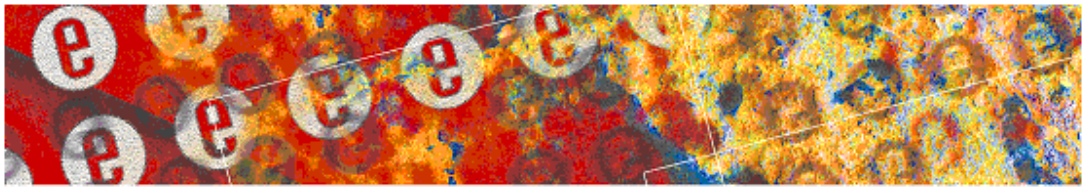

NATIONAL ARCHIVES OF AUSTRALIA

General Disposal Authority

For encrypted records created in online security processes

May 2004

ISBN 1 920807 04 7

CONTENTS

INTRODUCTION

Online security promotes trust and confidence when conducting business over unsecured networks such as the Internet. Part of the online security process may involve encrypting information by means of cryptographic keys to ensure integrity, authenticity and confidentiality during transmission.

The sender of encrypted electronic transactions may keep records of the encrypted form as evidence of what was sent. The receiver of encrypted transactions may retain the encrypted versions or make copies of them to verify the decryption process. A party to online transactions may deal with records of both outbound and inbound transactions in encrypted form.

Encrypted records created or received by Australian government agencies in online security processes generally are Commonwealth records subject to the *Archives Act 1983*.

In most cases, the encrypted form of the transaction has served its purpose (for both the sender and receiver) once the online security process is verified as trustworthy and the parties accept that the content of the receiver's decrypted form is the same as the sender's unencrypted form. Unless there are special reasons for retaining the encrypted form, keeping records in a form without encryption should be sufficient.

Recordkeeping systems operated by an agency should meet applicable standards and be designed to address business and security needs, as well as privacy requirements. A record's placement and storage within a recordkeeping system should therefore imply its continuing authenticity, integrity, reliability and useability.

However, storing records in encrypted form raises accessibility issues. The Archives recommends that records not be stored in an encrypted state longer than necessary. The Archives will only accept digital records of archival value into its custody in unencrypted or decrypted form.

The Archives has produced guidelines to help agencies effectively manage recordkeeping issues relating to online security processes (available at www.naa.gov.au/recordkeeping/er/summary.html).

Disposal authorisation

This General Disposal Authority (GDA) is issued to the heads of all Australian government agencies. It authorises arrangements for the disposal of records in accordance with section 24(2)(b) of the *Archives Act 1983*.

Under the Archives Act, the Archives' permission is required for the destruction or other disposal of Commonwealth records. Exceptions to this are where the destruction or disposal is required by any law, or is in accordance with a normal administrative practice, other than a practice of a department or authority of which the Archives has notified the department or authority that it disapproves.

Advice on the provisions of the Archives Act may be obtained from the National Archives of Australia.

Purpose

The purpose of the GDA is to permit the destruction of encrypted records, created during online security processes, that are no longer required.

The GDA covers encrypted versions of inbound and outbound electronic transactions. A number of conditions are attached to the use of the GDA.

The GDA does not cover the disposal of:

- the corresponding unencrypted records of a sending agency, or the decrypted records of a receiving agency;
- encrypted records that are subject to an exclusion category; or
- records subject to encryption outside the context of online security processes.

The disposal of these records is subject to the Archives' permission through other GDAs and records disposal authorities (RDAs).

Further information

For information about obtaining disposal authorisation see Appendix 8 of the DIRKS Manual – Procedures for developing a records disposal authority in the Commonwealth (available at www.naa.gov.au/recordkeeping/dirks/dirksman/contents.html).

Review

The Archives intends to review this authority within five years of the date of issue. Agencies using the authority should ensure that it is still current. Comments on the application and use of this authority are welcome.

Contact information

Inquiries concerning this disposal authority should be directed to the National Archives of Australia:

Queen Victoria Terrace
Parkes ACT 2600

PO Box 7425
Canberra Business Centre ACT 2610

Tel: (02) 6212 3610
Email: recordkeeping@naa.gov.au
Website: www.naa.gov.au/recordkeeping/

Glossary of terms

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.
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.
Encrypted record	A digital record that is the product of an encryption process.
Online security	Collective term to describe both authentication and encryption technologies where they are used to provide confidence and trust in the identity of a party transacting online, and confidentiality of the electronic transaction during transmission.
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: • records practitioners and records users; • 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; • the records themselves; • specialised information and records systems used to control the records; and • software, hardware and other equipment, and stationery.
Unencrypted record	A digital record that will be, or has been, subject to an encryption process.

GENERAL DISPOSAL AUTHORITY FOR ENCRYPTED RECORDS CREATED IN ONLINE SECURITY PROCESSES

Person to whom notice of authorisation is given:	Heads of Commonwealth institutions under the *Archives Act 1983*, as listed in National Archives file 2004/1153.
Purpose:	Authorises arrangements for the disposal of records in accordance with section 24(2)(b) of the *Archives Act 1983.*
Application:	The authority permits the destruction of encrypted records that result from the use of online security processes, subject to exclusions and conditions.

This authorisation applies to only the disposal of the records described on the authority in accordance with the disposal action specified on the authority. The authority will apply only if disposal takes place with the consent of the organisation that is responsible at the time of disposal for the functions documented in the records concerned.

4 MAY 2004

Authorising Officer,
National Archives of
Australia

Date of issue

Adrian Cunningham
Acting Assistant Director-General
Government Recordkeeping

Job Number: 2004/00238694

General Disposal Authority

Entry	Description of records	Disposal action
8626	Encrypted versions of inbound and outbound electronic transactions resulting from the use of online security processes except those covered by the attached *Exclusions.*	Destroy at agency discretion, subject to the attached *Conditions.*

Exclusions

1.1 The authority does not cover the disposal of encrypted records where:

(a) there is a legal requirement to keep or retain the records in encrypted form;

(b) the records are required, or likely to be required, for a current or pending court action, government inquiry or investigation, or are the subject of a current application for access under the *Freedom of Information Act 1982*, *Archives Act 1983* or other relevant legislation;

(c) there is a government policy or directive not to destroy the records;

(d) an agency has identified significant business or other reasons for the retention of the records;

(e) the records are subject to a disposal freeze which states that this authority does not apply. This authority may otherwise be applied to records covered by disposal freezes; or

(f) attempts to decrypt encrypted records are unsuccessful.

Notes on the Exclusions

(1) In the cases of (a) to (f) above, encrypted records must be retained together with the appropriate metadata and log files.

(2) In the case of (f) in particular, this will enable an agency to make a case in the event of factual disputes where the outcome may depend on proof of whose decryption method was at fault.

Conditions

Management of the online security process

1.1 Agencies must ensure that:

(a) adequate quality control and verification procedures for their online security processes are in place and are routinely applied;

(b) sufficient system documentation is kept to demonstrate that the online security process used routinely produces encrypted records that can be reliably and accurately decrypted; and

(c) sufficient system documentation is kept to demonstrate that the online security process used routinely produces decrypted records that maintain their authenticity, integrity, reliability and useability.

Recordkeeping requirements of encryption processes

2.1 Upon creation of encrypted records intended for transmission, agencies must ensure that the unencrypted versions of the records are retained and captured into an appropriate recordkeeping system together with associated log files and recordkeeping metadata.

2.2 Before transmission, agencies must ensure that encryption has been performed to a standard that permits the encrypted records to be accurately decrypted.

Recordkeeping requirements of decryption processes

3.1 Upon receipt of encrypted records, agencies must ensure that, before destruction, decryption is performed to a standard that ensures accuracy of translation and proper functioning of security and business processes.

3.2 Decrypted records should be retained and captured into an appropriate recordkeeping system together with associated log files and recordkeeping metadata.

Maintenance of decrypted and unencrypted records

4.1 Agencies must ensure that:

(a) the decrypted or unencrypted records are maintained for as long as required by any current disposal authority applying to the class of records to which they belong; and

(b) the decrypted or unencrypted records are kept in accordance with relevant recordkeeping standards and guidelines promulgated from time to time by the Archives for Australian government use.

Management of destruction process

5.1 Control records or recordkeeping metadata must be kept that adequately specify the types and ranges of encrypted records that are destroyed.

Management of electronic systems

6.1 In an electronic environment, agencies must ensure that they have appropriate systems and strategies in place to maintain their records in an accessible condition for as long as required.