Government of South Australia

GPO Box 2343
ADELAIDE SA 5001
Tel (08) 8204 8791
Fax (08) 8204 8777 DX:467
srsaRecordsManagement@sa.gov.au
www.archives.sa.gov.au

State Records of South Australia

Digital Rights Management - Implications for Recordkeeping

Introduction

Digital Rights Management (DRM) refers to technology that allows the creator/provider of digital information to control when and how that information is used. It consists of a set of technologies designed to apply and enforce persistent access restrictions to digital information, as specified by the information creator/provider.

State Records is concerned that the use of DRM technology may prevent South Australian State and Local Government from managing official records of government in accordance with the *State Records Act 1997*.

The purpose of this Recordkeeping Advice is to:

- inform State and Local Government agencies about DRM technology and the potential risks to records management for agencies considering implementation of DRM in their agencies, and
- provide advice to managers, information and records managers and IT personnel implementing and applying DRM technology in their agencies.

What is Digital Rights Management (DRM)?

Digital Rights Management[1] (DRM) is a persistent document-level protection technology. DRM is based on digital certificates and public key encryption technology.

DRM allows information creators/providers to restrict access/use permissions to information, including email messages. This means the creator/provider of digital information can at any time withdraw permission for a user to view digital information, can prevent the user from printing a copy of the information, forwarding the information, copying and pasting the information, or prevent storing a copy in an information system, such as an electronic document and records management system (EDRMS). For example, a contractor could use DRM to withdraw permission for a government agency to view copies of contract documents that the contractor had sent to the agency.

In addition, DRM allows information creators/providers to set time-based rights protection. That is, a future date can be set so that users of the information can no longer view or use the document after the rights expire. Additionally, time-based rights protection can be set so that documents are automatically deleted after the rights expire. For example, a manager could withdraw an email sent to a subordinate, leaving the subordinate with no evidence as to what they were instructed to do.

How is DRM Enabled and Deployed?

Enabling DRM in an agency requires the explicit deployment of a rights management server running Windows Rights Management Services for Microsoft (MS) Windows Server 2003 (or later) and the purchase of client licences to access the supporting infrastructure. DRM is an optional component of Windows Server 2003 (or later).

DRM is an optional function of MS Office 2003 (or later) software and can be applied in MS Office applications including Outlook, Word, Excel and PowerPoint. However, agencies can deploy MS Office 2003 (or later) without enabling DRM.

Windows SharePoint Services 3.0 also supports DRM on documents stored in document lists and libraries. DRM is an optional component of SharePoint lists and libraries. Care should be taken when implementing SharePoint Server 3.0 that deployment of DRM facilities does not occur other than by intent.

How Does DRM Work?

DRM is established on an agency's policy server as a set of 'rules' that allow information creators/providers to restrict access/use permissions to the information they create, for example *allow this memo to be edited by members of my workgroup during the next 3 days, but do not allow the memo to be shared outside of this group. At the end of 3 days, automatically delete of all copies*. When information creators/providers create documents requiring DRM, the rules from the policy server are applied. The selected rules applied to the digital information are unalterably bound to the document. When other users attempt to access that information, the client software contacts the policy server to verify those individuals' access/use rights to the information.

DRM and Recordkeeping

ISO 15489 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*. DRM means that an organisation or person cannot guarantee they will be able to maintain as evidence information received from another organisation or person. While it has always been the case that the copyright in a received document resides with the creator/provider of the document, not the receiver, there has always been an implicit right of use by the receiver to use the received document as part of the record of their business. With DRM, all rights must be made explicit, and this is not compatible with the implicit right of use of the document as a record.

Regulatory and Legislative Implications

Agencies intending to implement DRM technology will need to determine whether the application of DRM technology compromises their compliance with legislation for the retention, access and use of information. DRM technology has the potential to:

- impede the capture and management of official records in accordance with the *State Records Act 1997*
- hamper the preservation of digital information eg migrating to a different platform or application, or converting and transferring digital records to State Records, in accordance with the *State Records Act 1997* by preventing access to the files
- allow illegal disposal of official records contravening the State Records Act by setting time based rights so that documents are automatically deleted after the rights expire
- prevent access to information by others when they are entitled to it, in accordance with the *State Records Act 1997, Freedom of Information Act 1991, Information Privacy Principles* and other agency specific and government legislation
- compromise an agency's ability to meet the requirements of the *Electronic Transactions Act 2000,* by setting rules for electronic information that limit its retention or use, and
- result in breaches of obligations to provide access to and produce documentation to external monitoring or investigative authorities such as the Police, Auditor-General, Commissions of Inquiry, Courts, etc.

Records Management Practice Implications

DRM poses potential risks to good recordkeeping, including:

- auto-deletion which inhibits the ability of an agency to capture and maintain official records of its business
- print disabling thereby preventing agencies maintaining records in paper format
- forward disabling of email messages may inhibit their capture thereby preventing agencies capturing records of business
- expiration of documents set by creators/providers may conflict with authorised retention periods
- encryption keys may be lost, resulting in effective loss of the records, and
- DRM policies on external documents may not grant sufficient rights for the government to conduct its business using the documents.

The implementation of DRM technology may also impact on agencies' information systems, such as EDRMS to:

- register and retrieve digital documents, including email
- render documents to other formats, and
- cut and paste areas of text from documents for reuse.

In most cases State Government agencies can achieve appropriate rights access using a compliant EDRMS product from the Across-Government EDRMS Supply Panel. These products meet identified government requirements for access and security, to prevent unauthorised or improper use of information. For the same reasons, it is recommended that Local Government authorities also use an EDRMS Panel product.

Business Implications

DRM technology can prevent access to information that is already within an agency's systems, thereby obstructing an agency's ability to do business and keep adequate records. Inappropriate or outdated DRM rules may make the documents inaccessible when required and the hardware and software dependencies of DRM systems may make it difficult to ensure long-term access to the records.

In addition many, if not all, DRM systems depend on communicating with an external rights server before granting access to a document. The system can be designed so that it communicates with an external rights server every time a protected document is accessed. This means:

- access to documents may be reliant on successful communication with an external party, and hence could be constrained even if the government has rights to access the documents. This could lead to agencies relying on information for their decision-making that they cannot later refer to, and
- there is a potential risk that agency information security could be compromised, as this communication would have to open its firewall/s to permit the system to send this information.

Therefore, agencies need to know when DRM is applied, so that they can either refuse to accept the information on those terms, or can take appropriate measures to manage the risk.

Implementing and Applying DRM in Agencies

State Records recommends that agencies should only implement DRM if there is a clearly identified business reason for doing so (for instance receipt of tenders). In most cases agencies can achieve appropriate rights access using an EDRMS Supply Panel product.

If the agency has identified a potential business reason for applying DRM, the agency should:

- undertake an analysis across the agency to identify where the information resource is being created, stored, accessed and used, and
- assess the appropriateness of applying rights protection to the information resource using the *Principles for Agency Use of DRM Technology*[2], outlined below.

Principles for Agency Use of DRM

The aim of the following four principles is to ensure the use of DRM does not adversely affect the integrity, availability and confidentiality of government held information or related government systems and as a result conflicts with the requirements of the State Records Act. It is recommended that agencies intending to implement DRM use the principles as a guide when assessing the appropriateness of applying rights protection to digital information and records identified in their agencies.

Principle 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, and provide access to its information by others, when they are entitled to access it.

Principle 2

Government use of DRM technology must not compromise user privileges accorded to individuals who use government systems (internal or external), or the privacy of individuals of whom the government holds information.

Principle 3

The use of DRM technology must not endanger the integrity of government held information, or the privacy of personal information, by permitting information to enter or leave government systems, or be amended while within them, without prior government awareness and explicit consent.

Principle 4

The security of government systems and information must not be undermined by the use of DRM technology.

Meeting the Principles

The following questions are provided to assist agencies in meeting the Principles outlined above for identified information resource/s.

1. Is there a clearly identified business reason for applying DRM to the information?
    - Information, which is relied upon for government business, eg for decision-making, policy setting, or which provides the basis for citizen rights, should not be subject to external rights management.
    - Information that is being retained as official records under the State Records Act for business/accountability purposes in accordance with legislative or regulatory requirements should not be rights protected using DRM.

- Where information is subject to external rights management, agencies should create a non-rights protected record of the information. To do this agencies may require information creators/providers to either:
  - remove rights protections from documents
  - provide appropriate copies for access to enable their capture and use within agency information systems, such as EDRMS, or
  - to re-send the information using an alternative format or communication method.

2. What is the maximum length of time rights protection is to be applied to the information/records?
   - Rights protection should be set for a limited time only.
     - For temporary information/records, rights protection should not exceed the retention period set by an appropriate disposal schedule. It should be noted that this does not mean the restrictions cannot be removed earlier.
     - For permanent records rights protection is to be removed at or before the date of transfer of the records to the archives.
3. What is the full range of potential usage requirements?
   - Agencies need to ensure that adequate provision is made for the use of any information, at present and in the future, by all parties with rights to use that information.
   - When considering what ‘future’ encompasses, the agency should consider issues such as usage expiry mechanisms, provision for data migration, etc to ensure:
     - future access to information is not inadvertently lost as a result of DRM restrictions on the use of the hardware or software normally used to access the information, and
     - future requirements for migration (both of the information and its associated audit trail/s) to different platforms, data formats or software products are considered at the outset if implementing DRM.
4. When making use of DRM for communications, do intended recipients have reasonable access to the technology required to permit use of the information?
   - When exchanging information, both the creator/producer and the recipient should mutually agree on the application of DRM to the information.
5. What are the potential access requirements of other government agencies and citizens for the information?
   - There are requirements that apply to all government agencies, such as:
     - future availability for archiving with State Records of South Australia
     - access by the Auditor-General, and
     - meeting the requirements of the Freedom of Information Act, Evidence Act and the Electronic Transactions Act.

   Agencies need to design access rights that support the above access requirements.
6. Does the agency have the ability to identify harmful communications where the information is encumbered with externally imposed rights protection?
   - DRM’s use of encrypted traffic challenges the effectiveness of conventional, perimeter-based scanning of incoming data. Agencies need to consider whether they have adequate means of protection before applying rights protection, or accepting information with usage restrictions.
   - Agencies should reject the use of DRM technology, and information, encumbered with externally imposed rights protection, unless they are able to ensure that the communications and information are free of harmful content, such as worms and viruses.

Governance

State and Local Government agencies intending to implement DRM technology should establish a governance framework for the application and use of DRM technology in their agency. Governance of DRM needs to address:

- incorporating DRM in the agency's information management strategy and/or policy framework
  - how DRM fits within existing information and records management strategies
  - under what conditions/circumstances DRM may be used
- appropriate rights access being achieved using an EDRMS Supply Panel product
- who (staff positions) is responsible for establishing and administering digital rights. Positions responsible for administering or managing rights-protected documents have responsibility to ensure:
  - DRM policies are set, applied and managed centrally
  - DRM policies do not exceed retention periods
  - rights protected documents are accessible in any system exit processes
- how staff are to deal with rights protected information and
- establishment of screening processes to detect DRM protection on records from outside the agency.

Government CEs are responsible for the management, confidentiality and provision of access of agency information and will need to endorse the application and management of DRM in the agency. All staff should be made aware of the policies and procedures for the use of DRM through normal agency communication and training channels.

Additionally, agencies need to discuss the application of DRM technology with their information and records management and ICT staff, as well as their information systems software supplier/s to ensure that software will continue to function in effectively in a DRM environment.

State Records Policy and DRM

State Records considers DRM is not compatible with the State Records Act requirements of preserving and providing long-term access to archival records. It has been long standing policy that State Records will not accept the transfer of digital archival records for long term preservation that are protected using encryption or encryption based technologies eg DRM technology. To assist agencies further, State Records intends to establish a Digital Rights Management Standard and Guideline at a later date under the Keeping Electronic Information Strategy (KEIS) Governance Framework.

State Records, as part of the Council of Australasian Archives and Records Authorities (CAARA) is also working with ICT vendors like Microsoft Corporation and Adobe to establish a common set of requirements at a national and international level that meet the records management needs of government. CAARA is keen to ensure that access and disposal provisions of the various archives and records' legislation in our different jurisdictions are not unwittingly undermined by the application of DRM technology.

Further Information

For further information about DRM technology and DRM and recordkeeping:

Microsoft Corporation, *Enabling Information Protection in Microsoft Office 2003 with Rights Management Services and Information Rights Management – Technical – White Paper*. December 2003

Microsoft Corporation, *Information Rights Management in Microsoft Office 2003: Summary Technical White Paper*. April 2003

Microsoft Corporation, *Information Rights Management in the 2007 Microsoft Office System*. (accessed June 2007)

Microsoft Corporation, *Information Rights Management in Windows SharePoint Services Overview*. (accessed June 2007)

Microsoft Corporation, *Windows Rights Management Services Information*. (accessed June 2007)

New Zealand State Services Commission, *Trusted Computing and Digital Rights Management Principles & Policies*. September 2006

Shinder, Deb, Boost Office 2007 security with Information Rights Management, the Document Inspector, and the Trust Center. Techrepublic – White Paper. April 2007

Shinder, Deb, Safeguard Your Office 2007 Files with Encryption, Document Protection and Digital Signatures – Techrepublic – White Paper. April 2007

State Records NSW– Recordkeeping in Brief, (*RIB) 36 Information Rights Management and Recordkeeping*. (accessed June 2007)

US National Archives and Records Administration, NARA Bulletin 2007-02. archives.gov/records-mgmt/bulletins/2007/2007-02.html. April 30, 2007

[1] Digital Rights Management is also known as Information Rights Management, Document Rights Management, Rights Services Management or Enterprise Rights Management

[2] The New Zealand Government developed these Principles in 2006 for the use of *Trusted Computing and Digital Rights Management* within governments. The Principles cover the full spectrum of DRM issues relevant to government-held information, including privacy, accessibility, intellectual property and information security. The Principles and policies are available at www.e.govt.nz/policy/tc-and-drm/principles-policies-06/.