# Computer Associates Response to the MAC Report, "Australian Government Use of Information and Communication Technology"

In our testimony to the Joint Committee of Public Accounts and Audit, on 2 April 2003, Computer Associates ("CA") expressed the view that the government must take a holistic, federated approach to security and identity management issues.

This view is supported in the Management Advisory Committee's (MAC's) report, *Australian Government Use of Information and Communication Technology*, on which chairman Bob Charles, MP, invited CA to comment. As this paper notes, "[the Australian Government] is moving beyond single-agency IT installations and unrelated Internet web sites … [and] entering the complex phase of providing integrated service delivery both online and through other channels."

Clearly this move towards federated and interconnected sites requires an overarching policy, to ensure that internal agency initiatives can be integrated into the all-of-government solution that will emerge. This makes sense at the technical (ease and consistency of implementation), user (consistent experience), governance (legislative and legal conformance) and commercial (cost-effective) levels.

The MAC report provides a deliberately high-level overview of the issues related to each of these areas. In our opinion, it touches on all of the key areas that need to be considered. We also note that the report advises that Agencies should retain autonomy in managing their own infrastructure and systems, so long as they adhere to the all-of-government standards the oversight committee would produce. CA supports this approach. The proposed structure of the oversight committee allows the Agencies to have input into these standards, which will help with buy-in and compliance.

## Specific Comments

CA would make the following specific additions to the MAC report:

1. "Principles of ICT Governance to Optimise Commonwealth Outcomes" (p.12)

CA would add the following section:

- A Whole of Government, standards-based policy for identity management (information naming, categorisation and storage) is essential to ICT supported business processes.

We have singled this area out because it is critical to providing federated management and service to the Government's "customers" – both internal (the agencies) and external (the general public).

A federated service capable of supporting such a wide user population *must* implement a single, authoritative store of reference, which all agencies will refer to for user information and rights. This datastore is the cornerstone of a federated identity management strategy, and will rely on a consistent naming schema being instituted across all government agencies. This has been recognised in current state government initiatives (for example the OIT all of Government project in NSW; the Rosetta project in Vic), and is a guiding principle of identity management worldwide.

2. Appendix 3 – Secure Business Systems Working Group "1. The Culture of Security" (p.29)

CA agrees that "It is not possible to impose a security *culture* on agencies. [our italics]"

However, we would note that it is not only possible, but necessary, to use tools to enforce the security requirements that an organisation must follow.

An unofficial maxim of the security industry states that "Policy without enforcement breeds contempt". Thus, whilst we agree with all of the initiatives proposed in this appendix, we would add that there must be active measures taken to ensure compliance, wherever such mechanisms are possible and the cost-benefit analysis supports their implementation.

# Introduction to Public Key Cryptography

The following is a reasonably "generic" description of how Public Key Cryptography works, and its advantages over a symmetric key system. Alice and Bob have become Public Key icons as a result of these type of descriptions, and I'll continue to follow that convention when providing some examples below.

In "traditional" (symmetric) cryptography, a single, secret key is created that will be used to encrypt and decrypt messages. The major disadvantages to this approach are that:

- It requires a secure transmission mechanism to get the key to both communicating parties
- A new key has to be created and securely shared for each party you want to correspond with (if you use the same key, everyone who you've sent it to can read any messages you send, not just the ones intended for them).

  This has profound implications for large organisations – to set up an infrastructure that allows secure communication between any pair of employees from their total pool of *n* employees, they have to generate, distribute and manage *n!* keys.

For these reasons, public key cryptography and the public key infrastructure is the preferred approach to encryption in electronic transactions (i.e. on the internet).

In public key cryptography, a pair of complimentary (in this case, mathematically related) keys are created. The two keys are related in such a way that a message encrypted with one key can only be decrypted using the other key. In practice, one key (the *private* key) is kept securely by the "owner", and the other (the *public* key) is published. This means anyone can send a message to the key's owner, but only the owner can decrypt that message, as they have the only copy of the private key.

This has enormous advantages in the world of electronic transactions, as it:

- Removes the requirement to safely swap keys. One key is published to the world, and the other never has to be (and should never be) revealed to anyone.
- Allows you to publish only one key, as all correspondents can use the same key when sending messages to you (they still have to publish their own public key for you to correspond with them)

  Thus, where symmetric key cryptography requires n! keys, public key cryptography only requires n keys – which again has profound implications for large organisations.

- Introduces the concept of message integrity and non-repudiation. You can sign messages with your private key, and your correspondents can confirm it came from you by verifying the signature with your public key. A similar technique can be used to verify the message hasn't been altered since it was sent.

The following examples help illustrate how public key cryptography works in practice.

- Alice has a pair of complementary keys – what one key encrypts the other can decrypt
- Alice keeps one key private, in a secure store such as a smart-card (the Private Key)
- Alice makes the other key available to the public (the Public Key)
- Bob wants to send an encrypted message to Alice. He requests a copy of Alice's public key
- Bob uses Alice's public key to encrypt the message and sends it to Alice
- Alice decrypts the message using her private key

Both Bob and Alice have several advantages in this scenario:

- Alice isn't concerned about securely sending her public key to Bob. Even if other people get a copy of her public key, all they can use it for are to send Alice private messages. They can't use it to decrypt messages sent to Alice, or to impersonate Alice
  Alice can send her key using email, or even post it to a public directory
- Bob can be sure the message comes from Alice – Alice can use her private key to put a digital signature on the message, which her public key confirms comes from her

- If Bob follows the same procedure, and publishes his private key, these advantages are available to both correspondents, imposing a layer of trust and non-repudiation on an infrastructure that is inherently insecure (i.e. the internet)

Public Key Infrastructure is built on the foundation of public key cryptography. It is not a fool-proof solution to questions of identity management and fraud in the electronic world, but it is a cost-effective and manageable mechanism that takes significant steps towards achieving this goal.