NATIONAL PUBLIC KEY INFRASTRUCTURE WORKING GROUP

STRATEGIES FOR A PEAK BODY FOR AN AUSTRALIAN NATIONAL ELECTRONIC AUTHENTICATION FRAMEWORK [INCLUDING A PUBLIC KEY AUTHENTICATION FRAMEWORK (PKAF)]

A REPORT PREPARED FOR

THE NATIONAL OFFICE FOR THE INFORMATION ECONOMY

EXECUTIVE SUMMARY

> *"Legislators are faced with unique and fundamental policy choices regarding the role of government in the development of electronic commerce. Recognizing that government must play a role in enabling electronic commerce by removing traditional barriers, nearly every state [in the USA] has sought to eliminate barriers caused by traditional writing and signature requirements by drafting legislation designed to permit the authentication of documents and signatures through electronic means. In the electronic environment, however, the authentication of documents and signatures is considerably more difficult than in the traditional written environment. An original message may be virtually indistinguishable from a copy, and the potential for fraud is heightened by the ease of alteration"*[1]

Introduction

In late 1997, the Commonwealth Government, acting through the National Office for the Information Economy (NOIE), established the National Public Key Infrastructure (NPKI) Working Group to examine issues pertaining to setting up a peak body to oversee the development of a national framework for the authentication of users of online communications services, that would provide:

- a trusted system for the generation of digital signatures to give corresponding parties certainty in each others' identities;
- assurance of the integrity of electronic data used; and
- a means of ensuring non-repudiation of electronic transactions.

Background

The projected importance of the online economy has prompted communities and governments across the globe to examine the crucial issue of the authentication of parties to an online transaction (whether monetary or not).

Electronic authentication raises significant issues in respect of evidence and contract, liability, privacy and consumer protection, and sovereignty and international trade. *Public-key cryptography* offers the strongest forms of electronic authentication currently available, through *digital signatures* and other techniques.

[1] *Survey of State Electronic & Digital Signature Legislative Initiatives* - Internet Law and Policy Forum - 1997 - Authors Albert Gidari and John P. Morgan

A crucial question that arises relates to the role to be played by government in resolving electronic authentication issues particularly in relation to the establishment of *Public Key Infrastructures* (PKI). While governments may have expressed a preference for private sector leadership in such matters, many have recognised the essential facilitating role which they need to play in relation to the provision of an enabling legal/regulatory/policy framework.

Objectives of this Study

This study canvasses whether or not a peak body is required at this point in time, and provides business models and options for the structure, operations and role of a peak body to oversee a national framework if one is required. Other relevant flow-on issues affecting the national framework are also addressed.

Context

Australia's' ability to participate within the global economy is seen to be dependent upon its ability to have a trusted, secure environment to conduct business in the electronic medium.

A national *Public Key Infrastructure* (PKI) therefore needs to contribute solutions to the following issues:

- Privacy - keep information confidential;
- Access control - only allow selected recipients access to the information;
- Integrity - assurance that the information has not been altered;
- Authentication - proof of the originator of the information; and
- Non-repudiation - proof that information was sent by the originator.

The importance of a *national* PKI as opposed to, for instance, industry or community based infrastructures, is partially predicated upon the premise that users of online services will be operating within a national, and possibly international, 'open system'. Increasingly questions are being raised in relation to the viability and desirability of an open system model as opposed to a "closed" model in which certificates are used within a bounded context (eg between government and citizens, or within a payment system). In this "closed" context, legal force can be established, under contract law, by execution of (eg paper-based) agreements beforehand.

Process

This study has involved canvassing the opinions of a wide range of representatives from Commonwealth Government agencies, State and Territory Governments through GTTC representatives, suppliers of certification products and services, and user and other organisations. These views have been synthesised with those of the Working Group and combined with research into the history, current status and trends in relation to similar initiatives internationally. The logistics of producing a report within the short timeframe allowed for the study has meant that inevitably the choice of information included in or excluded from the report, and the editorial style adopted is largely that of the consultants rather than the Working Group.

The Working Group's agreed position is summarised in explicit recommendations.

This study has been undertaken in parallel with a study of the legal issues related to electronic commerce by the Attorney General's Expert Group on Electronic Commerce (AGEGEC). The recommendations of the Working Group are not seen as dependent upon nor in conflict with the preliminary recommendations of the AGEGEC.

Conclusions

Substantial work is being undertaken in relation to electronic authentication by state, federal and supra-national government bodies across the globe as well as fora and think-tanks. The output from this work points to the complexity and multi-dimensionality of the issues to be addressed and the rapidly changing views of the 'problem' and the possible 'solution'. This work will continue to illuminate and clarify the debate, to Australia's benefit. In this uncertain environment all ways forward involve some risk of being deemed inappropriate at some future time. However the Working Group believe that taking no action is similarly risky.

The Working Group recognises that the issue of electronic authentication transcends its implementation through the use of public key cryptography and has therefore adopted the term *Australian National Electronic Authentication Framework* (ANEAF) rather than NPKI where appropriate.

The Working Group concluded that a case exists for the establishment of a peak body to oversee an ANEAF, the key justifications being:

- to promote compatibility;
- to present and represent a single national view;
- to ensure user confidence;
- to provide consumers with reliable information;
- to promote a contestable market for CA services;
- to manage systemic risks;

- to facilitate the provision of value-added services (which rely on a robust PKI);
- to support legislation; and
- to promote export of trust-based services.

The conclusions reached in relation to the role and functions, and form and structure of the peak body are contained within the recommendations below.

Recommendations

Peak Body

The Working Group recommends the immediate establishment of a peak body to oversee the Australian National Electronic Authentication Framework.

The Working Group further recommends that the focus of the peak body should, in the first instance, be to establish a National Public Key Infrastructure under the ANEAF.

The Working Group recommends that the policy aspects of an NPKI peak body be separated from the operational aspects, into an Australian Policy Approval Authority (APAA) and one, or possibly more, Root Certificate Authorities (RCAs), respectively.

It is anticipated that a national RCA will be required as early as the end of 1998. In view of this tight timeframe, it is recommended that the issue of whether and how a national RCA is to be established be addressed by Government as a matter of the highest priority.

APAA Roles and Functions

The Working Group recommends that the APAA functions should be:

a) to facilitate stakeholder involvement;

b) to promote the required level of trust in electronic commerce in Australia;

c) to approve the establishment of any RCA;

d) to represent the ANEAF within the global environment[2];

e) to promulgate appropriate electronic authentication standards in association with Standards Australia and international standards bodies[3];

[2] An additional function to be considered by the APAA for later adoption, is the resolution of cross-certification issues at the RCA level and elsewhere.

[3] It was agreed that these standards were "minimal" in the sense that organisations could choose to exceed the promulgated standard.

f) to approve and oversee the establishment of a national evaluation and accreditation scheme; and

g) to manage systemic risk.

AAPA Operational Model

The Working Group recommends that the operational approach for the APAA should seek to utilise outsourcing to the greatest extent possible. This may be achieved by eg licensing outside organisations to perform eg evaluation functions.

The APAA should determine its policies with a view to minimising the costs of compliance by participating CAs, to the greatest extent consistent with the overall integrity of the ANEAF.

APAA Resourcing

The Working Group recommends that, once the eventual form and functions of the APAA have been decided in principle, a detailed costing of the APAA's operations should be undertaken.

Further, the Working Group recommends that, in the interim, a budget estimate of $1.3 million per annum should be used, independent of the structure selected.

The Working Group recommends that the possibility of the APAA eventually being self-funding should be investigated carefully.

APAA Structure and Form

There was broad support amongst the Working Group for a Government-based APAA.

The Working Group felt that the exact form of constitution of such a body was essentially a legal and political decision.

Thus the Working Group recommends that suitable legal opinion be sought as to the appropriate constitution of the APAA having regard to the following major influencing factors:

- the credibility and standing of the body with consumers and the CA industry;
- the need for a degree of independence;
- liability of the APAA and its board members, and organisations other than the APAA participating in the ANEAF, including any RCA, PCAs and other CAs;
- the need for broad community representation on the APAA.

Further, the Working Group recommends that the need for supporting legislation in respect of the management of liability be monitored.

STRATEGIES FOR A PEAK BODY FOR AN AUSTRALIAN NATIONAL ELECTRONIC AUTHENTICATION FRAMEWORK

TABLE OF CONTENTS

Executive Summary i

Introduction i
Background i
Objectives of this Study ii
Context ii
Process iii
Conclusions iii
Recommendations iv
Peak Body iv
APAA Roles and Functions iv
AAPA Operational Model v
APAA Resourcing v
APAA Structure and Form v

1. Introduction 6

2. Terms of Reference of Working Group 9

3. Background 10

3.1. Identification and User Authentication 10
3.2. Electronic Authentication 10
3.3. Electronic Signatures 11
3.4. Digital Signatures 11
3.5. Public Key Cryptography 12
3.6. Certification Authorities 12
3.7. Public Key Infrastructure 13
3.8. Roles and Functions of a Peak Body (PARRA) as Proposed in the PKAF Strategy Report 13
3.9. Related PKAF Activity 16

4. International Activity and Legal Models 17

4.1. Current Status Relating to PKI Laws and Frameworks 17
4.2. Open and Closed PKI Models 17
4.3. Legislative models 18
4.4. Approaches to the 'Peak Body' 19

5. Case for a National Framework and Peak Body 20

5.1. Three Important Contextual Issues 20
5.1.1. Planning Horizon 20
5.1.2. The Need to Maximise Participation by CAs 21
5.1.3. The Role of Government Facilitation 21
5.2. To Promote Compatibility 23
5.3. To Present and Represent a Single National View 23
5.4. To Ensure Consumer Confidence 23
5.5. To Ensure Market Efficiency 24
5.5.1. To Provide Consumers with Information 24
5.5.2. To Promote a Contestable Market for CA Services 24
5.5.3. To Manage Systemic Risks 25
5.6. To Facilitate the Provision of Value-Added Services 25
5.7. To Support Legislation 26
5.8. To Promote Export of Trust-based Services 27
5.9. To Limit Liability 27

6. Roles and Functions 28

6.1. Options 28
6.2. Arguments 28
6.3. Recommendations 30
6.3.1. Peak Body 30
6.3.2. APAA Roles and Functions 30

7. APAA Operational Model 32

7.1. Operations 32
7.2. Recommendations 33

8. APAA Resourcing 34

8.1. Fully Funded Model - Maximal 34
8.2. (Almost) Virtual Organisation - Minimal 34
8.3. Estimates of Costs 35
8.4. Industry Base 35
8.5. Sources of Funds 35
8.6. Recommendations 36

9. APAA Structure and Form 37

9.1. Accountability 37
9.2. Representation 37
9.3. Trade Practices 38
9.4. Recommendations 38

10. Root Certification Authority 39

10.1. Introduction 39
10.2. Functions 39
10.3. Who should be a RCA 39
10.4. How to ensure broad support for a Government facilitated RCA 40
10.5. Recommendation (already stated in 6.3.1 above) 40

11. Summary of Recommendations 41

11.1. Peak Body 41
11.2. APAA Roles and Functions 41
11.3. AAPA Operational Model 42
11.4. APAA Resourcing 42
11.5. APAA Structure and Form 42

Appendix A: Abbreviations 44

Appendix B: Glossary 46

Appendix C: User Authentication and Cryptography 54

Authentication 54
User Authentication 54
Other forms of Authentication 54
Identification and User Authentication 55
Cryptographic Techniques for User Authentication 55
Challenge and Response Protocols 55
Digital Signatures 56
User Authentication and Locking with Smartcards 56

Appendix D: Public Key Cryptography 57

Cryptographic Security Services 57
Symmetric and Public Key Cryptography 57
Symmetric Cryptography 58
Public-key Cryptography 58
Cryptographic Algorithms 59
Digital Signatures 59
Key Certificates 60
Certification Authorities 61
Registration Authorities 63
Cross-certification 63
Certification Authority Hierarchies 64
Public Key Infrastructure 65

Appendix E: International Approaches to Legislation and Peak Body66

Overview 66
Open' and 'closed' PKI models 66
Legislative models 67
Rule of equivalence 68
Framework of principles 68
Complete, prescriptive law 69
Characteristics of the legislation 70
Technology neutrality 70
Scope of the legislation 70
Definition of a signature 71
Licensing or registration of CAs 71
Issues relating to a peak authority 72
Issues related to liability apportionment 72
Model laws, guidelines and frameworks 72
American Bar Association Digital Signature Guidelines 73
NCCUSL Uniform Commercial Code Article 2B 73
NCCUSL Uniform Electronic Transactions Act 74
UNCITRAL Model Law on Electronic Commerce 1996 74
UNCITRAL Uniform Rules on Digital Signatures and Certification Authorities75
ICC GUIDEC 75
European Commission 76
Enacted or proposed legislation and regulations 76
United States of America 76
Federal 76
States 77
Denmark 79
Germany 79
Italy 80
United Kingdom 80
Japan 81
Malaysia 81
Singapore 82
South Korea 83
Functions and structure of the peak body 84
References 86

Appendix F: Non-legislative PKI initiatives 88

Government 88
United States of America 88
Canada 88
Australia 88
European Commission 88
ICE-TEL 91
IETF/IAB 91

Private enterprise CAs **92**
References **93**

APPENDIX H - Bibliography and Additional Reference Material **94**

General PKI related material **94**
Lists of links **94**
Papers **94**
PKI Projects and Studies **97**
PKI related standards (and standards under development) **97**
Legislation **97**
Summaries **97**
Legislation (enacted and proposed) and related material **97**
Argentina **97**
Germany **98**
Italy **98**
Japan **98**
Malaysia **98**
Singapore **98**
United Kingdom **98**
United States of America **98**
Model Legislation **100**
ABA **100**
FDA **100**
ICC **100**
NCCUSL **100**
UNCITRAL **100**

APPENDIX I - Methodology **101**

Process **101**

APPENDIX J - Consultation **104**

List of Interviewees **104**
Consultation Briefing Document **105**
NPKI —Interview Questions **109**

1. INTRODUCTION

With the increasing trend toward delivery of information and transactions by electronic means, effective authentication methods for electronic interaction are becoming increasingly important. *Public-key cryptography* offers the strongest forms of electronic authentication currently available, through *digital signatures* and other techniques. In support of public-key cryptography, Australia, and many other jurisdictions around the world, are looking to establish *Public Key Infrastructures* (PKI).

The Australian national public key infrastructure (NPKI) initiative is known as the *Public Key Authentication Framework* (PKAF). Support for PKAF has come from a broad range of constituencies. In 1996 Standards Australia published its PKAF Strategy Report[4]. A key recommendation of the report was the formation of a peak body for PKAF, known in that document as the *Policy and Root Registration Authority* (PARRA).

After reviewing the PKAF Strategy Report and substantial further internal and external consultation, the Commonwealth Government, through the Department of Communications and the Arts (DOCA) and the National Office for the Information Economy (NOIE), established the NPKI Working Group in late 1997 to examine issues pertaining to setting up a peak body for PKAF. This report is from that Working Group.

The Working Group members were appointed by the Minister of Communications, the Information Economy and the Arts and consisted of representatives from Commonwealth Government agencies, State and Territory Governments through GTTC[5] representatives, suppliers of certification products and services, and user and other organisations. The members were:

Mr Peter Blanchard	Tradegate ECA
Ms Jenny Clift	Attorney-General's Department (Electronic Commerce Expert Group)
Mr David Hart	Australia Post
Mr David Jonas	ETC Electronic Trading Concepts Pty Ltd (Chairperson)
Mr Peter Maynard	Department of Information Technology Services South Australian Government (GTTC)
Dr Philip McCrea	CSIRO
Mr Charles Moore	Signet Systems (Chair of Standards Australia WG IT 12/4/1)

[4] "*Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia*" (Standards Australia, Miscellaneous Publication MP75, 1996)

[5] Government Technology and Telecommunications Committee - a Commonwealth, State and Territory Government committee.

Mr Geoffrey Ross	RANDATA
Mr Lee Shipley	Australian Stock Exchange
Ms Ann Steward	Office of Government Information Technology (Project Gatekeeper)
Mr Brian Stewart	National Office for the Information Economy
Mr Randall Straw	Multimedia Victoria, Victorian Government (GTTC)
Mr Peter Thomson	Australian Payments Clearing Association Ltd

Support for the project was provided by the following officers from DOCA and NOIE:

Mr Phillip Hennig	National Office for the Information Economy
Dr Simon Pelling	Department of Communications and the Arts
Ms Saima Tuisk	National Office for the Information Economy

Valuable input was provided by:

Mr Adrian McCullagh, on behalf of the Attorney General's Electronic Commerce Expert Group; and

Mr Bill Osborne and Mr Craig Dowling on behalf of the Commonwealth Office of Government Information Technology.

The consultancy aspects of the project were undertaken by the following members of ETC Electronic Trading Concepts Pty Limited:

Mr Stephen Burns;

Mr Ian Christofis;

Dr Roger Clarke;

Ms Chuin-Nee Ooi; and

Mr Tony Rossiter.

Input was also obtained from a wide range of organisations not directly represented upon the Working Group. Some organisations represented on the Working Group were also interviewed. Refer to "APPENDIX J - Consultation" for details of persons and organisations interviewed. Information was also derived from research and prior work undertaken by the consultants. The logistics of producing a report within the short timeframe allowed for the study has meant that inevitably the choice of information included in or excluded from the report, and the editorial style adopted is largely that of the consultants rather than the Working Group.

Whilst the Working Group was primarily focused on a peak body for a "National Public Key Infrastructure" (NPKI) for Australia, the scope of its considerations included forms of electronic authentication other than those based on public-key cryptography. To reflect this scope, the term *Australian National Electronic Authentication Framework* (ANEAF) has been adopted for this report, rather than PKAF or NPKI which specifically refer to public-key cryptography[6]. In order to prevent confusion of terminology with the PKAF *PARRA*, and to align with international usage, this report will utilise the term Australian Policy Approval Authority (APAA) to represent the peak body, and the term Root Certification Authority (RCA) to represent the operational authority that performs the root certification functions identified within the PKAF strategy. The term Policy Creation Authority (PCA) has also been used to identify the certification authority that creates certificate policy within the ANEAF, this term is representative of the PKAF ICA.

This report not only canvasses whether or not a peak body is required at this point in time, but provides business models and options for the structure, operations and role of a peak body to oversee a national framework if one is required.

The current situation worldwide is that many of the conventional views about public key infrastructures, and the legal and regulatory frameworks introduced to address electronic signatures, are being seriously challenged. Extensive work is being conducted by state, federal and supra-national government bodies across the globe as well as by communities, fora and think-tanks. The output from this work points to the complexity and multi-dimensionality of the issues to be addressed and the rapidly changing views of the 'problem' and the possible 'solution'. This work will continue to illuminate and clarify the debate, to Australia's benefit. In this uncertain environment all ways forward involve some risk of being deemed inappropriate at some future time. However the Working Group believe that taking no action is similarly risky. In attempting to formulate a clear position on the various issues addressed by this report, the Working Group has encountered the complexity of some of these issues and the complex inter-relationships between them. The Working Group could not form a consensus on some issues. These have been identified for further work.

[6] Nevertheless, as a matter of practicality, it should be noted that public-key cryptography was the most mature and most widely deployed electronic signature technology at the time of the report.

2. TERMS OF REFERENCE OF WORKING GROUP

The Commonwealth Government wishes to facilitate the establishment of a peak body to oversee the development of a national framework for the authentication of users of online communications services. This framework would provide:

- a trusted system for the generation of digital signatures to give corresponding parties certainty in each others' identities;
- assurance of the integrity of electronic data used; and
- a means of ensuring non-repudiation of electronic transactions.

As a first step in this process, Government established a Working Group (WG) to specify details of the framework, in particular its oversighting body, and report to the Minister for Communications, the Information Economy and the Arts by the end of March 1998.

The twelve members of the Working Group (excluding the Chair) represent:

- Commonwealth Government Agencies;
- GTTC;
- Suppliers of Certification Products/Services; and
- User and other Organisations.

Whereas the Government did not prescribe mandatory direct government involvement in relation to the above, it expressed a clear preference for a national framework which is:

- **technologically neutral** - ie to the greatest extent possible it should not be limited to particular technologies, but should be able to be adapted to new authentication products and systems as they emerge,
  - ◊ however, the Government acknowledges that authentication techniques based on asymmetric (public key) encryption are currently the most widely accepted by industry; and
- **non exclusive** - that is, it is <u>not</u> envisaged that it should be compulsory for all certification authorities to operate under the national framework
  - ◊ although there is an expectation that most will, given the expected market advantages of doing so.

3. BACKGROUND

3.1. Identification and User Authentication

The term *user authentication* refers to any methods used to check (ie authenticate) the identity of a user. One dictionary definition is "to establish the validity of a claimed identity" [7].

It is important to understand the distinction between ***identification*** and ***user authentication***. These are normally defined as follows:

- Identification involves proffering of non-secret information, such as the name of the individual or the organisation. It is essentially "stating who you are".
- User authentication is the checking of the identity. ("Prove that it is you.") One could say it is the authentication of the identity of the user. It typically involves proving knowledge of secret information and/or possession of a token to verify the user's identity. Using cryptographic methods the user proves knowledge of a secret (a cryptographic key) without disclosing what that secret is.

In practice, the two may merge; identification may be subsumed in the process of user authentication. The proffering of secret information or possession of a token may in fact also be used to identify a user. A example is that the quoting of a licence number and other "fairly secret" data may act as both identification and user authentication.

3.2. Electronic Authentication

For widespread adoption of electronic methods of transacting business, industry and Government require, amongst other things, the ability to:

- provide authentication of the identity of electronic correspondents (*user authentication*); and
- hold parties to agreements (*non-repudiation*) submitted electronically.

For many services, it is essential to have mechanisms to verify that the party making use of the service is indeed who they claim to be. These user authentication mechanisms must work remotely and, preferably, using the same electronic communications channel that is used to deliver the service. Without reliable methods of confirming the identity of users, delivery of some types of services electronically poses many problems or indeed may be completely inappropriate.

[7] Definition 3 of authentication in "Information Security - Dictionary of Concepts, Standards and Terms" Longley, Shain & Caelli, Stockton Press 1992.

Public-key cryptography can provide the technical means to implement such protection. (Public-key cryptography can also provide confidentiality, but this is not the subject of this report.) Two common approaches are challenge and response protocols, and digital signatures.

3.3. Electronic Signatures

Electronic signature is a general term used to describe various 'electronic' methods that attempt to provide some or all of the functions of a hand-written signature. In essence, electronic signatures are methods of adding data to an electronic document as a means of authenticating it. Forms of electronic signatures include:

- digital signatures;
- digitised images of paper signatures; and
- biometric data, such as a recording of the dynamics (pen pressure and velocity) of a paper signature.

Whereas digital signatures are considered to provide the basis for strong authentication, some other methods are considered inappropriate as replacements for paper signatures because they can be easily copied and associated with a different document.

However in spite of the current emphasis on digital signatures, it considered likely that other strong electronic authentication methods may emerge in future and it is therefore considered inappropriate to enact legislation or set up statutory bodies which are narrowly confined to the specific technology of digital signatures only.

3.4. Digital Signatures

Digital signatures are a form of *electronic signatures*. Digital signatures allow messages to be "signed" in a way that undeniably associates the signer of a message with its content. Like its conventional counterpart, a digital signature links a particular person to an electronic document and so allows authentication of the identity of the person who sent the document. However, it offers greater security than a hand-written signature because it cannot be fraudulently applied to a different document. Furthermore, it can also verify that the document itself has not been altered in any way since it was digitally signed.

A digital signature is not a digitised image of a hand-written signature. It is a cryptographic checksum of the document. Public-key cryptography (see below) is used to generate and check digital signatures. To generate a digital signature, a private key of the sender is used. The matching public key of the sender can then be used by anyone to check the signature. The digital signature can be distributed with the document, typically by appending it.

3.5. Public Key Cryptography

Public-key cryptography involves mathematical computations using a key (a discrete piece of information, usually numeric, associated with a person, position, process, etc) and the data (eg the contents of a transaction or document), treating the data as a set of large numbers. This newer approach to cryptography allows one key to be public, the *public key*, while the other key, called the *private key*, is a secret known only by the owner of the key pair.

For encryption, a public key of the recipient is used to encrypt the message, and the matching private key of the recipient is used to decrypt the message. Anyone can encrypt a message but no-one else can decrypt the message because no-one else has the private key.

For digital signatures, the keys are used in the opposite manner: the private key of the sender is used to digitally sign the document, and the matching public key can be used by other people to verify the digital signature.

Public-key algorithms can be used to encrypt messages, authenticate users, exchange keys for use with symmetric algorithms, and to create digital signatures.

Many jurisdictions around the world are establishing arrangements of appropriate legislation, infrastructure and technical standards, to give some form of legal effect to digital signatures.

Refer to "Appendix D: Public Key Cryptography" for more detail.

3.6. Certification Authorities

Because the public key of anyone can be widely known, public key cryptography allows secure messages to be exchanged without the need for specific advance arrangements bilaterally between parties. However, there is still a need for assurance about the ownership of public keys, so that confidential messages are not encrypted using the public key of an imposter instead of the intended recipient, and so that someone cannot fraudulently sign messages claiming to be someone else.

A Certification Authority[8] provides assurance that a public key does in fact belong to the person whose identity is being associated with that key. It does this by providing certificates.

A Root Certification Authority is the top of a hierarchy of Certification Authorities (CA). It certifies the public keys of all the CAs directly below it in the hierarchy. These CAs may in turn certify the public keys of other CAs lower in the hierarchy, or certify the public keys of end-users directly.

Refer to the "Appendix D: Public Key Cryptography" for more detail.

[8] Certification Authorities are also known as Key Certification Authorities (KCA) and Certificate Authorities.

3.7. Public Key Infrastructure

Significant activity has already occurred, in Australia and internationally, towards establishing infrastructure to support the widespread use of public-key cryptography. This infrastructure is referred to as "public key infrastructure", a term which includes Certification Authorities, technical standards, policy, and supporting changes to the legal environment.

Public key cryptography can be used for a wide range of security purposes. Its use for securing internal computer systems within an organisation (eg to secure a Local Area Network), or even between closely inter-working organisations, does not require the formality and external recognition of a public key infrastructure as discussed in this document. Public Key Infrastructure is primarily concerned with providing effective authentication mechanisms between organisations or individuals, rather than securing computer systems.

Some pertinent public key infrastructure activities are:

- the Public Key Authentication Framework (PKAF) initiative in Australia, of which this project is a part;
- the presence of several operational commercial Certification Authority services in Australia;
- initiatives in various other countries and regions at a supra-national, national, state level to establish public key infrastructure; and
- establishment of an international public key infrastructure under the international credit card associations (Mastercard, Visa, et al) to support:
  - consumer payment transactions over open networks, such as the Internet, using the Secure Electronic Transaction (SET) protocol; and
  - the Europay/Mastercard/Visa (EMV) specification for financial applications on smartcards.

In addition, public-key cryptography is increasingly being used to augment or replace traditional (symmetric) cryptography within areas such as the payment system. Such initiatives could also potentially benefit from integration with a wider public-key infrastructure.

For further information refer also to "Appendix C: User Authentication and Cryptography" and "Appendix D: Public Key Cryptography".

3.8. Roles and Functions of a Peak Body (PARRA) as Proposed in the PKAF Strategy Report

The notion of a peak body for an Australian PKI was canvassed in the PKAF Strategy Report, and its discussion and conclusions have guided much of the thought and debate in this area since then. Therefore it is useful, at this point, to summarise pertinent aspects of the PKAF Strategy Report's discussions.

The PKAF Strategy Report[9] canvasses the options of having:

- no peak body;
- a peak body which is not itself a certification authority (CA); and
- a peak body which is the Root CA (RCA) for Australia.

It recommends the third option and describes the peak body, known as the Policy and Root Registration Authority (PARRA), as follows:

"The PARRA will create the overall guidelines that all users, associations of users, tiered levels of CAs and subordinate policy making authorities must follow. This will establish the overall infrastructure security policy.

6.1.1 PARRA Composition

The PARRA will administer a national policy committee which has representatives from appropriate organizations such as the inner budget Commonwealth Agencies, State and Territory Governments, Standards Australia, law agencies, industry and community groups. The committee needs to be as representative as possible of the views of all those who will be involved with using the PKAF.

6.1.2 PARRA Role

The role of this 'trusted' national body, is to establish and monitor overall PKAF policy and to act as a root for the national certification architecture. Additionally, the PARRA is responsible for establishing policy for interoperation and cross-certification with other international and multinational root authorities. (A multinational root authority might be established to service world-wide services, such as banking, provided by large multinational organizations or business sectors.)

The PARRA creates the overall guidelines that all users, associations of users and subordinate components of the PKAF architecture must follow thereby establishing the overall infrastructure security policy.

Having established policy, the PARRA is responsible for monitoring the adherence to it. The PARRA will also audit the CAs and other subsidiary organizations of the PKAF to ensure their continuing compliance with the policy.

6.1.3 PARRA Functions

Following is a proposed list of PARRA functions:

1. *Develops and publishes the PARRA public key.*
2. *Sets the general policies and procedures that all entities and end-users of the PKAF must follow.*
3. *Certifies certificates of the subordinate authorities.*

---

[9] "*Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia*" (Standards Australia, Miscellaneous Publication MP75, 1996)

4. Provides any required key material for each subordinate.

5. Carries out identification and authentication of international or multinational infrastructure roots it deems appropriate to recognize.

6. Signs certificates of subordinate entities and of national, international or multinational infrastructure roots it deems appropriate to cross-certify.

7. Publishes identification and locality information of subordinate entities (e.g. directory name, e-mail address, postal address, phone number and fax number).

8. Specifies information required from subordinate entities for a request of the revocation of the entity's certificate.

9. Receives and authenticates revocation requests concerning certificates it has generated.

10. Generates and publishes the national and international Certificate Revocation Lists (CRLs) for and from all subordinate and peer authorities.

11. Archives certificates, CRLs and audit files.

12. Provides cross-certification between any industry, international and multinational peak bodies.

6.1.4 PARRA Process

The subordinate authority generates and provides to the PARRA all the data required in the certificate creation. When the certificate is issued it will declare the PARRA as the issuer. The PARRA verifies the information (out-of-band) and "signs" it. The signed certificate is returned to the subordinate authority.

The PARRA also returns, in a secure manner, its public signature key within a Root PARRA certificate. This is the basis of the trusted certification path. The subordinate is then responsible for validating the returned certificate."

3.9. Related PKAF Activity

A number of separate bodies in Australia are currently working on aspects of the proposed Public Key Authentication Framework (PKAF):

- technical standards (Standards Australia IT/12/4/1 committee);
- legal frameworks (Attorney-General's Electronic Commerce Expert Group [ECEG]); and
- establishment of a Government Public Key Infrastructure (GPKI), known as Project Gatekeeper, to eventually come under PKAF, for the Commonwealth Government (3 working groups set up under the Office of Government Information Technology [OGIT]).

In addition, international activity is occurring within specific industries (eg financial services), the Organisation for Asia-Pacific Economic Cooperation (APEC), the United Nations Commission on International Trade Law (UNCITRAL), and other forums.

4. INTERNATIONAL ACTIVITY AND LEGAL MODELS

4.1. Current Status Relating to PKI Laws and Frameworks

Many governments across the globe have either enacted or are in the process of considering the enactment of legislation pertaining to the usage of digital signatures or other forms of electronic authentication. There are also a number of multi-national organisations which have developed or are developing model laws with regards to electronic authentication, such as the United Nations Commission on International Trade Laws (UNCITRAL) and the International Chamber of Commerce (ICC).

The issue as to whether a 'peak body' is established, and the role/s played by such a peak body, is usually dependent upon the legal framework which has been adopted/proposed by the jurisdiction to deal with electronic/digital signatures. A variety of approaches have been adopted; these are examined in section 4.5 below and in more detail in "Appendix E: International Approaches to Legislation and Peak Body".

4.2. Open and Closed PKI Models

Legislation has tended to adopt the X.509 model and largely deals with the usage of digital signatures in an 'open' PKI model.

An 'open' PKI is defined as one where consumers obtain a single certificate which attests to their identity from a third party certification authority, and use the same certificate in transactions with potentially numerous merchants. [Biddle 1997] In such an environment, a user of online services might go through a single authentication process (akin to the one hundred point check required to open a bank account) with a trusted third party, receive certification of his/her public key, and then be able to enter into electronic transactions/data exchanges with merchants, governments, banks, etc., thus using the same certificate and keypair for multiple purposes.

A 'closed' PKI is one where a contract or a series of contracts identifies and defines the rights and responsibilities of all parties to a particular transaction or where the certificates are used only within a known, bounded context. [Biddle 1997] Examples of usage of certificates in a closed PKI include a Government PKI (i.e. where a certificate is used only in transactions between the government and citizens of a country) and SET (where the certificate is used only within the payment system).

In considering the issue of open versus closed systems, it is worth noting that [ILPF 1997] included the following comments:

> *"… this project was initially conceived in Spring 1996. At that time, it appeared that industry efforts were being primarily directed towards developing open systems and therefore that open systems were going to be the prevailing business model. In fact, in the period during which this Report was written, the open system model has appeared to become an increasingly less viable business model. Instead, we believe that many consumer transactions which utilize certificates will occur in a 'closed system' or 'closed loop' model."*

4.3. Legislative models

The legislation that has been developed can be broadly divided into several distinctive categories. Debates continue as to whether there should be any legislation at all, and if so, which model of legislation should be used.

The legislation that has been enacted to date or is being considered has tended to be of one of the following types:

1. *a rule of equivalence* which equates electronic records and signatures with their paper counterparts. Examples of this model include the UNCITRAL Model Law on Electronic Commerce and the proposed Massachussetts Electronic Records and Signatures Act (MERSA).
2. *a framework of principles* which defers to the specification of rules and regulations which are required to implement and govern the usage of electronic signatures to a statutory entity. An example of this model is the California Digital Signatures Bill (AB 1577).
3. *a complete, prescriptive law*, which includes the specification of regulations which govern the usage of electronic signatures. Examples of this model include the Utah/ABA model and the Malaysian Digital Signatures Act 1997.

The specifics of the legislation can also be categorised based on the following characteristics:

- technology neutrality;
- scope of the legislation;
- the definition of an electronic or digital signature;
- the voluntary or mandatory licensing of certification authorities; and
- the issues relating to the establishment of a peak authority.

Refer to "Appendix E: International Approaches to Legislation and Peak Body" for full details.

4.4. Approaches to the 'Peak Body'

The issue as to whether a 'peak body' is established, is usually dependent upon the legal framework adopted by the jurisdiction to deal with electronic/digital signatures.

The 'Functions and structure of the peak body' section of "Appendix E: International Approaches to Legislation and Peak Body" provides an analysis of some of the approaches adopted internationally.

It is possible to differentiate between these by examining the approach to:

- **Technology** covering:
  - Digital signatures only; or
  - Electronic signatures in general.
- **Licensing of CAs** (with regards to offering of services to the public) approaches being:
  - Mandatory; or
  - Voluntary; or
  - No licensing.
- **Peak body functions** including one or more of the following**:**
  - Policy formulation;
  - Policy enforcement;
  - Licensing of CAs;
  - Root CA; and
  - Cross jurisdictional arrangements.

The 'entity' nominated to perform the 'peak body' function is almost without exception government. A contrary approach proposed by the USA Electronic Financial Services Efficiency Act 1997 (Baker Bill) proposes that a National Association of CAs (NACA) be charged with the responsibility, but that this be overseen by government.

5. CASE FOR A NATIONAL FRAMEWORK AND PEAK BODY

Electronic authentication raises significant issues in respect of evidence and contract, liability, privacy and consumer protection, and sovereignty and international trade.

A crucial question that arises relates to the role to be played by government in resolving these issues. While governments may have expressed a preference for private sector leadership in such matters, many have recognised the essential facilitating role which they need to play in relation to the provision of an enabling legal/regulatory/policy framework.

In this context, the case for the establishment of a peak body to oversee the ANEAF was canvassed with the persons and organisations interviewed.

Two issues are combined here and need ultimately to be separated:

- the case for the Australian National Electronic Authentication Framework (ANEAF) and peak body;
- the case for, and the extent of, facilitation of the ANEAF and peak body by Federal Government.

While one of the organisations interviewed felt that there was no case for a Government-facilitated National Peak Body (they felt that if such were needed it would emerge naturally from the market), almost all groups consulted felt there was a case, in terms outlined further below, for Government facilitating the establishment of a National Peak Body for the ANEAF.

In discussing the cases below, it should be emphasised that material presented represented the range of material elicited in interviews and not all of this was necessarily supported by the Working Group. The Working Group's position is summarised in explicit recommendations.

5.1. Three Important Contextual Issues

In developing the case for a Government-facilitated ANEAF peak body, three important issues need to be kept in mind.

5.1.1. Planning Horizon

It has become clear that planning should not be undertaken in the context of today's technological environment, but in terms of an environment that will come about in two to three years time. This is not to say that there is not a case for more urgent action, as people and institutions are exchanging keys now, and the Federal government will commence on 1 July 1998. Beyond this, however a number of facilitating factors appear to come together in the two to three year time frame:

- the widespread standardisation and adoption of smart cards as client security modules, managing keys in such a way as to assure the sole control of the key-holder over their use;

- the widespread inclusion of suitable standardised smart card readers in new desktop systems as a matter of course;
- ready availability of suitable standardised smart card readers as cheap upgrade options for existing desktop systems;
- in conjunction with an explosion of SMTP-based Internet mail, the adoption of common standards for the security of that mail (most probably based on a version of the S/MIME protocol using key recovery).

These changes are likely to lead to an environment where strong and dependable cryptographic authentication methods are widely available and in common use.

5.1.2. The Need to Maximise Participation by CAs

Since it has been specified by the Government that participation by CAs in any ANEAF is to be voluntary, it must be borne in mind that CAs will only participate if the costs of participation are outweighed by the benefits that accrue from participation.

On the one hand this means that the costs of participation must be minimised, consistent with maintenance of the overall integrity of an ANEAF.

On the other hand, reasons/incentives for participation must be provided. Possible 'incentives' include:

- Participation in a branded scheme with high consumer recognition;
- Measures which provide that digital signatures created within ANEAF have an evidentiary advantage in courts, over non-ANEAF digital signatures (the draft recommendations of the ECEG do not provide this);
- Access to Government business (the representatives of Project Gatekeeper were not supportive of this approach);
- Limitation of CA liability within the ANEAF (the draft recommendations of the ECEG do not provide this).

5.1.3. The Role of Government Facilitation

There is a general belief that appropriate Government facilitation will "lubricate the wheels of Electronic Commerce[10]" encouraging its development in a way that would otherwise not occur as quickly or effectively.

[10] *Electronic commerce* is a general term applied to the use of computer and telecommunications technologies in place of paper-based or face-to-face interaction, particularly on an inter-enterprise basis to support trading in goods and services, but also between consumers and businesses, between business and government, and between government and individuals. Electronic commerce uses a variety of technologies such as EDI (Electronic Data Interchange ie structured messages), email, facsimile transfer, electronic catalogues, Internet World Wide Web interaction, and directory systems, on open or closed networks. Electronic commerce content can include text, formatted documents, graphics, animation, video, audio, computer programs, etc.

Examples of Government facilitation of commerce in the past have included:

- Central banking - Central banks emerged to deal with a fundamental instability in the system of par banking, which predisposed the system, in the absence of central bank guarantees, to the possibility of catastrophic runs on financial institutions. Here, government intervention corrects a structural flaw in the system;
- Patent Laws - Patent law grants limited monopolies to holders of technical secrets, in return for making those secrets public so that they can be exploited generally at the termination of the monopoly. Arguably, this government intervention was a necessary precursor for the Industrial Revolution and the pace of technological advance that has followed; and
- Telecommunications Deregulation – Telecommunications carriers have long been regarded as possessing a natural monopoly[11] (AT&T was declared as such by the US Government as long ago as 1917); such instances of market failure are often used as justifications for Government intervention, although in recent years the tendency is for the lightest degree of intervention consistent with market efficiency (as opposed to measures such as nationalisation) – thus even though a natural monopoly would otherwise exists, light touch regulatory measures correct the market towards a more ideal competitive model.

A specific case for Government intervention in facilitating an Australian National Electronic Authentication Framework, in order to promote Electronic Commerce, has not necessarily been made in the sort of terms above. Strong arguments have been put forward in other terms. The debate is fertile. On the one hand, it can be argued that a heavy-handed approach could actually inhibit the development of Electronic Commerce, as, it has been argued, the German approach to electronic authentication may do. On the other hand, it can be argued that an absence of appropriate Government support could inhibit the development of the Certification Industry, and have a negative effect on Electronic Commerce generally. In this view, establishment of an appropriate environment is essential to position Australia as a net exporter of Certification Services.

The points below, indicate areas in which a “lubricatory” effect of intervention on Electronic Commerce may result.

[11] Refer to Section 5.5.2. To Promote a Contestable Market for CA Services

5.2. To Promote Compatibility

Compatibility has historically taken a long time to standardise in technological areas. As certification technologies are focused on global solutions, there has been a tendency to achieve industry consensus. As an example all certification authorities today, issue X.509 certificates that are compatible (even though there are some differences). This suggests there is a role for an ANEAF in promoting compatibility, but it is not obvious that the ANEAF can standardise the technologies. What ANEAF can do is to promote a consistent framework for compatibility.

This role should not be seen as a coercive one – such initiatives in Information Technology have a track record of failure (eg GOSIP). Rather, it should be seen as one of providing a framework of certainty, which those developing CA products and services can choose to adopt, ensuring that as an infrastructure emerges, compatibility is achieved with the minimum of reworking. The 'utopian' goal of such a framework is to allow all subscribers of accredited CAs to recognise and be recognised by all subscribers of other accredited CAs.

5.3. To Present and Represent a Single National View

This compatibility needs to be consistent with the emerging international framework. To this extent a single ANEAF would provide a single forum within which to develop a national position to be presented and represented in international fora. Conversely the ANEAF would provide a mechanism by which consistent emerging international trends could be reflected nationally.

Ultimately, this would extend to providing a single body for cross-certification of international authorities, facilitated by national policies for certification consistent with international trends.

A peak body backed by government would also be in a position to negotiate with other sovereign bodies on issues relating to an authentication infrastructure.

5.4. To Ensure Consumer Confidence

Given the current concerns and uncertainty amongst ordinary consumers[12] (both individual and business consumers), an ANEAF could have an important role to play in educating and reassuring consumers as to the integrity of digital signatures and the ANEAF in general. If performed effectively, this role would ensure that unnecessary doubts and uncertainty by consumers were not an inhibitory factor in the general uptake of Electronic Commerce.

[12] Consider the IBM advertising campaign exploiting fears about Internet security, which ran on television and other media from 1997.

5.5. To Ensure Market Efficiency

Three areas arise in which a Government-facilitated ANEAF would be able to promote and ensure efficiency of the market for CA services.

5.5.1. To Provide Consumers with Information

In order for a market to operate efficiently, it is necessary for consumers to be well-informed as to the merits and disadvantages of the various offerings. This can present difficulties when the product offered is "trust-based" as it requires the evaluation of a complex set of risk factors. This will be compounded during the setup phase by there being no history on which to base these assessments. It also presents difficulties when it is based on complex technology, such as public-key cryptography, because the general public cannot be expected to understand the technology to the extent required to make sound assessments.

This suggests that an important function of an ANEAF, is to provide quality labelling which allows consumers to compare offerings from different suppliers in a consistent fashion. In the absence of such labelling, there will be pressure for CAs to offer the cheapest possible product, regardless of risk, as the value of a high integrity product will not be immediately apparent.

One possible mechanism for this quality labelling would be the establishment of a strong ANEAF brand image, identified by a 'woolmark' or similar, which participants, through accreditation, would be able to display wherever their products and services were deployed in accordance with ANEAF requirements.

Thus a major purpose of an ANEAF may be to inform consumers, allowing them to make rational consumption decisions, improving market efficiency.

5.5.2. To Promote a Contestable Market for CA Services

There is evidence to suggest that, in the absence of an Australian National Electronic Authentication Framework, the provision of CA services may be a natural monopoly. This may be seen by considering the related area of directory services[13], which is also a natural monopoly. That is, in the absence of cross-listing arrangements, there is a natural tendency for a large directory (such as Yellow Pages) to grow at the expense of smaller competitors. (Consider the position of a subscriber trying to decide whether to list in a larger or smaller directory.)

---

[13] Directories and Certification services have much else in common:

- certificates can be, and in the case of confidentiality certificates, should be published in electronic directories;
- certificate revocation lists (CRLs) can be published in directories;
- CAs and RAs are in a position to collect directory entry information readily at the time of registration – so a lerge CA is in a position to also become a large directory provider.

For these reasons, coupled with the similar propensity of directory and certification markets to tend towards natural monopoly, it may be that the two should be considered together from a public policy perspective.

Similarly, a nationally dominant CA will tend to grow at the expense of smaller CAs, unless there is an arrangement which allows subscribers of the smaller CAs to recognise and be recognised by the subscribers of the large CA. An ANEAF could potentially provide such a mechanism.

Even if the above is not the precise mechanism by which a natural monopoly may emerge, a major purpose of an ANEAF may be to ensure competitive neutrality, allowing a healthy competitive market for authentication services to emerge.

5.5.3. To Manage Systemic Risks

As with the banking system, an ANEAF may be vulnerable to systemic failure. Systemic failure in relation to public key cryptography-based authentication may result from disabling events, including:

- algorithm failure;
- CA key compromise; and
- CA financial failure.

These events have the potential to have repercussions which extend to the entire market for CA services, and as such point to fundamental instabilities in that market.

An algorithm failure, as would occur, for instance, if mathematicians discovered a "fast" way of factoring, would render the vast of majority of present day signatures repudiable overnight, including those of CAs, perhaps irrespective of key lengths.

National co-ordinated contingency plans could control and manage the impact of such disabling events. For instance, plans in relation to algorithm compromise could ensure that, alternative algorithms were available and ready for rapid deployment if necessary.

The peak body of an ANEAF could be the natural body to develop and, if necessary, implement such contingency plans.

5.6. To Facilitate the Provision of Value-Added Services

Some interviewees felt that the real value of an ANEAF would begin to be realised, when certain value-added services were able to be provided in its context, further down the track. Examples of such services might be:

- the management of corporate delegations (eg purchasing authorities and limits);
- the authentication of attributes other than identity (eg professional qualifications); and
- the authentication of eligibility (eg proof of age for buying liquor over the Internet).

The peak body's role, then, would be to establish a sound environment in which such value-added services can be developed.

5.7. To Support Legislation

Nearly all interviewees felt that the primary purpose of an ANEAF, overseen by a suitable peak body, was to give support to any digital signature legislation, or electronic signature which may be passed by the Commonwealth Government. State and Territory Government legislation, if any, could also refer to the ANEAF. It was expected by the majority of interviewees that such legislation (possibly in conjunction with regulation) would, at the least, accredit ANEAF digital signatures in such a way as to provide certain legal presumptions as to the validity and effect of such signatures. These presumptions would not apply to non-ANEAF digital signatures.

This is seen as particularly important in dealings between parties with no prior agreement as to how digital signatures, or other electronic authentication methods, are to be viewed in law.

It has to be noted that the expectation of interviewees goes further than the forms of minimalist legislation proposed by the UNCITRAL Model Law on Electronic Commerce and others, including that under consideration by the Attorney-General's Expert Group on Electronic Commerce, in parallel with this study.

Minimalist legislation focuses on the primary task of recognising digital signatures in law. This recognition may be based[14] on four characteristics, deemed to render a digital signature functionally equivalent to a "physical" signature:

1. The signature must be unique to the signature-holder (but the signature-holder may have more than one signature);
2. The signature must be under the sole control of the signature-holder[15];
3. The signature must be verifiable;
4. The signature must be bound to the signed material, in such a way as to ensure the integrity of that material.

An ANEAF with its accreditation role, is not necessary to support minimalist legislation. Any digital signature, ANEAF based or not, can be recognised provided the four points above are shown to hold.

An ANEAF would however provide a degree of prior accreditation which would vastly simplify the task of proving the four points of functional equivalence in court.

The issue of whether to go further and give explicit legal recognition of ANEAF accreditation in some fashion, is one which will need to be considered further.

---

[14] As in the Californian legislation and the US Baker Bill.

[15] As a side point, it is worth noting that current digital signature technology appears to offer greater levels of assurance than physical signatures in all respects except point 2, which, in general, awaits standardised assured implementations

5.8. To Promote Export of Trust-based Services

Some interviewees expressed the view that an ANEAF might form a sound basis from which to export trust-based services to the region. It was pointed out that the Asian region was deficient to some extent in regulatory institutional infrastructure to support stable economic growth and this had been highlighted by recent events. Australia might be seen as a stable environment on which to base a regional authentication framework for Electronic Commerce.

5.9. To Limit Liability

The origin of the "Utah-style" legislative approach, was a study by the US Bar Association which suggested that the legal liabilities of CAs, in the absence of protective legislation, was such that it was felt no commercial CAs would ever emerge. If true, this is certainly a case for Government facilitation. Australian CAs interviewed expressed the view that limitation of their liability would be the primary incentive for belonging to an ANEAF.

It was felt that, as a general rule, participants in a ANEAF should bear liability when they act unreasonably and should be free of liability when they act reasonably. However, consider the situation where a consumer fails to adequately protect his or her private key, resulting in fraud. If the general principle—that parties acting unreasonably bear the resultant loss—applies, the consumer would bear potentially unlimited losses resulting from that fraud. Unlimited losses could be a major disincentive for consumers and CAs to participate in the system. Thus, consideration might be given to limiting liability even in the situation where a consumer does not act reasonably. Secondly, it appears that any dollar caps should be high enough to encourage the participants to act reasonably but low enough to avoid scaring consumers away from participating in the PKAF. Finally, it seems reasonable, that there should be no dollar cap for an intentional fraud.

With respect to both consumers and relying parties, while it makes sense for Certification Authorities to limit their liability for authorised certificates, it seemed to some, unreasonable for Certification Authorities to unduly limit their liability for issuing *unauthorised* certificates.

Except in test or demonstration situations, it was thought, that it would usually be unreasonable for CAs to disclaim all liability for direct damages or to establish a dollar cap so low as to effectively deny plaintiffs all meaningful monetary damage remedies.

The above views raise issues in regard to possible legislation, and in regard to establishing a legal opinion as to liability issues under various legislative models.

6. ROLES AND FUNCTIONS

6.1. Options

Two broad options emerged from interviews as to what the roles and functions of the peak body might be:

1. a full PARRA (Policy and Root Registration Authority) as conceived in PKAF (APAA and RCA combined), including:
   - policy formulation;
   - auditing and accreditation of ICAs;
   - root authority;
   - international cross-certification; and
   - root-level revocation-related functions.
2. a limited body (APAA) performing:
   - policy formulation, and;
   - auditing and accreditation of ICAs.

All interviewees agreed with the view that the role of the peak body should include:

- management of systemic risk; and
- maintenance of user confidence in the system.

Thus differences existed as to whether the following functions were required in the first instance:

- root authority;
- international cross-certification; and
- root-level revocation-related functions.

It should be noted that most interviewees, notwithstanding the list of functions above, believed that operational aspects, such as the root authority function or auditing of ICAs, might be and indeed, probably should be, outsourced.

6.2. Arguments

Option (1) was supported by a substantial minority. It was stated in support of this option, that PKAF had raised expectations that the peak body would be a PARRA, and the industry had made its plans based on that assumption (the typical absence of support for cross-certification in Australian developed security products – see footnote – is evidence for this).

Option (2) was the preferred option. Some felt that to give the peak body an operational role as a root authority was not necessary and would burden it financially during the start up phase. Strong arguments were put forward that the notion of a single root authority[16] as recommended in the PKAF Strategy Report was unnecessarily prescriptive, and did not take into account the pragmatic mechanisms by which users would gain trust in one or more roots outside the CA hierarchy. Against this must be balanced the view put forward by some, that without a root authority:

- compatibility between ICAs may suffer;
- as a matter of practicality neither CA nor Client technology yet supports cross-certification (see footnote);
- competitive neutrality may not be achieved as this is seen to require either a root authority or full cross-certification;
- international cross-certification (at a single point), when (and if) required, may not be possible.

The issue of whether an RCA is required in the first instance, should be kept apart from the issue of whether an RCA should be kept separate from an APAA, on which the Working Group agreed there were substantial grounds for separation, including:

- costs of establishment of an RCA capability, predisposing to possibly using existing infrastructure for provision of the RCA functions;
- the need for perceived independence of the two functions.

[16] There are two alternatives to a single root authority. In both cases, each ICA is in effect a root in its own right, with a self-signed certificate. It is anticipated that there will be half a dozen or so ICAs in Australia in the next few years.
In Case 1, without cross-certification, any certificate chain will terminate in the self-signed certificate of one of these half dozen or so ICAs. Thus signature verification software must be aware of each of these half dozen or so self-signed ICA certificates (instead of having to be aware of just one self-signed certificate in the case of a single root authority). This mode of operation is, in practice, how common browser and server software handles signature verification. Netscape Communicator 4 ships with 14 root CA self-signed certificates installed and recognised, and Microsoft Internet Explorer 4 ships with 7. Both allow more root CAs to be added, and recognition can be turned on or off (or made conditional). This system scales reasonably well and could be expected to work with up to tens of ICAs without difficulty. However, trust decisions have to be made with respect to each ICA.
In Case 2, the half dozen ICAs cross-certify each other in pairs by each signing a certificate for each other. If two ICAs X and Y cross-certify, pairs of certificates exist which allow, in effect, either X or Y to be regarded as the root authority depending on how the signature verification software chooses to construct the certificate chain. In a larger arrangement of mutually cross-certifying ICAs, this means that signature verification software only has to explicitly trust one of the ICAs in the system in order to acquire trust in all the others. In the simplest implementation of cross-certification in signature verification software, all N ICAs in the system must fully mutually cross-certify and $(N^2-N)/2$ cross-certification pairs are required (for half a dozen ICAs, 15 cross-certifications are required). Thus, such an arrangement does not scale well – one hundred ICAs would require almost 5,000 cross-certifications. An alternative implementation requires just N-1 cross-certifications, but is more difficult to administer and implement in software. In practice, most signature verification software, including the common browser and server software, and the offerings of Australian security product developers, does not support cross-certification.

6.3. Recommendations

6.3.1. Peak Body

The Working Group recommends the establishment of a peak body to oversee the Australian National Electronic Authentication Framework (ANEAF).

The Working Group further recommends that the focus of the peak body should, in the first instance, be on public key infrastructure rather than less mature technologies for electronic authentication. In particular, the priority should be to establish a National Public Key Infrastructure (NPKI) under the ANEAF.

The Working Group recommends that the policy aspects of an NPKI peak body be separated from the operational aspects, into an Australian Policy Approval Authority (APAA) and one, or possibly more, Root Certificate Authorities (RCAs), respectively.

The Working Group recommends the immediate establishment of an APAA.

It is anticipated that a national RCA will be required as early as the end of 1998. In view of this tight timeframe, it is recommended that the issue of whether and how a national RCA is to be established be addressed by Government as a matter of the highest priority.

6.3.2. APAA Roles and Functions

The Working Group recommends that the APAA functions should be:

a) to facilitate stakeholder involvement;

b) to promote the required level of trust in electronic commerce in Australia;

c) to approve the establishment of any RCA;

d) to represent the ANEAF within the global environment[17];

e) to promulgate appropriate electronic authentication standards in association with Standards Australia and international standards bodies[18];

f) to approve and oversee the establishment of a national evaluation and accreditation scheme; and

g) to manage systemic risk.

Functions not performed should include:

[17] An additional function to be considered by the APAA for later adoption, is the resolution of cross-certification issues at the RCA level and elsewhere.

[18] It was agreed that these standards were “minimal” in the sense that organisations could choose to exceed the promulgated standard.

h) operation of a national RCA; and

i) development of Australian Standards.

The Working Group recommends that measures of effectiveness be established for the APAA related to the functions above, and that the APAA be so established as to allow for regular evaluation of its performance against the identified measures.

7. APAA OPERATIONAL MODEL

7.1. Operations

The following is an example of how the APAA would operate, the actual process will be determined by the APAA when it is established, this example is used to illustrate the scope and interaction of the APAA.

1. The APAA endorses applicable standards for the elements of the ANEAF. This includes the RCA, PCA and other elements.
2. Accredit commercial evaluators, and auditors.
3. Prospective or renewing ANEAF elements then seek evaluation in all relevant areas, paying fees to the evaluators.
4. Evaluators forward the results of their evaluations to the peak body.
5. The secretariat of the peak body, assembles these and prepares a report for the board, recommending accreditation or not on the basis of the assembled evaluation reports.

Examples of areas, possible standards, and possible evaluators are provided in the table below:

Area	**Standards (International & National.)**	**Evaluators**
Premises	ASIO Protective Security Manual	Ex -ASIO personnel
People	Australian Security Evaluation Service	Australian Security Evaluation Service
Process	PKAF 12/4/1 AUS404 – US SAS70 (audit) ISO9000 (expensive)	
Technology	PKAF 12/4/1 ITSEC (expensive)	AISEFs (Admiral & CSC)
Corporate Governance	Corporations Act (assuming company form)	Auditors
Financial Stability	ASX Listing Standard	Auditors

Some comments are worth making in relation to the table provided above. Firstly, it is an example only. It will be up to the APAA to determine applicable standards and licensed evaluators. Secondly, interviewees expressed the following views, which will need to be taken into account by an eventual peak body:

- ISO9000 compliance is seen as cumbersome and expensive, alternatives would be welcome;
- ITSEC[19] (or eventually Common Criteria) accreditation is also expensive;

[19] European Information Technology Security Evaluation Criteria.

- if suitable standards other than national security (ASIO et cetera) standards can be found for premises and personnel, it would be preferred; and
- where possible international standards should be used, to minimise re-accreditation of components already accredited overseas.

An alternative to the above approach, based on current practice within the payments industry, was proposed. This relies on the concept of self-audit, and may reduce costs of compliance. The exact implementation of this varies, but might work as follows:

1. In addition to specifying standards and licensed evaluators, the APAA specifies publication standards for evaluation reports.
2. It does not accredit as such, but merely accepts letters from organisations claiming to have met accreditation requirements.
3. It then publishes those letters.

Legal liability in regard to accreditation lies with the RCA(s) and PCAs themselves, and the liability of the APAA is accordingly diminished

It has been noted that whereas self-audit is used in the financial sector, this is done within a context where financial institutions are already required to submit to prudential regulation and supervision. This may limit the advisability of self-audit, in an otherwise unregulated ANEAF.

7.2. Recommendations

The Working Group recommends that the following operational model for the APAA should be adopted.

Auditing of PCAs, should be outsourced to the greatest extent possible.

The APAA will specify applicable standards for the various different aspects of PCAs and subordinate CAs. Further it will identify licensed commercial evaluators (possibly doing the licensing itself in some areas). Prospective or renewing PCAs then will seek evaluation in all relevant areas, paying fees to the evaluators.

The Working Group did not recommend the adoption of self-audit techniques as this was inconsistent with the model finally recommended. This may be revisited by the APAA itself.

The APAA will determine its policies with a view to minimising the costs of compliance by participating CAs, to the that this does not compromise the achievement of integrity of the ANEAF.

8. APAA RESOURCING

A range of resourcing models from a maximal to a minimal one are considered below. Note that neither of these extremes is recommended.

8.1. Fully Funded Model - Maximal

The primary functions of APAA are performed by a voluntary board, and a full-time secretariat.

The secretariat might consist of the following personnel:

- Chief executive
- Legal counsel
- Audit specialist
- Technical specialist
- Administrative support
- Clerical support x 3

In addition to personnel, it is anticipated that costs would be incurred for the following:

- accommodation including boardroom
- office systems
- telephony including teleconferencing
- travel for board members and senior secretariat
- international travel for senior secretariat
- conferences for senior secretariat
- consultancy fees for legal, technical, audit and marketing
- advertising/marketing

8.2. (Almost) Virtual Organisation - Minimal

In this model, the primary functions of the APAA are performed by a voluntary board, and a full-time minimal secretariat, but technical, legal and audit advice are primarily provided voluntarily by participating RCA(s) and PCAs.

The secretariat for this model, might consist of the following personnel:

- Executive Officer
- Administrative support

In addition to these personnel, it is anticipated that costs would be incurred for the following:

- serviced office including boardroom
- office systems and telephony including teleconferencing
- travel for board members
- advertising/marketing

8.3. Estimates of Costs

Indicative broad estimates are based on annual budgets for a number of 'peak bodies', namely the Australian Payments Clearing Association (APCA), the Australian Domain Naming Authority (ADNA) and Tradegate/ECA.

While APCA has 14 full-time staff, much of its work is undertaken by committees staffed from its membership. Further it is seen as having lower requirements in relation to international travel and liaison requirements than an ANEAF peak body would have. APCA has an annual budget of $2.8m.

ADNA is a "virtual" organisation with no full time secretariat, but still has a planned budget of $150,000 per year. Its policy operations are probably less onerous than those of an ANEAF peak body.

Tradegate/ECA has a staff of 12 and a budget of $1.3m per year.

All bodies have less need for advertising/marketing than an ANEAF peak body would have, at least, initially.

There are a range of ballpark figures which might be used, depending on the degree to which the various functions identified are to be performed and the speed with which the organisation ramps up its operation.

On the basis of the foregoing the annual costs will be taken to be $1.3m as a purely indicative figure.

8.4. Industry Base

The Certification Industry is still developing, most if not all Certification Authorities globally are running at a loss, in order to establish a market. This is reflective of the immaturity of the Industry generally; within the global environment there are less than a dozen operational Certification Authorities.

It is expected that there will be three to eight ICA's operational within Australian over the next three years.

8.5. Sources of Funds

There was consensus amongst interviewees that Government seed funding would be required for at least the first few years of operation, as the ANEAF industry will earn negligible revenue in this time. Ultimately, the peak body could be self-funding, based on fees charged to the industry. However, a number of interviewees expressed concern that the move to self-sufficiency is unrealistic.

8.6. Recommendations

The Working Group recommends that, once the eventual form and functions of the APAA have been decided in principle, a detailed costing of the APAA's operations should be undertaken.

Further, the Working Group recommends that, in the interim, a budget estimate of $1.3 million per annum, should be used, independent of the structure selected.

The Working Group recommends that the possibility of the APAA eventually being self-funding should be investigated carefully.

9. APAA STRUCTURE AND FORM

Interviewees split almost evenly as to the form of the APAA.

1. A bare majority felt that it should be a statutory body, or Government business enterprise, reporting to the Minister for Communications, the Arts and the Information Economy, with an advisory group representing users of various types, as well as other community groups including privacy advocates.
2. A bare minority felt that it should be an independent body, probably a company with limited guarantee, controlled by a board representing users of various types, as well as other community groups including privacy advocates.

Those who supported (1) did so because they felt that the body needed the imprimatur of Government in order to be credible. Those who supported (2) did so because they felt that overt Government involvement would lessen the credibility and trust of the peak body, especially where such involvement included law enforcement or national security organisations.

9.1. Accountability

If a Government body, as in option 1, accountability through the Minister and Parliament would ensue through usual processes.

If independent, as in option 2, the situation is a little more difficult, but broadly, corporate reporting requirements together with periodic board initiated audits of peak body operations might suffice to ensure accountability to its membership. Nevertheless, options 2 are intrinsically less accountable than option 1.

9.2. Representation

As stated above, on the issue of representation on the board of the peak body there was almost consensus that membership should not be limited to CAs, but should mainly represent users of various types, as well as other community groups including privacy advocates.

A dissenting view commended the US Baker Bill model, in which the peak body membership consists solely of participating CAs. This is similar to the form of the Australian Payments Clearing Association in the Australian payments industry, which is owned by participating financial institutions.

There was dissent on the issue of the extent of Government representation. Some interviewees felt that a wide range of Government interests needed to be represented, including law enforcement and national security. Others felt that Government representation should be limited to its role as a (significant) user of certificates.

In achieving broad representation, the example of the Australian Domain Naming Authority (ADNA) was considered worthy of consideration. ADNA only has peak bodies on its board. Any entity may become an observer at that board by paying a $1,000 annual fee. Additionally, observers elect two members to represent them on the board. It should be noted that Australian CAs do not currently have an industry body which could represent them.

It is desirable that the composition of the board of the peak body can change with time according to community desires.

Beyond the board, ADNA has various committees which can have input into its deliberations. Such a subordinate committee might be an appropriate place for Government interests such as law enforcement or national security to be represented. Here too, standards bodies might be represented, as many interviewees expressed reservations about such bodies being represented at board level.

9.3. Trade Practices

Any peak body will need to comply with Trade Practices regulations. While it was initially felt that a statutory body might have the advantage of crown immunity, this is not at all certain. Given the importance of the objective of achieving competitive neutrality, it seems that the peak body should not seek immunity but should accept oversight by the ACCC as intrinsic to its operations.

9.4. Recommendations

There was broad support amongst the Working Group for a Government-based APAA.

The Working Group felt that the exact form of constitution of such a body was essentially a legal and political decision.

Thus the Working Group recommends that suitable legal opinion be sought as to the appropriate constitution of the APAA having regard to the following major influencing factors:

- the credibility and standing of the body with consumers and the CA industry;
- the need for a degree of independence;
- liability of the APAA and its board members, and organisations other than the APAA participating in the ANEAF, including any RCA, PCAs and other CAs;
- the need for broad community representation on the APAA.

Further, the Working Group recommends that the need for supporting legislation in respect of the management of liability be monitored.

10. ROOT CERTIFICATION AUTHORITY

As the committee has recommended the separation of the APAA from the RCA, this section looks at the issues associated with the Root Certification Authority.

10.1. Introduction

The Root certification authority supports the certification of subordinate PCA's as identified within the PKAF report.

Currently there exists a self-signed certificate that is referred to as the *root* certificate, due to its ability to terminate certification paths. This report does not restrict the Root Certification Authority to this technology, but will assume support for such a requirement within the ANEAF.

The committee has assumed from six to eight PCAs to support the ANEAF, as such the committee believes that the operation demands on a RCA are not cost/resource significant.

10.2. Functions

The functions of the RCA are:

a) Generates Root key-pairs, and any associate parameters depending on the algorithms required.

b) Establishes a trusted facility in which to operate the RCA and store the Root cryptographic information.

c) Certifies certificates of the subordinate authorities, subject to APAA approval.

d) Provides any required key material to each subordinate.

e) Signs certificates of national, international or multinational infrastructure roots, as approved by the APAA, to cross-certify.

f) Receives and processes revocation requests concerning certificates it has generated.

g) Generates and publishes the national and international Certificate Revocation Lists (CRL) for all subordinate and peer authorities.

h) Archives certificates, CRLs and audit files.

10.3. Who should be a RCA

The operation of an Australian RCA requires an investment in specialist security and cryptographic techniques that are not commonly available. In addition there is extensive physical, procedural, and personal security requirements that are investment intensive.

As identified within the PKAF and OECD reports the establishment of an authentication framework can be separated from any confidentiality framework; this provides Australia with the option to use existing national assets within the Defence Signals Directorate to support the requirements of the ANEAF for an RCA.

10.4. How to ensure broad support for a Government facilitated RCA

The traditional issues associated with such a proposal have been discussed within other forums, but it is suffice to state that there is a requirement that not only is the RCA secure, but that it must be seen to operate to meet the needs of the ANEAF.

As the RCA will operate under the policy and authority of the APAA, the processes are open to the membership of the APAA (see recommendation on a broad APAA representation).

10.5. Recommendation (already stated in 6.3.1 above)

It is anticipated that a national RCA will be required as early as the end of 1998. In view of this tight timeframe, it is recommended that the issue of whether and how a national RCA is to be established be addressed by Government as a matter of the highest priority.

11. SUMMARY OF RECOMMENDATIONS

11.1. Peak Body

The Working Group recommends the establishment of a peak body to oversee the Australian National Electronic Authentication Framework (ANEAF).

The Working Group further recommends that the focus of the peak body should, in the first instance, be on public key infrastructure rather than less mature technologies for electronic authentication. In particular, the priority should be to establish a National Public Key Infrastructure (NPKI) under the ANEAF.

The Working Group recommends that the policy aspects of an NPKI peak body be separated from the operational aspects, into an Australian Policy Approval Authority (APAA) and one, or possibly more, Root Certificate Authorities (RCAs), respectively.

The Working Group recommends the immediate establishment of an APAA.

It is anticipated that a national RCA will be required as early as the end of 1998. In view of this tight timeframe, it is recommended that the issue of whether and how a national RCA is to be established be addressed by Government as a matter of the highest priority.

11.2. APAA Roles and Functions

The Working Group recommends that the APAA functions should be:

a) to facilitate stakeholder involvement;

b) to promote the required level of trust in electronic commerce in Australia;

c) to approve the establishment of any RCA;

d) to represent the ANEAF within the global environment20;

e) to promulgate appropriate electronic authentication standards in association with Standards Australia and international standards bodies21;

f) to approve and oversee the establishment of a national evaluation and accreditation scheme; and

g) to manage systemic risk.

---

[20] An additional function to be considered by the APAA for later adoption, is the resolution of cross-certification issues at the RCA level and elsewhere.

[21] It was agreed that these standards were “minimal” in the sense that organisations could choose to exceed the promulgated standard.

Functions not performed should include:

h) operation of a national RCA; and

i) development of Australian Standards.

The Working Group recommends that measures of effectiveness be established for the APAA related to the functions above, and that the APAA be so established as to allow for regular evaluation of its performance against the identified measures.

11.3. AAPA Operational Model

The Working Group recommends that the following operational model for the APAA should be adopted.

Auditing of PCAs, should be outsourced to the greatest extent possible.

The APAA will specify applicable standards for the various different aspects of PCAs and subordinate CAs. Further it will identify licensed commercial evaluators (possibly doing the licensing itself in some areas). Prospective or renewing PCAs then will seek evaluation in all relevant areas, paying fees to the evaluators.

The Working Group did not recommend the adoption of self-audit techniques as this was inconsistent with the model finally recommended. This may be revisited by the APAA itself.

The APAA will determine its policies with a view to minimising the costs of compliance by participating CAs, to the greatest extent consistent with the overall integrity of the ANEAF.

11.4. APAA Resourcing

The Working Group recommends that, once the eventual form and functions of the APAA have been decided in principle, a detailed costing of the APAA's operations should be undertaken.

Further, the Working Group recommends that, in the interim, a budget estimate of $1.3 million per annum, should be used, independent of the structure selected.

The Working Group recommends that the possibility of the APAA eventually being self-funding should be investigated carefully.

11.5. APAA Structure and Form

There was broad support amongst the Working Group for a Government-based APAA.

The Working Group felt that the exact form of constitution of such a body was essentially a legal and political decision.

Thus the Working Group recommends that suitable legal opinion be sought as to the appropriate constitution of the APAA having regard to the following major influencing factors:

- the credibility and standing of the body with consumers and the CA industry;
- the need for a degree of independence;
- liability of the APAA and its board members, and organisations other than the APAA participating in the ANEAF, including any RCA, PCAs and other CAs;
- the need for broad community representation on the APAA.

Further, the Working Group recommends that the need for supporting legislation in respect of the management of liability be monitored.

APPENDIX A: ABBREVIATIONS

A-G	Attorney-General
ABA	American Bar Association
ADNA	Australian Domain Naming Authority
AISEF	Australian Information Security Evaluation Facility
AISEP	Australian Information Security Evaluation Program
ANEAF	Australian National Electronic Authentication Framework
ANSI	American National Standards Institute (U.S.A.)
APEC	Organisation for Asia-Pacific Economic Cooperation
ASC	Australian Securities Commission
ASIO	Australian Security Intelligence Organisation
ASX	Australian Stock Exchange
CA	Certification Authority
CRL	Certificate Revocation List
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DES	Data Encryption Standard
DNS	Domain Name System
DOCA	Department of Communications and the Arts
DSA	Digital Signature Algorithm
ECEG	Electronic Commerce Expert Group (Attorney-General's department)
FIPS	Federal Information Processing Standard (U.S.A.)
GPKI	Government Public Key Infrastructure
GTTC	Government Technology and Telecommunications Committee
IAB	Internet Architecture Board
ICA	Intermediate Certification Authority
ICC	International Chamber of Commerce
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
ITSEC	Information Technology Security Evaluation Criteria
MIME	Multipurpose Internet Mail Extensions
NCCUSL	National Conference of Commissioners on Uniform State Laws (U.S.A.)
NIST	National Institute of Standards and Technology (U.S.A.)
NOIE	National Office for the Information Economy
OGIT	Office of Government Information Technology
ORA	Organisational Registration Authority
PARRA	Policy and Root Registration Authority
PKAF	Public Key Authentication Framework
PKI	Public Key Infrastructure

POP	Post Office Protocol
RA	Registration Authority
SDSI	Simple Distributed Security Infrastructure
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SPKI	Simple Public Key Infrastructure
SSL	Secure Sockets Layer
UNCITRAL	United Nations Commission on International Trade Law

APPENDIX B: GLOSSARY

ADNA (Australian Domain Naming Authority)

The body that (arguably) is in charge of the domain name space .au. The authority of ADNA on the matter is still the subject of disputes.

AISEF (Australian Information Security Evaluation Facility)

See *ITSEC*.

AISEP (Australian Information Security Evaluation Program)

See *ITSEC*.

Algorithm

A finite set of well-defined rules for the solution of a problem in a finite number of steps.

ANSI (American National Standards Institute)

The national standards body of the United States of America, which is also the American representative to ISO.

APAA (Australian Policy Approval Authority)

A peak body undertaking the policy and accreditation functions formerly associated with PARRA in the PKAF strategy report.

Authenticode

A code signing system developed and trademarked by Microsoft.
See also *code signing*.

Asymmetric algorithm

See *Public key algorithm*.

Brand CA (BCA)

The second level CA in the SET certification hierarchy.
See also *SET*, *Certification authority (CA)*.

Certificate

A term first used by Loren Kohnfelder in 1978 to describe a signed record holding a name and a public key. Historically, it was used to refer to the binding between the globally unique name of a legal entity and the public key. However, recent developments suggest that the 'name' on the certificate could also be a property associated with the certificate holder. A certificate is digitally signed by a trusted third party, such as a certification authority, and usually contains other attributes about the certificate such as the validity dates for the key and the algorithms to be used with the key.

Certificate revocation list (CRL)

A list of certificates which have not expired for other reasons and have been revoked. A certificate revocation list includes information on the validity dates for the list, and is digitally signed by the issuing certification authority.

Certification authority (CA)

A trusted party which issues public key certificates. Certification authorities usually perform other functions related to issuing certificates, such as verifying the identity of the certificate holders and maintaining certificate revocation lists.

Certification hierarchy

A hierarchy of CAs, in which each CA is certified by the next higher CA in the hierarchy until a single trusted root CA is reached (which has a self-signed certificate).

Certification path

A series of certificates for CAs, each digitally signed by the next CA in the path.

Certification practice statement (CPS)

A declaration of the practices which a CA employs in issuing certificates generally, or employed in issuing a particular certificate.

Code signing

A system for ensuring the integrity and authenticity of software, by having a trusted party digitally sign the distributed binaries/source code. Active code signing proposals include Microsoft's Authenticode, JAR (a Java archive format with digital signatures) and the World Wide Web Consortium's DSig.

CRL

See *Certificate revocation list*.

Cross certification

A technique whereby two CAs can mutually recognise each other by each issuing a certificate for the other.

Cryptanalysis

The art and science of breaking or attempting to break cryptographically secured data.

Cryptographic algorithm

A mathematical function used to encrypt or decrypt a message.

Cryptographic system

A system based on cryptography, typically as a component of a larger system.

Cryptosystem

See *Cryptographic system*.

DES (Data Encryption Standard)

An algorithm specified by USA NIST and NSA to encipher and decipher data during transmission. DES is also specified in some Australian and international standards. DES transforms 64-bit message segments into 64-bit segments of cipher text, using a 56-bit key.

DSA (Digital Signature Algorithm)

A public key algorithm that can only be used for digital signatures developed by the USA NIST. DSA is specified in NIST FIPS 186.

Digital signature

The electronic means of duplicating the functionality provided by a handwritten signature. A digital signature is created by passing the document through a one-way hash function to obtain a cryptographic checksum of the document. This checksum is then encrypted with the private key of the signer — this is the digital signature. To verify the signature, the recipient passes the document through the same hash function to produce the checksum. The recipient then decrypts the digital signature with the public key of the signer and compares the result with the independently computed checksum. Digital signatures provide assurance over the integrity of the signed data and the authenticity of the signatory. Well implemented digital signatures provide stronger assurance than handwritten signatures.

EDI (Electronic data interchange)

A system allowing for inter-corporate commerce by the automated electronic exchange of structured business information.

EDIFACT

See *United Nations Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)*.

EFTPOS (Electronic funds transfer at point of sale)

The electronic transfer of funds from one account to another done at the point of sale of a product. It is usually initiated by the buyer using a card and a PIN (personal identification number) to access his/her account.

Electronic signature

A generic term used to describe various electronic means of assurance of the integrity and authenticity of a document. Manifestations of electronic signatures include digital signatures and signature dynamics.

EMV (Europay/Mastercard/Visa)

A set of specifications for a global payments framework using integrated circuit cards (smart cards), issued by Europay International, Mastercard International and Visa International. EMV includes the physical card specifications, terminal specifications, data structures used, security and communications protocols.

Encipher

A cryptographic technique in which as sequence of bits or characters is changed by means of a transformation.

Geo-political CA (GCA)

The third level CA in the SET certification hierarchy. The GCA allows a `brand' to distribute responsibility for managing types of certificates to grographic/political regions.
See also *SET, Certification authority*.

Global Server ID

A class of server certificates issued by Verisign for certain Microsoft and Netscape web servers. These certificates contain special key usage extensions which enable the usage `strong' encryption with clients using certain Microsoft and Netscape web browsers. At present, these certificates are issued only to financial institutions (globally) and approved U.S. companies.

GPKI (Government PKI)

A PKI that is limited in scope to government users and clients of the government.

IETF

See *Internet Engineering Taskforce*.

Intermediate Certification Authority (ICA)

In PKAF, a CA other than PARRA which certifies other CAs.

Internet Engineering Taskforce

A standards setting body of the Internet. Much of the work of the IETF is done in working groups, which are open to the anyone.

ISO (International Organization for Standardization)

A worldwide federation of national standards bodies. It is made up of a collection of member bodies, one from each country, each of is the national body most representative of standardisation in its country.

ITSEC (Information Technology Security Evaluation Criteria)

A European standard, based on a generalisation of US standards, for rating the security of Information Technology systems. In Australia the Defence Signals Directorate, in conjunction with accredited commercial organisations (AISEFs), uses the ITSEC criteria to evaluate products and systems. This is called AISEP. It is envisaged that CAs complying to PKAF requirements will have to meet defined ITSEC ratings.

ITU (International Telecommunications Union)

A worldwide consortium of telecommunications authorities with a major role in definition of international standards.

Key

A large number used as part of encryption, decryption, digitally signing or validation of digital signatures.

Message digest function

See *One-way hash function*.

MD5

A one-way hash algorithm developed by Dr. Ronald Rivest which is documented in IETF RFC 1321. MD5 produces a 128 bit hash.

NCCUSL (National Conference of Commissioners on Uniform State Laws

A body in the United States of America that is attempting to standardise the legislation enacted by the states by developing model legislation.

Organisational certification authority (OCA)

In PKAF, a CA which actually issues certificates to users (as opposed to certifying other CAs).
See also *Intermediate Certification Authority*.

Organisational registration authority (ORA)

RA that has the responsibility for verifying applicants within an organisation.

One-way hash function

An algorithm which outputs a single large number of fixed length (a hash), based on an arbitrary-length input file, which represents the information contained in the file. It is easy to calculate the hash given the input file, but it is difficult to work out what the input file was based on the hash. The hash is also unique to the file, i.e. it is extremely difficult to find two files which produce the same hash. Commonly used hash functions include MD5 and SHA-1.

PARRA

See *Policy and root registration authority*.

PCA

See *Policy Certification Authority*.

PKAF

See *Public key authentication framework*.

PKI

See *Public key infrastructure*.

Policy and root registration authority

The PKAF proposed Australian national root CA.
See also *Certification authority*.

Policy Certification Authority

A newer, more precise term for the PKAF proposed Intermediate Certification Authority or ICA.
See also *Certification authority*.

Private key

See *Public key*.

Public key

A key whose value can be published widely without compromising encryption or digital signature processes. Typically, a public key can be used to encrypt (but not decrypt) or to validate a signature (but not to sign). The public key is part of a pair. The other half, the Private or Secret Key, must be kept confidential and is used to decrypt messages encrypted with Public Key, or to digitally sign messages which can then be validated with the Public Key.

Public key algorithm

The class of cryptographic algorithms that uses the notion of key pairs—an encryption key and a decryption key—where it is infeasible to generate one key from the other. Typically, one key is kept private and the other is publicly published. Some public key algorithms can be used for digital signatures only, some are suitable for encryption and yet others are suitable for both purposes. Public key algorithms are also known as asymmetric algorithms.

Public key authentication framework

The outline for a PKI for Australia, restricted to authentication (digital signatures) published by Standards Australia.

Public key certificate

See *Certificate*.

Public key infrastructure

A framework for controlling the generation, certification, promulgation and revocation of public keys issued for encryption and digital signatures. Among other things, it typically includes legislation, regulations, bodies and technical standards. The proposed PKAF approach in Australia is an example of a PKI.

Registration authority (RA)

An entity that acts as an intermediary between a CA and an applicant for a certificate. The CA relies on the registration authority to verify the applicant's identity and other details, e.g. that the applicant has the private key corresponding to the public key to be bound to the certificate.

Root CA

See *Certification hierarchy*.

RCA (Root Certification Authority)

A Root CA, but, more particularly, emphasising the separation of the operational role of a peak body, from policy and accreditation functions.
See *APAA*.

RSA

A public key algorithm developed by Rivest, Shamir and Adleman which is currently one of the most widely used and implemented public key algorithms.

S/MIME (Secure multipurpose Internet mail extensions)

A protocol for secure electronic mail over the Internet.

Secret key

See *Private key*.

SET (Secure electronic transactions)

A protocol for accepting credit card payments over the Internet, designed by Mastercard and Visa.

SHA (Secure Hash Algorithm)

A one-way hash function developed by USA NIST and NSA for use with the Digital Signature Standard. SHA produces a 160 bit hash.

Signature dynamics

A form of electronic signatures which involves the biometric recording of the pen dynamics used in signing the document.

SMTP (Simple Mail Transfer Protocol)

A protocol used to transfer electronic mail on the Internet, defined in IETF STD 10.

SSL (Secure sockets layer)

A transport layer security protocol, originally developed by Netscape Communications Corporation, which provides confidentiality, integrity and authentication services to the upper layer protocols.

Symmetric algorithm

A cryptographic algorithm where the encryption key is the same as the decryption key.

Trojan horse

A program that appears to perform a useful function but also includes other hidden, unauthorised functionality, e.g. a program which appears to be an image viewer that will also silently delete key operating system files from the hard disk.

UN/EDIFACT (United Nations Electronic Data Interchange for Administration, Commerce and Transport)

A set of international standards for EDI message formats. It is one of two international standards describing the syntax of EDI transmissions. EDIFACT is administered by a working party of the United Nations Economic Commission for Europe (UN/ECE) and the syntax rules are published by ISO as ISO9735.

UNCITRAL (United Nations Commission on International Trade Law)

A Commission established by the General Assembly of the United Nations in 1966 to harmonise and unify the law of international trade.

Verisign

One of the first certification authorities to be set up, originally an offshoot of RSA Data Security Inc. Verisign has arguably issued more certificates than any other CA.

Web server

Software or specialised hardware which are capable of communicating with the HTTP protocol and are used to serve documents on the World Wide Web.

X.12

A set of standards for EDI messages, developed by ANSI.

X.400

A series of ITU recommendations for electronic messaging.

X.500

A series of ITU recommendations for directory services.

X.509

A standard which is part of the X.500 specification, which defines the format of a public key certificate.
See also *Certificate*.

APPENDIX C: USER AUTHENTICATION AND CRYPTOGRAPHY

Authentication

Authentication simply means checking that something is authentic - in other words verification, checking or testing validity. It is a very broad term which does not imply what is being verified, however it is often used to mean *user authentication.*

User Authentication

User authentication is industry jargon that refers to any methods used to check (ie authenticate) the **identity** of a user. One dictionary definition is "to establish the validity of a claimed identity". *User,* in this context, does not just refer to individual humans. It means any person, organisation, device, software application, etc, which is accessing a service or providing a service.

Other forms of Authentication

There are also other types of authentication of identity, but these may be considered forms of user authentication. For example:

- *authentication of the sender* of a message (note that this is separate to *message authentication*) eg by means of a digital signature on an email message.
- *authentication of receipt* of a message e.g. by obtaining a digitally signed receipt which contains the digital signature of the original message as a separate reply message.

User authentication is distinct from other forms of authentication that have nothing to do with checking identity. Some examples are:

- *message authentication,* which deals with authenticating the integrity of transmitted or stored data;
- *authentication of entitlement,* for example checking that someone is entitled to ride a bus, receive a pay-TV service, receive a concession, receive a government benefit (do they have a valid ticket, have they paid a subscription, do they have a concession card, are they eligible for Childcare Assistance and if so how much); and
- authentication of various physical attributes of a person, for example are they old enough to enter a hotel public bar, are they tall enough to ride a particular rollercoaster (note that this is a separate issue to use of biometrics).

Identification and User Authentication

Identification and *user authentication* are separate issues. Identification is "stating who you are". User authentication is the checking of the stated identity ("Prove that it is you."). Some examples are:

- the classic computer usage is to supply a User-ID (identification) and then supply a password (user authentication);
- in banking systems, the magnetic stripe card provides identification and testing knowledge of the PIN provides user authentication;
- for credit cards, the card provides identification and the signature provides authentication that the user authorised the transaction;
- call centres often ask for the caller's name (identification) then ask for other data eg mothers maiden name, date of birth, etc or a PIN (user authentication).

We can use the terms *identifier* and *authenticator* to refer to the information which is provided for identification and user authentication respectively.

Cryptographic Techniques for User Authentication

Cryptographic techniques can be used for *user authentication* . Two common approaches are challenge and response protocols, and digital signatures.

Challenge and Response Protocols

The most obvious way challenge and response protocols are used is when the user is directly presented with a challenge (typically a number of 8-16 digits) on a logon screen, to which they must provide the matching response (another similar size number) by entering the challenge into a device which calculates the correct response. The response is generated from the challenge essentially by encrypting the challenge under a secret key (using either public-key cryptography or symmetric cryptography). Each device has a different key, making them unique. The host or other device is able to check the response by decrypting the response to retrieve the challenge. The protocol is essentially proving that the user has control of the secret (key) without actually revealing the secret.

The challenge is typically based on a randomly generated number, so that the challenge for any particular logon attempt is unpredictable and previous challenge and response pairs cannot be recorded for fraudulent reuse.

In many protocols the challenge and response happen automatically without the user being aware of it. Most challenge and response protocols between two devices (eg between a smartcard and a card access device) are bi-directional so that both devices essentially generate a random challenge and check the response from the other device. This provides *mutual authentication*.

Digital Signatures

Digital Signatures have the advantage of being able to provide user authentication after-the-fact. No interactive protocol is required. At any time after a digitally signed message is received, the recipient can check the digital signature to authenticate the identity of the signer. Digital signatures also provide assurance over the *integrity* of the data in the message and prevent the signer from denying having signed it (*non-repudiation*).

User Authentication and Locking with Smartcards

In smartcard systems (and others), there may be several user authentication steps involved in performing a transaction. The first step may be user authentication to the smartcard itself (or to a specific application on the smartcard). This is also referred to as *unlocking*. Next, the smartcard may act as a proxy for the user and provide user authentication to the device or system which is communicating with the smartcard (eg card access device, remote host system, PC).

APPENDIX D: PUBLIC KEY CRYPTOGRAPHY

Cryptographic Security Services

Sensitive electronic transmissions can be made secure using state-of-the-art cryptography technology.

"*The basic function of cryptography is to separate the security of a message's content from the security of the medium over which it is carried.*" — Matt Blaze, AT&T Research.

Cryptography is the main technical tool used to provide data security. It is used to provide various security services such as:

- **confidentiality -** to ensure that only the intended recipients or authorised persons can read the data;
- **integrity** - to allow checking that the contents of documents or transmissions are unaltered;
- **authentication** of the sender of information - to allow checking that the sender is who they claim to be;
- **non-repudiation** - to prevent denial by the sender of having sent something (or to prevent denial of having sent a receipt for a previous message); and
- strong **access control**.

The methods used to provide these services include:

- encryption and decryption (for confidentiality);
- message authentication codes (for integrity);
- digital signatures (for integrity, authentication and non-repudiation); and
- "challenge and response" protocols (for access control), also known as "one-time passwords".

The underlying process used for all these methods is encryption. Confidentiality services use encryption directly. The other services make use of encryption in more complex ways.

Symmetric and Public Key Cryptography

There are two types of cryptography:

- Symmetric cryptography, which uses *symmetric* cryptographic algorithms. Simple symmetric algorithms were in existence before the Roman Empire.

- Public-key cryptography, which uses *asymmetric* cryptographic algorithms, also known as *public-key* algorithms. Public-key cryptography is based on mathematic techniques and was invented in the early 1970's.

Most modern data security products use both types of cryptography. Typically, traditional cryptography is used for encrypting data for confidentiality, while public-key cryptography is used to distribute traditional cryptography keys and for digital signatures.

Symmetric Cryptography

Traditional cryptography uses *symmetric algorithms* which are also called secret-key algorithms. The encryption key is the same as the decryption key and must be a shared secret between the sender and the receiver. The process of decryption is exactly the reverse of encryption and uses the same key. This is why it is called symmetric.

Symmetric algorithms are very fast to compute.

One of the most commonly known symmetric algorithms is the algorithm specified in the DES (Data Encryption Standard) specified in a USA Federal Information Processing Standard (FIPS) and subsequently in many other standards internationally including Australian standards.

Public-key Cryptography

Public-key cryptography uses public-key algorithms. These are also called *asymmetric algorithms* because the decryption key is different to the encryption key, although the two keys are related and must be generated as a pair. Public-key algorithms consist of mathematical computations using the key and the data, treating the data as a set of large numbers.

This newer approach to cryptography allows one key to be public, the *public key*, while the other key, called the *private key*, is a secret known only by the owner of the key pair. For encryption, a public key of the recipient is used to encrypt the message, and the matching private key of the recipient is used to decrypt the message. Anyone can encrypt a message but no-one else can decrypt the message because no-one else has the private key.

Public-key algorithms can be used to encrypt messages, authenticate users, exchange keys for use with symmetric algorithms, and to create digital signatures. However, most public-key algorithms can be used for only one or a few of these uses.

Public-key algorithms are computationally complex and are thousands of times slower than equivalent strength symmetric algorithms. This is the main reason why symmetric algorithms continue to be used in conjunction with public-key algorithms.

Commonly known public-key algorithms include RSA, DSA, El Gamal, and Diffie-Hellman.

Cryptographic Algorithms

An *algorithm* is a well-defined set of steps for doing something. *Cryptographic algorithms*, which are also called *ciphers*, take input data and convert it from an easily understood form to an incomprehensible form. This process is called *encryption*. The process can be reversed at some later stage (*decryption*) to retrieve the original data.

The encryption and decryption processes involve the algorithm, the data, and one or more *keys*. The algorithm specifies "how to do it"; the data and the keys are "what to do it with".

The input data can be any information that can be represented digitally, including computer files, electronic mail messages, and even audio and video signals such as telephone calls, radio, and television.

A key is simply another piece of data - effectively a large numerical value.

The decryption algorithm is effectively the inverse of the encryption algorithm. Both are cryptographic algorithms. When referring to cryptographic algorithms by name, both the encryption and decryption algorithms are included.

Cryptographic algorithms have a range of uses other than encryption, such as authenticating messages or data, authenticating users, and exchanging cryptographic keys. Some algorithms are suited only to a limited set of these purposes, possibly even excluding encryption itself.

Digital Signatures

Public key cryptography is used for digital signatures which provide:

- user authentication—users can be verified to be who they claim to be;
- integrity—information ends up at its destination as sent; and
- non-repudiation—the sender cannot deny having sent the information.

Using public key cryptography, users are able to uniquely identify themselves to the recipient(s) of their messages by digitally signing the messages with the user's appropriate private key. The recipient checks this signature by employing the sender's matching and widely known public key.

To generate a digital signature, a private key of the sender is used. The matching public key of the sender can then be used by anyone to check the signature. The digital signature can be distributed with the document, typically by appending it.

Digital signatures allow messages to be "signed" in a way that undeniably associates the signer of a message with its content. Like its conventional counterpart, a digital signature links a particular person to an electronic document and so allows authentication of the identity of the person who sent the document. However, it offers greater security than a hand-written

signature because it cannot be fraudulently applied to a different document. Furthermore, it can also verify that the document itself has not been altered in any way since it was digitally signed.

A digital signature is not a digitised image of a hand-written signature. It is a cryptographic checksum of the document.

Key Certificates

A key certificate is a small electronic document which is created by a Certification Authority to attest to the association of a particular public key with some other information, such as an identity. The certificate lists the identity of the subject, the public key of the subject, and other details such as the validity period. These details are signed by the Certification Authority by appending a digital signature. The signed data becomes the certificate.

It is often mistakenly assumed that there should be a one-to-one relationship between people and public keys. Each certificate makes a linkage between a particular public key and a particular identity. Neither the key nor the identity need be unique to that certificate. A single identity can be associated with multiple keys, used for different purposes, time periods, and so on. A single key could also be associated with more than one identity, however this is not recommended.

Certificates are not confidential and do not need any security protection because the digital signature of the certification authority can be used to ensure that the certificate is genuine, provided that the public key of the Certification Authority is reliably known.

A certificate in essence is a document signed (ie digitally signed) by the certification authority which states something like:

I, Certification Authority X, do hereby declare that the following public key belongs to person X and is valid from date 1 to date 2.

It may also state other things such as the purposes for which the certificate can be used (eg financial limits on the authority of a signature under the key in the certificate) and the policies under which the certificate has been issued (eg the level of assurance over the identity of the subject of the certificate).

The subject of the certificate is the person named in the certificate. This could be a person eg Kan Ishikawa or a role eg *Director, Quality Assurance*. Note that the certificate does not imply any level of trust in the subject her/himself. It simply associates the person with the public key, in a way that can be trusted, and makes no other representations about the subject. External parties can thus be assured that when they send messages confidentially using that public key that only the named subject will be able to read them, and that messages signed with the private key which matches the public key in the certificate could only have been signed by the subject of the certificate. This level of assurance is tempered

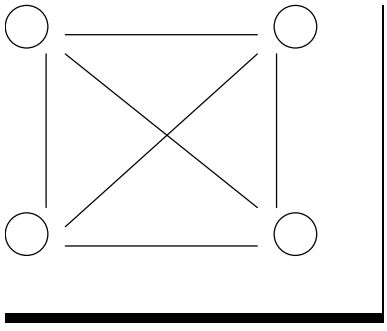
by the fact the subject needs to be exercising adequate control over the key, and that the key has not been revoked.

There is no assurance provided by the certificate that the recipient of the confidential information will not abuse the confidentiality by passing the information on to someone who should not see it. There is no assurance provided directly by the certificate that the a document signed by the subject was authored by the subject or that the subject has any claim over the intellectual property in the signed document or message, or that the subject will honour any commitment implied by the signed message. These issues need to be addressed in the normal manner as for paper documents.

Certification Authorities

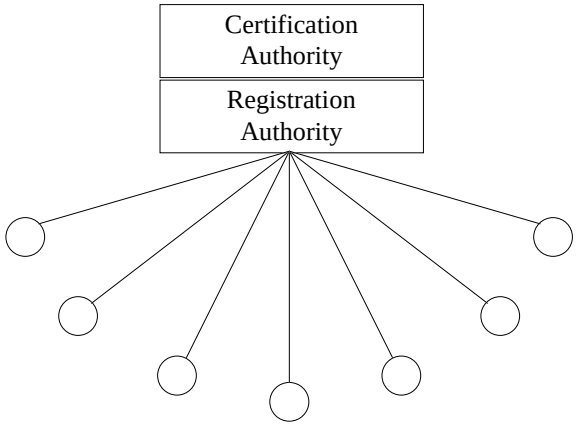
Because the public key of anyone can be widely known, at first glance public key cryptography allows secure messages to be exchanged without the need for advance arrangements between communicating parties. However, there is still a need for assurance about the ownership of public keys, so that confidential messages are not encrypted using the public key of an imposter instead of the intended recipient, and so that someone cannot fraudulently sign messages claiming to be you.

To set up secure communications, in the absence of Certification Authorities people could simply exchange public keys with each other directly using bilateral arrangements. However, public keys need to be exchanged in a manner that is trusted, so they could not be exchanged electronically. They would need to be exchanged by personally meeting, or sending a secure courier, etc. This would need to happen for each pair of people wishing to communicate. For four people, this would mean 6 meetings or couriers:



For 8 people, 28. For 100 people, 4,950. For 1000 people 499,500. (Mathematically, for *n* people this would mean *(n-1)+(n-2)* **+…**+1 bilateral arrangements.) For large numbers of people wishing to communicate this approach becomes impractical. (In jargon terms “it does not *scale* well.”)

Use of Certification Authorities (CA) provides a way of reducing the number of bilateral arrangements to manageable proportions. If each person can trust a CA then non-electronic bilateral arrangements only need to be made between each person and the CA, so only 1000 bilateral arrangements would be needed for 1000 people. (Mathematically the number of non-electronic bilateral arrangements is *n*.)

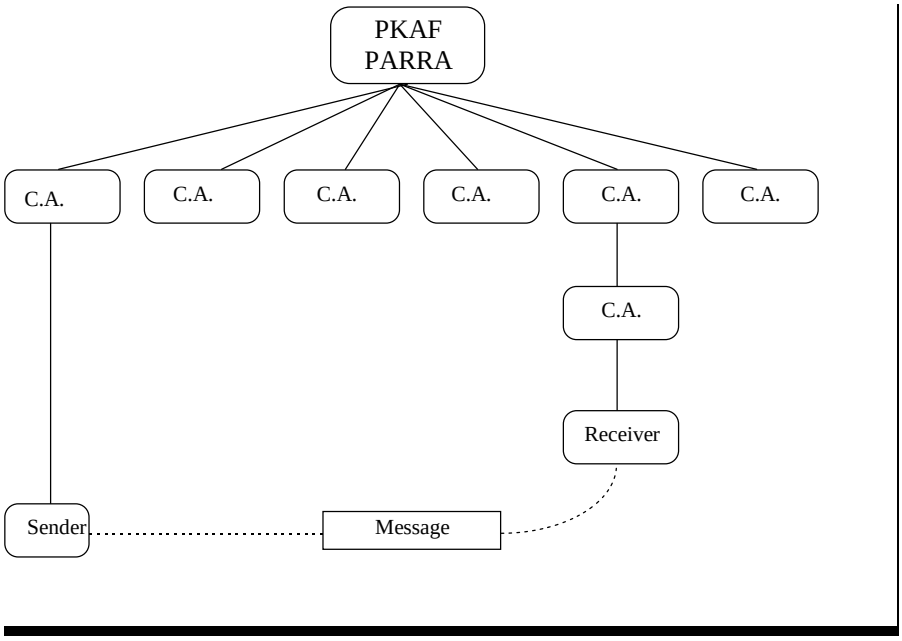


A Certification Authority[22] (CA) provides assurance that a public key does in fact belong to the person whose identity is being associated with that key. It does this by providing certificates.

The function of the CA is to securely issue and administer the components of public key security services such as digital certificates and encryption keys. A certificate is an electronic document that is digitally signed by the CA. The certificate contains various details including the name of the person for whom the certificate is for (the *subject*), the public key of the person, and validity dates. The certificate is said to *bind* the subject to the public key. Provided that everyone has obtained the public key of the CA in a way that can be trusted (via the non-electronic interaction with the CA), they can use that CA public key to check certificates from the CA to verify that the public key of another person does in fact belong to that person.

Expecting everyone in the world to interact with a single CA is not practical for various reasons, such as local coverage, sheer numbers, commercial competitive environments, etc. Consequently there needs to be a way for people who use different CAs to interact with each other. This is typically achieved by use of hierarchies of CAs. The approach is illustrated below as it has been proposed for the Australian Public Key Authentication Framework (PKAF) with the proposed Policy and Root Registration Authority (PARRA) as the *root CA.*

[22] Certification Authorities are also known as Key Certification Authorities (KCA) and Certificate Authorities.



Registration Authorities

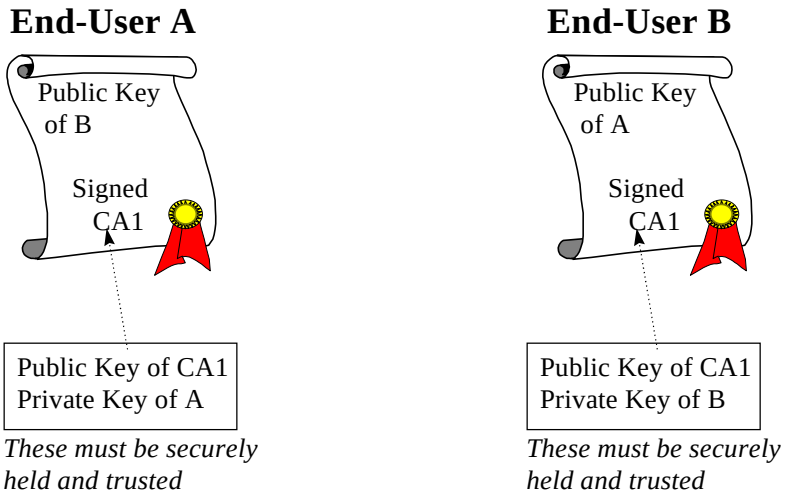
Certification Authorities work in conjunction with Registration Authorities (RA). The function of the RA is to reliably establish the identity of a user wishing to obtain keys and to establish secure means of communication with the CA. An RA does the actual checking of the identify of each user. It communicates securely with the CA to have certificates issued. Typically each CA will interact with multiple RAs.

In some cases the RA may be run by the same organisation that runs the CA. In other cases the RAs will be run by a separate organisation, such as the organisation to which the user belongs. In this case it is called an Organisation Registration Authority (ORA).

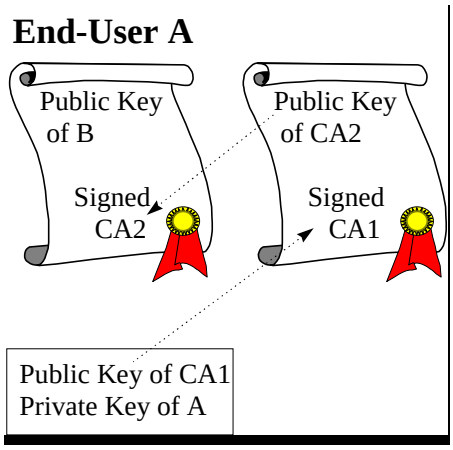
Cross-certification

If two end-users subscribe to the same CA service, they can check each other's certificates using the public key of that CA, provided that they can obtain that public key in an assured manner. This could be by obtaining it directly, outside of the normal electronic communication channels they use, or by obtaining it in another certificate which they can trust.

Ultimately one public key must be obtained in an "out-of-band" secure manner, such as by obtaining it by hand-delivery on some medium such as a floppy disk or a smartcard. All the other security rests on the trust in that public key.



If they subscribe to different CA services they can only check each other's certificates if there is a *chain* of certificates that leads back to the public key of a CA that they know and trust without reference to further certificates.



For practical, political and commercial reasons having everyone in the world use a single CA is not viable, so multiple CAs are likely to be used.

The certification of one CA by another is called cross-certification. A CA may determine to cross-certify another CA once it is assured that the policies, processes and technologies of the other CA are comparable and consistent with its own. Cross-certification could occur in one direction only.

Cross-certification provides a means by which a certificate issued by one CA will be recognised and accepted by another CA.

Certification Authority Hierarchies

Cross-certification becomes increasingly impractical for large numbers of CAs. To rationalise cross certification issues, CAs are often organised into hierarchies. Cross-certification can also be used in combination with CA hierarchies.

A Root Certification Authority is the top of a hierarchy of Certification Authorities (CA). It certifies the public keys of all the CAs directly below it in the hierarchy. These CAs may in turn certify the public keys of other CAs lower in the hierarchy, or certify the public keys of end-users directly.

There is no need for on-line connection between a CA and the entity below it. The lines in the diagram show the hierarchical relationship of certifying the public keys of each of the entities below, not an electronic connection.

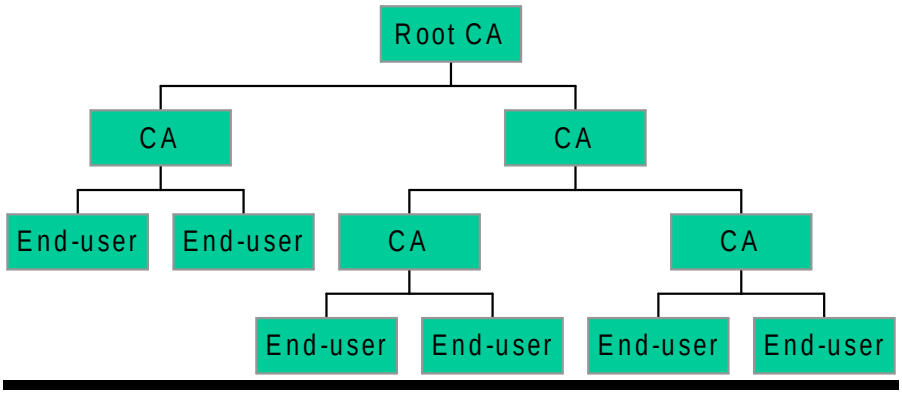


Figure 1 CA Hierarchy

For an end-user to check the certificate of any other user under the hierarchy, the chain of certificates always terminates in the public key of the Root CA.

Public Key Infrastructure

A Public Key Infrastructure (PKI) consists of CAs (possibly in a single hierarchy), policies and technical standards, and possibly legal support, to facilitate the use of public key cryptography technology.

APPENDIX E: INTERNATIONAL APPROACHES TO LEGISLATION AND PEAK BODY

Overview

Many governments across the globe have either enacted or are in the process of considering the enactment of legislation pertaining to the usage of digital signatures or other forms of electronic authentication. There are also a number of multi-national organisations which have developed or are developing model laws with regards to electronic authentication, such as the United Nations Commission on International Trade Laws (UNCITRAL) and the International Chamber of Commerce (ICC).

The Organisation for Economic Co-operation and Development (OECD) has not been directly involved in developing laws on electronic authentication, but remains on the fringe of the action with their laws and regulations on the usage of cryptography.

Model laws that are being developed by organisations in the United States of America, such as the American Bar Association (ABA) Digital Signature Guidelines and the work of the National Conference of Commissioners on Uniform State Laws (NCCUSL), have also been influential in the international arena.

The legislation that has been developed can be broadly divided into several distinctive categories. Debates continue as to whether there should be any legislation at all, and if so, which model of legislation should be used. Legislation has tended to adopt the X.509[23] model and largely deals with the usage of digital signatures in 'open' PKI model.

Open' and 'closed' PKI models

An 'open' PKI is defined as one where consumers obtain a single certificate which attests to their identity from a third party certification authority, and use the same certificate in transactions with potentially numerous merchants. A 'closed' PKI is one where a contract or a series of contracts identifies and defines the rights and responsibilities of all parties to a particular transaction or where the certificates are used only within a known, bounded context. [Biddle 1997]

Criticisms of the 'open' PKI model include the following:

- risk management in an 'open' PKI is fraught with problems. The scope of usage of the keypair is unlimited, thus making it difficult to quantify the liability exposure of the certification authority; [Biddle 1997]

[23] International Telecommunications Union (ITU) recommendation. The X.500 series of ITU recommendations for Directory Services are also international standards (with minor differences), developed jointly by ITU and ISO.

- there is a single point of attack. Since the certificate holder deals with only one keypair, there is only one private key that needs to be discovered for an attacker to, for all intents and purposes, masquerade as the certificate holder;
- there is greater incentive to attack a private key, since the key could potentially be used for unlimited purposes; and
- there could be privacy concerns associated with the 'personal digital trail' left by transactions authorised with the same keypair.

On the other hand, proponents of the 'open' PKI model argue that managing multiple keypairs and certificates could be too complicated and troublesome for users who are not well acquainted with the intricacies of doing so.

Most legislation deals with the usage of digital signatures in the context of an 'open' PKI.

In considering the issue of open versus closed systems, it is worth noting that [ILPF 1997] included the following comments:

> *"… this project was initially conceived in Spring 1996. At that time, it appeared that industry efforts were being primarily directed towards developing open systems and therefore that open systems were going to be the prevailing business model. In fact, in the period during which this Report was written, the open system model has appeared to become an increasingly less viable business model. Instead, we believe that many consumer transactions which utilize certificates will occur in a 'closed system' or 'closed loop' model."*

Legislative models

The legislation that has been enacted or being considered to date has tended to be of one of the following types:

1. a rule of equivalence which equates electronic records and signatures with their paper counterparts;
2. a framework of principles which defers to the specification of rules and regulations which are required to implement and govern the usage of electronic signatures to a statutory entity; or
3. a complete, prescriptive law, which includes the specification of regulations which govern the usage of electronic signatures.

Many of the recent laws in the second and third category also include rules of equivalence which are based on those included in the NCCUSL Uniform Commercial Code Article 2B and the UNCITRAL Model Law on Electronic Commerce 1996.

Rule of equivalence

[ISTEV 1997] describes the rule of equivalence as:

> *"… all the actual existing rules for hand written signature and paper document could be used also for digital signature and electronic document."*

[ILPF 1997b] chooses to describe the rule of equivalence as a 'signature-enabling' approach, and defines it as:

> *"The general laws permit any electronic mark that is intended to authenticate a writing to satisfy a signature requirement. … The net effect of this approach is to give legal recognition to both digital and electronic signatures for statutory and common law writing and signature requirements."*

This model merely introduces a clause which equates electronic signatures and records with their paper counterparts. It does not attempt to define what constitutes an acceptable electronic signature — this issue is left up to the courts. It is also silent on operational aspects and liability issues.

This is basically the approach which has been taken in the UNCITRAL Model Law on Electronic Commerce and the proposed Massachusetts Electronic Records and Signatures Act (MERSA).

Framework of principles

The framework of principles model is one where the legislation specifies principles underlying the law, but defers the specification of the rules and regulations required to implement and govern the usage of electronic signatures to a statutory entity. Most of the framework of principles model type of legislation use a criteria based definition of a signature, i.e. the definition of what constitutes a legally effective signature incorporates the requirements that the signature must fulfil in order to satisfy security and trustworthiness concerns.

One of the more prominent examples of the framework of principles legislation is the California Digital Signatures Bill (AB 1577). The California Bill leaves the implementation details to regulations adopted by the Secretary of the State. The California Bill uses a criteria based definition of acceptable electronic signatures. Under the California Bill, an electronic signature is acceptable if it has all of the following attributes:

1. it is unique to the person using it;
2. it is capable of verification;
3. it is under the sole control of the person using it; and
4. it is linked to data in such a manner that if the data is changed, the digital signature is invalidated.

The regulations, which have been released, define acceptable signature technologies based on these criteria. The regulations also specify the procedures for adding new signature technologies to the list of acceptable technologies. Criteria similar to those defined in the California Bill have been used in most of the framework of principles type legislation.

Complete, prescriptive law

[ISTEV 1997] describes this approach as one which:

> *"…define and rule every power and duty of trusted third parties, of private people and companies who intend to use digital signatures."*

[ILPF 1997b] describes it in further detail as:

> *"…a comprehensive effort that seeks to enable and facilitate electronic commerce with the recognition of digital signatures through a specific regulatory and statutory framework. It establishes a detailed PKI licensing scheme (albeit voluntary), allocates duties between contracting parties, prescribes liability standards, and creates evidentiary presumptions and standards for signature or document authentication."*

The most prominent example of the complete, prescriptive model is the Utah Digital Signature Act 1997. The Utah Act, which is based on the ABA Digital Signature Guidelines attempts to define a comprehensive scheme for the recognition of digital signatures in a state department licensed CA based PKI. There are four main categories to the Utah Act:

1. licensing of CAs;
2. issuance, suspension, and revocation of certificates issued by CAs;
3. duties, warranties, and obligations of licensed CAs, subscribers, third parties, and key repositories; and
4. rules regarding the recognition and validity of digital signatures. [ILPF 1997b]

The Utah/ABA model is described in further detail later in this document. The Utah/ABA model is the one which is most closely aligned with the model envisaged in the Australian PKAF Strategy Report. It should be noted that this model is increasingly falling out of favour internationally. Many of the countries and the U.S. states are opting for the alternative models described above, which are less prescriptive. International exceptions to this are Germany and Malaysia.

Characteristics of the legislation

The specifics of the legislation can also be categorised based on the following characteristics:

- technology neutrality;
- scope of the legislation;
- the definition of an electronic or digital signature;
- the voluntary or mandatory licensing of certification authorities;
- the issues relating to the establishment of a peak authority.

Technology neutrality

This has to do with whether or not the legislation deals specifically with digital signatures, as implemented with public key cryptographic systems, or with the more general issue of authentication using electronic or digital means. Legislation that is purely a rule of equivalence is generally technology neutral, i.e. its scope is not just limited to digital signatures, but also includes other forms of electronic signatures/authentication.

Technology specific legislation is designed to track technological capabilities very closely and tends to reflect current technical realities. Technology neutral legislation deliberately leaves the door open for several reasons:

- it is generally difficult to change legislation once it has been enacted;
- the technologies available are likely to change relatively quickly; and
- settling on one form of technology over others in legislation too early may distort the market for new, upcoming technologies.

Technology specific law that has been enacted to date have mostly been based on the hierarchical X.509 public key infrastructure model.

Scope of the legislation

Some of the enacted legislation has a very narrow scope, and deals specifically only with certain types of transactions, e.g. signing of health records, or with transactions between specified entities, transactions between the government and the public. Examples of this legislation includes much of what that has been enacted by the various state governments in the United States of America.

Some legislation has ‘general’ applicability, i.e. it covers all kinds of transactions, including those that take place between two private parties.

Definition of a signature

The definition of a signature tends to depend on the technology neutrality of the legislation. Some examples are:

1. The proposed Massachusetts legislation, which is a rule of equivalence, defines "electronic signature" as:

"any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual signature".

2. The Utah Digital Signature Act, which is a complete law, takes the prescriptive route of defining a "digital signature" as:

"a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:

(a) the transformation was created using the private key that corresponds to the signer's public key; and

(b) the message has been altered since the transformation was made.".

3. The Californian Digital Signature Act, which is a framework of principles, defines a set of criteria that have to be fulfilled for an electronic signature to be deemed acceptable:

   a) It is unique to the person using it.

   b) It is capable of verification.

   c) It is under the sole control of the person using it.

   d) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.

   e) It conforms to regulations adopted by the Secretary of State.

Licensing or registration of CAs

Most of the prescriptive legislation and the legislation based on a framework of principles includes guidelines dealing with the licensing or registration of CAs. In some cases, such as the Malaysian legislation, the licensing of CAs is compulsory, whereas in most others, the licensing of CAs is voluntary. In order to encourage the licensing, incentives such as liability limitations are given to the CAs if they are licensed. The proposed U.S. Electronic Financial Services Efficiency Act of 1997 (Baker Bill) registers CAs on the basis of membership of an industry association.

Issues relating to a peak authority

Most of the legislation makes provisions for the establishment of a peak body of some form or other to deal with matters pertaining to the usage electronic or digital signatures within the bounds of its geo-political authority. Pieces of legislation which include the licensing or registration of CAs tend to include the establishment of a peak authority which takes many forms, including the following:

- a Minister or the Secretary of State;
- a Federal regulatory authority or a State Government Department; and
- an industry association of CAs.

The peak authority also tends to be responsible for one or more of the following duties:

- formulation of policy, rules and regulations pertaining to the usage of electronic or digital signatures;
- enforcement of the rules and regulations that govern the usage of electronic or digital signatures;
- the licensing or registration of CAs;
- acting as the root CA;
- making the appropriate arrangements for the recognition of certificates issued outside the bounds of its geo-political authority.

Under most of the models, the peak authority is funded by the collection of membership dues, imposition of licensing fees and charging for services rendered.

Issues related to liability apportionment

Where the legislation has specified the voluntary licensing of certification authorities, there are usually several carrots thrown into the picture to encourage the licensing of certification authorities. For instance, the Utah Digital Signature Bill includes the limitation of the liability of a licensed CA to the stated reliability limit on the certificate, and evidentiary presumptions are made about a digital signature which is associated with a public key which has been certified by a licensed CA. This limitation of liability is seen by some to introduce market distortions.

Model laws, guidelines and frameworks

Many model laws and guidelines have been developed in response to the usage of electronic records and signatures, primarily in the context of commercial transactions. These model laws attempt to standardise and provide some uniformity in the legislation enacted by the various countries around the globe. They also provide the law makers with some insight into the thinking and the principles that underlie the laws.

Many of the model laws have been developed in the United States of America, where the various states tend to take a more fragmented approach to the enactment of legislation than in most other countries. The model laws include the Uniform Commercial Code and the Uniform Electronic Transactions Act that were developed by the NCCUSL and the ABA Digital Signature Guidelines.

In the international arena, UNCITRAL has been active in promulgating their Model Law on Electronic Commerce, and has been drafting a set of Uniform Rules on Digital Signatures and Certification Authorities. Other organisations that are developing their own guidelines with regards to electronic authentication include the ICC.

American Bar Association Digital Signature Guidelines

Summary: The American Bar Association (ABA) Digital Signature Guidelines is a set of guidelines with regards to general principles and operational obligations of the CA and the subscriber.

The Information Security Committee of the ABA started drafting a model law dealing specifically with digital signatures several years ago. However, due to numerous unresolved differences in opinion between members of the committee, the model law was never released. Instead, a set of Digital Signature Guidelines was released in its place. The Guidelines are not suitable for adoption as legislation and are not intended for that purpose. They are intended to assist in the drafting and interpretation of legislation. There are a lot of issues which are left unresolved in the Guidelines which will have to be cleared up before legislation is implemented.

The ABA Digital Signature Guidelines include a set of definitions and general principles. In addition to that, the Guidelines also specify operational obligations of the CA and the subscriber.

These Guidelines have been quite influential in the development of State legislation in the U.S. The Utah Digital Signature Act was largely developed by the same people who worked on these Guidelines, and generally adheres to the ABA Guidelines.

NCCUSL Uniform Commercial Code Article 2B

Summary: The NCCUSL UCC Article 2B includes a rule of equivalence which has been included in the legislation enacted by numerous States in the U.S.

Article 2B deals with transactions in information; it focuses on transactions relating to the ‘copyright industries’. Article 2B includes a rule of equivalence: “A record or authentication may not be denied legal effect, validity, or enforceability solely on the ground that it is in electronic form.” The drafting of Article 2B has been influenced by the UNCITRAL Model Law on Electronic Commerce 1996.

NCCUSL Uniform Electronic Transactions Act

Summary: The NCCUSL Uniform Electronic Transactions Act includes a rule of equivalence that provides legal recognition for electronic signatures. Additionally, signatures created by an electronic agent are deemed to bind the programmer/user of the agent.

The Act applies to electronic records and electronic signatures generated, stored, processed, communicated or used for any purpose in any commercial or governmental transaction. Section 301 of the November 1997 draft of the NCCUSL Uniform Electronic Transactions Act is a rule of equivalence that provides legal recognition for electronic signatures:

> (a) A signature may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic signature.
>
> (b) If a rule of law requires a signature, or provides consequences in the absence of a signature, that the rule of law is satisfied with respect to an electronic record if the electronic record includes an electronic signature.
>
> (c) A party may establish reasonable requirements regarding the method and type of signatures which will be acceptable to it.

Section 303 deems that signatures created by the operations of an electronic agent will bind the party that programs or selects the agent.

UNCITRAL Model Law on Electronic Commerce 1996

Summary: The UNCITRAL Model Law on Electronic Commerce is a framework of principles of law, with the addition of a few rules of equivalence. Its scope of application is limited to messages used in the context of commercial activities.

The UNCITRAL Model Law on Electronic Commerce is a framework of principles developed to facilitate global electronic commerce. It does not include all the rules and regulations necessary to implement the techniques set forth in the law. The Model Law is also based on a rule of equivalence which states that "Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message." (Article 5). The law applies to any data message that is used in the context of commercial activities.

The requirements for a signature are said to be met if a method is used to identify that person and to indicate that person's approval of the information contained in the data message and the method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstances, including any relevant agreement.

UNCITRAL Uniform Rules on Digital Signatures and Certification Authorities

Summary: The Uniform Rules on Digital Signatures and Certification Authorities is still in draft status. It is developed to harmonise laws relating to digital signatures and certification authorities. In line with the UNCITRAL Model Law on Electronic Commerce, the rules are likely to be media neutral.

The UNCITRAL Uniform Rules are still being drafted. They were developed in response to the need to harmonise the laws relating to digital signatures and certification authorities. It is also seen to promote the efficient utilisation of digital communication by establishing a security framework and giving written and digital messages equal status with regards to their legal effect. While paying special attention to digital signatures based on public key cryptosystems, it is generally felt that the Uniform Rules should be consistent with the media-neutral nature of the Model Law on Electronic Commerce.

The definition of a signature is similar to that of the Model Law on Electronic Commerce. However, in addition to that, a 'secure electronic signature' that has to meet the rules and regulations adopted has been defined. The Uniform Rules includes some guidelines with regards to CAs, such as the liability model used. In line with the International nature of its background, the Uniform Rules also include provisions for the recognition of foreign electronic signatures.

ICC GUIDEC

Summary: The ICC GUIDEC is a set of operational guidelines of limited scope dealing with transactions between commercial entities.

The International Chamber of Commerce (ICC) General Usage for International Digitally Ensured Commerce (GUIDEC) was created to "establish a general framework for the ensuring and certification of digital messages, based upon existing law and practice in different legal systems". [ICC 1997]

GUIDEC is limited in its scope—it deals only with transactions between commercial entities operating under lex mercatoria. The GUIDEC specifically does not deal with consumer transactions.

GUIDEC uses the term 'ensure' to denote the act of digitally signing an electronic document since it is felt that there is problem in the terminology given that a digital signature is not really a signature at all. GUIDEC deals primarily with the operational guidelines relating to the usage of digital signatures using public key cryptosystems.

The GUIDEC is not entirely technology specific—parts of the GUIDEC may be applied to other authentication methods.

European Commission

[EC 1997] indicated that regulatory inconsistencies between the member states of the European Commission (EC) should be discouraged, and thus, a coherent regulatory framework for electronic commerce should be created at European level.

The current EC position appears to be that they will not be enacting regulation for regulation's sake and in many cases, free movement of electronic commerce services can be effectively achieved by mutual recognition of national rules and of appropriate self-regulatory codes. Legislative actions should impose the fewest possible burdens on the market and keep pace with market developments. Legislation should also take account of business realities and meet general interest objectives such as privacy and consumer protection effectively and efficiently.

[EIF 1997] indicates that a common European framework for digital signatures and encryption should be in place by 2000 at the very latest. It is envisaged that common legal requirements will be established for CAs and common legal recognition of digital signatures will be implemented in all the member countries.

Enacted or proposed legislation and regulations

The legislation that is covered here is mainly legislation of the 'general' variety. Legislation that has been limited in scope has been omitted.

United States of America

Summary: Most States have legislation of very limited scope. Only a very limited number of States have 'general' legislation. There is significant fragmentation in the approaches taken by the States—three major models of legislation and hybrids of these models have been enacted to date. Several pieces of legislation have been proposed in Congress, but none have been passed to date.

Federal

Various electronic signature bills have been introduced in Congress, with the Electronic Financial Services Efficiency Act of 1997 (Baker Bill) and the Digital Signature and Electronic Authentication Law (SEAL) of 1998 being the latest. It appears that the Baker Bill is unlikely to be passed, and SEAL is a limited scope legislation relating only to usage of electronic authentication techniques by financial institutions.

States

Most of the states in the United States of America have enacted legislation of some sort that provide for the usage of electronic signatures under specified circumstances. The first piece of electronic signature related legislation to be passed was the Utah Digital Signature Act in 1995. Most of the legislation that has been enacted by the states have been limited in their transactional scopes, e.g. the laws only apply in transactions with the government, or in transactions with health care providers.

The 'Generalised' laws that have been enacted to date fall into four different categories:

- the Utah/ABA model, which is a complete, prescriptive model that is specific to digital signatures;
- the California model, which is a framework of principles which defers the specification of rules and regulations to another document;
- the Massachusetts model, which is purely a rule of equivalence; and
- hybrids of two or more of the models above, e.g. Illinois.

Comprehensive summaries of the legislation that has been enacted by the States in the United States of America can be found in [ILPF 1997b], [McBride 1998] and [Massachusetts 1997].

In light of the fact that these models tend to be quite different and have some degree of influence in the development of legislation globally, they are described in further detail below:

- Utah/ABA

  As the name of the model suggests, the Utah Digital Signature Act was largely influenced by the ABA Digital Signature Guidelines. It has the following characteristics:

  - The legislation is specific to the usage of digital signatures created with public key cryptosystems. It is highly prescriptive, and includes many of the rules and regulations required for the daily operation of CA related services, such as the auditing of licensed CAs;
  - The licensing of CAs is provided for in the legislation and is voluntary. The incentive for licensing takes the form of evidentiary presumptions of authenticity and liability limitations;
  - A Government department acts as the peak body, and is responsible for the creation and enforcement of other policies, rules and regulations pertaining to the legislation, licensing of CAs and the recognition of certificates issued by CAs in other jurisdictions; and
  - Private keys are considered to be personal property of the holder and they have a duty of reasonable care to safeguard the key against unauthorised usage.

- California

  The California model is a framework of principles which has the following features:

  - it is deliberately technology neutral and the uses a criteria-based definition of what constitutes an acceptable electronic signature, i.e. the signature has to be unique to the person using it, capable of verification, under the sole control of the person using it, linked to data in such a manner that if the data are changed, the signature is invalidated and adheres to the appropriate rules and regulations;
  - the rules and regulations are not part of the legislation, but deferred to another document. Under the Californian legislation, Secretary of State has the responsibility for creating rules and regulations.

  The current set of rules and regulations issued in California includes the following:

  - the inclusion of public key cryptosystem based digital signatures and signature dynamics as technologies deemed to be acceptable by the government, and provisions with regards to procedures for adding other technologies to the list of acceptable technologies;
  - the maintenance of a list of approved CAs by the California Department of Information Technology.

- Massachusetts

  The proposed Massachusetts Electronic Records and Signatures Act (MERSA) is a rule of equivalence based on the draft NCCUSL Electronic Transactions Act. MERSA includes the following rules:

  - A record may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic record. If a rule of law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies that rule of law.
  - A signature may not be denied legal effect, validity or enforceability solely because it is in the form of an electronic signature. If a rule of law requires a signature, or provides consequences in the absence of a signature, an electronic signature satisfies that rule of law.

- Illinois

  The Illinois Electronic Commerce Security Act is a hybrid of the various models:

  - It includes rules of equivalence based on the draft NCCUSL Electronic Transactions Act that deem the electronic form of records and signatures to be equivalent to their paper counterparts;

- It is a framework of principles in that it defers a lot of the rules, regulations and procedures to the Secretary of the State;
- The Illinois Act is both technology neutral and technology specific. It allows for the usage of electronic signatures in general, but it also includes specific provisions which relate to the usage of public key cryptosystems based digital signatures; and
- It includes the legalities associated with the issuance and revocation of certificates.

Denmark

Summary: No legislation to date. Some considerations being debated.

The Danish Ministry of Research and Information Technology was supposed to present a rule of equivalence to put electronic documents on an equal footing with paper documents during the 1996/97 Parliamentary Session. To date, no legislation has been passed in Denmark.

The Danish Government, in close cooperation with the DG XIII of the European Commission is organising the Copenhagen Hearing (23—24 April 1998) to clarify specific questions on the development and use of digital signatures.

Germany

Summary: Legislation specifying the circumstances under which digital signatures can be deemed secure was enacted in 1997. The Legal Ordinance which establishes the rules and regulations relating to the legislation is still being developed. Legislation dealing with the legal effect and validity of digital signatures is still being developed.

Article 3 of the Information and Communications Services Act 1997 deals with the general conditions under which digital signatures are deemed secure. CAs should be licensed. The legislation provides for a peak body in the form of the federal regulatory authority for telecommunications and posts. The peak body is responsible for:

- enforcing the rules and regulations relating to the usage of digital signatures;
- licensing other CAs;
- acting as a root CA; and
- charging fees and expenses incurred in the provision of public services.

The German legislation also specifically provides for the usage of pseudonyms, and the provision of reliable time stamping services by the CA. The legislation defers most of the rules and regulations to a Legal Ordinance (SigV). SigV provides operational guidelines to CAs, and is still being developed. The latest draft of SigV is dated 8 October 1997.

The German Federal Justice Ministry is in the process of drafting legislation that deals with the legal effect and validity of digital signatures.

Italy

Summary: Framework of principles legislation specific to digital signatures enacted in 1997. Regulations relating to the legislation were enacted in November 1997.

Italian legislation on electronic signatures was enacted on 15 March 1997. The Italian legislation is a framework of principles which deals specifically with digital signatures. The technical rules and regulations were enacted by Presidential decree in November 1997.

Certification authorities have to be registered by the Authority of Information Technologies. Section 10 of the Italian legislation specifically provides for the storage of a digital signature in a separate file and the association of a single digital signature with a set of documents. [Buonomo 1997]

United Kingdom

Summary: A Public Consultation Paper on the detailed proposals for legislation of the licensing of trusted third parties was issued in 1997. The consultation paper also included the escrow of encryption keys used for confidentiality by the trusted third party. No legislation has been enacted yet based on the consultation paper.

In March 1997, the U.K. Department of Trade and Industry introduced a Public Consultation Paper on Detailed Proposals for Legislation with regards to the Licensing of Trusted Third Parties (TTPs) for the Provision of Encryption Services.

All TTPs that offer services to the public must be licensed. The body in charge of licensing TTPs will initially be the Department of Trade and Industry, given its experience in licensing telecommunications companies. Additionally, TTPs are charged with the escrow of encryption keys used for confidentiality.

Japan

Summary: No legislation to date. Certification Authority Guidelines issued.

The Certification Authority Working Group (WG8) of the Electronic Commerce Promotion Council of Japan (ECOM) issued an alpha version of a set of guidelines for certification authorities in April 1997. The guidelines cover operational and managerial relating to the issuance, revocation, publication and archiving of certificates. To a certain degree, it also includes guidelines on policy creation and approval. The public key infrastructure specified in the guidelines conform to the strict X.509 hierarchy.

Malaysia

Summary: Prescriptive digital signature law (based on the Utah/ABA model) enacted in 1997. Licensing of certification authorities is mandatory. There are no licensed certification authorities yet, but a pilot project is currently bring run.

Malaysia enacted legislation in 1997 to provide for and regulate the use of digital signatures. Most of the rules and regulations of the Malaysian Digital Signature Bill 1997 are similar to that of the Utah Digital Signature Act: The main differences include the following features of the Malaysian Bill:

- licensing of certification authorities is mandatory, and penalties are imposed for the operation of unlicensed certification authorities. Written exemption from licensing has to be obtained from the Minister to operate an intra-organisational certification authority;
- procedural regulations related to the enforcement of the regulations, such as search and seizure, are included in the legislation;
- the form and structure of the peak body is largely left unspecified. The Minister is the topmost body of authority, and has to appoint a Controller of certification authorities who, in turn, is empowered to appoint officers and servants as necessary; and
- it is also unspecified if the peak body will act as the root certification authority.

There are no licensed CAs in Malaysia at present. MIMOS, which is a non-profit government owned research and development enterprise, has established a certification authority service, branded as *mTRUST*. *mTRUST* has been running some public pilot tests on their certification services since late December 1997 to raise public awareness of the usage of digital signatures. They are initially offering personal certificates for use with electronic mail and server certificates for web servers, and are planning to offer SET 1.0 certificates in future. [MIMOS 1997]

Singapore

Summary: Rule of admissibility of computer output as evidence enacted. Considering UNCITRAL Model Law on Electronic Commerce and a digital signature law (model unspecified).

Amendments made to the Singaporean Evidence Act in 1996 included the addition of two new sections (ss35 and 36) to provide for the admissibility of computer output as evidence. [Lim 1997] It specifies three circumstances where computer output is considered valid as evidence:

- where there is an express agreement between the proceedings that the authenticity and accuracy of the contents are not disputed;
- where it is shown that the computer output was produced by a process that has been checked, approved and certified as such by an appointed agency. It is presumed that the output from an approved process is correct, unless it can be proved to the contrary; and
- where it is shown that the computer output was generated by a system that was operating properly at all material times. In this case, where unapproved/uncertified processes are used, it is presumed that the output is unreliable unless proven to be so by the party tendering the evidence. [Goh 1996]

The Electronic Commerce Hotbed (ECH) Policy Committee has identified that there is a need for Singapore to conform to international standards and models, avoid over-regulation and also to retain the flexibility to adapt quickly to a changing world. It has recommended that Singapore enact a commercial code based on the UNCITRAL Model Law on Electronic Commerce, currently referred to as the Electronic Transactions Bill (ETB), and legislation to provide for the recognition of digital signatures and a public key infrastructure with certification authorities.

It is envisaged that the issues addressed by the ETB will include the following:

- the authentication of the identity of the originator of electronic records and messages;
- the legal recognition of electronic signatures;
- the retention of records by electronic means;
- the integrity of electronic records transmitted over networks;
- legal responsibilities of service providers;
- the formation and validity of electronic contracts;
- the legislative framework for certification authorities and digital signatures; and
- cross certification of foreign digital signatures. [Lim 1997]

South Korea

Summary: Limited rule of equivalence enacted.

The draft Bill on Promotion of Trade Business Automation contains a provision which states that digital signatures of electronic documents for application or for approval shall be regarded as properly signed as stipulated by the laws and decrees relative to trade. [Hof 1998]

Functions and structure of the peak body

Technology (is the legislation technology specific):

- DS: Digital signatures only
- ES: Electronic signatures in general

Licensing of CAs (with regards to offering of services to the public):

- M: Mandatory
- V: Voluntary
- N: No licensing

Peak body functions:

- F: Policy formulation
- E: Policy enforcement
- L: Licensing of CAs
- R: Root CA
- I: Cross jurisdictional arrangements

Items that are in italics have been enacted, the others are proposals.

Country/Legislation	Techno-logy	CA Licensing or Register	Peak body	Peak body functions	Structure	Funding	Notes
Germany/Digital Signature Law 1997	*DS*	*V*	*Telecommunications federal regulatory authority*	*ELR*	*Federal regulatory authority*	*Charge for services rendered*	
Italy/1997	*DS*		*Authority for Information Technology In Public Administration (AIPA)*	*FEL*	*Government department?*		
United Kingdom/ TTP proposal	DS	M	Department of Trade and Industry	L	Government department		
Malaysia/Digital Signatures Bill 1997	*DS*	*M*	*Minister*	*FELI*	*Minister to appoint a Controller of CAs, Controller to appoint officers and servants as necessary*		

Country/Legislation	Techno-logy	CA Licensing or Register	Peak body	Peak body functions	Structure	Funding	Notes
USA/Electronic Financial Services Efficiency Act 1997 (Baker Bill)	ES	M	National Association of Certification Authorities	FELI	Industry association	Charge for services rendered, membership	
USA/Florida Electronic Signature Act 1996	*ES, DS*	*V*	*Secretary of State*	*FELI*			
USA/Utah Digital Signature Act 1996	*DS*	*V*	*Division of Corpora-tions and Commercial Code within the Utah Department of Commerce*	*FELIR*	*Government department*	*Charge for services rendered*	
USA/ Massachussetts Electronic Records and Signatures Act	ES	Not applicable. This is purely a law of equivalence.					
USA/California AB 1577 1995, Regulations 1997	*ES*	*M?*	*Secretary of State*	*R*			
USA/Illinois Electronic Commerce Security Act	*ES, DS*		*Secretary of State*	*FEL*		*Charge for services rendered*	

References

[ABA 1996] American Bar Association "Digital Signature Guidelines" 1996

[Argentina 1997] Argentina Resolution 45/97 <*http://www.sfp.gov.ar/firma.html*> <*http://www.jus.gov.ar/firma/index.html*>

[Biddle 1997] Biddle, C. B. "Legislating Market Winnners: Digital Signature Laws and the Electronic Commerce Marketplace", World Wide Web Journal, Volume 2, Issue 3 (Summer 1997), 1997

[Buonomo 1997] Buonomo, G. "Italian Laws and Regulations Concerning the Creation, Storage, and Transmission of Documents by Means of Computer-Based Systems and Digital Signature", Presentation at the OECD Workshop on Cryptography Policy, Paris, 9-10 December 1997 <*http://www.oecd.org/dsti/sti/it/secur/act/emef21.pdf*>

[EIF 1997] European Internet Forum (an initiative of DGXIII of the European Commission) "Towards a European Framework for Digital Signatures and Encryption" Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on ensuring Security and Trust in Electronic Communication (COM (97)503) <*http://www.ispo.cec.be/eif/policy/97503.html*>

[EC 1997] "A European Initiative in Electronic Commerce" Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions (COM (97)157) <*http://www.cordis.lu/esprit/src/ecomcom.htm*>

[ECOM 1997] Electronic Commerce Promotion Council of Japan (ECOM) "Certification Authority Guidelines" April 1997 <*http://www.ecom.or.jp/eng/output/ca/eng-guideline.htm*>

[Florida 1996] Florida Department of State (Digital Signature Advisory Committee) "Report to the Joint Legislative Committee on Information Technology Resources", 30 November 1996 <*http://www.dos.state.fl.us/digsig/finalreport.html*>

[Germany 1997] German Information and Communication Services Act 1997 and related documents <*http://www.iid.de/rahmen/*>

[Goh 1996] Goh, S. H. "Policy Implications of the Internet in Singapore" 1996 <*http://www.ncb.gov.sg/nii/96scan5/shamic1.html*>

[ICC 1997] International Chamber of Commerce "GUIDEC: General Usage for International Digitally Ensured Commerce" <*http://www.iccwbo.org/guidec2.htm*>

[ILPF 1997] Internet Law and Policy Forum "The Role of Certification Authorities in Consumer Transactions" Report of the ILPF Working Group on Certification Authority Practices, 14 April 1997 <*http://www.ilpf.org/work/ca/draft.htm*>

[ILPF 1997b] Internet Law and Policy Forum "Survey of Electronic and Digital Signature Legislative Initiatives in the United States", 12 September 1997 <*http://www.ilpf.org/digsig/digrep.htm*>

[ISTEV 1997] ISTEV "Legal and Regulatory Issues for the European Trusted Services Infrastructure — ETS" 1997 <*http://www.cordis.lu/infosec/src/stud2fr.htm*>

[Italy 1997] Italian Digital Signature Legislation and related documents <*http://www.notariato.it/forum/*>

[Lim 1997] Lim, C. "Building a Legal Framework for Electronic Commerce" November 1997 <*http://www.ech.ncb.gov.sg/view/ech/powerpoint/CharlesLim/sld001.html*>

[Malaysia 1997] Malaysian Digital Signature Bill 1997 <*http://www.mycert.org.my/digital.html*>

[MIMOS 1997] MIMOS "MIMOS initiates the First Public Key Infrastructure Pilot in Malaysia", Press release, 23 December 1997 <*http://www.mtrust.com.my/press/press1.html*>

[Massachussetts 1997] Commonwealth of Massachussetts "State Government Electronic and Digital Signature Legislation" <*http://www.magnet.state.ma.us/itd/legal/sigleg7.htm*>

[McBride 1998] McBride Baker & Coles "Summary of Electronic Commerce and Digital Signature Legislation", Version of 18 March 1998 <*http://www.mbc.com/ds_sum.html*>

[UK 1997] United Kingdom Department of Trade and Industry "Licensing of trusted Third Parties for the Provision of Encryption Services" Public Consultation Paper on Detailed Proposals for Legislation", March 1997 <*http://dtiinfo1.dti.gov.uk/pubs/*>

[UNCITRAL 1997] UNCITRAL "UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996" 1997 <*http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm*>

[UNCITRAL 1997b] UNCITRAL "Draft Uniform Rules on Electronic Signatures" 12 December 1997

[UNCITRAL 1998] UNCITRAL "Report of the Working Group on Electronic Commerce on the Work of its Thirty-Second Session" 10 February 1998

[Hof 1998] van der Hof, S. and Koops, B. J. "Digital Signature Law Survey" Version 2.2, January 1998 <*http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm*>

APPENDIX F: NON-LEGISLATIVE PKI INITIATIVES

Government

Many of these non-legislative PKI initiatives are limited in scope to transactions with the Government.

United States of America

NIST has been coordinating the efforts to set up a Federal Public Key Infrastructure for quite a while. The U.S. Federal PKI initiative appears to be limit its scope to transactions within and with the Government. A lot of valuable work has been done with regards to the specification of the operational guidelines, but it has yet to be implemented.

Canada

Instead of focusing on legislation, the Government of Canada has chosen to focus on developing a Government of Canada Public Key Infrastructure (GOC PKI). The GOC PKI provides a basis for the use of digital signatures and secure internal and external secure electronic transactions. It is envisaged that the GOC PKI will be fully implemented by end of 1998. The policies relating to the GOC PKI will be developed by the Policy Management Authority (PMA), which is an inter-departmental committee chaired by the Treasury Board Secretariat.

The technology used in the GOC PKI is provided by Entrust.

Australia

The Office of Government Information Technology (OGIT) is in the process of developing a government public key infrastructure, Project Gatekeeper.

European Commission

DGXIII INFOSEC has had 8 projects, some of which include pilot trials, running since January 1997:

- **Oparate** (OPerational and ARchitectural Aspects of TTPs for Europe)

  Oparate seeks to investigate the operational and architectural aspects of TTP service provision. The scope of the project includes organising a TTP to provide services effectively and how different systems may be combined or made to interoperate. A field trial is being conducted with 3 interworking CAs in France, Belgium and Netherlands.

- **Eurotrust**

  Eurotrust is a an effort at designing a pan-European TTP hierarchy, operate a pilot certification service, assess the operability of the service and based on that, plan a commercial service. The deliverables of this project include a certification policy statement, the pilot infrastructure and an assessment report to the Commission

  The trust model used is based on the X.509 hierarchy, with a Top Level CA (TLCA) at the European level, a Policy CA (PCA) at the National level, and an Organisation CA (OCA) at the organisational level.

- Oscar (Open Signature Certification ARchitecture)

  Oscar deals with the specification of the functional requirements and design of a TTP service to support digital signatures which is adapatable to the range of needs of user communities across Europe and provides a basic level of interoperability between communities. Requirements were gathered from user communities, a demonstration pilot was developed and the functional design and pilot assessed by a user community.

  Oscar uses the X.509 certificate infrastructure, and includes trusted time stamping services.

- **Krisis** (Key Recovery in Secure Information Systems)

  Krisis deals with key recovery in confidentiality services. It involves:

  - the collection of commercial requirements for a pan-European confidentiality service;
  - the comparison of different key management and key recovery schemes from a commercial point of view;
  - an analysis of the interoperability aspects of key recovery schemes;
  - establishing a pilot infrastructure for key recovery with centers in five European countries:
    - France (operated by Bull Ingenierie)
    - Germany (operated by IABG)
    - The Netherlands (operated by Philips Crypto)
    - Switzerland (operated by r3 security engineering)
    - United Kingdom (operated by DERA)
  - developing the technical and policy requirements based on the results of the pilot.

It appears as though commercial companies see a need for key recovery for data stored on permanent devices, but prefer to operate the scheme themselves. Foreign key recovery centers were generally unacceptable, as are government operated ones. Local key recovery centers operating under strict legal control are acceptable only if there is a choice of centers. The companies would prefer to use a single scheme on an international basis.

The four schemes that will be analysed as part of the project are:

- IBM SecureWay
- CertCo SecureKEES
- Royal Holloway
- TIS RecoverKey

- **Mandate**

  Mandate is an implementation of electronic cheques.

- **Aequitas**

  Aequitas is a project set up to study the legality of encrypted electronic messages as proof in criminal litigations. Ad Aequitatem is an experimental TTP service set up at the University of Zarazoga. The certification authority used is FESTE.

- **Euromed-ETS**

  Euromed is a TTP service for health care in Europe.

- **Eagle**

  Eagle is a study on the commercial aspects of TTPs and the regulatory situation and plan in Germany, France, Netherlands, United Kingdom and Sweden.

There are several new projects which have just commenced, most of which are to finish at the end of 1998:

- Keystone, which is the specification of a cross-domain public key infrastructure architecture for Europe, based on the results of previous INFOSEC and ACTS projects;
- A study which examines the legal issues of evidence and liability in the provision of trusted third party services, of which the deliverables include guidelines for harmonisation of European evidence law and European TTP services;
- Bests, which is a business environment study of trusted services, which among other things, looks at the legal issues and business issues related to the provision of TTP services such as potential liabilities, cross-border issues, operational costs and options for cost-recovery or profit making, licensing procedures and self-regulation issues; and
- Comets, which is to develop a financial model and guidelines to show the viability of TTP services on the basis of the analysis of business and legal elements, taking into account technical, business and regulatory cost factors.

ICE-TEL

The ICE-TEL project which has been running since mid-1996 seeks to establish a large scale public key certification infrastructure in a number of European countries that caters to industrial and academic research users of the Internet. ICE-TEL is funded by the Telematics for Research Initiative within the European Telematics Applications Programme of the European Commission.

The project includes the following:

- development and deployment of the tools required for the provision of the security infrastructure on a variety of platforms (Unix, PC, Macintosh);
- development and deployment of security toolkits to integrate the public key based security services into any application;
- development and deployment of security enabled user services which allow the use of the certification infrastructure without further application integration;
- support the integration of security services into applications and provide secure testbeds for applications.

The applications that have been selected to test the tools:

- secure communication between administrations and electronic request and delivery of documents in the region of Torino, coordinated within the EU-sponsored “Information Society Network”;
- secure communication between national Computer Emergency Response Teams (CERTs) and other distributed network support groups; and
- provision of a security enabled electronic Directory service for a large British research agency.

The ICE-TEL project uses a hybrid X.509 and PGP trust model. There is a top level CA which is responsible for certifying the PCAs. The initial root CA was run by GMD Darmstadt in Germany. PCAs have been set up in Norway, Sweden, Slovenia, Austria, Italy, Portugal, Denmark, United Kingdom and Spain.

The Phase II X.509 v3 certification infrastructure is being established. The current root CA is run by UNI-C in Denmark.

IETF/IAB

There are some standards that have been or are being developed by the IETF (Internet Engineering Task Force) which deal with standards related to the establishment of a public key infrastructure. These include:

- Privacy Enhanced Mail (PEM);
- Domain Name System Security Extensions (DNS-SEC);
- Simple Public Key Infrastructure (SPKI); and

- Public Key Infrastructure, X.509 based (PKIX).

The trust model used in PEM is X.509 based. PEM is currently not in widespread use, since PGP and S/MIME emerged as the early winners in the standards fight. The trust model used in DNS-SEC is similar to the hierarchical tree structure of DNS. The trust model used in SPKI is based on SDSI, and is very different from current existing proposals. The PKIX working group is defining protocols to establish an X.509 certificate based public key infrastructure.

Private enterprise CAs

There are quite a number of CAs which have been set up in the absence of any legislation. Many of these CAs issue certificates to organisations in geo-political jurisdictions outside of that of the CA. Examples of these CAs include Verisign (U.S.) and Thawte (South Africa) and in Australia: Australia Post, KPMG, Telstra, Signet, and Certificates Australia.

These companies have effectively developed a public key infrastructure in the absence of specific legislation. Contractual arrangements are used to cover most of the issues related to liabilities and most of the companies have issued their own certification practices statements. The public keys of the CA are distributed as part of software packages such as the Netscape Communicator and Microsoft Internet Explorer, and are also downloadable from the CA's WWW site. In practical usage terms, the public key infrastructure set up by these CAs is probably the most widespread in the world.

Certificates are issued in different classes, with each class serving a different purpose and/or having different levels of assurance. These certificates, which are currently actively used on the Internet, include:

- server certificates for use with SSL-enabled web servers;
- SSL client certificates (some classes of very low assurance, which just serve to bind the public key to an electronic mail address, some classes of higher levels of assurance for which verification of photo-identification is required);
- personal certificates for use with S/MIME-enabled mail; and
- software providers certificates for use with code-signing initiaves.

The SET certificate management architecture makes use of X.509v3 certificates. The SET specification includes several levels of CAs, including the SET Root CA, the Brand CA (BCA), Geo-political CA (GCA), Policy CA (PCA), Merchant CA (MCA), Client CA (CCA). Most of the CAs that are currently in operation are contemplating issuing SET certificates in the near future.

References

NIST Federal PKI project materials <*http://csrc.ncsl.nist.gov/pki/*>

ICE-TEL project materials <*http://www.darmstadt.gmd.de/ice-tel/*>

INFOSEC materials <*http://www.cordis.lu/infosec/*>

GOC PKI materials <*http://www.cse.dnd.ca/cse/english/gov.html*>

Project Gatekeeper materials
<*http://www.ogit.gov.au/gatekeeper/index.html*>

APPENDIX H - BIBLIOGRAPHY AND ADDITIONAL REFERENCE MATERIAL

General PKI related material

Lists of links

Avellan, J. "Digital Signatures Links" <*http://www.qmw.ac.uk/~tl6345/*>

Branchaud, M. "PKI Survey — References" <*http://www.xcert.com/~marcnarc/PKI/*>

Caldwell, K. "Software Industry Issues: Digital Signatures" <*http://www.softwareIndustry.org/issues/1digsig.html*>

Commonwealth of Massachusetts, Information Technology Division Legal Department "The PKI Page" <*http://www.state.ma.us/itd/legal/pki.htm*>

European Commission Legal Advisory Board "Digital signatures and encryption" <*http://www2.echo.lu/legal/en/ecommerc/digsig.html*>

ICRI "DigiSig Links" <*http://www.law.kuleuven.ac.be/icri/projects/digisig_lb_eng.htm*>

ILPF "Selected Bibliography on Certification Authorities and Digital Signature Reference Material", Appendix 5 of The Role Of Certification Authorities In Consumer Transactions, A Report Of The ILPF Working Group On Certification Authority Practices" <*http://www.ilpf.org/work/ca/app5.htm*>

Kelm, S. "Comprehensive list of Public Key Infrastructure (PKI) links" <*http://www.pca.dfn.de/eng/team/ske/pem-dok.html*>

Papers

Biddle, C. B. "Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure", San Diego Law Review, Vol. 33, November 1996 <*http://www.softwareIndustry.org/issues/docs-org/digsig.pdf*>

Biddle, C. B. "Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace", World Wide Web Journal, Volume 2, Issue 3 (Summer 1997), 1997

Biddle, C. B. "Public Key Infrastructures And Digital Signature Legislation: 10 Public Policy Questions", Lunchtime Workshop, CFP 1997, <*http://www.state.ma.us/itd/legal/biddle1.htm*>

Bender, N. S. "Digital Commerce and the Utah Digital Signature Act" <*http://www.law.miami.edu/~bender/internt.html*>

Berkovits, S., S. Chokhani, J. A. Furlong, J. A. Geiter and J.C. Guild "Public Key Infrastructure Study: Final Report", MITRE Report for NIST, 1994 <*http://csrc.ncsl.nist.gov/pki/documents/mitre.ps*>

Blaze, M., J. Feigenbaum and J. Lacy "Decentralized Trust Management (PolicyMaker)" AT&T Research, 1996 *<ftp://research.att.com/dist/mab/policymaker.ps>*

Blaze, M., J. Feigenbaum and A. D. Keromytis "The Keynote Trust Management System", March 1998, *<http://search.ietf.org/internet-drafts/draft-angelos-spki-keynote-00.txt>*

Branchaud, M. "A Survey of Public-Key Infrastructures", McGill University, March 1997 *<http://www.xcert.com/~marcnarc/PKI/thesis/>*

Burr, W. "Public Key Infrastructure Technical Specifications: PartC: Concept of Operations: TWG-96-102", Version 2.3, 25 November 1996 *<http://csrc.nist.gov/pki/twg/conops.ps>*

Information Technology Security Strategy Legal Issues Working Group, Government of Canada Electronic Commerce Secretariat "A Survey Of Legal Issues Relating To The Security Of Electronic Information", June 1995 *<http://canada.justice.gc.ca/Commerce/index_en.html>*

Chadwick, D. W., A.J. Young and N. Kapidzic Cicovic "Merging and Extending the PGP and PEM Trust Models — The ICE-TEL Trust Model", 1997 *<http://fw4.iti.salford.ac.uk/ice-tel/trust/ieee/>*

Ellison, C. "Establishing Identity Without Certification Authorities", Proceedings, 6th USENIX Security Symposium, San Jose, 1996 *<http://www.clark.net/pub/cme/usenix.html>*

European Internet Forum (an initiative of DGXIII of the European Commission) "Towards a European Framework for Digital Signatures and Encryption", Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on ensuring Security and Trust in Electronic Communication (COM (97)503) *<http://www.ispo.cec.be/eif/policy/97503.html>*

European Commission "A European Initiative in Electronic Commerce" Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions (COM (97)157) *<http://www.cordis.lu/esprit/src/ecomcom.htm>*

Florida Department of State (Digital Signature Advisory Committee) "Report to the Joint Legislative Committee on Information Technology Resources", 30 November 1996 *<http://www.dos.state.fl.us/digsig/finalreport.html>*

Ford, W. "A Public Key Infrastructure for U.S. Government Unclassified but Sensitive Applications", NORTEL Federal Systems report for NIST, 1 September 1995 *<http://csrc.ncsl.nist.gov/pki/documents/fordrept.ps>*

Ford, W. "Strawman Certificate Policy Definitions: Mid-Level Policies for Digital Signature and Encryption", Report for Government of Canada Policy Management Authority Committee, 29 April 1997 *<http://www.state.ma.us/itd/legal/straw5.htm>*

Froomkin, M. "Digital Signatures Today", Proceedings, Financial Cryptography 1997, *<http://www.law.miami.edu/~froomkin/articles/digsig1.pdf>*

Froomkin, M. "The Essential Role of Trusted Third Parties in Electronic Commerce", 75 Oregon Law Review 49, 1996
<http://www.law.miami.edu/~froomkin/articles/trusted.htm>

Greenwood, D. "Electronic Signatures And Records: Legal, Policy And Technical Considerations", 1997 *<http://www.state.ma.us/itd/legal/e-sig.htm>*

ILPF Working Group on Certification Authority Practices, "The Role of Certification Authorities in Consumer Transactions" Report of the ILPF Working Group on Certification Authority Practices, Internet Law and Policy Forum, 14 April 1997
<http://www.ilpf.org/work/ca/draft.htm>

ISTEV "Legal and Regulatory Issues for the European Trusted Services Infrastructure—ETS" 1997 *<http://www.cordis.lu/infosec/src/stud2fr.htm>*

Masse, D. G. and A. D. Fernandes "Economic Modelling and Risk Management in Public Key Infrastructures", 15 April 1997 *<http://www.chait-amyot.ca/docs/pki.html>*

Maurer, U. "Modelling a Public-Key Infrastructure", Proceedings of the 1996 European Symposium on Research in Computer Security (ESORICS '96), 1996
<ftp://ftp.inf.ethz.ch/pub/publications/papers/ti/isc/Pub_Key_Model.ps>

Nazario, N. "Federal Public Key Infrastructure Technical Specifications, Part B: Technical Security Policy TWG96-001", Version 1, 24 January 1996
<http://csrc.ncsl.nist.gov/pki/tspolicy.ps>

NIST "Public Key Infrastructure Technology", ITL Bulletin, July 1997
<http://www.nist.gov/itl/lab/bulletns/july97bull.htm>

NIST "Federal Public Key Infrastructure Technical Specifications, Part A: Requirements for the Federal Public Key Infrastructure", Version 1, 31 January 1996, *<http://csrc.ncsl.nist.gov/pki/require5.ps>*

NIST "Federal Public Key Infrastructure Technical Specifications, Part D: Interoperability Profiles", 27 September 1995 *<http://csrc.ncsl.nist.gov/pki/cross.ps>*

OECD, "OECD Emerging Market Economy Forum: Workshop on Cryptography Policy", Maison de la Chimie, Paris, 9–10 December 1997,
<http://www.oecd.org/dsti/sti/it/secur/act/emef.htm>

Rivest, R. and B. Lampson "Simple Distributed Security Infrastructure 1.0"
<http://theory.lcs.mit.edu/~cis/sdsi.html>

Rivest, R. and B. Lampson "Simple Distributed Security Infrastructure 2.0"
<http://theory.lcs.mit.edu/~cis/sdsi.html>

Wright, B. "Electronic Commerce Legislation Frequently Asked Questions"
<http://www.state.ma.us/itd/legal/wright1.htm>

Zimmerman, P. "PGP 5.0 User's Guide"

PKI Projects and Studies

Government of Canada PKI *<http://www.cse.dnd.ca/cse/english/gov.html>*

United States Federal PKI *<http://csrc.ncsl.nist.gov/pki/>*, *<http://gits-sec.treas.gov/fpki.htm>*

ICE-TEL *<http://www.darmstadt.gmd.de/ice-tel/>*

INFOSEC ETS, European Commission DG XIII *<http://www.cordis.lu/infosec/src/ets.htm>*

PKI related standards (and standards under development)

Ellison, C. "SPKI Certificate Documentation"
<http://www.clark.net/pub/cme/html/spki.html>

Ellison, C. "SPKI Requirements" *<http://www.clark.net/pub/cme/html/spki-reqts.html>*

IETF PKIX Working Group "PKIX Charter"
<http://www.ietf.org/html.charters/pkix-charter.html> (see also PKIX Internet Drafts linked in from this page)

IETF SPKI Working Group "SPKI Charter"
<http://www.ietf.org/html.charters/spki-charter.html> (see also SPKI Internet Drafts linked in from this page)

Legislation

Summaries

Commonwealth of Massachusetts, Information Technology Division Legal Department "State Government Electronic and Digital Signature Legislation"
<http://www.state.ma.us/itd/legal/sigleg7.htm>

van der Hof, S. and Koops, B. J. "Digital Signature Law Survey", Version 2.2, January 1998 *<http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm>*

Koops, B. J. "Crypto Law Survey" Version 12.1, March 1998
<http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>

Morgan, J. P. and A. Gidari "Survey of Electronic and Digital Signature Legislative Initiatives in the United States", Internet Law and Policy Forum, 12 September 1997 *<http://www.ilpf.org/digsig/digrep.htm>*

Smedinghoff, T. J. "Summary of Electronic Commerce and Digital Signature Legislation", McBride Baker & Coles *<http://www.mbc.com/ds_sum.html>*

Legislation (enacted and proposed) and related material

Argentina

Argentina Resolution 45/97 *<http://www.sfp.gov.ar/firma.html>*,
<http://www.jus.gov.ar/firma/index.html>

Germany

Kuner, C. "Law of Electronic and Internet Commerce in Germany" (Unofficial translations of the German materials)
<http://ourworld.compuserve.com/homepages/ckuner/>

German Information and Communication Services Act 1997 and related documents
<http://www.iid.de/rahmen/>

German Telecommunications Act 1996
<http://www.bundesregierung.de/bmpt/tkg.html>

Italy

Buonomo, G. "Italian Laws and Regulations Concerning the Creation, Storage, and Transmission of Documents by Means of Computer-Based Systems and Digital Signature", Presentation at the OECD Workshop on Cryptography Policy, Paris, 9-10 December 1997 *<http://www.oecd.org/dsti/sti/it/secur/act/emef21.pdf>*

Italian Digital Signature Legislation and related documents
<http://www.notariato.it/forum/>

Japan

Electronic Commerce Promotion Council of Japan (ECOM) "Certification Authority Guidelines", April 1997, *<http://www.ecom.or.jp/eng/output/ca/eng-guideline.htm>*

Malaysia

Malaysian Digital Signature Bill 1997 *<http://www.mycert.org.my/digital.html>*

MIMOS "MIMOS initiates the First Public Key Infrastructure Pilot in Malaysia", Press release, 23 December 1997 *<http://www.mtrust.com.my/press/press1.html>*

Singapore

Goh, S. H. "Policy Implications of the Internet in Singapore", 1996
<http://www.ncb.gov.sg/nii/96scan5/shamic1.html>

Lim, C. "Building a Legal Framework for Electronic Commerce", November 1997
<http://www.ech.ncb.gov.sg/view/ech/powerpoint/CharlesLim/sld001.html>

United Kingdom

United Kingdom Department of Trade and Industry "Licensing of trusted Third Parties for the Provision of Encryption Services", Public Consultation Paper on Detailed Proposals for Legislation", March 1997 *<http://dtiinfo1.dti.gov.uk/pubs/>*

United States of America

See Smedinghoff, T. J. "Summary of Electronic Commerce and Digital Signature Legislation", McBride Baker & Coles *<http://www.mbc.com/ds_sum.html>* for a more complete listing.

California “Assembly Bill 1577: Digital Signatures” 2 May 1995 *<http://www.softwareIndustry.org/issues/docs-org/ab1577.txt>*

California “Proposed Digital Signature Regulations for California” *<http://www.ss.ca.gov/digsig/digsig.htm>*

Florida “Florida Statutes (Supplement 1996) Chapter 282: Communications And Data Processing” *<http://www.leg.state.fl.us/citizen/documents/statutes/1996/chapter_282.html>*

Illinois “Electronic Commerce Security Act, 1997 House Bill 3180” *<http://www.mbc.com/iecsa.html>*

Iowa *<http://www2.legis.state.ia.us/GA/77GA/Legislation/HF/02400/HF02474/Current.html>*

Kansas *<http://www.ink.org/bills/2059.html>*

Kentucky *<http://www.state.ky.us/agencies/elecsig/>*

Massachusetts “Massachusetts Electronic Records and Signatures Act”, Draft, 4 November 1997 *<http://www.state.ma.us/itd/legal/mersa.htm>*

Minnesota *<http://www.revisor.leg.state.mn.us/cgi-bin/bldbill.pl?bill=S0173.1&session=ls80>*

Missouri *<http://www.house.state.mo.us/bills98/bills98/HB1126.HTM>*, *<http://www.house.state.mo.us/bills98/biltxt98/intro98/HB1126I.htm>*, *<http://www.house.state.mo.us/bills98/fiscal98/2254-02N.ORG>*

New Mexico *<http://legis.state.nm.us/>*

Ohio *<http://OhioActs.avv.com/122/hb243/home.htm>*

Texas “Digital Signature: Law and Proposed Rules” *<http://www.state.tx.us/EC/digital_signature.htm>*

Texas “House Bill 984: Digital Signature” *<http://www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?TYPE=B&LEG=75&SESS=R&CHAMBER=H&BILLTYPE=B&BILLSUFFIX=00984&VERSION=5>*

Texas “Texas Government Code, §2054.060: new section: §201.14 Digital Signatures” *<http://www.state.tx.us/EC/S201-14.htm>*

Utah “Utah Digital Signature Act 1996” *<http://www.commerce.state.ut.us/web/commerce/digsig/act.htm>*

Utah “Utah Digital Signature Program” *<http://www.commerce.state.ut.us/web/commerce/digsig/act.htm>*

Vermont “1997 Vermont Senate Bill 206” *<http://www.leg.state.vt.us/docs/1998/bills/intro/S-206.HTM>*

Virginia “1998 Virginia Senate Bill 154” *<http://leg1.state.va.us/cgi-bin/legp504?981+ful+SB153ER>*,

Model Legislation

ABA

American Bar Association "Digital Signature Guidelines" 1996 <*http://www.abanet.org/scitech/ec/isc/dsg-toc.html*>

FDA

U.S. Food and Drug Administration "21 CFR Part 11: Electronic Records; Electronic Signatures" <*http://www.fda.gov/cder/esig/part11.htm*>

ICC

International Chamber of Commerce "GUIDEC: General Usage for International Digitally Ensured Commerce" <*http://www.iccwbo.org/guidec2.htm*>

NCCUSL

NCCUSL "Revision Of Uniform Commercial Code, Article 2: Sales", Draft, 1 March 1998 <*http://www.law.upenn.edu/library/ulc/ucc2/ucc2298.htm*>

NCCUSL "Uniform Commercial Code, Article 2B: Licences", Draft, March 1998 <*http://www.law.upenn.edu/library/ulc/ucc2/2b398.htm*>

NCCUSL "Uniform Electronic Transactions Act", Draft, 25 November 1997 <*http://www.law.upenn.edu/library/ulc/uecicta/eta1197.htm*>

NCCUSL "Reporters Memorandum: Uniform Electronic Transactions Act Draft of 25 November 1997", 1 December 1997 <*http://www.law.upenn.edu/library/ulc/uecicta/etam1197.htm*>

UNCITRAL

UNCITRAL "UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996" 1997 <*http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm*>

UNCITRAL "Draft Uniform Rules on Electronic Signatures", 12 December 1997

UNCITRAL "Report of the Working Group on Electronic Commerce on the Work of its Thirty-Second Session", 10 February 1998

APPENDIX I - METHODOLOGY

The methodology used to produce this report is shown below:

Process

Activity	Details
Project Initiation meeting	Meet with members of DOCA/NOIE to commence the project, adjust the schedule, etc. Some preliminary work will be done prior to this meeting.
Prepare Initial Documents and circulate to Working Party	Initial documents to include Project methodology and timetable, outline of Exposure Drafts and skeleton of final report.
Phone Conference with Working Group	Meeting and/or phone conference with the Working Group to discuss and agree scope/content of Initial Documents.
Research	Synthesize pre-existing research. Update and/or conduct new research with a view to determining, amongst other issues: • fine details of key overseas initiatives (including scope, structure, metrics and economics, accreditation/cross certification and audit processes); • status of and plans for Australian and key international Certification Authorities; and probable service metrics in Australia, and 'take up rates'.

Activity	Details
Prepare drafts of Briefing Paper and Questions	See *Appendix 0 APPENDIX J - Consultation* List of Interviewees The following organisations were interviewed: 1. ACCC - Australian Competition and Consumer Commission (consumer protection and competitive neutrality) - 2. ACS - Australian Computer Society (technology) 3. ADNA - Australian Domain Administration Limited 4. AIPO - Australian Industrial Property Organisation (intellectual property, electronic watermarking) 5. ASC - Australian Securities Commission (business authorities and delegations) 6. ATO - Australian Taxation Office 7. AUSCERT - Australian Computer Emergency Response Team (systemic risk) 8. Australia Post 9. Australian Information Industry Association 10. APCA - Australian Payments Clearing Association 11. ASX - Australian Stock Exchange 12. Centrelink 13. CLEB - Commonwealth Law Enforcement Board (law enforcement) - 14. DOCA NOIE 15. DSD - Defence Signals Directorate 16. HIC - Health Insurance Commission 17. Human Rights and Equal Opportunity Commission (privacy and social equity) 18. ISACA - Information Security, Audit and Control Association (audit) 19. ICA - Institute of Charted Accountants 20. Institute of Company Directors 21. Institute of Company Secretaries 22. KPMG 23. Multi Media Victoria 24. Tradegate-ECA See *Consultation Briefing Document* for details of the briefing paper and *Appendix 0 NPKI —Interview Questions* for the questions asked.

Activity	Details
Active consultation	Circulate Briefing Document to interviewees (refer to *Appendix - 0 List*), and then conduct face to face meetings and phone calls with a limited number of key opinion leaders (including the members of the Working Group) in each of the following categories: • Commonwealth Government; • Attorney General's Expert Group; • State Governments; • Standards Bodies (eg Standards Australia PKAF); • Key Peak Bodies/Industry Associations (eg APCA); and • Providers of authentication products and services.
Revision of Exposure Drafts	Revise Exposure Drafts to reflect results of consultation and circulate to Working Group.
Workshop of Exposure Drafts	Workshop Exposure Drafts with Working Group.
Draft Report	Develop Report based upon Exposure Drafts
Workshop draft report with PKAF Working Party	Obtain Working Group Feedback and amend report to produce final.
Presentation	Present findings to Working Group and key stakeholder executives
Prepare HTML Report	Preparation of report in HTML form

APPENDIX J - CONSULTATION

List of Interviewees

The following organisations were interviewed:

1. ACCC - Australian Competition and Consumer Commission (consumer protection and competitive neutrality) -
2. ACS - Australian Computer Society (technology)
3. ADNA - Australian Domain Administration Limited
4. AIPO - Australian Industrial Property Organisation (intellectual property, electronic watermarking)
5. ASC - Australian Securities Commission (business authorities and delegations)
6. ATO - Australian Taxation Office
7. AUSCERT - Australian Computer Emergency Response Team (systemic risk)
8. Australia Post
9. Australian Information Industry Association
10. APCA - Australian Payments Clearing Association
11. ASX - Australian Stock Exchange
12. Centrelink
13. CLEB - Commonwealth Law Enforcement Board (law enforcement) -
14. DOCA NOIE
15. DSD - Defence Signals Directorate
16. HIC - Health Insurance Commission
17. Human Rights and Equal Opportunity Commission (privacy and social equity)
18. ISACA - Information Security, Audit and Control Association (audit)
19. ICA - Institute of Charted Accountants
20. Institute of Company Directors
21. Institute of Company Secretaries
22. KPMG
23. Multi Media Victoria
24. Tradegate-ECA

Consultation Briefing Document

This document was sent prior to each briefing to ensure the interviewees were familiar with the terms and concepts of NPKI. The aim was to obtain their **business perspective** on the proposed infrastructure.

Introduction

The Commonwealth Government wishes to facilitate the establishment of a peak body to oversee the development of a national framework for the authentication of users of online communications services, that would provide:

- a trusted system for the generation of digital signatures to give corresponding parties certainty in each others' identities;
- assurance of the integrity of electronic data used; and
- a means of ensuring non-repudiation of electronic transactions.

As a first step, Government has established a Working Group (WG) to determine details of the framework and in particular its oversighting body and report to the Minister for Communications, the Information Economy and the Arts by the end of March 1998.

The ten members of the Working Group (excluding the Chair) represent :

- Commonwealth Government Agencies;
- State Governments;
- Suppliers of Certification Products/Services; and
- User and other Organisations.

The Working Group is to examine business models and practical options for the structure, operations and role of a peak policy and, possibly, root registration authority (PARRA) which will oversee the national framework, and which addresses other relevant flow on issues affecting the national framework.

Whereas the Government is not prescribing mandatory direct government involvement in relation to the above, the Government has expressed a clear preference for a national framework which is :

- technologically neutral; and
- non exclusive.

ETC Electronic Trading Concepts Pty Limited has been retained to provide specialist consulting assistance to the Working Group.

This briefing document has been prepared in order to support the consultation with persons and organisations outside of the Working Group.

Background

> *"As electronic commerce becomes commonplace, there is a growing need for users to ensure that electronic transactions can be validated. Compatible national and international systems of "digital signatures" are necessary for the introduction of secure electronic commerce."* - From 'Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia' report by Standards Australia Task Group.

For widespread adoption of electronic methods of transacting business, industry and government require, amongst other things, the ability to:

- provide authentication of the identity of persons as individuals or delegates/agents (*user authentication*); and
- hold parties to agreements (*non-repudiation*) submitted electronically.

Public-key cryptography, in the form of digital signatures, can provide the technical means to implement such protection. With appropriate legislation, infrastructure and technical standards, digital signatures can be given legal weight. Many jurisdictions around the world are establishing such arrangements.

In Australia work in relation to electronic authentication is being undertaken by a range of bodies including :

- technical standards (Standards Australia IT/12/4/1 committee); and
- legal frameworks (Attorney-General's Electronic Commerce Expert Group [ECEG]); and
- establishment of a Government Public Key Infrastructure, to eventually come under PKAF, for the Commonwealth Government (3 working groups set up under the Office of Government Information Technology [OGIT]).

Issues

The key issues to be addressed by the Working Group and upon which the consultants will be seeking wide spread input include :

- Options for the role and functions of the peak oversighting body;
- Organisations and industry sectors that should be represented on the oversighting body;
- Options for the corporate structure of the peak body;
- Potential resource requirements of such a body;
- Possible mechanisms for overseeing the body's work and ensuring its integrity;
- Relevant technical standards for authentication products and services;

- Scope and form of capability standards for the accreditation of organisations providing authentication products and services;
- Mechanisms for evaluating the effectiveness of the authentication framework and the operations of the peak body; and
- Other issues relevant to the overall topic under consideration.

Further detail regarding certain issues is provided below.

Scope and Objectives

A significant topic of discussion is the extent of the role of the peak body and the possible separation of the root authority from the policy defining functions.

Another issue for discussion relates to the issue of "technology independence" particularly in regard to matters of 'Public Key' versus more general 'Digital Authentication'.

Trust & Public Confidence

This issue relates to "what constitutes *Trust* in its various forms and how this may be achieved". A further, related issue of Public Confidence (and possibly Systemic Risk) also needs to be addressed.

Policies and Audit

Issues to be examined include:

- what is meant by a policy in terms that can persuade laypersons;
- what is the difference between a policy and a standard?
- how are policies to be policed?
- what is the role of audit, self-audit, external audit ?
- who will audit the auditors? and
- how does this relate to trust?

Role of Legislation/Regulation

This addresses the issues of the need for legislation/regulation to support digital signatures in their various forms. This may be in the form of specific digital signature legislation but may also include others, as suggested by Wallis including the Uniform Consumer Credit code, the Privacy Act 1988, and the Financial Transactions Reports Act 1988.

Is there a case for an "Australian" national peak body, unless national jurisdiction is somehow an issue?

Privacy and Social Equity

This addresses privacy and other issues of social equity. It is possible that some implementations of electronic authentication may be seen to be privacy invasive and/or be seen to discriminate against those who cannot or will not use technology based solutions. It could also be argued that a digital signature infrastructure may be of considerable benefit to Australians living and working in remote areas.

International Co-operation

Issues at stake include the related activities, and influence of international bodies (eg APEC, Uncitral, ISO) as well as the power of the worldwide product development industry, and the extent to which these will determine the way in which digital signatures are going to work globally.

Functions and Processes

This seeks to flesh out the possible functions and processes of a peak body. Possible functions and processes include :

- oversight of accreditation of elements of a National PKI
- licensing of accrediting organisations
- dispute resolution
- seeking community views on proposed policies
- promulgation of policies for a national PKI

Corporate Structure, Governance and Funding

This seeks to examine the issues of ownership, structure, management and funding of a peak body.

Further Information

For further information please contact :

Steve Burns of ETC Electronic Trading Concepts Pty Limited on:

- Telephone : 02 9299-4755
- Email : stephen.burns@etc.com.au

Phillip Hennig of Department of Communications and the Arts on:

- Telephone: 02 6271-1083
- Email: phennig@dca.gov.au.

NPKI —Interview Questions

Refer to the National Public Key Infrastructure (NPKI) Briefing paper for background.

1. What should be the role and functions of a peak body oversighting NPKI

If you believe a peak body is necessary the role and function options include;

a) monitoring overall framework policy;

b) accrediting/certifying certification authorities (CAs);

c) auditing CAs to ensure compliance with agreed standards and principles;

d) acting as the root for the national certification architecture;

e) cross certifying other international root authorities;

f) generating and publishing national and international Certificate Revocation Lists (CRLs); and

g) archiving certificates, CRLs and audit files.

2. What organisations (both public and private sector) and industry sectors should be represented on the oversighting body?

Options include:

- Providers of authentication products and services;
- Peak bodies representing users of authentication products and services;
- Government bodies; and
- Standards development bodies.

3. What should be the corporate structure of the peak body?

Options include:

- an incorporated body;
- a government business enterprise or statutory authority; or
- a cooperative non-profit organisation.

4. How should resource requirements needed in oversighting the national framework be met in terms of :

- staff;
- fixed assets; and
- recurrent funding?.

5. How should the work of the peak body be overseen in order to ensure its integrity;

6. **What, if any, should be the relevant technical standards for authentication products and services?**

Options include:

- the work of Standards Australia working group 12/4/1;
- ITSEC;
- standards developed by international standards developing bodies.

7. **What should be the scope, and form, of capability standards used for accrediting organisations providing authentication products and services?**

8. **What mechanisms should be put in place to evaluate the effectiveness of the authentication framework and the operations of the peak body? What should be the criteria for measuring effectiveness?**

9. **Are there any other issues relevant to the effective operation of a national user authentication framework?**