Submission No. 58

Attention: Committee Secretariat
Re: Inquiry into the Management and Integrity of Electronic
Information in the Commonwealth

1. Re: Trusted Computing Environment.

Modern systems are generally built in layers, with each layer depending on the integrity of those below for correct and secure operation. The idea of a trusted computing environment is to secure the lowest layers in hardware, which can be made difficult to modify and, therefore, circumvent. Each layer, starting with the hardware, can certify the layer above it, thus providing a chain of trust that encompasses everything from the hardware to the applications.

AUUG regards hardware and software that allows the creation of trustworthy environments as desirable and a natural extension of many existing market developments. There is a clear demand for security features, leading to the wide availability of password protected BIOS programmes, encrypting web servers and secure operating systems to name only a few examples. AUUG believes that the marketplace is continuing to aggressively innovate in the area and that industry standards will emerge in a timely fashion.

Microsoft is part of an industry consortium, led by Intel, known as the Trusted Computing Platform Alliance. AUUG regards the TCPA as an example of industry experimentation in the area of trusted computing, and it is unclear whether this consortium's proposed technologies will succeed or fail in the market. In practice, their success will depend on a compelling case for adoption and clear cost benefits.

AUUG regards Microsoft's "Palladium" technologies (the software designed to run on a trusted computing platform), with some concern. Clearly, one use of a "trusted environment" is to prevent unauthorised applications from running, or to prevent them from accessing some files. It is easy to see how, say, a word processor competing with Office may be regarded by Microsoft as "untrustworthy" and therefore be prevented from running by Palladium. Combined with Microsoft's market power and proven anti-competitive behaviour, it is of real concern that trusted computing platforms may be misused to reduce competition (and hence, innovation) in the marketplace.

At the same time, it is clear that the current generation of "trusted platforms" is less than effective. For instance, Microsoft's "X-Box" entertainment console was designed to run only authorised software (i.e. behave as a trustworthy system). These security measures have proved ineffective in preventing unauthorised software from being used on these devices, throwing some doubt on the overall effectiveness of Microsoft's apprach to this problem.

AUUG recommends that the Commonwealth should actively monitor developments in trusted platforms, but that it is premature to set policy or standards in this area. When the technology develops to suitable maturity, AUUG urges the Commonwealth to maintain a vendor neutral stance, in order to promote competition and interoperability in the marketplace.

2. Re: Gatekeeper.

AUUG regards the Commonwealth's Gatekeeper strategy as a generally well architected framework for promoting secure online authentication. In particular AUUG notes that the following key attributes:

- * Based on strong, open, international standards (especially X.509).
- * No key escrow requirements.
- * Strong accreditation requirements for certification authorities.
- * Contractually enforced privacy requirements.

AUUG is of the opinion, however, that the Gatekeeper strategy is currently weak in addressing the issue of certificate revocation. While the certification of keys and the creation of digital signatures has been specified in find detail, Gatekeeper is relatively silent on policies and operational requirements for creating and using revocation lists. While the issue of certificate revocation is difficult, AUUG regards it as a key element of any viable long-term public key infrastructure.

In any X.509 based system, including Gatekeeper, the Certification Authorities play a pivotal role. Compromise of a CA carries the potential for widescale fraud, denial of service and general loss of trust in the system as a whole. It is not clear to AUUG how the current Gatekeeper policies can be effective in preventing compromise in many forseeable circumstances.

In general, Gatekeeper relies on contractual requirements, common law remedies and withdrawal of accreditation to maintain standards. However, these are probably not sufficient to guarantee security if, say, a CA goes out of business. Neither do they mitigate the catastrophic failure of a compromised CA. It is also unclear how jusridictional issues may interact with Gatekeeper if international entities are accredited under the programme. These are not simple issues to deal with, however they suggest systemic weaknesses that the Commonwealth may wish to address.

Lastly, Gatekeeper potentially creates barriers for international entities wishing to do business with the Commonwealth. AUUG notes that this is not always a negative; subjecting external parties to the rigours of the Gatekeeper registration adds significant value to the system. AUUG notes that Gatekeeper has embarked on a "cross recognition" programme to recognise external authorities and certificates. This has the potential to "water-down" the assurances of the Gatekeeper programme, and should be approached with care and appropriate controls.

Michael Paddon
AUUG Inc.