

## **Emerging computer technologies create new risks for councils**

The E-local Government Strategy Project Team discussed the emerging technologies of Digital Rights Management (DRM) and Trusted Computing at their April 2005 meeting. These technologies will cause problems for councils in pursuing their record-keeping role as they allow for new kinds of control over computers and digital 'objects'. The strategy team has asked that Local Government New Zealand write to all council Chief Executives advising of the issue, taking note of the E-government Unit's advice and asking that staff with information management responsibilities be provided with this background paper.

The E-Government Unit (EGU) has been working for more than a year on issues with these emerging technologies and there is background material on the e-government unit website <http://www.e-govt.govt.nz/trusted/index.asp>. In particular there is a link to the information about preventing the accidental importation of files with DRM features which may later become unusable.

***The E-Government Unit is advising that central government agencies do not accept digital documents or records that have had DRM applied to them nor should they turn on the trusted computing features called (Information Rights Management or IRM) of computers with Microsoft server 2003 or Microsoft Office 2003 until work on the policy issues covering this issue has been carried out. It is expected that the work will be complete by the end of 2005.***

### **Two classes of emerging technologies**

Trusted computing and DRM are two classes of emerging technologies that present potential challenges to the integrity of government-held information. They are separate and different types of technologies. They offer some similar types of risks and challenges to councils.

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 can 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.

This is occurring under the auspices of the Trusted Computing Group (TCG). The five "promoter" members of this group are Microsoft, Intel, IBM, HP, and AMD. For information about the TCG and its objectives, see: <https://www.trustedcomputinggroup.org/home>

### **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 during this year worldwide. The design of software that will utilise trusted computing technologies is lagging behind the production of the hardware. 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 availability of DRM**

An early form of DRM called Information Rights Management (IRM) is part of Microsoft Server 2003 and Office 2003, which are now available to agencies. These products ship with IRM disabled, and require a number of steps to be taken at both the server and application level before it can be used. Adobe PDF (called LifeCycle DRM) also contains DRM features.

### **Some issues of concern to councils**

The onus of security is passing from protecting a computer network with firewalls to providing security at the level of individual documents or other kinds of 'digital objects' such as images video and audio files. Digital objects protected in this way may not be able to be copied, printed, forwarded or archived and in addition it will be possible for the object to expire, or become inaccessible at a given point in the future or after particular number of uses. In addition, to use the objects there may need to be a validation against an external computer to the organisation to confirm that the user can view or edit the object. Where a software licence has lapsed or been superceded by a later version there is a danger that the external computer may not permit access to the files.

While there are legitimate copyright reasons for the approach taken by computer companies to protect intellectual property, the power that this gives to companies and individuals could undermine legitimate record keeping.

Trusted computing technologies may enable agencies such as banks or others to ensure that the person that they are dealing with is legitimate. But they may also entail monitoring of the activities undertaken on a computer, and communication of this information remotely. What information is communicated, and to whom, are issues of concern to councils. There are privacy implications, as well as government and local sovereignty issues to be considered.

All of these issues are also of concern to members of the public and so there are civil rights and privacy issues for citizens in their relationships with business and government.

The international picture seems to be mixed and internationally governments appear to be on the back foot with this issue. While hardware suppliers are well advanced in these projects governments internationally are lagging behind in their ability to legislate and make policy for the consequences of these issues.

### **E-government response**

The E-government Unit has established a cross-government steering committee to manage an all-of-government response to these issues. Over the coming year, there will be continued research and policy work to develop appropriate policies and practices regarding government use of these technologies. Local government representation on this group is being sought.

In the short term, and until such policies and practices can be put into place, the Minister of State Services has agreed that the E-government Unit should advise central government agencies to not accept digital objects that have had DRM applied to them or turn on the Trusted Computing features on computer servers.

There are two main mechanisms presently available for creating DRM digital 'objects' as described above. With objects using Microsoft's IRM it is possible to identify the status of the file created from information in the header. For objects created using the Adobe technology identifying affected documents is less straightforward. The e-government unit has provided guidance on how agencies can avoid introducing digital rights management documents into their systems. Information about this and the e-government response is available here:

<http://www.e.govt.nz/trusted/trusted.asp>

Jan Rivers,

Local Government New Zealand

13/4/05