



LEGAL LIABILITY AND
e-transactions

A scoping study for the National Electronic Authentication Council

August 2000

MARK SNEDDON, PARTNER, CLAYTON UTZ

This report was commissioned by the National Electronic Authentication Council (NEAC) to create awareness about legal liability surrounding the use of authentication technologies in electronic transactions. The opinions contained in the report are those of the author, Mark Sneddon, Partner, Clayton Utz, and not necessarily the National Electronic Authentication Council (NEAC) or the National Office for the Information Economy (NOIE). The NEAC's response to the recommendations is included at the close of the report.

© Commonwealth of Australia 2000

ISBN 0 642 75080 7

DOCITA 22/00

Published by the National Office for the Information Economy (Commonwealth Department of Communications, Information Technology and the Arts) to provide information on electronic commerce initiatives.

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Department. Requests and inquiries concerning reproduction and rights should be addressed to:

The Secretary

Department of Communications, Information Technology and the Arts

GPO Box 2154

CANBERRA ACT 2601

Australia

Telephone: (02) 6271 1000

Facsimile: (02) 6271 1800

Email: dcita.mail@dcita.gov.au

Website: <http://www.dcita.gov.au> or <http://www.noie.gov.au>

Designed and typeset by Green Advertising #13228



Ministerial foreword

Industry and government are increasingly interested in the use of authentication and public key technologies to provide dependable and secure e-commerce transactions. Authentication and public key technologies are a key enabler in the deployment of e-commerce transactions.

The primary focus of activity in the authentication area (both in Australia and overseas) has been on digital signatures involving the use of public key cryptography—also known as public key infrastructure (PKI).

The reliable identification of the parties to an electronic transaction such as tax and regulatory returns with government agencies is a basic pre-requisite for reliable electronic transactions. Equally, contracts between business parties which require a high degree of reliability and security can be completed using PKI technologies. Electronic transactions may carry substantial legal and financial liabilities if one of the parties is not who they purport to be.

A key issue which may be delaying wider take-up of public key authentication technology is the liability of parties to an electronic transaction. Losses could arise from defective issue or maintenance of digital certificates and supporting infrastructure. Managing liability and sharing any losses in ways which give confidence and equity to the parties is a core objective in the development and marketing of PKI.

This report brings much needed clarity to identifying and assessing liability issues in the use of electronic authentication systems. It also identifies various liability allocation models, and makes useful recommendations to the National Electronic Authentication Council for further assessing how various models might best work in Australia's legal and commercial environment.

A handwritten signature in black ink that reads "Richard Alston". The signature is written in a cursive style.

Richard Alston

Minister for Communications, Information Technology and the Arts

Introduction to NEAC

This report on electronic authentication and liability was commissioned by the National Electronic Authentication Council (NEAC). NEAC was established in 1999 by the Commonwealth Government to oversee the development of a national framework for the electronic authentication of online transactions.

NEAC is a national focal point for authentication matters: providing advice to Government, industry and consumers on authentication issues; encouraging the development of relevant standards; and facilitating the wider use of authentication products issued by Government agencies for electronic transactions.

NEAC reports to the Commonwealth Government through the Hon. Richard Alston, Minister for Communications, Information Technology and the Arts. The National Office for the Information Economy (NOIE) manages the Secretariat for NEAC.

NEAC's thirteen members represent industry providers and users of authentication products and services, consumer organisations, the small business and retail sectors, banking and finance, professional services, academia, the legal sector and relevant government agencies. NEAC's mission is to build industry and consumer confidence in the use of authentication technologies and electronic commerce.

NEAC MEMBERS

COMMONWEALTH GOVERNMENT

Dr Rod Badger (Chair)
Deputy CEO
National Office for the Information
Economy

Mr Peter Anderson
General Manager
Office of Government Online

Mr Peter Ford
First Assistant Secretary
Information and Security Law Division
Attorney-General's Department

INDUSTRY ASSOCIATIONS

Mr Stephen Wilson
Chairman
Certification Forum of Australia

Mr Rob Durie
Executive Director
Australian Information Industries
Association

Mr Stephen Carroll
Director
Australian Bankers Association

Mr Charles Britton
Senior Policy Officer
Australian Consumers Association

Mr Philip Holt
Managing Director
Australian Business Limited

Mr Tom Muecke
Chairman
Small Business Coalition

Ms Anne Molyneux
Director – Intellectual Capital
CPA Australia

Mr Michael Lonie
Executive Officer E-commerce
Australian Retailers Association

INDIVIDUAL MEMBERS

Mr Oliver Barrett
Head - Technology and
Communications
Minter Ellison

Mr Michael Cook
General Manager
Department of Communications,
Information, Local Government,
Planning and Sport
Queensland Government
(Representing Online Council
Officials)

Ms Jennifer Seberry
Professor of Computer Science
University of Wollongong

SECRETARIAT

Catherine Higgins
Project Manager, E-Commerce
National Office for the Information Economy (NOIE)

Consultant's role

The consultant was asked to:

- examine the extent to which existing Australian law defines actions that result in parties to an electronic transaction incurring liability, particularly those actions related to the electronic authentication of parties;
- examine and identify any issues or actions that are specific to authentication in electronic transactions that are not adequately covered by existing Australian law; and
- having regard to the *Electronic Transactions Act 1999*, examine and identify the risks that these gaps in existing law present to the parties using electronic authentication systems, including the sender and recipient of information and the third party that certifies the identity of those parties.

As there are a range of possible legislative, contractual, insurance and standards-related solutions to these risks the consultant was asked to include in the report a brief assessment of the costs and benefits of proposed solutions, with a particular focus on identifying specific actions that NEAC could take.

In preparing the report, the consultant was required to examine:

- any relevant work being undertaken, in both the private and government sector (including State and local governments); and
- the Electronic Transactions Act.

The consultant was also required to have regard to any relevant existing standards and codes of business practice.

Contents

Executive summary	1
1. Introduction	5
2. Reader's guide to the report	7
3. Adequacy of current Australian law to determine liability allocation between parties in a PKI	9
3.1 Participants in electronic authentication in a PKI and liability events	9
3.2 Analysing some factual scenarios to uncover areas of liability uncertainty	10
3.3 S v RP v CA: Some specific variations on the general fact scenario concerning the application of the existing law	12
3.4 Broad assessment of the level of certainty of the application of Australian law regarding liability in the relationships of S, RP and CA	14
3.5 Summary	16
4. Private law mechanisms for managing legal liability uncertainty	17
4.1 Strategies for managing legal liability uncertainty	17
4.2 Private law mechanisms: disclaimers, contract, insurance	17
4.3 Managing legal liability between end users (S and RP)	18
4.4 Managing legal liability of CA to S and RP	18
4.5 The Verisign model for management and allocation of risk and responsibility	19
4.6 Viability of the Verisign model under Australian law	28
5. Legislative solutions for managing legal liability uncertainty	37
5.1 Analysis of different legislative models	37
5.2 Technology-specific approach	37
5.3 Two-tier approach	40
5.4 Minimalist (or technology-neutral functional-equivalence) approach	42
6. Assessment of liability management options and recommendations to NEAC on further work	43
6.1 Assessing liability management solutions	43
6.2 Adequacy of existing law and private law mechanisms for managing legal liability in S-CA, S-RP and CA-RP relationships	43
6.3 Need for legislative intervention in liability allocation	44
6.4 Other matters	47
6.5 International harmonisation of liability management solutions	49
6.6 Recommendations for NEAC's further work	50
7. NEAC's response to the recommendations	51
Appendix A	53
Glossary	61

Executive summary

1. The aim of this report is to provide to DOCITA and NOIE (for the use of NEAC) a scoping study to clarify the issue of legal liability in the use of electronic authentication systems (primarily those using a public key infrastructure (PKI)) and to identify options and make recommendations as to where NEAC might undertake further work on this issue.
2. The report analyses the legal liability of the following parties in a public key infrastructure:
 - a subscriber ('S') for a digital certificate in which S's identity will be linked to a public key associated with a private key controlled by S;
 - the certification authority ('CA') which issues the digital certificate and the registration authority ('RA') which carries out the subscriber identification process; and
 - a relying party ('RP'), who receives a digitally signed electronic communication and acts in reliance on a relevant digital certificate by using the public key stated in the certificate and linked to S's identity, to verify that the communication was signed using the corresponding private key and thus infers that the communication originated from S.
3. To simplify the analysis in this report, we have assumed that there is only one CA and that the CA is also carrying out the functions of the RA.

Liability is examined in three relationships:

- S – CA
 - S – RP
 - CA – RP
4. Australian law relevant to liability is briefly summarised in Appendix A. Factual scenarios are used in the report to analyse the degree of certainty Australian law provides to the three participants (S, RP, CA) as to their legal liability. The following broad assessments are made:
 - (a) **S v CA**

Existing Australian law relating to contract and to compensation for negligence causing pure economic loss is adequately certain to manage liability allocation between Ss and CAs.
 - (b) **S v RP**

In general S is not bound by a message unless it was digitally signed by S or a person acting with S's authority. RP may have an action against S in negligence if RP can establish that S owed RP a duty of care to take reasonable care with S's private key and S was careless with his private key. In Australia, the law of negligence in relation to pure economic loss does not adequately provide guidance for this aspect of the relationship between S and RP. There is also uncertainty as to the application of agency law in the case of an undisclosed agent X who signed a message using S's private key.

(c) CA v RP

Australian law does not provide adequate guidance as to whether or not a CA will owe a duty of care to an RP who is unknown to the CA (either because the RP does not consult the CA's certificate repository or CRL or does so anonymously) and therefore is a member of a large and diffuse class which is incapable of determination. If a RP does become known to a CA because of such consultation, there is a stronger argument that the CA owes such a RP a duty of care. It is unclear whether RPs are under any general legal duty to S or the CA to check the CA's certificate repository or CRL.

5. The report then considers whether **private law mechanisms** for managing legal liability uncertainty (e.g. disclaimers, contracts, insurance) are adequate to deal with any uncertainty in the general law in the three relationships. The Verisign CA model for private law management of liability is considered in detail and its viability under Australian law is evaluated.
6. **Legislative models** for managing legal liability uncertainty are considered and different legislative models categorised and analysed.
7. An assessment is made of the adequacy of existing law and private law mechanisms to manage legal liability which provides the following conclusions:

(a) S v CA

Current law and private law mechanisms are in general adequate to manage liability allocation between Subscribers and CAs but adequacy of legislative protection of consumer and small business subscribers from one-sided CA contracts should be reviewed.

(b) S v RP

Current law and private law mechanisms are in general adequate to manage liability allocation between Subscribers and Relying Parties subject to (i) the continuing development of suitable risk management measures such as certificate reliance limits and insurance cover and (ii) review of the adequacy of legislative protection of consumers and small business from one-sided contractual liability allocations.

(c) CA v RP

It is unclear whether current Australian law and private law mechanisms can give adequate certainty in managing liability allocation in the CA-RP relationship. Further research on private law mechanisms and the current law is required. Depending on the outcome of that research consideration may need to be given to legislation to impose mutual duties and liabilities (with limits) on CAs and RPs.

8. The report makes the following recommendations for future work by NEAC in the area of authentication and legal liability:
 - 8.1 (a) Undertake further research on the adequacy of private law mechanisms under Australian law to provide certainty in managing liability allocation in the CA – RP relationship.
 - (b) If that research suggests that private law mechanisms cannot provide adequate certainty, consider whether legislation is necessary to impose duties and liabilities

and appropriate limits of these on CAs and RPs and what its form should be. Various international models should be considered, particularly the European Union Directive on a Common Framework for Electronic Signatures 1999.

- 8.2 Evaluate whether there is adequate legislative protection of consumers and small business (both as Subscribers and Relying Parties) against unfair contractual liability allocation in all of the relationships S – CA, S – RP, CA – RP. If not, consider whether additional legislative protection is required and whether this could be tightly focussed to minimise uncertainty of application.
- 8.3 Consider ways to encourage the development of:
- (a) insurance products for Subscribers, Relying Parties and CAs; and
 - (b) risk management features for PKI certificates such as per transaction reliance limits and periodic reliance limit caps;
- which parties can use to accurately measure and manage their risk.
- 8.4 Consider how to encourage CAs and vendors of computing platforms to provide trusted computing platforms and software to end users for:
- secure storage of private keys and operation of signing mechanisms;
 - secure certificate management and verification functions.

1

Introduction

The aim of the project is to provide to DOCITA and NOIE (for the use of NEAC) a scoping study on the issue of legal liability in the use of electronic authentication systems (primarily those based on a public key infrastructure (PKI)) and to identify options and make recommendations as to where NEAC might undertake further work on this issue. This report was prepared by Mark Sneddon with the assistance of Philippa Hore and Paul Noonan of Clayton Utz.

2

Reader's guide to the report

Section 3 of the report assesses the adequacy of current Australian law to determine the allocation of liability among three parties to a PKI: a Subscriber for a digital certificate, a Certification Authority which issues a certificate and a Relying Party who relies on the certificate.

Section 3 uses factual scenarios to pose legal liability issues and assess the level of certainty in the application of Australian law to these scenarios. A background summary of relevant Australian law is provided in Appendix A relating to:

- legal requirements for a signature;
- law relevant to one person being bound by the actions of other persons or electronic devices; and
- principles of liability in negligence.

Sections 4 and 5 consider strategies for managing uncertainty as to legal liability in a PKI. Section 4 considers the private law mechanisms of disclaimers, contracts and insurance. It examines in detail the Verisign CA model for managing legal liability under US law and considers its viability under Australian law.

Section 5 examines different legislative models around the world for managing legal liability allocation in a PKI and categorises these.

Section 6 assesses whether private law mechanisms are adequate to manage liability allocation under Australian law; whether legislative intervention is required and, if so, the type of legislative intervention. The section considers the international 'transportability' of private law and legislative mechanisms. It concludes with recommendations as to further work which NEAC could undertake in the area of electronic authentication and legal liability.

3

Adequacy of current Australian law to determine liability allocation between parties in a PKI

3.1 PARTICIPANTS IN ELECTRONIC AUTHENTICATION IN A PKI AND LIABILITY EVENTS

- (a) The participants in public key infrastructure most likely to incur liability are:
- a subscriber ('S') for a digital certificate in which S's identity will be linked to a public key associated with a private key controlled by S;
 - the certification authority ('CA') which issues the digital certificate and the registration authority ('RA') which carries out the subscriber identification process; and
 - a relying party ('RP'), who receives a digitally signed electronic communication and acts in reliance on a relevant digital certificate by using the public key stated in the certificate and linked to S's identity, to verify that the communication was signed using the corresponding private key and thus infers that the communication originated from S.

To simplify the analysis in this report, we have assumed that there is only one CA and that the CA is also carrying out the functions of the RA. In practice, there may be multiple CAs used to establish a chain of trust and there may be a separate RA who verifies the claimed identity of S. If there are multiple CAs or a separate CA and RA, each of these parties will have to manage their liability to each other, to S and to Relying Parties.

- (b) Examples of events which could cause one or more of the PKI participants to incur liability are:
- compromise of S's private key (the subject of a certificate), leading to unauthorised creation of S's digital signature and incorrect attribution of that signature to S in reliance on the certificate;
 - failure on the part of the CA to suspend or revoke a compromised private key on request;
 - compromise of CA's private key leading to the creation of 'forged' certificates;
 - CA issues a certificate that wrongly links the identity of one person with a public key allocated to another;
 - breach of the security of stored information;
 - incorrectly generated or allocated attribute certificates;
 - interrupted access to the CA's certificate repository or CRL;
 - wrongful suspension or revocation of a certificate; and
 - duplicate key generation by the CA/RA.

A thought-provoking analysis of risks for end users in a PKI is contained in an article by two leading cryptographers and computer security consultants: Ellison and Schneier 'Ten Risks of PKI: What you're Not Being Told About Public Key Infrastructure' (2000) 16 (1) *Computer Security Journal*, available at www.counterpane.com/pki-risks.html.

3.2 ANALYSING SOME FACTUAL SCENARIOS TO UNCOVER AREAS OF LIABILITY UNCERTAINTY

This section of the report posits some factual scenarios of electronic authentication (focussed on PKI) and uses them to analyse the degree of certainty Australian law provides to participants as to their legal liability. The relevant law is not set out in full here—interested readers can find a summary of it in appendix A.

The report does not attempt to provide legal advice on the PKI fact scenarios but to identify where the application of Australian law to them is sufficiently uncertain that options should be identified for public policy initiatives or private sector risk management action.

(A) A PKI DISPUTE - GENERAL FACT SCENARIO

Assume RP receives an electronic message accompanied by a PKI digital signature. The message appears to come from and be authored by S and either the message is accompanied by a digital certificate digitally signed by CA linking S's identity with a public key or RP obtains such a certificate from CA's online repository. S's apparent authorship of the message is verified by RP by using the public key in the certificate to decrypt and compare the message digest.

RP acts to its detriment in reliance on the message and the belief confirmed by the certificate that the message has been authored by S. For example, the message instructs RP to pay money to C (a third party) against S's promise of reimbursement.

S claims he never authored or sent the message and disclaims liability to RP. The money is not recoverable from C.

S doesn't know how the digitally signed message was sent to RP. It is possible that a third party X may have obtained access to S's private key, which is located in S's personal computer, and used it to sign the message to RP. S cannot conclusively prove this. Neither can RP conclusively disprove this. (The following discussion assumes that if X does exist, X cannot be found and be made liable so a loss must be allocated between S, RP and CA. In practice the loss might be recoverable from X.)

(B) EVIDENTIAL UNCERTAINTY

In the absence of a prior contract between S and RP governing the allocation between them of the risk of unauthorised messages, S would be legally responsible for the message if a court was persuaded on the balance of probabilities that in fact the message was digitally signed by S or by a person acting with S's authority (applying the law of agency and, where relevant, s. 15 of the *Electronic Transactions Act 1999* (Cth)). Usually RP would be trying to establish that S was legally responsible for the message, and therefore RP would have the burden of proving this. (This is the same allocation of burden of proof as in paper-based commerce - in general, the recipient carries the risk of relying on a forged or unauthorised manual signature.)

To decide the issue a court would have to weigh the prima facie evidence that the message was signed with S's private key against any reasonable explanation S could advance as to how the message was signed with his key without his authority. In such a dispute, RP would start with the prima facie advantage provided by the strength of the cryptographic association of the message with S's private key. But that would not be a conclusive advantage. S may be able to adduce

evidence of a likely alternative explanation, such as an interloper misusing the key while S's computer was switched on but S was temporarily away from his computer, or a trojan program such as Back Orifice 2000 having captured S's private key and transferred it to a third party who uses it to impersonate S.

This *evidential uncertainty* is caused by the nature of the digital signature technology, not the law:

- (i) Digital signature technology can prove to a very high degree of probability that a private key corresponding to a public key was used to sign a message but it cannot prove who used the private key to sign the message—that is left to inference. The inference is weaker if the holder of the private key has to keep it on a non-trusted computing platform such as a standard home or office personal computer. Better evidence of the signer's identity may be provided by other electronic authentication methods such as biometric identifiers (probably used as access methods to enable the use of the private key which is held on and does not leave a smart card that is a trusted computing platform).
- (ii) Digital signature technology cannot distinguish between an authorised digital signature and an unauthorised one, whereas in most cases a forged manual signature can be distinguished from a genuine signature with enough care and expertise.

(C) UNCERTAINTY IN THE APPLICATION OF THE EXISTING LAW

Even if S can establish on the evidence that he did not personally sign the message (and again assuming no contract between S and RP governing the allocation between them of the risk of unauthorised messages):

- (i) S may be made responsible for the message through the law of agency or through section 15 of the *Electronic Transactions Act* (e.g. if an employee of S for whose acts S is legally responsible signed the message).
- (ii) RP may have an action against S in negligence if RP can establish that S owed RP a duty of care to take reasonable care with S's private key and S was careless with his private key.

In each of these cases it will again be a question of what evidence RP can produce to convince a court that S was responsible for the message or liable in negligence. But there is also a question as to whether S can be legally responsible on these grounds. The application of the law in these cases is not always clear. This is due to the nature of the common law, which is expressed in general principles and fleshed out in the specifics of cases. If there are no precedents in the case law that closely mirror a particular fact scenario, it is often a matter of conjecture as to how the existing principles of law would apply to that particular scenario. Some specific fact scenarios and commentary are provided below to illustrate this.

3.3 S V RP V CA: SOME SPECIFIC VARIATIONS ON THE GENERAL FACT SCENARIO CONCERNING THE APPLICATION OF THE EXISTING LAW

Assume that the following facts are added to the general fact scenario outlined above.

- (a) S expressly authorised X to send the message.

X would be S's agent with actual authority. Accordingly, S would be bound, as X's principal, by the contract with RP formed by the message. S may also be bound by the message pursuant to section 15(1) of the Electronic Transactions Act 1999 (Cth). [Application of Australian law highly certain].

- (b) S permits X to access and use S's private key and digital certificate for defined limited purposes which do not include the message sent to RP (assume this is consistent with S's contractual duties to the CA).

- (i) S takes reasonable care to monitor X's use of the key and certificate.

X's act is outside the scope of X's actual authority. It is unlikely or at least unclear whether the doctrine of apparent authority would apply in this case to make S responsible for X's use of the private key, because RP is unaware of the existence of X as agent. (The same is true if X is an intelligent software agent rather than a legal person.) If S has taken reasonable care to monitor X's use of the key and the certificate, S will not be liable to RP in negligence. [Application of Australian law reasonably certain except as to apparent authority of an undisclosed agent].

- (ii) S does not take reasonable care to monitor X's use of the key and certificate.

Whether or not S's failure to take reasonable care would entitle RP to recover from S in negligence is not clear in Australian law at present. There is no general duty of care in Australia to avoid causing economic loss to another. A duty will only be owed where the relationship between the parties is sufficiently proximate. In general proximity requires that the duty be owed to a specific class which is identified or ascertainable at the time of the act of negligence. It would probably not be necessary that the class to whom the duty was owed could be identified with complete accuracy. The imposition of such a duty is more likely where the plaintiff (a member of the class) is unable to avoid the loss by taking reasonable steps to pursue its own interest.

In this fact scenario, the scope of the class to which S may owe a duty is potentially very wide - it could include all possible recipients of communications which X could send using S's private key and digital certificate. Such a class would be so wide as to be almost indeterminate and, accordingly, it is unlikely that a duty of care would be imposed on S.

However, if RP belonged to a more precisely defined class (for example the class the members of which regularly received messages from S) then it is more likely that a duty of care would be imposed and S would be liable to RP in negligence [Application of Australian law uncertain].

(c) S discovers that the security of the private key and digital certificate have been compromised and informs the CA before RP receives the message sent by X.

(i) RP does not check the Certificate Revocation List (CRL) maintained by the CA.

Assuming there is a duty to check the CRL or RP has been adequately notified of the risks in not doing so, S is unlikely to be liable to RP. RP's loss has either been caused by its own negligence or, even if S's negligence has caused the private key and certificate to be compromised, S will have a defence of contributory negligence which, in the circumstances, is likely to be close to complete. [Application of Australian law reasonably certain].

(ii) RP checks the CRL but the CA has not posted the revocation within a reasonable time of S's advice.

If the CA's failure to post the revocation results from a negligent act or omission on the part of the CA or one of its employees, RP may have an action against the CA in negligence causing pure economic loss. However, RP is a member of a potentially indeterminate class (i.e. all possible relies on the compromised signature and certificate). Accordingly, it may not be possible for RP to establish that the CA owed it a duty of care. [Application of Australian law uncertain]. In practice, the CA may have purported to create an online contract limiting its liability to RP. Whether it can create such a contract through an online interaction when RP checks the CRL is somewhat uncertain and the CA's ability in Australian law to limit its liability to RP will be affected by legislation (such as consumer and small business protection legislation), so the outcome even with a contract may be uncertain.

There are many other scenarios potentially giving rise to liability between S, RP and CA. In some of these the application of Australian law will be clear and in others it will be uncertain until a test case creates a precedent. One of the principal areas of uncertainty is the existence of a duty of care giving rise to liability in negligence between S and RP and between a CA and RP. This issue is considered in more detail below.

3.4 BROAD ASSESSMENT OF THE LEVEL OF CERTAINTY OF THE APPLICATION OF AUSTRALIAN LAW REGARDING LIABILITY IN THE RELATIONSHIPS OF S, RP AND CA

Assume an event causing loss to a participant in a PKI occurs because of careless acts or omissions of one or more of the other participants. The issue will be whether the careless participant owes a duty of care to the affected party that will give rise to a liability in negligence to compensate that party. Contractual limitations of liability and statutory controls on such contracts must also be taken into account.

(a) S -v- CA

S will almost always be in a contractual relationship with the CA. The CA will seek to use that contract to exclude or at least limit its liability to S. A prudent CA would seek, in particular, to exclude liability for its negligent acts or omissions.

If the consideration for the S/CA contract is less than \$40,000 or the services supplied by the CA are of a kind ordinarily acquired for personal, domestic or household use or consumption, the *Trade Practices Act* or equivalent consumer and small business protection legislation will imply certain non-excludable warranties by the CA into the contract. These warranties will limit the ability of the CA to exclude or limit its liability to S for negligence.

To the extent that the CA cannot, or does not, exclude all liability, a subscriber which incurs loss as a result of the negligent act or omission of a CA may be able to avail itself of actions in both contract and negligence against the CA.

CA LIABILITY IN CONTRACT

The fact situations outlined above do not appear to raise any issues which cannot be adequately dealt with by the law in Australia relating to remedies for breach of contract. However, if the contractual allocation of risk in the S-CA contract is unfairly one-sided, the contract may be subject to challenge for unconscionable conduct under the federal *Trade Practices Act* or equivalent legislation or under the NSW *Contracts Review Act 1980*.

NEGLIGENCE

It is likely that the CA would owe a duty of care to S, because S is a particular person whom the CA knew would be likely to suffer economic loss as a consequence of negligence on the part of the CA. S would owe a duty of care to the CA for the same reason. Liability in negligence will almost always be regulated by the contract between them subject to consumer and small business protection legislation.

- Existing Australian law relating to contract and to compensation for negligence causing pure economic loss is adequately certain to manage liability allocation between Ss and CAs.

(b) S -v- RP

In general S is not bound by a message unless it was digitally signed by S or a person acting with S's authority.

However, assume that S negligently allows its private key to be compromised and that the RP acts to its detriment in reliance on an electronic communication sent with the compromised key by an imposter.

NEGLIGENCE

The principal uncertainty in the application of the law of negligence to the S - RP relationship is whether the relationship is sufficiently proximate that one party would owe the other a duty of care.

The High Court acknowledged in the recent case of *Perre v Apand Pty Ltd* that the law in Australia relating to compensation for negligence causing purely economic loss is uncertain, unsatisfactory, still developing and that there is no governing principle which can provide general guidance as to the outcome on particular facts.

In the fact scenario proposed, the RP would be a member of a potentially very large class comprising all possible recipients of electronic communications from S. This class is so large and diffuse as to be almost incapable of determination at the time of S's negligent act or omission. This may mean that S does not owe a duty of care to a particular RP.

This analysis may be different if an RP regularly received electronic communications from S. There may then be a sufficiently proximate relationship between them giving rise to a duty of care.

- In Australia, the law of negligence in relation to pure economic loss does not adequately provide guidance for all aspects of the relationship between S and RP. As noted earlier, there is also uncertainty as to the application of agency law in the case of an undisclosed agent X who signed a message.

(c) CA -v- RP

NEGLIGENCE

- *For the reasons outlined above for the S-RP relationship, Australian law does not provide adequate guidance as to whether or not a CA will owe a duty of care to an RP who is unknown to the CA (either because the RP does not consult the CA's certificate repository or CRL or does so anonymously and therefore is a member of a large and diffuse class which is incapable of determination). If a RP does become known to a CA because of such consultation, there is a stronger argument that the CA owes such a RP a duty of care. Most CAs would attempt to make such consultation subject to an online contract which would limit CA's liability to the RP in contract and in negligence.*

CONTRACT

On receipt of an electronic communication, RPs need to access the CA's certificate repository or CRL.

It is unclear whether RPs are under any general legal duty to S or the CA to check the CA's certificate repository or CRL.

If the RP does check either the repository or CRL, this gives the CA the opportunity to attempt to create an online contract between itself and the RP. A prudent CA would seek to ensure that such a contract excludes or limits all CA liability to the extent possible.

There is some uncertainty as to the effectiveness of such attempts to create online contracts, depending upon how they are implemented. The principal uncertainties relate to the adequacy of the means of incorporating terms by notice, whether RP provides consideration to found a contract and the effect of consumer and small business protection legislation on contracts which are one-sided in favour of the CA.

- It is very uncertain how Australian law will apply to the relationship and allocation of risk between CAs and RPs.

3.5 SUMMARY

In the legal relationship between S and CA, it is likely that contracts will provide a reasonable degree of certainty, subject to statutory or regulatory override for consumer and small business protection purposes if the contracts are unduly one-sided in favour of the CA.

The same conclusion applies to the S–RP relationship if that is governed by a master contract that allocates risk. If the S–RP relationship is not governed by such a contract, the law is reasonably clear as to when S will be bound by a message signed using S's private key. However, S's liability to RP in negligence for carelessness with the private key is unclear.

Liability allocation in the CA–RP relationship also has very significant elements of uncertainty unless it is governed by a contract. There is practical and legal uncertainty as to whether such contracts can be created and effective in all cases for the CA–RP relationship.

4

Private law mechanisms for managing legal liability uncertainty

4.1 STRATEGIES FOR MANAGING LEGAL LIABILITY UNCERTAINTY

Broadly, there are three methods to manage legal uncertainty in a PKI:

- (a) Private Law mechanisms: Use non-contractual disclaimers and contracts to limit and allocate liability between parties in a PKI. If practical, insure against liability risks.
- (b) (Usually in conjunction with (a)). Wait for test cases to clarify the application of existing legal rules to legal liability issues that are currently uncertain.
- (c) Legislate or regulate new legal rules to reduce or eliminate areas of uncertainty in the existing law.

Essentially the policy-maker's choice is to leave parties to use private law mechanisms (a) or to intervene by legislation or regulation (c) or to do a mixture of (a) and (c).

The remainder of this section of the report considers the adequacy of private law mechanisms to handle legal liability uncertainty and examines in detail Verisign's use of private law mechanisms and the degree to which the Verisign model would work under Australian law.

The next section considers the range of legislative responses around the world. Some jurisdictions have created new rules relevant to legal liability. Others (including Australia) have deliberately refrained from doing so, leaving the issue to private law mechanisms.

4.2 PRIVATE LAW MECHANISMS: DISCLAIMERS, CONTRACT, INSURANCE

Statutory and regulatory frameworks for allocating and managing risk require state action such as legislation. In the absence of such state action, parties must rely on private law mechanisms for managing the risk of legal liability. (Of course, there are many important non-legal risk management techniques such as high quality technical solutions, business processes, key and certificate management protocols and the use of standards and auditing. This report is concerned only with legal mechanisms for managing legal liability.)

Broadly, these legal mechanisms are:

- non-contractual disclaimers (e.g. a statement on a CRL web site or in a certificate that the user relies on information at their own risk);
- contractual provisions allocating risk between parties to the contract; and
- insurance against a risk.

Non-contractual disclaimers can be effective to limit liability (subject to statutory or regulatory override) provided they are sufficiently drawn to the attention of the person to whom liability is sought to be limited.

Contracts provide a stronger bases for limiting or allocating liability because there is usually no question of adequacy of notice (although where terms are incorporated by notice the issue arises). Contractual provisions are however subject to legislative and regulatory provisions designed to protect weaker parties (usually consumers and small business) from over-reaching or unfair liability allocation in contracts.

Having limited their liability to the extent permitted by law, parties may insure their risk. There is a developing market in insurance products for parties to a PKI. For example, The St Paul Insurance Company offers Errors and Omissions Liability insurance cover to CAs which covers claims against the CA for economic loss by those relying on the CA's certificates and Certificate Revocation List (CRL). Similar cover is available for RAs.

Some CAs (e.g. Verisign) exclude their liability to S and RP to the maximum extent permitted by law but then offer to Subscribers (including a RP who is also a Subscriber) an extended warranty (for a fee) which restores some of that liability subject to monetary and other limits (Verisign calls this the Netsure Protection Plan). The CAs then insure their risk of liability under the extended warranty with an insurer such as The St Paul or (in the case of Verisign) Lloyds of London. Part of the fee paid by S for the extended warranty is paid on to the insurer as a premium for the insurance cover.

4.3 MANAGING LEGAL LIABILITY BETWEEN END USERS (S AND RP)

End users are free to contract in advance to allocate liability between them (e.g. for loss arising from unauthorised messages as discussed above). This is not a viable solution in an open system where interactions occur between strangers without a prior contract.

Where a prior contract does allocate liability these provisions will be subject to legislative and regulatory protections for consumers and small business, both general (e.g. unconscionable conduct and unfair contracts legislation) and specific (e.g. the EFT Code of Conduct for electronic funds transfers messages between customers and financial institutions).

4.4 MANAGING LEGAL LIABILITY OF CA TO S AND RP

In order to evaluate the possible approaches to Certification Authority legal liability management, we reviewed a number of existing and proposed CA frameworks and contracts to determine how they have managed the allocation of risk and responsibility of the various parties involved. Frameworks reviewed included:

- Entrust.net (based in Texas and with offices in Canada, the US, the UK, Switzerland, Germany and Japan);
- 128i (based in New Zealand);
- Identrus (formed by eight financial institutions including the Bank of America, Chase Manhattan and Deutsche Bank, but as far as we could ascertain, yet to come into operation);
- Globalsign (a Belgian company with offices throughout Europe); and
- Verisign.

The information available about the respective rights and responsibilities of the parties involved in the Verisign framework was far more comprehensive than for the other Certification Authorities (with the exception of Globalsign, which appears to have substantially adopted the Verisign model). Verisign have clearly done a great deal of work in scoping the respective liabilities of parties involved in PKI infrastructures, and their documents are extremely detailed. As a result, the following analysis concentrates on Verisign's model.

Set out below is a summary of the Verisign model. This is followed by an analysis of various aspects of the Verisign system when considered against the Australian legislative, regulatory and common law environment.

4.5 THE VERISIGN MODEL FOR MANAGEMENT AND ALLOCATION OF RISK AND RESPONSIBILITY

Verisign's Certification Practice Statement ('CPS') is a lengthy and detailed document that purports to control the provision and use of Verisign's public certification services, including applications for certificates, validation of applications, certificate issue, acceptance, suspension and revocation. It is complemented by a number of other documents, such as subscriber agreements.

Verisign offers three levels of certificates, each with particular functionality and security features:

(A) CLASS 1 CERTIFICATES

These are issued to individuals only. They confirm that the user's name/alias and email address are in Verisign's repository and are typically used for web browsing and email security.

Class 1 certificates do not authenticate subscriber identity. User name is considered 'Nonverified Subscriber Information'. As a result, these certificates are not intended for commercial use where proof of identity is required.

(B) CLASS 2 CERTIFICATES

Again, these are issued to individuals only. They confirm that the application identity provided by the subscriber does not conflict with information in well recognised consumer databases (by comparing the name, address and other personal information on the application against widely referenced databases such as credit bureaus). They are used typically for inter- and extra-organisational email, 'low risk' transactions, personal email, password replacement, software validation and online subscription services.

Class 2 certificates provide reasonable but not foolproof assurance of a subscriber's identity. Again, the information they contain is considered to be Nonverified Subscriber Information.

(C) CLASS 3 CERTIFICATES

These are issued to individuals and to organisations. Various procedures are used to obtain probative evidence of the applicant's identity (e.g. individuals must physically appear before a trusted third party such as a notary and organisations must provide authorisation records, which are checked against third party business databases).

The private key for class 3 certificates must be generated and stored in a trustworthy manner according to applicable requirements (for example in a hardware based crypto module). They are used primarily for e-commerce applications like e-banking, EDI and membership-based online services and provide stronger assurance of an applicant's identity than Class 2 Certificates.

(D) CLASS 3 ORGANISATIONAL (SERVER) CERTIFICATE

These provide assurances to an entity trying to authenticate a web site and its owner. Identity is validated by comparing information provided by the applicant to third party business databases or official records.

SUBSCRIBER LIABILITY

Subscribers are required to apply for certificates and, if accepted, must enter into a subscriber agreement with Verisign, in which they agree to be bound by the terms of the CPS. The application, CPS and Subscriber Agreements allocate risk and limit liability in relation to subscribers in a number of ways, as set out below.

(A) PROVISIONS IN RELATION TO SUBSCRIBER'S KNOWLEDGE OF PKI SYSTEMS, PROTECTION OF PRIVATE KEYS AND UNDERSTANDING OF THE DOCUMENTATION

Applicants must acknowledge that they have been advised to receive proper training in the use of public key documents prior to applying for a certificate and that documentation, training and education about digital signatures, certificates, PKIs and the CPS are available from Verisign. They must also acknowledge that they are exclusively responsible for protecting their private key(s) from compromise, loss, disclosure, modification or unauthorised use and, in completing the application, they confirm the information included is correct and that they have read, understood and agreed to the terms of the relevant subscriber agreement.

(B) REPRESENTATIONS BY SUBSCRIBERS ON ACCEPTING A VERISIGN CERTIFICATE

By accepting the certificate, the subscriber agrees to be bound by the continuing obligations of the CPS and the applicable Subscriber Agreement (for the particular type of certificate issued), and assumes a duty to prevent key disclosure. In accepting, the subscriber represents that:

- each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational;
- no unauthorised person has had access to the subscriber's private key;
- all representations in the application are true;
- all information in the certificate is true to the extent the subscriber has knowledge of it; and
- the certificate will be used exclusively for authorised and legal purposes, consistent with the CPS.

(C) INDEMNITY BY SUBSCRIBERS WHO ACCEPT A VERISIGN CERTIFICATE

By accepting the certificate, the subscriber agrees to hold Verisign, the IA and their agents and contractors harmless for any acts or omissions resulting in liability, loss or damage caused by use or publication of a certificate and arising from:

- misrepresentations of fact by the subscriber (or anyone acting on instructions from anyone authorised by the subscriber);
- failure by the subscriber to disclose a material fact if done negligently or with intent to deceive; or
- failure to protect the subscriber's private key adequately.

(D) THIRD PARTY LIABILITY

Subscribers are liable to third parties in relation to any misrepresentations in certificates when the third party reasonably relies on those misrepresentations.

(E) INFRINGEMENT AND OTHER DAMAGING MATERIAL

Subscribers represent and warrant that their use of names does not infringe on third party rights in relation to trade names, trade marks (etc), and that they are not using the name for unlawful purposes (for example misleading and deceptive conduct). Subscribers indemnify IA's from any loss or damage resulting from a breach of this representation and warranty.

LIABILITY AND RELYING PARTIES**(A) STATEMENTS ON CERTIFICATES**

Certificates issued by Verisign contain a field containing a brief statement aimed at Relying Parties, regarding liability and purporting to incorporate by reference the entire CPS. In some cases, the relevant field only has 64 bytes however, which means that the statement is limited to:

'ou = www.verisign.com/repository/CPSIncorp.by.REF.Liab.Ltd(c)97'

Another version of the statement on the certificate is:

'Warning: Use of this certificate is strictly subject to the Verisign Certification Practice Statement. The issuing authority disclaims certain express and implied warranties, including warranties of merchantability, or fitness for a particular purpose, and will not be liable for consequential, punitive and certain other damages. See CPS for details.'

It is not clear from the CPS when the longer statement appears on certificates and when the abbreviated statement appears. In either case, Verisign claims that, because the statements point to the full text of the CPS, the terms of the CPS will be incorporated into an agreement with the party accessing the message.

(B) TERMS OF CPS

The CPS provides that recipients can rely on digital signatures from a subscriber if the digital signature was created during the operational period of a valid certificate and can be verified by referencing a validated certification change, and reliance is reasonable in the circumstances (i.e. if the circumstances indicate a need for additional assurances, they should be sought).

(C) VERISIGN REPOSITORY, RELYING PARTY AGREEMENT AND CERTIFICATE REVOCATION LIST USAGE AGREEMENT

The Verisign Repository is a publicly available collection of databases for storing and retrieving certificates and other information in relation to certificates. It includes details of certificates, CRLs and other suspension and revocation information, current and prior versions of the Verisign CPS and educative information about digital certificates.

Under the heading 'Certificate Status and Information', Relying Parties can click on icons for 'Check the Status of a Digital ID' and 'Find the Certification Revocation List'.

Clicking on 'Check the Status of a Digital ID' brings the Relying Party to a page where they can search Verisign's online database for anyone's Digital ID by entering the name, email address, or serial number and issuer name of the Digital ID into a box, and clicking a search button. Above the boxes in which information is to be entered to conduct a search is the statement:

'By clicking the SEARCH button you accept the terms of our Relying Party Agreement'

The statement has a link to the Relying Party Agreement ('RPA'), which provides that:

- Relying Parties must read the RPA prior to validating a digital ID or using Verisign's database of certificate revocations or other information. If users do not agree to the terms of the RPA, they are not authorised to use the Verisign Repository;
- Relying Parties agree to be governed by the terms of Verisign's CPS;
- knowledge and acceptance of the terms of the RPA is demonstrated by Relying Parties submitting a query to search for, or verify the revocation status of a digital ID, or by otherwise using or relying upon any information or services provided by Verisign's Repository or web site.

The RPA also summarises some of the terms of the CPS (for example the limited obligations of, and warranties by Verisign contained in the CPS and the limitations of type and quantum of liability - see A1.4 in Appendix A for details).

Clicking on 'Find the Certification Revocation List' brings the Relying Party to an index of certificate types. The Relying Party simply clicks on the certificate type that they are interested in to obtain access to a file containing a general description of that type of certificate and a Revocation List detailing the serial number of revoked certificates and the date of revocation. There is no requirement to enter search information on this page, so there is no 'SEARCH' button to click. In amongst the items in the index are two text documents. One is called 'CRL Usage Agreement' and

the other is called 'Readme.txt'. There is no compulsion or request to read either document. Both link through to the Certificate Revocation List Usage Agreement ('CRLUA'), which provides that:

- CRL users must read the CRLUA before downloading, accessing or using any CRL provided by Verisign. If users do not agree to the terms of the CRLUA they are not authorised to download, access or use Verisign's CRLs.
- the CRLUA becomes effective when users download or otherwise access any Verisign CRL.
- individual users are governed by the Relying Party Agreement, which is incorporated by reference into the CRLUA;
- Verisign affiliates or customers using the CRLs are governed by the terms of their agreements with Verisign, as well as the terms of the CRLUA;
- CRL users agree to be governed by the terms of Verisign's CPS;
- intellectual property in the CRLs is the property of Verisign and users are not permitted to do things like copy, sell or rent them;
- knowledge and acceptance of the terms of the CRLUA is demonstrated by users downloading, accessing or using any Verisign CRL or information in a CRL.

The CRLUA also summarises some of the terms of the CPS (for example the limited obligations of, and warranties by Verisign contained in the CPS and the limitations of type and quantum of liability –see below for details).

NON-VERISIGN ISSUING AUTHORITIES

Issuing Authorities (IA's) that are not owned and operated by Verisign must satisfy various criteria to participate in the Verisign PKI. For example, they must be reasonably able to bear the risk of liability to subscribers and recipients of certificates and other persons who may rely on the certificates and time stamps they issue. IAs are also required to maintain insurance coverage for errors and omissions. They are required to execute an IA Agreement with Verisign.

IAs are required to keep an audit trail of all activities. They are required to conduct an initial investigation of all employees, consultants and contractors to determine their competence and trustworthiness. They must also take all necessary precautions to prevent the loss, disclosure, modification or unauthorised use of their own private key(s).

If an IA ceases to operate, it is liable for paying reasonable restitution (not to exceed the certificate purchase price) to subscribers for revoking their certificates before their expiration date.

LIMITED OBLIGATIONS AND WARRANTIES OF VERISIGN AND ISSUING AUTHORITIES

(A) REFUNDS

The CPS provides for unconditional refund of the fee paid for the certificate within 30 days of certificate issuance. After that, refunds are only available if Verisign has breached a warranty or material obligation under the CPS or NetSure Protection Plan.¹

(B) WARRANTIES, DISCLAIMERS AND LIMITATIONS OF LIABILITY WHERE NETSURE PROTECTION PLAN DOES NOT APPLY

Where the NetSure Protection Plan does not apply, Verisign and the IAs give very limited express warranties and exclude all other warranties and obligations of any type. Most of the CPS is occupied with disclaimers, limitations and exclusions of liability.

Verisign and the IAs warrant and promise to do the following in accordance with the CPS:

- provide infrastructure and certification services, including the Verisign Repository;
- provide controls and foundation for the Verisign PKI, including IA key generation, key protection and secret sharing procedures;
- perform application validation procedures required under the CPS for each certificate class;
- issue certificates in accordance with the CPS and honour the representations to subscribers and relying parties in the CPS;
- publish certificates;
- perform obligations of the IA and support rights of subscribers and relying parties who use the certificates;
- suspend and revoke certificates;
- provide for expiration, re-enrollment and renewal of certificates;
- comply with miscellaneous provisions in the CPS.

Verisign and the IAs also warrant that their private keys are not compromised (unless they give notice via the Verisign Repository).

Apart from the above, the CPS provides that IAs and Verisign disclaim all warranties and obligations of any type, including any warranty of merchantability, fitness for purpose, or accuracy of information provided. They also exclude any liability for negligence or lack of reasonable care.

Further, except as expressly provided, the IAs and Verisign:

- do not warrant the accuracy, reliability, fitness for purpose (etc) of information in certificates or otherwise published or disseminated by them;

- shall not incur liability for representations of information in a certificate, provided the certificate substantially complies with the CPS;
- do not warrant 'non-repudiation' of any certificate;
- do not warrant any software.

(C) EXCLUSION OF ELEMENTS OF DAMAGE

Neither the IA's nor Verisign accept liability for indirect, special, incidental or consequential damages, loss of profits, loss of data, etc, arising from or in connection with the certificates, digital signatures or any related services or transactions.

(D) DAMAGE AND LOSS LIMITATIONS WHERE NETSURE PROTECTION PLAN DOES NOT APPLY

The CPS sets out liability caps for both Verisign and the IA's in relation to claims by all people in relation to specific types of certificates as follows:

Class 1 - US\$100

Class 2 - US\$5,000

Class 3 - US\$100,000

NETSURE PROTECTION PLAN PROVISIONS: EXTENDED WARRANTY

The NetSure Protection Plan (the 'Plan') is a program provided by Verisign and backed by Lloyds of London. The Plan is designed to provide extended warranty protection to subscribers of Verisign-issued certificates. The Plan applies exclusively to 'NetSure Subscribers', who are persons issued with a certain class and type of certificate after certain dates. The Plan does not apply to people issued with demonstration, free or test certificates, nor does it offer any protection to Relying Parties.

For the persons covered, the Plan replaces the limited warranties, disclaimers of warranty and exclusions and limitations of liability in the CPS and other service agreements with an enhanced set of limited warranties, which give greater protection. Verisign is permitted to seek and recover damages from persons who may be responsible for the insured's losses.

Details of the Plan are summarised below.

(A) LIMITED WARRANTIES PROVIDED BY PLAN

Limited warranties give protection against:

- Issuing Authority/Verisign supplied content of subscriber certificates;
- reliance on certificates of others (except for any Nonverified Subscriber Information they might contain);
- unauthorised use, unauthorised disclosure or compromise of private keys (unless unauthorised use or disclosure was wholly or partially caused by the Covered Person's intentional conduct or failure to exercise reasonable care to safeguard his/her/its private key);

- unauthorised revocation and loss of use of certificate (applies to certificate owners and Covered Persons seeking to rely on a certificate);
- erroneous issuance and impersonation of a Verisign certificate; and
- delay in requesting revocation.

Covered Persons can receive payment for any incidental or consequential damages caused by a breach of one or more of these limited warranties (but this is subject to the limitations set out in the Policy).

In addition, if Verisign or an IA breaches one of these limited warranties, a NetSure Subscriber can request that their certificate be revoked and they are entitled to a full refund of the amount paid for the certificate.

(B) EXCEPTIONS

The limited warranties do not apply to loss or damage suffered by a Covered Person as a result of (for example):

- their unreasonable reliance on information in a certificate;
- their failure or unreasonable delay in properly communicating a request for revocation of a certificate;
- their failure to exercise reasonable care to protect their private key;
- their failure to apply reasonable security measures to verify digital signatures;
- their failure to use reasonable security measures in using certificates, including failure to determine that a Verisign certificate is operational or failure to validate a certificate chain;
- a force majeure event;
- acts by any person whose conduct damages relevant Internet/telecommunications services (e.g. computer viruses);
- failure of communications infrastructure or storage media;
- brown outs, power failures etc; and
- illegal acts by the Covered Person, a Subscriber or any person relying on a certificate.

(C) LIMITS TO COVERAGE

Limits apply, depending on the class of certificate obtained by the Covered Person. Verisign promises to pay the insured up to certain limits if it breaches one of the warranties provided under the Plan. The most Verisign will pay for ALL breaches during the Operational Period of a certificate is:

Class 1 Certificate US\$1,000

Class 2 Certificate US\$25,000

Class 3 Certificate US\$50,000

Server Certificate US\$100,000

This is called the 'Certificate Lifetime Limit'. Payments made by Verisign under the Plan reduce the Certificate Lifetime Limit. In addition, there is a claim limit for loss sustained due to relying on the Verisign certificate of another, based on the type of certificate relied on (e.g. if the customer holds a class 2 certificate and relies on a class 1 certificate, the per reliance limit is US\$1,000).

Cover under the Plan is dependent on the insured having fulfilled their obligations under the CPS (e.g. by taking precautions to prevent loss or unauthorised use of their private key and using computer systems that are reasonably secure from intrusion or misuse).

(D) DISCLAIMERS OF WARRANTY

The Plan contains specific disclaimers of warranties for:

- accuracy or reliability of Nonverified Subscriber Information;
- representations in certificates where those certificates were prepared substantially in compliance with the service agreement;
- nonrepudiation;
- the standards or performance of hardware or software not under licence to, or exclusive ownership or control of Verisign; and
- the obligations, responsibilities and liabilities of non-Verisign IAs (on-site customers).

There is also a general disclaimer to the extent permitted by law of all other express or implied warranties, including merchantability, fitness for purpose and accuracy of information. The Policy also disclaims liability for any acts by an issuing authority that may be held to be negligent, reckless or offences of strict liability.

(E) LIMITATIONS OF LIABILITY

The following overall limitation is placed on Verisign's liability for general contractual damages suffered by all persons as a result of reliance on a single certificate:

Class 1 Certificate	US\$100
Class 2 Certificate	US\$5,000
Class 3 Certificate	US\$100,000
Server Certificate	US\$100,000

Verisign disclaims liability for certain kinds of damages, including punitive, indirect, special or consequential (except as expressly provided in the Plan).

4.6 VIABILITY OF THE VERISIGN MODEL UNDER AUSTRALIAN LAW – ASPECTS OF THE AUSTRALIAN LEGISLATIVE ENVIRONMENT WHICH IMPACT ON THE VERISIGN MODEL

As is evident from the description above, Verisign has gone to great lengths to try to limit any liability it may have to third parties, whether they be certificate subscribers or relying parties. Taken on its face, the Verisign documentation substantially limits Verisign's exposure. However, an Australian CA will be unable to fully replicate the Verisign limitations of liability given relevant Australian legislative, regulatory and common law rules. This section covers some relevant legislative rules. Subsequent sections cover relevant common law and regulatory rules.

In Australia, consumer protection laws imply non-excludable terms into certain contracts, and prevent unfair conduct such as overly one-sided contractual liability allocation.

For constitutional reasons, consumer protection laws are effected by a combination of Federal, State and Territory Acts.² The *Trade Practices Act 1974* (Cth) ('TPA') in general applies to corporations rather than individuals (unless for example those individuals are engaging in interstate trade or commerce or are aiding or abetting a breach of the TPA by a corporation). The actions of individuals are otherwise covered by the relevant State or Territory Acts. For ease of reference, the provisions of the TPA will be used to illustrate the application of these consumer protection laws to PKI systems.

(A) IMPLIED TERMS OF MERCHANTABILITY, FITNESS FOR PURPOSE AND DUE CARE AND SKILL IN 'CONSUMER CONTRACTS'

The TPA implies into all 'consumer contracts' a number of non-excludable conditions and warranties.³ Any term of a contract that has the effect of excluding, restricting or modifying rights or liability under these implied terms will be void.⁴ For these purposes a person is taken to have acquired goods or services as a 'consumer' if they acquire goods or services either where the price did not exceed A\$40,000 or, if the price exceeds A\$40,000, where the goods or services are of a kind ordinarily acquired for personal, domestic or household use or consumption.⁵

In relation to goods, the warranties and conditions include the following:

- a condition that goods supplied by description will comply with that description;⁶
- a condition that goods will be of merchantable quality (this right does not apply if goods were sold at auction or if the relevant defect was specifically drawn to the consumer's attention before the contract was made, or the consumer examined the goods prior to sale, and that examination should have revealed the defect⁷); and

² *Trade Practices Act 1974* (Cth), *Fair Trading Act 1992* (ACT), *Consumer Affairs and Fair Trading Act 1990* (NT), *Fair Trading Act 1987* (NSW), *Fair Trading Act 1989* (Qld), *Fair Trading Act 1987* (SA), *Fair Trading Act 1990* (Tas), *Fair Trading Act 1985* (Vic) and *Fair Trading Act 1987* (WA).

³ *Trade Practices Act 1975*, Part V, Division 2.

⁴ *Trade Practices Act 1974*, section 68.

⁵ *Trade Practices Act 1974*, section 4B. To fall within the definition, the person must not have acquired the goods for the purpose of resupply or to use them in a process of production, manufacture or repair.

⁶ *Trade Practices Act 1974* (Cth), section 70.

⁷ *Trade Practices Act 1974*, section 71(1). Goods are of 'merchantable quality' if they are as fit for the purpose or purposes for which goods of that kind are commonly bought as it is reasonable to expect having regard to any description applied to them, the price (if relevant) and all the other relevant circumstances (section 66 (2)).

- a condition that where the purpose is made known the goods are fit for the purpose⁸.

In relation to services, the warranties and conditions are as follows:

- a warranty that services will be rendered with due care and skill;⁹
- a warranty that any materials supplied in connection with the services will be reasonably fit for the purpose for which they are supplied;¹⁰ and
- if the consumer makes known any particular purpose for which the services are required, a warranty that the services and materials supplied will be reasonably fit for that purpose (unless the consumer does not rely, or it is unreasonable for him or her to rely on, the corporation's skill or judgement).¹¹

Where a breach occurs of any of the conditions and warranties set out above, the consumer has a right to take action for breach of contract, rather than an action for breach of the *Trade Practices Act*.¹²

Because the definition of 'consumer' is so broad, these conditions and warranties will be implied into an enormous number of contracts including, presumably, a substantial proportion of the contracts entered into between Australian Certification Authorities and their subscribers, and between Certification Authorities and relying parties (if indeed a contract has come into existence between CAs and relying parties—this issue is dealt with in more detail below).

As it is not possible to exclude these conditions and warranties in Australia, it is not open to Australian Certification Authorities to include in their contracts the broad disclaimers adopted by Verisign. As set out above, Verisign disclaims all warranties and obligations that are not specifically included in the CPS, including any warranty of merchantability or fitness for purpose. Australian businesses could disclaim these warranties 'to the extent permitted by law' (i.e. to non-consumer contracts), but the limits to this disclaimer must be appreciated.

In cases where the cost of the goods or services in question does not exceed A\$40,000, and the goods or services are not those ordinarily acquired for personal, domestic or household use, the TPA permits suppliers to limit their liability to the replacement or repair of the goods, or the cost of their replacement or repair or, in the case of services, to the resupply of the services or the cost of resupply.¹³ However, this is subject to an overriding test of fairness. In determining what is 'fair', a court will consider all the circumstances of the case, including the strength of the bargaining positions of the respective parties and whether the buyer knew or ought reasonably have known of the existence of the limitation. However, assuming for a moment that PKI services are not ordinarily acquired for personal, domestic or household use (which is by no means clear), it is questionable whether a court would view the imposition of this sort of liability cap by a Certification Authority as

8 *Trade Practices Act 1974*, section 71(2). This condition will not apply where the circumstances show that the consumer does not rely, or it was unreasonable for him or her to rely, on the skill or judgement of the vendor.

9 *Trade Practices Act 1974*, section 74 (1).

10 *Trade Practices Act 1974*, section 74 (1).

11 *Trade Practices Act 1974*, section 74 (2).

12 *E v Australian Red Cross Society* (1991) 27 FCR 310.

13 *Trade Practices Act 1974*, section 68A.

'fair'. This is because the potential losses suffered by subscribers or relying parties as a result of a breach of one of these conditions or warranties could be too significant to be compensated for by a resupply of CA services or the cost of replacing a certificate (for example, if a certificate was not promptly revoked by the CA on being advised of its compromise and a subscriber or relying party suffered a loss as a result).

(B) LEGISLATIVE PROHIBITIONS ON UNFAIR CONDUCT

The *Trade Practices Act* imposes on corporations a general duty to trade fairly, by prohibiting them from engaging in unconscionable conduct:

- in the supply of domestic goods or services to consumers;¹⁴ and
- in the supply or acquisition of goods or services worth up to A\$1 million to businesses that are not listed companies.¹⁵

The term 'unconscionable' is not defined in the Act, which instead relies on the concept as defined by the courts from time to time. Whether a court will find that conduct is unconscionable will depend on all the circumstances of the case, but generally unconscionable conduct occurs 'whenever one party to a transaction is at a special disadvantage in dealing with the other party because of illness, ignorance, inexperience, impaired faculties, financial need or other circumstances affecting his ability to conserve his own interests, and the other party unconscientiously takes advantage of the opportunity thus placed in his hands'.¹⁶

Whilst the courts are entitled to take into account whatever considerations they see fit, the TPA sets out various issues to be taken into account in determining whether conduct was unconscionable. The list differs slightly for unconscionable conduct in relation to consumers as opposed to businesses.

For consumers the factors to be considered include:

- the relative bargaining power of the parties;
- whether conditions imposed by the supplier were reasonably necessary for the protection of its legitimate interests;
- whether the consumer was able to understand the documentation;
- whether undue influence was exerted, or unfair tactics used; and
- the amount for which and circumstances under which the consumer could have acquired equivalent goods or services from a third party.

For businesses, the factors to be considered include those listed above, as well as:

- the extent to which conduct was consistent with conduct in similar transactions with like customers;
- the requirements of any industry code applicable to the supplier;

14 *Trade Practices Act 1974* (Cth), section 51AB.

15 *Trade Practices Act 1974* (Cth) section 51AC.

16 *Blomley v Ryan* (1956) 99 CLR 362 per Kitto J (at 415).

- any risks to the business consumer arising from the supplier's intended conduct that the supplier should have foreseen would not be apparent to the business customer;
- the extent to which the supplier was willing to negotiate the terms and conditions of any contract of the supply of goods and services;
- the extent to which the parties acted in good faith.

These considerations are not exhaustive. The circumstances in which a court might find that conduct is unconscionable are very broad. They include, for example, lack of education or lack of assistance or explanation in circumstances where assistance or explanation are necessary.

Remedies available for unconscionable conduct include remedial orders (such as rescission of any contract entered into as a result of unconscionable conduct) and injunctions.¹⁷ Section 87(1) gives the Court a wide discretion to make orders 'as it thinks fit'. Application for relief may be made by a party who has suffered loss or damage as a result of a contravention or by the ACCC on their behalf.

Certification Authorities in Australia need to be mindful of these unconscionability provisions when formulating their contractual arrangements. The Australian Competition and Consumer Commission ('ACCC'), which is responsible for overseeing compliance with the TPA, has indicated that clearly one-sided contracts present a high risk situation for a party seeking to enforce them. Some examples of terms and conditions that the ACCC has indicated may be considered to be one sided are those which:

- appear to exclude the legal rights of the weaker party;
- state that the weaker party has agreed to, read or understood terms when this is not so;
- purport to agree that no misrepresentations have been made by the stronger party, or
- require a weaker party to comply with onerous or unrealistic conditions;

The ACCC has also indicated that the failure to negotiate reasonable amendments to standard form terms and conditions will be considered as a factor towards unconscionability, particularly when high risks are involved for the weaker party.

The Verisign model certainly poses a risk of unconscionability claims. This is because the model relies on a number of standard term agreements which contain no provision for negotiation of terms by subscribers or Relying Parties. Although many of the agreements are not themselves lengthy or complex (for example, the Relying Party Agreement is only a couple of pages long), they all incorporate the terms of the CPS, which is a lengthy and quite complex document.

In addition, the agreements contain some quite onerous terms and limitations of liability. In some cases it isn't even clear that a particular agreement is to apply to users who take certain actions (for example, it isn't clear that the Certificate Revocation List User Agreement is to apply to people who access Verisign's CRLs). The agreements also contain statements that the contracting party has read and understood the terms of the agreement, which has been identified by the ACCC as a particular risk factor in relation to unconscionability. Taking all of this into account, and particularly in

circumstances where a particular user might have a special disadvantage (for example poor language or literacy skills or a lack of business acumen), there is a significant risk that some transactions that take place in the Verisign framework would be found to be unconscionable.

As a result, in formulating their PKI framework, Certification Authorities will need to balance this risk against the obvious advantages of using standard form contracts. Some methods to adopt to limit the likelihood of claims of unconscionability being made include:

- use of plain English;
- avoidance of technical terms;
- providing special notice of unusual terms (particularly when click through agreements are used);
- inclusion in application documentation of a recommendation that applicants should seek legal advice prior to making the application for a certificate, and inclusion of an acknowledgement by the subscriber in the subscriber agreement that this recommendation has been made.

(C) ASPECTS OF THE AUSTRALIAN COMMON LAW WHICH IMPACT ON THE VERISIGN MODEL

(i) Contract

There is little doubt that the Verisign model creates binding contracts with the following parties which incorporate the terms of the CPS:

- Subscribers (who enter into subscriber agreements with Verisign which incorporate the CPS by reference); and
- Non-Verisign Issuing Authorities (who enter into Issuing Authority agreements with Verisign which incorporate the CPS by reference).

However, the issue is not as clear in relation to Relying Parties. This presents a potential exposure for Verisign and other certification authorities adopting the Verisign model. If there is no agreement with Relying Parties, the allocations of risk and responsibility to Relying Parties, and Verisign's limitations on its own liability will not be binding on the Relying Parties.

As set out above, Verisign endeavours to contractually bind Relying Parties to the terms of the CPS in three ways:

(A) By including a statement on certificates

As set out above, this statement appears on certificates in either long or short form, as follows:

Short form:

'ou = www.verisign.com/repository/CPSIncorp.by.REF.Liab.Ltd(c)97'

Long form:

'Warning: Use of this certificate is strictly subject to the Verisign Certification Practice Statement. The issuing authority disclaims certain express and implied warranties, including warranties of merchantability, or fitness for a particular purpose, and will not be liable for consequential, punitive and certain other damages. See CPS for details!'

In both cases, Verisign claims that, because the statements point to the full text of the CPS, the terms of the CPS will be incorporated into an agreement with the party accessing the message. In this way, Verisign purports to limit its liability to Relying Parties in the manner set out in the CPS.

It is doubtful whether either the short or long form statement would be seen as creating a valid contract between the Relying Party and Verisign. The short form statement is so brief that it would be very difficult to argue that a Relying Party should realise that it is intended to create a contract between them and a Certification Authority which incorporates another document by reference, and that in that document the Certification Authority limits its liability to the Relying Party.

Even when the statement is given in its long form, there are two other fundamental requirements for formation of a contract that may be difficult to establish (1) an intention on the part of the Relying Party to enter into a legal relationship with Verisign and (2) whether there was consideration moving from the Relying Party to Verisign.

(B) By requiring Relying Parties to enter a Relying Party Agreement

Relying Parties may access Verisign's Repository to check that a given certificate has not been revoked. As set out above, there are two ways that a user can search for revocation information - by clicking on the icon for 'Check the Status of a Digital ID' or on the icon for 'Find the Certification Revocation List'.

Relying Parties who click on 'Check the Status of a Digital ID' are advised that, when they click the 'SEARCH' button, they are accepting the terms of Verisign's Relying Party Agreement. There is a link to the terms of that agreement so that the Relying Party can review them if they wish. The status of click through agreements such as this is not clear in Australia, where there is no relevant legislation or case law on point.

In the United States, click through agreements have been held by the courts to be enforceable provided that the terms of the agreement are 'commercially reasonable' and not otherwise unconscionable or subject to any other defence available under contract law, and the customer has had a reasonable opportunity to consider them and decide whether or not to accept them.¹⁸

It appears likely that Australian courts will take a similar approach, so that, in order to be enforceable a person relying on a click through agreement would need to demonstrate that it had done all that was reasonable in the circumstances to bring the terms and conditions to the attention of the other party.¹⁹ This might include taking reasonable steps to draw the customer's attention to the relevant terms and conditions prior to entering the transaction (especially any terms that might be particularly onerous), providing the customer with a reasonable opportunity to consider those terms prior to entering the transaction, and requiring the customer to click to 'accept' those terms and conditions prior to any product or service being provided.

It is not clear whether the Verisign Repository Notice constitutes reasonable steps to give notice of onerous terms and conditions to satisfy Australian law on incorporation of terms. There is a separate issue as to whether a Relying Party provides any consideration to support the Relying Party Agreement as a contract.

(C) By requiring users of CRLs to enter into Certification Revocation List User Agreements

The situation is less clear in relation to users who click on 'Find the Certification Revocation List'. In this case, user's attention is not clearly drawn to the CRLUA, and it is probable that a court would find that the terms of the CRLUA are not binding on users in the circumstances because it could not be said that reasonable steps have been taken by Verisign to draw the customer's attention to the relevant terms and conditions. It appears that users of the certification revocation list would only come across the CRLUA by chance or out of curiosity, rather than as a result of understanding that, in using the CRL, they are accepting the terms and conditions of the CRLUA. However, it does not appear that major changes would be required to reduce exposure in this regard. The manner in which users' attention is drawn to the CRLUA could simply be altered so that the approach is consistent with that taken for the Relying Party Agreement. The uncertainty in relation to consideration discussed above would also apply here.

(ii) Tort

Assuming for a moment that the statement on certificates set out above is not binding on Relying Parties in a contractual sense (meaning that contractual restrictions on common law obligations will not be effective), there remains an issue in relation to whether the statement may nevertheless be effective to limit the tortious liability of Verisign and, in particular, liability for negligence.

Disclaimers can prevent liability for negligence in two ways:

- in the context of negligent misstatement, a disclaimer may prevent a duty of care arising by dissuading relevant parties from relying on the information provided; and
- a disclaimer may provide a defence to negligent acts generally, by allowing the defendant to show that the plaintiff voluntarily assumed the risk.

In the case of the short form disclaimer on certificates, it is highly unlikely that Verisign could argue that Relying Parties had voluntarily assumed any risk. There is not enough information on the certificate to argue that a Relying Party would know what risks they were assuming when they used the certificate.

In the case of the longer form statement on certificates, it may be that the statement is sufficient to inform Relying Parties of the facts creating the risk what the risk of using the certificate is. However, there may be a problem in establishing that the risk was undertaken voluntarily by the Relying Party. The Relying Party's decision would have to be totally free of constraints to be voluntary. As a result, if the Relying Party has no real choice in relying on the certificate (for example because they can't enter a transaction in any other way or check information against any other source but Verisign), they will not be assumed to have voluntarily undertaken to run the risk and the statement will be ineffective to limit Verisign's liability for negligence.

(iii) Summary of Common Law

In summary, it is unclear whether under Australian law a Verisign-type notice on a certificate could create an effective disclaimer affecting Relying Parties. It is also unclear that the Verisign model creates a binding contract with a Relying Party under Australian law (and, even if it does, whether its terms would survive scrutiny under consumer and small business protection legislation). This leaves an uncertain level of exposure of a CA to a Relying Party in negligence under Australian law. Further research is needed to evaluate the degree of uncertainty and explore whether alternative models could produce workable levels of certainty under Australian law.

(D) ASPECTS OF THE AUSTRALIAN REGULATORY ENVIRONMENT WHICH IMPACT ON THE VERISIGN MODEL

The Verisign liability limitation model will need to fit with existing regulatory regimes directed toward protecting consumers and small business in using electronic authentication methods. One such regime is the EFT Code of Conduct which allocates liability between a customer and a financial institution for unauthorised electronic messages instructing a debit to the customer's account. The Code is currently being revised to cover all forms of electronic authentication including digital signatures. The draft Code regime is generally more favourable to consumer and small business subscribers who originate messages than the Verisign terms and conditions. The Code does not directly affect the liability of a CA intermediary because it allocates risk only between the customer (subscriber) and financial institution (Relying Party). However, in deciding whether to use digital

signatures and certificates supplied by a CA, a financial institution would need to consider the extent to which the contractual liability arrangements of a PKI system were compatible with the institution's regulated liability allocation under the EFT Code.

5

Legislative solutions for managing legal liability uncertainty

5.1 ANALYSIS OF DIFFERENT LEGISLATIVE MODELS

The state of laws and regulations relating to electronic authentication around the world has been described as ‘legislative chaos’,²⁰ with a number of quite different legislative approaches being adopted. A useful categorisation of the different approaches throughout the world has been formulated by Aalberts and van der Hof (1999).²¹ Their framework has been used below. It is based on three broad categories:

- technology-specific approach (usually focussed on PKI);
- two tier approach: technology specific approach and a technology-neutral approach; and
- minimalist or technology neutral approach.

5.2 TECHNOLOGY-SPECIFIC APPROACH

This approach concentrates on the regulation of the technology of digital signatures. It focuses on the legal status of the digital signature and can be broken down into 3 subcategories – technical, legal consequences and organisational. These are outlined below.

37

(A) TECHNICAL

This approach sets digital signature technology as the technical standard for secure electronic commerce. It concerns itself with the general use of digital signatures, without dealing with the legal consequences that arise out of that use.

Example – German Digital Signature Law (GDSL)

The GDSL is focussed on providing a safe and secure infrastructure for the use of digital signatures, in order to enable electronic commerce to flourish. It sets content and security standards for digital signatures, but does not contain any liability allocation provisions. Compliance is voluntary.

(B) LEGAL CONSEQUENCES

This approach concentrates on the recognition of digital signatures for legal purposes and includes liability allocation rules or presumptions.

(i) Models regulating the duties and liabilities of certification authorities and subscribers

Generally the approach adopted under the legal consequences model is to couple the imposition of duties on certification authorities and subscribers with limitations of their liability to third parties. Some of the duties imposed are absolute (that is, they cannot be

²⁰ B.P. Aalberts & S. van der Hof, Digital Signature Blindness, *Analysis of legislative approaches toward electronic authentication*, November 1999, Online available at <http://cwis.kub.nl/~frw/people/hof/ds-fr.htm>.

²¹ See footnote 1.

contracted out of) and some are negotiable (that is, they will apply in the absence of a contrary agreement by the parties). This approach has been adopted for example in Utah²² and Minnesota.²³ The manner in which rights and liabilities are generally allocated in this model is outlined below.

(A) Representations and indemnities by subscribers

In accepting a certificate from a certification authority, subscribers certify to all who reasonably rely on the certificate that:

- they rightfully hold the private key corresponding to the public key listed in the certificate; and
- all representations made by the subscriber to the certification authority in relation to issuing the certificate or made by the subscriber in the certificate itself are true.

This certification cannot be disclaimed or contractually limited.

A duty may also be imposed on subscribers to exercise reasonable care to retain control of the private key and prevent its disclosure to unauthorised persons.

Subscribers indemnify the issuing certification authority for any loss or damage caused by issuing a certificate in reliance on false information which is provided by the subscriber negligently or with intention to deceive.

(B) Warranties and obligations of certification authorities

By issuing a certificate, certification authorities warrant to the subscriber that:

- the certificate contains no information that the certification authority knows to be false;
- the certificate satisfies all material requirements of the relevant legislation; and
- the certification authority has not exceeded any limits of its licence in issuing the certificate.

The certification authority can't disclaim or limit these warranties.

Unless the subscriber and certification authority otherwise agree, a certification authority, by issuing a certificate, is required to:

- act promptly to suspend or revoke a certificate in accordance with the requirements of the relevant Act; and
- notify the subscriber within a reasonable time of any facts known to the certification authority which significantly affect the validity or reliability of the certificate once it is issued.

22 Utah Digital Signature Act 1995.

23 Minnesota Electronic Authentication Act.

By issuing a certificate, a certification authority certifies to all who reasonably rely on the certificate that (for example), the information in the certificate is accurate and the certification authority has complied with all applicable laws in issuing the certificate.

(C) Recommended reliance limits

By specifying a recommended reliance limit in a certificate, the issuing certification authority and the subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

(D) Limitations of liability of certification authorities

Where reliance limits have been recommended in a certificate, a certification authority will not be liable in excess of the amount specified in the certificate for either a loss caused by reliance on a misrepresentation in the certificate or failure to comply with the relevant Act in issuing the certificate.

Unless a certification authority waives its rights, it won't be liable for loss caused by reliance on false or forged digital signatures.

The liability of certification authorities is limited to direct, compensatory damages. They are not liable for punitive or exemplary damages; damages for lost profits, savings or opportunity; or damages for pain or suffering.

(E) Duties of relying parties

This model does not as a general rule impose duties on relying parties. In fact, they generally provide that courts adjudicating disputes involving digital signatures are required to presume that the recipient of a digital signature has no knowledge or notice that the signer either:

- breached their duty as a subscriber; or
- does not rightfully hold the private key used to affix the digital signature.

(ii) Models which also regulate the duties and liabilities of repositories

Some legislatures, for example Malaysia²⁴ and Missouri,²⁵ regulate the duties and liabilities of repositories of certificates in addition to those of certification authorities and subscribers.

For example, a non-excludable liability may be imposed on repositories for losses suffered by persons relying on a certificate more than one business day after the repository has received a request to publish notice of revocation where that notice was not published. This liability may be limited by the recommended reliance limit on the certificate and/or by

²⁴ Malaysian Digital Signatures Act.

²⁵ Missouri Digital Signature Act.

excluding liability for punitive or exemplary damages, and liability for repositories may otherwise be excluded.

(C) ORGANISATIONAL

In this approach, digital signatures are not set as the technical standard, but instead requirements are imposed in relation to the organisation of certification authorities, for example regulating their operations, security, supervision and licensing. The aim is to promote confidence in electronic transactions by ensuring that certification authorities are reliable and secure. These models contain no explicit legal liability consequences for parties using CA services.

Example - Japan's ECOM Certification Authority Guidelines

The Japanese guidelines offer guidance to certification authorities in relation to management, operation, system and facility requirements. They are not binding and contain no provisions dealing with the legal consequences regarding the use of digital signatures.

The Guidelines recommend that certification authorities determine their own policies in relation to their own duties and the duties of persons acquiring or using their certificates, and that the policy should be disclosed in the certification authority's CPS. The Guidelines set out situations in which certification authorities may be liable and recommend that certification authorities should define their level of responsibility and liability for compensation for losses in each situation (for example where certification management requirements, key control requirements or revocation controls are violated).

5.3 TWO-TIER APPROACH

Tier 1 provides legal recognition (e.g. for form purposes) of a wide range of electronic signatures and Tier 2 provides special legal consequences (often relevant to liability allocation) for PKI digital signatures or 'secure electronic signatures' based on a digital signature paradigm. Examples of legislation which adopts this approach are:

(A) EUROPEAN UNION DIRECTIVE ON A COMMON FRAMEWORK FOR ELECTRONIC SIGNATURES 1999

The Directive is an example of a regime which imposes duties on CAs, imposes liability on CAs in some situations but also allows for liability of CAs to be capped in some circumstances.

The Directive focuses on liability allocation for CAs, but does not address liability allocation for signers or reliers. The approach taken by the Directive effectively imposes a duty of care on CAs to verify information provided by applicants for certificates and to ensure that certificates contain all information necessary to be considered a qualified certificate.

The Directive provides that if a CA issues a certificate, then that CA is liable to any person who reasonably relies on the certificate unless the CA can show that it has not acted negligently. Member states are also required to ensure that a CA is liable if it fails to register the revocation of a certificate unless the CA can show that it did not act negligently.

The Directive requires EU member states to ensure that CAs may define use and value limits for any certificate which they issue provided that those limits are recognisable to third parties. The CA will not be liable for damages arising from uses of the certificate outside such limits.

(B) SINGAPORE: ELECTRONIC TRANSACTIONS ACT 1998 ('SETA')

SETA imposes some duties on participants and allows for liability to be capped or excluded in some instances.

SETA provides for attribution of an electronic record by attributing it to the message originator if the originator actually sent the record or if the record was sent by an authorised agent of the originator or an information system programmed by or on behalf of the originator to operate automatically.

A recipient is entitled to regard an electronic record as being that of the purported originator if the recipient verifies that the record came from the originator by applying a procedure agreed between the parties to authenticate the record. A recipient may also assume that a record came from the purported originator if it has been verified by a third party (probably a CA).

The Act imposes on addressees a duty to use reasonable care to verify that an electronic record is that of the purported originator.

SETA allocates to the relier the risk that a digital signature is invalid, if, having regard to specified factors, the reliance was, in the circumstances, not reasonable. The Act is silent as to whether, if the reliance was reasonable, liability for an invalid signature will fall on the originator or the CA.

SETA absolves CAs from liability for loss caused by reliance on a false or forged digital signature if, with respect to that signature, the CA complied with the requirements of the Act.

CAs are also absolved from liability, in excess of an amount specified on a certificate as the 'recommended reliance limit', for loss caused by reliance on a misrepresentation in the certificate or any fact which the certificate is required to confirm.

(C) UNCITRAL DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

The Draft Uniform Rules are an example of a regime which imposes duties on participants and provides opportunities for CAs to limit their liability in certain defined situations.

The Draft Uniform Rules contain a presumption of attribution that an electronic communication has been sent by the purported originator in the absence of evidence to the contrary.²⁶

Article 8 imposes obligations on subscribers to exercise reasonable care to avoid unauthorised use of their signature device and to notify appropriate persons without undue delay if they know their signature device has been compromised, or if there is a substantial risk of this. Subscribers are also required to exercise reasonable care to ensure the accuracy and completeness of material representations they make in relation to the certificate. Subscribers will be liable for a failure to satisfy any of these requirements.

Article 9 imposes obligations on CAs. These include exercising due diligence to ensure the accuracy and completeness of all material representations which the CA makes that are relevant to the life cycle of the certificate or which are to be included in the certificate. The latter category would, presumably, include the identification information provided by the subscriber.

CAs are required by Article 9 to provide reasonably accessible means by which to enable relying parties to ascertain any limitations on the purposes or value for which the signature device may be used. They must also provide a means for subscribers to notify them that their signature device has been compromised. CAs must also utilise 'trustworthy' systems, procedures and human resources in performing their services (matters to be considered in determining if a system is 'trustworthy' are set out in Article 10).

CAs will be liable for a failure to satisfy any of the above requirements.

Under Article 11, relying parties will bear the legal consequences of their failure to take reasonable steps to verify the reliability of an electronic signature or, where an electronic signature is supported by a certificate, their failure to take reasonable steps to:

- verify the validity, suspension or revocation of the certificate; or
- observe any limitation with respect to the certificate.

5.4 MINIMALIST (OR TECHNOLOGY-NEUTRAL FUNCTIONAL-EQUIVALENCE) APPROACH

Legislation which adopts a minimalist approach does not address specific technological solutions. It is, in fact, technology neutral. This type of legislation provides legal recognition of a wide range of electronic signatures (e.g. for form purposes) but most examples do not make provision for sender attribution or allocation of liability.

Examples of legislation which adopts a minimalist approach are:

- UNCITRAL Model Law 1996 . The Model Law does contain a presumption of sender attribution but this has not been followed in any technology-neutral implementation of it, including the legislation drafted in the following jurisdictions.
- Australia. *Electronic Transactions Act 1999* (Cth) and corresponding Bills in the State Parliaments of NSW and Victoria.
No presumption of sender attribution. No rules for allocation of liability.
- Canada. Uniform *Electronic Commerce Act*, drafted by the Uniform Law Conference of Canada.
No presumption of sender attribution. No rules for allocation of liability.
- United States of America. Uniform *Electronic Transactions Act*, drafted by the NCCUSL (National Conference of Commissioners on Uniform State Law) enacted in several States.
No presumption of sender attribution. No rules for allocation of liability.
- United Kingdom. *Electronic Communications Bill*.
No presumption of sender attribution. No rules for allocation of liability.

It is noteworthy that all the major first world common law countries have joined Australia in adopting the minimalist approach.

6

Assessment of liability management options and recommendations to NEAC on further work

6.1 ASSESSING LIABILITY MANAGEMENT SOLUTIONS

This section of the report examines the adequacy of current Australian law and private law mechanisms for managing legal liability. It then examines whether any legislative intervention is required. Tentative conclusions are provided with a recommendation of further initiatives NEAC could undertake to promote adequate levels of certainty and reasonable risk/reward propositions for all parties to a PKI.

6.2 ADEQUACY OF EXISTING LAW AND PRIVATE LAW MECHANISMS FOR MANAGING LEGAL LIABILITY IN S-CA, S-RP AND CA-RP RELATIONSHIPS

(A) S V CA

Liability allocation in this relationship will almost invariably be controlled by contract. Contract terms including extended warranties backed by insurance and the use of certificates with stated reliance limits and limited duration should provide adequate risk management mechanisms for Subscribers and CAs vis a vis each other. Direct insurance cover for Subscribers may also emerge.

The main weakness in private law mechanisms in this relationship is that CAs may impose onerous, one-sided liability allocations on Subscribers. This risk will be greatest if government coerces Subscribers to use digital signatures and certificates or the market for CA services is immature and uncompetitive (as it is currently), making it unlikely that CAs will compete to offer better liability terms to subscribers. In this scenario policy-makers need to consider whether Subscribers have adequate legislative or regulatory protection against one-sided liability allocations in their contracts with CAs.

Conclusion: current law and private law mechanisms are in general adequate to manage liability allocation between Subscribers and CAs but adequacy of legislative protection of consumer and small business subscribers from one-sided CA contracts should be reviewed.

(B) S V RP

If S and RP have a master contract governing their electronic relationship, they can allocate liability for unauthorised and altered messages in that contract. The comments above about the adequacy of legislative and regulatory protection of the weaker party from unfair contracts apply here also.

If they do not have such a contract, S will be bound by messages digitally signed by S or with his authority. There may be some evidential uncertainty in determining that issue but not significant uncertainty as to the legal rule. Where S claims that messages have been digitally signed without S's authority, RP may seek to sue S in negligence. It is unclear whether S owes RP a duty of care in negligence to take reasonable care of S's private key.

RP therefore carries a risk of relying on unauthorised or altered messages that appear to come from S. RP may have recourse against the CA, although the CA is likely to have limited its liability to the maximum extent permitted by law. RP's other options to manage its risk are:

- insurance - either direct insurance or insurance cover obtained through a CA (for example, Verisign's extended warranty cover to the reliance limit of the certificate if RP is also a Verisign Subscriber);
- normal commercial checks equivalent to those that might be used in paper-based commerce that is concluded at a distance, such as email, fax or telephone call backs to confirm the message and its authenticity, using reliance limits (or credit limits) for the apparent message sender.

Conclusion: Current law and private law mechanisms are in general adequate to manage liability allocation between Subscribers and Relying Parties subject to (a) the continuing development of suitable risk management measures such as certificate reliance limits and insurance cover and (b) review of the adequacy of legislative protection of consumers and small business from one-sided contractual liability allocations.

(C) CA V RP

If the CA can effectively impose liability limitations on the RP by a notice in a certificate or by an online contract if the RP consults the CA, then the CA can manage its liability exposure to the RP. The extent to which a CA can follow the Verisign model to impose such liability limitations under Australian law is unclear.

This issue requires further research including the testing of models somewhat different to those used by Verisign under US law. Even if a model is effective under Australian common law, the effect of consumer and small business protection legislation on the model needs to be considered.

Conclusion: It is unclear whether current Australian law and private law mechanisms can give adequate certainty in managing liability allocation in the CA-RP relationship. Further research on private law mechanisms and the current law is required. Depending on the outcome of that research consideration may need to be given to legislation to impose mutual duties and liabilities (with appropriate limits) on CAs and RPs.

6.3 NEED FOR LEGISLATIVE INTERVENTION IN LIABILITY ALLOCATION

Current Australian government policy settings are to let parties in a PKI determine liability allocation among themselves using private law mechanisms against the background of existing law, rather than to create new legislative rules such as presumptions of message attribution or new legal duties or liability caps.

Some jurisdictions have legislated rules or presumptions of attribution for electronically signed messages which would resolve the evidential and legal uncertainty discussed above in the relationship of RP and S. Australia deliberately did not do this in the *Electronic Transactions Act 1999* for reasons set out in the

Electronic Commerce Expert Group's report which were adopted by the Government: The relevant paragraphs of the report state:

- '4.5.76 Government policy in this area of electronic commerce should, as noted in paragraph 4.2.13, promote a competitive market for new technologies by clearing apparent legal obstacles, rather than trying to create solutions for obstacles which may not arise in practice. A legislative allocation, as between apparent originators and addressees of data messages, of the commercial risk of unauthorised messages or of messages altered in transit, may involve pre-emptive assumptions about efficient and fair business practices in a wide commercial context and may have serious unintended consequences.
- 4.5.77 It is our view that, in general, legislation should not create rules which either prefer or disadvantage electronic commerce compared with paper-based commerce. The use of signatures on paper for commerce at a distance (by mail or facsimile) involves the risk of forged or unauthorised signatures. However, there is no general legislative rule that entitles an addressee to presume that a signature is the genuine signature of the apparent signer. The law of agency will often entitle the addressee in the case of unauthorised application of a genuine signature to assume that the apparent signer is bound. The presence of the apparent signer's name or letterhead or other indicia of authority will usually be good evidence that the signature is genuine. But the apparent signer is free to adduce evidence of forgery or unauthorised use and, in general, the addressee takes the risk that the signature was a forgery and therefore not binding on the apparent signer³⁸.
- 4.5.78 The law should not seek to place addressees of electronically signed data messages in a better position than addressees of manually signed paper-based messages. In both cases, addressees should be able to rely on the rules of agency and in both cases originators should be free to adduce evidence of forgery or unauthorised use without legislative obstacles such as article 13(2)(b) and (3) of the UNCITRAL Model Law on Electronic Commerce 1996. It is our view that legislated attribution rules should not go beyond restating the common law. This means that, as in paper-based commerce, addressees will have to manage the commercial risk of forgery or unauthorised signature. They can do this by requiring reliable authentication methods or seeking additional authentication indicia which create a strong evidential basis that the apparent originator did send the data message. Where an addressee and originator regularly exchange messages they can agree on specific attribution rules for their communications in a trading partner agreement.'

The Expert Group did note that as the market for electronic authentication services develops there may be a need for the development of more detailed attribution rules.

Following our review of the existing law, private law liability allocation mechanisms and international legislative developments and current government policy settings, we make the following points on the need for legislative intervention.

Private Law Mechanisms for allocating legal liability appear adequate for managing legal liability in the relationships of S v RP, S v CA and CA v RP, subject to two exceptions:

- (a) Contractual exclusions and limitations of liability may be overly one-sided in favour of the party with stronger bargaining power. This can lead to an allocation of risk and reward among the parties which either deters one group of parties from participating in a PKI or, if they are forced by government requirement or economic necessity to participate, exploits that group.

In the context of the S v RP, S v CA and CA v RP relationships, this issue can be dealt with by legislative or regulatory intervention in favour of the weaker party (usually a consumer or small business). Existing laws (e.g. *Trade Practices Act* and *NSW Contracts Review Act*) deal with this issue at a very general level and it is not yet clear how they will apply in the context of electronic authentication liability. Other more targeted regulatory regimes like the EFT Code of Conduct are much clearer in application but apply to particular transaction types.

The Attorney-General's Expert Group on Electronic Commerce considered this issue in the context of the S v RP relationship. The Group preferred negotiated contractual allocations of liability to legislatively imposed allocation of liability but also recommended legislative protection against unfair contractual allocation provisions (based on the model of s.68A(3) of the *Trade Practices Act* 1974).

'4.5.79 The commercial risks of acting on forged or unauthorised data messages will vary according to the type of commerce being conducted. Attribution rules agreed by the parties in specific contexts are more likely to produce efficient and fair allocations of risk than general legislative rules which apply to a wide variety of data messages and authentication methods. However, we are mindful of the need to protect parties in a significantly disadvantaged bargaining position from having unfair attribution and risk allocation rules imposed on them through contract. In our view this problem can be dealt with by providing that parties can establish their own attribution and risk allocation rules by agreement but that a party cannot rely on agreed rules of attribution unless it is fair and reasonable to do so in all the circumstances. A non-exhaustive list of matters relevant to evaluating fairness and reasonableness should include:

- the reliability and security of any procedures which are used by the originator and addressee to authenticate the originator of the data message or to ensure that the content of the message received is the same as that which was sent; and
- the reliability and security of the access device used by the originator to operate such procedures.'

(Footnotes deleted)

Although such a provision was included in the first draft of the Electronic Transactions Bill, it was removed on the grounds that it was a consumer/small business protection measure which should be placed in consumer protection legislation rather than in general facilitative legislation like the Bill.

NEAC may wish to consider whether there is adequate legislative protection of consumers and small business users against unfair contractual liability allocation.

- (b) The uncertainty as to whether CAs and RPs can manage liability allocation in their relationship (if not resolved on further research and consideration of alternatives to the Verisign model), may justify legislation.

Further research might indicate that it is not possible for parties to manage their liability exposure using private law mechanisms. If so, the result could be that a market for certification services will not develop for want of participants or such a market will allocate resources inefficiently because of legal uncertainty. In this case, legislative clarification of rights, duties and liabilities of CAs and RPs may be warranted. For example, RPs could be required to check the current validity of a certificate before they can reasonably rely on it. CAs could be made liable to RPs on their certificates in a more meaningful way than under the Verisign model but in return could be given the ability to impose enforceable reliance limits on certificates, which are helpful to all parties to a PKI in managing their legal liability. The European Union Directive on a Common Framework for Electronic Signatures 1999 is drafted to achieve these results.

If a legislative course is followed, our preliminary view is that the European Union Directive on Electronic Signatures provides a more useful model for Australia than the current version of the UNCITRAL Draft Uniform Rules on Electronic Signatures because it is focussed on balancing duties and liabilities of CAs towards RPs. The UNCITRAL Draft Rules legislate for duties and liabilities as between end users (S and RP), which we consider unnecessary and a departure from current Australian policy settings. As between CAs and RPs they appear to impose duties more akin to a legislated version of the Verisign model.

A full evaluation of various legislative models should await a sound understanding of the adequacy or otherwise of Australian law concerning the CA v RP relationship (which requires more research). The warning of Biddle against legislative forcing or protection of unsustainable business models should be considered,²⁷ along with other policy analyses.²⁸

6.4 OTHER MATTERS

There are two other important matters relevant to legal liability allocation where NEAC may be able to take a constructive role:

(A) DEVELOPMENT OF RISK RELIANCE AND CONTAINMENT MEASURES AND INSURANCE PRODUCTS

The work of St Paul in drafting insurance products for RAs and CAs and of Verisign in developing liability caps and reliance limits for certificates under the Netsure Protection Plan is extremely helpful for Subscribers, CAs and RPs in evaluating levels of risk and making rational reliance

²⁷ Biddle, B. 'Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace' at www.w3journal.com/7/53.biddle.wrap.html.

²⁸ Eg. Baum, 'Technology Neutrality and Secure Electronic Commerce: Rule Making in the Age of Equivalence' (1999) available at www.verisign.com/repository/pubs/tech-neutral.

decisions. It would seem very desirable for NEAC to explore whether it could encourage the development of these risk management and insurance mechanisms in the Australian market. NEAC could examine whether risk management and insurance arrangements of the following types could be developed:

RPs who were not Subscribers could rely on a certificate up to its reliance limit;

- some certificates could carry periodic reliance limit caps (e.g. a total reliance limit of \$10,000 per 24 hour or 7 day period) with the cumulative level being monitored and advised by a CA or other trusted repository which RPs had to access in order to be able to claim under the periodic reliance limit;
- insurers offer direct insurance to Subscribers and Relying Parties in addition to insuring Subscribers through a CA's extended warranty program.

(B) RECOGNISING THE INSECURE COMPUTING PLATFORMS OF MOST END USERS AND ENCOURAGING DEVELOPMENT OF TECHNICAL SOLUTIONS TO IMPROVE END USER SECURITY

Most end users (S and RP) use standard personal computers which are non-trusted computing platforms. Until more secure solutions (such as smart cards) are widely distributed in the market, this situation has the following implications:

(i) Key Storage and Signing Mechanism

Subscribers who have to use personal computers to store their private keys can, at best, protect their keys by password access to the PC. However, a security chain is only as strong as its weakest link and, on a regular PC, the security of 1024 bit RSA encryption is diminished to an 8 character password often with no firewall protection. Liability allocation rules need to take account of this practical reality for most end users and the consequent vulnerability of keys to theft by colleagues or other third parties or to trojan horse programs. NEAC may be able to encourage the development and roll out of more secure end user computing platforms.

It is consistent with the least cost avoider approach of economically efficient liability allocation rules, to impose some liability on those who control of influence the security of end user platforms as an incentive for them to innovate to improve the security of those platforms and thus reduce the incidence of losses. This point is elaborated in the context of sharing liability between EFT system providers and users in the ASIC EFT Working Group's Discussion Paper on an Expanded EFT Code of Conduct (July 1999) pp. 28-29, available at www.asic.gov.au.

(ii) Certificate Management

Relying parties using a regular PC can have fake certificates planted in their browser's repository by a trojan without their knowledge. If the RP's authentication software does not check the status of a certificate online at a CA but in the certificate repository of their Internet browser the RP can be tricked into relying on an untrustworthy certificate.

NEAC could examine the availability, user-friendliness and security of certificate management and verification software available to end users and, if this is found unsatisfactory, encourage the development and distribution of better products.

More details on these and other limitations of current implementations of PKI with non-trusted end user computing bases can be found in Ellison and Schneier, 'Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure' (2000) 16(1) Computer Security Journal (at www.counterpanel.com/pki-risks.htm) and a forthcoming article by McCullagh and Caelli, 'Non-Repudiation in the Digital Environment' in the Bond University Law Review.

6.5 INTERNATIONAL HARMONISATION OF LIABILITY MANAGEMENT SOLUTIONS

E-commerce is a global phenomenon. Authentication of remote parties will occur across borders and legal liability issues will arise between parties in different jurisdictions. Australian domestic solutions to liability management issues (whether common law or legislation) are not necessarily applicable or operative in other jurisdictions.

The issue of cross-border recognition of certificates and certification authorities is a difficult one. It is made more so where one jurisdiction enacts a peculiar licensing regime for CAs or gives such CAs and their certificates special legal privileges.

In general, private law mechanisms for liability allocation, especially those based on contractual allocation of liability and contracts of insurance, will be 'transportable' among the large number of countries which hold to the principle of party autonomy. These countries will start from the position of holding parties to their contracts, although their domestic systems of laws may contain different rules for excusing performance or overriding harsh or unconscionable terms in these contracts. Contractual allocation of risk is likely to receive wider recognition and enforcement across these countries than the legislative allocation of risk of one country related to the dispute.

This is another reason for preferring private law mechanisms to legislative solutions where possible, as we have recommended for the relationships of S – CA and S – RP. But if private law mechanisms cannot provide an adequate domestic solution (as may be the case for the CA – RP relationship), then a legislative solution is needed. That legislative solution should first be appropriate for domestic needs and secondly, be capable of harmonisation with the law applying in Australia's major trading partners. The EU Directive on Electronic Signatures is already law for the European Union and is a possible mode for legislation on the CA – RP relationship, if further research indicates legislation is necessary. The UNCITRAL Draft Rules may also achieve widespread acceptance. (This remains to be seen as their content is more controversial than that of the Model Law on Electronic Commerce of 1996.) But the Draft Rules take a different approach to that recommended in this report by legislating for the S – CA and S – RP relationships and dealing differently with the CA – RP relationship.

If Australia later consider a legislative allocation of liability, it will need to consider the international compatibility of that legislative model with the law of our major trading partners.

6.6 RECOMMENDATIONS FOR NEAC'S FURTHER WORK

- (a) (i) Undertake further research on the adequacy of private law mechanisms under Australian law to provide certainty in managing liability allocation in the CA – RP relationship.
- (ii) If that research suggests that private law mechanisms cannot provide adequate certainty consider whether legislation is necessary to impose duties and liabilities and appropriate limits of these on CAs and RPs and what its form should be. Various international models should be considered, particularly the European Union Directive on a Common Framework for Electronic Signatures 1999.
- (b) Evaluate whether there is adequate legislative protection of consumers and small business (both as Subscribers and Relying Parties) against unfair contractual liability allocation in all of the relationships S – CA, S – RP, CA – RP. If not, consider whether additional legislative protection is required and whether this could be tightly focussed to minimise uncertainty of application.
- (c) Consider ways to encourage the development of:
- insurance products for Subscribers, Relying Parties and CAs; and
 - risk management features for PKI certificates such as per transaction reliance limits and periodic reliance limit caps;
- which parties can use to accurately measure and manage their risk.
- (d) Consider how to encourage CAs and vendors of computing platforms to provide trusted computing platforms and software to end users for:
- secure storage of private keys and operation of signing mechanisms;
 - secure and user-friendly certificate management and verification functions.

7

NEAC's response to the recommendations

- **FURTHER RESEARCH INTO PRIVATE LAW MECHANISMS FOR CERTIFICATION AUTHORITIES AND RELYING PARTIES AND, IF NEEDED, EVALUATE LEGISLATIVE RULES FOR CA – RP**

The scoping study analysed the adequacy of current Australian law to determine the allocation of liability among three parties to a PKI: a Subscriber for a digital certificate, a Certification Authority which issues a certificate, and a Relying Party who relies on the certificate. The study considered the private law mechanisms of disclaimers, contracts and insurance, as well as statutory provisions and the common law.

The study found that Australian law and private law mechanisms are adequate except in the case of the relationship between the Certificate Authority (“CA”) and the Relying Party (“RP”). Australian law and private law mechanisms do not provide adequate clarity or guidance as to whether or not a CA will owe a duty of care to a RP who is unknown to the CA (either because the RP does not consult the CA’s certificate repository or CRL or does so anonymously and therefore is a member of a large and diffuse class which is incapable of determination). The extent to which a CA could impose contractual liability limitations under Australian law is unclear.

The issue requires further research including the testing of models somewhat different to those used US law. Even if that model is effective under Australian common law, the effect of consumer and small business protection legislation on the model needs to be considered.

National Electronic Authentication Council supports further research on private law mechanisms and the current law in this regard. The working group under NEAC and the NOIE secretariat will be charged with writing a consultancy scope to progress this research. It is agreed that this further research will be sponsored by NEAC.

- **EVALUATE ADEQUACY OF CONSUMER/SMALL BUSINESS PROTECTION IN ALL RELATIONSHIPS**

NEAC notes the study’s findings that current law and private law mechanisms are in general adequate to manage liability allocation between Subscribers and CAs, but adequacy of legislative protection of consumer and small business subscribers from one sided CA contracts should be reviewed. The main weakness in private law mechanisms in this relationship is that CAs may impose onerous, one-sided liability allocations on Subscribers, which might prejudice the beneficial take-up of PKI and e-commerce.

NEAC considers that it should sponsor some further evaluation and analysis into the adequacy of legislative protection of consumers and small business (both as Subscribers and Relying Parties). This analysis would assess a range of relatively unfair and fair models for allocating contractual allocation in all of the relationships – S-CA, S-RP, CA-RP.

- **ENCOURAGE DEVELOPMENT OF INSURANCE PRODUCTS AND BETTER RISK MANAGEMENT FEATURES FOR ALL PARTIES**

NEAC notes the scoping study's finding that there has been some work by St Paul (USA) in designing insurance products for RAs and CAs and of Verisign (USA) in developing liability caps and reliance limits for certificates under the Netsure Protection Plan. This appears to help Subscribers, CAs and RPs in evaluating the levels of risk and making reliance decisions.

NEAC will work with industry groups such as the Certification Forum of Australia (CFA) to explore the development and deployment of risk management and insurance mechanisms in the Australian market. In particular, NEAC will examine, in consultation with the Certification Forum of Australia, whether risk management and insurance arrangements suitable to the Australian market can be developed. NEAC and the CFA could sponsor a development workshop on this subject to facilitate such developments.

It should also be noted that there are a number of companies entering the Australian market presently who are keen to engage with PKI users to develop and deploy risk management and insurance products.

- **ENCOURAGE DEPLOYMENT OF TRUSTED COMPUTING PLATFORMS AND SOFTWARE TO END USERS (S AND RP)**

The scoping study identified that most end users (S and RP) use standard personal computers which are non-trusted computing platforms, and that until more secure solutions such as smart cards are widely distributed in the market private keys are vulnerable to theft and there are consequent liability implications.

NEAC is considering the suggestion that it encourage the development and roll out of more secure end user computing platforms by working with industry groups and in an industry development context. NEAC is seeking advice of notable academic experts in this field to ascertain how successful Australian-based efforts and solutions at developing and deploying trusted computer platforms may be.



Appendix A

Legal requirements for a signature

A1.1 WHAT CONSTITUTES A SIGNATURE AT COMMON LAW?

- Any kind of mark acceptable provided it is affixed by the person or by some person authorised by the person intended to be bound;
- unless there is some specific legislative requirement the mark can be affixed by some mechanical means;
- the mark can be highly insecure such as a mark that has been effected by a pencil;²⁹
- at the time of affixing the mark the signatory has the necessary intention to be bound by the contents of the document or, in the case of a witness, the necessary intention to be associated with the document as a witness; and
- the mark can be located anywhere on the document, it does not have to be at the foot of the document unless there is a legislative requirement as to form as in a will, specifying where the signature is to be placed.³⁰

A1.2 STATUTE - ELECTRONIC SIGNATURE REQUIREMENTS (WHERE SIGNATURE REQUIRED UNDER A LAW OF THE COMMONWEALTH)

Electronic Transactions Act 1999 (Cth), section 10(1):

'If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if:

- in all cases—a method is used to identify the person and to indicate the person's approval of the information communicated; and
- in all cases—having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and
- if the signature is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the method used as mentioned in paragraph (a) be in accordance with particular information technology requirements—the entity's requirement has been met; and

²⁹ *Geary v. Physic* [1826] 5 B&C 234 at 238, per Bayley J.

³⁰ Extracted from McCullagh, A. *et al* 'Electronic Signatures: Understand the Past to Develop the Future' (1998) 21:2 *University of New South Wales Law Journal* 452 at 457.

- (d) if the signature is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned in paragraph (a):

A1.3 LAW RELEVANT TO ONE PERSON BEING BOUND BY THE ACTIONS OF OTHER PERSONS OR ELECTRONIC DEVICES

(A) LAW OF AGENCY AND ESTOPPEL

AGENCY

Definition

- (i) Agency—‘the fiduciary relationship which exists between two persons, one of whom expressly or impliedly consents that the other should act on his behalf so as to affect his relations with third parties [principal], and the other of whom similarly consents so to act or so acts [agent].’³¹
- (ii) The existence of an agency relationship depends not on the terminology of the parties but on the true nature of the agreement or the exact circumstances of the relationship between the alleged principal and agent.

Formation

Except in relation to certain statutory provisions requiring an appointment in writing, no formality is required for the valid appointment of an agent. Agency may be created by:

- (i) express or implied agreement (contractual or otherwise) of principal and agent;
- (ii) subsequent ratification by the principal of the agent’s acts done on behalf of the principal;
- (iii) operation of law, as in the case of agency by necessity, or under statute;³² or
- (iv) agency by estoppel and apparent authority. Here, the existence of the agency relationship will be implied from the conduct of the parties towards each other which makes it reasonable to infer consent to the relationship of agency. Agency by estoppel applies where the supposed agent is not, in fact, authorised to act for the principal but is allowed by the principal to appear as if she is. Apparent, or ostensible, authority arises where the agent is allowed by the principal to appear to have a greater authority than she in fact has.³³

The onus of proof of the relationship of agency lies upon the person dealing with anyone as agent and seeking to impose liability upon another as principal.

31 Reynolds, F.M.B., *Bowstead & Reynolds on Agency* 16th Edition, Sweet & Maxwell, 1996, 1-001.

32 For example the *Sale of Goods Act 1958* (Vic) s54 (3)—unpaid seller of Goods exercising the right to resell.

33 *Bowstead & Reynolds on Agency*, 1-009. This separation of the two concepts, though useful for definitional purposes, arguably is of little practical importance, as both arise from conduct of the principal which gives rise to an estoppel. The discussion which follows relies heavily on Halsbury, which treats both as variations on the same theme.

The law imposes fiduciary duties on the agent in relation to the principal. These duties are not necessarily contractual, as there need not be a contract between principal and agent. They originate from equity, as do the fiduciary obligations of a trustee.³⁴

An agent must be distinguished from an amanuensis, who performs a clerical or administrative role between the appointor and a third party, the appointor in essence acting for himself or herself in the transaction.³⁵ This distinction may be relevant to whether an autonomous electronic device performing tasks according to pre-programmed instructions of a party are to be regarded, in law, as an agent of that party (see below).

AGENCY BY ESTOPPEL AND APPARENT AUTHORITY

Estoppel

Three general classes of estoppel are recognised at common law:

- (i) estoppel by record or judgment;
- (ii) estoppel by deed; and
- (iii) estoppel in pais.

Estoppel in pais includes both estoppel by convention and estoppel by representation. At common law, estoppel in pais is confined to assumptions or representations relating to an existing state of affairs. While these instances of estoppel in pais apply equally in equity, equity extends further than the common law to include, under the doctrine of promissory estoppel, representations as to future conduct.

Equity also developed the category of proprietary estoppel, including both the passive form of 'estoppel by acquiescence' and the active form of 'estoppel by encouragement'. Promissory and proprietary estoppel, historically developed as separate categories, are now regarded as aspects of a broader principle of equitable estoppel. It has been suggested in the High Court of Australia that estoppel in pais and equitable estoppel may be unified under one overarching substantive doctrine of estoppel, although that view has not yet been authoritatively adopted by the Court.

*Agency by Estoppel*³⁶

Agency by estoppel arises where one person ('principal'), by words or conduct, represents to another that a third person has been authorised as agent, and in reliance the other person enters into transactions with the third person within the scope of that ostensible authority.

The principal is estopped from denying the fact of the third person's agency under the general law of estoppel.

The onus of proof of the existence of actual or ostensible authority lies on the person dealing with the agent.

The holding out by the principal must be to the particular individual, rather than merely to persons in general who may not have acted on the holding out. Holding out is more than estoppel by negligence; it is necessary to prove affirmatively conduct amounting to holding out. Such conduct would include the case of a principal who allows an agent to hold himself or herself out as having authority (estoppel by acquiescence).

³⁴ *Bowstead*, 1-013.

³⁵ *Halsbury* 15-5, citing *Maye v Colonial Mutual Life Assurance Society Ltd* (1924) 35 CLR 14 at 30, 37, 44.

³⁶ *Halsbury*, 15-60.

However, no representation made solely by the agent as to the extent of his or her authority can amount to a holding out by the principal. A person who assumes to act as an agent is estopped from being able to deny acting on the principal's behalf.

Persons dealing with a company are entitled to assume that a person who is held out by the company to be an officer or agent of the company has been duly appointed and has authority to exercise the powers and perform the duties customarily exercised or performed by an officer of the kind concerned.

Statutory rules as to the appointment and authority of officers and agents of a company and the assumptions which a person dealing with a company is entitled to make are set out in sections 128 and 129 of the *Corporations Law*.

REMEDIES

Where a principal suffers loss as a result of acts of the agent outside the scope of the agent's authority, the principal may have a right to sue for breach of the contract of agency (if the agency arises from a contractual relationship) or for breach of the fiduciary duty owed by the agent to the principal.

(B) ELECTRONIC TRANSACTIONS ACT 1999 (CTH) S.15 AND EQUIVALENT STATE AND TERRITORY LEGISLATION

Sections 15(1) and (2) of the *Electronic Transactions Act 1999*(Cth) state:

- '(1) For the purposes of a law of the Commonwealth, unless otherwise agreed between the purported originator and the addressee of an electronic communication, the purported originator of the electronic communication is bound by that communication only if the communication was sent by the purported originator or with the authority of the purported originator.
- (2) Subsection (1) is not intended to affect the operation of a law (whether written or unwritten) that makes provision for:
 - (a) conduct engaged in by a person within the scope of the person's actual or apparent authority to be attributed to another person; or
 - (b) a person to be bound by conduct engaged in by another person within the scope of the other person's actual or apparent authority.'

The effect of subsections (1) and (2) is that, for the purposes of a law of the Commonwealth, the question of whether the sender of an electronic communication was acting 'with the authority of the purported originator' will fall to be determined by the common law (as varied by other legislation), in particular as it relates to agency, estoppel, tort and vicarious liability. Except where other legislation applies, the common law will also regulate the enforceability of electronic communications for purposes other than a law of the Commonwealth.

The Electronic Commerce Expert Group recommended that Australian legislation should not introduce statutory presumptions or rules of attributions but should provide that the common law applies, subject to contractual attribution rules agreed between parties.³⁷

The Explanatory Memorandum to the *Electronic Transactions Bill* 1999 describes section 15 as restating the existing common law in relation to the attribution of communications. The EM also states that sub-s.15(1) is not intended as a codification of the common law. It must be read with sub-s.15(2) which is intended to ensure that the operation of the existing common law of agency, including the doctrines of apparent and actual authority, are preserved. In fact, sub-s.15(2) also preserves any statutory rules of attribution (as well as common law). (It does not seem to speak directly to the law of vicarious liability e.g. for an employee's act. But vicarious liability for an employee's communication does not arise from a rule of law attributing the communication to the employer as the originator of the communication. It arises from law attributing liability to the employer for a communication of the employee.)

One writer makes the point that Australia's *Electronic Transactions Act* is unique in that it appears to allow the common law rules of agency to apply to the question of whether autonomous electronic devices can be regarded, in law, as the agents of the persons on whose behalf they carry out pre-programmed actions.³⁸

The common law does not, in fact, provide much guidance on this issue. There does not appear to be any case law on point. The definition of agency above states that the consent of the agent to act in that capacity is needed. It is difficult to conceive of a machine 'consenting' to act in any real sense of the word.

Bowstead states that 'if only the relations between principal and third party are in issue, it may not be necessary for the agent to have agreed to, or even perhaps to have knowledge of, the conferring of authority at all, if it can be established that the principal had conferred it'.³⁹ However, he goes on to say that '... a person incapable of understanding the nature of what he is doing cannot act as agent',⁴⁰ which would appear to rule out a machine.

The amanuensis analogy referred to above appears to have been persuasive in the hypothetical example given by one US commentator who concludes that a telegraph company should not be regarded as the agent of the sender of a telegram.⁴¹ The author's conclusion is based on the fact that 'the sender does not hold out the telegraph clerk as his agent with power to contract on his behalf.'

Of course, the opposite is true in the case of a piece of an electronic device programmed to assent to contracts if defined criteria are met (e.g. accept all offers above \$20,000). In that case the software or other device is being held out by the programmer as having power to enter into contracts on his or her behalf. If the party to whom the holding out is being made is content to rely on the representation being made (that the machine is the agent of a disclosed or undisclosed principal) then there would not appear to be a problem with accepting that the laws of agency apply.

Applying the laws of agency to machines will not be problematic where the 'principal' and the other party to the contract have agreed in a prior contract or through a course of conduct that one or both parties may use electronic devices to assent to contracts.

In theory, the agency analysis could be problematic if the other party to the contract is not aware that the machine is acting as an agent for an undisclosed principal. Traditionally in this situation, the contracting party can sue both the agent or the principal (if he or she can be identified) on the contract entered into by

38 Kerr, Dr Ian R., *Providing for Autonomous Electronic Devices in the Uniform Electronic Commerce Act*.

39 *ibid.*, 1-005.

40 *ibid.*, 2-012.

41 A.L. Corbin, *Corbin on Contracts* ' 105 (1963), cited in Baum, Michael S., *Federal Certification Authority Liability and Policy - Law and Policy of Certificate-Based Public Key and Digital Signatures* U.S. Department of Commerce, 112.

the agent. This would be of little comfort in the case of a machine. However, it is likely that a machine will always purport to enter into a contract on behalf of an identified person, so this problem may not arise in practice.

Problems may arise if a machine erroneously acts outside its actual authority in assenting to a transaction and the principal purports to repudiate the contract. The issue would then be whether or not, in the eyes of the other party to the contract, the machine had apparent authority to enter into the contract. The onus would be on that party to establish the apparent authority and if it was unable to do this, it might be left exposed.

A1.4 PRINCIPLES OF LIABILITY IN NEGLIGENCE

Definition

Negligence is the failure to take reasonable precautions to avoid foreseeable risk of injury to another.⁴²

Elements

The plaintiff must prove that the:

- (a) defendant owed plaintiff a duty to take reasonable care;
- (b) defendant breached that duty by failing to take reasonable care;
- (c) defendant's breach of duty caused the injury or damage suffered by the plaintiff; and
- (d) injury or damage suffered was not too remote a consequence of the breach of duty.

Duty of Care

The scope of the duty of care determines the class of persons to whom a defendant will be liable in negligence. There are two elements of the duty of care:

- (a) reasonable foreseeability—an assessment of whether a reasonable person in the position of the defendant would have foreseen that his or her act (or omission) would cause injury to the plaintiff or to a class of persons of which the plaintiff is a member; and
- (b) proximity (which may be physical, circumstantial or causal⁴³), between the defendant and the plaintiff. A finding by a court that the requisite degree of proximity exists to found a duty of care will often involve considerations of public policy which 'underlay and enlighten the concept [of proximity]'.⁴⁴

RELEVANT CATEGORIES OF NEGLIGENCE

Act or Omission Causing Purely Economic Loss

There is no general duty of care in Australia to avoid causing economic loss to another. However, such a duty may be owed to a specific class which is identified or ascertainable at the time of the act of negligence.

⁴² Halsbury 415-70.

⁴³ *Sutherland Shire Council v Heyman* (1985) 157 CLR 424, per Deane J. at 510 - 511.

⁴⁴ *Hill v Van Erp* (1997) 188 CLR 159, per Dawson J at 178 and *Pyrenees Shire Council v Day (Eskimo Amber Pty Ltd v Pyrenees Shire Council)* (1998) 192 CLR 330 per Kirby J at 419 - 420.

Complete accuracy in identification of the class is probably not required. The imposition of such a duty is more likely where the plaintiff is unable to avoid the loss by taking reasonable steps to pursue its own interest.⁴⁵

Negligent Misstatement - Cause of action in both tort and contract

Where a plaintiff has suffered purely economic loss in reliance on an alleged negligent misstatement, the elements of negligence may be found to be satisfied on particular facts conforming to the principle first established in the *Hedley Byrne* case⁴⁶ and developed in subsequent case law.

Under the *Hedley Byrne* principle there is no requirement that the statement be a factual representation, inducing a contract with the maker of the statement. Moreover, the principle is not limited to the giving of advice as distinct from factual information.⁴⁷ Accordingly, a statement of opinion (or an undertaking) may give rise to a tortious liability for a negligent misrepresentation or misstatement, as may the giving of careless information or advice.

However, a person is under no duty to take reasonable care that advice or information given to another is correct, unless the maker of the statement knows, or ought to know, that the other relies on him or her to take such reasonable care and may act in reliance on the advice or information which he or she is given, and unless it would be reasonable for that other person so to rely and act.

Reliance as a key determinant of the existence of the requisite proximity was emphasised by the High Court in *San Sebastian Pty Ltd v Minister Administering Environmental Planning and Assessment Act 1979 (NSW)*.⁴⁸ The judgment in that case has been summarised as standing for the proposition that ‘... a relationship of sufficient proximity to raise a duty of care may well exist where a provider of advice or information directs his statement to a class of persons with the intention of inducing members of the class to act on the statement in circumstances where he ought to realise that they may suffer economic loss if the statement is not true. This means that a proximate relationship sufficient for duty could exist, not only as between a speaker and an individual intended recipient and user of advice, but also as between the speaker and members of a class where such members were the intended recipients and users of that advice.’⁴⁹

Concurrent liability in contract and tort

Entry into a contract does not preclude reliance on pre-contractual negligence for a cause of action in damages. The giving of negligent information or advice may, however, also constitute the breach of an express or implied term guaranteeing that competent advice has been given or requiring competent advice to be given. The possibility of causes of action in both contract and tort is raised in such a case:

- (a) Where a pre-contractual statement which involved the giving of negligent information or advice is embodied in an express term, the pre-contractual negligence in the giving of the advice may also constitute a breach of contract giving rise to a claim for damages in both tort and contract;
- (b) Where the information or advice is given in the performance of a contract it may also constitute the breach of a duty of care.

45 *Perre v Apond Pty Ltd* (1999) 164 ALR, 606.

46 Established in *Hedley Byrne & Co Ltd -v- Heller & Partners, Ltd* [1964] AC 465.

47 *Balkin & Davis*, 430.

48 (1986) 162 CLR 340 at 355, joint judgment.

49 *Katter, N.A., Duty of Care in Australia* LBC Information Services Sydney, 1999, 161.

Generally, the courts have been willing to recognise a choice in such cases between damages in tort or contract. Although the High Court has not decided the issue, the general approach of the cases has been to treat the rights and obligations created by any resultant contract as not superseding and replacing the tortious duty of care.

CONTRIBUTORY NEGLIGENCE

At common law, contributory negligence is a complete defence to a claim of negligence.⁵⁰ In the case of *Astley v Austrust*,⁵¹ the High Court held that legislative provisions apportioning liability where there has been contributory negligence do not apply to actions for breach of contract. As a result, in the absence of an express contractual provision allowing for apportionment, a plaintiff will not be able to reduce an award of damages to the extent that the plaintiff has contributed to its own loss.

VICARIOUS LIABILITY

A corporation or an individual may be liable for a tort either directly or vicariously. A corporation is directly liable for torts committed by its managing or directing bodies or organs. It is vicariously liable for acts of its employees within the course or scope of their employment,

A corporation may be liable notwithstanding that the tort involves wilful wrongdoing, malice or fraud. However, this might not be so where the tortious act or omission is totally in fraud of the corporation, and the corporation derives no benefit from it. The fact that the corporation derives no benefit from the tortious act does not of itself mean that it is not liable.

Except in the case of the tort of deceit or the use of a motor vehicle a principal will not be vicariously liable for the acts of his or her agent unless the agent is also the 'servant' of the principal and then only for acts of the servant within the scope of employment.⁵² In those specified instances, the principal will be liable for the acts of the agent carried out in within the scope of the actual or apparent agency authority.

50 The common law position has been altered in all Australian jurisdictions by apportionment legislation such as the *Wrongs Act 1958* (Vic), s 26(1).

51 (1999) 161 ALR 155. The Federal Government plans to introduce legislation to overrule the decision in *Astley v Austrust*.

52 Balkin & Davis 798 f.



Glossary

(adapted from *Electronic Commerce: Building the Legal Framework*, the Report of the Attorney-General's Electronic Commerce Expert Group, 1998)

ACRONYMS

ACCC	Australian Competition and Consumer Commission
CA	certification authority
CPS	certification practices statement
CRL	certificate revocation list
CRLUA	certificate revocation list user agreement
EDI	electronic data interchange
IA	Issuing authority
NCCUSL	National Conference of Commissioners on Uniform State Law
PKAF	public key authentication framework
PKI	public key infrastructure
RA	registration authority
RP	relying party
RPA	relying party agreement
RSA	A type of a symmetric cryptosystem, named after its inventors, Ron Rivest, Adi Shamir and Len Adelman, of the Massachusetts Institute of Technology.
S	subscriber
TPA	<i>Trade Practices Act 1974</i> (Cth)

DEFINITIONS

Asymmetric cryptosystem

An information system utilising an algorithm or series of algorithms which provide a cryptographic key pair consisting of a private key and a corresponding public key. The keys of the pair have the properties that (1) the public key can verify a digital signature that the private key creates, and (2) it is computationally infeasible to discover or derive the private key from the public key. The public key can therefore be disclosed without significantly risking disclosure of the private key. This can be used for confidentiality as well as for authentication of identity.

Authentication (of identity)

Means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communication system, often the identity of the originator of an electronic communication.

Certificate

A set of information which at least: identifies the certification authority issuing the certificate; unambiguously names or identifies the certificate owner (subscriber); contains the owner's public key and is digitally signed by the certification authority issuing it.

Certification

Means attesting to certain information about entities or transactions in the electronic environment.

Certification Authority

- (a) A certification authority provides to users a digital certificate that links a subscriber's public key with some assertion about the subscriber, such as the subscriber's name. Certification authorities may offer other services such as time-stamping, key management services and certificate revocation services.
- (b) An independent trusted source which attests to some factual element of information for the purposes of certifying that information in the electronic environment.

Closed network/closed user group

Systems in which certificates are used within a bounded context such as within a closed trading group. A contract or series of contracts identify and define the rights and responsibilities of all parties to a particular transaction.

Certification Practices Statement

A statement of the Certification Authority's practices with respect to a wide range of technical, business and legal issues that may be used as a basis for the Certification Authority's contract with Subscribers and relationships with Relying Parties.

Confidentiality

The property of data or information that is not made available or disclosed to unauthorised individuals, entities or processes.

Cryptography

The principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use.

Cryptographic key

A parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

Digital signature

Data appended to a message that allows a recipient of the message to prove the source and integrity of the message.

Electronic commerce

A broad concept that covers any trade or commercial transaction that is effected using electronic means; such as facsimile, telex, EDI, Internet, and the telephone.

Electronic data interchange

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

Electronic signature

Any symbol or method executed or adopted by a party with present intention to be bound by or to authenticate a record accomplished by electronic means. Digital signatures are a type of electronic signature.

Encryption

The transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.

Hash function/hashing

A hash function is a mathematical process based on an algorithm which creates a digital representation or compressed form of the message, often referred to as the message digest in the form of a hash value or hash result of a standard length which is usually much smaller than the message but nevertheless substantially unique to it.

Integrity

The property that data or information has not been modified or altered in an unauthorised manner.

Open network/system

A network in which parties who may not be known to each other, and who may be in different state or national jurisdictions, will conduct transactions or exchange/trade data. Participants in an open network will not necessarily have pre-existing contractual arrangements with the parties they transact with through the open network.

Private Key

The private or secret key of a key pair, which must be kept confidential and is used to decrypt messages encrypted with the public key, or to digitally sign messages which can then be validated with the 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 messages.

Public key cryptography

An asymmetric cryptosystem where the encrypting and decrypting keys are different and it is computationally infeasible to calculate one from the other, given the encrypting algorithm. In public key cryptography, the encrypting key is made public, but the decrypting key is kept secret.

Public key infrastructure

Supporting services, including non-technical aspects, for the management of the use of public keys on a wide scale. Certification authorities and related certificate management systems constitute the core of public key infrastructures, but other supporting infrastructural services, both technological and legal, are also required.

Relying party

The recipient of an electronic communication or other person using that communication who will rely on a certificate as part of a process of authenticating the identity of the originator of the communication.

Subscriber

An individual who obtains a certificate from a certification authority. When originating an electronic communication, this person will send the certificate or refer the recipient to the certificate so the recipient can authenticate the identity of the originator of the communication. Since both consumers and merchants may have digital certificates which are used to conclude a transaction, they may both be subscribers in certain circumstances. This person may also be referred to as the signer of a digital signature or the sender of data message signed with a digital signature.

Time stamping

An electronic equivalent of mail franking.

Trusted third party

An entity trusted by other entities with respect to security related services and activities, such as a certification authority.

Verify

To determine accurately that: (a) the digital signature was created by the private key corresponding to the public key; and (b) the message has not been altered since its digital signature was created.

