it is generally the recipient of the authenticator whose technology supports the session key exchange using its public key (server gated cryptography) generally supported by a webserver certificate. As such, the sender is reliant on the security of the recipient's public key technology for the security of the overall transaction. The fact that the sender is reliant on the recipient's security technology to protect their authenticator in transit is a factor that courts will need to take into consideration in the case of disputed transactions.

### Combined Technologies

It is possible to chain several secured technologies in a single transaction. For example a sender may have a number of passwords stored on their PC or on a token. The 'wallet' of passwords or the token may protect the passwords with symmetric cryptography. A password or biometric can be used to release the required password for the transaction (chained technology). The password could then be protected in transit by symmetric cryptography established by asymmetric cryptography (secured technology).



**Figure 31: Combined Technology**

These types of implementations are already being used and indicate the complexity in establishing legal and policy frameworks for electronic transactions.

### **USE IN ELECTRONIC BUSINESS MODELS**

The use of hybrid technologies in the different business models identified in the general issues chapter (Chapter 1) will vary depending on how the component technologies are linked together.

#### **Open Model**

Hybrid technologies can provide greater security for transactions in open business models. Chained technologies can be used to protect asymmetric public keys through technologies such as shared secrets and biometrics. However it is the asymmetric cryptography element that is actually used in determining the business model. The shared secret or biometric elements of chained technologies are generally under the control of the sender or recipient and do not impact on the business model.

Secured technologies are not generally used in an open model. While an open model technology such as asymmetric cryptography may be used to secure a shared secret or biometric, the other technology has to be established in advance. The establishment of that relationship establishes a closed business model. For example the use of open model asymmetric cryptography to protect a credit card number is not an open business model. First the credit card number in itself is not an authenticator although the additional three-digit authentication number on the back of the card is. Second there is a pre-existing relationship between the credit card holder and issuer and the merchant and the issuer. This makes it a closed business model.

#### **Closed Model**

Hybrid technologies can also provide greater security in closed business models. In the secured technology approach symmetric or asymmetric cryptography can be used to secure shared secrets, and biometrics. The use of symmetric cryptography as the securing technology will generally establish a closed system as there is a need for a prior arrangement to transfer the keys.

Chained technologies can be used to secure authenticators prior to, during or after their transmission. As all the likely individual technologies can be used in closed environments the hybrid can also be used in a closed environment provided the necessary prior arrangements are in place.

#### **Open-But-Bounded Model**

Chained technologies can be used in open-but-bounded business model. Generally this model will involve the use of asymmetric cryptography as the technology used to initiate the protection of the authenticator during transmission. An example of the use of hybrid technologies in an open-but-bounded business model is the use of ATMs in the finance sector. In certain cases a user may use their credit or debit cards issued by Financial Institution A on an ATM operated by Financial Institution B provided there is an agreement between the two financial institutions to do so. The user uses a shared secret (PIN or Password) recognised by Financial Institution A. The shared secret is protected by technology used by Financial Institution B. There is not, however, an agreement between the user and Financial Institution B. The agreement between the financial institutions forms the boundary for this model.

## USER REQUIREMENTS

Hybrid technologies can meet user concerns regarding electronic authentication and improve user confidence in electronic commerce. In secured technologies the extra layer of security can meet user concerns regarding identity theft. One of the more common causes of concern in undertaking electronic commerce is the possible theft of credit card numbers transmitted over the Internet. While a credit card number is a low strength authenticator, it is a common source of identity theft. Misuse of credit card numbers is a common fraudulent activity and in most cases mechanisms are in place to protect the credit card owner. The use of technologies such as symmetric and asymmetric cryptography can reduce the likelihood of their capture and subsequent misuse. Although it is beyond the scope of this report, it should be noted that most thefts of credit card numbers occur from inadequately protected databases. However the securing of the numbers in transit can increase consumer confidence. Consequently hybrid technologies of the type described can meet user requirements.

In chained technologies the inclusion of extra technologies at either the sender or recipient end can improve confidence in the authentication of the transaction. A number of economies have used the UNCITRAL Model Law on Electronic Commerce as the basis for their legislation. The Model Law includes under *Article 7. Signature*:

*Where the law requires a signature of a person, that requirement is met in relation to a data message if:*

*(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message.*

The inclusion of a step to trigger the authenticator, particularly if that step is under the sole control of the sender, can increase certainty that the person indicated their approval of the information in the data message. This is sometimes referred to as 'intention to sign'.

One issue that needs to be addressed is ensuring legal effect for hybrid technologies. In some economies technology specific legislation gives legal effect to the PKI element but not to other elements. In other economies at least partial support for chained technologies is implicit even in technology specific legislation by the incorporation of requirements for users to secure their private keys. An example is the European Union Electronic Signatures Directive requirement for the use of a secure signature creation device.

In some economies legislation giving legal effect to electronic authentication is based on the fact that the method used was reasonable in respect of the transaction. This is generally left to the courts to decide. The added security of both chained and secured technologies can add additional weight to any claim that an authenticator was in fact reasonable.

One of the key requirements for users is that hybrid technologies be seamlessly integrated to facilitate their use. Such integration is generally beyond the capability of individual users. Another factor is that in many cases applications have not been designed to support such integration.

Legal and integration aspects will need to be addressed at both government and industry levels if user requirements are to be addressed.

## CERTIFICATION MODELS

Certification is the process whereby a trusted person binds an individual or entity (including a machine, device or process) to a particular authenticator. In hybrid technologies, that process relates

to an individual authenticator and therefore to a single element of the hybrid process. It is possible for several certification processes to occur when hybrid technologies are used for a single transaction.

### **Formal Certification**

In chained technologies the certification process most commonly involves an ASP formally certifying the public key of the sender. However it is possible for two formal certification processes to be involved. An ASP may certify the public key of the sender while another ASP may certify a Kerberos ticket it issues for the recipient. It is possible for a biometric to be formally certified although this is more likely to occur with secured technologies.

In secured technologies the formal certification process will generally relate to the securing technology. For example, a webserver certificate used to set up a symmetric cryptography session key to protect a password may be formally certified by an ASP. An exception could be where an ASP formally certifies a biometric which may be protected by a securing technology.

### **Informal Certification**

The most common example of informal certification in hybrid technologies relates to the certification of asymmetric public keys. The use of PGP, SDSI or SPKI implementations of asymmetric cryptography in either chained or secured technology are an example of informal certification.

### **No Certification**

It is possible for hybrid technologies to operate without certification in any of the elements. An example would be a VAN which provides secure communications by issuing participants with symmetric keys. Issue of the keys does not involve certification of the user by the VAN operator. The user uses a password for authentication with the recipient. A third party would generally not have certified the password. This is use of a secured technology without certification.

## **TRUST**

The use of hybrid technologies can increase user trust by providing greater assurance that one or more of the following factors applied to the transaction:

- (a) the authenticator was appropriately protected by the sender;
- (b) the authenticator was appropriately protected in transit; and
- (c) the authenticator was properly applied on receipt.

The more factors that apply the higher degree of trust there will be that the transaction has come from the person to whom the authenticator relates.

The use of chained technologies can increase trust by adding elements that satisfy (a), (c) or both. It will not, however, satisfy (b) unless it is combined with a secured technology as part of the chain. The use of secured technologies can increase trust by adding elements that satisfy (b).

There is an assumption that the use of hybrid technologies automatically increases the security, and consequently strength, of the authenticator. This is not always the case. Poor integration of the elements of both chained and secured technologies can negate the added security that may potentially be offered. There is a distinct lack of guidance for users, product manufacturers and system integrators in the implementation of hybrid technologies. Standards, protocols and best practice guides have been developed for a number of the elements that are used to make up hybrid technologies. However, the only examples found of standards or protocols for the integration of those

elements in hybrid technologies, dealt with specific implementations using symmetric or asymmetric cryptography to protect information, including shared secrets and biometrics, during transmission. These include protocols for SSL and standards for electronic funds transfer in the financial institutions sector.

## **LIABILITY**

In addition to the liability issues already identified in respect of the elements that make up a hybrid technology, there are a number of issues arising from the hybridisation process.

The use of hybrid technologies can result in a higher liability for senders in respect of their transactions. The greater assurance that a transaction came from the individual to whom the authenticator is related can increase their liability in respect of transactions using that authenticator. However, the use of hybrid technologies can present problems for senders if they are held liable for transactions for which they are not responsible. If the products being used in the various elements have been supplied by different vendors the user may be required to establish the element that failed as part of the process of establishing liability. Furthermore if a system integrator has been used to integrate the various elements there may be a need to establish its liability.

The use of hybrid technologies can also complicate the liability situation for recipients. If more than one ASP is involved in the hybrid process, the ASP responsible for mis-authentication will need to be determined before liability can be established. As with senders, recipients may also need to establish whose products have failed, to be able to determine liability as a result of the failure.

## **ROLES OF PARTICIPANTS**

As there are a number of technologies involved in the hybrid technology approach, there is an increased number of participants in the authentication process.

With individual technologies senders have a responsibility to protect the authenticator be it a private key, secret key or shared secret. Chained technologies may provide a tool to assist the sender in undertaking that protection. However in some instances the senders still have a role to protect the element under their control. For example if the sender has a key or shared secret protected by storage in a wallet or on a token protected by a PIN or password then the sender still has a role in protecting that PIN or password.

With secured technologies the sender may have a role in ensuring that the securing technology is either appropriately applied or protected. A secret key for symmetric cryptography used to protect a shared secret needs to be protected to the same level as the shared secret. If the sender is relying on session keys generated by SSL then the sender will need to check the webserver certificate to ensure that the authenticator is being sent to the appropriate recipient.

With chained technologies, recipients need to ensure that the elements under their control are appropriately protected and configured. For example a Kerberos ticket server needs to be correctly configured to issue the appropriate ticket for a particular sender. For secured technologies the recipient has a role in ensuring that the securing technology is appropriately applied and protected. If webserver certificates are used for SSL then the recipient has a responsibility to ensure that the private key associated with that certificate is appropriately protected.

Hybrid technologies involve the integration of two or more technologies. In some cases that integration will occur on the sender or recipient's system. In many cases the technical integration will be beyond users' capabilities. They will be reliant on product manufacturers or system integrators to

effect the integration. There is a role for manufacturers and integrators to ensure that the integration does not introduce vulnerabilities. For example if a password wallet and symmetric cryptography applications are integrated as part of a hybrid technology the user needs to be assured that the channel used to carry a password to the encryption application does not allow that password to be compromised. There is also a further role for manufacturers in ensuring the interoperability of the various elements making up a hybrid technology.

Where an authentication service provider provides a service as an element of a hybrid technology process its role will primarily only relate to that element. However, where other elements of the process rely on the element provided, the ASP may have a role in ensuring that the service it provides will support the entire process. For example in secured technologies if a certification authority is providing webserver certificates to authenticate a recipient who in turn is establishing an SSL session to protect a PIN or password, then the ASP has a role in ensuring that the webserver certificate can be validated as part of the process even though the final authentication of the sender does not involve the ASP.

With chained technologies the role of ASPs is integral to the final authentication process. For example if a Kerberos ticket server issues a ticket on the basis of a digital signature validated by an ASP then the ASP process is critical to the final authentication process.

There is a significant role for standards making and protocol development bodies in ensuring that the appropriate standards and protocols are developed for the integration of the various elements of hybrid technologies. These standards or protocols can be used by manufacturers in product development and by accreditation bodies in evaluating the implementation of hybrid technologies.

There is a role for governments in ensuring that electronic transactions using hybrid technologies for authentication are granted legal effect. The fourth APEC Ministerial meeting of the telecommunications and information industry adopted a Programme of Action<sup>3</sup> that included the following points proposed by the then Electronic Authentication Task Group (now the eSecurity Task Group):

*There is a variety of business models, authentication technologies, and implementations of electronic commerce. There should be free choice of these models, technologies and implementations.*

*It should be recognised that in authenticating an electronic transaction multiple technologies may be used.*

*When developing legal and policy frameworks, consideration should be given to the role of multiple technologies.*

*Legal and policy frameworks that focus on specific technologies can impede the use of multiple technologies.*

Implementation of these points within APEC and internationally has been inconsistent. This issue is discussed further in the legal issues chapter (Chapter 9).

### **INTEROPERABILITY**

Where chained technologies are implemented there is a need for interoperability between consecutive elements of the chain to ensure the transfer of the authenticator. This does not necessarily require that the initial and final elements are interoperable. For example a private key passed from a token to an asymmetric cryptography system to digitally sign a transaction requires the asymmetric cryptography application to be able to accept the key from the token. The recipient's system needs to be able to

---

<sup>3</sup> <http://www.apectelwg.org/apec/are/telminsub02.html>



interpret and validate the digitally signed transaction but the fact that the private key was stored on a token is not relevant to the processing of the transaction. It may, however, be relevant in establishing the degree of trust in the transaction.

With secured technologies it is necessary that both the securing and authentication technologies are interoperable. For example if a biometric is secured by symmetric cryptography then the sender and recipient must both have the same symmetric cryptography algorithm and key, and both must have the same biometric processing application. In addition the recipient must have a previously established template of the biometric.

## **ACCREDITATION**

A number of protection profiles for authentication technologies have been, or are in the process of being, developed as part of the implementation of ISO/IEC 15408 (also known as the ‘common criteria’). These include cryptographic technologies, biometrics and smart cards. These profiles relate to the products and not to their implementation or integration with other authentication technologies. There are not, however, any protection profiles for combining individual elements in hybrid technologies.

Some economies and non-APEC countries have adopted a specification for information security management systems based on ISO/IEC 17799. This would allow accreditation of implementations of hybrid technologies in individual organisations but not of the products themselves.

A number of economies and non-APEC countries have accreditation schemes for certification authorities which may be an element of a hybrid technology approach. In some of these processes there is an implication that users must be provided with the technology to secure their private key. However, as yet, none of these processes specifically focus on the hybrid technology approach.

An exception to the above is in respect of SSL where protocols exist for products which can be used as a securing technology to protect authenticators. However no formal scheme exists for evaluating implementations against that protocol.

## **CULTURAL DIFFERENCES**

The use of hybrid technologies does not generate any specific cultural differences over the cultural differences identified for the individual component technologies.

## **AWARENESS**

While there is some awareness among government, business and users on the use of individual authentication technologies, the same cannot be said about their combined use as hybrid technologies. The exception is SSL where there is significant awareness of its use in securing online transactions including protection of the three-digit authentication code on credit cards. While there is some awareness of the use of asymmetric cryptography to transfer keys for symmetric cryptography, this is generally considered in the context of the confidentiality of message content rather than the protection of an authenticator.

Hybrid technologies are emerging as the most common implementation of authentication and there is a need for governments and product developers to increase the awareness of the community of the role of hybrid technologies. Lack of awareness of hybrid technologies is a major impediment to the early adoption of electronic authentication and consequently electronic commerce.



## **Government Awareness**

Within some governments there is considerable awareness of the use of hybrid technologies in security agencies. However this awareness rarely extends to the legal and policy developers responsible for developing the framework for electronic commerce. In most cases awareness relates to the individual technologies, particularly PKI, rather than the integration of those technologies.

A similar situation exists in inter-governmental organisations such as APEC, OECD and UNCITRAL with most delegates only being aware of the individual authentication technologies. The lack of government and inter-governmental awareness has hampered the development of appropriate frameworks to support the use of hybrid technologies. It also places limitations on governments' abilities to promote community awareness on the use of hybrid technologies.

## **Academic Awareness**

A number of academic research institutions have considerable awareness of the development of hybrid technologies. However this has been slow in finding its way into teaching curriculums. Once this occurs an increase in community awareness can be expected.

## **Business Awareness**

There is some awareness among security professionals and system integrators of the role and use of hybrid technologies. However this awareness does not, in general, extend to business users who may be implementing electronic authentication. Furthermore there is little in the way of literature on hybrid technologies to provide guidance for business users. There are a number of professional bodies and manufacturers' groups but these tend to address individual authentication technologies rather than hybrid technologies.

There are, however, signs that this may be changing. The PKI Forum, an international multi-vendor and end-user alliance, has been addressing the role other technologies can play in conjunction with PKI. They have released papers on the role of smart-cards<sup>4</sup> and biometrics<sup>5</sup> in the context of PKI implementation.

## **Individual User Awareness**

As with business users, there is very little awareness of the role and use of hybrid technologies among individual users. Even more than business users, individual users tend to rely on commercial off-the-shelf products and on product manufacturer and vendor advice when selecting electronic authentication products. As mentioned previously these products and advice are generally technology specific rather than addressing hybrid technologies.

## **LEADERSHIP**

Increased use of hybrid technologies will be facilitated by leadership and sharing of experience by those who have already adopted the approach or support its adoption.

---

4 *PKI Note: Smart Cards*, [http://www.pkiforum.org/pdfs/smartcard-two\\_color.pdf](http://www.pkiforum.org/pdfs/smartcard-two_color.pdf)

5 *PKI Note: Biometrics*, <http://www.pkiforum.org/pdfs/biometricsweb.pdf>

## **Governments**

A number of government agencies have already adopted hybrid technology approaches. Those who have done so can adopt a leadership role by making the general community aware that such approaches are feasible and highlighting the benefits of such approaches. Providing it does not compromise the security of their operations, they can document and publish their experiences.

Governments also have a leadership role in developing and implementing legal and policy frameworks that support the use of hybrid technologies. A number of governments have established electronic authentication advisory bodies or published advice on the use of electronic authentication. That advice can include information on the implementation of hybrid technology approaches.

## **International Organisations**

International organisations, both governmental and business, can provide leadership by recognising the role of hybrid technologies and developing legal and policy frameworks that support their use at the international level. APEC has already achieved such leadership through the ministerial endorsement of its activities in addressing multiple technologies, encouraging economies to support their use and in the development of this report.

## **Business Corporations**

A number of business corporations are already using hybrid technologies often transparently to users. They can provide leadership by publicising the benefits to their clients and partners. Business can also provide leadership by continued implementation of hybrid technologies. There is a role for business associations in promoting the increased security advantages of hybrid technologies among their membership.

## **Users and User Groups**

There is little awareness of the role and use of hybrid technologies among individual users. There is a leadership role for user groups in advising their membership of the increased security advantages of hybrid technologies and how to use such technologies.

## **IT Industry**

There are a number of IT industry groups that can undertake a leadership role in respect of hybrid technologies. Technology specific industry groups can examine the integration of their technologies with other technologies to form hybrid technologies and encourage development of the necessary products. IT industry and IT security groups can provide leadership by encouraging members to develop hybrid technologies and their integration.

## **Academic Institutes**

Academic institutions can provide leadership by undertaking research and development in respect of hybrid technologies.

## Chapter 8

# A brief tutorial on cryptography for the novice<sup>1</sup>

The objective of this tutorial is to provide an introduction to public key related cryptographic technologies to permit a basic understanding of how they are applied to support and enhance e-commerce.

The tutorial will discuss cryptography in the context of the security services with which we are familiar and to which we have grown accustomed in the 'paper world'. This tutorial will introduce their digital equivalents in the context of e-commerce.

In cryptography fundamentals the two main families of cryptography will be covered: symmetric, or secret key cryptography, and asymmetric, or public key cryptography. Certificates and how they are used to protect the integrity of public keys will also be discussed.

We use security services every day in our workplaces and society has established an intricate set of laws and customs surrounding the use of these security services. For example, if we need to identify someone, we ask him or her to appear in person, perhaps with some credentials. Or, he or she is introduced to us by a common acquaintance.

If we need to send a paper document securely, we wrap it in an envelope, a double-envelope, a sealed diplomatic bag, or a strongbox. And, if we need to enforce access to buildings, rooms, facilities, computers or information we do so with locks, keys, combinations and guards.

We verify the integrity of paper documents, by checking their signatures and the handwriting. In certain cases, documents are sealed with wax, stamped, or embossed. Anti-forgery features are used on bank notes and cheques.

In the paper world, we authorise transactions like cheques and purchase orders with a signature.

Non-repudiation is the security service that prevents either the sender or the recipient of a transaction from denying it occurred. We primarily rely on contracts and witnesses to prevent such denials.

To summarise the above, the traditional security services that support commerce in the paper world, and how these services are provided are listed below.

---

<sup>1</sup> The Task Group would like to express its appreciation to Bob Stevens, Communications Security Establishment, Canada, for his work in drafting this chapter.

## Electronic Authentication—issues relating to its selection and use

Identification:	Face-to-face meetings, credentials.
Authentication:	Introductions through mutual acquaintances.
Confidentiality:	Sealed envelopes, locked boxes.
Access Control:	Locks, keys, combinations, and security guards.
Integrity:	Handwriting, signature, hand delivery, notaries.
Authorisation:	Signatures.
Non-repudiation:	Signatures on contracts, witnesses, purchase orders, and receipts.

## THE ELECTRONIC WORLD

Now that we live in a digital world, many of the old paper world mechanisms are not possible:

- We may never get to meet the recipients of our electronic messages.
- All electronic documents look the same—zeroes and ones are eminently forgeable.
- We need new services to replace envelopes, locks and combinations.

Not only do our messages and files need new security mechanisms, but the security mechanisms themselves may require additional security mechanisms. Two main security mechanisms are used to provide the digital equivalents of the paper world security services:

- encryption, and
- digital signature.

Encryption is the process by which plain text data are transformed to conceal their meaning. Encryption is a reversible process effected by using a cryptographic algorithm and key.

Digital signature will be described later—for now, we'll assume it is possible to uniquely mark a document. For those who need it, here is a more formal definition of digital signature:

*Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.*

## SECURITY SERVICES

Below are the common terms used to describe security services and the mechanism that support them in the electronic world:

- digital signature
- identification and authentication
- access control
- non-repudiation
- authorisation
- integrity
- encryption (encipherment)
- confidentiality and privacy
- integrity
- continuity of authentication.

Authentication is defined as those measures designed to provide against fraudulent transmission and imitative communications deception by establishing the validity of transmission, message, station or individual. If a user has a unique signature, then the user should be able to sign a random challenge, and no one else should be able to create a duplicate or forgery of the signature.

Non-repudiation can be achieved by implementing a protocol where a user or a process has to send a signed transaction or acknowledgment. Future attempts to deny the transaction can be refuted by storing the signed transaction and producing it for the dispute resolving authority.

Finally, having the sender seal it with his unique signature can ensure a message's integrity and authenticity.

## **Pervasive Security Services**

Just as the justice, legal, and law enforcement community provides pervasive, or universally enjoyed security services, similar services exist in the digital world. Here is a list of those associated with e-commerce:

- trusted third party
- audit
- key management
- generation, registration
- distribution
- storage, archiving
- update
- revocation, expiry, suspension
- destruction.

Trusted (electronic) third parties are the equivalents of notaries, or judges whose impartiality is widely recognised. Audit is defined as an independent review and examination of system records and activities to assess the adequacy and effectiveness of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. Key management is the administration and use of the generation, registration, certification, de-registration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

## **CRYPTOGRAPHY FUNDAMENTALS**

Cryptography is the discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and prevent its unauthorised use. While it is possible to use analogue processes to perform cryptography, the vast majority of cryptosystems are digital. It is therefore necessary that all data (voice, fax, video, images, messages, files) be in digital form, that is, converted to binary numbers. Cryptography generally takes one or several numbers as an input, performs some sort of calculations on those numbers, and produces another number as the output. A cryptographic algorithm specifies which standardised set of calculations is to be performed. Cryptographic algorithms therefore perform mathematical calculations (permutations, combinations, or transformations) on the data.

In order to achieve the desired level of confidentiality (secrecy), a cryptographic key is used to control the cryptographic computation process. Cryptographic keys are also just numbers that control the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification). Different cryptographic keys produce different mathematical results. Key guessing is a basic form of cryptographic attack.

The chances of guessing keys diminish exponentially as the key size increases. Below is a 64-bit cryptographic key in digital form. It could also be displayed using alphanumeric symbols such as those on modern computer keyboards.

```
1101101110111011
1011101000110000
1100011011010101
0011011011011101
```

**Figure 32: Cryptographic Key**

The desired secrecy to be achieved through encryption is in part dependent on the uniqueness of the cryptographic key used by communicating users. Key lengths are normally expressed as ‘number of bits’. Chances of guessing a 64-bit key are 1:10 000 000 000 000 000 000 for each try. The chance of getting hit by lightning is 1: 9 000 000 000.


There are two fundamental cryptographic techniques:

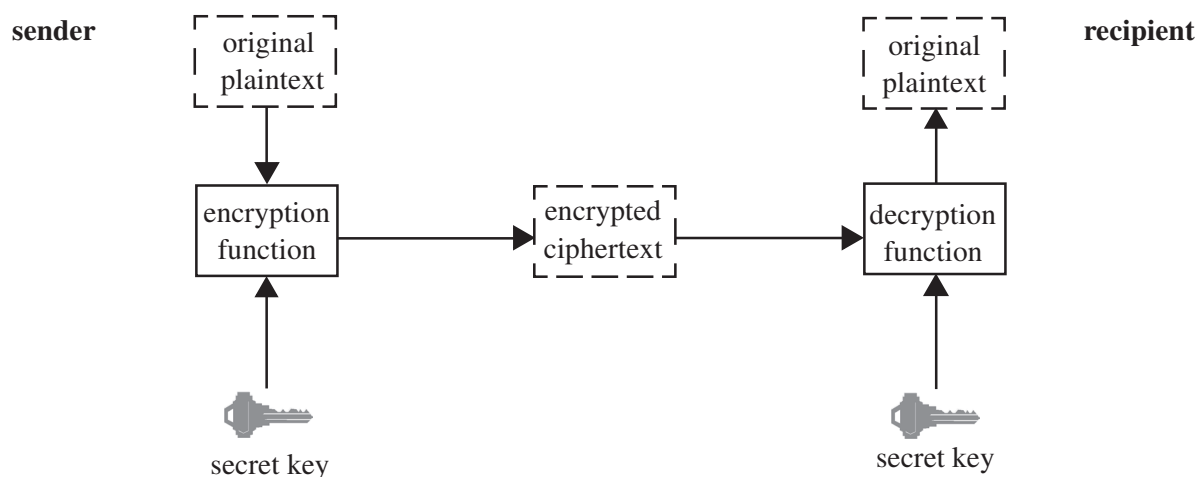
- symmetric cryptography, and
- asymmetric cryptography.

### Symmetric Cryptographic Technique

This cryptographic technique uses the same secret key for both the sender’s and the recipient’s transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the sender’s or the recipient’s transformation. Communicating parties must:

- use the same encryption algorithm,
- use similar implementations,
- use the same key.

The shared key must be kept secret. It is quite possible that two parties using the same algorithm may not inter-operate due to the lack of a shared key or differing implementations of the same algorithm. The following examples use  to represent a key. However, no physical key is involved.



**Figure 33: Symmetric Cryptography**

Remember that the original plaintext is digitised. It is therefore just a number (composed of zeroes and ones). The encryption function enciphers the plaintext by precisely scrambling the plaintext using an agreed algorithm. The encrypted ciphertext is another number, generally the same size as the first (plaintext) number. An observer cannot guess (or decipher) the original number (plaintext) from the ciphertext. Neither can the recipient, unless he has the same secret key that the sender used to create the ciphertext. For now, we'll assume the keys were generated and distributed by magic. (It will become clear that this is expensive magic.)

### Symmetric Key Management

Key management includes the systems, people and processes that are used to request, generate, distribute, store, account for and destroy key material. It is one of those pervasive security services mentioned earlier. There may also be a requirement for archiving key material but this need not be part of the traditional key management process.

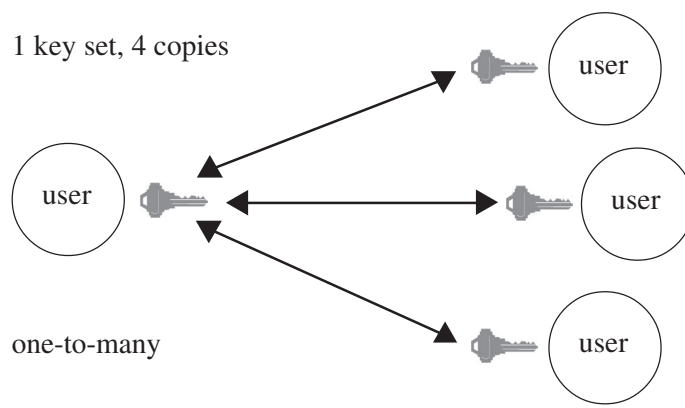


Figure 34: Symmetric Cryptography Key Management (One-to-many)

In the figure above, the user wants to share data with three recipients. The three recipients all share a common key, and can therefore decipher any data sent to any of their peers. The advantage of this is that only one key is required for all four users. The disadvantage of this is that no two of the four users can send a secret that will remain their private secret. Also, if one of the people loses their key, everyone must get a new key.

Below is a depiction of the key distribution to satisfy a situation where four people would want private communications with each other.

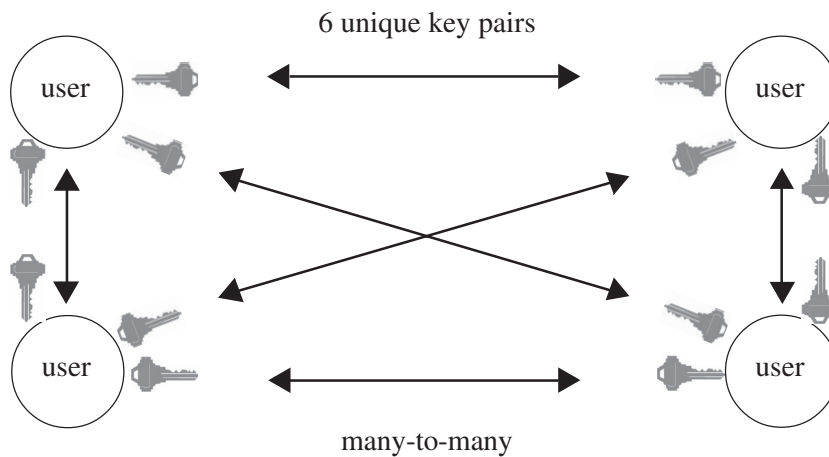


Figure 35: Symmetric Cryptography Key Management (Many-to-many)



Here, each pair of users has its own key. For four users, six keys are needed. In general, for  $n$  users,  $\frac{1}{2} (n(n-1))$  keys are required to give everyone a unique key pair. This quickly becomes unmanageable. Ten thousand users would need almost fifty million:  $\frac{1}{2} (10\,000 \times 9999) = 49\,995\,000$ . Secure distribution is the major challenge, particularly in any global network. So, for large numbers of users, if each pair of users requires a unique key, symmetric key management becomes a complex and very expensive proposition.

Symmetric cryptography is the most common method of encipherment due to its speed and ease of hardware implementation. However, key management costs are typically the highest cost of operating a symmetric cryptosystem. Some security services are not easily implemented. For example, it is difficult to provide a digital signature using only secret keys. An important characteristic of a digital signature is that it be verifiable by a third party. In the case of symmetric algorithms, the argument would be “well, only the two of us knew the key, and I didn’t sign it, so he must have.” Yet this would require revealing the secret key to the third party. Further, since both sender and recipient have the same keys, neither could conclusively prove that the other signed something.

## **ASYMMETRIC CRYPTOGRAPHIC TECHNIQUE**

This is a cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. The following paragraphs will attempt to decipher the meaning of this.

In asymmetric cryptography, two keys are used and form a ‘key pair’. One of the pair is referred to as the ‘public key’, the other as the ‘private key’. Depending on the security service to be delivered, either may be used to perform the initial computation or the reverse computation on data, as will be seen as this portion of the chapter is developed.

The term public key implies that the key is openly available and this is the uniqueness that makes this cryptographic technique more suitable for e-commerce applications. The private key must be kept protected from disclosure hence its name. As with symmetric cryptography, parties must implement the same algorithms and the implementation of the algorithms must be compatible. Each party therefore has at least one key pair associated with itself as a user, one being publicly available, the other kept secret.

A note here on the confusion that has been created by the indiscriminate use of the term public key. Public key cryptography is a phrase commonly used to describe or denote asymmetric cryptography. The two are therefore synonymous unless referring specifically to the public key portion of a public-private key pair.

Encryption, to provide confidentiality (privacy), is done by using the recipient’s public key. While it seems counter-intuitive to use a public key to encrypt data, only the recipient has the private key that is needed to decrypt the data. Public encryption keys are required for the recipient every time someone wishes to encrypt something for that recipient.

Two important points:

- The recipient’s key must be published and highly available (or held locally) or the encryption cannot occur.
- Changes to the public encryption keys must not be allowed, otherwise an attacker could replace a recipient’s public key with his own. The sender would then mistakenly encrypt the message for the hacker instead of for the intended recipient. This latter point will be discussed later in the chapter under certification.

The diagram below depicts encryption with the recipient's public key and decryption with the recipient's private key.

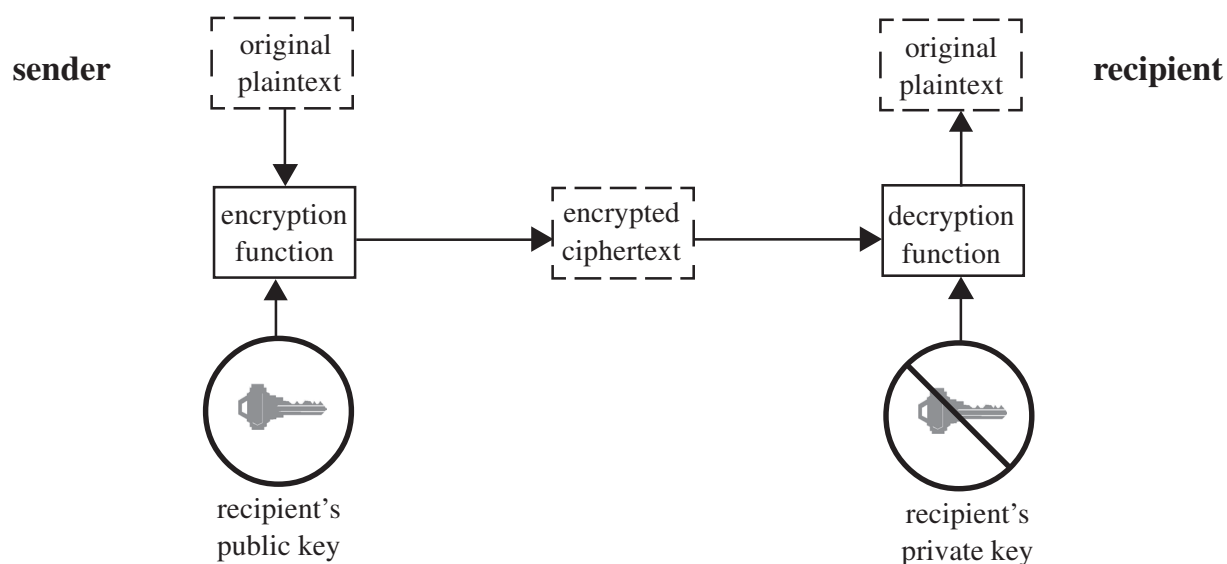


Figure 36: Asymmetric Cryptography (encryption)

### Asymmetric Cryptography Key Management

As previously stated public keys need to be published and protected from modification. Individual users can generate key pairs locally or they may be generated at a central facility. Where key pairs are generated centrally, it is essential that security measures for the generation and distribution of the key pair ensure that only the individual for whom the key pair is generated has access to the private key. It is also normal to have separate encryption and signature key pairs (signature keys will be explained further in the tutorial).

Since each user has a unique key associated with it, the scale of distribution is one to one, one key pair per user. This scale of distribution is much more efficient and cost effective than that for symmetric cryptographic systems when the number of users exceeds certain thresholds. Remember the case for 10 000 users: 50 000 000 keys for a symmetric system versus 10 000 for an asymmetric system. This becomes very important when keys must be revoked or changed for any reason. In the case of symmetric systems, for a closed community of interest, all of the keys are the same therefore all must be changed if there is a compromise. In an asymmetric system, only those compromised need to be changed in most cases. There are specific cases when all must be changed but these are exceptional and even then the one-to-one ratio limits the problem.

Public keys may be published in many different ways: manually distributed (hugely inefficient), printed in phone book style directories, made available on a web server, an ftp site, or on an X.500 directory.

Public keys can be protected from modification by keeping them on super high-assurance systems, however this is very expensive. Instead, they are normally 'certified', that is signed by a certification authority (CA) whose signature all parties trust. More on this topic later.

While at first, it may seem less expensive from a key management perspective to generate keys locally, if key pairs are generated locally by users, at least the public key may still need to be sent to a central location to be certified and returned. For a number of reasons, it may be desirable to have

separate encryption and signature key pairs. Different algorithms and key lengths may be used, and key-handling procedures may be different.

Because the keys are published, and the organisation handing out the keys may not have any way to directly contact the users of the keys, revocation of compromised, expired, and otherwise unusable keys becomes a challenge. Blacklists<sup>2</sup> can be used to meet this requirement. The bottom line is that the one-to-one nature of public key management makes this a very viable technology for large numbers of users. There are some penalties though, because of the long key lengths and computational times associated with asymmetric cryptography as compared to symmetric products and systems.

The security of asymmetric algorithms is based on the difficulty of solving certain mathematical problems. Well-designed asymmetric algorithms can be extremely difficult to break. The calculations performed to conduct asymmetric cryptography tend to be computationally intense. As a result, in general asymmetric cryptographic techniques are slower than symmetric cryptographic techniques. A chosen plaintext attack is an attack where the attacker does not attempt to decipher the ciphertext. Rather, the attacker successively encrypts all possible values of the plaintext and compares his ciphertext with the original ciphertext. This only works when there are relatively few possible values for the plaintext.

## DIGITAL SIGNATURE

A digital signature is not a digitised image of the sender's hand-written signature. It has nothing to do with real signatures. It is a calculation, a number, which when attached to a message or a data packet, can be shown to have been created by one and only one sender. A more formal definition is: *Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.* Encryption can be provided by a number of cryptographic technologies. However, no other technology supports digital signatures as well as asymmetric cryptography. Below is a pictorial representation of a digital signature process.

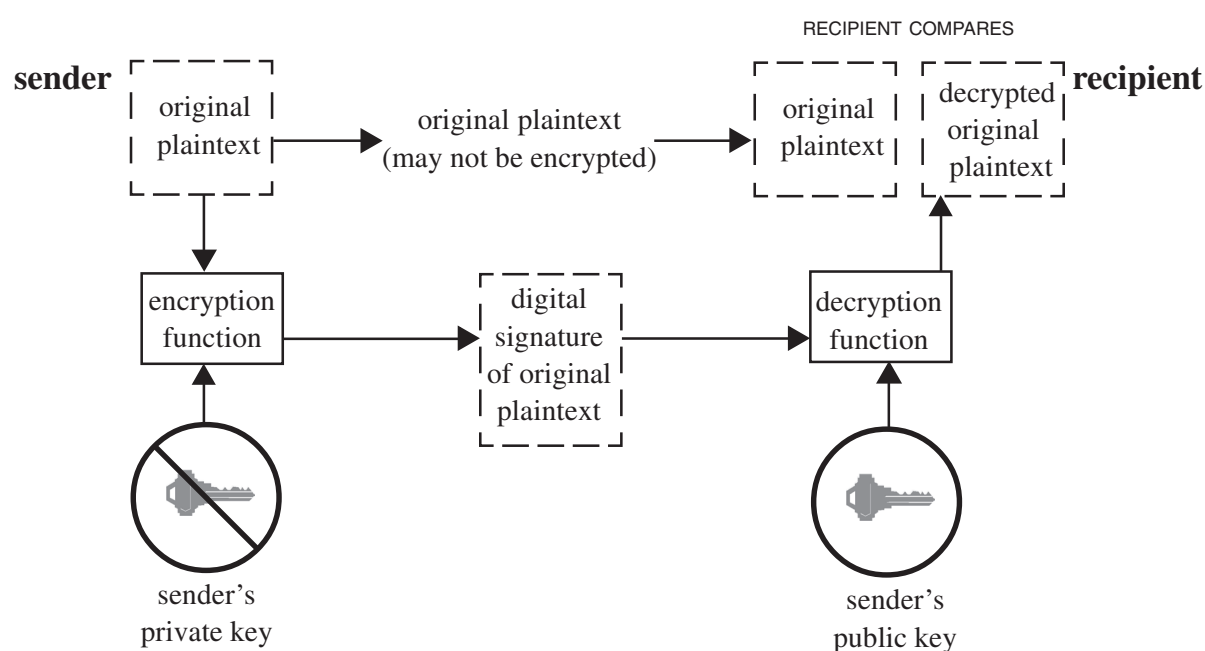


Figure 37: Digital Signature

<sup>2</sup> These lists, generally known as certificate revocation lists, are discussed in more detail in Chapter 2.

Note that for the digital signature, the original plaintext is now encrypted with the sender's private key. Now anyone who has the sender's public key can verify the signature on the message. Note the difference in the use of the public and private keys in that when encrypting to achieve confidentiality the recipient's public key is used to encrypt the message, and only the recipient can decrypt the message. A digital signature is ordinarily the same size as the original message. It is important to realise that the original message must also be sent from sender to recipient so that it can be compared with the signed copy. The original message may not necessarily be protected by a confidentiality service en route.

Since a digital signature is the same size as the message that was signed, we double the size of the message to be transferred. This is one of the potential penalties of using asymmetric cryptography to provide a digital signature. To avoid this, we use a hash function to 'summarise' the message. A hash function has the characteristic that it takes a large input and produces a small, fixed length output. Even minor changes in the input message will cause significant changes in the hash. The hash function must also be a one way function; it should not be possible to guess two input messages whose calculated hashes are the same. If this were possible, an attacker could make up a false message and replace the original message, and the signature would still verify correctly.

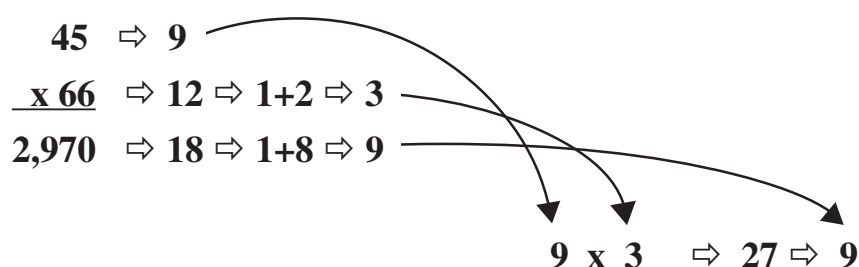


Figure 38: Example of Hash Function

Above is a simple hash function used by accountants for hundreds of years to check their calculations. This simple hash function adds the digits of the input numbers to come up with a hash for each number. If the answer is more than a single digit number, the digits are added again until there is only one digit. To check the calculation, the hash results from the operands on the top of the calculation are combined in the same manner that the operands are—in this case, they are multiplied. If the hash of the results of the real calculation is equal to the results of the multiplication of the hashes, then the calculation was probably correct. Note that in this example there are only nine possibilities for the results of the hash. This makes this a particularly poor choice for a hash algorithm, since one in nine messages will arrive at similar hashes. It would therefore be easy to spoof such a message. Figure 39 is a pictorial representation of a digital signature provided through a hash function.

The figure shows that the original plaintext is sent to the recipient, unchanged. The same hash function is used on both sides to calculate a hash of the original message. The sender signs this hash with his private key, and the recipient uses the sender's public key to verify the signature on the hash. If the signed copy of the hash is identical to the hash that the recipient calculates for himself, then he knows the message has not been changed, and he can be sure that it came from the sender.

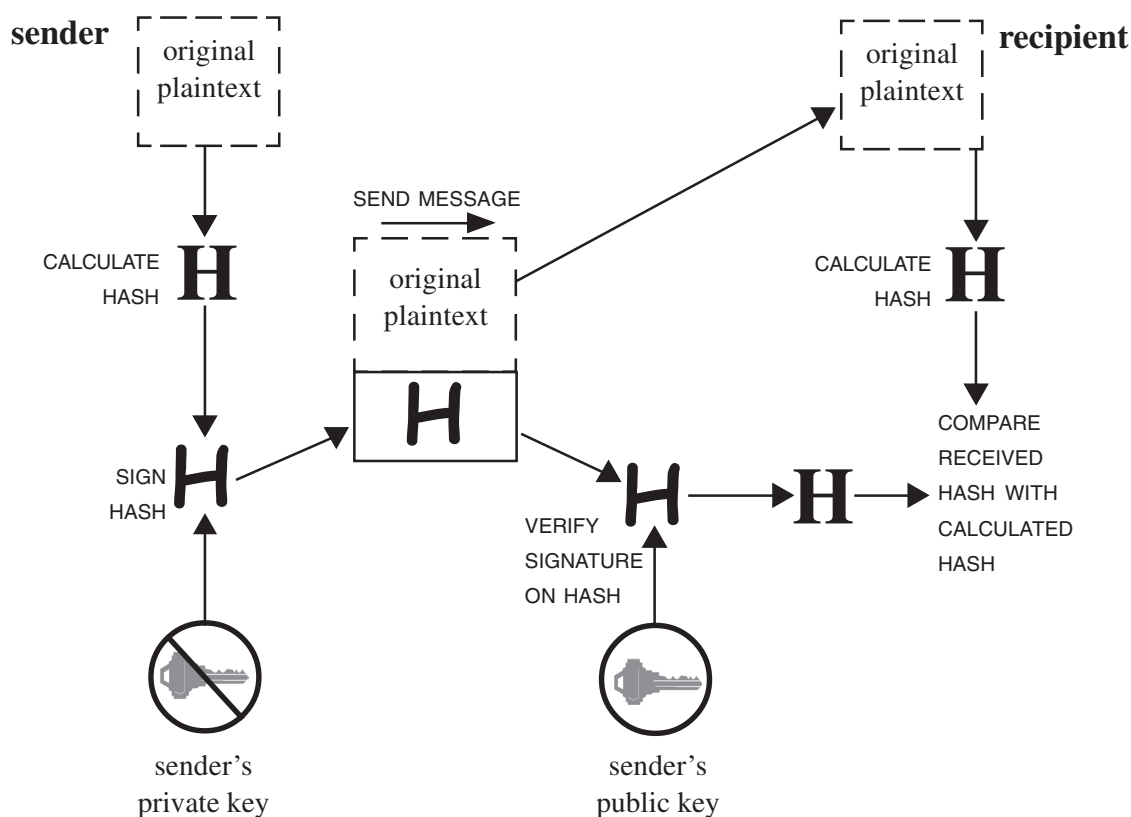


Figure 39 : Digital Signature Using Hash Function

## CERTIFICATES

A certificate in the sense of public key system or PKI is essentially a public key that has been signed by a CA. A CA is normally a trusted third party, that is a source that both sender and recipient trust. The issue here is that the CA is trusted to ensure the identification of each user, to post the correct and trusted public key in the certificate and to digitally sign the certificate so that its authenticity and integrity can be validated.

The main rationale for certificates is to protect the integrity of public keys. For the users to trust the signature of the trusted third party, they must have the signature verification key of the trusted third party in their possession. How this key is given to them is part of the initialisation challenge for public key systems. A very important part of a public key is an entry stating the location of the blacklist that would indicate whether this key has been compromised or suspended. The figure below is a pictorial representation of the contents of a typical digital certificate.

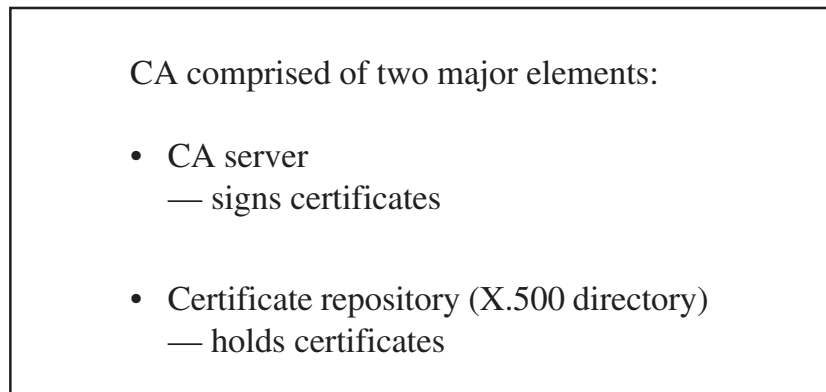
VERSION	
CERTIFICATE SERIAL NUMBER	
SIGNATURE ALGORITHM ID	
ISSUER (CA) x.500 NAME	CERTIFICATION
VALIDITY PERIOD	AUTHORITY
SUBJECT (USER) x.500 NAME	SIGNATURE
PUBLIC KEY	
ISSUER UNIQUE ID	
SUBJECT UNIQUE ID	
EXTENSIONS	

Figure 40: X.509 Version 3 Certificate Format

The important fields here are:

- the signature algorithm ID which tells users which algorithms to use,
- the user's name,
- the user's public key,
- the extensions which can be used to specify how the certificate is used.

The figure below shows the components of a typical CA. There is also a management component associated with a CA which is responsible for the identification and authentication of registered users.



**Figure 41: Certification Authority (CA)**

The CA Server holds a private signing key that corresponds to the CA public verification key held by all users. This key is the most sensitive element in the entire cryptosystem. If the key of the CA server is compromised, then no certificate in the system can be trusted, and all must be recreated from scratch. The X.500 directory is populated by the CA server with user public key certificates. The CA signs all the user public keys in the X.500 server. This reduces the burden placed on the X.500 server to protect the integrity of the keys. If the keys were changed, it could still deny or reduce service to users who needed them, but at least the trust of the public keys would not be compromised.

Electronic Authentication—issues relating to its selection and use



## Chapter 9

# Legal issues

There are a number of legal issues associated with the use of electronic authentication. These include the legal effect of electronic transactions and electronic signatures, liability and privacy which are addressed below.

This chapter does not address the legal frameworks of individual member economies. Information on the legal frameworks of APEC economies and other countries and organisations can be found at the Digital Signature Law Survey<sup>1</sup>.

### INTERNATIONAL LEGAL FRAMEWORK

The United Nations Commission on International Trade Law (UNCITRAL) has adopted model laws on electronic commerce and electronic signatures including guides to the enactment of the model laws. It is currently examining electronic contracting.

### UNCITRAL Model Law on Electronic Commerce

The *UNCITRAL Model Law on Electronic Commerce*<sup>2</sup> contains several articles relating to the use of authentication in electronic commerce. A number of other articles relate to message integrity and are relevant to the use of digital signatures.

#### Authentication

**Article 4—Variation by agreement**—allows parties to select the authentication techniques for transactions between them. This can provide a bridge for transactions between economies that have different rules for electronic authentication.

**Article 7—Signature**—provides that where the law requires a signature, that requirement is met if a method is used that identifies a person and indicates that person's approval of the information contained in the message. Furthermore the method must be as reliable as appropriate for the purpose for which the data message was generated or communicated.

**Article 9—Admissibility and evidential weight of data messages**—provides that nothing in the rules of evidence shall deny admissibility of a data message solely on the grounds that it is a data message; or if it is the best evidence that a person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form. Furthermore data messages shall be given evidential weight

---

1 <http://rechten.kub.nl/simone/ds-lawsu.htm>

2 <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>

taking into account the reliability of the manner in which the data message was generated, stored and communicated; the reliability of the manner in which integrity was maintained; the manner in which its originator was identified; and any other relevant factor. This article relates to both authentication and integrity. The current lack of agreed international standards for the security and implementation of electronic authentication can lead to differing views on what constitutes ‘reliability’<sup>3</sup>.

**Article 13—Attribution of data messages**—provides that a message is deemed to be from the originator if the sender had authority to act for the originator. An addressee is entitled to assume a message is from the originator if the addressee established the originator used a technique previously agreed with the originator or if the message came from someone whose relationship with the originator enabled them access to the agreed procedure. The provision does not apply if the originator advises the message is not from the originator or the addressee should have known it was not from the originator. This has implications in terms of the transfer of authenticators or other means of establishing ‘authority to act’.

### Integrity

**Article 8—Original**—provides that where the law requires information to be presented or retained in its original form that requirement is met if there is a reliable assurance as to the integrity of the information from the time it was first generated in its final form. The integrity requirement does recognise that changes may occur in the normal course of communication, storage and display. Furthermore the information required to be presented must be capable of being displayed to the person to whom it is to be presented. Again, establishing what is meant by reliable is subject to interpretation.

**Article 9—Admissibility and evidential weight of data messages**—provides, as mentioned above, that integrity is an issue in establishing the evidential weight given to a data message.

## UNCITRAL Model Law on Electronic Signatures

The *UNCITRAL Model Law on Electronic Signatures*<sup>4</sup> addresses a number of issues related to the use of types of electronic authentication that meet the requirements of the Model Law.

**Article 3—Equal treatment of signature technologies**—provides that nothing in the Model Law shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature subject to it meeting reliability criteria. While this is a technology neutral approach, one of the reliability provisions relates to the ability to detect message alteration and consequently will exclude some of the technologies outlined in this report from the provisions of the Model Law. In other words the excluded technologies are electronic authenticators but not electronic signatures.

**Article 5—Variation by agreement**—provides that provisions of this law can be derogated from, or their effect varied by agreement, unless that agreement would not be effective under applicable law. This provision has the potential to limit the ability to vary by agreement allowed under Article 5 of the Model Law on Electronic Commerce. Its implementation may inhibit the ability of parties to use agreements to bridge the differences between differing implementations of the Model Law.

**Article 6—Compliance with a requirement for a signature**—provides that where the law requires a signature, that requirement can be met in relation to a data message if an electronic signature is used which was as reliable as was appropriate for the purpose of the data message. Reliability is

<sup>3</sup> This is already apparent with PKI where different economies have established different criteria for assessing their schemes thus indicating different interpretations of what constitutes ‘reliability’.

<sup>4</sup> <http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf>

established if the signature creation data is linked to, and under the control of, the signatory and no other person; if any alteration to the electronic signature after the time of signing is detectable; and if any alteration to data is detectable. As mentioned above this will exclude a number of electronic authentication technologies from the provisions of this model law.

**Article 7—Satisfaction of article 6**—allows countries to make determinations on which electronic signatures satisfy the provisions of Article 6 consistent with recognised international standards. As mentioned above the lack of agreed international standards is a problem in implementing this article and Article 9 of the Model Law on Electronic Commerce. This has been recognised by a number of international organisations including APEC and is the subject of ongoing activity.

**Article 8—Conduct of the signatory**—provides that a signatory shall exercise reasonable care to avoid unauthorised use of its signature creation data and notify any person reasonably expected to rely on the electronic signature in the event of compromise or substantial risk of compromise of the data. Furthermore a signatory shall exercise reasonable care to ensure accuracy and completeness of representations in certificates. A signatory shall be liable for its failures in respect of this article. In some economies this is a legislated requirement while in other economies it is established by contract between the service provider and the person to whom the signature creation data is issued or whose signature creation data is certified.

**Article 9—Conduct of the certification service provider**—provides that a certification service provider for electronic signatures shall

- act in accordance with representations in respect of its policies and practices;
- exercise reasonable care to ensure the accuracy and completeness of representations relevant to the certificate;
- provide reasonably accessible means to relying parties;
- ensure a timely revocation service and utilise trustworthy systems, procedures and human resources.

A certification service provider shall be liable for its failures in respect of this article. This is a factor to be taken into consideration when determining liability of service providers to both subscribers and relying parties.

**Article 10—Trustworthiness**—sets out factors relevant to establishing trustworthiness of certification service providers including financial and human resources, hardware and software systems, procedures for processing certificates and applications for certificates, records retention, availability of information to signatories and relying parties, audit processes and accreditation. These factors need to be taken into consideration in the development of accreditation, assessment or audit processes.

**Article 11—Conduct of the relying party**—sets out the obligations for relying parties to verify the reliability of an electronic signature, or if it is supported by a certificate to verify the validity, suspension or revocation of the certificate and observe the limitations with respect to the certificate. This could impact on the extent of liability of both signatories and certification service providers.

**Article 12—Recognition of foreign certificates and electronic signatures**—provides that geographic location shall not impact on legal effect of an electronic signature. The relevant factor for legal recognition is a substantially equivalent level of reliability to that required in the jurisdiction where legal effect is sought. Relevant international standards shall be regarded when establishing whether there is substantially equivalent reliability. Parties can agree between themselves to use certain types of electronic signatures or certificates. Establishing a ‘substantially equivalent level of reliability’ is the focus of work in a number of international organisations including APEC.

## Hague Conference on Private International Law<sup>5</sup>

The Hague Conference on Private International Law is currently addressing aspects of electronic commerce. Of particular relevance is their work on jurisdiction and dispute resolution which, while directed at broader aspects of electronic commerce, will impact on electronic authentication. The work has not yet been finalised.

## European Commission Directive on Electronic Signatures

The Council of the European Union has adopted a *Directive on a Community framework for electronic signatures*<sup>6</sup>. This will directly impact on those wanting to use electronic authentication for transactions with parties in European Community (EC) and has wider implications extending to global interoperability of electronic authentication schemes.

At the core of the directive are the concepts of a secure-signature-creation device and a qualified certificate. These are defined in the directive.

**Article 3—Market access**—allows provision of certification services without state authorisation. However it requires supervisory processes for issuance of qualified certificates and processes for determination of conformity with secure signature creation devices requirements. Determinations of one member state are to be recognised by other member states.

**Article 4—Internal market principles**—provides that member states cannot restrict provision of certification services originating in another member state and that products complying with the directive are permitted to circulate freely within the internal market.

**Article 5—Legal effect of electronic signatures**—provides that advanced electronic signatures based on qualified certificates and created by a secure-signature-creation-device satisfy legal requirements of signatures and are admissible as evidence. Other electronic signatures are not to be denied legal effect and admissibility in evidence. The definition of electronic signature in the directive is broader than that in the UNCITRAL Model Law on Electronic Signatures and can cover a range of electronic authentication techniques.

**Article 6—Liability**—provides that a certification service provider issuing qualified certificates shall be liable for damage as regards accuracy of information in the certificate, or for any assurance that the signatory holds the corresponding signature creation data, unless it can prove that it didn't act negligently. Certificate service providers may indicate limitations on the use of a qualified certificate in the certificate, and shall not be liable for damages if limitations are exceeded.

**Article 7—International aspects**—provides that member states shall ensure that qualified certificates issued outside the EC are recognised if the service provider has been accredited by a member state, if its certificates are guaranteed by a service provider within the EC that meets the requirements of the directive, or if the service provider is recognised under an agreement with the EC.

To support this process the Internet Engineering Task Force (IETF) has produced RFC 3039 *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*<sup>7</sup>. In addition APEC is working with the European Electronic Signature Standardization Initiative (EESSI)<sup>8</sup> to ensure consistency between their work on electronic signatures.

---

5 <http://www.hcch.net/e/workprog/e-comm.html>

6 [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett)

7 <http://www.ietf.org/rfc/rfc3039.txt?number=3039>

8 <http://www.ict.etsi.fr/eessi/eessi-homepage.htm>

**Article 8—Data protection**—provides that certification service providers shall comply with the provisions of the personal data protection directive. Personal data can only be collected from the data subject or with the explicit consent of the data subject. Use of pseudonyms is permitted.

## **ASSURANCE AND EVIDENCE OF LEGAL EFFECT IN CROSS BORDER TRANSACTIONS**

The eSecurity Task Group was originally established as the Public Key Authentication Task Group to develop PKI interoperability in the Asia Pacific region to facilitate electronic trade and commerce. Key objectives have been to establish interoperability at the legal and policy level and to ensure that users have access to a certificate that can be used for trade and commerce in the Asia Pacific region in particular and internationally in general.

Legal framework, government administration and cultural differences in APEC economies have resulted in differences in approaches to PKI that are currently impeding its implementation. Some of these differences are fundamental and are unlikely to be resolved in the foreseeable future. It is now necessary to look at technical means of bridging those differences. This section addresses existing approaches and how the APEC objective might be achieved. It draws heavily on the work of the PKI Forum<sup>9</sup>, the Internet Engineering Task Force (IETF) PKIX Working Group<sup>10</sup> and some unpublished work of the European Electronic Signature Standardization Initiative<sup>11</sup>. Without that initial work this section would not have been possible.

The basic APEC definition of electronic authentication is: *the means by which the recipient of a transaction or message can make an assessment as to whether to accept or reject that transaction.*<sup>12</sup>

As electronic authentication schemes and legislation have developed, two basic aspects of that definition have emerged:

- trust that the person sending the transaction is the person they claim to be (assurance); and
- whether the transaction has legal effect in the jurisdiction that the sender or receiver wants it to have legal effect (legal effect).

One or both elements may need to be met before a recipient will accept or will be permitted to act or accept the message or transaction.

In PKI, assurance is achieved by the CA issuing a certificate that binds a public key to an individual, organisation, role or attribute. Assurance of that binding can be established through an individual examining the policy and practices of a CA evidenced through documentation such as the certificate policy (CP), certification practice statement (CPS), CA disclosure statement<sup>13</sup> or other documentation provided by the CA. This could include the results of any independent audit of the CA and its practices. Alternatively an individual could rely on the results of a third party assessing the documentation and practices of the CA and determining the level of assurance. The third party could be the individual's CA, an independent assessment scheme or a government licensing or accreditation scheme.

---

9 <http://www.pkiforum.org>

10 <http://www.ietf.org/html.charters/pkix-charter.html>

11 <http://www.ict.etsi.fr/eessi/eessi-homepage.htm>

12 Asia Pacific Economic Cooperation, Telecommunications Working Group, Business Facilitation Steering Group, *Public Key Authentication Task Group Preliminary Report*, September 1997, <http://www.apecsec.org.sg/telewg/16tel/bfsg/matrix/TELEWG-BFSG-3e-2.html>

13 A draft for a PKI Disclosure Statement is at <http://www.verisign.com/repository/pds.txt>

Legal effect can be established through written contractual arrangements between transacting parties or through legislation. In some cases legislation may not permit transacting parties to enter into contractual arrangements regarding electronic signatures. Where contractual arrangements are permitted, the parties can agree on the assurance and legal effect of the PKI scheme and how that is advised. Where legal effect is established through legislation, the requirements to establish legal effect will vary according to how that legislation is framed. In some cases the legal effect is granted, or certain presumptions apply, only where a digital signature and its associated certificate were issued by a CA which is recognised by a regulatory body at the time of the transaction. This is a significant departure from the paper world where once a signature is associated with an individual, that signature generally has effect irrespective of the time when it is used. It is this need to establish legal effect of a signature at the point of time at which each transaction is received that significantly complicates the use of digital signatures.

Three different legislative approaches have been used by governments:

- technology neutral,
- technology specific, and
- two tiered.

The technology neutral approach has been adopted by Australia; Canada; New Zealand and the United States<sup>14</sup>. Under this approach it is left for courts to decide whether an authentication technology was reasonable or appropriate for the transaction. Legal effect is based solely on the level of assurance of the scheme. There is no specific requirement for evidence of legal effect in these jurisdictions. Individuals need to rely on case law to establish whether a particular scheme meets the test of reasonableness. Schemes such as the American Bar Association PKI Assessment Guidelines<sup>15</sup> and Webtrust for CAs<sup>16</sup>, as well as other emerging standards-based-assessment processes such as the Certification Forum of Australasia<sup>17</sup> scheme can assist individuals in assessing whether a particular PKI scheme is likely to meet the test of reasonableness.

However, even in technology neutral jurisdictions, schemes such as the Canadian Government PKI, the Federal Bridge CA (US Government) and Gatekeeper (Australian Government) have implemented approaches for ensuring a particular level of assurance. In these cases there is a need to establish a process to ensure that a particular CA has met the required level of assurance.

The technology specific approach has been adopted by Hong Kong, China; India and Malaysia. Under this approach legal effect is only granted to schemes, generally PKI, that meet the licensing or accreditation requirements specified through the legislation. Individuals will need to know whether a scheme meets the requirements for legal effect in these jurisdictions. Generally the competent authority such as the licensing or accrediting body established under the relevant legislation will test that the level of assurance of a scheme meets the requirements of the legislation. Thus evidence of legal effect also covers level of assurance. Individuals do not need to establish the level of assurance of the scheme.

The two tiered approach has been adopted by the European Union member states; Japan; Korea; Singapore and South Africa. Under this approach general legal effect is given to all electronic authentication schemes but specific legal effect or presumptions attach to those schemes, generally PKI, that meet the requirements specified in the legislation—the top tier. The test of reasonableness

---

14 In the United States different legislative approaches have been adopted at the state and federal level. Which approach takes precedence has yet to be tested.

15 <http://www.abanet.org/scitech/ec/isc/pag/pag.html>

16 <http://www.webtrust.org/certauth.htm>

17 Australasia is a term for Australia and New Zealand



and level of assurance requirement of technology neutral approaches would apply to the lower tier while the evidence of legal effect requirements of technology specific approaches would apply to the top tier.

While much has been spoken and written about business process engineering, the basic principles of the paper world now apply in the electronic environment. Contracts are still formed and need to meet the legal requirements in the appropriate jurisdiction or jurisdictions. This could be the sender's jurisdiction, the recipient's jurisdiction or both. In some cases, as in the paper world, a third jurisdiction is nominated as the jurisdiction whose laws apply to the contract. Businesses can use lawyers to examine the laws of the appropriate jurisdiction, however they need to know whether the scheme supporting the transaction was recognised or had legal effect in the appropriate jurisdiction at the time of the transaction. A further factor is that a CA may be located in yet another jurisdiction. Again legal effect has to be established in the appropriate jurisdiction.

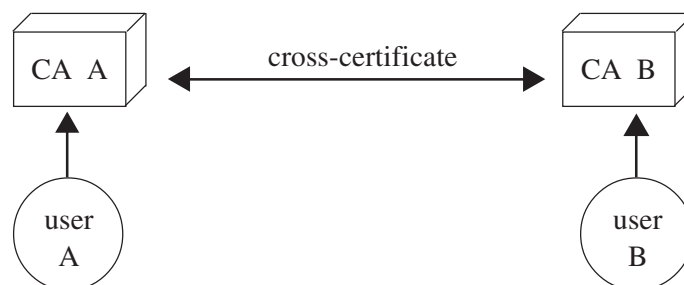
In March 2001 the PKI Forum issued a discussion paper<sup>18</sup> which primarily addressed inter-domain interoperability. The paper identified seven basic approaches to interoperability:

- cross-certification,
- bridge CA,
- cross-recognition,
- certificate trust lists,
- accreditation certificate,
- strict hierarchy, and
- delegated path discovery and validation.

These approaches are not mutually exclusive. A number were developed as a means of establishing a trust relationship similar to establishing a level of assurance. In most, but not all, cases the approaches were not developed to evidence legal effect in the jurisdiction which is only a recently emerging concept in the electronic authentication debate.

### Cross-certification

Cross-certification is the process where one CA issues a certificate to another CA following a mapping of the respective policies and practices to ensure an equal or higher standard of certificate. The process can be unidirectional (the technical term is unilateral but this has caused some confusion among policy makers who assume that only one party is involved in the decision and this is not always the case) or bi-directional (bilateral). Where one CA is operating at a higher level than the second CA the cross-certificate would be unidirectional.



**Figure 42: Cross-certification**

<sup>18</sup> PKI Forum Technical Work Group, *CA-CA Interoperability Project Discussion Paper*, [http://www.pkiforum.org/pdfs/ca-ca\\_interop.pdf](http://www.pkiforum.org/pdfs/ca-ca_interop.pdf)



The process of cross-certification is well established and potentially simple to implement technically. The approach requires the mapping exercise to be conducted with each CA with which a relationship is to be established. It also requires a relationship between the sender and relying parties' CAs. If a third jurisdiction is involved it further requires a relationship with a CA in that jurisdiction.

The approach can establish assurance. Where legal effect is dependent on recognition or licensing, a cross-certificate from a CA established for licensing in the relevant jurisdiction can evidence that legal effect.

### Bridge CA

The bridge CA concept was developed to reduce the number of cross-certification mappings required for a CA to operate with a number of other CAs. Each CA cross-certifies with the bridge CA. This removes the requirement for individual cross-certification by CAs under the bridge CA. The bridge CA can itself cross-certify with other bridge or root CAs.

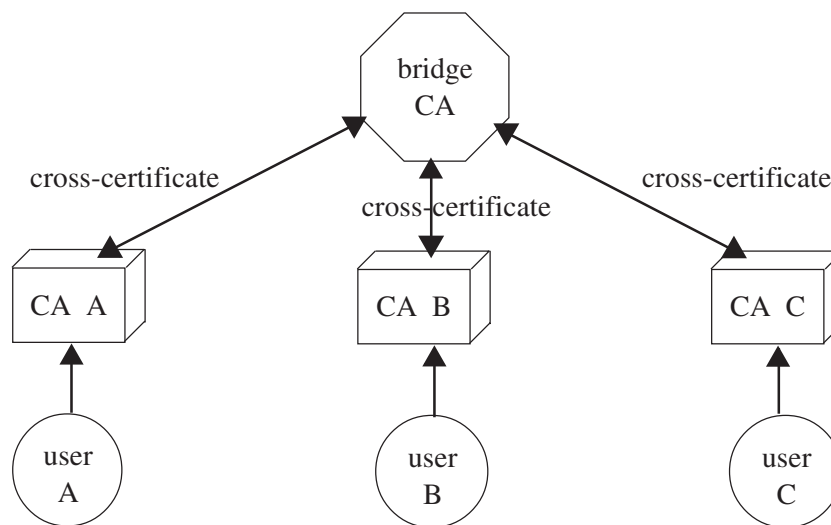


Figure 43: Bridge Certification Authority

The cross-certification process used by a bridge CA can establish assurance. Furthermore if a bridge CA is established as part of a licensing or accreditation scheme to give legal effect, or has cross-certified with a CA or bridge CA established for that purpose it can provide evidence of legal effect. The approach requires a relationship between the sender and relying parties' CAs. If a third jurisdiction is involved it further requires a relationship with a CA in that jurisdiction.

### Cross-recognition

Cross-recognition is an approach developed by the PKI Interoperability Expert Group and discussed in Chapter 3. The approach was developed to address the situation where there was not a relationship between the relying party and sender's CAs. It also transfers the decision to accept a transaction to the relying party rather than the relying parties CA. (See figure 44.)

The means of implementing cross-recognition was not discussed in the original paper outlining this approach. Assurance and legal effect can be established through cross-certificates (unidirectional or bi-directional), accreditation certificates, trust lists or even statements such as a list of CAs on a website. The level of assurance or weight of evidence of legal effect will depend on the particular approach.

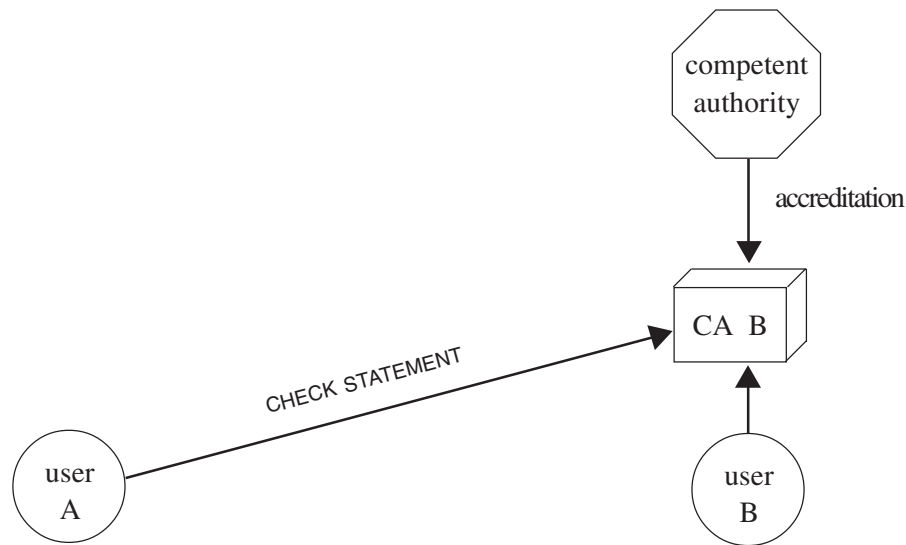


Figure 44: Cross-recognition

### Certificate Trust Lists

The trust list approach has been utilised in browsers for some time through lists of CAs whose certificates can be trusted. However current implementations are relatively insecure as there is no mechanism to ensure that invalid entries cannot be imported into a trust list. This can be overcome by developing an approach that allows the trust lists to be signed by a competent authority. There are examples of trust lists being signed and published by users of PGP. The trust lists can either be downloaded and imported into browsers or accessed through online means such as the Online Certificate Status Protocol (OCSP) or the Simple Certificate Validation Protocol (SCVP). The problem is for users to identify the particular trust list or lists relevant to a transaction. A further problem is that the trust list for the CA and the CRL or status information for an individual certificate are likely to be in different locations, thereby complicating processing and adding additional bandwidth requirements. The advantage is that the approach does not require a relationship between the sending and relying parties' CAs nor with the relevant CA in a third jurisdiction.

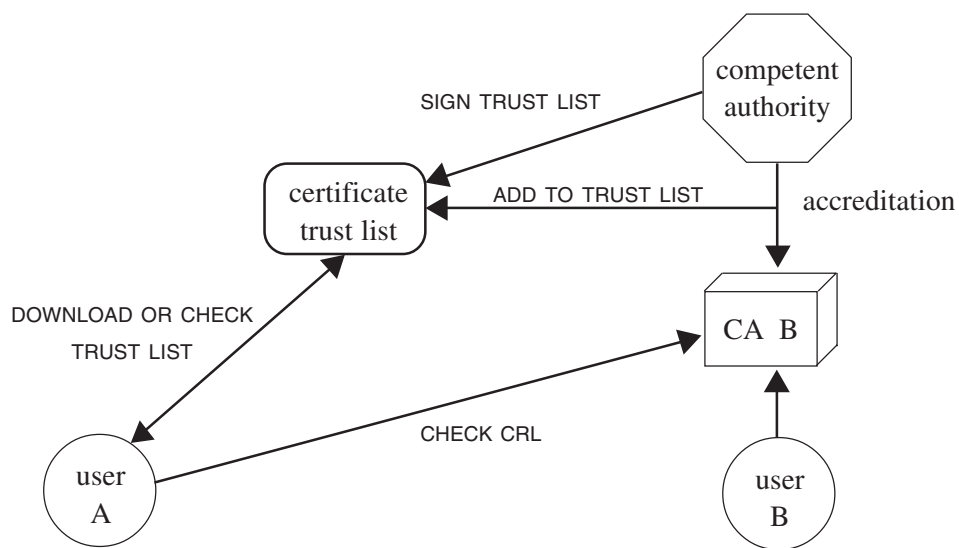


Figure 45: Certificate Trust List

The trust list and check of CRL or status information can establish assurance. If the trust list is generated and signed by a competent authority that is part of a licensing or accreditation scheme to give legal effect it can provide evidence of that legal effect. Downloading a trust list runs the risk that a certificate may not have the assurance or legal effect at the time of the transaction.

The trust list approach will require further examination of the costs and benefits.

### Accreditation Certificate

The concept of an electronic accreditation certificate has been developed by the Australian Government Gatekeeper scheme<sup>19</sup>. Under that approach, an electronic accreditation certificate is issued by a CA established under Gatekeeper for that purpose. While there are similarities between a CA issuing accreditation certificates and a root CA in an hierarchical scheme there are two fundamental differences.

First the accreditation certificate approach does not have a CP and CPS with which an accredited CA must comply. Accredited CAs can be root CAs for their own schemes. The approach focuses on ensuring that a certificate issued by an accredited CA meets a predetermined level of assurance. The approach could also be used for licensing where this is required under a legislative approach.

The second difference is that the approach does not preclude the accredited CA being subordinate to another CA or scheme. As multinational schemes emerge, it is important that a particular CA has the ability to meet both the requirements of the superior CA of the multinational scheme and the requirements of schemes in particular jurisdictions where these requirements are compatible.

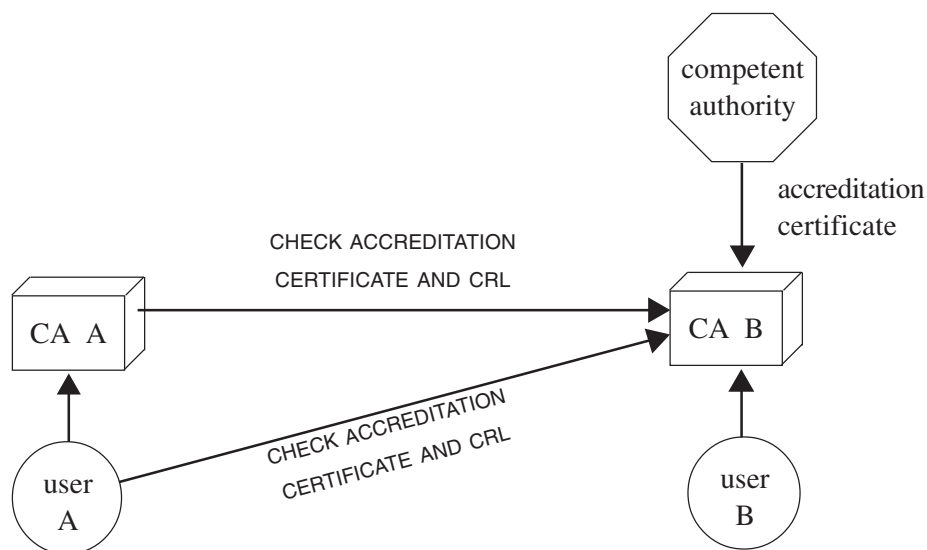


Figure 46: Accreditation Certificate

An accreditation certificate can be used as a unidirectional cross-certificate by an accredited CA providing assurance and, where the accrediting body is part of a licensing or accreditation scheme to give legal effect, it can provide evidence of that legal effect.

19 <http://www.govonline.gov.au/projects/publickey/gac.htm>

## Strict Hierarchy

The concept of strict hierarchy was part of the original development of PKI. In some quarters there was a view that there would be a single world hierarchy with a single international root. The single international hierarchy approach has now been discarded.

The hierarchical approach requires subordinate CAs to comply with the CP and CPS of the root CA. As the level of assurance required varies from scheme to scheme this requirement is no longer considered appropriate. A number of multinational schemes have been developed that provide a hierarchical approach for particular industry sectors, in some cases including other sectors with which they wish to interoperate.

The hierarchical approach can allow the root CA to interoperate as can any other CA under the approaches discussed in this section.

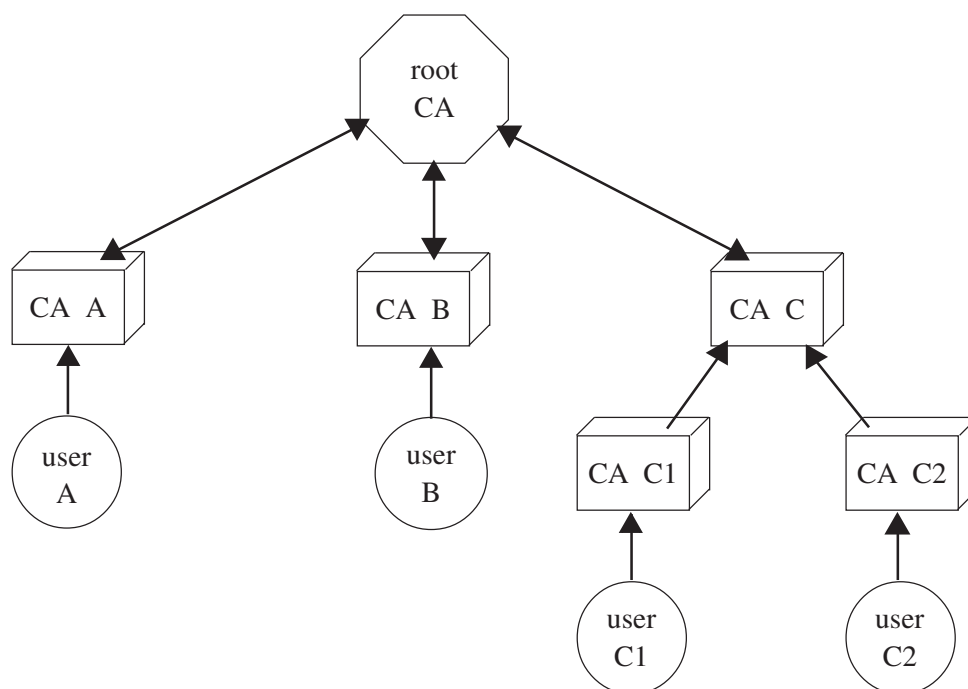


Figure 47: Strict Hierarchy

As all certificates track back through a structure of CAs to the root CA this approach can provide assurance. Where the root CA is part of a licensing or accreditation scheme to give legal effect it can provide evidence of that legal effect.

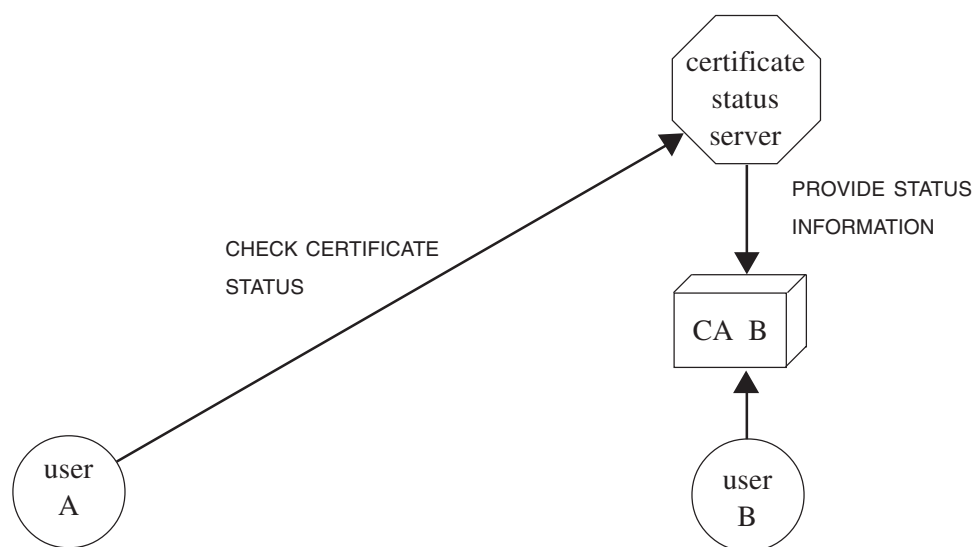
## Delegated Path Discovery and Validation<sup>20, 21, 22</sup>

Delegated path validation was developed to allow for checking of individual certificates. In many respects a certificate status server performs a similar role to a certificate trust list. Options under OCSP allow for responses to be signed. SCVP is less developed but appears to allow tracking beyond the server. SCVP also allows for responses to be signed.

20 Internet Engineering Task Force, PKIX Working Group. *Delegated Path Validation and Delegated Path Discovery Protocols*; <http://www.imc.org/draft-ietf-pkix-dpv-dpd>

21 Internet Engineering Task Force, PKIX Working Group. *Online Certificate Status Protocol, version 2*, <http://www.imc.org/draft-ietf-pkix-ocspv2>

22 Internet Engineering Task Force, PKIX Working Group. *Simple Certificate Validation Protocol*, <http://www.imc.org/draft-ietf-pkix-scvp>



**Figure 48: Delegated Path Discovery**

It is feasible that a certificate status server could be established specifically for the purpose of providing information on the status of CAs that meet requirements for assurance or legal effect in a particular jurisdiction. This could be achieved by storing the certificates of recognised CAs on a server operated by the competent authority in the relevant jurisdiction. The overhead for the user would be diminished if a protocol such as SCVP could be further developed to allow that server to refer the status request for an individual certificate back to the issuing CA or to another certificate status server, to check current validity and return the results to the relying party. The approach may be able to build on existing schemes whereby directories of cross-certificates or accreditation certificates could carry out the role of a certificate status server.

Because of liability implications, the response may need to be in two parts. The competent authority confirms that certificates issued by the sender's CA are legally recognised in that particular jurisdiction, while the issuing CA confirms that the certificate is valid. In other words, legal effect is established by the competent authority and assurance is provided by the issuing CA.

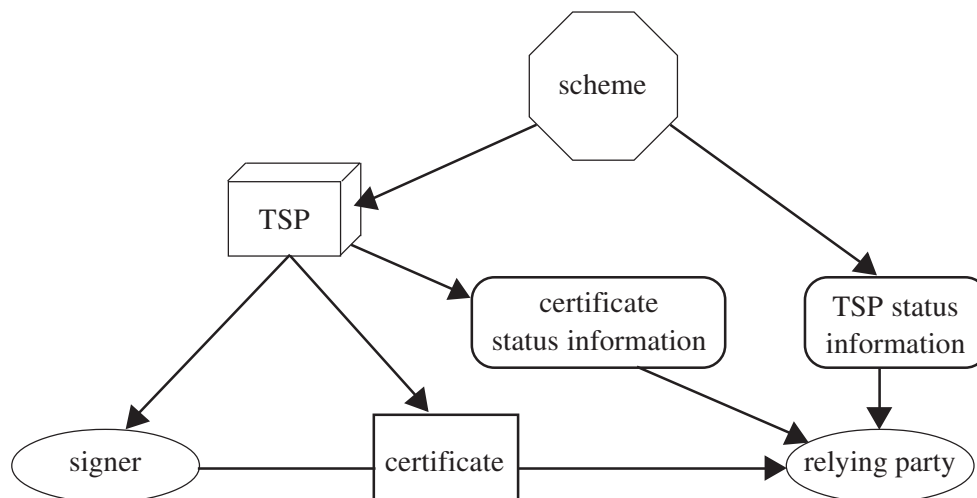
In many aspects this is similar to the role carried out by validation authorities. If a VA were to provide information on both assurance and legal effect by storing relevant directories of certificates, CRLs and accreditation information, the assurance and legal effect could be available from a single source. This would add value significantly.

### Harmonised Trust Service Provider Status Information

The European Electronic Signatures Standards Initiative has produced a technical report *Provision of harmonized Trust Service Provider status information*<sup>23</sup>.

The report outlines an approach to allow relying parties to access information on whether a trust service provider was operating under the approval of a recognised scheme at the time it provided its services. This would state whether the trust service provider was recognised as issuing qualified certificates. The approach is similar to the certificate trust list approach discussed above. The status information could include an indication of the legal as well as trust status.

<sup>23</sup> [http://portal.etsi.org/sec/el-sign.asp#TR\\_102\\_030](http://portal.etsi.org/sec/el-sign.asp#TR_102_030)



**Figure 49: Provision of Trust Status Information**

The technical report goes a step further and suggests the format for the provision of the information.

In summary the cross-certification, bridge CA and hierarchical approaches will not work where there is not a direct or chained relationship between the sending and relying parties' CAs. The other approaches do not require this relationship.

Where the relationship does not exist the development of SCVP and signed certificate trust lists could address this issue. Whichever approach is adopted any application will need to allow the relying party to nominate the jurisdiction that they wish to check. Further work is required in this area and APEC economies have a role to play in that development.

However, regardless of the particular approach adopted, there is a requirement for a jurisdiction to examine the level of assurance of schemes in other jurisdictions. This may involve examination of the CP and CPS of a root or bridge CA or of individual CAs. Alternatively it may involve examination of the assessment, accreditation or licensing processes. As noted in the PKI Interoperability Expert Group mapping exercise, the lack of accepted international standards, particularly for the CA as opposed to the products used by the CA, is hampering the examination of foreign schemes. APEC economies have a role to play in promoting the development of these standards.

## LIABILITY

There are a number of liability issues that need to be addressed. These include:

- liability of the user for misuse of their authenticator, including failure to adequately protect the authenticator from misuse;
- liability of an authentication service provider in certifying the holder of an authenticator;
- liability of an authentication service provider for losses incurred through failure to provide a service or for negligence or misfeasance in providing a service.

There have been some suggestions that liability should be addressed through legislation. Others feel that contractual arrangements would suffice although there is a contract privity problem involved where the relying party has no prior contractual arrangement with either the user or the user's authentication service provider.

The contract privity problem has existed in aspects of international trade for centuries. While the scale of electronic commerce will increase dramatically with the uptake of the new technology, existing approaches to international trade may, in the short term, be able to handle problems that arise.

The OECD addressed these issues as they relate to cryptographic authenticators in the Liability Principle of its Cryptography Policy Guidelines.

7. *LIABILITY*

*WHETHER ESTABLISHED BY CONTRACT OR LEGISLATION, THE LIABILITY OF INDIVIDUALS AND ENTITIES THAT OFFER CRYPTOGRAPHIC SERVICES OR HOLD OR ACCESS CRYPTOGRAPHIC KEYS SHOULD BE CLEARLY STATED.*

*The liability of any individual or entity, including a government entity, that offers cryptographic services or holds or has access to cryptographic keys, should be made clear by contract or where appropriate by national legislation or international agreement. The liability of users for misuse of their own keys should also be made clear. A keyholder should not be held liable for providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful access should be liable for misuse of cryptographic keys or plaintext that it has obtained.*

This principle could be extended to any authentication scheme in which case the thrust of the principle would be that contracts or legislation can be used to establish the liability of users, relying parties or authentication service providers. However this principle does not address the contract privity problem between service providers and relying parties either.

In some cases, governments have intervened to set limits on liability in the debit and credit card field as a consumer protection issue. At this stage this does not appear to have occurred in respect of general online activities. The OECD has issued Guidelines for Consumer Protection in the Context of Electronic Commerce<sup>24</sup> which include the following guideline:

*Businesses engaged in electronic commerce should provide sufficient information about the terms, conditions and costs associated with a transaction to enable consumers to make an informed decision about whether to enter into the transaction.*

While the guideline refers to a transaction, it would also include the use of authentication in that transaction. It could also be reasonably extended to apply to an electronic authenticator used in multiple transactions by a consumer with a particular business. In other words business should provide information on the terms and conditions associated with the authentication of electronic transactions.

Under the guideline on payment systems, the guidelines go on to include:

*Limitations of liability for unauthorised or fraudulent use of payment systems, and chargeback mechanisms offer powerful tools to enhance consumer confidence and their development and use should be encouraged in the context of electronic commerce*

This again could logically be extended to cover limitations of liability for the authentication related to a transaction as well as a payment system in the consumer environment.

In addition to the OECD principle, UNCITRAL has addressed the requirements for the conduct of signatories, relying parties and certification service providers in its Model Law on Electronic Signatures. The articles hold the parties liable for their failure to meet the specified requirements.

The European Commission Directive on Electronic Signatures requires member states to ensure that certification service providers are liable for damage caused to parties who rely on their certificates in specified circumstances unless the certification service provider can prove that it has not acted negligently.

---

<sup>24</sup> Organisation for Economic Cooperation and Development, *Guidelines for Consumer Protection in the Context of Electronic Commerce*, 9 December 1999, [http://www.oecd.org/dsti/sti/it/consumer/prod/CPGuidelines\\_final.pdf](http://www.oecd.org/dsti/sti/it/consumer/prod/CPGuidelines_final.pdf)



While liability can be clearly established between a user and its authentication service provider through the contact terms and conditions at the time an authenticator is issued or received, this does not assist the recipients in establishing liability if they rely on an authenticator. While it would be impractical to include all terms and conditions with an authenticator to allow the recipient to make a judgement, it may be possible to develop a series of model terms and conditions<sup>25</sup> which could be referenced with the authenticator.

There is also the question of whether governments should limit liability to encourage the establishment of authentication service providers. The counter argument is that limiting liability may discourage electronic transactions of a value above the legislated liability limit. In these cases it may be necessary to allow users, recipients and authentication service providers to negotiate a contract incorporating liability greater than the statutory limit possibly based on a higher fee. Limiting liability may also discourage rigorous adoption of standards by authentication service providers and detract from the trust and certainty sought to be achieved by authentication schemes.

Decisions as to whether to adopt a contractual or legislative approach will be a matter for individual jurisdictions. However, when considering which approach to adopt, jurisdictions need to take into consideration that other jurisdictions may take the other approach and make appropriate provisions for accommodating the differences.

### PRIVACY

A significant issue for individual users is the privacy of their personal information provided as part of an electronic authentication process. In a number of economies the protection of personal data is mandated in either electronic transactions or data protection legislation. In general the legislation is based on the *OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data*. The Guidelines and other OECD material on privacy in the electronic environment are available at the OECD website<sup>26</sup>.

The Council of the European Union has adopted *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*<sup>27</sup>. Chapter IV of the directive covers the transfer of personal data to third countries. Where electronic authenticators are sent from European Union member countries to APEC economies, the provisions of the directive may apply. Economies will need to take this into consideration when developing their electronic authentication frameworks.

A number of privacy groups have expressed concerns regarding the use of electronic authentication. While recognising the privacy enhancing capabilities the technologies offer, they are concerned that implementations without adequate privacy protection will adversely impact on individuals.

There is a concern that electronic authentication is being used in the electronic environment for transactions where authentication is not required in the physical or paper environment. In many transactions the fact that a payment has been made is more important than who has made that payment. In other cases authentication of membership of a community is more important than authentication of individual identity within that community. System designers will need to ensure that their schemes do not include excessive authentication requirements.

---

25 The Certification Services Agreements Work Group of the American Bar Association is currently working on such model terms and conditions <http://www.abanet.org/scitech/ec/isc/workgroups.html>

26 [http://www.oecd.org/EN/about\\_further\\_page/0,,EN-about\\_further\\_page-43-nodirectorate-no-no-13-no-no-1,00.html](http://www.oecd.org/EN/about_further_page/0,,EN-about_further_page-43-nodirectorate-no-no-13-no-no-1,00.html)

27 [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett)

Another concern is that association of authenticators and transactions can allow the building of profiles of individual's activities. This is of particular concern in economies where a single authenticator is mandated for individuals. Measures to prevent the consolidation of transaction data can address this issue.

In a number of economies there is not community support for single national identifiers. Individual identifiers are used for specific purposes. There is concern that the introduction of electronic authentication can result in the adoption of electronic national identifiers. Most of these economies have adopted technology neutral approaches to electronic transactions and do not regulate electronic authentication giving individuals the opportunity to use multiple authenticators. Where single national identifiers are not used in the physical or paper world, policy makers need to ensure that they are not created in the electronic world through inappropriate electronic authentication requirements.

A major concern is the security of data supplied in the authentication process. That data could have been provided to an authentication service provider or to the recipient of an authenticated transaction. The recipients of personal data need to ensure that appropriate security measures are in place to protect that data. Where an authentication service provider publishes information as part of its services they need to ensure that the person to whom that data relates is aware that it will be published and has given informed consent to that publication. This should be included in the agreement between the individual and the service provider.

It could be argued that by using an authenticator, the individual to whom that authenticator relates has consented to the transfer of the personal data involved. This is not necessarily the case. Individuals may not be aware of what information is being transferred and what is done with it on receipt. Authentication service providers need to ensure individuals are aware of the implications of using the authenticators they issue. This should be included in the agreement between the individual and service provider.

Recipients of transactions also need to inform individuals of the use they will make of authentication data as well as how it will be protected. This could be included in the recipients' privacy policy. The OECD has developed a *Privacy Policy Statement Generator*<sup>28</sup> to assist organisations in developing their privacy policies.

## Public Key Infrastructures

Public key infrastructures to support asymmetric cryptography and digital signatures have raised serious concern among privacy groups. Greenleaf and Clarke in their paper *Privacy Implications of Digital Signatures*<sup>29</sup> expressed the concern as:

*Digital signatures represent one of the most explosive clusters of privacy-threatening technologies, motivations and processes that has yet been invented. Enormous care must be invested in the development of digital signature infrastructure, and the parallel development of privacy protections*

It is the public key infrastructures that raise the concerns and not the digital signatures themselves. However it does evidence the concerns among privacy groups.

The Australian Privacy Commissioner expressed the concerns as follows:

*A key issue for the Australian community in the information age is how they can be confident of their privacy while taking advantage of the developments offered in information and*

---

28 <http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm>

29 <http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html>

*communications technology. This is reflected, for example, in recent research into attitudes to privacy conducted by my Office that indicated more than half of all internet users had more concerns about the security of personal information when using the internet.*

*Public key technology (PKT) and its surrounding infrastructure—public key infrastructure (PKI)—is a powerful technology which offers benefits to enhance privacy of individuals. It can, for example, provide confidentiality of online communications, authentication of parties in online transactions, as well as non-repudiation of transactions and message integrity.*

*However, there are privacy risks associated with PKI and these need to be carefully managed.*

As a result the Commissioner developed *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals*<sup>30</sup>. While directed at government agencies, the guidelines are equally applicable for private sector PKIs. The guidelines are:

***Agency Client Choice on the Use of PKI Applications.*** *Agencies should allow their clients to choose whether to use PKI for a particular transaction and to offer them alternative means of service delivery. The alternative need not always be an online alternative. In providing this choice agencies should advise their clients of the privacy risks and advantages associated with their use of PKI and alternative methods for that transaction.*

***Awareness and Education.*** *Agencies and their contracted PKI service providers should cooperate closely to ensure that their clients are fully informed of the proper use of PKI and of the risks and responsibilities associated with the use of PKI, including the secure management of private keys.*

***Privacy Impact Assessments (PIAs).*** *Agencies should undertake a Privacy Impact Assessment before implementing a new PKI system or significantly revising or extending an existing PKI system.*

***Evidence of Identity.*** *When developing PKI applications or contracting with PKI services providers, agencies should ensure that only minimum EOI that is necessary for, or directly related, to the process is collected.*

*In addition, where a client wishes to obtain more than one certificate then the client should be given a range of options including:*

*consenting to use a Gatekeeper certificate of equal or higher value to apply for a new certificate;*

*consenting to the re-use of EOI documentation previously provided by the client; or*

*providing documentation on registration for an additional certificate.*

***Aggregation of Personal Information.*** *In the course of PKI transactions with clients, agencies and their contracted PKI service providers should ensure that no detailed history of client transactions is created or used by the agency or contracted PKI service provider, except to the extent that this is required for system maintenance or evidentiary purposes.*

*Agencies and contracted PKI service providers, should not use PKI transactions to collect personal information that is not necessary, or directly related to, the PKI business transaction.*

***Single or Multiple Certificates.*** *Agencies should allow clients to use more than one certificate, where these are fit for the purpose of the relevant application. Agencies should also recognise certificates they have not issued where these certificates are fit for the purpose of the relevant application.*

---

<sup>30</sup> <http://www.privacy.gov.au/publications/pki.doc>

**Subscriber Generation of Keys.** *Where an agency issues certificates or contracts for their issue, the agency should allow its clients the option of generating their own keys, provided that the agency is satisfied that subscriber key generation can be implemented securely.*

**Public Key Directories.** *Agency clients should be allowed to opt out of including their public keys in a public key directory (PKD) where the PKD is published.*

**Pseudonymity and Anonymity.** *Agencies should provide their clients with anonymous and pseudonymous options for transacting with them, to the extent that this is not inconsistent with the objectives and operation of the relevant online application.*

These guidelines address the major privacy issues raised by the use of PKI. They do not, however, address the use of attribute certificates as their use is still being considered by the Australian Government for its Gatekeeper scheme. Attribute certificates can evidence membership of a community of interest without the need for individual identity certificates and consequently reduce some privacy concerns.

If individual users are to adopt the use of digital signatures within a PKI, implementations will need to incorporate privacy protections similar to those set out above.

## Biometrics

Most of the privacy concerns regarding biometrics have been addressed at their use in the physical world. However a number of the concerns apply equally to the use of biometrics as electronic authenticators. The Electronic Privacy Information Center (EPIC) expressed the concerns as follows<sup>31</sup>:

*There are significant privacy and civil liberties concerns regarding the use of such [biometric] devices that must be addressed before any widespread deployment. Briefly there are six major areas of concern:*

**Storage.** *How is the data stored, centrally or dispersed? How should scanned data be retained?*

**Vulnerability.** *How vulnerable is the data to theft or abuse?*

**Confidence.** *How much of an error factor in the technology's authentication process is acceptable? What are the implications of false positives and false negatives created by a machine?*

**Authenticity.** *What constitutes authentic information? Can that information be tampered with?*

**Linking.** *Will the data gained from scanning be linked with other information about spending habits, etc.? What limits should be placed on the private use (as contrasted to government use) of such technology?*

**Ubiquity.** *What are the implications of having a electronic trail of our every movement if cameras and other devices become commonplace, used on every street corner and every means of transportation?*

The Australian Privacy Commissioner in a paper *Biometrics and Privacy The End of The World as We Know It or The White Knight of Privacy?*<sup>32</sup> noted:

*The task I have as the Privacy Commissioner, along with other Commissioners, is to engage actively with the issue. We need to consider what can be done to protect privacy while still achieving the benefits that biometrics is capable of bringing to society and to individuals.*

---

<sup>31</sup> <http://www.epic.org/privacy/biometrics/>

<sup>32</sup> <http://www.privacy.gov.au/news/speeches/sp80notes.doc>

## Chapter 9. Legal issues

*Indeed, wherever possible, the real objective should be to seek ways of ensuring that biometric technologies achieve these benefits while actually enhancing privacy.*

The development of guidelines such as those developed for PKI could increase user confidence in the use of biometric authenticators which conform with those guidelines.