STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

Trusted Computing and Digital Rights Management Standards and Guidelines

e-government
www.e.govt.nz

DEVELOPMENT GOALS

State Services Commission
July 2007
Version 1.0
ISBN 978-0-478-30315-5

Trusted Computing and Digital Rights Management Standards and Guidelines

Preface to TC/DRM Standards and Guidelines

The New Zealand Government Trusted Computing and Digital Rights Management (TC/DRM) Standards and Guidelines are a supplement to the TC/DRM Principles and Policies, published in 2006. The Principles and Policies seek to ensure that the use of trusted computing and digital rights management technologies do not adversely affect the integrity (including availability and confidentiality) of government-held information.

The Standards and Guidelines aim to:

- assist government agencies with the work of developing operational practice, appropriate for their own business drivers and statutory responsibilities, in response to the framework provided by the Principles and Policies
- to provide vendors with guidance on what governments need from TC/DRM products, in order to be able to comply with the TC/DRM Principles and Policies.

The Standards and Guidelines were developed in 2006/07, by a working group of public and private sector officials.

Agencies must ensure that these Standards and Guidelines are integrated with their existing internal policies and standards, so that they are referred to at the applicable times in each agency's business activities. To assist in this integration work, this document groups the Standards and Guidelines based on the activity each one relates to. Two of the groupings deal with government as a *recipient* of information potentially encumbered with DRM.

The third grouping - 'Applying DRM' - deals with government as a *generator* of information potentially encumbered with DRM.

The fourth grouping deals with the end-to-end process that can lead to TC/DRM functionality being implemented in a government agency, beginning with planning and ending with deployment. The aim of these Standards and Guidelines is to ensure that agencies have adequate awareness of the potential TC/DRM Policy implications of decisions at each stage of the process, and take appropriate measures to comply.

The final grouping, 'Vendor Guidelines' is directed to vendors rather than agencies. It is intended to assist vendors in understanding the requirements of government and the issues raised by TC/DRM, and how these issues might be addressed by vendors. The term 'vendor' should be interpreted in the loosest sense, as being any provider of ICT technology (hardware, software, etc) or information product. The term should, therefore, be interpreted to include providers of free products, such as open source software.

Table of Contents

1 Receiving information

This section provides standards and guidelines for use when agencies are receiving digital information. Any information an agency receives could come with TC/DRM encumbrances, or packaged with TC/DRM software (e.g. DRM-protected music CDs). Receipt of such information generates risks for the integrity of government information. Therefore this section is oriented around detection, and applies to *all* situations where government receives digital information.

1.1 Detecting TC/DRM encumbrances and functionality

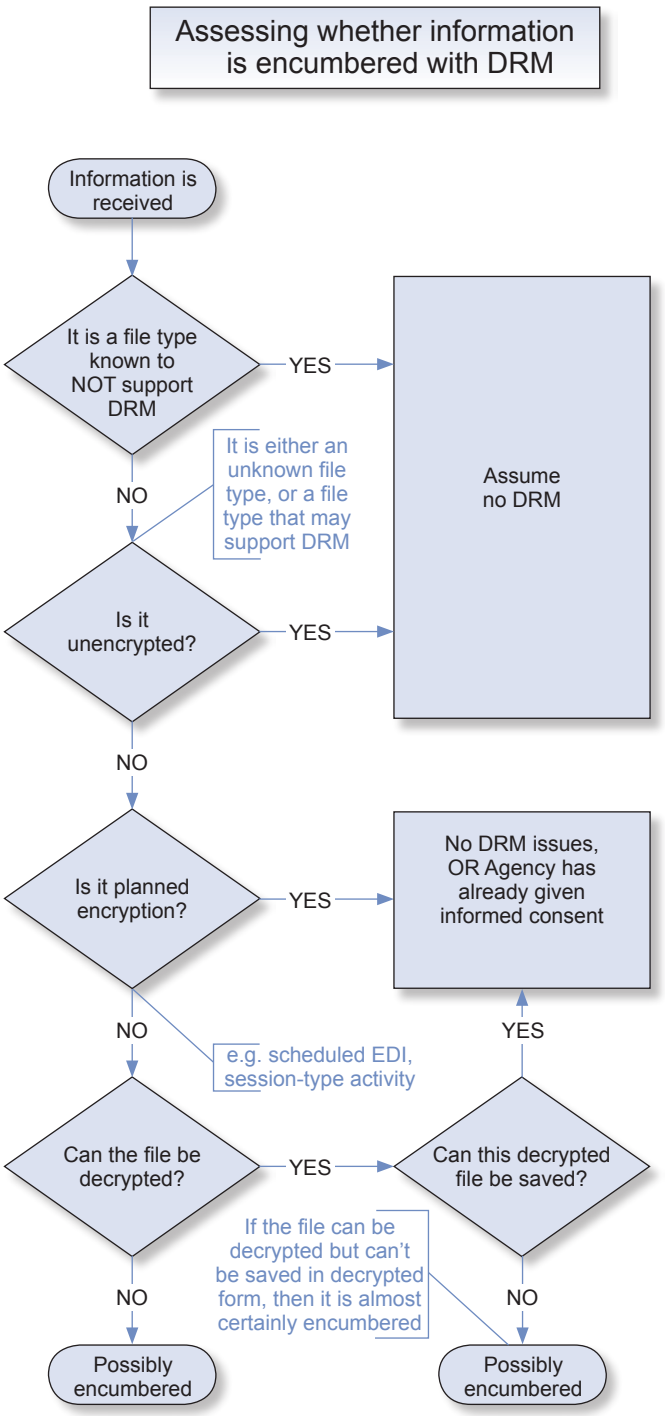
Guideline
Detecting DRM encumbrances

In order to comply with *Policy 1, Informed consent to externally-imposed digital encumbrance,* agencies will need to be able to detect the presence of DRM encumbrances when receiving information.

It is likely that DRM encumbered information will be encrypted. Any DRM system that doesn't encrypt encumbered information would be easy to circumvent.

File readers and content filters can read the vast majority of file types, so if such readers or filters cannot read a file, the file is probably encrypted. If information is encrypted, then it could be because of a DRM encumbrance. If a program can read encrypted information but can't save it in unencrypted form, then it is almost certainly encumbered.

Agencies can use the following decision logic to assess whether information is encumbered with DRM:



Some DRM systems could store encumbrance details in a non-encrypted Rights Expression Language (REL) wrapper[1], for which there are published standards such as ISO/REL and ODRL. An agency can use the information in an REL wrapper both as a confirmation of the presence of an encumbrance, and also to obtain the actual details of the encumbrance.

Standard
Requirement for contractual declaration of DRM features

When information is supplied to a government agency under a commercial arrangement, there must be a legally enforceable document signed by the vendor stipulating all and any DRM features on the information being passed. If information is stated to be unencumbered, this should be checked by the agency and if found to be encumbered, it should be treated as a breach of contract and penalties enacted.

Rationale

It will not always be easy for an agency to check for the presence of DRM encumbrances, as there is no universal technical standard for confirming their presence or absence. Thus the onus should be on vendors of such information to advise its nature.

This standard supports *Policy 1, Informed consent to externally-imposed digital encumbrance.*

[1] An REL wrapper is a data structure that 'wraps' around other data in the file, and expresses the digital rights and restrictions associated with that data.

2 Accepting DRM-encumbered information

This section provides standards and guidelines for use in deciding whether to accept DRM-encumbered information. There are situations where this can be acceptable, and others where it is not. When the standards and guidelines allow for acceptance, and the agency chooses to do so, this section prescribes actions to mitigate risk to the integrity of government information.

2.1 Restrictions on senders/suppliers

Standard
Limitations on sending encumbered information to government

All information supplied to a government agency under statutory obligation, must be free of DRM encumbrances. Except by prior agreement, all other information sent to the government (whether solicited or unsolicited) must be free of digital encumbrance. Government agencies are not obliged to accept DRM encumbrances on any communications to them, except where they have bound themselves by contract to do so.

Rationale

Government agencies may not be able to keep adequate records if communications sent to them carry DRM encumbrances. DRM encumbrances introduce risk to government's ability to adequately access and use the information as provided for by statute.

This standard supports *Policy 1, Informed consent to externally-imposed digital encumbrance.*

2.2 Deciding whether to accept

Standard
Requirement to prove inability to revoke DRM rights

When agencies receive encumbered information required for execution of public business, the inability to revoke government access must be proven before accepting the information.

Rationale

Some DRM systems require contact with a rights management system in order to check the current rights settings for encumbered information. In such cases, the rights settings could be altered unilaterally by the vendor subsequent to the government accepting the information, resulting in degradation or total loss of access.

This standard supports *Policy 2, Conditions for externally-imposed digital encumbrance.*

Guideline
Proving inability to revoke DRM rights

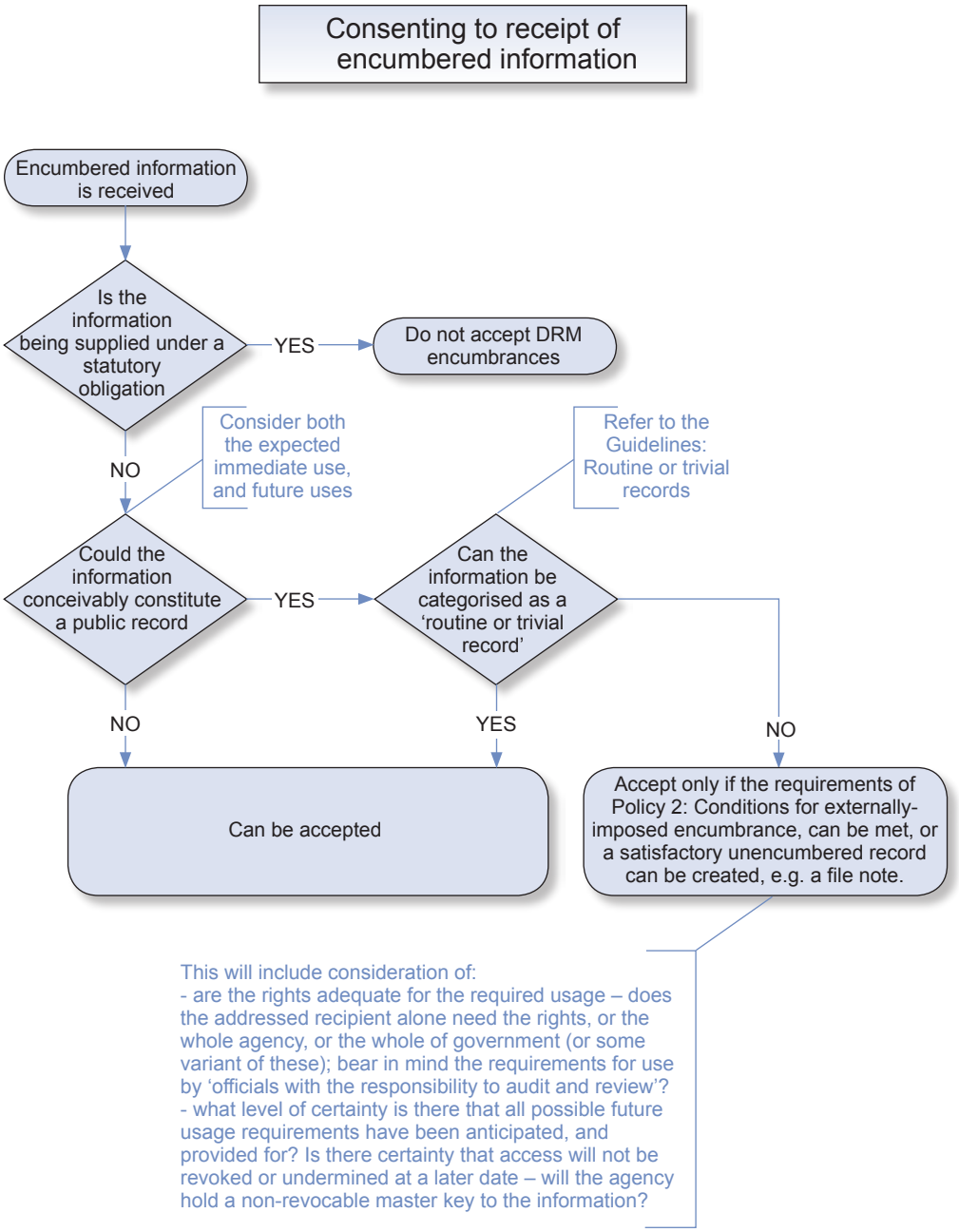
When agencies receive encumbered information required for execution of public business, the inability (either in perpetuity or for an agreed period of use) to revoke government access must be proven. One way of doing this is by placing a copy in a protected location that is never accessible to the vendor's systems, and confirming that the information can still be used while in this location. To prevent misleading results due to network mechanisms such as caching, this location should have no prior knowledge of current network users, and no synchronisation with the internet or systems connected to the internet, i.e. it should be a 'quarantined' machine.

Guideline
Testing for future expiry of DRM rights

Some DRM systems enable usage rights to be limited to a certain time period. Depending on the mechanism used, agencies may be able to test for this by advancing the operating system date to see whether access to the information is lost. However, agencies should note that date detection may not necessarily rely on the operating system date – it may use the system hardware clock, which is not alterable by the user, or refer to an external time source.

Guideline
Deciding whether to grant consent

Factors to consider when deciding whether to consent to receipt of information with DRM encumbrances, are shown in the following diagram:



It is difficult to fully predict the future effects when either applying DRM or accepting DRM-protected information. Such actions should not even be considered unless there are compelling reasons to do so, and the effects of the usage have been stringently considered.

Guideline
Definition of routine or trivial records

Policy 1, Informed consent to externally-imposed digital encumbrance, notes categories of information for which it is possible that an external encumbrance may not compromise the public record. The Chief Archivist has authorised several classes of routine or trivial records for destruction as soon as they are no longer administratively required.

Archives New Zealand's General Disposal Authority GDA/3 (http://www.archives.govt.nz/continuum/documents/publications/gda3) lists these classes as follows:

- Personal correspondence - correspondence with family or friends, doctor's appointments, light-hearted banter, lunch dates, etc.
- Received for information only - circulated material not meant to result in action from the recipient such as bulletins, newsletters, internal circulars, etc.
- Trivial work related material - routine housekeeping information, meeting notices and arrangements, contact details, reminder notes, copies of minutes, circulated notices, staff movements, copies of publications, room bookings, etc.
- Incomplete material - messages or memos never completed or shown to anyone else, never sent for comment, approval or to file, seen by no-one except the creator.
- Externally sourced material from a bulletin board or listserv - material not directly addressed to the recipient or their agency, includes information downloaded from libraries, databases, or received due to membership in a discussion group or listserv, etc.
- Received advertising material - advertising flyers, brochures, catalogues, pricelists.

2.3 Actions to take if accepting

Standard
Record the basis for acceptance of encumbrance

If encumbered information is accepted, the basis for accepting it must be formally recorded.

Rationale

Recording the basis for acceptance enables the agency to account for its decision, and demonstrate that risk factors have been adequately considered.

This standard supports *Policy 2, Conditions for externally-imposed digital encumbrance.*

Guideline
Boilerplate contract text to ensure full control of government-owned information

It is expected that in normal cases, information created for government ownership will be unencumbered with DRM restrictions. Occasionally, it is possible that a government agency will ask for or allow information to be encumbered (perhaps for security reasons), in which case the encumbrance must be under the full and exclusive control of the agency (and not of the creator).

The State Services Commission has developed boilerplate contract text to assert this requirement. The text is included as an appendix to this document *(Appendix 1, Control of Government Owned Information - Suggested Boilerplate Clauses)*.

3 Applying DRM

This section provides standards and guidelines for use when a government agency wishes to apply DRM encumbrances to information. It addresses the risks that the encumbrance may result in recipient needs not being met, that DRM could be used for a purpose for which it is inadequate or inappropriate, and that the encumbrance could jeopardise government's future ability to use the information.

3.1 Meeting recipient needs

Standard
Support informed consent of DRM recipients

Government agencies applying DRM encumbrances to information for supply to another party, whether government or non-government, must provide notification to the recipient of the presence of the encumbrance, and the details of the encumbrance,

If notification is provided through use of a Rights Expression Language (REL) wrapper, the REL must be a published standard, e.g. ISO/REL, ODRL.

Rationale

Government agencies must model the behaviour they require from others, in terms of declaring the presence of DRM encumbrances.

This standard supports *Policy 1, Informed consent to externally-imposed digital encumbrance.*

Guideline
Recording the link between encumbered copies and the record version

Agencies sending encumbered information to other parties should keep a record of what was provided and the nature of the encumbrance. Agencies should keep a record of the correlation between the sent version and their unencumbered record copy.

Guideline
Requirement to provide future support for use of encumbered copies

Circumstances may arise where an agency has provided an encumbered copy of information to another party. Agencies should make provision to support use of encumbered information for as long as the terms and conditions of access allow. If there are no explicit terms and conditions of access, the access should be supported for as long as the agency retains the unencumbered original. Supporting use of encumbered information will, for example, entail maintaining the servers and certificates required to allow access.

3.2 Is DRM appropriate for purpose?

Guideline
Is DRM appropriate for SIGS[2]

DRM may not be an appropriate mechanism to apply SIGS protections (e.g. 'sensitive', 'confidential'). Agencies should check with the Government Communications Security Bureau as to whether particular DRM solutions are appropriate for a particular kind of use.

3.3 Providing for future access requirements

Guideline
Avoiding potential vendor lock-in

TC/DRM encumbrances could hamper the implementation of digital preservation strategies if they limit permissible management activities for information (e.g. reformatting), and they introduce additional complexity that needs to be managed over time.

Agencies accepting or creating TC/DRM-protected information should:

- as far as possible, identify future digital preservation requirements, such as migration from data formats that are becoming obsolete
- determine whether the TC/DRM technology will support these requirements
- determine whether this locks the agency into a specific vendor's proprietary solution.

Standard
Ensuring minimum government access requirements are met

Agencies applying digital restrictions to information must ensure that their record copy of the information is unencumbered.

Rationale

Keeping an unencumbered original copy of information as the record copy avoids any risk of TC/DRM-related access problems for other agencies with a requirement (possibly unanticipated) to access the information. It obviates the need for an independent agency to be able to take full control of the access rights, as prescribed in *Policy 8, Independent usage capability.*

Archives New Zealand will sometimes need to migrate information to a new file format for digital preservation purposes, due to impending obsolescence of the existing format. Having an unencumbered record copy will support this requirement.

This standard supports *Policy 7, Common privilege definitions, and Policy 8, Independent usage capability.*

[2] SIGS – Security in Government Sector, a manual setting out security requirements for government agencies, see http://www.security.govt.nz/

4 Planning, procuring, configuring and deploying systems

This section provides standards and guidelines for use by government agencies in ICT planning, and systems procurement, configuration and deployment. They aim to ensure that TC/DRM implications are considered throughout the system's lifecycle.

These considerations apply even at the enterprise/technical architecture level. Use of TC/DRM technologies could form part of an agency's ICT strategy, e.g. trusted computing forms the basis for some network access control solutions. TC/DRM technologies could come bundled as part of a product that forms a fundamental part of an agency's technical platform, e.g. embedded in desktop computer and mobile phone hardware and operating systems. It is important these implications are thought through in advance, so that an agency's ICT planning positions it for compliance with the government's TC/DRM Principles and Policies.

There are steps that can be taken during the procurement process to ensure adequate disclosure of TC/DRM functionality, to ensure that the product being purchased will be compliant with the TC/DRM Policies and Principles.

In some cases, a product's compliance with the TC/DRM Principles and Policies will hinge upon how it is configured, what it is used for and how it is used. This section provides some measures to address this aspect.

4.1 Support for informed consent

Standard
Software must support user awareness of DRM encumbrances

Software that enforces DRM encumbrances must either:

- have a notification mechanism, to tell the user each time an encumbered file is opened that restrictions apply, and allow viewing of the restrictions if desired, or
- in the case of software where most or all of the information handled by the software is encumbered in a standard manner, an acceptable alternative to 'per use' notification is for agencies to ensure that users know that all such information should be regarded as encumbered.

Rationale

Notification of an encumbrance on each usage will enable users to know whether they need to make separate notes, in order to maintain an appropriate record.

This standard supports *Policy 2, Conditions for externally-imposed digital encumbrance*.

4.2 Ensuring continued access to information

Standard
Attestation criteria must remain stable

For government systems that use hardware or software attestation, agencies must ensure that the attestation criteria cannot be changed without the agency's prior approval.

Rationale

Unapproved changes to attestation criteria could result in an agency losing access to its information.

This standard supports *Policy 5, Assurance of future accessibility.*

Standard
Requirement for access to information independent of attestation

Government systems that use hardware or software attestation, must either have a means to bypass it, or must keep a backup of the system's information in an open data format in unencumbered form in a suitably secure data store.

Rationale

These provisions mitigate the risk of a failure in the attestation mechanism resulting in loss of access to government information. The data backup provision ensures there is no dependence on proprietary hardware or software, or decryption.

This standard supports *Policy 5, Assurance of future accessibility.*

4.3 Ensuring effective security

Standard
Ensuring effectiveness of defences

Before implementing TC/DRM features, an agency must ensure that its security systems (including anti-virus, firewalls, intrusion prevention and detection systems) remain effective for information imported using the TC/DRM services/channels, or if not, that such information is processed only in an isolated environment.

Rationale

Agencies may receive information that is encrypted in order to enforce externally imposed digital restrictions, and consequently be unable to check for harmful content. There is a risk that such information may be accepted with harmful content.

There will always be a risk of DRM-protected information being a vector for viruses, and no way for anti-malware software to check it, unless there is some far-reaching cooperation between software vendors and anti-malware developers.

This standard supports *Policy 13, Ability to identify harmful communications.*

Guideline
Seek vendor assurance against unauthorised information modification/deletion

Agencies may wish to safeguard their ability to comply with *Policy 9, Modification/deletion by hardware/software*, by seeking an assurance from ICT product vendors. This will need to be built into an agency's procurement process. Clearly the agency will have power to obtain a stronger assurance when purchasing a bespoke system, than when it purchases a commodity product. In the case of a bespoke system, the agency could require provision of a warranty as part of the contract. In the case of a commodity product, it may be not be possible to get any sort of direct assurance from the vendor, and may instead be necessary to rely on market intelligence, including information sharing with other governments and New Zealand government agencies.

Guideline
Use unencrypted mode when running remote attestation

When using remote attestation, agencies should always run the attestation communications in unencrypted form (if able to do so), so that the traffic can be inspected. If this is not possible, then agencies should ensure that they have some other way of mitigating the risks resulting from not being able to inspect system-initiated communications leaving or entering their systems.

4.4 Ensuring compliance of new systems with policies

Guideline
Issues to consider in the IT procurement process

Procurement processes need to have checks to identify what TC/DRM functionality is included in the vendor products. The functions should be assessed against the requirements of the TC/DRM Policies and Standards.

Agencies should ensure that any TC/DRM solution proposed for procurement has a communications specification that meets the requirements of *Policy 12,Communications specifications.*

Guideline
Seek RFP disclosure of inclusion of TC/DRM functionality

Agencies are required by *Policy 10, Awareness of TC/DRM functionality*, to ensure that they are aware of the inclusion of TC/DRM functionality when deploying hardware or software, or using externally-provided information.

One measure that can be taken is to seek a declaration by vendors in RFP responses that propose IT products. The RFP should seek a declaration from the vendor as follows:

- Which of the proposed products include TC/DRM features, as defined by the TC/DRM Principles and Policies.
- Which features are activated by default, and which are present but de-activated.
- What functions, if any, rely on the TC/DRM features and will become unavailable when the TC/DRM features are disabled.

Alternately, the vendor can declare that TC/DRM functionality is absent.

An example of 'present but de-activated' is the Trusted Platform Module (TPM) which now ships in most new PCs and laptops, but is turned off by default, and requires user initiative to activate.

Of particular interest is the inclusion of functionality using:

- remote attestation
- system-controlled encryption of information (rather than user-controlled)
- date and duration-based restrictions (for instance, where software or information is only going to be accessible for three months from activation, or until 1 January 2008, or opened 20 times)
- information that installs its own reader or modifies the platform it runs on.

Guideline
Managing risks to privacy of personal information

Agencies are required by *Policy 11, Knowledge of information flows*, to be sufficiently aware of information flows into or out from their TC/DRM systems, to ensure that their systems don't contribute to a breach of the Privacy Act. TC/DRM systems may involve transmission of encrypted information, or communications with third party systems, and this may result in a privacy risk profile that differs from most of an agency's other applications. Suppliers of DRM-protected content in particular are likely to have an interest in who is using the information supplied and how they are using it.

The third party communications risk is as follows:

- Information viewing software may 'phone home' (i.e. contact the software vendor's server) and transmit personal information (e.g. name of the user, name of the file they're reading) without the agency's full knowledge and acceptance.
- Alternately, the agency may be aware of it, but the individual user may not be informed.
- Alternately, all relevant parties may be informed, but a third party receiving the information may not comply with the Privacy Act, nor be subject to its provisions unless explicitly contracted to be so.

Agencies can avoid these risks by using software known or warranted to not collect personal information. If collection of personal data is to occur, then ensure that it is consistent with the requirements of the Act, and that there is legal protection against non-compliance by a third party. Users need to be advised in advance of what information would be collected, why, and how it will be managed, etc (as per the Privacy Act).

Guideline
Recognising policy implications of deploying software to browse DRM-encumbered information

Use of TC/DRM could require communications, e.g. to check rights against the information provider's rights management server, or to attest that the viewing software is uncompromised. *Policy 12, Communications specifications* requires that agencies will only operate TC/DRM solutions when they are fully cognisant of the content of any communications, and the events or conditions that trigger them. Agencies should note that software which enables a DRM-protected file to be accessed, constitutes a TC/DRM solution, and so is subject to *Policy 12, Communications specifications*. Agencies should take measures to reduce the risk that staff will install such software without regard for the consequences, in order to get access to the information they wish to use.

Guideline
Perform impact assessment when activating trusted computing

Agencies should note that when a TPM (Trusted Platform Module) or other trusted computing equivalent is activated on a computer, there is the potential for it to be used by operating system or application software on the computer to encrypt previous openly accessible information in an attempt to make the platform more secure. This could also have the effect of preventing migration of information to a different application, or preventing usage of the information on a different machine. Agencies should perform an assessment to identify such possibilities and their impact, prior to activating trusted computing on their computers.

Guideline
Ensure system compatibility with TC/DRM Policies

Agencies should not deploy a TC/DRM system until they have satisfied themselves that its characteristics and usage will meet the requirements of the TC/DRM Principles and Policies. If in doubt, advice should be sought from the steward of the policies.

Agencies are encouraged to share information about TC/DRM products with each other, and make use of any information-sharing facilities provided by the steward.

Guideline
Preventing unwanted auto-installs of TC/DRM software

There have already been examples of TC/DRM software being bundled with encumbered information, and auto-installing when the recipient attempts to access the information, e.g. some Sony-BMG music CDs. The installation could be performed without the user's knowledge. Agencies can reduce the likelihood of auto-install by locking down desktop and browser environments.

Guideline
Avoid deploying software in auto-update mode

Software products, especially those that already have TC/DRM features, should not be run in auto-update mode which could change their functionality, unless the agency can first assess how that change in functionality could affect government requirements.

4.5 Configurability

Guideline
Minimise needless exposure to unexpected TC/DRM side-effects

As TC/DRM security features become freely available, e.g. as standard hardware components, or as operating system or application system features, agencies should turn off such features by default. They should only be used in situations when the agency has identified a specific purpose for them, and their unique strengths are better than alternatives. Otherwise their effects could be largely transparent until something goes wrong, or until the agency finds itself unable to make a change to software or to migrate data, as a consequence of passively allowing the TC/DRM features to operate.

4.6 Appropriate use

Guideline
Don’t deploy TC/DRM solely for email security

Agencies should avoid deploying DRM-based systems solely as a means of securing emails. Other systems can be used to achieve this goal (e.g. GSN or SEEMail for agency-to-agency communications), without the risks to accessibility of government information that DRM introduces.

5 Vendor Guidelines

This section is intended to assist vendors in understanding the requirements of government and the issues raised by TC/DRM, and how these issues might be addressed by vendors. The term 'vendor' should be interpreted in the loosest sense, as being any provider of ICT technology (hardware, software etc) or information product. The term should, therefore, be interpreted to include providers of free products, such as open source software.

The requirements can be summarised as followed:

- Real-time notification of the presence, nature (static or dynamic) and details of encumbrances.
- Provision for long-term access to government information.
- Support for anti-malware scanning of information and communications (or provide/suggest alternative means of protection).
- Configurability of TC/DRM features, for instance for notifications, communications, attestation and trust, and the ability to have them turned off by default (or at least provide the choice during installation).
- Pre-purchase notification of TC/DRM functionality and communications needs.
- Independent verification of the TC/DRM specifications and features.

5.1 Notification of encumbrance

Use rights expression wrappers

Software that applies DRM encumbrances should use rights expression wrappers to declare the encumbrance. The wrappers should not be encrypted, and should conform to a published REL (Rights Expression Language) standard, e.g. ISO/REL, ODRL.

The rights statement should be stable and not subject to unilateral external change – any change needs to include the informed consent of the recipient.

The rights statement should disclose the fact that the information is protected, and who has what access rights (e.g. can't copy, can print).

Consuming applications should be certified as correctly interpreting the REL.

Use of rights expression wrappers will assist agencies in determining whether encrypted information is subject to a DRM encumbrance, and knowing the details of any such encumbrance.

Confirm non-revocation of access

Vendors should provide solutions for agencies to satisfy themselves that no access expiry exists on encumbered information, and that rights are non-revocable.

Software support for informed consent process

Where digital rights have been applied externally, agencies will need software support to:

- consistently identify files that have digital rights attached
- view the rights and enable a consent/reject decision process
- inform users on each use of the information, that usage restrictions are attached, and enable easy viewing if required
- ensure that rights remain fixed except by mutual consent of the agency and rights-holder.

The notification mechanism that informs users of attached rights should be controlled by the organisation, not by the vendor or the user. There should be a choice between passive notification, e.g. through appearance of a clickable icon, and active notification, such as a modal dialogue. The degree of passive or active notification should be configurable based on the source of the information. There should be an option to whitelist particular sources, e.g. information produced within the organisation.

5.2 Long term access to government information

Support for digital preservation

It is important not to overlook the needs of government for longer-term usage of its information. Software vendors are encouraged to support these needs in their products by:

- protecting against premature expiry of usage rights
- enabling migration of TC/DRM-protected information from data formats that are becoming obsolete.

Support time-based expiry of restrictions

Information providers may wish to apply usage restrictions in the short term, but without having a requirement for the restrictions to remain in force beyond a certain point. After that point, they become a needless hindrance to the recipient. Products that enable time-based expiry of restrictions would make TC/DRM use acceptable in a wider range of contexts.

5.3 Anti-malware scanning

Support scanning of information and communications

Suppliers of products that apply TC/DRM restrictions to the use of information, can assist agencies by providing a means for an agency to:

- inspect the information, using its normal scanning tools, e.g. anti-virus software
- inspect any TC/DRM communications required to use it.

5.4 Configurability

Support granular control of remote attestation

Trusted computing platforms should enable granular control of remote attestation, i.e. the user should be able to enable remote attestation per communications partner and even per communication, not just as a global setting. This will help users to ensure that use of this function is confined to the purposes for which it was enabled, and thus minimise the risk of it being misappropriated for unwanted communications.

Support for enterprise-level control of TC/DRM feature usage

Vendors incorporating TC/DRM as optional features into their products, should:

- generally have them set to 'off' by default
- enable enterprise-level control of the capability.

By providing safeguards against inappropriate usage of the features, vendors will make their products more acceptable to government.

5.5 Pre-purchase notification of functionality and communications needs

Disclosure of TC/DRM functionality

Vendors selling hardware, software or information products should declare whether the product includes TC/DRM functionality, and provide documentation of these functions, options and procedures to remove those controls. Information products, for example, sometimes come bundled with DRM software, and the presence and functionality of such software should be declared.

Declarations of TC/DRM functionality should be kept up-to-date with all subsequent versions of the product, including patches.

Disclosure of TC/DRM communications

Suppliers of any products with TC/DRM features should support agencies in complying with *Policy 12, Communications specifications*, by creating communications specifications for their products.

General product specifications are unlikely to be appropriate, as they will often contain a large volume of irrelevant detail which makes it difficult to find the information agencies actually require. Instead, suppliers should separately document, in business terms, 'the triggers and content of any communications (including attestation and other background communications) that leave from or arrive at the computer'.

Some examples of the types of communications that need to be included in the specification are:

- remote attestation
- communication with a digital rights management server
- activation or heartbeat communications.

For each communication agencies will need to know:

- When: what triggers the communications?
- Who: where/what is the end point of the communications, and who else may it be shared with?
- How: what communications methods and protocols are used? Is it encrypted, signed?
- Are any of the details above configurable (per computer, -user, -application or -use)?

The communications specification should be kept up-to-date with all subsequent versions of the product, including patches.

Industry standard communications specification

Vendors are encouraged to collaborate to create an industry standard for a TC/DRM communications specifications.

Provide warranty against unauthorised information modification/ deletion

Vendors should provide warranties that their products will not make unauthorised modification or hinder access to government information, without explicit government approval (notwithstanding software bugs and other unintended activity). This will support agencies in complying with *Policy 9, Modification/deletion by hardware/software.* Vendors could submit their products to an independent certification programme, for confirmation that their products do not behave in this way.

Provide privacy warranty or disclosure

Vendors should, where applicable, warrant that their products do not collect personal data without explicit user permission. Alternately, they should declare the type of data to be gathered and its intended usage, and provide appropriate legal remedies to the purchaser for any mis-use of the information.

5.6 Independent verification

Establish independent body to verify communications specification

Vendors are encouraged to collaborate to create a certification programme, where an independent body certifies that their products conform to their TC/DRM communications specifications.

6 Appendix 1 - Control of Government Owned Information Suggested Boilerplate Clauses

The following are suggested boilerplate clauses for Government contracts, the purpose of which is to enable Government agencies to retain control of information provided by outside contracting parties. These clauses are intended for use in situations in which the Government will be the owner of the relevant information. They are not intended to apply where a Government agency obtains a licence to use information as opposed to ownership of/copyright in it.

It appears necessary to have two clauses. The first clause (entitled "Exclusive Control of Information") is intended for use in fairly simple contracts where, for example, a Government agency has commissioned a specific piece of work (whether it be written, audio or visual). The second clause (entitled "Ownership and Intellectual Property Rights") amalgamates the substance of the first clause into a broader intellectual property rights clause. This latter kind of clause may be more appropriate for higher value and/or more complex transactions, where potentially wider-ranging intellectual property rights are at stake.

The starting point in both clauses is a contractual prohibition on digital rights restrictions. The second clause allows an exception if permission is specifically given by the contracting Government agency. This ought to ensure that any restrictions imposed on specific items of information are the subject of discrete consideration. It would be the contracting agency's responsibility, when determining whether to permit a given restriction, to consider compliance with TC/DRM policy 3 ('any DRM encumbrance applied to the government's master copy of any information it owns, must be under the government's full and exclusive control').

The appropriateness of either clause will depend on a particular contract's subject-matter and, as is usual with boilerplate clauses, the clauses may need to be modified to accommodate the particular features of the given agreement.

EXCLUSIVE CONTROL OF INFORMATION

1.1 Subject to any specific qualifications in this Agreement to the contrary, all title to and property (including all intellectual property rights) in Information supplied by [Supplier] to [Government agency] under or in connection with this Agreement shall be the property of [Government agency].

1.2 Without limitation to clause 1.1 above, no digital rights restrictions shall be applied to or embedded within that Information. Such restrictions include, without limitation, restrictions on [Government agency's] ability, either on receipt of the Information or at any time in the future, to save, copy, archive, view, print, [listen to], forward or otherwise distribute the Information.

1.3 Any permission under clause 1.2 above shall specify the particular type of permitted restriction and its duration.

1.4 **Information** means [all materials, documentation, data and information, in whatever format and of whatever type of media] [to be completed if necessary by reference to the subject-matter/information under the agreement that the Government agency will own].

OWNERSHIP AND INTELLECTUAL PROPERTY RIGHTS

1.1. Subject to clause 1.7, all title to and property (including all Intellectual Property Rights) in any thing or process supplied by [Supplier], its agents and/or permitted subcontractors under the Agreement(s), including but not limited to software, hardware and Information produced or obtained in any manner whatsoever in performing the [Services] (collectively, "Things and Processes"), shall be the property of [Government agency].

1.2. Ownership of all Things and Processes (including all Intellectual Property Rights that subsist therein) shall vest in [Government agency] at the time when such Things and Processes come into existence. [Government agency] grants [Supplier] a non-exclusive and revocable licence to use all Things and Processes to the extent necessary to enable [Supplier] to perform its obligations under the Agreement(s).

1.3. Without limitation to clause 1.1 above, no digital rights restrictions shall be applied to or embedded within the Information referred to in clause 1.1 unless specifically permitted in advance and in writing by [Government agency]. Such restrictions include, without limitation, restrictions on [Government agency's] ability, either on receipt of the Information or at any time in the future, to save, copy, archive, view, print, [listen to], forward or otherwise distribute the Information. Any permission under this clause 1.3 shall specify the particular type of permitted restriction and its duration

1.4. **Intellectual Property Rights** means all intellectual property rights, title to, and interests (including common law rights and interests) in any jurisdiction including, without limitation:

- patents, trade marks, service marks, copyright, registered designs, trade names, domain names, symbols and logos;
- patent applications and applications to register trade marks, service marks and designs; and
- tools, techniques, computer programme code, specifications, rights in circuit layouts, ideas, concepts, materials, documentation, know-how, data, inventions, discoveries, developments, trade secrets, information and logical sequences (whether or not reduced to writing or other machine or human readable form).

1.5. **Information** means [all materials, documentation, data and information, in whatever format and of whatever type of media [to be completed if necessary by reference to the subject-matter/information under the agreement that the Government agency will own].

1.6. All materials, documentation, data and information (including all Intellectual Property Rights subsisting therein) supplied by [Government agency], or derived from information supplied by [Government agency] shall remain the property of [Government agency]. [Government agency] grants [Supplier] a non-exclusive and revocable licence to use such materials, documentation, data and information to the extent necessary to enable the [Supplier] to perform its obligations under the Agreement(s).

1.7. Nothing in this clause 1 shall operate to transfer the Intellectual Property Rights in any pre-existing software, materials, documentation, data and information of the [Supplier] that become incorporated in any Thing or Process supplied by [Supplier] under the Agreement(s). [Supplier] grants [Government agency] a non-exclusive, perpetual, non-revocable and royalty free licence to use (including but not limited to accessing, reading, copying, modifying, adapting, displaying and sublicensing) all of the Intellectual Property that existed prior to the commencement of the Agreement(s) and that is supplied by [Supplier] in performing its obligations under the Agreement(s). For the purpose of this clause, "pre-existing" means existing prior to the date of the Agreement(s).

1.8. [Supplier] acknowledges that it has obtained all necessary rights and licenses:

(a) to supply any Thing and/or Process (including but not limited to any Intellectual Property Rights subsisting therein) supplied by [Supplier], its agents and/or permitted subcontractors under the Agreement(s); and

(b) on behalf of [Government agency], for [Government agency] to use (including but not limited to accessing, reading, copying, modifying, adapting and displaying) any Thing or Process (including but not limited to any Intellectual Property Rights subsisting therein) supplied by [Supplier], its agents and/or permitted subcontractors under the Agreement(s).

1.9. [Supplier] undertakes (at its own expense) upon request, to execute confirmatory documentation, and do all things as may be reasonably required, for the purpose of confirming [Government agency's] ownership of any Thing or Process (including but not limited to any Intellectual Property subsisting therein) supplied by [Supplier] under the Agreement(s) or to ensure that no digital rights restrictions are applied to any Information.

1.10. Nothing in this clause 1 will prevent either party from using techniques, ideas and know-how gained during the performance of the Agreement(s) in furtherance of its normal business, to the extent that this does not involve a disclosure of information in breach of clause [ ] (Confidentiality) or an infringement of any Intellectual Property Right.

1.11. For the avoidance of doubt, the rights vested in and granted to [Government agency] under this clause are vested in and granted to her Majesty the Queen in right of the Government of New Zealand, including all government departments.