



NATIONAL ARCHIVES OF AUSTRALIA

Recordkeeping and Online Security Processes

Guidelines for Managing
Commonwealth Records Created or
Received Using Authentication or
Encryption

May 2004

© Commonwealth of Australia 2004

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 National Archives of Australia. Requests and inquiries concerning reproduction and rights should be directed to the Publications Manager, National Archives of Australia, PO Box 7425, Canberra Business Centre ACT 2610.

ISBN 1 920807 05 5

CONTENTS

ABBREVIATIONS	5
<hr/>	
1. INTRODUCTION	6
<hr/>	
1.1 Background	6
1.2 Purpose	7
1.3 Scope and audience	8
1.4 Acknowledgments	9
1.5 Further information	9
2. E-BUSINESS AND AUTHENTICATION AND ENCRYPTION TECHNOLOGIES	10
<hr/>	
2.1 Strategies for e-government	10
2.2 Public key infrastructure	12
2.3 The Gatekeeper strategy	16
2.4 Other means of online authentication	17
2.5 Other forms of security technology	18
3. RECORDKEEPING IMPLICATIONS AND RECOMMENDATIONS	19
<hr/>	
3.1 Setting the scene	19
3.2 Authenticity and non-repudiation	20
3.3 Confidentiality and accessibility	22
3.4 Meeting legislative requirements	24
3.5 Current standards and policies	27
4. RECORDKEEPING STRATEGIES	31
<hr/>	
4.1 Recordkeeping, security and information management framework	31
4.2 Records to be retained as national archives	35

5.	IMPLEMENTATION CHECKLIST	37
5.1	Initial considerations	37
5.2	Technology considerations	37
5.3	Recordkeeping considerations	37
APPENDIXES		38
	Glossary	38
	Further reading	42

ABBREVIATIONS

ACSI	Australian Communications Security Instruction
AFDA	Administrative Functions Disposal Authority
AGIMO	Australian Government Information Management Office
AGD	Attorney-General's Department
ANAO	Australian National Audit Office
CA	Certification Authority
CEO	Chief Executive Officer
CRL	Certificate revocation list
DSD	Defence Signals Directorate
ETA	Electronic Transactions Act
FOI	Freedom of Information
GDA	general disposal authority
GPKI	government public key infrastructure
IPP	information privacy principles
IT	information technology
PIN	personal identification number
PKAF	public key authentication framework
PKI	public key infrastructure
PSM	Protective Security Manual
RA	Registration Authority
RDA	records disposal authority

1. INTRODUCTION

Key points

- ⇒ User trust and confidence in paper-based transactions needs to be duplicated in electronic transactions (1.1.2).
- ⇒ Systems and infrastructures (or online security technology) have been developed to foster trust in electronic transactions (1.1.3).
- ⇒ Online security technology presents technical challenges for recordkeepers in ensuring that recordkeeping requirements are met and that electronic transactions are captured and stored appropriately (1.1.4).

1.1 Background

1.1.1 Business, security and the world of paper

The successful conduct of business has always required certain security measures to be in place. In the paper world, well established procedures ensure that business transactions are conducted in a predictable and confidential manner, and produce certifiable evidence to meet legal requirements. These processes are also reasonably safe from fraudulent activity.

Paper-based documents are unique and original, and thus provide proof of a transaction. Sealed envelopes, written (and sometimes witnessed) signatures, letterheads, time stamps (such as postmarks), and trusted delivery systems are safeguards that help provide the degree of trust necessary to enable consumer confidence in business transactions. Documents and records are generally filed systematically and remain accessible from the point of creation with limited maintenance or intervention.

1.1.2 Business, computers and ... what security?

In contrast, the systems that support online activities (known as electronic business or e-business) are fundamentally insecure. A document created electronically is not inherently unique and could be one of any number of identical copies, each indistinguishable from the 'original'. The content of transactions created and sent or received electronically may be modified freely and without detection. Digital documents also have the potential to become inaccessible within a short period of time due to hardware and software obsolescence.

Other issues arise when transacting electronically. Consider the case where a document containing recommendations is sent via email to a manager who relies on them to make certain business decisions. How could the manager be sure that the sender:

- was who they said they were
- had the authority to make recommendations
- would not later repudiate either the contents of the document or having sent the email?

1.1.3 Secure solutions for e-business in government

In April 2000 *Government Online – The Commonwealth Government’s Strategy* outlined various principles and standards that agencies should satisfy when placing information and services online.¹ In addition, to enable government business and services to be conducted electronically in a secure manner, systems and infrastructures have been developed to foster the same trust in computer-based commerce as that enjoyed in the traditional world of paper.

Depending on the level of confidence needed, these systems use various forms of online security technology based on authentication and encryption processes. These processes include cryptographic keys and biometrics for a high level of security. More common solutions for a lower level of security use passwords and personal identification numbers (PINs).

1.1.4 Recordkeeping implications

For implementation of e-business in the Australian Government to be successful, it is important that records created in the course of delivering services online are as reliable and retrievable as those produced in the paper world. The use of authentication and encryption processes within the framework of a public key infrastructure (PKI) creates special issues for recordkeeping.

- **Technical challenges** – technologies used to create a secure environment and enable trustworthy online transactions create technical challenges for recordkeeping.
- **Recordkeeping considerations** – authentication and encryption technologies have special recordkeeping requirements that must be met to ensure that appropriate business needs and legislative requirements are satisfied.
- **Electronic recordkeeping systems** – the design of electronic recordkeeping systems must ensure the integrity of the information they store. Such facilities should be secure and provide appropriate access controls, and be capable of completely and accurately capturing and retaining electronically executed transactions.

These and other issues outlined in these guidelines, must be addressed before an appropriate records management strategy can be identified and put in place.

1.2 Purpose

These guidelines provide a tool that Australian Government agencies can use to identify strategies for managing and keeping records of online transactions that are conducted using online security technology. Having such strategies in place will help agencies to operate efficiently, be accountable for their actions, and fulfil their legislative obligations. In order to provide an understanding of the issues involved and the options available for consideration, these guidelines:

- look at e-business in government and the technology that makes trusted online service delivery possible;

¹ National Office for the Information Economy (now Australian Government Information Management Office), *Government Online: The Commonwealth Government’s Strategy*, April 2000, published online at www.agimo.gov.au/publications/2000/04/govonline

- outline the potential recordkeeping implications and make a number of recommendations; and
- identify relevant recordkeeping requirements and strategies for meeting these requirements.

The National Archives of Australia has also developed a general disposal authority (GDA) to authorise disposal of encrypted records resulting from online authentication processes to use in conjunction with these guidelines.

The guidelines contribute to the overall development of recordkeeping systems appropriate to e-business environments. They acknowledge and build upon existing Australian Government standards, policies and legislation relating to electronic recordkeeping and e-commerce activity.

The *Better Services, Better Government* strategy, released by the then National Office for the Information Economy in November 2002, maps out the next steps towards providing better government services through the use of technology.² The strategy includes a requirement to comply with National Archives directions on making and keeping records.

1.3 Scope and audience

These guidelines are for use by all Australian Government agencies and businesses contracted to government that are subject to the *Archives Act 1983* and which:

- use authentication and encryption technologies to facilitate e-business;
- provide secure online service delivery through the Australian Government public key infrastructure (GPKI) framework; and/or
- collect and manage information to support GPKI activities.

Records arising from the conduct of e-business that do not occur within the framework of online security should be managed according to the standards defined in the National Archives *e-permanence* suite of recordkeeping products.

The *e-permanence* products provide advice and guidance on identifying, capturing, managing and disposing of records of business processes, including digital documents and records resulting from online activity.

For further information, please visit our recordkeeping overview at:
www.naa.gov.au/recordkeeping/overview/summary.html

² National Office for the Information Economy (now Australian Government Information Management Office), *Better Services, Better Government: The Federal Government's E-government Strategy*, Commonwealth of Australia, November 2002, published online at <http://www.agimo.gov.au/publications/2002/11/bsbg>

1.4 Acknowledgments

The National Archives would like to thank the following organisations for their assistance in the development of these guidelines:

- Attorney-General's Department
- Australian Customs Service
- Australian Government Information Management Office
- Defence Signals Directorate
- Department of Defence
- Health Insurance Commission
- IP Australia
- Public Record Office Victoria
- Records and Archives Services, Monash University
- State Records New South Wales

1.5 Further information

For further information or to provide comments about these guidelines please contact:

Director
Recordkeeping Standards and Policy
National Archives of Australia
Email: recordkeeping@naa.gov.au
Phone: (02) 6212 3610

2. E-BUSINESS AND AUTHENTICATION AND ENCRYPTION TECHNOLOGIES

This section provides information on the framework and basic functioning of the main forms of online security technology. Readers who are already familiar with online security technology may want to skip to 3 – Recordkeeping implications and recommendations.

Key points

- ⇒ The Australian Government is committed to delivering services online (2.1).
- ⇒ The technologies used by an agency to support its e-business should be chosen after an analysis of security requirements and the application of risk management (2.1).
- ⇒ PKI is the most highly regulated approach (2.2.1).
- ⇒ Australian Government agencies wanting to use digital certificates must use Gatekeeper (2.3).
- ⇒ Agencies can use solutions other than public/private key technology for implementing authentication and encryption processes (2.4).
- ⇒ Some of these other authentication techniques have privacy implications, especially for the collection and storage of personal information (2.4).
- ⇒ All external and internal users of passwords and PINs should be educated about the proper storage and use of such mechanisms (2.4.1).
- ⇒ Privacy regulations relating to storage of personal information must be strictly adhered to, and biometric information must be kept secure and accessible only to authorised personnel (2.4.3).

2.1 Strategies for e-government

The Prime Minister's December 1997 Industry Statement, *Investing for Growth*, recognised the potential of the information economy and envisaged an initial leadership role for the Australian Government.³ It noted that advantages of conducting business electronically include:

- improved public access to a wide range of government services, especially for those in remote and rural areas;
- availability of government services 24 hours a day, seven days a week;
- reduced cost of service delivery in some cases;
- improved quality of some services, including opportunities for implementing better business practices; and
- benefits for the national economy.

³ *Investing for Growth*, address by the Prime Minister the Hon. John Howard MP, 8 December 1997, published online at www.pm.gov.au/news/speeches/1997/industry.htm

In December 1998, *A Strategic Framework for the Information Economy* was released. It addressed the need for a cohesive whole-of-government strategy for implementing government e-business.⁴ This publication outlined key strategic priorities, and covered skills, infrastructure, electronic commerce, industry development, health, culture and regulation.

Focusing on the strategic move towards placing information and services online, *Government Online – The Commonwealth Government’s Strategy* was released in April 2000. This report identified key enablers that facilitate the development and implementation of e-business in government:

- **authentication** – ensuring the identity of a transacting party, and the integrity and security of information exchanged online;
- **privacy** – protecting the collection, security and publication of personal information;
- **security** – addressing storage of information after a transaction is completed;
- **metadata** – applying contextual detail in a way that makes it easy to find information about transactions, and enables related transactions to be conducted together;
- **electronic publishing and recordkeeping guidelines** – ensuring agencies meet both whole-of-government information publishing principles and legal obligations regarding the management of Commonwealth records; and
- **accessibility** – addressing agency obligations to ensure that no social group is excluded from accessing information and services online.

In November 2002, *Better Government, Better Services* was released. This strategy maps the next stage of government online, or ‘e-government’. Its objectives focus on the integrated application of new technologies to government information, service delivery and administration. *Better Government, Better Services* affirms that the key enablers outlined in *Government Online* continue to remain relevant as the essential building blocks for developing sophisticated online service delivery.

In addition to high-level policy, the Australian Government has developed a legal and regulatory framework, known as Gatekeeper, that supports the development and use of online transactions through a government public key infrastructure (GPKI).

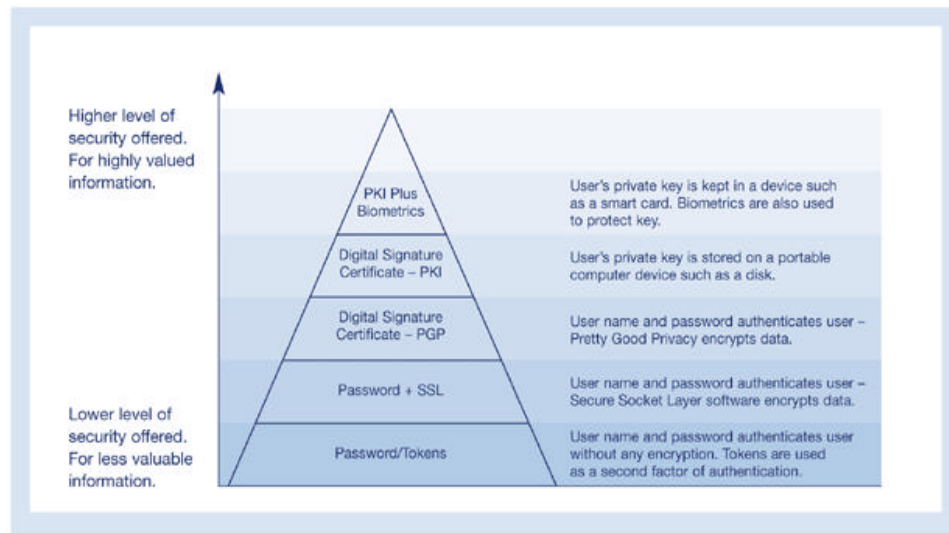
Agencies can choose from a wide variety of technological systems and products to address the requirements of the key enablers. For authentication, in particular, agencies can choose the level of security needed to meet identified risks. Low-risk online activity may require only a password or a PIN, while high-risk transactions might demand implementation of a government-accredited and tightly controlled framework such as the GPKI.

⁴ National Office for the Information Economy (now the Department of Communications, Information Technology and the Arts), *A Strategic Framework for the Information Economy*, December 1998, published online at www2.dcita.gov.au/ie/publications/1998/12/framework

The different technologies available to address authentication requirements of e-business are outlined in Figure 1.⁵ The pyramid indicates that only a very few organisations employ PKI plus biometric technology, while the use of passwords and tokens is widespread.

Figure 1: The pyramid of authentication technologies

The Pyramid of Authentication Technologies



Source: National Office for the Information Economy (now the Department of Communications, Information Technology and the Arts), *Trusting the Internet*, 2002, p. 8, reproduced with permission.

2.2 Public key infrastructure (PKI)

PKI facilitates the uptake and practice of e-business by providing a high level of assurance for the security and authenticity of information transmitted over unregulated, unpoliced networks such as the World Wide Web. To do this, a PKI environment utilises linked services, technologies, standards, legislation and a hierarchical chain of trusted authorities that support the use of public key based digital signatures and encryption on a large scale through the issuance of digital certificates. PKI is usually chosen for high-risk online activities as it provides assurance of:

- **confidentiality** – only intended recipients can read electronic communications;
- **data integrity and security** – electronic communications cannot be changed without detection;

⁵ For further discussion, see National Office for the Information Economy (now the Department of Communications, Information Technology and the Arts), *Trusting the Internet*, 2002, published online at www2.dcit.gov.au/ie/publications/2002/07/trusting_the_net.


- **authentication** – the authenticity of parties involved in an electronic transaction can be verified; and
- **non-repudiation** – parties involved in an electronic communication normally cannot deny their involvement.

Depending on their needs, agencies can choose to utilise PKI services through an established PKI provider, or they may choose to provide PKI services themselves, either in-house or by contracting services to a suitable vendor. Building a PKI in-house requires a secure facility, cryptographic hardware and software, operational infrastructure and specialist technical knowledge.

2.2.1 How does a public key infrastructure work?

PKI makes use of public key technology, whereby public and private cryptographic key pairs enable the secure transmission of information over an unsecured network. The public key and necessary identifying information is contained on a digital certificate. The private key is kept secret, stored securely on a smart card, a token such as an i-button, or on a computer's hard drive protected by a pass-phrase.

Figure 2: A sample digital certificate

Bob's identifying information: name, organisation, address	
Bob's public key	
digital certificate validity dates	
digital certificate number	
issuing authority's digital signature and ID information	

In a PKI, key pairs are obtained and shared, via digital certificates, through a trusted authority. There are two main types of trusted authority.

- **Registration Authorities (RAs)**. RAs provide an evidence of identity service when new subscribers request digital certificates, and manage requests for certificate renewals and revocations.
- **Certification Authorities (CAs)**. CAs issue digital certificates to subscribers. The digital certificate verifies a subscriber's identity and contains their key pair(s), thus enabling them to encrypt messages and sign them with their unique digital signature. These certificates bind the identity of users to their public key material in a trusted and legally recognised manner.

The roles of such trusted authorities do not have to be separate. They can, and often are, assumed by one organisation.

Other components of a PKI include the following.

- **Certificate or key holders** (the subscribers) are issued digital certificates and keys that enable them to encrypt and digitally sign documents. Subscribers may be individuals or organisations and, where automated responses are required, applications and devices.
- **Relying parties** receive, validate and accept digital signatures from the certificate holders.
- **Repositories** store and make available certificate revocation lists and may be part of a Certification Authority.

It is very important to plan for PKI use. An agency must define the scope and structure of its PKI use including:

- use of an organisation-wide digital certificate or individual employee certificates;
- use of public and private authentication (signing) keys, and public and private confidentiality (encryption) keys; and
- development of a key management plan (see 3.2 – Authenticity and non-repudiation).

2.2.2 Using public key infrastructure

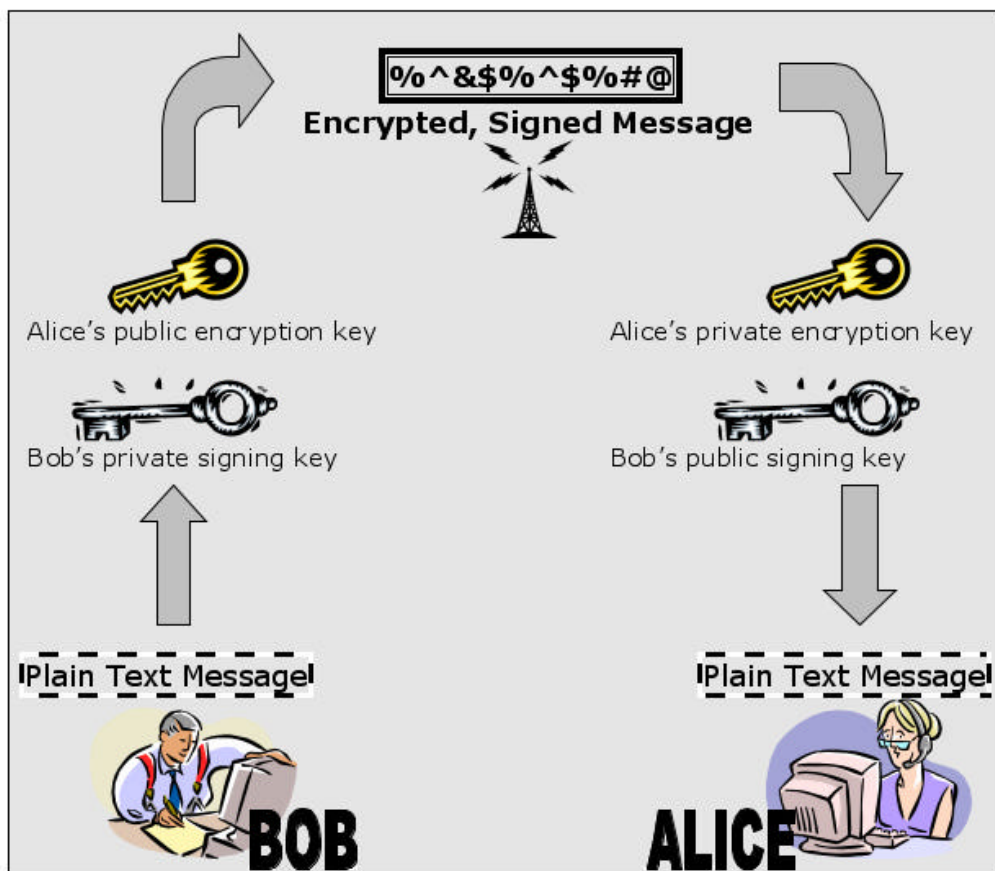
Subscribers in a PKI use their digital certificates to transact with each other in a secure, confidential manner. For example, messages can be encrypted for confidentiality, and digitally signed for authentication and non-repudiation purposes. The use of digital signatures within an accredited framework is legally recognised by the Australian Government (see the *Electronic Transactions Act 1999*).⁶ If implemented properly, digital signatures can be used in a manner similar to traditional signatures written on paper. They may be attached to documents including email, reports, automated transactions and web pages, and can be used in conducting Internet transactions. A single digital signature, covering a record or group of records, may also act as a seal.

Like written signatures in the paper world, digital signatures enable forensic investigation techniques for trying to determine if someone has tampered with a document.

A digital signature should not be confused with an electronic signature (a combination of electronic, audit and system processes). Nor should it be confused with a digitised signature (a scanned facsimile of a written signature). Neither of these provides the same level of assurance of identity or transactional integrity as a digital signature (see Gatekeeper – Frequently Asked Questions at www.agimo.gov.au/infrastructure/gatekeeper/faq/)

⁶ See the *Electronic Transactions Act 1999*, published online at: comlaw.gov.au/

Figure 2: How public key infrastructure works



Bob sends a secure message to Alice using PKI

Bob wants to send a secure message to Alice. He digitally signs the message with his private signing key, stored on his computer or on a token. His computer then scrambles the plain text message using Alice's public encryption key, available from her digital certificate, and sends the message. Only Alice, the intended recipient, is now able to decrypt the message.

Alice receives the message and her computer decrypts it using her private encryption key, stored on her computer or on a token. Her PKI software then uses Bob's public signing key, available from his digital certificate, to verify his digital signature and check the integrity of the message content.

Source: 'Adapted from Government of Canada Public Key Infrastructure Secretariat'.

2.3 The Gatekeeper strategy

The Gatekeeper strategy was published in 1998, and provides a sound framework through which both government and private sector organisations can pursue and promote electronic commerce in an environment of authenticity and integrity.⁷

Since 1999, it has been mandated that Australian Government agencies wishing to use digital certificates must use Registration Authorities and Certification Authorities accredited under the Gatekeeper framework administered by the Australian Government Information Management Office (AGIMO).

Gatekeeper accreditation ensures that organisations and other providers wanting to offer GPKI services meet all applicable legislative requirements in their set-up and implementation documentation. Relevant legislation includes the *Electronic Transactions Act 1999*, the *Privacy Act 1988* and the *Evidence Act 1995*. Use of Gatekeeper digital certificates is appropriate for business transactions or information up to the 'Highly Protected' classification, as described in the *Commonwealth Protective Security Manual*.⁸

Organisations awarded full Gatekeeper accreditation may include both government and non-government organisations.

By October 2003 Gatekeeper accreditation had been granted to the following nine organisations:

- Australia and New Zealand (ANZ) Banking Group Limited (22 August 2003 as a Core Registration Authority; ANZ has also achieved Gatekeeper Recognition)
- Australia Post (20 December 2001 as a Core Registration Authority)
- Australian Taxation Office (16 June 2000 as a Certification Authority and Core Registration Authority)
- Baltimore Certificates Australia Pty Ltd (20 November 2000 as a Certification Authority)
- eSign Australia Limited (5 April 2001 as a Certification Authority and Core Registration Authority; eSign is also accredited to issue ABN-DSCs)
- Health eSignature Authority Pty Ltd (19 January 2001 as a Registration Authority – Extended Services)
- PricewaterhouseCoopers under the name 'beTRUSTed' (7 March 2002 as a Certification Authority and Core Registration Authority; beTRUSTed is accredited to issue ABN-DSCs)
- Telstra Corporation Limited (9 October 2001 as a Certification Authority and Registration Authority – Extended Services; Telstra is also accredited to issue ABN-DSCs).

For further information on accreditation see the AGIMO website at www.agimo.gov.au/infrastructure/gatekeeper/accreditation

⁷ For detailed information, see www.agimo.gov.au/infrastructure/gatekeeper/.

⁸ Information about the *Protective Security Manual* can be found at www.ag.gov.au/www/protectivesecurityHome.nsf/HeadingPagesDisplay/Protective+Security+Manual?OpenDocument

Government services to business and the public that may make use of Gatekeeper include:

- client service information and support
- secure online communication (email)
- procurement
- purchase of goods and services
- payment of goods and services
- payment to suppliers
- receipt of revenue
- online submission of forms
- online submission of declarations and mandated reports.

For example, the Health Insurance Commission is using GPKI-enabled technology across the Australian health sector to facilitate and coordinate the use of different types of online services. These services include secure transmission of:

- pathology results, to or from general practitioners;
- referrals and hospital discharge summaries to or from general practitioners; and
- online prescription claims from pharmacies.

2.4 Other means of online authentication

Government policy does not mandate the use of PKI for authenticating online transactions. Agencies may use other forms of authentication that are appropriate to their security requirements and risk assessment. Non-PKI models of authentication cost less to implement and maintain, and are suitable for less sensitive projects.

Common authentication techniques are generally based upon the following factors. A client:

- has knowledge of something such as a password;
- possesses something such as a smartcard;
- exhibits certain characteristics such as a fingerprint; or
- is trusted and has previously established authentication.

2.4.1 Passwords

Password mechanisms include pass-phrases and personal identification numbers (PINs). Although most authentication schemes rely on these mechanisms to some extent, they constitute a major vulnerability of e-business when used in isolation. Responsible user behaviour is necessary to prevent accidental disclosure. Passwords and PINs may also be subject to large-scale 'dictionary' and/or eavesdropping attacks.

2.4.2 Personal tokens

Tokens usually consist of a small hardware device (eg smartcard, key, i-button, or magnetic stripe card) used in conjunction with a password or PIN. They may require an electronic or a human interface. Since an illegal user must learn the password or

PIN in addition to gaining possession of the token, fraudulent use is often linked to careless behaviour on the part of the password/PIN holder.

2.4.3 Biometrics

Biometric authentication mechanisms include fingerprints, voice or handwriting recognition, and retinal scans. While these are not easily replicable, they must be stored and communicated in a protected form, because they are susceptible to copying and replaying in order to impersonate an authorised individual.

2.5 Other forms of security technology

In lowering the risks associated with conducting business over the Internet, it is not usually sufficient to use authentication techniques by themselves. In addition to being assured of knowing who the clients are, it is necessary to protect the packets of information while they are in transit. Many technological solutions address common security risks of using the Internet. When used in conjunction with authentication mechanisms, these safeguards and services also provide:

- integrity
- confidentiality
- access control

For more detailed information, refer to the publication *Online Authentication – A Guide for Government Managers*, 2002, available online at www.agimo.gov.au/publications/2002/07/online_auth/

3. RECORDKEEPING IMPLICATIONS AND RECOMMENDATIONS

Key points

- ⇒ The use of online security technology requires the creation and maintenance of appropriate records (3.1).
- ⇒ Recordkeeping metadata can be used to document important details relating to the validation of a digital signature (3.2.2).
- ⇒ Agencies that need to re-validate digital signatures should consider maintaining a key management plan (3.2.2).
- ⇒ The National Archives recommends that, for accessibility reasons, records should not be stored in an encrypted form (3.3.2).
- ⇒ Recordkeeping metadata can be used to document the encryption details of a record (3.3.2).
- ⇒ Agencies sending and receiving encrypted records should document their encryption activities and be able to prove the reliability and integrity of the encryption technologies used (3.3.2).
- ⇒ Records that are encrypted to ensure confidentiality during transmission can be disposed of afterwards if certain conditions are met (3.3.3).
- ⇒ Certain legislative requirements affect the use of online security technology (3.4).
- ⇒ Some Australian Government agencies have specific roles in relation to the use of online security technology (3.5.2).

3.1 Setting the scene

From both operational and legal perspectives, the use of online security technology by government agencies raises a number of recordkeeping issues. This section of the guidelines identifies recordkeeping challenges arising from the use of the technology and suggests appropriate ways to address these issues.⁹

The application of digital signatures to ensure the authenticity and non-repudiation of electronic transactions, and the use of encryption to ensure confidentiality of content, are processes that raise issues concerning the integrity, reliability and accessibility of digital records. These issues must be managed from the moment of document creation. For example, accessibility will be compromised if records management fails to ensure ongoing ability to decrypt encrypted records. Or, the integrity of transactions using digital signatures will be compromised unless steps are taken to ensure the continuing validity of related documentation once the transaction is complete.

⁹ Recordkeeping and archival requirements were originally considered in section 3.2.6 of Standards Australia, *Standards for the Implementation of a Public Key Authentication Framework (PKAF)*, 1996.

3.2 Authenticity and non-repudiation

3.2.1 Digital signatures

Digital signatures are most often used within the trusted hierarchy of a PKI. In the Australian Government environment, it is mandatory for digital signatures to be supported by Gatekeeper, or for public key technology that supports digital signatures to be provided by Gatekeeper-accredited authorities. If managed appropriately, digital signatures can provide legal assurance of non-repudiation in relation to online transactions. That is, they can provide a legal association between a person, entity or system and a particular transaction. Digital signatures can also be used as a kind of 'seal' to ensure the continuing integrity of records held in electronic systems. The application of a digital signature permits detection of any alterations to the record, and thus enables verification of a record's authenticity.

Digital signatures may be used in a number of different scenarios. They may be:

- automatically assigned by a computer system on behalf of an entity in the event of high-volume automatic transaction processing;
- applied by an individual in the case of document creation or ad hoc messaging such as email; or
- automatically applied to data objects (including documents and records) by a computer system according to predetermined business rules.

3.2.2 Recordkeeping for digital signatures

Digital signatures must be managed carefully if a digitally signed record of an electronic transaction is to retain its authenticity, and therefore its evidential value.

Agencies may consider two approaches to capturing and maintaining records relating to the use of a digital signature:

- using recordkeeping metadata
- maintaining a key management plan.

An agency will need to take a risk-managed approach when deciding how to meet its requirements for the re-validation of digital signatures over time. It will need to consider the importance of the transaction and the potential need for re-validation at some time in the future.

If the level of risk is regarded as low to medium, then the application of recordkeeping metadata would be an appropriate method of demonstrating the validity of a digital signature at a particular point in time.

If the level of risk is regarded as medium to high, then maintaining a key management plan with access to required keys and digital certificates for the life of the record might be the preferred option.

Recordkeeping metadata

To ensure that a transaction retains its trusted status, agencies may decide to use the 'Digital signature' sub-element of *the Recordkeeping Metadata Standard for Commonwealth*

Agencies to store information relating to use of a digital signature.¹⁰ Information in this metadata sub-element can include:

- the unique identifier of the relevant digital certificate and its issuing authority;
- details of the digital signature attached to the record; and
- date and time stamps showing when the digital signature was successfully applied or validated.

Key management plan

A key management plan is the best way to ensure continuing access to both public and private key pairs. If managed appropriately, the continuing availability of signing keys (used for applying and verifying digital signatures) can be relied upon to verify record authenticity or ensure non-repudiation. This is particularly important where records will be active for long periods of time (potentially after a CA has ceased functioning) or where keys with differing validity dates have been used to facilitate a transaction during the course of its lifetime.

The key management plan should consider the following:

- maintenance of keys for the life of the record;
- availability of digital certificates;
- access to certificate revocation lists (CRLs);
- appropriate key recovery measures;
- date and time stamping;
- collection of appropriate audit and event logs; and
- security of the private key.

For further information about developing a key management plan see Part 3, Chapter 8, 'Communications Security', of the Defence Signals Directorate's *Australian Government Information Technology Security Manual (ACSI 33)* published online at www.dsd.gov.au/library/infosec/acsi33.html.

Agencies that maintain a key management plan should be able to demonstrate:

- the integrity and reliability of the authentication systems they use to digitally sign and/or validate digitally signed records;
- the integrity and reliability of the recordkeeping system(s) in which the digitally signed records are subsequently stored; and
- the security of their recordkeeping system(s).

¹⁰ For more information on recordkeeping metadata and its use, see National Archives of Australia, *Recordkeeping Metadata Standard for Commonwealth Agencies*, 1999, published online at www.naa.gov.au/recordkeeping/control/rkms/summary.htm.

In order to meet these requirements, a valid chain of evidence (or audit trail) must be established, preserved and kept accessible over time to support accountability and in case of dispute. This may involve keeping logs of the following types of events:

- origin or destination of the authenticated transaction;
- time and date the authenticated transaction was sent or received;
- time and date the authenticated transaction was stored;
- time and date of any failed attempts to validate a digital signature; and
- actions of trusted personnel.

3.3 Confidentiality and accessibility

3.3.1 Encryption

Encrypting records by means of cryptographic key pairs ensures that documents, email messages, automated transactions and other digital objects remain confidential during transmission from one party to another. An electronic transaction may be encrypted by an individual on an ad hoc basis, or automatically by a computer system according to predetermined business rules.

The advantage of PKI in this situation is that parties do not need to be known to one another before transacting, as long as they are both subscribers within the GPKI. The public keys used to encrypt the transaction are accessible through known channels and there is no need to share private keys through a secured conduit.

3.3.2 Recordkeeping for encrypted records

If electronic transactions are stored in an encrypted form, they may become inaccessible over time. The most likely reason is the unavailability of the private key needed for decryption.

The National Archives therefore recommends that records not be stored in their encrypted form. Instead, once received, they should be decrypted and stored in an appropriately secure facility (preferably a tamper-proof recordkeeping system), together with the metadata, audit logs and digital certificate information required to establish an evidentiary trail and to provide contextual information.

If, as an additional protective measure, encryption is applied in a single transaction to cover all information stored on a secure server, agencies will need to ensure that the relevant encryption keys are securely managed over time. They must be updated when necessary, so that records contained on the server remain accessible. Keys should be available to authorised personnel only.

Agency procedures should ensure that successfully decrypted records are captured and stored within a suitable recordkeeping system. The system should meet applicable standards and address business and security needs, as well as privacy considerations. A record's capture and storage within the system should affirm its continuing authenticity, integrity, reliability and usability. This will negate the need for retaining the record in encrypted form.

If the agency is using a system that has implemented the *Recordkeeping Metadata Standard for Commonwealth Agencies*, it should consider using the 'Encryption details' sub-element.¹¹ The information captured would include:

- the unique identifier or serial number of any digital certificate used in the transaction and its issuing authority; and
- date and time stamps of the encryption and decryption process.

Certain procedures will minimise the business risk of disputes. For example, if an agency receives an encrypted record that fails to decrypt, it should retain it together with the information detailed above. This will provide support in the event of factual disputes where the outcome may depend on proof of whose encryption applications were at fault.

Where an agency is the sender of the encrypted record, it should keep documentation that demonstrates the reliability and integrity of its encryption technologies. It should be able to show that the system routinely produces encrypted records that can be reliably and accurately decrypted without alteration.

To further establish a reliable audit and evidentiary trail relating to encrypted transactions, the agency should also retain unencrypted versions of records intended for later encryption and transmission, together with associated log files, recordkeeping metadata and appropriate digital certificate information.

Key management

As a general rule, keys and other material required to decrypt data should be accessible for the life of that data.

Where encryption is only used for confidentiality during transmission, there should be no need for a key management plan. Continued access to the encryption keys is unnecessary if the sending agency retains a record of the unencrypted transaction and the receiving agency retains a decrypted record of the transaction. However, both agencies should ensure that the records are captured with recordkeeping metadata relating to the encryption process.

If an agency decides to retain records in their encrypted form, then an ongoing key management plan is essential for enabling future access (see 3.2.2).

3.3.3 Disposal of records

While some decryption processes, particularly high-volume automated transactions, may not retain an encrypted version of a record after successful decryption, many such processes will. Encrypted records that remain in the custody of the receiving agency should not be disposed of as normal administrative practice.

Rather, the National Archives has developed a general disposal authority (GDA) for records that have been encrypted during online security processes. This GDA also

¹¹ National Archives of Australia, *Recordkeeping Metadata Standard for Commonwealth Agencies*, 1999, published online at www.naa.gov.au/recordkeeping/control/rkms/summary.htm.

covers the disposal of encrypted records where the sending agency retains an unencrypted version in its recordkeeping system.¹²

The GDA provides information on the issues that should be considered when disposing of encrypted records. It authorises the disposal of encrypted records, provided that adequate unencrypted or decrypted versions exist, and the conditions and exclusions attached to the GDA are observed.

3.4 Meeting legislative requirements

The environment in which online security occurs is heavily regulated in order to create a framework that ensures that electronic transactions carry evidential value, are secure from unauthorised access and are legally recognised.

Relevant legislation and related standards prescribe the practices of online security. The Gatekeeper framework mandates the creation and maintenance of certain types of data objects and records to ensure systems, their products, and the resulting records remain reliable and retain integrity over time.

3.4.1 Legislation

Agencies need to comply with the following legislation in relation to their online authentication and encryption activities, and their recordkeeping obligations in respect of these activities.

Archives Act

Information created and received in the course of business by an Australian Government agency is a Commonwealth record. Under the *Archives Act 1983*, the National Archives regulates the disposal of Commonwealth records.

Under the Act, disposal of records can only be carried out if:

- the Archives gives permission;
- there is a law positively requiring a particular disposal action;
- the disposal is a 'normal administrative practice' that the Archives has not disapproved; or
- the disposal action is to return the records to the rightful custody of the Commonwealth.

Records can be disposed of via an agency-specific records disposal authority (RDA) or a general disposal authority (GDA) such as the *Administrative Functions Disposal Authority (AFDA)*, which covers records across government arising from common administrative activities.¹³ For example:

- An agency that operates as a CA and/or an RA providing PKI services under Gatekeeper would need to ensure that records relating to these business activities were covered under their own records disposal authority.

¹² *General Disposal Authority for Encrypted Records Created in Online Security Processes*, published online in pdf format at www.naa.gov.au/recordkeeping/disposal/authorities/gda/PDF/gda_encrypted.pdf

¹³ National Archives of Australia, *Administrative Functions Disposal Authority*, 2000, published online at www.naa.gov.au/recordkeeping/disposal/authorities/GDA/AFDA/summary.html

- An agency that makes use of PKI by contracting the services of an already established CA and/or RA would be able to dispose of the administrative records relating to these activities using the AFDA function/activity pairing TECHNOLOGY AND TELECOMMUNICATIONS – Security.
- The records created or received using online security processes such as PKI, should be disposed of according to the business activity to which they pertain, which may be classed within an agency's own records disposal authority or the *Administrative Functions Disposal Authority*.

It is important to note that unauthorised alteration of a record as evidenced by an unverifiable digital signature, or inability to decrypt an encrypted record, may constitute de facto destruction of a Commonwealth record.

Further, the provision of access must also be taken into account. Records that need to be retained for more than 30 years according to specific classes in disposal authorities, must be accessible to the public (subject to certain exclusions), and decisions taken at creation/capture may have a bearing on the ability to meet this requirement.

Electronic Transactions Act

The *Electronic Transactions Act 1999* allows electronic transactions to be considered in the same legal light as those conducted on paper, subject to certain conditions. This means, for example, that a digital signature has the potential to be treated as equivalent to a hand-written signature, thus providing legal certainty for e-business and a basis for the successful operation of schemes such as the GPKI. Notable provisions of the Act include:

- an Australian Government agency must accept electronic transactions from the business community or the public;
- an Australian Government agency must obtain consent from a non-government organisation to conduct electronic transactions;
- organisations have the right to specify certain technological requirements for electronic transactions, such as the use of digital signatures (for authenticity) or encryption (for confidentiality);
- organisations have the right to specify certain formats for the storage of digital records to facilitate the ongoing integrity and accessibility of information;
- the integrity of information contained in an electronic transaction must be maintained, and the information must remain accessible for future reference; and
- systems used to generate and store electronic transactions must ensure the continuing integrity and accessibility of those transactions.

Privacy Act

While the use of authentication and encryption technologies can enhance the privacy of individuals and organisations transacting electronically, there are some important guidelines based on the *Privacy Act 1988* that must be followed to ensure that privacy risks associated with the use of PKI and related technologies are managed appropriately. In particular, Australian Government agencies should adopt the following recordkeeping practices:

- all personal information must be protected by security safeguards, and must not be disclosed without the consent of the individual concerned, unless required by law;
- records containing personal information must be up-to-date and accurate, and must be used only for relevant purposes;
- retention schedules should allow retention of personal information only for the period required for use;
- access to personal information must be provided on demand by the relevant individual;
- an individual must be informed of the purpose for which personal information is being collected, and provide his or her consent;
- individuals must be given information about the importance and available means of maintaining key security;
- the manner in which digital certificates are used must prevent the use of an individual's public key as an identifier to link, match or cross-reference personal information about that individual held in different databases; and
- security measures must be reviewed over time to address potential hazards, such as changes to technology.

Australian Government agencies must also comply with the 11 Information Privacy Principles set out at section 14 of the Privacy Act. The Privacy Principles are published online at www.privacy.gov.au/publications/ipps.html

It should be noted that the Privacy Act applies to many private sector organisations from 21 December 2001. The Privacy Commissioner has indicated that developments in the use of PKI by private sector organisations will be monitored.¹⁴

Evidence Act

The *Evidence Act 1995* requires Australian Government agencies ensure that Commonwealth records in all formats remain admissible under the rules of evidence. Although the Electronic Transactions Act states that an electronic transaction may be provided where there is a requirement to produce a document in writing, it is still essential for evidential purposes that the document's content can be authenticated.

The Evidence Act requires that:

- in the case of a computer or similar document, a party may be permitted to examine and test the way in which the document was produced or has been kept; and
- recordkeeping or similar systems should capture and store records which are authentic, reliable and accurate.

¹⁴ For more information, see Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to Communicate or Transact with Individuals*, 2001, published online at www.privacy.gov.au/government/guidelines/index.html. For privacy policy pertaining to Gatekeeper and Gatekeeper accreditation requirements, see the AGIMO website at www.agimo.gov.au/infrastructure/recommendations.

In the case of records of electronic transactions, it is necessary to give evidence that the system output is what it purports to be. Therefore, an agency should maintain documentation that attests to the reliability of the systems used.

If a digitally signed record tendered in court as evidence has been altered without appropriate authorisation since the time and date of signing, its evidential value will be substantially reduced.

Freedom of Information Act

The *Freedom of Information Act 1982* (FOI) provides for public access to information held by Australian Government agencies. All relevant information requested under FOI must be readily identifiable and accessible.

Recordkeeping systems must be designed to take account of such practical considerations. Agencies need to be aware that information must be accessible until it can be legally disposed of – a requirement that can extend for decades in some cases.

3.5 Current standards and policies

The following standards and policies provide a framework to guide agencies in the implementation of authentication and encryption technologies, and to help them meet relevant requirements and conform to best practice.

3.5.1 Digital recordkeeping

The National Archives, as the Australian Government's recordkeeping authority, develops and promulgates standards and guidelines to enable agencies to meet their recordkeeping obligations. These standards and guidelines are known as the *e-permanence* suite of products.

e-permanence products should be used in conjunction with these Recordkeeping and Online Security Guidelines in order to ensure that all records created are accurate, meaningful, authentic and accessible, and are captured in appropriate systems for as long as required. The following products may be useful to agencies implementing or maintaining online security technology.

- *e-permanence made e-easy: A Manager's Guide to the Strategic Management of Records and Information* is a guide to the full range of *e-permanence* products and their appropriate use. Download in pdf format (630 kb) at www.naa.gov.au/recordkeeping/overview/e-permanence.pdf. This booklet is also available in hardcopy from the National Archives. Email recordkeeping@naa.gov.au to request a copy.
- *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records* provides advice on the creation, management and long-term preservation of digital records. The guidelines are complemented by a checklist to allow agencies to assess the management of their digital records. Both the guidelines and the checklist are published online at www.naa.gov.au/recordkeeping/er/guidelines.html.
- *Archiving Web Resources: A Policy for Keeping Records of Web-based Activity in the Commonwealth Government* and its companion Guidelines provide guidance in establishing internal mechanisms for creating, managing and retaining web-based records. Both the policy and the guidelines are published online at www.naa.gov.au/recordkeeping/er/web_records/intro.html

- The *Recordkeeping Metadata Standard for Commonwealth Agencies* enables agencies to identify, authenticate, describe and manage their digital records in a systematic and consistent way to meet business, accountability and archival requirements. Explanatory material is included with the standard, detailing its purpose, scope, application, and features. The standard is published online at www.naa.gov.au/recordkeeping/control/rkms/summary.htm
- *DIRKS: A Strategic Approach to Managing Business Information* is a comprehensive manual designed to provide guidance on the development of a number of practical tools (eg a business classification scheme, disposal authority, recordkeeping system).

Steps A–C outline the process of analysing an agency’s business environment and determining its recordkeeping requirements. Steps D–H assist agencies to assess the extent to which existing organisational strategies (such as policies, procedures and practices) satisfy recordkeeping or information management requirements.

These steps will also assist agencies to redesign existing strategies or design new strategies to address unmet or poorly satisfied requirements and implement, maintain and review these strategies.

If an agency is implementing an e-business strategy, DIRKS will prove invaluable in ensuring the strategy is integrated successfully and operates in an accountable, efficient manner.

The DIRKS Manual is published online at www.naa.gov.au/recordkeeping/dirks/dirksman/dirks.html

3.5.2 Online security

Online security is paramount for the successful conduct of e-business. Within the Australian Government, several bodies are dedicated to supporting a trusted and secure electronic operating environment. Security of information systems and networks, and the content stored within them, is an essential aspect of secure transactions and secure recordkeeping.

Common principles for e-security in government include:

- the need to develop and disseminate a security policy;
- recognising that different risks apply to electronic transactions when they are in transit, and when they are stored;
- acknowledging that information security involves managing risks to an agency’s business critical information assets, and is therefore a managerial responsibility; and
- effective information security involves a combination of physical, personnel and computer security, and includes policies, procedures, trusted people and trusted technology, disaster preparedness and recovery, contingency planning and training.

In 2002, the Australian National Audit Office (ANAO) published a report called *Internet Security within Commonwealth Government Agencies*. The report found that:

better performing agencies in this audit had comprehensive knowledge of their systems, clearly defined responsibilities for key players, an active approach to

maintaining security and the ability to respond quickly to issues and incidents as they arise.¹⁵

Two of the report's recommendations were:

- **Agencies should ensure that relevant documentation is kept up to date.** Security documentation (such as policies, plans and network descriptions) is of most use to security administrators when it is comprehensive and kept up to date.
- **Security administrators should regularly review logs.** Access logs and event logs are a rich source of information for the web server administrator. Analysing these logs may provide considerable insight into the usage patterns of a website and highlight suspicious or unusual activity.

According to the ANAO report, the top five risks to information security are:

- unsafe data storage practices
- lack of access controls
- unprotected file distribution
- unsatisfactory 'perimeter' defence
- ineffective virus detection.

Following the recommendations in these guidelines will assist agencies to ensure that the first three of these risks are met in relation to online authentication and encryption technologies.

The following agencies have developed products to assist in managing risks to the security of Australian Government information and IT systems.

Australian Government Information Management Office (AGIMO)

AGIMO has a general policy role in defining standards and frameworks relevant to government use of online technologies, including online security. It has the strategic goal of creating a secure and trusted electronic operating environment for the public and private sectors. AGIMO also chairs the E-security Co-ordination Group.

AGIMO's publication *Online Authentication: A Guide for Government Managers* is a helpful introduction to many of the issues that need to be considered when implementing online security technology.¹⁶ *Government Online Security Measures*, including a website and internet system security checklist, was jointly developed with the Defence Signals Directorate.¹⁷

¹⁵ Australian National Audit Office (ANAO) Report No. 13, *Internet Security within Commonwealth Government Agencies*, 2002, published online at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256ACD00215C7C

¹⁶ National Office for the Information Economy (now Australian Government Information Management Office), *Online Authentication: A Guide for Government Managers*, 2002, www.agimo.gov.au/publications/2002/07/online_auth

¹⁷ National Office for the Information Economy (now Australian Government Information Management Office), *Government Online Security Measures*, published online at www.agimo.gov.au/infrastructure/government/.

AGIMO manages Gatekeeper, and has published detailed and stringent specifications for all organisations wishing to become accredited. Requirements include compliance with Australian Government procurement policy, security policy and planning, physical security, technology evaluation, Certification Authority policy and administration, personnel vetting, legal issues and privacy considerations.

Documentation can be found in the publications section of its website at www.agimo.gov.au/publications. The Gatekeeper concepts and operations manual specifies the types of records that must be kept by a CA or RA.

Compliance with Gatekeeper is mandatory for all Australian Government agencies wishing to implement a PKI or use digital certificates. Where strong digital signature-based authentication is used to identify or authenticate business customers online, agencies must use the Australian Business Number (ABN) as the identifier and the Gatekeeper-compliant ABN-Digital Signature Certificate as the authentication tool. Further information is available in *Online Authentication: A Guide for Government Managers*.

Attorney-General's Department (AGD)

The AGD publishes the *Commonwealth Protective Security Manual*. This manual provides Australian Government agencies with a baseline framework for physical, information and personnel security. It clearly identifies the following set of minimum standards.

- The Australian Government expects that each of its agencies will prepare a security plan using risk management principles.
- Minimum standards, whether imposed by legislation or government policy, must form part of every agency's security plan.
- Each agency must establish and maintain a security environment appropriate to its functions and responsibilities.
- The risk environment must be monitored continuously, and the security plan must be evaluated to ensure that the treatments and strategies are effective and cost efficient.

With regard to information security, there is a strong emphasis on ensuring the availability, integrity and confidentiality of Commonwealth information holdings. Copies of the *Commonwealth Protective Security Manual* are available from the Protective Security Coordination Centre, through the Attorney-General's Department website www.ag.gov.au.

Defence Signals Directorate (DSD)

The DSD has developed *Australian Government Information Technology Security Manual* (ACSI 33) to provide guidance for agencies that need to protect their information systems in line with the standards outlined by the *Protective Security Manual*. ACSI 33 is published online at www.dsd.gov.au/library/infosec/acsi33.html.

The DSD identifies the National Archives' role in the implementation of security controls relating to electronic information, in particular storage and accessibility requirements, and directs users of ACSI 33 to the National Archives' policies and guidelines.

4. RECORDKEEPING STRATEGIES

Key points

- ⇒ Authentication and encryption issues need to be addressed early and considered as part of an agency's overall recordkeeping, security and information management framework (4.1).
- ⇒ A strategy for and policy on information management and recordkeeping is necessary for the success of an online security program (4.1.1).
- ⇒ Recordkeeping and information systems should be in place to securely store and maintain an agency's records, including those transmitted using online security technology (4.1.2).
- ⇒ Agencies need to know what records relating to their online security activities should be created and captured (4.1.3).
- ⇒ The business manager, records manager and IT manager need to have assigned responsibilities and roles in order to establish effective and accountable online security processes (4.1.4).
- ⇒ Records that are to be retained as national archives will only be accepted for transfer to the National Archives if they are no longer encrypted (4.2).
- ⇒ Unencrypted or decrypted records should be transferred to the National Archives with contextual information that attests to the validity of the original digital signature (4.2).

4.1 Recordkeeping, security and information management framework

Authentication and encryption issues need to be addressed early and considered as part of an Australian Government agency's overall recordkeeping, security and information management framework. Developing such a framework involves:

- developing a policy and strategy for information resource management;
- assessing and implementing recordkeeping and information systems to maintain required records;
- identifying recordkeeping requirements; and
- assigning responsibilities.

4.1.1 Develop policy and strategy

To ensure the success of an online security program, especially when it involves the use of digital signatures and encryption, a strategy and companion policy for information resource management (including recordkeeping) should be developed. Preferably, the strategy should be developed as part of the online security program, and be in place before implementation of the program occurs. Recordkeeping related to online security technology should be part of an agency's overall information management or recordkeeping policies.

Carefully thought-out strategy and policy documents are necessary, whether records will be captured and stored via an agency's existing recordkeeping system(s), or as part of a separate system. Records created as part of an online security program have special ongoing management issues, as discussed in section 3. The strategy should take these issues into account.

The *Australian Standard for Records Management*, AS ISO 15489 – 2002 endorsed by the National Archives for use in Australian Government agencies, recommends that a recordkeeping strategy should:

- be systematic
- address the principles for good recordkeeping
- identify specific recordkeeping requirements
- delineate the responsibilities of records, business and IT managers
- outline an appropriate preservation plan
- be kept up-to-date to ensure that it remains relevant.¹⁸

It is imperative that recordkeeping standards are mandated and approved at the highest level within an agency. All staff should be aware of the strategic importance of recordkeeping in supporting e-business activities and enabling the online security framework. The policy document should be widely distributed to all staff by the chief executive officer and be included in the induction of new staff. The National Archives has produced a guide to writing a recordkeeping policy, published online at www.naa.gov.au/recordkeeping/overview/policy/summary.html.

4.1.2 Assess and implement a recordkeeping system

In order to achieve a strategic approach to managing business information, based on the Australian Standard for Records Management, agencies should know:

- the context and environment in which they operate;
- the functions, activities and transactions they perform; and
- their recordkeeping requirements, including how they link to its functions and activities.¹⁹

Following this approach to online security programs will enable agencies to have the information required to establish information systems or assess existing systems, and manage records in accordance with identified needs. If the right records are created, captured and maintained appropriately in a secure system, they will be meaningful and accessible to those who need them for as long as required. They will provide evidence against negligence, misleading and deceptive conduct, incomplete/inaccurate processing, security failure, and ineffective or inappropriate authentication mechanisms. A properly functioning recordkeeping system also minimises the risk of breaching legislative requirements on privacy and intellectual property.

The National Archives has published various products to help agencies design and implement recordkeeping systems appropriate to their needs, such as *DIRKS – A Strategic Approach to Managing Business Information*. (See section 3.5 – Current standards and policies, for further information about DIRKS and other useful products.)

¹⁸ See Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002 *Records Management*, Sydney, NSW, 2002.

¹⁹ Standards Australia, AS ISO 15489 – 2002.

4.1.3 Identify recordkeeping requirements

As well as managing records created by authentication and encryption processes, agencies need to know which records relating to their online security activities should be captured to support business needs, satisfy accountability requirements and meet general expectations of the broader community. Knowing recordkeeping requirements will facilitate the development of appropriate recordkeeping strategies and actions.

Deciding which records to keep, and for how long, is a process that relies on an assessment of business risks, costs and benefits. Steps A–C of DIRKS can provide invaluable assistance in determining recordkeeping requirements for specific business environments, including online security.

Reports published by the ANAO also include helpful guidelines on recordkeeping requirements. For example, the audit reported in *Internet Security within Commonwealth Government Agencies* (2002), specifically asked agencies to provide documentation that included ‘security policies and plans, threat and risk assessments, network diagrams, and a description of their Internet services, assets and connectivity’.²⁰

The report also addressed the use of contractors and included several recordkeeping requirements that agencies should follow when contracting-out services. Contractors must provide agencies with access to data, records, accounts and other financial material, or material relevant to the performance of the contract, however and wherever stored or located, under the contractor’s or its subcontractors’ custody, possession or control, for inspection and/or copying. Contractors are also required to create and keep full and complete records in accordance with applicable standards, and maintain them in a way that facilitates access. This includes the records of all electronic transactions.

Recordkeeping requirements relating to GPKI services should be documented in formal contracts, with particular attention to the storage, retention and accessibility requirements of digital certificates and associated keys, digital signatures and encrypted records.

It is worth noting that ANAO found that documentation from agencies with part or all of their IT environment outsourced, contained inconsistencies or had gaps in coverage.

For further information on recordkeeping requirements related to outsourcing, see the National Archives publication, *Records Issues for Outsourcing (including General Disposal Authority 25)* published online at www.naa.gov.au/recordkeeping/outsourcing/outsourcerecords/summary.html

4.1.4 Assign responsibilities to records, business and IT managers

Online security is a complex web of software, hardware, technology providers, external service providers, personnel, policies, procedures and agreements. Each of these elements may impact on several areas within an agency that use or provide these services. To ensure that all recordkeeping requirements relating to online security are addressed in a comprehensive manner, it is essential that recordkeeping responsibilities are identified, assigned and promulgated across an agency.

²⁰Australian National Audit Office (ANAO), Report No. 13, *Internet Security within Commonwealth Agencies*, 2002, clause 4.2, published online at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256ACD00215C7C

Managers in the records, business or e-business, and IT areas will all have a role in the implementation and delivery of online security services. Establishing communication channels is a useful way of enabling information flow. Meetings should be held to ensure that questions and issues are addressed. Procedures can then be developed and disseminated to provide a measure of control.

Interoperability of systems is essential for ensuring optimum accessibility of information, and provides long-term cost savings to an organisation. If an area responsible for implementing online security has established communication channels with other areas likely to have some responsibilities, the required specifications are more likely to be known and understood. Checklists can be developed to ensure any new systems purchased will have the desired characteristics. High-level schema can be written for existing systems that may not be fully interoperable.

Some of the questions that managers should be asking to ensure complete functionality are listed below.

Business manager

It is essential that the person responsible for overseeing the implementation of online security processes in an agency ensures adequate information flow to support areas, such as the IT and recordkeeping sections.

- Have communication channels been established with all relevant work areas?
- Are the proposed online security processes appropriate for the business activities to which they relate?
- Have all online security processes been tested to ensure they produce reliable electronic transactions, and the test results documented?
- Has the recordkeeping policy and accompanying strategy been integrated with existing policy, and distributed and approved by the business area?
- Do the business plan and risk assessments include recordkeeping considerations, such as evidential, legislative and accessibility requirements?
- Has a key management plan been developed, if necessary?
- Are relevant personnel accredited and security cleared where appropriate, including contracted staff?
- Are all systems suitably secured according to Australian Government guidelines?
- Are contingency arrangements in place for a disruption in power, a security breach or a systems failure?
- Is there a policy in place for the ongoing monitoring and review of systems and strategies?

Records manager

If an agency uses digital certificates or performs online security processes, the records manager must ensure appropriate recordkeeping strategies for these transactions.

- Has a recordkeeping policy and accompanying strategy been developed and approved? Note that it should take account of the business needs of the agency's authentication and encryption activities.

- Have all recordkeeping requirements been identified, including legislation, standards and evidentiary requirements?
- Is there a disposal authority specifying retention requirements for electronic transactions?
- Is the recordkeeping system that captures and stores records of electronic transactions capable of maintaining the records appropriately, in a manner that preserves the content, structure and context of the records, and ensures their accessibility over time?
- Does the system maintain the authenticity of electronic transactions by, for example, capturing contextual metadata?
- Does the system allow for migration of records to new software platforms in a way that retains the authenticity and integrity of the records?
- Does the system have sufficient security controls? Do they meet Australian Government guidelines?
- If a key management plan is necessary, has the recordkeeping section contributed to its development?

IT manager

The IT manager should be in close liaison with the business area responsible for implementing online security processes, as well as the recordkeeping section (or equivalent).

- Do existing systems meet stringent online security requirements?
- Are there sufficient personnel available to maintain the system to specifications?
- Does the system capture sufficient transaction-level detail as identified by the records or business manager?
- If more than one system is used, are they interoperable?
- Do systems meet Australian Government standards for security, and are all logs and audit trails checked on a regular basis?
- Is there a contingency plan for physical security threats, such as loss of power? Does the plan include proper back-up and recovery procedures?
- If electronic transactions are not captured into a function-specific recordkeeping system, does the system capture and store records of electronic transactions? Is it capable of maintaining the records appropriately, in a manner that preserves the content, structure and context of the records, and ensures their ongoing accessibility and integrity?
- If a key management plan is necessary, has the IT area contributed to its development?

4.2 Records to be retained as national archives

Some records that result from electronic transactions processed within online security systems in the Australian Government may be appraised as being national archives – that is, assessed as having continuing value according to criteria specified by the National Archives. These records will eventually be transferred to the National

Archives and, subject to certain provisions, made available for public access after 30 years.

The National Archives custody policy is to accept any record deemed to have archival value, regardless of format, as soon as its business need has ceased. However, the National Archives will only accept digital records created and used as part of online security processes in unencrypted or decrypted form. This will ensure that these records remain accessible, readable and retrievable. To preserve the quality of its collection, the National Archives also needs to ensure that records received into its care retain contextual information so that the integrity of the records is maintained.

Why? It is impossible for the National Archives to gain access to and store all the components of authentication schemes necessary to ensure their ongoing functionality. The Archives will be unable to re-validate digital signatures attached to records because it will not attempt to gain possession of the relevant public and private keys (or equivalent device).

Similarly, the National Archives will not have the ability to decrypt records. There are many different means by which a record may have been encrypted and it would not be possible to guarantee the ongoing functionality of each one – or even gain access to the various schemes.

If a record is transferred to the National Archives, it is unlikely that there will be a continuing business need for any attached digital signatures to remain functional. However, an agency needs to make a risk management decision on whether it continues to support the key management plan for records that have been transferred to the National Archives. The agency may choose to capture appropriate recordkeeping metadata as sufficient proof that the digital signature was valid at the time of the transaction. On the other hand, the risk management process could require the agency to maintain the key management plan to provide access to the public key for the purpose of re-validation.

Unencrypted or decrypted records should be transferred together with the contextual information (eg encryption details such as the name of the CA or RA provider, the reference number of the digital certificate that contained the public key, and the date and time of the transaction).

Meeting the recordkeeping recommendations contained within these guidelines will ensure the accessibility, readability, integrity and completeness of digital records created during online security processes, and ensure that records transferred as national archives will be well controlled and accompanied by appropriate metadata. Records transferred to the custody of the National Archives will be stored in conditions that ensure their security and long-term preservation and accessibility.

5. IMPLEMENTATION CHECKLIST

The intention of this checklist is to serve as a tool that Australian Government agencies can use when planning to use authentication and encryption technologies.

5.1 Initial considerations

- Has your agency established the level of online security needed?
- Have online security processes been included in your agency's recordkeeping, security and information management framework?

5.2 Technology considerations

- Has your agency chosen the type of technology it will use, based on its security requirements and risk assessment?
- If your agency wishes to use PKI, have you applied to use Gatekeeper technology?
- If your agency wishes to become a Certification Authority or Registration Authority, have you applied for Gatekeeper accreditation?
- If your agency will use other forms of online security technology, have you investigated the privacy, user training, storage and access considerations related to particular forms of technology?

5.3 Recordkeeping considerations

- Has your agency developed a strategy and policy on information management and recordkeeping?
- Has your agency put recordkeeping and information systems in place to securely store and maintain its records?
- Does your agency know what records relating to its online security activities should be created and captured to meet legislative, business and community expectations?
- Does your agency produce documentation to prove the reliability and integrity of the encryption technologies it uses?
- Is your agency aware of the requirements imposed by Australian Government agencies with specific roles in the use of online security technology?
- Are staff with specific roles, such as the business manager, records manager and IT manager, aware of their responsibilities?
- Will recordkeeping metadata be used to document important details relating to the validation of a digital signature and the encryption of a record? If so, are procedures and systems in place to allow its capture and maintenance?
- Will your agency require a key management plan?

- Is your agency familiar with the conditions attached to the use of the *General Disposal Authority for Records that have been Encrypted during Online Security Processes*?
- Has your agency made arrangements to ensure that ‘retain as national archives’ records can be transferred to the National Archives in an unencrypted form, with appropriate contextual information?

APPENDIXES

Glossary

Australian Business Number-Digital Signature Certificate (ABN-DSC)	A digital certificate linked to an entity's ABN. The certificate identifies an individual with an associated entity that has an ABN.
Authentication	Authentication is the process of establishing that the sender of a message is who he/she claims to be.
Authenticated transaction	An electronic transaction that has a digital signature attached to it.
Certification Authority (CA)	A body that generates, signs and issues public key certificates which bind subscribers to their public key.
Certificate revocation list (CRL)	The published directory that lists revoked and/or suspended certificates. The CRL may form part of the certificate directory or may be published separately.
Cryptographic keys	Data elements used to encrypt or decrypt electronic messages. They consist of a sequence of symbols that control the operation of a cryptographic transformation, such as encipherment.
Decrypted record	A digital record that was subject to an encryption process but that has since been successfully deciphered.
Digital certificate	An electronic document signed by the Certification Authority which: <ul style="list-style-type: none">• identifies a key holder and the business entity he or she represents;• binds the key holder to a key pair by specifying the public key of that key pair; and• should contain any other information required by the certificate profile.
Digital record	Record communicated and maintained by means of digital computer technology. Digital records are a subset of electronic records.
Digital signature	An electronic signature created using a private signing key.
Disposal authority	Formal instrument that defines the retention periods and consequent disposal actions authorised for classes of records described in the authority. Previously referred to as disposal schedules.
Electronic business (e-business)	Business activity that is conducted online.

Electronic commerce (e-commerce)	All business transactions that are conducted by electronic means.
Electronic record	See Digital record .
Electronic transaction	A discrete packet of data transmitted in the course of conducting business activity online, whether in the form of a message, automated transaction or other type of digital communication.
Encryption	Encryption is the conversion of data into a secret code for transmission over a public network.
Encrypted record	A digital record that is the product of an encryption process.
Gatekeeper	The Australian Government strategy to develop public key infrastructure to facilitate government online service delivery and e-procurement.
Government public key infrastructure (GPKI)	The GPKI is the collective term for the standards, products, services and service providers certified under the Gatekeeper strategy. It also refers to the policies created for the management of those standards, products, services, and the relationships between them.
Key pair	A pair of asymmetric cryptographic keys (ie one decrypts messages which have been encrypted using the other) consisting of a public key and a private key.
Non-repudiation	Non-repudiation prevents an individual or entity from denying having performed a particular action related to electronic data (such as origin, intent or ownership).
Online authentication	A system, technology or process that ensures the integrity, security and authenticity of electronic transactions conducted via an unsecured, public network.
Private authentication key	The key used by the key holder to digitally sign messages on behalf of an organisation.
Private confidentiality key	The key used by the addressee to decrypt messages, which have been encrypted using the corresponding public confidentiality key.
Public authentication key	The key which corresponds to a private authentication key, used to authenticate a digital signature.
Public confidentiality key	The key which corresponds to a private key held by the addressee, which is used to encrypt a message to protect the confidentiality or privacy of the contents.
Public Key Authentication Framework (PKAF)	A Public Key Authentication Framework is an Australian standard (AS/NZS 4539) that provides a structure for the generation, distribution and management of public key certificates.

Public key infrastructure (PKI)	The combination of hardware, software, people, policies and procedures needed to create, manage, store and distribute keys and certificates based on public key cryptography.
Public key technology (PKT)	Public key technology is the hardware and software used for encryption, signing, verification as well as the software for managing digital certificates.
Registration Authority (RA)	An entity that performs services in relation to registration and verification of the identity of applicants for public key certificates, as described in the Registration Authority accreditation criteria.
Record	Information in any format created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.
Recordkeeping system	Framework to capture, maintain and provide access to evidence over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. Recordkeeping systems include: (1) both records practitioners and records users; (2) a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices; policy statements, procedures manuals, user guidelines and other documents which are used to authorise and promulgate the policies, procedures and practices; (3) the records themselves; (4) specialised information and records systems used to control the records; and (5) software, hardware and other equipment, and stationery.
Relying party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
Retain as National Archives (RNA)	The disposal action for records appraised as having archival value.
Subscriber	Either the person, or the business entity and the person who acts on behalf of the business entity, that is in possession of or has control of the private authentication key and who uses that key to digitally sign/receive messages.
Unencrypted record	A digital record that is intended for encryption but has not yet been subject to an encryption process.

Further reading

Commonwealth legislation

Archives Act 1983, published online at comlaw.gov.au

Electronic Transactions Act 1999, published online at comlaw.gov.au

Evidence Act 1995, published online at comlaw.gov.au

Freedom of Information Act 1982, published online at comlaw.gov.au

Privacy Act 1988, published online at comlaw.gov.au

Publications

Attorney General's Department, *Commonwealth Protective Security Manual*, published online at www.ag.gov.au/www/protectivesecurityHome.nsf/HeadingPagesDisplay/Protective+Security+Manual?OpenDocument

Australian National Audit Office, *Report No. 13 (2002): Internet Security within Commonwealth Government Agencies*, 2002, published online at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256ACD00215C7C

Defence Signals Directorate, *Australian Government Information Technology Security Manual (ACSI 33)*, 2004, published online at www.dsd.gov.au/library/infosec/acsi33.html

Department of Industry, Science and Resources (now the Department of Industry, Tourism and Resources), *Investing for Growth* (the Prime Minister's December 1997 Industry Statement), 1997.

National Archives and Records Administration and Federal Public Key Infrastructure Steering Committee's Legal/Policy Working Group, *Records Management Guidance for PKI-Unique Administrative Records*, 2003, published online at www.archives.gov/records_management/policy_and_guidance/pki_guidance.html

National Archives of Australia, *Archiving Websites: A Policy for Keeping Records of Web-based Activity in the Commonwealth Government*, 2001, published online at www.naa.gov.au/recordkeeping/er/web_records/intro.html

National Archives of Australia, *Archiving Websites: Guidelines for Keeping Records of Web-based Activity in the Commonwealth Government*, March 2001, published online at www.naa.gov.au/recordkeeping/er/web_records/guide_contents.html

National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*, 2004, published online at www.naa.gov.au/recordkeeping/er/guidelines.html

National Archives of Australia, *DIRKS: A Strategic Approach to Managing Business Information*, 2001, published online at www.naa.gov.au/recordkeeping/dirks/summary.html

National Archives of Australia, *Recordkeeping Issues for Outsourcing (including General Disposal Authority 25)*, 1998, published online at www.naa.gov.au/recordkeeping/outsourcing/outsourcerecords/summary.html

National Archives of Australia, *Recordkeeping Metadata Standard for Commonwealth Agencies*, 1999, published online at www.naa.gov.au/recordkeeping/control/rkms/summary.htm

National Office for the Information Economy (now the Australian Government Information Management Office), *Gatekeeper Accreditation*, 2003, published online at www.agimo.gov.au/infrastructure/gatekeeper/accreditation

National Office for the Information Economy (now the Australian Government Information Management Office), *Better Services, Better Government: The Federal Government's E-government Strategy*, 2002, published online at www.agimo.gov.au/publications/2002/11/bsbg

National Office for the Information Economy (now the Australian Government Information Management Office), *Online Authentication: A Guide for Government Managers*, 2002, published online at www.agimo.gov.au/publications/2002/07/online_auth

National Office for the Information Economy (now the Australian Government Information Management Office), *Government Online: The Commonwealth Government's Strategy*, 2000, published online at www.agimo.gov.au/publications/2000/04/govonline

National Office for the Information Economy (now the Department of Communications, Information Technology and the Arts), *Trusting the Internet*, Commonwealth of Australia, July 2002, published online at www2.dcita.gov.au/ie/publications/2002/07/trusting_the_net

National Office for the Information Economy (now the Department of Communications, Information Technology and the Arts), *Gatekeeper: A Strategy for Public Key Technology in Government*, 1998, published online at www.dcita.gov.au/Article/0,,0_1-2_1-4_14172,00.html

National Office for the Information Economy (now the Department of Communications, Information Technology and the Arts), *A Strategic Framework for the Information Economy*, 1998, published online at www2.dcita.gov.au/ie/publications/1998/12/framework

Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies Using PKI to Communicate or Transact with Individuals*, 2001, published online at www.privacy.gov.au/government/guidelines/index.html

Public Service Commissioner, *Values in the Australian Public Service*, Direction 2.6, published online at www.apsc.gov.au/publications00/values6.htm

Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002, Standards Australia, Sydney, 2002.

Standards Australia, *Information Technology – Public Key Authentication Framework (PKAF)*, AS 4539.1.1 – 2002, Standards Australia, Sydney, 2002.

Standards Australia, *Strategies for the Implementation of a Public Key Authentication Framework (PKAF)*, Standards Australia, Sydney, 1996.