

Electronic Signatures and PKI Frameworks in Australia

SHARON CHRISTENSEN AND ROUHSHI LOW

A National Approach to Electronic Transactions

The Australian government's information economy policy, *Investing for Growth* released by the Prime Minister in December 1997¹ established a light-handed regulatory framework to support and encourage the development of the information economy. The National Office of the Information Economy (NOIE)² was established in 1997 to develop and coordinate Australian government policy in this area. As part of the government's strategy, the *Electronic Commerce Expert Group* (ECEG)³ comprising representatives from business, the private legal profession and government, was set up to report on the legal issues arising from the development of electronic commerce.

The ECEG's Report, *Electronic Commerce: Building the Legal Framework*,⁴ released for public comment on 2 April 1998, recommended that the Commonwealth should enact legislation based on the UNCITRAL Model Law on Electronic Commerce⁵ to promote the growth of electronic commerce. Following this recommendation, the *Electronic Transactions Act 1999 (Cth)* was enacted commencing on 15 March 2000. The primary

objective of this Act was to facilitate the development of electronic commerce in Australia by broadly removing existing legal impediments that may prevent a person using electronic communications to satisfy obligations under Commonwealth law. Prior to 1 July 2001 it only applied to laws of the Commonwealth specified in the regulations and after July 2001 to all laws of the Commonwealth unless specifically exempted. The *Electronic Transactions Regulations 2000 (Cth)* from 1 July 2001 specified laws to which the Act does not apply.

Recognising that a national approach to electronic transactions was essential to the success of electronic commerce in Australia, the government in close cooperation with the State and Territory governments developed a uniform Electronic Transactions Bill for adoption in all Australian jurisdictions.⁶ The uniform Bill was closely modelled on the Commonwealth's *Electronic Transactions Act 1999* and mirrored the substantive provisions of the Commonwealth's *Electronic Transactions Act 1999*. On 3 April 2000, all jurisdictions had endorsed the uniform Bill⁷ and to date, the following States and Territories have enacted complementary legislation: New South Wales⁸,

¹ *Investing for Growth*, Address by the Prime Minister The Hon John Howard MP, National Press Club, Canberra, 8 December 1997, available at <http://www.pm.gov.au/news/speeches/1997/industry.htm>.

² The NOIE homepage is at <http://www.noie.gov.au/>. However on 8 April 2004, the Australian Government Information Management Office (AGIMO) was established, replacing NOIE. Functions of the former NOIE relating to the promotion and coordination of the use of new information and communications technology to deliver Government policies, information, programs and services have been placed with AGIMO. Functions of the former NOIE relating to broader policy, research and programs have been transferred to the Office of the Information Economy in the Department of Communications, Information Technology and the Arts (DCITA). in the Department of Communications, Information Technology and the Arts (DCITA). Australian Government Information Management Office website: <http://www.agimo.gov.au/>. DCITA website: http://www.dcita.gov.au/Subject_Entry_Page/0,,0_1-2_1,00.html.

³ See: <http://www.ag.gov.au/agd/www/securitylawHome.nsf/0/38A611AD4AB77CB0CA256B9D00182477?OpenDocument>

⁴ Report of the Electronic Commerce Expert Group to the Attorney General, "Electronic Commerce: Building the Legal Framework", 31 March 1998, available in electronic format at <http://152.91.15.15/aghome/advisory/eceg/ecegreport.html>.

⁵ UNCITRAL Promulgated by UNCITRAL in 1996: UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, additional Article 5 bis adopted in 1998, General Assembly Resolution 51/162 of 16 December 1996. The text and Guide to enactment are available in electronic format at <http://www.uncitral.org/en-index.htm> [hereafter UNCITRAL Model Law and Guide to Enactment].

⁶ This was necessary given the constitutional limitations on the Commonwealth government enacting legislation that could impact on the State common law.

⁷ See http://www.law.gov.au/aghome/agnews/2000newsag/725_00.htm.

⁸ *Electronic Transactions Act 2000* (NSW) (date of commencement: 30 November 2001).

Victoria,⁹ Queensland,¹⁰ Tasmania,¹¹ Northern Territory,¹² Australia Capital Territory,¹³ Western Australia¹⁴ and South Australia.¹⁵

The Commonwealth and State's legislation are heavily influenced by the Model Law on Electronic Commerce published in 1996 by the United Nations Commission on International Trade Law (UNCITRAL). Although in 2001 UNCITRAL adopted a Model Law on Electronic Signatures, these further developments have not been incorporated within the legislation operating in Australia.

The Legislative Framework and Digital Signatures

The Electronic Transactions Acts at Commonwealth and State level are based on two principles: functional equivalence (also known as media neutrality), and technology neutrality. Functional equivalence refers to the equal treatment of paper and electronic transactions: transactions conducted using paper documents and transactions conducted using electronic communications should be treated equally by the law and not given an advantage or disadvantage against each other. The principle of technology neutrality prohibits discrimination between different forms of technology.

Each *Electronic Transactions Act* contains provisions consistent with ss 9-12 (division 2) of the Commonwealth Act by making provision for how a requirement, under a law of the particular jurisdiction, for writing or a signature may be met by means of an electronic communication. The aim of the sections is to ensure that an electronic document is not invalidated merely because it is electronic and not in a paper form. For an electronic document to meet the requirements of a State law that requires a document to be signed, certain criteria must be met. For example, the *Electronic Transactions Act 1999* (Cth), s 10¹⁶ sets out the basic elements an electronic signature method must satisfy. These are:

- a method is used to identify the person and to indicate the person's approval of the information communicated (the method used to identify the person is called an 'electronic signature');
- the method was as reliable as was appropriate for the purposes for which the information was communicated; This requirement ensures that a signature method that was appropriate at the time it was used is not rendered invalid later.¹⁷ Some factors that could be taken into account when determining the appropriateness of the signature method are set out in the Explanatory Memorandum¹⁸ –
 - i. the function of signature requirements in the relevant statutory environment;
 - ii. the type of transaction;
 - iii. the capability and sophistication of the relevant communication systems; and
 - iv. the value and importance of the information in the electronic communication.
- where a person must provide a signature to a Commonwealth entity the person must comply with any information technology requirements in relation to the signature method; and
- where the signature is required to be given to a person who is not a Commonwealth entity, that person must consent to the use of that signature method.

On the basis of these criteria, the method a person chooses to use must both identify the person and their approval of the contents of the electronic communication, but does not have to verify the integrity of the communication. Section 10 reflects the technologically neutral approach of the Act, and for this reason should be viewed as providing minimum requirements for signature methods. Instead of specifying detailed standards

*The principle of
technology
neutrality
prohibits
discrimination
between different
forms of
technology*

⁹ *Electronic Transactions (Victoria) Act 2000* (Vic) (date of commencement: 1 September 2000).

¹⁰ *Electronic Transactions (Queensland) Act 2001* (Qld) (date of commencement 1 November 2002).

¹¹ *Electronic Transactions Act 2000* (Tas), (date of commencement: 1 June 2001).

¹² *Electronic Transactions (Northern Territory) Act 2000* (NT) (date of commencement: 13 June 2001).

¹³ *Electronic Transactions (Australian Capital Territory) Act 2000* (ACT) (date of commencement: ss 1 & 2: 8 March 2001; ss 3-15: 1 July 2001).

¹⁴ *Electronic Transactions Act 2003* (WA) (date of commencement: 2 May 2003).

¹⁵ *Electronic Transactions Act 2000* (SA) (date of commencement: 1 November 2002, see Gaz. 29 August 2002, p 3212).

¹⁶ This section is based on Article 7 of the UNCITRAL Model Law on Electronic Commerce which deals with electronic signatures and aims to ensure that a data message is not denied legal effect on the sole ground that it was not authenticated in a manner peculiar to paper documents.

¹⁷ Revised Explanatory Memorandum to the *Electronic Transactions Bill 1999* (Cth), 31.

¹⁸ Revised Explanatory Memorandum to the *Electronic Transactions Bill 1999* (Cth), 31-32.

for particular types of signature methods, s 10 allows any method to qualify as an electronic signature so long as the method identifies the person and indicates that person's approval of the contents of the electronic communication. In certain types of transactions, parties or the government may consider specifying additional requirements, particularly where the security of the communication between the parties is critical. Consideration will need to be given to:

- the methods to be used to ensure that persons and organizations participating in an electronic transaction can be reliably identified and to ensure that they have in fact sent and approved of the contents of communications to which their electronic signature is attached;
- the methods to be used to reliably ensure the integrity of information contained in electronic documents and communications; and
- how a person or organization will consent to the use of the methods and technical standards prescribed by the other party to ensure reliability relating to the integrity, authenticity and non-repudiation of electronic communications and documents.

To date, government agencies only specify general or open standards that the signature method should comply with, for example signatures used for the Australian Taxation Office must be Gatekeeper accredited.¹⁹ It is suggested that additional requirements should be specified for certain transactions where the authenticity of data and the integrity of a transaction is important.²⁰

Public Key Infrastructure (PKI) and the Federal Government's Gatekeeper Strategy

There is at present no legislative regime in Australia dealing specifically with PKI. The Australian government's response to the growing

need for a national public key technology framework is the Gatekeeper strategy,²¹ released in May 1998. This strategy, compiled by the Office of Government Information Technology (NOIE), details a framework and guidelines for the implementation and use of PKI technology by Federal government agencies within Australia. It is mandatory for all Federal government agencies to use Gatekeeper when an online authentication system is required. The major aims of the Gatekeeper Strategy are to encourage confidence in the online economy and to ensure trust between all users at each level of transactions with government.²² The strategy includes a process to enable private certification authorities to gain accreditation as certification authorities.²³ The accreditation criteria for Certification and Registration Authorities released in December 1998 includes compliance with Commonwealth Government procurement policy, security policy and planning, physical security, technology evaluation, Certification Authority (CA) and Registration Authority (RA) policy and administration, personnel vetting, legal issues, and privacy considerations.²⁴ Service providers that have been accredited by the Gatekeeper Competent Authority include the Australian Tax Office and VeriSign Australia Pty Ltd.²⁵

ABN-DSC Digital Certificates

As part of the Gatekeeper initiative, the Australian government has developed a Gatekeeper digital certificate base around the Australian Business Number. The Australian Business Number Digital Signature Certificate (ABN-DSC Digital Certificate) is a digital signature certificate linked to a business entity's ABN, and designed to facilitate online service delivery and foster the use of digital certificates and e-commerce among Australian businesses. This means that businesses will only need to use one primary type of digital certificate to deal online with Australian Government agencies. Only Gatekeeper accredited Certification Authorities are able to issue an ABN-DSC which must comply with the standard specifications.²⁶

¹⁹ Discussed below.

²⁰ For example a land transaction where the purpose of requiring a signature is to minimise fraudulent transactions: Christensen, Duncan and Low "The Statute of Frauds in the Digital Age - Maintaining the Integrity of Signatures" (2003) E-law Journal, Murdoch University (December 2003) <http://www.murdoch.edu.au/elaw/issues/v10n4/christensen104.html>.

²¹ The Gatekeeper website is: <http://www.agimo.gov.au/infrastructure/gatekeeper>.

²² State and Territory governments are also interested in adopting Gatekeeper. For example, Gatekeeper accredited digital certificates will be required for use of the Victorian Land Exchange system.

²³ A 12-month transition of the Gatekeeper accreditation process from AGIMO to the National Association of Testing Authorities, Australia (NATA) has commenced.

²⁴ A detailed discussion of the Gatekeeper Strategy is found in Boyle, "An Introduction to Gatekeeper: the Government's Public Key Infrastructure" (2001) 11(1) *Journal of Law and Information Science* 38-54.

²⁵ For a complete list see <http://www.agimo.gov.au/infrastructure/gatekeeper/accredited>.

²⁶ For the specifications for an ABN-DSC refer to ABN-DSC Broad Specifications at www.govonline.gov.au.

Examples of developments in this area include

- The Project Angus digital signature certificates issued to businesses by Australian banks were accepted as an ABN-DSC and therefore able to be used in online transactions with Commonwealth agencies.²⁷
- The ANZ Bank's Identrus public key infrastructure (PKI) implementation achieved Gatekeeper recognition in 2003, allowing ANZ's Identrus digital certificates to be used in the government sector.²⁸

while a generic framework provides flexibility initially, further legislation or amendment is required to satisfy the requirements of all types of transactions, particularly those requiring writing and signatures for validity. ■

Australian Government Authentication Framework

More recently in May 2004, the Australian Government Information Management Office (AGIMO) released an initial exposure draft on the proposed Australian government Authentication Framework (AGAF).²⁹ The framework aims to facilitate trust in the growing number of online transactions by providing a means for aligning business processes with authentication techniques based on a business risk assessment. The proposed framework is similar to online authentication frameworks in the UK, US and Canada.

This follows from an earlier Discussion Paper released by the AGIMO in May 2002 on the potential for a National Authentication Technology Framework.³⁰ The paper broadly examines the trends in relation to authentication technologies (PINS, passwords, PKI, SSL, biometrics), and considers the possible future of the Gatekeeper accreditation framework, and AGIMO's role in relation to authentication technologies (PKI and biometrics in particular).

Conclusion

Australia's approach to the growth of e-commerce has been to provide a generic regulatory framework in the form of the *Electronic Transactions Act 1999* (Cth). As observed by Simon Grant, it is a 'minimalist legislative approach' when compared to some other jurisdictions such as the European Union. The consensus is that

²⁷ Project Angus involves the four major Australian banks - Australia and New Zealand Banking Group Limited, Commonwealth Bank of Australia, National Australia Bank Limited and Westpac Banking Corporation investigating ways to develop effective electronic trust and payment services in Australia for business e-commerce. The banks' digital certificate initiative is known as 'Project Angus'. Banks involved in Project Angus have agreed to obtain Gatekeeper accreditation.

²⁸ Identrus is an organization formed by global financial institutions to aid the growth of bank-to-bank and business-to-business e-commerce. Further information about Identrus can be obtained at <http://www.identrus.com>.

²⁹ Available at: http://www.agimo.gov.au/__data/assets/file/31772/AGAF_Overview_4_Business.pdf.

³⁰ The consultation paper is available in electronic format at: http://www.agimo.gov.au/__data/assets/file/12283/NATF_Discussion_paper_July2002.pdf and the subsequent feedback: <http://www.agimo.gov.au/infrastructure/authentication/natf>.

³¹ S Grant and S Matthews, 'Trust me: Public Key Infrastructure (Part 2)' (2002) (12) *E Law Practice* 48.

© Sharon Christensen and Rouhshi Low, 2004

Sharon Christensen, LLB (Hons), LLM (QUT) is the Gadens Professor of Property Law, Faculty of Law, Queensland University of Technology

Rouhshi Low, LLB, LLM (Qld), M Tech (QUT) is a Sessional Lecturer, Faculty of Law, Queensland University of Technology