ADRI

Statement on the Application of Digital Rights Management Technology to Public Records

ADRI-2008-001-v1.0

CAARA

Council of Australasian Archives and Records Authorities

Version 1.0
6 August 2008

Further copies of this document can be obtained from the ADRI Web site http://www.adri.gov.au/ or http://www.adri.govt.nz/

Document Control

Version	Date	Author	Comment
1.0	6 August 2008		Version approved by CAARA

Endorsement

This document has been approved by the Council of Australasian Archives and Records Authorities as a Position Statement on 6 August 2008.

Acknowledgements

We would like to acknowledge the help given by those people and organisations who commented on drafts of this document.

Australasian Digital Recordkeeping Initiative (ADRI)

The Australasian Digital Recordkeeping Initiative (ADRI) is composed of representatives from all state and national archival authorities in Australia and New Zealand. The members of ADRI are:

- National Archives of Australia
- Archives New Zealand
- Public Record Office Victoria
- State Records NSW
- ACT Territory Records
- Archives Office of Tasmania
- Northern Territory Archives Service
- Queensland State Archives
- State Records South Australia
- State Records Office Western Australia

The aim of the Initiative is to develop and harmonise a uniform set of standards, guidelines, and practices for digital recordkeeping. A related aim is to improve the organisational capability, capacity, and expertise within the collaborating institutions in relation to digital recordkeeping.

ADRI is a working group of the Council of Australasian Archives and Records Authorities (CAARA). CAARA is the peak body of government archives and records institutions in Australia and New Zealand.

Contents

1 Purpose of the Position Statement

This Position Statement is developed to ensure records access and disposal provisions of the various archives and records legislation in different jurisdictions are not undermined by the application of Digital Rights Management (DRM) technology to public records.

2 Background

DRM provides a technological approach to copyright protection for digital content, using software that allows creators/providers to control what happens to documents and messages after they are sent. DRM can regulate the types of actions that can occur with information (for example, view, print, copy or modify) and the time frame in which that information remains accessible. DRM is also known as Information Rights Management, Document Rights Management, Rights Services Management or Enterprise Rights Management.

CAARA members recognise that the use of DRM technology may impair the ability of governments in Australia and New Zealand to capture full and adequate records ensuring the preservation of and access to government business, decisions and communications.

CAARA supports copyright owners protecting their intellectual property. However, legitimate copyright interests have to be balanced against the legislative requirements for governments to manage and preserve the evidence of their decisions and activities. Records access and disposal provisions must also be observed, including records where copyright may be held by third parties.

3 DRM challenges for recordkeeping

DRM challenges one of the principles underlying recordkeeping. Australian and International Standard AS ISO 15489 for Record Management defines a record as "information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".

The potential risks to good recordkeeping that are posed by DRM technologies include:

- auto-deletion – inhibits the ability of an agency to capture and maintain full records of its business
- print disabling – for agencies maintaining records in paper format, this prevents agencies keeping records in accordance with their processes
- forward disabling of email messages – prevents capture into many systems thereby preventing agencies capturing records of business; and
- encryption – through loss of keys and passwords, encryption can prevent access and therefore effective loss of records to government and the public
- security – each time a protected object is accessed, there is communication between DRM systems and external rights services, which may affect information security and access provisions.

4 Considerations for public authorities

Public authorities intending to use DRM technology need to determine whether application of the technology will compromise their compliance with legislation for the retention, access and use of information. Where DRM technology is deemed to be acceptable, the considerations are:

- DRM encumbered information is disclosed to and/or understood by the public authority
- where a public authority chooses to use DRM technology for information it owns, it retains full and exclusive control over that information
- assurances are sought from vendors to ensure future accessibility for any legitimate users
- DRM constraints are only imposed if there is clear business reason for doing so
- modifications to Government information may not be undertaken without explicit Government approval
- any use of DRM does not hinder the long-term access to information for reasons such as hardware or software dependencies, loss of security access keys or outdated DRM rules.

5 Position Statement

1. For as long as it has any business or statutory requirements to do so, government must be able to:
   - use the information it owns/holds
   - provide access to its information to others, when they are entitled to access it, including future provision for audit, archival, legal and other purposes.
2. Government use of digital rights management technologies must not compromise the privacy accorded to individuals who use government systems, or about whom the government holds information.
3. The use of digital rights management technologies must not endanger the integrity of government-held information, or the confidentiality and protection of personal information, by permitting information to enter or leave government systems, or be amended while within them, without prior government awareness and explicit permission.
4. The security of government systems and information must not be undermined by use of digital rights management technologies.

These principles are drawn from policy advice *Trusted Computing and Digital Rights Management Principles and Policies*, September 2006, issued by the New Zealand State Services Commission. In 2007, the New Zealand Government released *Trusted Computing and Digital Rights Management Standards and Guidelines* to assist agencies and vendors in the application of the principles and policies. The Standards and Guidelines are a useful set of tools to explore and implement new software that may or may not have DRM implications.

6 Scope

The principles are suitable for adoption by all 'agencies' as defined by CAARA members' archival legislation or other standards and instruments.