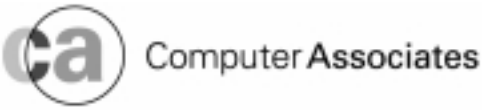
Submission to the Joint Committee of Public Accounts and Audit

Management and Integrity of Electronic Information Enquiry

By

Computer Associates



Executive Summary

This submission to the Joint Committee of Public Accounts and Audit focuses on one aspect related to the "Management and Integrity of Electronic Information" that Computer Associates (CA) believes would make a significant impact on ensuring the privacy, confidentiality and integrity of the Commonwealth's Electronic Data while at the same time providing significant gains in the effectiveness and competitiveness of all government businesses - *Identity Management.*

Identity Management can be defined as the management processes required to securely control and track access to the Commonwealth's Electronic Data and critical IT resources (applications, networks) via authenticated user identities.

The introduction of web-based technologies has forced government departments to change the way they conduct business. Today, they *must* find new ways to securely control access to government resources. In addition, departments must be able to manage increased security risks associated with the escalating volume of user administration and the need to provide improved business products and service. To succeed both government departments and associated businesses need to build comprehensive Identity Management and security capabilities into all aspects of their business strategies.

An Identity Management strategy would provide the government's customers[1] with enablers and solutions to improve security, quality of service and radically reduce administration costs and complexities. Specifically, and relevant to the Committee's Terms of Reference, benefits to the government and its customers would be delivered in the following areas:

- Reduced security risks and improved ability to authenticate a diverse user population.
- Strengthened processes for managing access to government data.
- Enhanced capability to respond to changing regulatory and compliance environments.
- Delivery of a service that while federated offers new levels of delegation granularity, allowing government initiatives to be consolidated and secured at a Federal level but control delegated to state or locals governments as required.

This submission gives a high level overview of Identity Management concepts and the immediate and long-term benefits for the government, its departments and customers. A more detailed description of the concepts, technical characteristics and benefits of Identity Management are available on request.

[1]Throughout the submission the term customer(s) represents all parties that interact with the government, these parties could include: Government employees, citizens, ratepayers, taxpayers, government suppliers, partners, foreign governments or citizens etc…

Contents

1. Government's Electronic Business Challenges and Risks

1.1 Web-Based Business Growth

The growth of web-based services and government businesses over the last five years has been substantial. The electronic business boom has attracted users by the millions, and online transacting has become the most convenient way to conduct both government and non-government business. Customers are no longer restricted by currency, geographic location or hours of operation, as web-based businesses accept universal currency, are accessible from around the world and are available around-the-clock.

As governments surged to embrace their national and international customer-base, they did not fully conceive the sheer number of users the Web would attract or how it would impact business operations, particularly for managing external and internal users. As a result, governments have unwittingly left themselves open to threats and vulnerabilities, such as website vandalism, stolen user information and breaches of customer and citizen confidentiality.

1.2 Business Security Fears

The Web has changed the way governments conduct business, and has challenged traditional paper-based business strategies. Today's governments are replacing the customary methods with a business approach that includes new concepts and new technology.

Additionally, there is now the need to accommodate new risks, including viruses, denial of service and website attacks, as well as the lack of awareness surrounding where, when or how the next attack will occur.

A new business environment has evolved where governments are faced with numerous challenges, including how to manage users, how to validate each user's identity, and how to store confidential user information.

2. Government's IT Department Challenges and Risks

2.1 Managing Heterogeneous Systems

Today's governments have had to integrate their information systems and often combine disparate technologies. This becomes even more challenging as a result of government department consolidation, centralisation/de-centralisation and outsourcing.

To accommodate these changes, the IT department must administer a large number of heterogeneous systems and applications. It must also manage a huge influx of new users and adjust their privileges accordingly. To add to this complexity, many government departments have implemented security solutions that have been time-consuming and costly for the IT department to integrate and customise for their business environment, and that ultimately allow multiple points of failure.

The sheer number of issues associated with managing individual systems, legacy applications and a host of methods for users to authenticate is a monumental task for the IT department. This task becomes even more difficult when governments are looking for the IT department or their outsourcer to "do more with less". Security can be an area that is easily ignored, or where it is felt that costs reductions can be made.

3. Identity Management

With the new challenges faced by governments today, new concepts and practices are required to effectively regain control of security.

Crimes covering the theft or misuse of identity and information have been well documented within the Government sector. They range from the recent example of a Centrelink customer with 37 different 'identities'[2], through to ensuring that a passport is issued to the right individual.

Whole of Government Identify Management strategies and solutions can be employed to enhance the privacy, confidentiality and integrity of the Commonwealth's electronic information and its business activities. A Whole of Government Identity Management solution has the potential to reduce the opportunity for fraud, identity impersonation and outright theft.

Identity Management can be defined as the management processes required to securely control and track access to the Commonwealth's Electronic Data and critical IT resources (applications, networks) via authenticated user identities.

Identity Management can be global (covering all transactions within the Government) or local (covering interactions with a single agency only). At the local level, the current agency security systems cater for the management of remote users at the cost of implementing extensive Identity Management solutions at each agency. This requires a Government Service user to manage multiple access points/systems and to prove (register) their identity at each entry point.

At a global level, Identity Management is a process that allows a user to interact with all Government (and affiliated) systems with such authority as required, using a single identity method and yet which does not raise the privacy issues around a single point of access management such as occurred with the Australia Card. Some Government approaches to this issue have been the Medicare Card, Australian Business Number and the Australian Tax File Number. To address privacy issues associated with the potential misuse of these initiatives, the Government has implemented (through legislation) strict controls on what these numbers may be used for.

What is required by Government is a single solution that can:

- reliably and accurately validate an external user;
- provide assured details to the accessed system(s);
- not be used for health or medical screening;

[2] As discussed by Amanda Vanstone at a CA/Argus seminar on the 20/11/2002

- does not allow details to be used for purposes other than those mandated; and,
- does not allow for proxy access (i.e. providing someone else your user name / password for access to an account).

The proper use of a global Identity Management solution would significantly reduce identity theft / fraud, reliably identify a user and yet allow scarce investigative resources to be more gainfully targeted into high risk areas of security.

The following sections outline a range of issues related to Identity Management.

3.1 Role-Based User Provisioning

User provisioning is a key component of Identity Management and is the process for managing user identity government-wide and beyond.

In any system(s) accessed, a user may have one or more roles allocated to allow access to the information services. For example, in a global scenario, a Tax Agent may have the ability to look at Centrelink benefits for himself and nominated family, access the Department of Immigration web-systems for information, access the personal components of the ATO web systems for himself and nominated family but also have access to lodge taxation claims for a wide range of people all through the same identity. A departmental scenario is similar in range but limited to the information systems within the individual department.

The overall management of access roles is the largest management component of any user access policy consuming up to 50% of security management effort. Other issues relate to the continued checking of identity for the provision of Government Services. For example, Centrelink requires its clients to re-confirm identity with a 100 Point ID check each 6 months (or more often for a high risk profile client). This is time consuming and yet may not provide a high level of security or identity management as to gather 100 points may simply require time and access to a false birth certificate. With the advent of a more rigorous identity solution a 500-1000 point check could be instituted at registration with a guaranteed ID thereafter.

Within a Government agency, users/clients can be readily managed as an entity with user provisioning through policy based directory management systems tied into the HR systems. As a person is hired, promoted, changes jobs, joins/leaves committees, etc, their access can be automatically updated and reset accordingly through these policies/roles.

User provisioning encompasses the identification of:

- The types of customers the government will manage
- The systems, applications and other business resources those customers will need access to
- The levels of access to those resources customers will need
- How the government will create, update and delete customers accounts

- What the strain will be on the IT department to administer the quantity and different types of customers
- How the government will guarantee secure access to its resources

These processes need to remain open and adaptable to accommodate future changes in technology and in the business environment. Governments and business will build user provisioning methods into their business strategy over the next few years, as noted by Gartner: *"By 2005, 60% of Global 2000 enterprises will have implemented user provisioning systems to manage their internal and external user access requirements for Web and non-Web applications."* [3]

User provisioning is a critical enterprise function that provides customers with the proper resources at minimal cost and involves managing a user's life cycle, from creating various user accounts on different systems and extending user access to external services, to temporarily suspending user access or permanently revoking user accounts. Strong user provisioning reduces security risks, including weak passwords, and minimises obstacles to user/customer/citizen productivity by increasing access time. User provisioning also provides centralised management capabilities. Using role-based account creation and workflow access rights to business resources, centralised management enables an automated approach across the entire security infrastructure.

3.2 Managing User Identity

Governments can identify different types of users according to their business function: employees, customers, citizens, suppliers, partners and more. Each user within each of these groups owns a separate online "user identity" that should be managed as part of the governments process management strategy. In this way the government can effectively manage secure user identity and lower costs.

Government departments can build an identity management strategy using the common set of requirements that each group of users shares as the foundation. For example, internal user accounts can be organised according to an employee's role in the department. As an employee develops his or her career, the user account is changed to reflect his or her new responsibilities. It is convenient for users to own their online user identity and for their user identity to move with them, so it is dynamically updated according to their specific role. This also increases an employee's productivity, as he or she can change roles within the organisation and can automatically access the systems appropriate to his or her role.

Once an organisation has attracted a customer, supplier or partner, it is vital to ensure that the process of registering his or her identity and submitting a transaction is straightforward, smooth and secure. A trusted environment also ensures customer, partner and supplier trust and loyalty.

[3] Gartner, Inc., "User Provisioning in Transaction Incident Management,"

A. Dang van Mien, R. Witty, March 2002. Global 2000 is an industry term commonly used by analysts to refer to the top 2000 enterprises worldwide, based on revenue

If users find it too complex to register or too difficult to maneuver around a website, they will quickly take their business elsewhere. Delivering effective customer service personalises the user experience. To feel valued, users need to know that the information they provide is kept confidential and secure.
It is far easier for the organisation to manage one single user identity rather than multiple identities for one user. The same can be applied to customers, suppliers and partners. Their identity can be managed according to users' needs, enabling the organisation to deliver quality and customer service and most likely retain the customer.

Internal user accounts can be organised according to an employee's role in the organisation. An organisation must also guarantee that the user's access to business resources is straightforward, smooth and secure.

Let's consider an employee in an Australian Embassy who needs to access new procedures and policies for his or her new role, which are kept on a server in the Foreign Affairs and Trade Department head office in Canberra. Traditionally the employee would have to get approval from his or her manager, and send that approval to Canberra to gain access to the server. Today, it is more convenient and cost-effective for the user's identity to be automatically updated according to his or her new role. This can be managed through a delegation of administrative responsibilities, which takes the burden off the IT department to be the sole conduit for managing users. For example, a human resources (HR) manager can change the employee's role in an HR application. User provisioning tools, which are implemented by the IT department and integrated with the HR application, would have predefined access rights for that particular type of role. As soon as the employee joins that role, their access permissions to business resources are dynamically updated according to the permissions preset by the IT department. This is an enormous aid to the organisation, as it shares the task of managing users among non-IT departments. This ultimately reduces business costs and effectively automates business processes.

3.3 A Directory Infrastructure

A directory allows government agencies and businesses to group system files, such as employee information, into a hierarchical structure so that they can be more easily accessed. An identity management solution is only complete with a strong foundational backbone based on a directory architecture. The strength of this architecture allows directories to synchronise, replicate and link information between information stores in a noncomplex, distributed environment—without the need for a centralised repository of information. In today's electronic age, users want to quickly perform their online transactions. Directories provide extremely fast lookup capabilities across geographically distributed locations, which is key to government business success. Government is often challenged with integrating disparate technologies and consistently managing information. This results in information being duplicated, fragmented and dispersed throughout the enterprise. As the organisation grows, business-critical applications increasingly require a directory solution that combines the highest levels of performance, reliability and industrial-strength security.

3.4 User Authentication

Using strong authentication methods, including biometrics, smart cards and digital certificates to validate a user's identity is comparable to making a transaction in person and validating the person's identity using a credit card as a guarantee. Governments can validate this information while ensuring all information communicated between the business and the user remains confidential, establishing a level of trust between the two parties.

The trusted foundation for supporting user authentication is a Public Key Infrastructure (PKI). PKI is the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke Public Key Certificates based on public key cryptography. PKI helps ensure repeat business by protecting distributed user identity and allowing transactions to take place in a trusted environment.

3.5 Single Sign-On and Secure Access

Similarly to the way user provisioning provides streamlined access for a user, simplified access to business applications is enabled through single sign-on (SSO) technology. From both an administrative and user perspective, single sign-on relieves the frustration of having to remember multiple passwords to access multiple systems. Implementing single sign-on functionality helps reduce the IT department's administrative overhead by providing one interface to manage multiple systems. Security breaches have become common around password theft and unauthorised access to systems, which has created a need for a strong authentication method to be implemented.

Web-based technology has provided different access points to government, allowing users to connect via the Internet, Extranet and Intranet. Users want the assurance that they are conducting their transactions in a trusted, secure environment. Therefore, enabling secure access to business resources has never been more critical.

3.6 Self-Registration and Self-Administration

The government must also realise the value of user self-registration and self-administration, since staffing budgets are more restricted and user productivity is crucial to business growth. For example, a user can register with a business by submitting a web form. He or she is then assigned a user ID and password to perform a business transaction with little or no human intervention and thereby reducing manual errors and decreasing user downtime. As password resets are common issues raised with help desks, the ability for a user to reset a forgotten password has far-reaching benefits for the business operations, the IT department's workload and the user's productivity.

One such cost benefit can be readily illustrated. In the current Government environment, costs for the resetting of passwords vary between $48 per time to $200 per time with the average user requiring approximately 1.5 password resets a year. This involves many millions of dollars per year in costs to the Government that could be avoided.

3.7 Account Mobility

A key requirement for the identity management strategy is for user accounts to remain mobile. Employees are constantly moving around an organisation and many users now travel as part of their business roles, connecting to business resources from different access points. It is essential that a user's identity moves as he or she moves. Users must also be given the same level of access how ever and where ever they connect to the business network. The identity management infrastructure must be flexible to accommodate this type of mobility.

Further to geographical mobility, the occupational mobility to join and depart committee structures, being promoted, etc, all compound the issues noted above. All Government departments suffer this to a greater or lesser degree. On average the Government employee turnover rate is about 12%, which includes moves due to promotion, etc. This means that 12% of the employee population is required to have its access reviewed and adjusted each year.

3.8 Web Services

The identity management infrastructure must also be open and extensible to support future Web services and integration with other business environments. Although standards for the architecture are still emerging, Web services security will enable a user to securely access multiple websites using the same user identity, requiring business technology to be interoperable.

3.9 User Life-Cycle Management

Government departments can benefit from a "hire-to-retire" concept for employees, where management of an employee's identity starts when he or she joins the government. This concept gives employees appropriate physical facilities and system access and manages their online identity until they leave. In addition, when an employee leaves the government, his or her associated user accounts can be deleted from a single-point interface, which can access multiple systems. This eliminates security holes due to missed system access removal (The recent issue surrounding "Michael Wooldridge's unauthorised use of the Department of Health's email system two months after leaving his post" [4] highlights these types of holes in security systems).

4. Conclusion

As more and more people demand access to the Commonwealth's electronic information, the requests are no longer restricted to government employees but now come from citizens, ratepayers, taxpayers, government suppliers, partners, overseas governments/citizens. The rapidly fluctuating user populations and rapid employee/customer turnover have made identity management, provisioning and access control a key security and risk management issue.

A well defined, business driven strategy and architecture for identity management can go a long way towards addressing the inherent complexities, risks and costs associated with protecting the Commonwealth's electronic information, as well as opening up opportunities to efficiently deliver new services and products.

[4] As reported in the Australian Financial Review on the 8/6/2002

5. About Computer Associates

5.1 Company Background

Computer Associates International, Inc. is the world's leading business software company and is focused on delivering the software that manages eBusiness. CA delivers innovative technology, services and training to provide end-to-end infrastructure.

CA's solutions address all aspects of eBusiness management including Enterprise Management, Security, Storage, eBusiness Transformation and Integration, Portal and Knowledge Management, Predictive Analysis and Visualisation. The company supplies commercial enterprises, government agencies, educational institutions and research organisations.

CA is headquartered in Islandia, New York, has more than 1,200 software products and complementary services, operates in more than 100 countries and has 17,000 employees. CA's products are used by over 95 percent of Fortune 500 companies.

5.2 Computer Associates in Australia

Computer Associate's first Australian office was established in Sydney in 1984, followed by other offices around Australia. The company now employs approximately 600 Australians, working from offices in the ACT, NSW, VIC, QLD, SA and WA.

Computer Associates' software is used by the Australian Electoral Commission (AEC) to calculate the results of every election in Australia, by Australia Post to ensure every computer in every Post Office can be managed and by the Army to coordinate training services.

Other Government clients include the Australian Taxation Office, Centrelink, Australian Customs, Australian Federal Police, and many more.

Other Australian clients include Telstra, Commonwealth Bank, ANZ Bank, Adelaide Bank, BHP, St. George Bank, NRMA, ACTEW Corp, the Brisbane City Council, and many more.

5.3 Supporting R&D hubs in Australia

CA Australia hosts three R&D facilities that develop products for use around the world. In Victoria, there are two sites with more than 80 staff, one at Richmond and the other at Mooroolbark, that specialise in security software. The third facility is located in Sydney at French's Forest and specialises in storage management software.