

Trusted Computing and the Integrity of Government Information
Issues Being Addressed by the New Zealand Government (July 2005)

The New Zealand State Services Commission

Executive Summary

Trusted computing and digital rights management (DRM) are emerging classes of technologies that have implications for the integrity of government-held information.

These implications concern continuing government access to its own information, ensuring that such access will be under its exclusive control, and that sensitive information will be protected from disclosure to unauthorised third parties.

The New Zealand Government's State Services Commission has been investigating these implications, and is in the process of developing principles and policies regarding the appropriate use of these technologies.

Until such all-of-government principles and policies have been adopted, New Zealand government agencies have been advised to not use these technologies.

The next steps include the State Services Commission undertaking further work in this area:

- Investigating appropriate and practicable means for agencies to configure their systems to actively filter out DRM from any files or records that are received, or to return such files to the sender – in the short to medium term.
- Coordinating the process through which government agencies should consider and report on the long-term implications of the use of trusted computing and DRM for their own agency.
- Developing principles regarding New Zealand Government use of trusted computing, and consulting with various parties about them including New Zealand government agencies, other governments, and members of the Trusted Computing Group.
- Monitoring what other countries are doing with regard to trusted computing and integrity of government information, and continuing to share our work with them through channels such as the OECD.
- Continuing to engage in dialogue with key ICT industry players in the field of trusted computing.

Introduction

A quick overview about trusted computing is that it:

- has implications regarding the integrity of government-held information

- heralds a sea change in the way software will be written and delivered, digital content² will be created and accessed, and users will have control over their own information
- is available now in only a limited range of products, but while it is very early days for these technologies, their use will become ubiquitous in a wide range of electronic devices
- offers benefits related to protection of intellectual property and the security of online transactions, but also offers risks including:
 - external parties monitoring a user's information without permission
 - software companies controlling access to data generated with their software
 - external parties controlling access to electronic records, including provision for them to disappear after being sent.
- should not be used by the government until and unless it can be satisfied that:
 - it will continue to have access to its own information
 - such access will be under its exclusive control
 - sensitive information will be protected from disclosure to unauthorised third parties.

Two Classes of Emerging Technologies

Trusted computing and digital rights management (DRM) are separate and different types of technologies, but they offer some similar types of risks and challenges to government. They could also potentially be deployed in ways that mutually reinforce each other.

Trusted computing is being developed to provide a more secure environment for a computer user and for the providers of software and digital content. It will work by requiring users, software and devices to authenticate themselves over a network. The security chip on the computer, together with new software designed to work with it, will look to see what programs are being loaded, and will only allow approved software to be used.

DRM describes and identifies content protected by intellectual property rights, and enforces usage rules set by rights holders. When applied to documents, music or film, DRM will be able to regulate the types of actions that can be done with the content (for example, view, print, copy or save) and the time frame in which that content is accessible.

The Availability of Trusted Computing

Trusted computing technologies are increasingly being built into new computers. Dell, IBM and Hewlett-Packard are producing computers with this functionality, and 20 million such computers are expected to be sold worldwide over the coming year. The design of software

² Increasingly, digital content is the main medium of storage for all created items, including learning materials, books, music, designs, games and video materials.

that will utilise trusted computing technologies is lagging behind the production of the hardware. But by the time such software is available (in a couple of years, for example in the next version of Windows, called Longhorn), the hardware that will support it is expected to be ubiquitous.

The scale of deployment of trusted computing is potentially so great, that it could eventually be included within most electronic devices that are used for information storage, delivery or use – including PCs, PDAs and mobile phones.

The Availability of DRM

DRM functionality is currently available within Microsoft Office (called Information Rights Management), and Adobe PDF (called LifeCycle DRM). It is expected to become increasingly used in a very wide range of electronic equipment.

What Is this Issue About?

The complexity of the issue derives from the fact that trusted computing:

- is highly technical and difficult for a lay audience to understand (it is also poorly understood by many people working in information technology)
- holds promise for the development of further new technologies and applications not yet thought of
- like many emerging technologies, has apparent potential for both great benefit or great harm depending on how it is deployed, regulated, and managed
- is being promoted by a group of international corporations, and the scope for New Zealand to influence what will happen may be quite limited
- is seen by a number of reputable commentators as having wide-ranging and potentially damaging implications for government.

What Are the Potential Uses of the Technology?

As trusted computing is an emerging technology, many uses for it are at the early stages of development. Some of these are identified below:

- **Financial transactions** – trusted computing would allow financial applications to run in a far more secure environment. For example, it would allow safer storage of passwords, PINs and account numbers; stored data could be isolated from potential viruses; and spoofing by false inputs could be prevented.
- **Digital rights management (DRM)** – DRM technologies protect intellectual property rights, and enforce rules set by rights holders on the use of digital content. DRM is currently used to control access to and use of digital content, and will be further enhanced and strengthened when deployed in combination with trusted computing.
- **Software licensing** – software licensed to a particular user for a particular machine would not work for another user or at another machine, unless specific permission was secured from the licensor.

- **Online elections** – trusted computing could overcome risks inherent in running online elections with election software on an individual’s PC. It would allow the voting server to make sure that the user’s voting software had not been altered.

Potential Concerns

There are concerns regarding trusted computing that have been raised about a wide range of issues, including economic-based concerns (such as the potential effect of trusted computing to strengthen monopolies and limit interoperability and competition). However, the current focus for this paper is on issues related to the integrity of government-held information and processes.

Because the technology is at an early stage of deployment, it is not possible to determine the consequences of individual aspects of the design – these will only become apparent when the use of the technology is widespread. When this occurs (expected to be over the next 3-5 years), it will be clear how the behaviour of individuals, businesses and governments are changed.

At this stage, we have identified the following five areas of potential concern:

- **Access to data** – DRM, integral with trusted computing, will allow a user to access software and data on their machine only to the extent that such use is consistent with terms and conditions set by a third party – these conditions can be set by the creator of the data and by the software company. Such control could potentially preclude the New Zealand government from having access to its own information.
- **Privacy** – The remote attestation feature of trusted computing will entail a user’s computer reporting to a remote system in a reliable and trustworthy fashion. This technology will work only by having each computer assigned a unique identity, which will also provide the potential for breaches of user privacy by software developers.
- **Long-term management** – Long-term management of government information produced using trusted computing systems could be dependent on continued use of the technology. If at some stage in the future, one vendor’s technology was abandoned in favour of a different system, then historical records may not be able to be decrypted.
- **Permanence of records** – DRM features within trusted computing technology will enable the creator of a digital record to specify that content will disappear after a specific period of time. This is one of a very wide range of controls that will be able to be applied to documents, even after a document has been distributed, and regardless of how many copies were distributed. The implications of government’s access to its own records being able to be “turned off”, whether intentionally or by accident, are significant.
- **Legal obligations of agencies** – The advent of trusted computing is expected to affect the business processes and legal obligations of government agencies in many ways. Issues that need to be considered include legal obligations under New Zealand legislation such as the Official Information Act, Archives Act, Evidence Act, National Library Act and Evidence Amendment Act.

Annex 1 contains examples, which illustrate some of these risks.

Actions to Date

In November 2003, the New Zealand State Services Commission issued advice to government agencies to not enable DRM features of recently available software called “information rights management” which is part of Microsoft Server 2003 and Office 2003. This message is also still posted on the Commission’s E-government web site (<http://www.e.govt.nz/trusted/trusted.asp>). The reasons for this advice are still relevant today, and this advice has recently been reconfirmed.

Research and analysis has been undertaken by the Commission to keep informed about the latest trusted computing developments and to better understand their implications for New Zealand. This work has included:

- communicating with government agencies, research organisations and various technology and policy experts around the world
- having preliminary discussions with representatives of various New Zealand government agencies, including the Ministry of Economic Development, National Library, Archives New Zealand, Government Communications Security Bureau, and the Office of the Privacy Commissioner
- engaging a technical expert to evaluate the technologies and explore some of their implications for New Zealand government agencies
- engaging with representatives of private sector developers of these technologies to test whether our understanding of the technologies is in accord with their latest thinking, and to have drafts of our consultant’s work peer reviewed by them.

Trusted Computing Steering Group Convened

Ten New Zealand government agencies have appointed representatives to the newly-established Trusted Computing Steering Group.

The purpose of the Trusted Computing Steering Group is to oversee the way that government responds to the significant challenges it will be facing regarding the integrity of government-held information. It will work to ensure that the strategy and policy issues are addressed from an all-of-government perspective.

Representatives on the group are from the State Services Commission, Archives, Ministry of Economic Development, National Library, The Treasury, Police, Government Communications Security Bureau, Ministry of Justice, Department of Prime Minister and Cabinet, Department of Internal Affairs, and the Office of the Privacy Commissioner.

The group will be addressing a range of issues, and will also be looking at the best ways to engage in consultation and communication across government.

Trusted Computing Working Group Being Established

Government agencies will need principles in the short-to-medium term (and perhaps standards in the longer term) regarding government use of trusted computing technologies

to mitigate risks to the integrity of government-held information. There is also a risk that if government-wide principles are not developed, then each agency may separately develop their own, leading to inconsistencies and interoperability issues between agencies. The Trusted Computing Working Group is being established to develop such government-wide principles.

It was felt that the most appropriate way for such principles to be developed would be through the structure and process of a working group established under the E-government Interoperability Framework (e-GIF).

The e-GIF is a set of policies, guidelines and technical standards covering ways to achieve interoperability of public sector data and information resources, information and communications technology, and electronic business processes. It covers business services, access, network architecture, presentation and security. [The latest version of the e-GIF policy framework is available at www.e.govt.nz/docs/e-gif-v-2-1/index.html. Some background information about e-GIF is provided in the following document: <http://www.e-government.govt.nz/interoperability/cabinet-paper.asp>]

The principles to be developed by the working group will need to take account of :

- Issues related to storage and retrieval of information in the context of any legislation, policies or requirements under which government agencies operate
- Identification of instances for which use of trusted computing and DRM may enhance agencies' operations
- Practices that should be adopted to ensure that risks of the use of these technologies would be mitigated
- The practicability and acceptability of such principles in the vendor community
- The process and means by which such principles could be communicated to agencies, and the challenges of having them accepted and adopted
- The international context of such principles.

Following the first stage of work to develop the principles, the group is expected to consider whether standards may need to be developed, and to address issues of governance, development of policies, maintenance of the principles and policies, processes for refreshing them, and international benchmarking.

The working group will include:

- Representatives from central government agencies most likely to be affected by use of these technologies, or most likely to be affected by adoption of the principles
- Two representatives from the vendor community
- Two representatives from local government.

Next steps

The State Services Commission will continue to undertake work in this area which will include:

- Investigating appropriate and practicable means for New Zealand government agencies to configure their systems to actively filter out DRM from any files or records that are received, or to return such files to the sender – in the short to medium term.
- Coordinating the process through which government agencies should consider and report on the long term implications of the use of trusted computing and DRM for their own agency.
- Consulting on the principles regarding government use of trusted computing, including with other governments and members of the Trusted Computing Group.
- Monitoring what other countries are doing with regard to trusted computing and integrity of government information, and continuing to share our work with them.
- Liasing with our colleagues internationally to find shared opportunities to develop appropriate collective government policies and positions on issues related to trusted computing.
- Continuing to engage in dialogue with key ICT industry players in the field of trusted computing.

Annex 1

Examples that Illustrate Risks to the Integrity of Government Information from Trusted Computing

Note: These examples are presented only to illustrate the scale and range of potential risks from implementation of trusted computing technologies. They reflect worst case, but legitimate, scenarios. The extent to which they eventuate will be dependent on how the behaviour of individuals, businesses and governments change as a result of the technology.

These risks may be mitigated through development of appropriate government policies and practices, combined with some (limited) opportunity to influence the way these technologies may be designed and deployed by software and hardware companies.

Access to Data

If DRM were to be permitted in emails or other documents – without adoption of appropriate policies and practices – the myriad of interactions and vulnerabilities may result in a loss of certainty as to what content can be accessed through what software, on what terms it may be accessed, by whom it may be accessed, and for how long it can be accessed.

The complexity of these issues can be illustrated by the following example:

- An agency receives an email from an outside party. It has two attachments. The first is a Word document from an outside party and the second is a PDF document from yet another party
- The email and the documents were all created with DRM enabled but with open permissions for guests
- Continuing access is limited with each document having different controls by time, by the number of accesses and the number of times copies are made from the document
- Recipients are unaware of the permissions, as the guest access and the limitations are ‘silent’
- The email is forwarded on to many. Additional comments are provided. The email and its attachments become evidentially important
- The guest permissions expire with varying effect (some users have saved one or more of the attachments). The originator of the email dies. The PDF is authored outside the jurisdiction and the author cannot be contacted. The author of the word document is not co-operative
- The DRM permissions mean that it is not possible for anyone to obtain access to the email or either of the attachments.

Privacy

Trusted computing will work by assigning a unique identity to each computer, and each computer will report its configuration to a remote system in a reliable and trustworthy fashion. However, this will also provide the potential for breaches of user privacy.

Concerns have been expressed about the fact that information about the configuration of a user's computer, and work being done on it, may be communicated to a software owner (or others) without the user's permission or knowledge.

Examples of these concerns include:

- externally held registers of information about a user's machine or software, with potential for abuse (data matching)
- external monitoring of a user's computer to determine what software and data is held there.

Although software developers may be encouraged to build applications that use personally identifiable information in ways that inform users of what is being shared and how it will be used – there is no guarantee that this will happen. These aspects of the technology, therefore, increase the significance (for the end user) of:

- the risk that a user may grant such permission (to enable disclosure of personal identity and information) without realising that they have done so (e.g., by clicking on “I agree” to a complex end user licence agreement), or without understanding the implications of doing so
- the future potential for software companies to collect and report on a user's personal information without even seeking permission from the user, and without the user's knowledge.

In response to concerns about privacy, “trusted third parties” may be established and used for the purpose of associating particular communications with any specific computer. The reliance on a trusted third party, however, will introduce its own privacy risks, as that party could disclose its knowledge of a user's identity and communications. Thus, the independence, reliability and integrity of any trusted third parties that may be established would become critically important to the integrity of government-held information.

Long term management

Software enabled to work with trusted computing will have its security policy administered remotely by a server. Such remote policy enforcement could lead to “remote control” of software running on a user's trusted computing system.

For example, if a program were to be written to receive a “revocation list” of banned documents it is no longer permitted to display, this would be downloaded from time to time and used to screen all files that the application opens. Files could be revoked by content, by the serial number of the application that created them, and by a number of other criteria – and would be impossible for the user to override.

In that case, a remote authority could revoke documents already resident on computers around the world; those computers would, despite the wishes of their owners, comply with the revocation policy.

A foreign organisation (or government), with access to the TC certification master keys, could prevent the New Zealand government from having access to its own information when that information is held electronically.