Department of the Premier and Cabinet
Government of Western Australia

# WESTERN AUSTRALIAN GOVERNMENT
# OFFICE OF e-GOVERNMENT

# IDENTITY & ACCESS MANAGEMENT FRAMEWORK
## (Final Draft V2.0)
**15 September 2005**

**Prepared by**
**Convergence e-Business Solutions Pty Ltd**

**WESTERN AUSTRALIAN OFFICE OF e-GOVERNMENT**
**IDENTITY & ACCESS MANAGEMENT FRAMEWORK (Final V2.0)**

## CONTENTS

**WESTERN AUSTRALIAN OFFICE OF e-GOVERNMENT**

**IDENTITY & ACCESS MANAGEMENT FRAMEWORK (Final V2.0)**

## Preamble

The purpose of Identity and Access Management is to ensure that those who should have access to information and/or services and/or assets do, and those who shouldn't, don't.

Failure to assure the efficacy of Identity and Access Management will result in a variety of consequences ranging from the trivial to those that erode confidence in government institutions, and threaten property and lives.

Identity and Access Management has always been important. The emergence of IT-based and telecommunication-networked environments has heightened the importance of this issue because:

- Information is stored in highly concentrated forms, can be altered without leaving 'physical' evidence, and can be 'copied' in large volumes, at high speed.
- Services (eg process control/SCADA systems) can be 'controlled' without having to pass (or circumvent) physical barriers.
- Assets (eg funds) may be 'obtained' in a largely non-physical or invisible manner.

Identity and Access Management (Id&AM) has also assumed greater importance because of the need to satisfy the twin pressures of:

- Demand for improved (anywhere, anytime) service delivery by customers; and
- Requirements for increased operating efficiency by the fiscal agencies of governments.

An increasing response to both of the above is the migration of services from people-intensive counter and phone channels to online channels. The Internet has made this technically, logistically and economically feasible. The connection of government systems to the Internet, a vast, open global network, has raised the IT security stakes by orders of magnitude, bringing a new urgency to the requirement for governments to effectively address Identity and Access Management.

An effective response to the Identity and Access Management challenge requires that management of agencies have a comprehensive and unified approach to:

- the 'identification' and active control of information, services and assets, the determination of the intrinsic value and/or sensitivity of these; and
- the 'identification' and active control of entities who may legitimately gain access to information, services and assets, and the determination of what rights they may have in regard to these.

This report presents a Framework for the Western Australian Government to assist in the planning, architecting and assessment of approaches to Identity and Access Management.

The Framework is regarded as appropriate for usage at an agency, agency-cluster; and whole-of-government level.

The Framework is intended to assist in the achievement of:

- effectiveness (ensuring the efficacy of Id&AM);
- efficiency (ensuring the cost-effectiveness of Id&AM approaches)
- interoperability (ensuring the harmonisation of approaches through the use of standards, protocols, guidelines and agreed best-practices to ensure inter-working between Id&AM environments for the benefit of agencies and users).

The first two are of most importance at an agency level. The third is important in an agency-cluster and whole-of-government context.

The Framework is intended to cover all 'human' classes of users of information including government employees, contractors, service providers, suppliers and business and citizen customers along with the agents for these. The Framework is also seen as broad enough to encompass treatment of technology-based 'users' (eg hardware, applications).

The Framework is exclusively focused on the 'electronic' environment – ie one in which information and/or services and/or assets may be 'accessed' by gaining access to computers across telecommunications networks.  Many of the key principles and processes could and should be applied to the 'non-electronic' instances of Id&AM as well.

While the Framework factors in the business environment and key drivers of the Government, it has not been framed to take account of the current (As Is) environment (as summarised in the *Findings and Conclusions* report), nor does it provide guidance on the impacts that the implementation of the Framework will have on agencies, nor the key steps that should be taken in implementation.  These matters are left to the companion document, the *Id&AM Action Plan*.

The development of the Framework and the *Id&AM Action Plan* have been tempered by the consideration of privacy and public policy issues, and has sought to take into account the acceptability of the impacts on the organisations and people affected by it.  It is important that agencies approach the implementation of the Framework with the same mindset.

# 1. Introduction to Identity & Access Management

## 1.1. Importance of Identity & Access Management

This section examines the factors that make an improved approach to Identity and Access Management increasingly essential. The Framework is intended to assist agencies and the WoWAG in achieving these improvements.

The knowledge of who is requesting services and their authority to access these services has long been a fundamental element of the effective operation of internal government systems and in the provision of government services to the general population of individuals and organisations.

The need for, and extent of measures taken to establish certainty of identity, and the access rights of such identities, is a matter of judgement that will be affected by:

- The impact of acting on a false assumption of identity and the extent to which other control systems and measures can identify and remedy any ramifications. The negative impacts could include:
  - compromising privacy and personal safety;
  - financial risks;
  - legal risks;
  - reputation risks.
- The costs of implementation of the appropriate identity authentication, access control and audit measures.
- The suitability of these measures for particular user categories, addressing usability, privacy and other public policy considerations, and business case aspects.

These factors apply regardless of whether the services are delivered fully electronically, remotely via telephone or facsimile, or face to face.

Historically, as business systems were developed and services delivered electronically these issues of user identification and authority, and the associated risks of “getting it wrong”, were handled implicitly within each business system domain and solutions were tailored to the specific constituency that utilised the services.

The explosion in electronic service delivery globally sees governments and large private sector organisations facing a number of issues that are rapidly driving change from this multi-siloed approach to one of managing their diverse user base in a coordinated and consistent manner across the entire organisation.

These issues include:

**Increasing threat levels from external parties**

The range and ‘value’ of services delivered continues to expand (this is true in an agency and WoWAG context) and presents a more attractive and larger target for malicious and fraudulent attack.

We are experiencing an increasingly hostile global environment where systemic and targeted attacks on government and private sector computer systems are becoming common place and are technically within the capability of potentially millions of people globally.

The scale and speed of attacks that can be mounted presents enormous problems in timely detection and impact management.

The geographic and jurisdictional remoteness of many attacks further complicates detection, and law enforcement.

**A drive to greater integration of business systems**

Many services are becoming cross-agency, cross-government and even cross-jurisdictional. This is in turn driving the formation of even more identity domains with the need to meld identities known to one domain into the broader operational environment.

Usability, administration and governance are all affected by *weakest link* issues.

**Multiple services take-up by both internal and external users**

Users are becoming flooded with different identities and credentials required for access to systems supporting their work, personal business and recreational activities.

Increasingly this results in poor user perception, impacted usability and additional help desk costs.

**Requirements for increasing flexibility of organisational structure**

There are increasing demands to disassemble and re-assemble organisations and related business systems to adapt to different political, market or regulatory requirements.

Existing agency or business systems approaches to identity management make re-alignment of applications and users difficult and potentially overtake benefits that might have occurred otherwise.

**Decreasing ability to manage services and online access to them**

Increasing deployment of systems with their own independent user management facilities poses serious issues for operational risk personnel who seek a top down view of access permissions (and various combinations of these) and their enforcement.

Handling day to day staff movements and organisation structural changes is becoming increasingly complex with no effective single point of monitoring or control across the enterprise.

## 1.2. Foundation Definitions

The area of Identity and Access Management is beset by multiple interpretations of each term individually and the collective of the two terms.

In addition the confusion of the notion of 'identity' (ie an instance or view of a person or organisation) with 'entity' (the person or organisation) leads to a range of 'problems' (eg those related to privacy).

An essential pre-condition for establishing and agreeing an Id&AM Framework is to gain agreement on the precise meaning of key terms to be used within the Framework.

Clarification of the concepts of 'entity' and 'identity' are provided below. This is followed by definitions for each of Identity Management and Access Management.

A Glossary of terms used within this report, and others germane to the area of Identity and Access Management is provided in Appendix A.

### 1.2.1. The Concepts of 'Entity' and 'Identity'

The clarification of 'entity' from 'identity' is important from a privacy perspective as requirements to authenticate 'identity' often make the un-required leap to 'entity'.

An entity is something that exists in the real world. It encompasses all manner of real-world things, including people, and 'legal persons' such as corporations, trusts, superannuation funds, and incorporated associations. An entity has a range of characteristics, features or attributes.

An identity is a presentation of some underlying entity, such as that associated with some role the entity performs. An identity also has a range of characteristics, features or attributes.

The presumption is often made that an entity has a single identity. In fact, it may have many, and human entities almost always have multiple identities. This is because people perform many social, economic and political functions, as citizens, consumers, sole traders, members of unincorporated business enterprises, employees and contractors; and as agents both for other natural persons and for legal persons such as associations and corporations.

Many individuals are known by different names in different contexts. In some cases, the intention is dishonourable or criminal; but in most cases the adoption of multiple personae is neither, but rather reflects the diversity of contexts in which they act. These include within their family, their workplace(s), their profession, community service and art. In common law countries, people are in no way precluded from using multiple identities or aliases. Actions that take advantage of multiple or situation-specific identities in order to cause harm or circumvent the law are, on the other hand, criminal offences.

Even within an organisation, it is normal for a single human entity to play many roles. A person may hold a substantive position, but may be acting up, or sideways, and may be performing two or more such roles at the same time. A person may switch into such roles as fire warden, first aid officer, selection committee member and disciplinary process delegate, and may do so with or without giving up some or all of their other roles.

Some of these role-changes are controlled by a human resources authority, but many are not, and many could not be, because they are operationally-determined (e.g. by the outbreak of an emergency). Many roles are occupied by multiple people, successively, or at the same time, or during an overlap handover/takeover period.

A further challenge is that care must be taken in associating data with the correct thing, i.e. entity, identity or role. This is of especial concern where the data is sensitive, or the data could give rise to recriminations or reflect negatively on the person it is associated with.

In short, identity management, identity-based access management, and role-based access control (RBAC), are all complex matters.

### 1.2.2. Identity Management

The definition provided by David Temoshok, Director, Identity Policy/Management, US Government GSA Office of Government-wide Policy is regarded as suitable:

> *"Identity Management is a set of policies and supporting processes and infrastructure, for the creation, maintenance, and use of identities and their attributes, credentials, and entitlements. [It]*
>
> - *Involves policy, technology and process*
> - *Must enable enterprises to create a manageable life cycle*
> - *Must scale from internally facing systems to externally facing applications and processes"*

### 1.2.3. Access Management

A variation of the above definition is used:

> *"Access Management is a set of policies and supporting processes and infrastructure, for the establishment, maintenance and disestablishment of user access permissions relating to information and/or services/applications and/or assets. [It]*
>
> - *Involves policy, technology and process*
> - *Must enable enterprises to create a manageable life cycle*
> - *Must scale from internally facing systems to externally facing applications and processes"*

## 1.3. Evolution of Identity Management as Core Business Infrastructure

The issues nominated in the Preamble have led governments and businesses globally to the view that a more structured and organized enterprise-wide approach is required for managing and controlling the "who, when, what, why and how" of user access to 'corporate' resources including those accessible through networks.

As a result there has been a recent, but rapid evolution and maturing of so called *Identity and Access Management* as an enterprise-wide function encompassing *policies, processes, systems* and *technologies* that address the operational risks, systems usability, and technology management issues surrounding internal and external user access to systems at an enterprise level.

Within technology platforms, the recognition of Id&AM as a separate function has its precedents in the previous and now widely accepted practice of unbundling major functional elements such as communications and database management from within business applications. This has enabled enterprises to separately manage infrastructure in order to standardise, optimise, and potentially share the component policies, processes, technologies and systems across all enterprise business application areas.

Moreover, an Id&AM approach leads to a shift in systems design and management from one of *application centricity* to one of *user centricity*.

This 'new' Id&AM paradigm seeks to:

- abstract identity authentication and permissions management from the legacy of previous siloed development of systems and their access mechanisms;
- link access to the role or roles that an identity plays leading to the increasing architecting and deployment of role based access control (RBAC) approaches;
- automate the establishment, maintenance and disestablishment of user authentication credentials and application access rights through the adoption of pan-system provisioning and deprovisioning applications.

## 1.4. Western Australian Government Context

Western Australia's e-Government Strategy (see 1.5 below) is focused on improving service delivery, increasing the internal efficiency of the Government and increasing community participation.

Beyond this implementation of e-Government, the WA Government is also involved in implementing a wide range of significant whole-of-government, joined-up-government and shared services initiatives.

Establishment of the environment necessary to support the above requires that a range of security and management concerns be addressed including that of Identity and Access Management (Id&AM).

Addressing the Id&AM issue is seen as particularly important given the range of shared services (eg Shared Corporate Services Program), whole-of-government (eg whole-of-government directory and IP Telecommunications) and joined-up government (eg TRELIS, SLIP, CJIP[1]) initiatives that are currently in train. These cover facilities including collaboration tools, records management, library/resource sharing, intranet, email gateways, call centre services, directory services and IP-based telecommunications.

In response to the above, the Office of e-Government has committed to the development an *Identity and Access Management Framework and Action Plan* for the Western Australian Public Sector. This report presents the *Framework.*

The Government's goals in this regard are to enable:

- Greater information sharing and collaboration between agencies.
- More efficient management of resources across government (including effective workforce planning).
- Smoother transition for machinery-of-government changes.
- Secure and trusted transaction and information sharing environments, both within government and with external public and private sector environments.
- Reduced expenditure of funds, time and effort in the production and dissemination of information.

[1] Transport's Executive & Licensing Information System, The Shared Land Information Platform and the Criminal Justice Integration Project.

- A more whole-of-government rather than agency-centric approach to the business of government.
- Improved service through enabling users to use the same identity and authentication credentials across services within a department and across government.

The Framework (and the companion reports) build upon an earlier report, *Position Paper for the Foundations of Whole-of-Government Identity and Access Management for the Western Australian Public Sector* (see section 1.7 below).

The Government is adopting an enterprise architecture approach to the planning, architecting and evaluation of its technology portfolio (see 1.6 below) and requires the contextualisation of the Framework within the Enterprise Architecture.

## 1.5. e-Government Strategy

The e-government vision for Western Australia that underpins this Strategy is: A *more efficient public sector that delivers integrated services and improved opportunities for community participation.*

By definition the implementation of integrated approaches will require at least a harmonisation of approaches to Id&AM or more probably, in relation to the more advanced joined-up service initiatives, a formalised technically joined-up approach based upon a 'scheme' or 'federated' approach to authentication and access control. See section 4.2 and Appendix B for further discussion on these Id&AM models.

Other perspectives that add weight to a harmonised or aggregated approach to the authentication and access management for e-government services across all agencies relate to:

- the savings in capital and operating costs that can be achieved by rationalising elements of the Id&AM process/technology stack; and
- the simplification of management of credentials for end users, whether businesses or citizens, that have a requirement to interact with multiple agencies.

## 1.6. Enterprise Architecture

The WA Government is planning to use an Enterprise Architecture (EA) approach to the definition, planning, implementation and benchmarking of its approach to ICT and the implementation of its e-Government Strategy. The EA approach is intended to encompass:

- Business Architecture.
- Information Architecture.
- Application Architecture.
- Technology Architecture.
- Enterprise Architecture Management and Project Evaluation**.**
- Funding, Procurement and Review**.**

Security and privacy, key components of a complete and unified Id&AM approach, play into each aspect/layer of the EA and will need to be considered by agencies and at an extended-enterprise level at a whole-of-WA Government level. This area is examined in further detail in section 4.

## 1.7. Learnings from previous Id&AM Position Paper

The Office of e-Government has developed a *Position Paper for the Foundations of Whole-of-Government Identity and Access Management for the Western Australian Public Sector*.

The paper highlights that, at present, in relation to government employees and contractors:

- There is no consistent approach to establishing and then managing identity. Each agency has its own policies/procedures and provides its own infrastructure and solution to support identity/identification, authentication and access control.

- There are no government-wide standards or policies governing how these individuals are then given access to the information held by government.

The report notes that the same is true for those within the community, both business and citizen, who interact with government. This results in the probability that citizens who transact with multiple agencies may need to re-establish their identity when dealing with each agency.

This lack of consistency in managing identities and their access rights across government is seen as leading to inefficiencies in the way that government operates and delivers services to the community.

These findings were corroborated during the 'As Is' phase of this project – see *Findings and Conclusions* report.

## 1.8. Privacy Law

The consideration of the privacy and public policy impacts of the proposed Id&AM Framework have been seen as important to ensure its 'legality' and acceptability to individuals both inside and outside of the Western Australian Government.

While consideration of the privacy and public policy implications of the Id&AM initiative has been complicated by the absence of any comprehensive privacy law in Western Australia, these matters have been addressed both in this report (section 4.6 and Appendix H) as well as in the *Id&AM Action Plan.*

# 2. Introduction to Identity & Access Management Framework

## 2.1. Scope and Positioning

The Id&AM Framework is intended to provide the context for the definition of those core policy, governance, commercial (eg business case), technical and operational elements of Id&AM that are required to facilitate consistency of the approach to **identity** across all aspects of users' online dealings with Government across all electronic channels including:

- Registration & enrolment of users[2]
- Creation of identifiers
- Classification of applications
- Authentication of users
- Authorisation of transactions
- Administration (including Tracking and Reporting)
- Audit.

### 2.1.1. Inclusion within Id&AM Framework

The Id&AM Framework includes:

- Authentication, authorisation and audit (ie not just authentication)
- Authentication of assertions that are related to persons including assertions of entity, identity, role, persistent pseudonymity and anonymity.
- Coverage of internal and external users.
- Coverage of agency, agency-cluster and WoWAG contexts.

### 2.1.2. Exclusions from Id&AM Framework

The Id&AM Framework excludes:

- Authentication of assertions related to value, qualification and other attributes and the 'nil condition'[3].
- Management of identities in relation to physical access control (eg premises).
- Coverage of Enterprise Architecture other than positioning Id&AM within the EA stack.

### 2.1.3. Positioning relative to Enterprise Risk Management and Information Security Management Systems

Agencies need to have in place a formal standards-based Enterprise Risk Management plan/strategy and Information Security Management Systems plan.

The Id&AM Framework provides a view across the territory covered by Enterprise Risk Management approaches and Information Security Management Systems, but drills down into more detail on identity and access related matters than either of the former.

To assist agencies, a synopsis of *National and International Standards and Guidelines* and *Information Systems Security Context* are provided in Appendices E and F.

[2] This encompasses establishment of 'delegation' where appropriate.

[3] For the sake of completeness the WA Government Authentication Framework, a component of the WA Government Id&AM Framework, provides some coverage of these non-identity based assertions.

## 2.2. Synopsis of the Framework

Diagram 1 below depicts a Framework for Identity and Access Management (Id&AM). This Framework has been developed based on contemporary thinking and developments within the subject area and in particular, developments within other governments in Australia. Where appropriate the Framework has been finessed to meet particular aspects of the WA Government and its agencies.

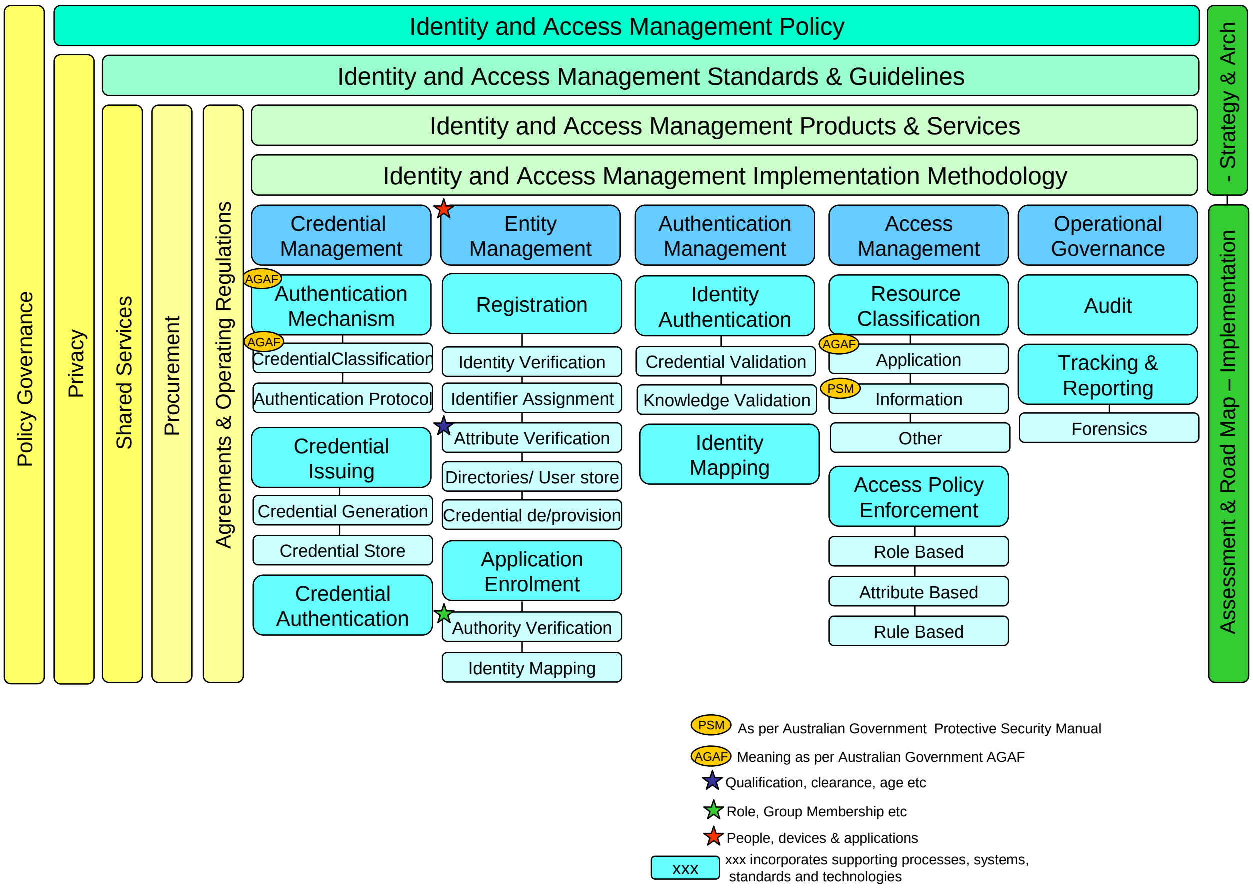


**Diagram 1 - Id&AM Framework**

The Framework is technology, architecture and business process neutral and has been developed to accommodate varying implementation models for Id&AM as they emerge over time.

The Framework draws upon existing better-practices in this area as defined by the Australian Government's Authentication Framework (AGAF), and its supporting Guides[4], and the Commonwealth Protective Security Manual (PSM) in specific areas.

The Framework incorporates:

**Strategy and Architecture Components**

- An Id&AM Policy incorporating the minimum requirements for the protection of government assets against unauthorised electronic access.
- Standards and Guidelines to support implementation and ongoing observance of the policy.
- Products and services that implement the standards along with a Methodology for implementation of policy within the enterprise.

[4] See http://www.agimo.gov.au/infrastructure/authentication/agaf

### Governance and Operational Components

- Overarching governance approach for the implementation and operation of the Id&AM Policy across government. This would include mechanisms to assess the level of adoption and implementation of the Id&AM Policy within government.
- Shared Services that may be leveraged by a number of government agencies. Services could include know-how, processes and operating infrastructure.
- Procurement and Capital Expenditure rules/guidelines, processes and services (eg common use contracts or shared services arrangements) to maximise economic and user outcomes, to reduce the risk of obsolescence and to 'ensure' interoperability.
- Privacy policy management in the context of identity management, including the need or otherwise for the completion of Privacy Impact Assessments

### Functional Components

These components support the implementation of the Policy. The proposed Framework has been developed to accommodate changing needs and the emergence of new technologies and business practices over time.

Where practical, the Framework draws upon other contemporary work completed in Australia and in leading jurisdictions internationally. These are referenced within the diagram and detailed in the diagram legend.

As also described through the legend (in diagram 1), the functional components identified embrace processes, systems, standards and technologies.

Each of these components is describe in detail in the sections below.

## 2.3. Identity and Access Management Lifecycle

Diagram 2 provides a birds-eye view of the Id&AM lifecycle showing once-off, periodic and repetitive events. The diagram also shows the abstracted elements of the underlying technology architecture, in order to contextualise what applications and data stores are involved in which events.

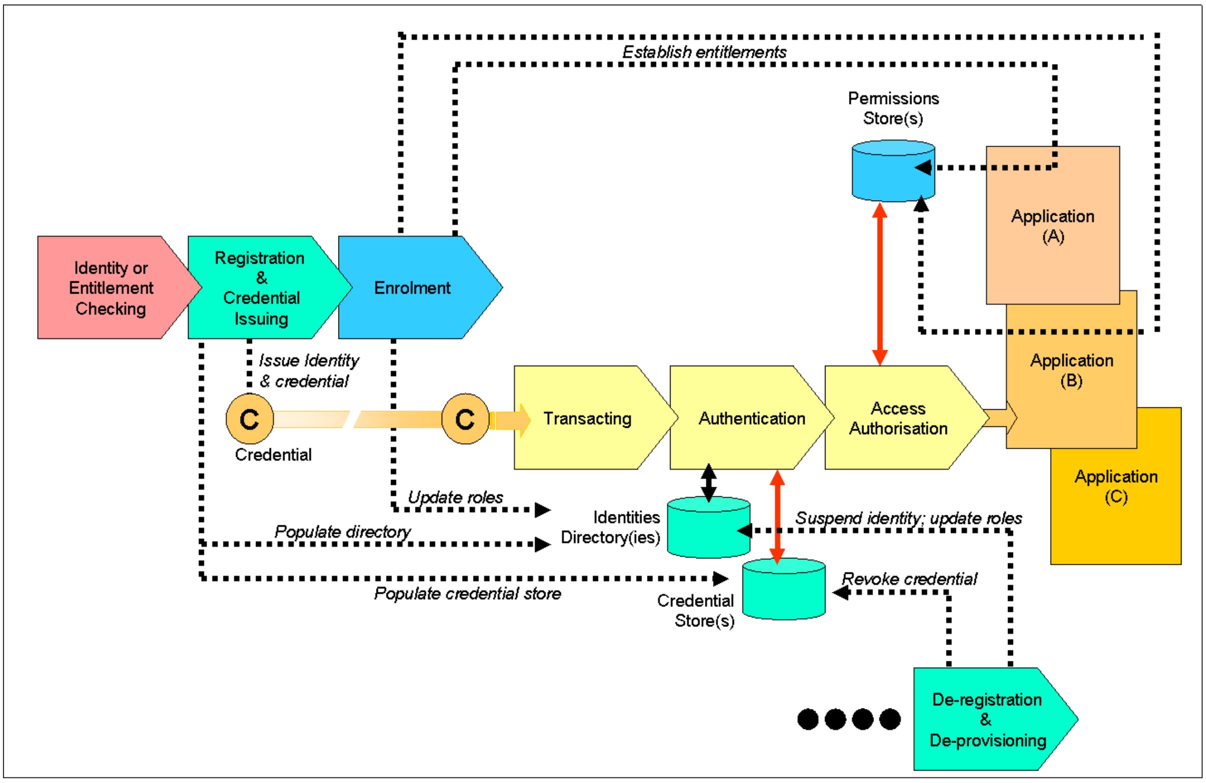


**Diagram 2 - Id&AM Lifecycle**

# 3. Major Planks of the Framework

## 3.1. Introduction

This section discusses the major planks of the Framework as illustrated in the diagram below:

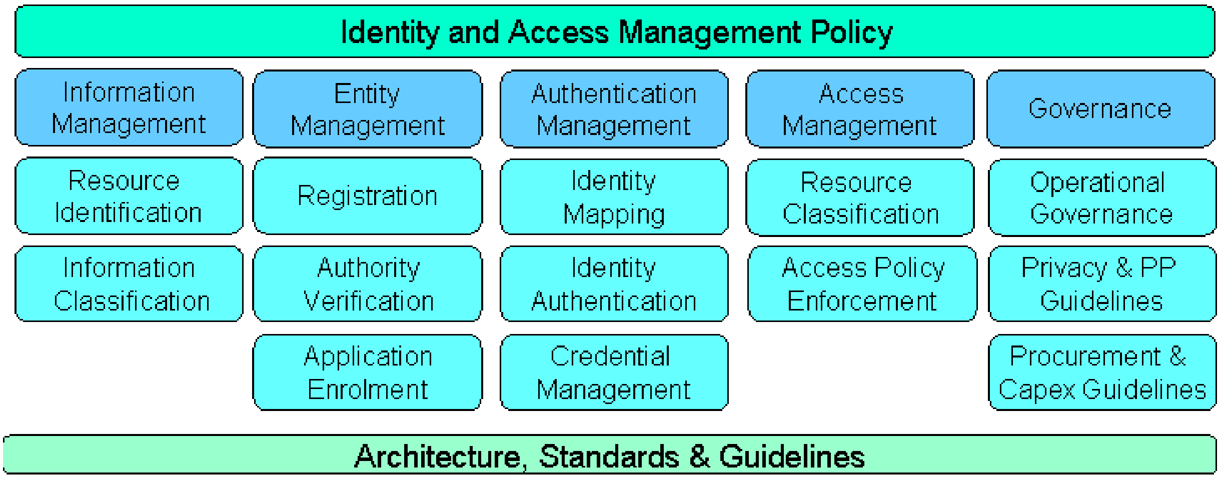


**Diagram 3 - Id&AM Framework**

## 3.2. Entity Management

Entity Management refers to the group of processes that support the:

- provision (and de-activation) of an authentication credential to a user and
- the enrolment of, and granting of authorities to, the user in respect to various application, systems or resources.

These major functions are shown within diagram 1 above as:

- Registration - including conducting evidence-of-identity (EOI) or evidence-of-relationship (EOR) validation in most cases.
- Authority Verification.
- Application Enrolment/De-enrolment.

While often completed as part of a single process, each of these functions is relatively independent of the others, albeit the implied sequence typically applies.

Moreover, these major functions are essentially user "activation" tasks that unlike day to day application access and transacting are completed infrequently during a user's lifecycle.

### 3.2.1. Registration

User registration will typically incorporate all or some of the following elements:

- The verification or checking of identity documentation in order to achieve a level of confidence in the identity of the individual or business or its representative that is otherwise unknown. This might include:
  - face-to-face contact and the sighting of original documentation such as company registration information, passports, drivers licence etc.
  - reliance of checks already completed by another agency or trusted third party
  - online validation of a pre-existing relationship determined through knowledge-based authentication of the relationship.

  The exact nature of the checking will depend on the assurance level that is required in respect to the veracity of the claimed business identity.

The Financial Transactions Reporting Act (FTRA) provides guidelines on minimum identification methods for the financial sector, often referred to as 100 point checks. These and similar checks are in broad use across a range of industries and are the subject of ongoing review and refinement to ensure continuing confidence in their use.

The Australian Government Authentication Framework (AGAF) and its associated *Better Practice Guides* provide guidance on the requirements for assignment of assurance levels to the identity verification process.

- The assignment of an identifier for the user which is unique within the domain.
- Where required, the collection and / or verification of 'attributes' of the user. These can vary widely depending on any provisions made for attributes within the Id&AM Policy. Within the WA Government environment, attributes might well be used for maintaining security clearance, police check status, or other individual specific information that may be of use across agencies.
- The issuance of a credential to the individual or business that will be used as the key element of subsequent online authentication of the user. Details of the credential, and methods of validation, will be held in a directory or user store. A credential can include a password, a token of some kind such as a smart card or one-time-password device, or a digital certificate.

  Authentication Mechanisms, incorporating the selection and use of credentials are dealt with in more detail in Appendix C.
- The creation of user entries in a directory or user store that will provide an electronic record of the user or business' identity and any associated information to be used in subsequent maintenance of the directory. This electronic record should ideally also maintain information or indexes to information detailing the checks (eg EOI) that were completed as part of registration.

  This directory will typically be maintained by the issuer of the identifier and may include information provided as part of the registration process that is privacy sensitive (this will be more germane in an individual as opposed to a business context).

  The extent and availability of this registration related information to relying parties needs to be considered carefully where an identifier is to be used openly across government agencies, or more broadly.

User registration can be completed by a government agency, on behalf of government agencies (as in the WA Government *Shared Services* environment) or increasingly commonly for business, by third parties that issue credentials that can be utilised to authenticate users to a range of organisations. Examples of the latter include:

- Verisign, as a Gatekeeper certificate issuer and an ABN-DSC issuer, is an example of a non-government individual and business credential issuer.
- HeSA[5] (Health eSignature Authority), as an issuer of certificates to health service providers, including individuals and businesses.
- Private sector issuers such as banks who internationally are issuing credentials to businesses and individuals designed for third party use.

In many situations it is likely that agencies dealing with businesses may elect to delegate the user registration of business employees, and potentially the issuance of the related credential, to an authorised party within the business. The extent to which such identities can be relied upon outside of the specific application domain needs to be carefully considered and is ultimately defined by policies analogous to agency-issued identities and credentials addressing the liabilities and obligations of the various parties.

[5] HeSA is a federal Health Information Commission (HIC) initiative. Limited use of HeSA certificates planned within the WA Department of Health.

### 3.2.2. Application Enrolment & Identity Mapping

User enrolment into an application system is a one time activity that provides a user with authorised access to specific application and information resources.

Application enrolment needs to accommodate two types of users:

- users that have registered within the application's domain and thereby are "known" within the domain and have an identifier and credential that is recognised within that domain.
- users that have registered within another agency's domain, or within a trusted external domain, and thereby are initially unknown within the application domain, and have an identifier that is potentially meaningless outside the issuing domain.

For the first category of user, enrolment proceeds as a **natural extension of the registration process** described above. In this case, which is typical in an employee registration, the user will be issued with a credential and, based on verification of user authorities, will be given access permissions to access various agency applications and information resources.

The assurance level of the credential used in this context is well understood by the agency as the agency was the issuer of the credential and previously completed all elements of the registration and issuance processes.

Whilst there is a logical separation of registration and enrolment within the entity management systems, to the user, registration and enrolment steps would be seen as a seamless processes and indistinguishable from one another.

For the second category of user the enrolment method requires the mapping of an externally issued identifier into the application's domain as is the case in a federated identity management environment.

Issues that need to be considered from an application owner's perspective in supporting this type of user access include:

- The suitability of the authentication mechanism associated with the identifier, addressing both the robustness of the identification process and the strength of the credential (password, token, smart card etc) as described in Appendix C.
- Accessibility and ongoing availability of credential validation services from the issuer of the credential.
- Commercial and legal issues, including liabilities, relating to reliance on the identifier and associated authentication mechanism.
- Broader consideration of the agency's online deployment strategy, taking into account the number of third party credentials issued by various issuers and the extent of overlap of the credential holders with the particular agency application concerned

Once the authentication mechanism has satisfied the 'fitness-for-purpose' test, processes need to be developed to link the credential holder with the agency's 'instance' of, or knowledge of, the credential holder. These may take the form of an alternate identifier, and/or a user record/entry in a database or directory. This might involve the mapping of, say, a digital certificate to an account number, licence number or other internal application based identifier that represents the relying agency's existing record of the business, or representative of the business.

This mapping would be achieved through matching of user details against records held within the agency's application systems. This matching process, or establishment of 'Evidence of Relationship', is similar in affect to the completion of an EOI which is normally done at registration time.

Once the mapping is established through this process, access permissions for various transactions offered by the agency will be established described below.

### 3.2.3. Authority Verification

Authorities relate to specific business applications or groups of applications, and in particular relate to the specific access permissions or privileges granted to a user by the application or information owner (application owner).

Permissions are assigned upon the verification of the authority of a user to undertake specified processes or access specified information. Permissions are typically assigned on a *role*, *group membership* or *rule* basis by the application owner.

The authority verification process may be completed directly by the application owner through, for example, reference to physical authority documents prepared by the HR department.

Alternatively, in the case of businesses, authority verification may be delegated by the application owner to an authorised business representative. Administration of this delegated verification process, and the subsequent assignment of permissions, might be effected through electronic or manual workflows.

Similarly, individuals may delegate their existing authority to deal on their behalf to an agent which may be an individual or business.

## 3.3. Information Management

### 3.3.1. Significance of Information Management to Id&AM

Id&AM is intended to ensure that entities gain access to only information (and services and assets) to which they are entitled.

The determination of who gains access to information is largely determined by the relationship between the entity (and possibly their role) and the information.

The protection of information is often seen as falling within the process and systems that make up an Id&AM regime. This perspective fails to appreciate the vital role that Information Management plays in the early and ongoing determination of the fundamental rules that govern information and its disposition.

Information has certain intrinsic characteristics that need to be tightly coupled with the information irrespective of the form it is in or the location. These characteristics or attributes relate to:

- Ownership – who is the fundamental owner of the data.
- Guardianship – who is the guardian or custodian of the data.
- Sensitivity – how sensitive is the data from a privacy, commercial or other (eg national security) perspective. This is handled by classifying the data.

These attributes will play a major role in determining who is able to access the information to add, view, alter or delete it. They should be created when the data set is initiated, 'travel' with the data set and be referenced whenever decisions are made regarding the data set – eg creation, maintenance or decommissioning of datastores and/or the applications that access such stores.

### 3.3.2. Information Classification and Control

For Id&AM to have integrity it is essential that agencies have a consistent approach to the classification and control of all information.

ISO-IEC 17799 – 2000, *Information technology code of practice for information security management* provides an appropriate framework within which agencies should approach this matter.

This commences by noting that:

- "[i]nformation is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected."
- Information security is characterized here as the preservation of:
  - a) confidentiality: ensuring that information is accessible only to those authorized to have access;
  - b) integrity: safeguarding the accuracy and completeness of information and processing methods;
  - c) availability: ensuring that authorized users have access to information and associated assets when required.

It continues:

- Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. All major information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.
- Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.
- Procedures for the handling and storage of information should be established in order to protect such information from unauthorized disclosure or misuse. Procedures should be drawn up for handling information consistent with its classification.

Section 5, *Asset classification and control*, describes the requirement for:

- [undertaking an] Inventory [of information assets]
- [undertaking] Classification [of information assets]
- Information labelling and handling.

Information/data classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled / secured and is also indicative of its value in terms of Business Assets.

The classification of information should be guided by:

- The views of the owners of the data and representatives and advocates for such owners.
- State and national and in some cases international laws (eg Archives Acts, Privacy and Data Protection Acts).
- Contractual requirements.
- National and international standards and best practices.
- Economics / costs (subject to the above criteria taking precedence).

Leading organisations now implement *Information Lifecycle Management* (ILM) that depends critically on data classification. In order to manage the enterprise data throughout its life cycle, the enterprise must establish what kinds of data it is managing and what policies to follow in regard to it.

### 3.3.3. Classification Schema

There is a requirement for the agencies to adopt a standardised approach to the classification of information. Without this a key foundational component of Id&AM will be missing.

OeG has previously made a recommendation to all agencies indicating that where there is a business requirement to adopt a data classification scheme, then the recommended scheme is that outlined in Part C of the *Commonwealth Protective Security Manual* (PSM).

The PSM was developed and is maintained by the Protective Security Policy Committee operating under the aegis of the Attorney-General's agency, in particular, the department's Protective Security Coordination Centre.

The PSM 'sets out the policies, practices and procedures that provide a protective security environment that is not only fundamental to good business and management practice, but essential for good government. It also lays down the procedures designed to ensure that agencies and departments approach protective security measures in a way that is consistent across government'.[6]

Excerpts from the PSM are provided in Appendix D.

Part C (Information Security) of the PSM defines:

- three classes of information:
  - Public Domain
  - Unclassified
  - Classified – divided into national security and non-national security categories.
- four categories of national security classifications:
  - Restricted
  - Confidential
  - Secret
  - Top secret.

While the PSM may provide an appropriate broad framework in relation to information security management its classification schema, aspects of its Commonwealth Government-centricity are problematic.

It may also not be sufficiently granular to meet the operating requirements of most WA agencies when attempting to support Id&AM schemes applicable to all classes of information and users.

Alternatives need to be examined, and, possibly developed. Appendix J contains an excerpt from the *Data Security and Classification Guidelines* of the University of Massachusetts by way of an example.

## 3.4. Authentication Management

Authentication Management refers to the group of processes that support the authentication of a user identity and, for federated environments, the subsequent mapping of the authenticated identity to a previously linked identity within the application system domain.

### 3.4.1. Identity Authentication

Identity Authentication can be achieved through either:

- Validation of an electronic credential using a defined authentication protocol; or,
- Knowledge based authentication.

Credentials include passwords, tokens, smart cards etc and are issued by the associated user registrar, for example WA Government's pending Shared Corporate Services in the case of many WA Government employees.

Knowledge based authentication requires the user to respond to user specific information challenges from the authentication service which can be tailored to meet the assurance needs of the application.

Knowledge based authentication is typically used as part of application enrolment and identity mapping or to support the automated provisioning of token based credentials to existing users where their current credentials (say password) are considered of too low assurance to underpin the issuance of a higher grade credential such as a token.

[6] Excerpt from Foreword to the PSM 2000.

Identity authentication is generally completed at the commencement of a session, but increasingly two unrelated trends are emerging:

- Application systems are implementing processes that require re-authentication of users at critical points within a session in order to ensure the authenticated user is still present.
- Application systems are prepared to “trust” user authentication completed elsewhere, provided suitable evidence of this authentication can be passed to them securely and the authentication was recently completed. Whilst this is the basis of and is fundamental to “federated identities”, it is also applicable within traditional single domain environments.

To support this, credential issuers are required to provide an authentication service and interfaces to enable the validation of credentials which is usually completed through an “authentication protocol” executed between the authentication service and the user/credential. The outcome of the validation is passed to the requesting service in a secure and trusted manner and standards such as SAML are increasingly used to communicate these outcomes.

### 3.4.2. Identity Mapping

Once an identity is authenticated, or is passed to an application as an authenticated identity in a federated model, the identity is mapped onto the “application specific” identity.

This mapping may be completed as a part of the Id&AM Framework or, less likely, as an integral part of the application system.

As it is probable that both situations will exist, or be required, and the Framework needs to accommodate this mapping functionality.

## 3.5. Access Management

Access management has two major elements:

- The classification of the **identity authentication** assurance requirements relating to the application system or information to which access is requested.
- The enforcement of the of the user access policy for the specific application or information resource.

### 3.5.1. Application Classification

For the purposes of the Framework an *application* is considered a combination of processes and information resulting in some well defined outcome.

AGAF and other formalised Id&AM frameworks have defined structured methodologies for the classification of the sensitivity of applications which is defined by the impact that might arise from an (identity) assertion being accepted as true when it is actually false.

The AGAF classification is shown below.

| **Level 1 – Minimal Risk** |
|---|
| **Level 1** authentication is appropriate for e-Government transactions in which **minimal damage** might arise from the assertion being accepted as true when it is actually false. This might result in at most:<br>▪ minimal inconvenience to any party; or<br>▪ no risk to any party’s personal safety; or<br>▪ no release of personally or commercially sensitive data to third parties; or<br>▪ minimal financial loss to any party; or<br>▪ no damage to any party’s standing or reputation; or<br>▪ no distress being caused to any party;<br>▪ no threat to agencies’ systems or agencies' capacity to conduct their business; or<br>▪ no assistance in the commission of serious crime or hindrance to its detection. |

**Level 2 – Low Risk**

**Level 2** authentication is appropriate for e-Government transactions in which **minor damage** might arise from the assertion being accepted as true when it is actually false. This might result in at most:

- minor inconvenience to any party; or
- no risk to any party's personal safety; or
- no release of personally or commercially sensitive data to third parties; or
- minor financial loss to any party; or
- minor damage to any party's standing or reputation; or
- minor distress being caused to any party;
- no threat to agencies' systems or agencies' capacity to conduct their business; or
- no assistance in the commission of serious crime or hindrance to its detection.

**Level 3 – Moderate Risk**

**Level 3** authentication is appropriate for e-Government transactions in which **moderate damage** might arise from the assertion being accepted as true when it is actually false. This might result in at most:

- significant inconvenience to any party; or
- no risk to any party's personal safety; or
- the release of personally or commercially sensitive data to third parties; or
- significant financial loss to any party; or
- significant damage to any party's standing or reputation; or
- significant distress being caused to any party; or
- moderate threat to agencies' systems or agencies' capacity to conduct their business; or
- assistance in the commission of serious crime or hindrance to its detection.

**Level 4 – High Risk**

**Level 4** authentication is appropriate for e-Government transactions in which **substantial damage** might arise from the assertion being accepted as true when it is actually false. This might result in at most:

- substantial inconvenience to any party; or
- risk to any party's personal safety; or
- the release of personally or commercially sensitive data to third parties; or
- substantial financial loss to any party; or
- substantial damage to any party's standing or reputation; or
- substantial distress being caused to any party;
- significant threat to agencies' systems or agencies' capacity to conduct their business; or
- assistance in the commission of serious crime or hindrance to its detection.

These Application Assurance Levels provide a threshold for the minimum authentication assurance level requirements for identity authentication for users accessing the applications and as such provide guidance on the credential types that should be used for user identity authentication in applications of various classifications.

### 3.5.2. Access Policy Enforcement

The access policies for an application are defined by the application owner.

This policy will stipulate the conditions of user access to the application or information which might include a combination of:

- Identity authentication assurance level requirement
- User role, such as payroll supervisor
- Membership of a Group, such as help desk
- Specific rules based around such things as user attributes (eg clearance level etc), time of day, location, user identifier etc

The Id&AM Framework recognises that policy enforcement can be implemented over a number of architectural layers as described below.

The extent of policy enforcement that is implemented within an authorisation layer, as opposed to implicitly within the authentication layer, or explicitly within the business application layer needs to be carefully assessed during application design stage.

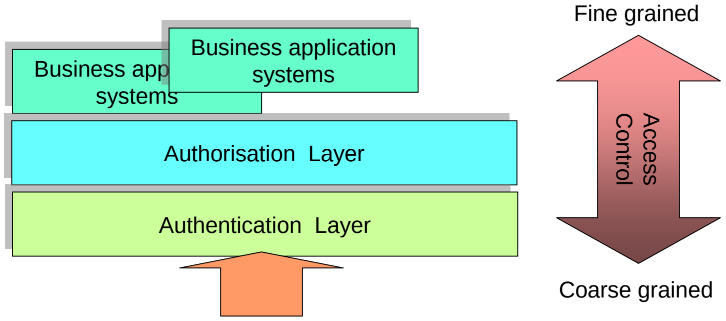


**Diagram 4 - Access Control Layers**

The above illustrates multiple business applications operating through unified authorisation and authentication layers. In this model, as general principles:

- fine grained access is more typically implemented within the business application. Examples of 'fine grained' access controls may include rules relating to individual data fields in a record that may be viewed/changed.
- Coarse grained controls are often implicitly implemented within the authentication systems. Coarse grained control might include validation of authorities that are intrinsic to the credential and identifier, including such attributes as employee, medical practitioner, registered subscriber, authorised officer of a company, an Australian registered company, etc.
- Medium grained controls will predominate and include access controls applicable to an individual and would typically provide control of access (authorisation) to an individual transaction or class of transactions. It is unlikely that these controls would 'interrogate' information held within a transaction to determine permission to access the business application. Role and Group Membership based access would likely be implemented within this layer.

## 3.6. Credential Management

### 3.6.1. Authentication Mechanisms

Credentials are typically issued as part of the user registration processes as described in Section 3.1 and provide a means whereby a user can authenticate their identity electronically to a business application.

In the context of this Framework, credentials include passwords, specialised authentication devices termed tokens which upon request generate one time passwords or other device specific codes, smart cards, digital certificates etc.

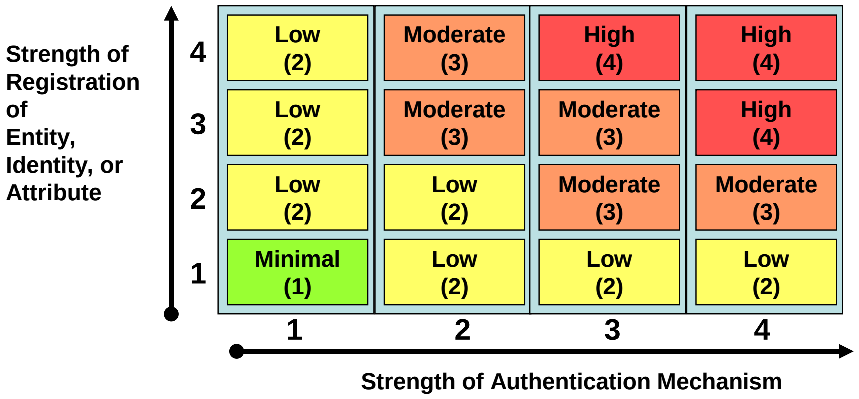
The strength of the identity authentication attained from the use of a credential is a product of:

- The strength and robustness of the identity verification and screening process completed by the registering agency or third party.

- The strength of the *authentication mechanism* which is a product of the physical and logical elements of the credential, such as cryptographic algorithm strength, PIN protection, tamper-resistance etc, and the manner in which the credential is used which is termed the authentication protocol.

This duality is shown in the figure below where the horizontal axis “Strength of Authentication Mechanism” reflects the combined strength of the credential and the authentication protocol.

**Authentication Assurance Level Matrix**



| Strength of Registration of Entity, Identity, or Attribute | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 4 | Low (2) | Moderate (3) | High (4) | High (4) |
| 3 | Low (2) | Moderate (3) | Moderate (3) | High (4) |
| 2 | Low (2) | Low (2) | Moderate (3) | Moderate (3) |
| 1 | Minimal (1) | Low (2) | Low (2) | Low (2) |

Strength of Authentication Mechanism

**Diagram 5 – AGAF Assurance Level Table**

Appendix B provides a more detailed discussion of the authentication mechanism alternatives and their typical applications.

The table below sets out the AGAF recommendations on credential assurance levels.

The Framework recognises that the effective “strength” of authentication mechanisms will change over time as new threats emerge and a review of the currency of the following table is proposed within the *Id&AM Action Plan*, along with the standardisation of credential types for each assurance level across government agencies.

| Authentication Mechanism Assurance Level | Authentication Mechanism Candidates | AGAF |
|---|---|---|
| **Minimal (1)** | None, passwords | None |
| **Low (2)** | Passwords, One Time Password (OTP) Tokens | Passwords |
| **Moderate (3)** | OTP Tokens, PIN protected Tokens, Certificates, Secondary Channel (phone, code book), Knowledge Based | Tokens |
| **High (4)** | Secondary Channel, Certificates, Smart Cards, Biometrics (iris scan etc) | Certificates |

### 3.6.2. Credential Issuing

The issuing of users with their credentials is an important element of the user registration process requiring assurance levels commensurate with the strength of registration and the authentication mechanism. Credential issuance involves the issuance of a credential and the associated access codes (if any) to enable the credential for use within an authentication and permissions management environment.

Areas that need to be considered include:

- The methods of protection of shared secrets such as cryptographic keys from the time of issuance until they are in the certain custody of the end user.

- Methods of activation of the credential upon receipt by the user. This would typically be achieved through some sort of activation code entered into a device such as smart card or token, a phone call to a help desk or IVR centre, or a mailed confirmation.
- The implementation and activation of any special software or equipment required by the credential such as a smart card reader and software, special application software, etc. The ATO's Common-use Signing Interface (CSI) software, used for business aceess, is an example of this requirement, albeit the ATO have decoupled the implementation of their CSI from the credential issuance process.

Difficulties in any of the above areas will result in potentially significant help desk imposts and loss of user confidence in the authentication regime.

### 3.6.3. Credential Validation

Credential validation services are provided by the credential issuer which in most cases also completes all other elements of user registration.

Credential validation is typically completed within authentication servers that are supplied as part of the credential vendor product suite, although increasingly single authentication services are emerging that are able to present a single authentication interface to application systems/portals/access management systems that "brokers" validation requests pertaining to a range of credential types and issuers.

### 3.6.4. Credential Generation and Linkage

The Framework recognises a trend to abstraction of the credential generation and authentication processes from other elements of Id&AM and in particular supports the deployment of credentials that in themselves have no attributes that link them to a particular identifier or identity of a user.

This linkage is instead established within a directory or user store that references the issued credential.

This concept supports a "late binding" of a previously issued credential to a user identity as is implemented within the Canadian e-Government environment using anonymous certificates.

In order that this approach is plausible, credential issuers must (inter alia):

- Provide an independent credential validation service
- Pass control of the management of the token status (for suspension, revocation, etc) to the token holder and provide mechanisms to enable this.
- Ensure the integrity of the issuing service in respect to uniqueness of token identifiers.

## 3.7. Agreements and Operating Regulations

As highlighted and expanded upon in Section 4.3 below, implementation of the Framework in whatever guise, will require the development and implementation of various agreements between end-users, application service providers, and identifier and credential issuers.

These agreements will specify (inter alia) the various obligations and remedies of the participants in respect to liabilities, dispute resolution, privacy, and operational performance.

The *Id&AM Action Plan* sets out major initiatives in homogenising an approach to these agreements across government.

## 3.8. Governance

The I&AM Framework raises many issues that require detailed consideration during its implementation, as well as during the operation of agency and/or shared-services Id&AM solutions, and the ongoing 'maintenance'/updating and 'enforcement' of the framework.

The governance issues raised by the adoption of a WoWAG Id&AM Framework relate to both a WoWAG context and an agency specific context.

The nature of some of the key issues is depicted in the diagram below. NB the position of the slider-bars is intended to be illustrative only.

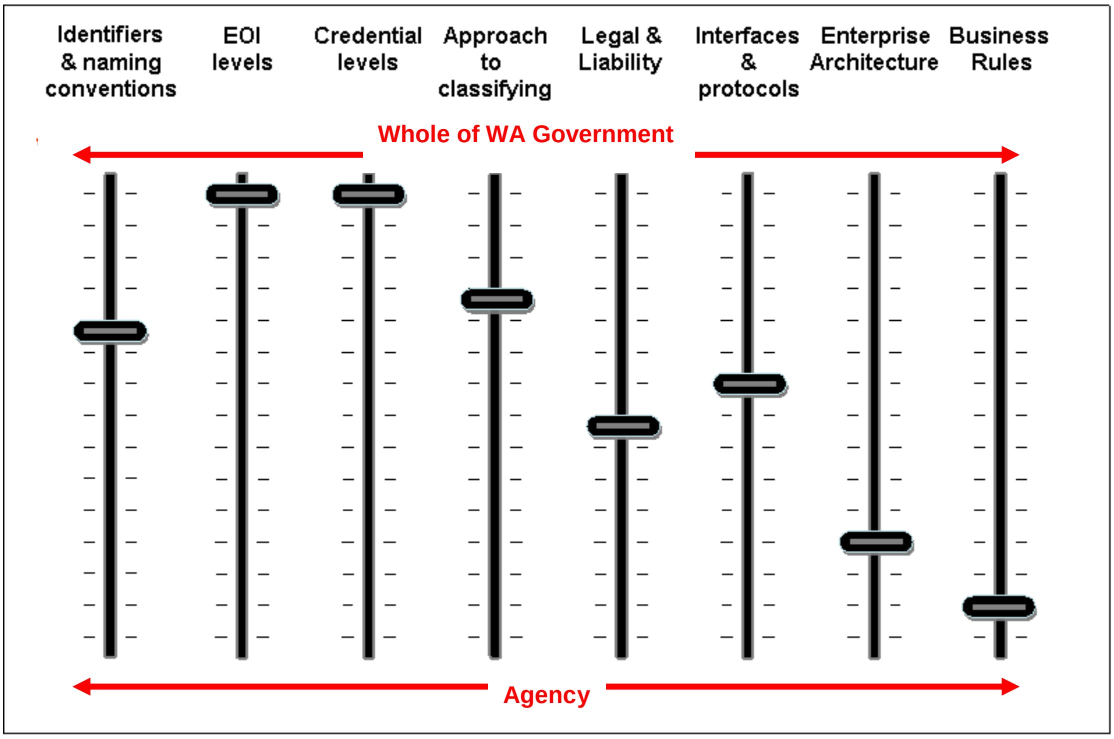


**Diagram 6 - Decision Framework - WoWAG and Agency Issues**

The Id&AM Framework has WoWAG and agency implications. As a result, an approach encompassing two governance domains is required. Diagram 7 below provides a proposed structure covering both governance requirements.

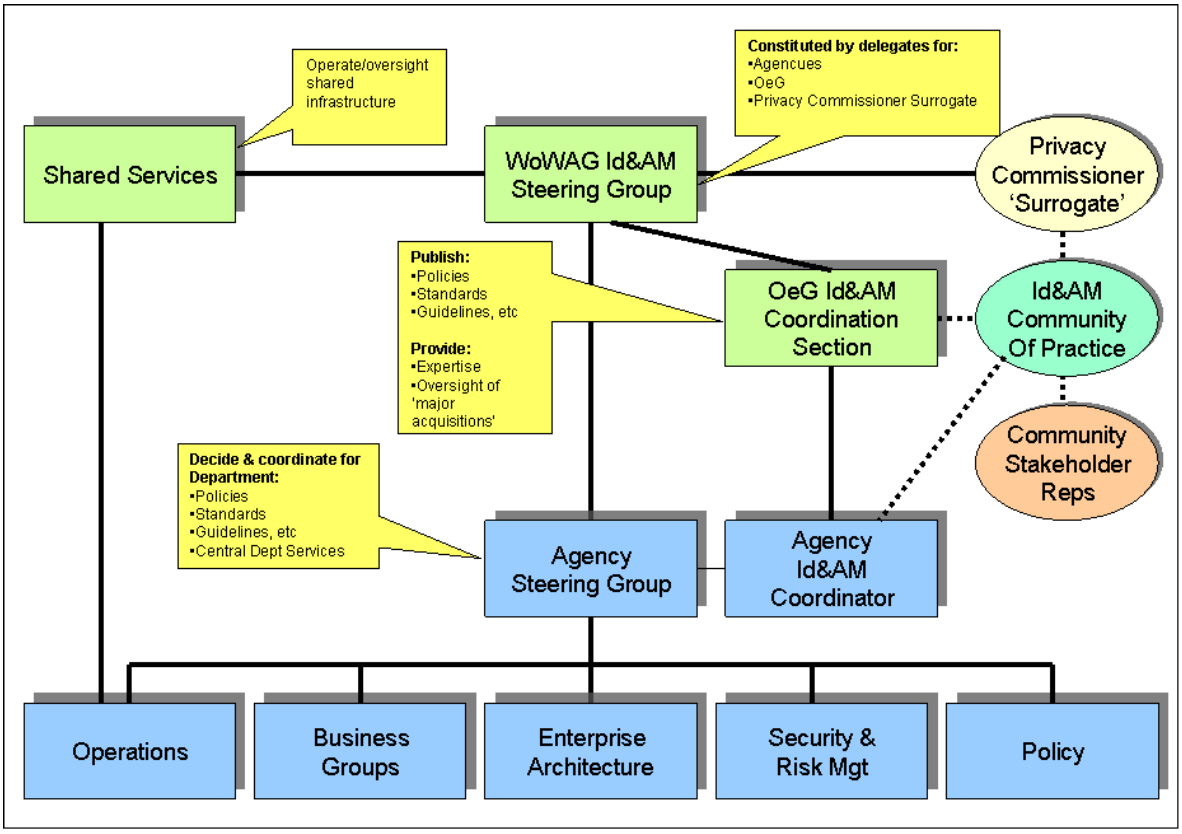

Operate/oversight shared infrastructure
Constituted by delegates for:
•Agencues
•OeG
•Privacy Commissioner Surrogate
Shared Services
WoWAG Id&AM Steering Group
Privacy Commissioner 'Surrogate'
Publish:
•Policies
•Standards
•Guidelines, etc
Provide:
•Expertise
•Oversight of 'major acquisitions'
OeG Id&AM Coordination Section
Id&AM Community Of Practice
Community Stakeholder Reps
Decide & coordinate for Department:
•Policies
•Standards
•Guidelines, etc
•Central Dept Services
Agency Steering Group
Agency Id&AM Coordinator
Operations
Business Groups
Enterprise Architecture
Security & Risk Mgt
Policy

**Diagram 7 - Proposed WoWAG and Agency Governance Structure**

The governance structure particularly that suggested for agencies is intended to be primarily illustrative rather than prescriptive. It may well be that agencies have existing governance arrangements that can be expanded to effectively encompass Id&AM rather than establishing a new and separate structure. Any governance structure established for the purposes of Id&AM would of course sit under the e-Government Sub-Committee of the Strategic Management Council.

### 3.8.1. WoWAG Governance Structure

A WoWAG Governance Structure is required for a number of reasons:

- To drive the Id&AM Framework initiative forward once this initial project is completed.
- To co-ordinate WoWAG activities in the areas of standards and best practices.
- To maintain an ongoing liaison with key users in the community and advocacy groups concerned with issues of privacy, equity of access, etc.
- To manage the examination of the logistics and benefits associated with shared credentials, infrastructure and services. If a positive value case is derived for this, it will be necessary for a group to oversight the detailed specification, acquisition and operational aspects of this.

The proposed structure envisages the formation of a WoWAG Identity Management Steering Group (Id&AMSC) consisting of representatives from the OeG, agencies and a 'surrogate' for the Privacy Commissioner function.

The persistence for this arrangement would be provided by nominated Id&AM Policy Officers in the OeG.

The WoWAG Id&AMSC would be responsible for:

- Oversighting the implementation and ongoing evolution of the Framework.
- Developing and promulgating policy, standards and best practice guidelines.
- Establishing and receiving reports from Community of Practice.
- Establishing and co-ordinating education and training.
- Managing community liaison.

The WoWAG Id&AMSC would be supported and advised by:

- Id&AM and Directory Services policy staff with the OeG.
- Secretariat Services in the OeG
- Community of Practice consisting of:
  - Representatives of OeG.
  - Agency Id&AM specialists.
  - Representative/s of a surrogate for a Privacy Commissioners Office (eg Information Commissioner, Corruption & Crime Commission, Auditor General) and user members from the public and user advocacy representatives in relation to the ongoing requirement to address privacy and public policy issues. The Privacy Impact Assessment panel that will need to be established to undertake the PIA[7] for the Id&AM Framework could provide an ongoing source of community input and advice to the appropriate Community of Practice.

It is vital that the governance structure and processes encompass all stakeholders, and not merely be limited to government agencies. A conventional manner in which this can be achieved is as follows:

- a sub-committee of the Steering Committee which brings together the representatives of and advocates for stakeholder groups that are outside government per se;

[7] See Section 4.6

- at least two members on the Steering Committee who are also members of the public policy sub-committee, who are representatives of or advocates for those stakeholder groups, and who are required to represent the interests of all members of that sub-committee.

### 3.8.2. Agency Governance Structure

An Agency Governance Structure is required:

- To drive the implementation of the Framework within the agency.
- To co-ordinate agency ID&AM activities in the areas of standards and best practices.
- To examine the logistics and benefits of using Shared Infrastructure and Services, as described above and to oversight implementation activities, where appropriate.

The proposed structure envisages the formation of an agency Id&AM Steering Group (Id&AMSC) consisting of representatives from the Technology (Architecture and Security), Business (including Finance) and Policy (eg Privacy) business units. It is envisaged that the agency IDMSC would be chaired by the IT Director (or CTO/CIO) or Head of Security Services.

The agency Id&AMSC would be responsible for:

- Oversighting the implementation and ongoing evolution of the Framework within the agency.
- Developing and promulgating agency policy, standards and best practice guidelines based upon WoWAG policies, etc
- To nominate representative/s to the WoWAG IDMSC and to maintain an ongoing liaison with this body.
- To nominate representative/s to the appropriate Communities of Practice and ensure the agency's views are achieving an adequate hearing.
- Establishing and co-ordinating education and training within the agency.
- Managing community liaison, where agency domain-specific circumstances make this necessary.

The agency Id&AMSC would be supported and advised by:

- Identity Management Section/Specialist Group within the Security/Business Assurance Unit of the agency.
- Directory and other security specialists from the IT Business Unit.
- Secretariat Services in the Security/Business Assurance Unit of the agency.
- Those agency representatives who are members of the WoWAG Community of Practice.

It is important that the governance arrangements include explicit features designed to ensure that all stakeholder groups have, and are seen to have, the ability to be informed, and to have their points of view reflected, in the design, implementation and operation of the agency Id&AM Framework.

The persistence for this arrangement would be provided by an Id&AM Co-ordinator probably sited in the Security/Business Assurance unit of the agency.

### 3.8.3. WoWAG vs Agency Responsibilities

To achieve WoWAG consistency, but without creating unreasonable bottlenecks and lack of agility by agencies, it will be important to agree upon the division of responsibility between WoWAG and agency structures for the:

- development of policies;
- development or selection of standards;
- development of model processes and best practices guides;
- conducting of community consultation and communication;

- development and conducting of appropriate awareness raising, education and training in the areas of IDM.

A synopsis of the recommended division of responsibility is provided in Attachment 1 (Summary of Recommendations).

# 4. Foundational, Enabling and Integration Elements

This section details the foundational, enabling and integration aspects of the Framework. These support and/or represent the actualisation of the positions expounded in the major planks of the foundations.

## 4.1. Model Architecture

A candidate WA Government Id&AM architecture is presented below:

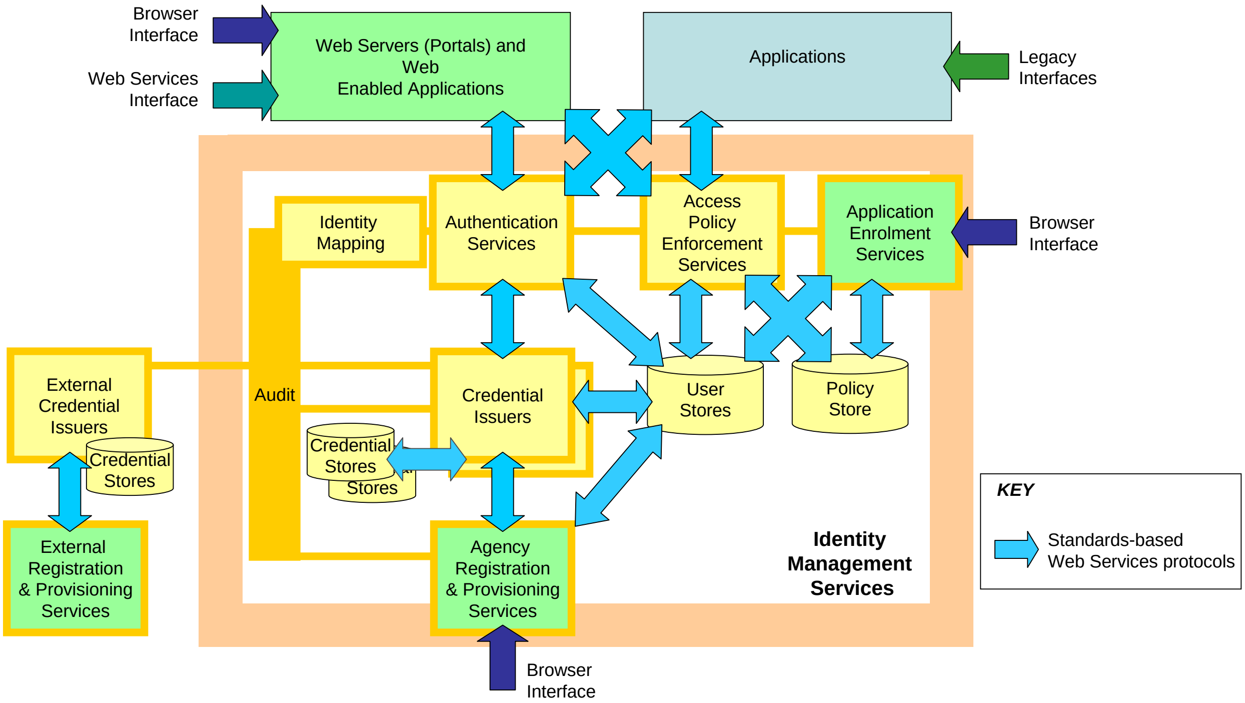

Browser Interface
Web Services Interface
Web Servers (Portals) and Web Enabled Applications
Applications
Legacy Interfaces
Identity Mapping
Authentication Services
Access Policy Enforcement Services
Application Enrolment Services
Browser Interface
External Credential Issuers
Credential Stores
Audit
Credential Issuers
User Stores
Policy Store
Credential Stores
Stores
External Registration & Provisioning Services
Agency Registration & Provisioning Services
Identity Management Services
KEY
Standards-based Web Services protocols
Browser Interface

**Diagram 8 – Candidate Id&AM Architecture**

Key elements of the architecture are:

- The architecture is neutral in respect to authentication model selection (federated, scheme, silo etc) and supports the sharing of many aspects of the infrastructure regardless of the authentication model/s used by particular agencies or within applications.

  It is considered likely that the WA Government agencies will implement a hybrid authentication model, with decisions on implementation architecture being based on the constituency (internal and external users) and on the extent to which users need or seek to access multiple services provided by various government agencies.
- The architecture supports contemporary practice of separation of the business application from issues relating to both the authentication of the identity of users and course and medium grained management of access to the business application.

- The architecture is directory neutral and can support centralised or agency based user stores, with all major services utilising these stores for information in respect to identity, assurance levels associated with the identity, authentication mechanisms and detail on roles providing associated access permissions to various data and services.

  In the absence of a WoWAG directory or other cross-agency directories or user stores, agencies may elect to adopt an agency meta-directory or similar, in order to provide a single view of users to agency applications. Some alignment of information held within these agency meta-directories would assist any future consolidation at a WoWAG level if required.
- The architecture supports a WoWAG or agency-cluster shared services mode of operations from operational, technology and authentication model perspectives. It is intended that such a service could provide an opt-in facility for agencies to save capital and ongoing costs.
- The identity management services can be made available to other delivery systems such as IVR, mobile GSM etc as they emerge. This enables the use of common authentication mechanisms across delivery channels, where appropriate, and within the constraints of the channel.
- The architecture recognizes and supports the rapid evolution of standards in the area of identity management driven by OASIS[8] and other groups, particularly Liberty Alliance[9], aimed at enabling the inter-working of various identity management implementations both at a technology and an operational level. Through the use of web services, authentication and permissions management service requests can be satisfied regardless of origin provided the requesting agent has permission to access these services. It is expected that as these standards mature they will be better supported in commercially available identity management products. At this point it is expected that greater exploitation of, and potentially reliance upon, these standards will be imbedded with commercial business application packages.
- The architecture supports multiple assurance levels for authentication, thereby enabling alignment of application assurance requirements with the authentication mechanism. It is possible for the same identity to have multiple methods of authentication, and hence 'step-up-authentication' would be possible if required by different applications within the same session. This could be invoked from the application.
- The architecture supports credentials currently issued by WA Government agencies, as well as external credentials such as those accepted by the Australian Government and potentially banks. The *Id&AM Action Plan* proposes the development of policy and guidance on compliance requirements of other non-government issuers. This would be accommodated within the formal assessment of Credential Assurance Levels for particular credentials.

  Notwithstanding the above, the extent to which existing WA Government agencies' credential management systems can be leveraged within the architecture needs further investigation.

[8] Refer http://www.oasis-open.org/home/index.php

[9] Refer http://www.projectliberty.org/

- The architecture supports separation of identity authentication from permissions to access various application services. Enrolment for application services is a fundamental element of the architecture which enables the dissociation of the authenticated Identity from the business application's internal knowledge (such as company number, employee number etc) of the authenticated Identity.

  The architecture supports the mapping of the authenticated Identity to the application identifier to be effected within the Identity Mapping service (as in a federated identity management environment) or within the business applications. There are privacy implications of both approaches.

  Notwithstanding the above, even in a shared services environment, the business service owner retains full control over access to the business service.
- The architecture encompasses a robust audit and controls structure and serves as a single point of audit and alert in respect to access to government business systems. Alerts monitoring can be centralised or under the control of individual application owners or departments.

## 4.2. Trust Models

The proposed Id&AM Framework is neutral in respect to the trust models, or combinations thereof, which might be adopted within and across WA Government agencies. This is a necessary position as agencies, clusters of agencies and WoWAG will need to operate or participate within a number of trust models.

The capacity for multiple trust models to share 'components' is discussed in section 4.2.5 below.

Trust models requiring accommodation within the Framework are summarised below and presented in more detail in Appendix B.

These are:

- Silo Model
- Centralised Model
- Scheme or Community Model
- Federated Model

These models differ from each other principally in the nature of the relationship between the identifier/credential provider and the service provider/s that relies upon such credentials (the relying party).

### 4.2.1. Silo Model

In the silo model the Credential Provider (CP) is also the relying party or Service Provider (SP) and has full control over all aspects of the value chain from registration of the user through to authentication and allocation and enforcement of access policies for the application/s.

Key elements are:

- The Identifier is naturally meaningless outside its application domain.
- Terms and conditions of use of the credential by the user, and of reliance on it by the service provider are well defined and purpose specific.
- The potential for use of the credential by other parties is typically limited by lack of technology capability for credential validation outside its domain, and by a lack of business provisions required to prescribe the credentials "allowed" usage.

This is the predominant model currently in use within the applications within WA Government agencies for both internal and external users, and not surprisingly in most other government and private sector environments.

### 4.2.2. Centralised Model

A centralised model in the WA Government context would be essentially a government silo where all identifiers and credentials used within government applications are issued and validated centrally.

National identity card implementations are centralised models.

This model is presented for completeness only.

### 4.2.3. Scheme or Community Model

In this model there are multiple of identifier and credential providers and multiple service providers that rely on the issued credentials.

Key elements are:

- Identifiers issued across the participant CPs are unique within the scheme.
- Common standards and conventions apply across all CPs in respect to the registration credential issuance processes including, required evidence of identity, credential strength, end user agreements etc.
- CPs provide credential validation services to SPs so that they can authenticate identities.
- Service Providers and CPs enter into scheme agreements that cover obligations and accountabilities of scheme membership including liabilities, dispute resolution, and privacy.

The most obvious "scheme" implementation is in the credit card area which operates globally supporting thousands of millions of users through thousands of banks (CPs) and millions of merchant service providers (SPs).

The global banking scheme Identrus also operates on this basis as does the federal government's ABN DSC (ABN Digital Signing Certificate).

The prospective issuance of unique WA Government employee numbers is an example of a scheme based trust model within the WA environment on the issuance side at least. In this example, Corporate Shared Services clusters would each be issuing employee identifiers under essentially the same (WA Government) policies in respect of evidence of identity etc.

In its currently planned form however, necessary validation services of any associated credential (such as a password) is not supported without specific implementation within an agency application system.

### 4.2.4. Federated Identity Model

In its simplest form, federation of identities enables identifiers created in one domain to be accepted within another domain subject to bi lateral agreement/s between the CPs and SPs.

Key elements of federated identity models are:

- Identifiers are unique only within the CP environment and as such when accepted by SPs there is a need for mapping of the CP identifier onto the SP domain.
- Authentication of credentials is completed by the CP and this "authenticated" status and potentially other information is passed to the SP in a trusted manner. This can provide the basis of a simplified sign-on regime across otherwise disparate domains.
- Identity authentication does not necessarily require direct exposure of a CPs credential validation service to third parties.
- Federating with a CP necessitates strong alignment between the CP's registration policies and the assurance level needs of the SP.

In addition to the necessary business arrangements between CPs and SPs, there is a need for technical alignment between CPs and SPs in order that information can be passed between the providers. In a scheme environment, as discussed above, these technical matters form part of the scheme.

Whilst there are few flagship exemplars of federated identity management implementations, the concept is essentially an extension of well proven "physical world" identity trust models in use today such as passports, which are issued in one jurisdiction (CPs) and relied upon (or not) by other jurisdictions (SPs).

The Framework and proposed *Id&AM Action Plan* accommodate the use of federated identities and variants of that model.

#### 4.2.5. Trust Models and Shared Componentry

The achievement of efficiency and effectiveness of Id&AM across the WA Government and its user bases will require the examination of a number of operational models.

These are described below by examining the components that could be shared within the context of a number of the trust models presented above and in Appendix B.

**Shared Components**

Three key 'shareable' elements/components of Id&AM are presented below. These are: infrastructure and solutions, processes and credentials.

| Shared Component | Explanation |
|---|---|
| Infrastructure and Solutions<br>- operational sharing<br>- technology procurement | This encompasses:<br>– User directory/s<br>– Authentication Solutions/Service<br>– Authentication 'hardware' eg cryptographic processors.<br>– Delegated User Administration facilities (eg through portal)<br>– Application Permissions Management Solutions |
| Processes | This encompasses:<br>– User outreach/awareness raising<br>– Evidence of identity checks; qualification checks; authority checks; police clearances; etc<br>– User registration and deregistration<br>– Maintenance of user details<br>– Help desk in relation to credentials<br>– End-user agreements |
| Credentials | This encompasses:<br>– User authentication credentials |

**Operational Models**

The table below is intended to identify the 'art of the possible' in relation to sharing of components within the three trust models.

| Trust Models >>> | Siloed | Scheme/ Community | Centralised | Federated |
|---|---|---|---|---|
| **Shared Components** | | | | |
| **Infrastructure & Solutions** | √[10] | √ | √ | √ |
| **Processes** | √ | √ | √ | √ |
| **Credentials** | X | √ | √ | √ |

[10] The use of shared/outsourced platforms is entirely possible for a siloed trust model

**Evaluation Framework**

In determining which operating model/s to adopt it will be necessary for agencies (or clusters of agencies) to evaluate possible models using the following criteria:

1. Benefits to the agency (as an issuing and/or relying party), cluster and/or WoWAG.
2. Benefits to external users (from eg having a common credential for use across cluster or WoWAG).
3. Whether and how sharing of one or more components might work.
4. Operational, contractual/legal, risk management and commercial issues.
5. Degree of extensibility to new user bases, new applications and new organisations.

## 4.3. Operational Governance

One of the major drivers for abstraction of the Id&AM functionality from a siloed and typically bespoke application environment is the ability to define, implement and monitor the day to day operational risk parameters at an agency or WoWAG level.

The Framework contemplates a hierarchical treatment of Id&AM related risks and controls delivered through a robust electronic audit facility delivering support for both audit alert events and forensic analysis after the fact.

The Id&AM services would form part of a higher order operational risk management approach to the implementation and operation of e-Government services.

## 4.4. Identity & Access Management Policy

An Identity & Access Management Policy position both at a WoWAG and agency level represents a useful and possibly important way in which to obtain traction for the Framework.

It is proposed that the Western Australian Government follow the lead of the Victorian Government by developing and promulgating an Id&AM Policy along the lines of that presented in Appendix G.

## 4.5. Procurement & Capital Expenditure and Systems Development Guidelines

A number of process streams that have ‘gateway events’ associated with them present opportunities to ensure the adoption of the letter or spirit of the Id&AM Framework. These include:

- Procurement rules and guidelines and Common-Use contract arrangements. These can assist in enforcing/re-enforcing key goals including:
    - Interoperability of technical platforms and services.
    - *‘Share rather than Buy’* and *‘Buy rather than Build’* approaches.
- Capital Expenditure Approval Frameworks. These provide similar opportunities to enforce ‘financial’ and ‘technical’ policy.
- Systems Development Life Cycle Methodologies. Once again these provide similar opportunities to enforce ‘financial’ and ‘technical’ policy.

Detailed guidelines should be developed by lead ‘agencies’ (eg OeG, Treasury & Finance, Shared Corporate Services) in collaboration with key operational agencies.

## 4.6. Privacy and Public Policy

Experiences in other Australian and international jurisdictions have highlighted the importance of adequately address privacy and public policy aspects within an Id&AM environment.

Of especial importance is the embodiment in the emergent approach to centralised identity management of privacy threats both for staff of WA Government agencies and for Western Australians in general. In addition, the provision of services may be affected, and there may be differential impacts on various categories of people, which would give rise to access and equity concerns.

These matters are as important to agencies individually as they are to whole of WA Government considerations. The absence in Western Australia of a Privacy Act and the Office of a Privacy Commissioner makes the issue more rather than less complex.

While privacy aspects are not a primary focus of this project, they remain crucially important to the future disposition of the Framework.

The acceptability to stakeholders of the Framework, and of specific features of it, is likely to be a significant factor in the speed and effectiveness of adoption, both by agencies and by individuals. Consultation with stakeholder groups is likely to be a key factor in the acceptability of the scheme, and hence in its adoption. At worst, outright opposition could undermine the return on the investment. At this stage, however, no consultations have been undertaken with stakeholders other than government agencies.

It is therefore essential that further consideration and consultation be undertaken in relation to these matters prior to the 'promulgation' of the Framework.

In order to address these risks in a comprehensive manner, the following sequence of activities should be undertaken:

- stakeholder analysis, in order to ensure a full understanding of the segments of the population that have an interest in, or are affected by, the Id&AM Framework;
- stakeholder consultation, a process whereby representatives of and advocates for the identified stakeholder groups have the opportunity to understand the nature of the proposal, and to provide comments, with a reasonable expectation that their comments will be reflected in the proposal as it is articulated;
- stakeholder participation, which involves ongoing consultation, through the phases of implementation and during the operation of the scheme.

Appendix H provides a detailed examination of privacy and other public policy issues arising from the Id&AM Framework.

This addresses the following aspects of privacy and public policy:

- service-provision, access and equity;
- rights of employees and contractors;
- privacy.

A range of recommendations are provided including conducting a full Privacy Impact Assessment (PIA).

## 4.7. Business Case Guidelines

The benefits of adopting an Id&AM approach of the type proposed by the WoWAG Id&AM Framework accrue through:

- Improved ability to define and enforce robust authentication risk management practices at an organisational or whole of government level.
- Potential to provide services through "shared infrastructure" with likely benefits in cost, quality and speed of roll-out of business applications.
- Improved user service with users able to utilise the same identity and authentication credential across a range of services within a agency and/or across WoWAG.
- Reduced costs in user management with streamlined provisioning, de-provisioning, and help desk services.
- Improved capacity to develop integrated services as required in many joined-up government applications.

The opportunity costs of not progressing down this path are highlighted in the quotes from two overseas government projects:

- *"Not undertaking a consolidated authentication approach would cost an additional $200 million in development costs, $26 million in acquisition costs and would delay implementation of the E-Government initiatives to 2005 and beyond."*
  Steve Timchak, Program Manager, E-Authentication Initiative, eGov, USA

- *"Not proceeding with an all-of-government approach to authentication risks a proliferation of inconsistent government authentication processes. Access to online government services would become more complex, expose government services to security and privacy breaches. Some services delivered by smaller agencies would never be able to be delivered over the Internet securely and economically."*  
  New Zealand Government

The balance of this section provides a framework within which agencies and the Government as a whole can consider the value (cost, benefit and risk) issues associated with various implementation options and shared infrastructure/services approaches to authentication. Appendix J examines cost and benefit categories in more detail.

### 4.7.1. Categories of Value

The US Government's Value Measuring Methodology provides the basis for the evaluation of value cases. This encompasses the examination of the broad government and community 'values' derived from authentication initiatives divided for convenience into five categories:

| | |
|---|---|
| Direct Customer | This captures the value to the end user associated with the proposed 'new' approach. |
| Social (non-user) | This relates to the second order effects derived by individuals and businesses in the broad. |
| Government Financial | This identifies the direct budgetary benefits accruing to agencies and the WA Government as a whole. |
| Government Operational / Foundational | This covers step-change operational savings that may accrue as well as the value of an infrastructure that may be usable to meet future demand. |
| Strategic / Political | This identifies the extent to which the initiative enhances the ability of an agency and the Government as a whole to fulfil its mission. |

By way of example an analysis of the values that arise from the deployment of the Id&AM Framework are seen, in order of importance as:

| **Value Category** | **Nature of 'Net Benefit'** |
|---|---|
| Direct Customer/Internal User | Avoidance of time, effort and cost involved in the application for multiple credentials.<br>This has to be evaluated against the potential increase in 'intrusiveness' created by fewer credentials. |
| Government Financial | 1. Reduction in:<br>- cost of infrastructure and solutions and<br>- operational processes<br>for provision of online access to internals and externals.<br>2. Reduction is usage of non-electronic delivery channels (externals). |
| Government Operational/Foundational | Provision of a scalable and interoperable platform for deployment of online services to internals and externals. |

| Value Category | Nature of 'Net Benefit' |
|---|---|
| Strategic Political | Enabling the deployment of the WA e-Government Strategy. |
| Social (non-user) | Consistency of approach enabling user certainty. |

### 4.7.2. Categories of Costs

The broad cost areas associated with the implementation of the Id&AM Framework, and the order of magnitude of these costs, are summarised below:

| Cost Category | Upfront | Ongoing |
|---|---|---|
| Awareness Raising, Education and Training | Low | Low |
| Privacy Impact Assessment | Low | Low |
| Policies and Procedures | Low | Low |
| Existing Technology Platforms | High | High |
| Existing Data Stores | High | Nil |
| New Technology Platforms & Solutions | Medium to High | Medium to High |
| Security / Audit / Validation | Medium | Medium |
| Legal Costs | Low | Low |

## 4.8. Standards, Processes, Procedures

The Government's goal should be to seek harmonisation of Id&AM approaches across agencies for the purposes of achieving uniform excellence (and the associated certainty that this is so), interoperability at assurance, process, legal and technical levels, and the financial benefits associated with sharing expertise, facilities, credentials etc.

The areas to be covered by agreed standards, processes and procedures are listed below:

- Authentication Related:
  - Authentication/Trust Models
  - Application Assurance Levels
  - Credential Assurance Level
  - Data Classification
  - User Clearance Levels
  - Credentials/Tokens
  - Registration Levels
  - Credential Issuer Reliance Levels
  - Evidence of Identity Levels
  - Authentication Services
  - Registration Services
- Authorisation Related:
  - Enrolment
  - Permissions Management Services

- Directory Related
  - User Naming Convention/s
  - User Identifiers
- Technology Set
- Standardised Agreements (MOUs, User Agreements)
- Application Development Toolkits

A listing of these and proposed approach to each of these has been provided in Attachment 1.

Further coverage will be provided in the *Id&AM Action Plan*.

### 4.8.1. Technology Standards

Technology standards play a crucial role in determining the robustness, interoperability, scalability and extensibility of agency's approaches to Id&AM.

The diagram below superimposes possible standards onto the model Id&AM architecture.

The issue of technology standards will be addressed in further detail in the *Id&AM Action Plan*.

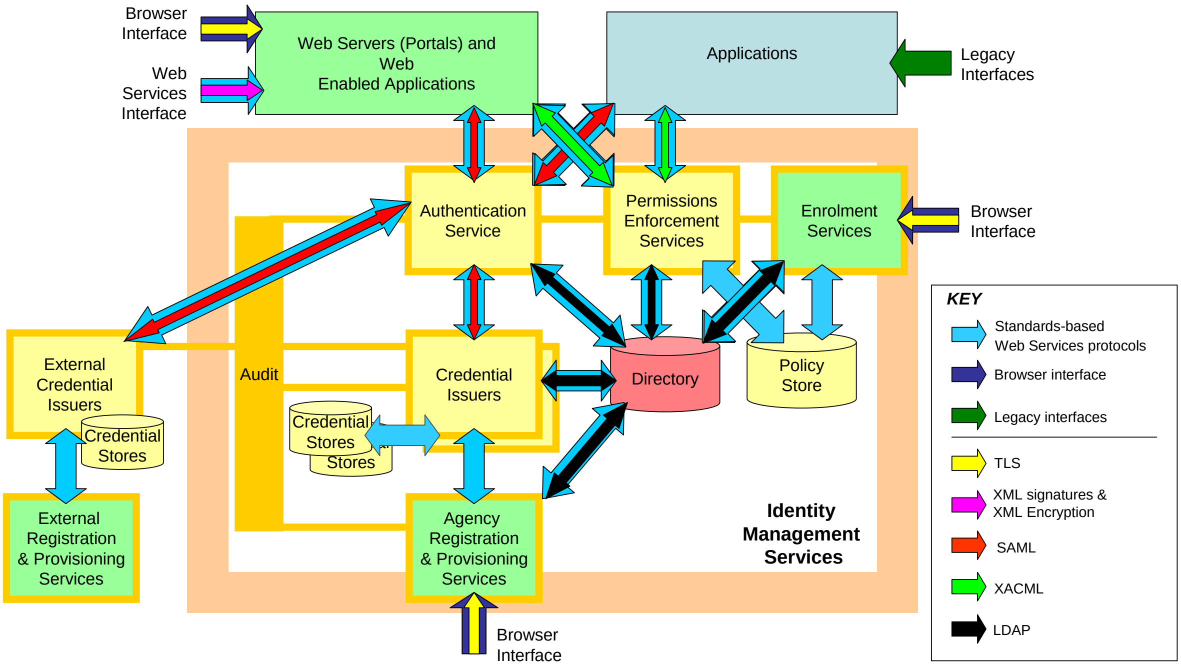

Browser Interface
Web Services Interface
Web Servers (Portals) and Web Enabled Applications
Applications
Legacy Interfaces
Authentication Service
Permissions Enforcement Services
Enrolment Services
Browser Interface
Audit
External Credential Issuers
Credential Stores
Credential Issuers
Credential Stores
Stores
Directory
Policy Store
External Registration & Provisioning Services
Agency Registration & Provisioning Services
Identity Management Services
Browser Interface
KEY
Standards-based Web Services protocols
Browser interface
Legacy interfaces
TLS
XML signatures & XML Encryption
SAML
XACML
LDAP

**Diagram 9 – Id&AM Model Architecture with Standards**

## 4.9. Maturity Assessment Approach

The assessment of the maturity of Id&AM approaches by agencies enables their management to gauge the degree of exposure faced by organisations and determine whether and where to focus future resources.

Two aspects of maturity need to be considered as illustrated in the matrix below:

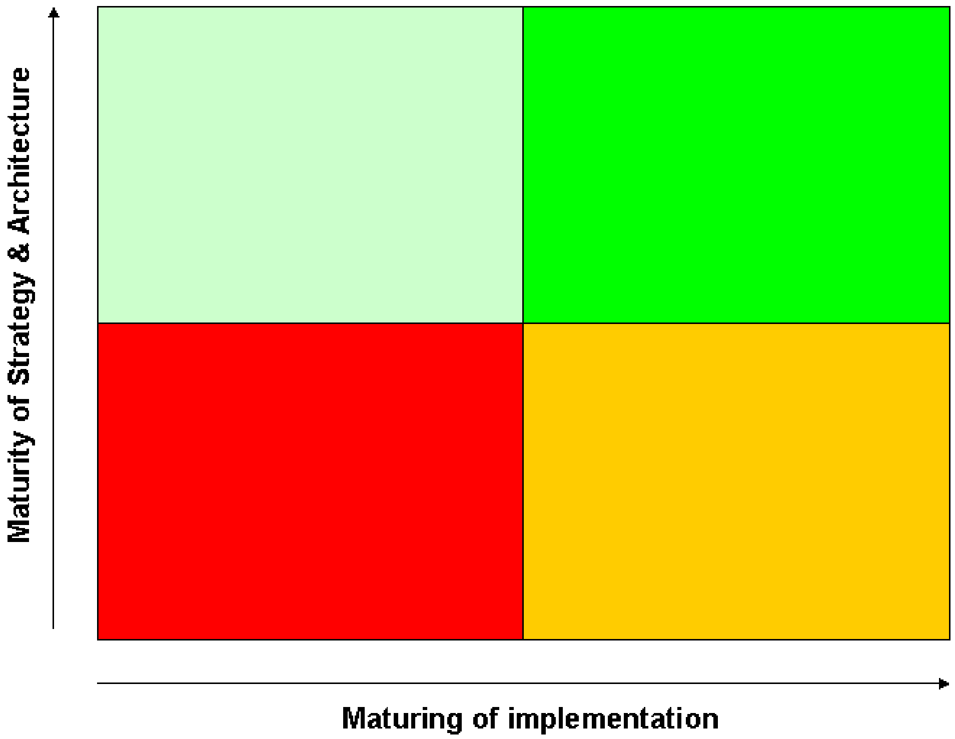

Maturity of Strategy & Architecture
Maturing of implementation

**Diagram 10 – Id&AM Maturity Matrix**

Suggested criteria for the establishment of the level of maturity are detailed below.

### 4.9.1. Maturity of Strategy & Architecture

Suggested evaluation criteria that may determine the maturity of an agency's strategic and architectural approach to Id&AM are seen as:

- Policies - completeness, currency and strength of compliance regime.
- Methodology/s used to plan, architect, build, operate, monitor and enhance/remediate.
- Standards – policy, process, management and technology.
- Products – key technology and management products in place or under contemplation.

One possible approach to graphically depicting an agency's strategic and architectural maturity is illustrated in diagram 11 below.

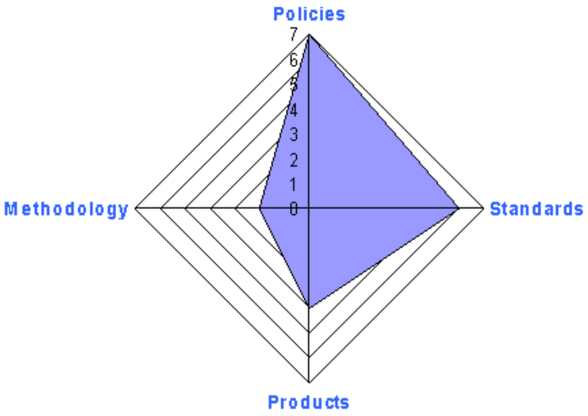


**Diagram 11 – Id&AM Strategic & Architectural Maturity 'Dashboard'**

### 4.9.2. Maturity of Implementation

Suggested evaluation criteria that may determine the maturity of an agency's operational approach to Id&AM are seen as:

- Entity Management - efficacy, completeness, interoperability, diversity, financial/commercial feasibility
- Information Management - efficacy, completeness, interoperability, diversity, financial/commercial feasibility
- Authentication Management – efficacy, completeness, interoperability, diversity, financial/commercial feasibility
- Authentication Mechanisms – diversity, fitness for purpose, capturing user base, approach to issue, maintenance and revocation/recovery, financial/commercial feasibility
- Access Management - efficacy, completeness, interoperability, diversity, financial/commercial feasibility
- Operational Governance – coverage of all issues; efficacy of tracking, detection, feedback/reporting and remediation loop.

One possible approach to graphically depicting an agency's operational maturity is illustrated in diagram 12 below.

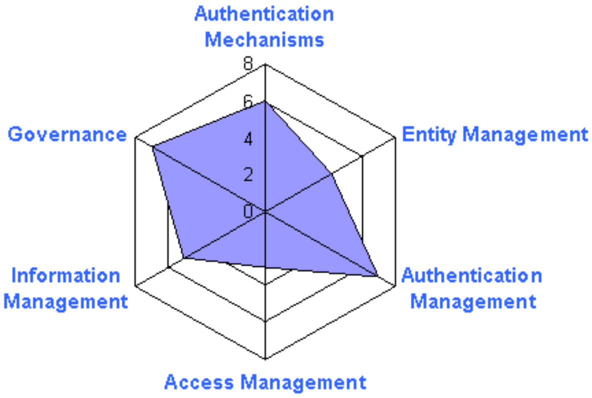


**Diagram 11 – Id&AM Operational Maturity 'Dashboard'**

## 4.10. Relationship between Framework & WA Enterprise Architecture

### 4.10.1. WA Public Sector Enterprise Architecture Programme

The WA Government regards enterprise architecture as a key tool to ensure that Information and Communication Technology (ICT) projects are aligned to the Government's and agencies' strategic priorities. Enterprise Architecture (EA) is seen as providing a blueprint to guide strategic and detailed decisions.

Enterprise architecture provides a formal description of the factors that should shape the purposes for which information technology is deployed, and how it is deployed. These include: business functions, rules, principles and technical specifications and standards.

The basic enterprise architecture model, as represented by most major architecture frameworks, and adopted by the Government consists of the following elements:

- Business Architecture - this articulates the enterprise's business goals and strategy that will influence the ICT environment, and key business processes.
- Information Architecture - describes the information (data) standards and the principles that guide the use of information to support the aims of the enterprise.

- Application Architecture - this kind of architecture provides a blueprint for the individual application systems to be deployed, their interactions, and their relationships to the core business processes of the enterprise.
- Technology Architecture - describes the infrastructure that supports the enterprise's applications and information.
- Enterprise Architecture Management and Project Evaluation **-** describes a methodology for the creation and maintenance of all of the architectures (business, information, application, technology) and the evaluation of projects and standards for adherence to the enterprise architecture.
- Funding, Procurement and Review **-** is closely linked to the Enterprise Architecture Management and Project Evaluation and is the means by which the appropriate funding or procurement mechanisms are selected. This process also entails review over the project's lifecycle[11].

In developing the Enterprise Architecture Programme, OeG will develop an Enterprise Architecture Toolkit  that contains a number of tools to help agencies undertake ICT project in line with the enterprise architecture, including project management guidelines, change management and people management guidelines.

A draft representation of the WA Public Sector Enterprise Architecture Model is provided below:

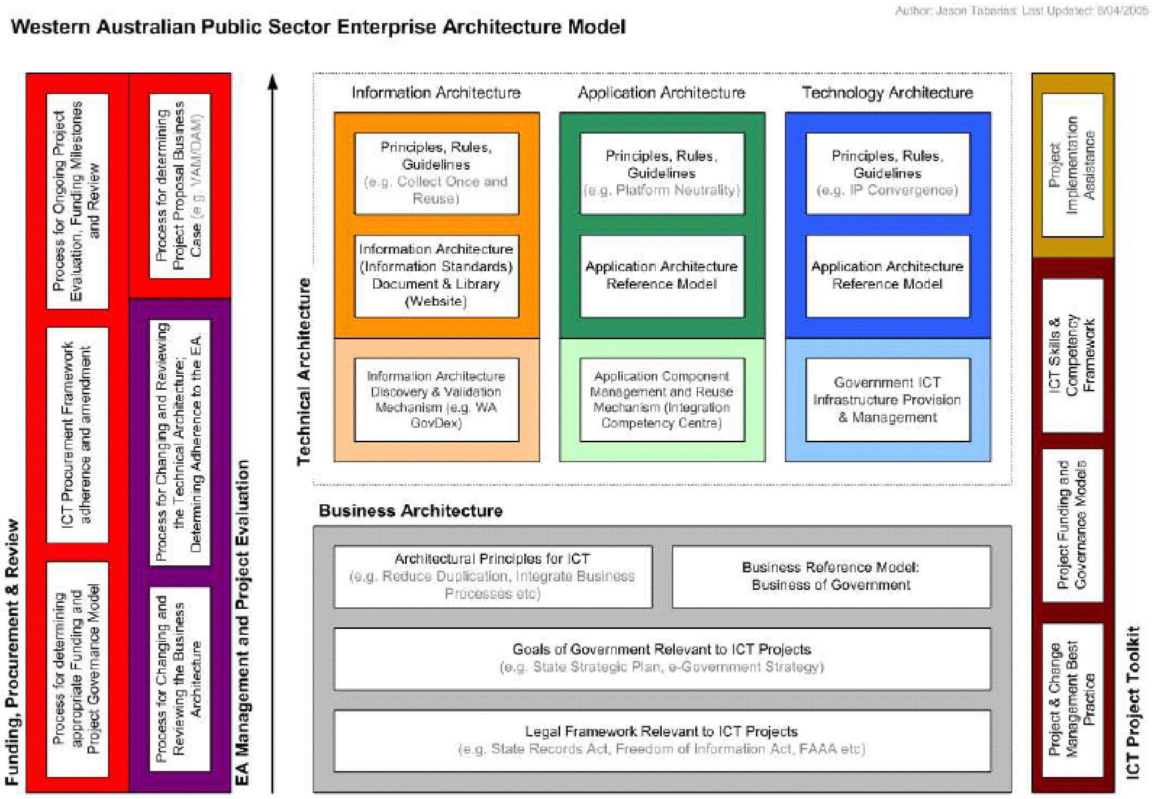

Author: Jason Tabarias. Last Updated: 8/04/2005
Western Australian Public Sector Enterprise Architecture Model
Funding, Procurement & Review
Process for Ongoing Project Evaluation, Funding Milestones and Review
ICT Procurement Framework adherence and amendment
Process for determining appropriate Funding and Project Governance Model
Process for determining Project Proposal Business Case (e.g. VAM/DAM)
Process for Changing and Reviewing the Technical Architecture; Determining Adherence to the EA.
Process for Changing and Reviewing the Business Architecture
EA Management and Project Evaluation
Technical Architecture
Information Architecture
Principles, Rules, Guidelines
(e.g. Collect Once and Reuse)
Information Architecture (Information Standards) Document & Library (Website)
Information Architecture Discovery & Validation Mechanism (e.g. WA GovDex)
Application Architecture
Principles, Rules, Guidelines
(e.g. Platform Neutrality)
Application Architecture Reference Model
Application Component Management and Reuse Mechanism (Integration Competency Centre)
Technology Architecture
Principles, Rules, Guidelines
(e.g. IP Convergence)
Application Architecture Reference Model
Government ICT Infrastructure Provision & Management
Business Architecture
Architectural Principles for ICT
(e.g. Reduce Duplication, Integrate Business Processes etc)
Business Reference Model: Business of Government
Goals of Government Relevant to ICT Projects
(e.g. State Strategic Plan, e-Government Strategy)
Legal Framework Relevant to ICT Projects
(e.g. State Records Act, Freedom of Information Act, FAAA etc)
Project Implementation Assistance
ICT Skills & Competency Framework
Project Funding and Governance Models
Project & Change Management Best Practice
ICT Project Toolkit

**Diagram 13 - WA Government (draft) Enterprise Architecture**

[11] This approach also aligns with current Department of Treasury and Finance thinking regarding Project Definition and Strategic Asset Management.

### 4.10.2. Id&AM Framework and Enterprise Architecture

The table below is intended to detail what Id&AM matters need to be considered in the development and maintenance of key aspects of the Government's and agencies' enterprise architecture models.

The Id&AM issues/actions are categorised in relation to the major management planks of the Framework:

- Information Management
- Identity Management
- Access Management.

The requirements for each of these are analysed against the following aspects of the EA:

- Business Architecture
- Information Architecture
- Application Architecture
- Technology Architecture.

| | Business Architecture | Information Architecture (IA) | Application Architecture (AA) | Technology Architecture |
|---|---|---|---|---|
| **ID& AM Categories** | | | | |
| **Information Management**<br>Principles applying to information that will be stored in enterprises data stores. | Prescribed/consistent rules & processes to determine the ownership and classification of information. | Prescribed/consistent rules for & approaches to embedding ownership and classification into information records or link ownership/classification to information 'objects' via metadata. | Prescribed/consistent rules for application architecting and development to enforce recognition of ownership/ classification data associated with information. | Procurement, development and integration rules related to platforms, systems software, utilities, middleware to enable implementation of IA and AA architectures. |
| **Identity Management**<br>Principles applying to users that will gain access to information. Users may be people, applications or devices. | Prescribed:<br>(i) approaches to determining user identification requirements;<br>(ii) identity, attribute and authority-level verification/ checking standards;<br>(iii) registering users and issuing credentials;<br>(iv) revoking credentials. | Prescribed:<br>(i) dataset for storing information relating to identities;<br>(ii) data-standards and protocols. | Prescribed architecture and/or standards for implementing user identity management and storage. | Recommended technology platform (eg directories) and standards for implementing identity management. |
| **Security/Access Management**<br>Principles applying to physical and virtual access to machines, networks and premises. | Prescribed processes for:<br>(i) determining classes of users and their access permissions to machines, networks and premises.<br>(ii) issuing and deactivating access 'artefacts' (could be manual or electronic) and the stores thereof. | Prescribed:<br>(i) dataset for storing information about machines, networks and premises;<br>(i) dataset for storing information relating to access privileges of users;<br>(ii) data-standards and protocols applicable to the above datasets. | Prescribed rules for application systems that:<br>(i) manage access permissions data;<br>(ii) are required to enable users to gain access to machines, networks and premises. | Recommended technology platform/s and standards for implementing access management. |

**Table depicting cross reference between Identity & Access Management Framework and WA Government Enterprise Architecture Model**

## Attachment 1 – Summary of Proposed Approach

The Summary of Proposed Approach contains a synopsis of key positions for the Government to review. For each component the similarities or differences in approach relative to Internal and External users is provided. Guidance is also provided in relation to the relative roles/responsibilities at a WoWAG and Department level. Finally, guidance is provided in relation to non-WA Government jurisdictions / sectors with which alignment or consistency is desirable.

| Aspect | Proposed Approach | Similarities or Differences in Approach | | Actions/Implications | | Alignment / Consistency with |
|---|---|---|---|---|---|---|
| | | Internal Users | External Users | WoWAG | Agency | |
| **INFORMATION MANAGEMENT** | | | | | | |
| Data Classification | Develop and implement data classification scheme. | identical | Identical | Develop & maintain | Adopt where appropriate | Commonwealth Government Protective Security Manual (PSM) |
| **ENTITY MANAGEMENT** | | | | | | |
| Identifiers | Implement a uniform approach across Western Australian Government.<br>Internal users to have an identifier that is unique across Government. Identifier is ideally persistent if user changes agency.<br>Authoritative source for Internal users is HR systems. | Identifier being agreed with Shared Corporate Services is primary identifier | For individuals, a WA Government Customer Number allocated centrally. Usable by one or more agencies at user option. Users have option to have multiples & merge & split. | Central Id number issuer. | Use central ID issuing service. | |

| Aspect | Proposed Approach | Similarities or Differences in Approach | | Actions/Implications | | Alignment / Consistency with |
|---|---|---|---|---|---|---|
| | | Internal Users | External Users | WoWAG | Agency | |
| | | | For business users, ABN is preferred identifier, potentially with subordinate 'personal' identifier within business.<br>For business, may accept other identifiers such as HeSA, and map to WoWAG Identifier | | | |
| Registration | Develop & continue to maintain best practice approach and align approaches with Credential Assurance Levels and EOI Levels. | Drive to consistency of process through HR shared services approach | Some variations in process | Develop & maintain | Adopt and adapt | Commonwealth<br>Banking Industry |
| Evidence of Identity (EOI) | Develop & continue to maintain best practice approach and align approaches with Credential Assurance Levels and Registration Levels.<br>Consideration of inclusion of attributes such as 'Police checks' in record of EOI processing – ie to reduce duplication of processes. | Some variations in process and nature of evidence | | Develop & maintain | Follow | Commonwealth<br>Banking Industry |
| Enrolment | Treat as distinct from registration. The enrolment process supports the mapping of one identity domain to another, and thereby supports federated approaches to identity management | Some variations in process.<br>Need will exist until all applications migrate to single identifier usage | Some variations in process.<br>Likely to persist indefinitely | Develop & maintain | Adopt and adapt | |

| Aspect | Proposed Approach | Similarities or Differences in Approach | | Actions/Implications | | Alignment / Consistency with |
|---|---|---|---|---|---|---|
| | | Internal Users | External Users | WoWAG | Agency | |
| User Clearance Levels | Develop and implement user clearance level scheme.<br>This is distinct from attribute verification which is dealt with in EOI above | identical | Identical<br>Unlikely to arise | Develop & maintain | Adopt where appropriate | Commonwealth PSM |
| ID Mgt Role of Agency Meta-directories or agency user stores | Those agencies that have this facility should make it the authoritative reference for user 'system-identity' information for the legacy applications. Other agencies should investigate business case for meta-directory. | Applicable immediately | Policy yet to be determined | Set policy | Adopt | |
| **AUTHENTICATION MANAGEMENT** | | | | | | |
| Credential Assurance Level | Follow AGAF (Authentication Technique) model.<br>Extend to develop detailed criteria along lines of US Gov 'Credential Assessment' approach incorporating Authentication Protocol<br>Supported by recommendations in relation to:<br>- Evidence of Identity<br>- Evidence of Record Ownership<br>- Credentials/Tokens<br>- Credential Issuer Reliance | Identical | Identical | Develop & maintain | Follow<br>WoWAG<br>guidelines | Commonwealth |
| Credential Issuer Reliance Levels | Introduce notion of reliance level of credential issuer to support possible use by WA Government agencies of externally issued credentials.<br>Also supported by the development of MOUs to apply between agencies issuing credentials to internal or external users. | Identical | identical | Develop & maintain reliance evaluation criteria | Agencies to make own assessment s based upon threat-risk factors. | |

| Aspect | Proposed Approach | Similarities or Differences in Approach | | Actions/Implications | | Alignment / Consistency with |
|---|---|---|---|---|---|---|
| | | Internal Users | External Users | WoWAG | Agency | |
| **ACCESS MANAGEMENT** | | | | | | |
| Application Assurance Levels | Follow AGAF 1-4 level model.<br>Develop more detailed procedures/ criteria to determine assurance level. | Identical | Identical | Develop & maintain | Follow WoWAG guidelines | Commonwealth |
| Role-based Access Control | Move to role-based access control to ensure scalability and efficacy of three-tier Id&AM architecture.<br>Harmonisation of role definitions will support federated Id&AM. | Identical | Identical | Develop and maintain guidelines & facilitate sharing of experiences. | Analyse, architect & implement. | Best practice implementations (eg DoJ). Consider WoWAG 'standards' or at least 'definitions'. |
| **GOVERNANCE** | | | | | | |
| Privacy and Public Policy | Privacy and Public Policy Impact Assessment should be standard requirement in determining authentication approach. | Policy and process differ from external | Policy and process differ from internal | Determine policy & best practice. | Conduct P&PPIAs. | Follow/share best practice with Commonwealth |
| Cost-Benefit Analysis | CBA should be standardised requirement. Should evaluate shared services/infrastructure for internal and shared development & tokens for externals. | Consider internal impacts | Consider internal and external impacts | Determine policy & best practice | Adopt and adapt | Follow/share best practice with Commonwealth |
| Standardised Agreements (MOUs) – to cover reliance on credentials issued by others. | Develop and implement | Variation to reflect intra-dept reliance | Variation to reflect reliance on or by external credential provider | Develop & maintain | Adopt and adapt | |

| Aspect | Proposed Approach | Similarities or Differences in Approach | | Actions/Implications | | Alignment / Consistency with |
|---|---|---|---|---|---|---|
| | | **Internal Users** | **External Users** | **WoWAG** | **Agency** | |
| **SHARED SERVICES** | | | | | | |
| ID Mgt role of WoWAG Directory | A WoWAG directory could provide an effective authoritative reference for user 'system-identity' information on a WoWAG basis (being aggregation of agency identity data). The logistics of this will require careful examination.<br>The case for this has yet to be determined and will require rigorous examination of the privacy and public policy issues. | Applicable immediately | Policy yet to be determined | Evaluate business case, set policy and operate | Use | |
| Registration Services | Examine opportunities for sharing or using external service providers to complete registration processes | N/A | Use at agency option | Provider | User | |
| Authentication Services | Examine opportunities for sharing of authentication services and thereby credentials across agencies.<br>This may provide an interim step to a fully integrated environment | Identical to external users, but likely simpler implementation due to proposed single identifier regime | Use at agency option | Provider | User | |
| Permissions Management Services | Examine opportunities for Shared Services. | N/A | Use at agency option | Provider | User | |

| Aspect | Proposed Approach | Similarities or Differences in Approach | | Actions/Implications | | Alignment / Consistency with |
|---|---|---|---|---|---|---|
| | | Internal Users | External Users | WoWAG | Agency | |
| **ARCHITECTURE, STANDARDS AND GUIDELINES** | | | | | | |
| Architecture Model | Hybrid | Primarily Scheme based due to proposed single identifier and underpinning common MOUs | Primarily siloed.<br>Federated at option of Users and agencies. | Develop detailed architectures | Adopt and adapt architectures | Commonwealth where practical to use of Commonwealth recognised credentials eg Gatekeeper, Identrus |
| Endorsed Credentials | Develop & continue to maintain standardised list and align approaches with Credential Assurance Levels.<br>Support one, two and multiple factor approaches:<br>- User-ID/Password<br>- Shared Knowledge (KBA)<br>- Shared Secrets<br>- PKI (soft)<br>- PKI (hard)<br>- Challenge Response<br>- Smart cards and other tokens<br>- Biometric<br>Supported by recommendations in relation to Credential Assurance Level. | identical | identical | Develop & maintain | Follow | Commonwealth<br>(possibly banks to the extent that existing tokens could be leveraged). |
| Application Development Toolkits | Assess requirement/demand for these (eg Customer signing interface - CSI) | Requirements will differ | Requirements will differ | Develop & maintain | Adopt where appropriate | Allow/share best practice with Commonwealth |
| Technology Feasibility | Technology Impact Assessment should be standard requirement in determining authentication approach | Consider internal impacts | Consider internal and external impacts | Determine policy & best practice | Adopt and adapt | Follow/share best practice with Commonwealth |

| Aspect | Proposed Approach | Similarities or Differences in Approach | | Actions/Implications | | Alignment / Consistency with |
|---|---|---|---|---|---|---|
| | | **Internal Users** | **External Users** | **WoWAG** | **Agency** | |
| Standards | Develop standards for authentication and permissions management interfaces (assumes that token/credential standards are defined within the Assurance Level elements above) | identical | identical | Develop & Maintain | Follow | Commonwealth |
| Technology Set | Define accredited technology set including development toolkits | identical | Use at agency option | Develop & Maintain | Adopt and Adapt | |

## Appendix A – Glossary

| TERM | DEFINITION |
|---|---|
| Access Authorisation | The system controls and surrounding processes that provide or deny parties the capability and opportunity to gain knowledge of or to alter information or material on systems.<br>In practice, the act of authorising access usually occurs after authentication has been successful. |
| AGAF | The Australian Government Authentication Framework.<br>The Framework covers the rules to be applied to authentication of external (ie non-Commonwealth Government) entities when dealing with them online.<br>The Framework provides a risk management approach to authentication that aligns business needs and processes with appropriate authentication solutions and technologies. |
| Assertion | A statement made that purports to be true.<br>Categories of Assertion that may be subjected to Authentication include Agents, Attributes, Credentials, Data Integrity, Entities, Identities, Location, and/or Value.<br>eg – "I am Sheila Smith", "I am an authorised signatory", "I am the authorised agent of Bob Black", "This communication is coming from Geelong". |
| Assurance level | The degree of trust associated with the authentication credentials that are proffered.<br>The AGAF and the proposed WAGAF have four assurance levels (1-4): Minimal, Low, Moderate, High. |
| Assurance level 2 | A specific level on a hierarchical scale representing successively increased confidence that a target of evaluation adequately fulfils the requirements[12] |
| Authentication | To establish as genuine or valid[13].<br>The process of testing of an Assertion, in order to establish a level of confidence in the Assertion's reliability. |
| Authentication<br>2 | Authentication is how computer systems verify that a person or computer acting on a person's behalf is who or what they claim to be. It is a secure and trusted form of identification[14]. |
| Authentication Technique | The amalgam of the Authentication Mechanism and the Registration process. The AGAF and WAGAF allow for a range of authentication techniques to be applied. Each has an associated level of assurance associated with it.<br>eg use of single-factor authentication and a registration process that does not require physical evidence of identity. |

[12] Based on definition in RFC2828

[13] The Times English Dictionary - 2000

[14] Source: www.stanford.edu/group/itss/pcleland/help/glossary.htm

| TERM | DEFINITION |
|---|---|
| Authentication Mechanism | The 'technology' approach used to support the act of authentication eg: UserID-Password, PKI, Smartcards, Biometrics.<br>These can be single-factor (eg UserID-Password) or multi-factor (eg password+Smartcard). |
| Authentication Assurance Level | The level of trust/certainty associated with the Authentication Technique.<br>The AGAF and the proposed WAGAF have four assurance levels (1-4): Minimal, Low, Moderate, High. |
| Authority | Permission to perform a specified act.<br>eg: access and/or modify data; approve the registration and/or enrolment of users. |
| Authority to deal | Broadly based permissions that can be associated with an identity – eg those based upon role, financial delegation |
| Biometrics | A measure of an Attribute of a Natural Person's physical self, or of their physical behaviour. In principle at least, a Biometric can be used:<br>• to validate an entity (where the entity is a Natural Person);<br>• as an Authenticator for an Assertion involving an Entity; and<br>• as a means of restricting the use of a personalised Token to the appropriate Natural Person.<br>Examples include: fingerprint, voice-print, iris-scan |
| Certificates | See Digital Certificate |
| Classification | Determining the 'status' of a user or information resource for security purposes. The matching of the two then provides a capacity to determine user access rights to the information resource.<br>See Data Classification. |
| Clearance Level | The formal Classification associated with a person – eg cleared to 'Top Secret' level. |
| Credential | Information identifying a party that has physical or digital existence, and that assists in the process of Authentication of an Assertion. |
| Credential<br>2 | Information, passed from one entity to another, used to establish the sending entity's access rights[15]. |
| Credential<br>3 | A set of access permissions. Media independent data attesting to, or establishing, the identity of an entity, such as a birth certificate, driver's license, mother's maiden name, social security number, finger print, voice print, or other biometrics.[16] |
| Credential Store | The systems-based repository that holds user credentials. |

[15] Source: INFOSEC-99

[16] Source: ANSI X9.69

| TERM | DEFINITION |
|---|---|
| Data Classification | Classification of data (eg documents, computer records) according to defined ‘security’ rules. This enables access to such data to be provided or refused based upon the ‘security’ classification of the party seeking access. |
| Data Classification 2 | Restriction imposed by the government on documents … that are available only to certain authorized people[17] |
| De-provisioning | The removal of records on systems relating to the authentication credentials and/or access permissions of users. |
| Digital Certificate | A character string that has been digitally signed by an Entity (a Certification Authority) and that makes one or more Assertions about a Public Key and another Entity, as specified by the relevant terms of contract. |
| Digital Certificate 2 | A secure electronic identity that certifies the identity of the holder. Issued by a Certification Authority, it typically contains a user's name, public key, and related information. A digital certificate is tamper-resistant and cannot be readily forged, and is signed by the private key of the Certification Authority which issued it[18]. |
| Digital Certificate 3 | In an X.509-based scheme, an electronic document signed by the CA which:<br>(1) identifies a Key Holder and the Business Entity he or she represents;<br>(2) binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair; and<br>(3) should contain any other information required by the Certificate Profile. |
| Digital signature | A string of characters appended to a digital object that demonstrates that the originating device had access to a particular Private Key.<br>An important use is to enable Authentication of the Identity that generated, sent, or takes responsibility for that digital object. This assumes that a considerable number of conditions hold. See Public Key Infrastructure.<br>The technique applies Public Key Technology as follows:<br>• a relatively short string of bits is generated from the content of the digital object, by applying an agreed one-way Hash Function to it;<br>• that string is then encrypted with the signer’s Private Key, and appended to the digital object;<br>• any other party that has Access to the digital object can also generate that string by applying the same Hash Function to it;<br>• any other party that has Access to the signed digital object can decrypt the Digital Signature by applying the putative signer’s Public Key to it;<br>• if the generated string and the decrypted signature are equal, then the signature was generated by a device that had Access to the appropriate Private Key. |

[17] Source: www.cogsci.princeton.edu/cgi-bin/webwn

[18] Source: www.cio-dpi.gc.ca/pki-icp/beginners/glossary/glossary_e.asp

| TERM | DEFINITION |
|---|---|
| Digital signature<br>2 | A very large number created in such a way that it can be shown to have been done only by somebody in possession of a (secret) key and only by processing a document with a particular content. It can be used for the same purposes as a person's handwritten signature on a physical document. Something you can do with public key cryptography.[19] |
| Enrolment | The act of setting up permissions that enable a known user to gain knowledge of or to alter information or material on systems.<br>eg a known user will be enrolled into the email, HR, Financial etc systems.<br>Multiple enrolments into various systems may occur after a user has been Registered.<br>Although 'Registration' and 'Enrolment' are sometimes used as synonyms, a distinction is being drawn here between the two terms. |
| Entity | A real-world thing.<br>Categories include objects, animals, artefacts, natural persons, and legal persons (such as corporations, trusts, superannuation funds, and incorporated associations). |
| Evidence of Identity | Proof (eg in the form of documents) usually produced at the time of Registration (ie when authentication credentials are issued) used to substantiate the identity of the presenting party. |
| Hard certificates | Digital certificates stored on a hardware token (eg smartcard) together with the associate private key. |
| Harm | Anything that has harmful consequences for an entity, and includes injury to persons, damage to property, loss of value of an asset, or loss of reputation and confidence. |
| Identification | The process whereby data is associated with a particular Identity. It is performed through the acquisition of data that constitutes an Identifier for that Identity. |
| Identifier | One or more data-items concerning an Identity that are sufficient to distinguish it from other Identities, and that are used to signify that Identity.<br>Identifiers include names. A natural person may use more than one name, and variants of each name.<br>Identifiers also include 'id numbers' or 'id codes' issued by other Entities that the Entity interacts with. An Entity may be assigned many such numbers and codes.<br>A legal person may have many names (e.g. associated with business units, divisions, branches, trading-names, trademarks and brandnames), and multiple 'id numbers' and 'id codes' assigned by other Entities that the Entity interacts with. |
| Identities Directory | Directory in which core information is held relating to identities – eg directory and meta-directories proposed by Project Rosetta. |

[19] Source: www.w3.org/People/Berners-Lee/Weaving/glossary.html

| TERM | DEFINITION |
|---|---|
| Identity | A particular presentation of an Entity.<br>An Identity may correspond to a Role played by the Entity.<br>An Identity may be used by the Entity in its dealings with one other Entity, or with many other Entities.<br>An organisation may maintain an Account within its records that corresponds to an Identity. |
| Identity Authentication | The process of testing an Assertion that a particular Entity is appropriately using an Identity, in order to establish a level of confidence in the Assertion's reliability.<br>In particular, the process of cross-checking, against additional Evidence of Identity (EOI), the Identity signified by an Identifier acquired during an Identification process. |
| Identity Management | The policies, rules, processes and systems involved in ensuring that only known, authorised Identities gain access to networks and systems and the information contained therein. |
| Knowledge Based Authentication (KBA) | An authentication approach in which a user is challenged to provide one or more answers to questions/challenges provided by the party undertaking the authentication. The information sought could be 'shared secrets' provided by the user during a registration process and/or personal information (eg address, date of birth, mothers maiden name, etc) and/or transactional data (eg date, amount, reference number of last payment). |
| Multi factor authentication | An Authentication process in which multiple forms of Evidence are used, in order to increase the level of confidence in the Assertion.<br>In the case of Identity Authentication, this involves two or more of the following:<br>• an additional Identifier provided by the person;<br>• knowledge demonstrated by the person ('something you know');<br>• an act performed by the person (something you can do);<br>• a Credential provided by the person ('something you have');<br>• a Biometric surrendered by the person ('something you are' or something you do). |
| Onboarding | The process of Registering and Enrolling online users. |
| Password | A form of Challenge-Response Authentication in which a string of characters is used to assist in the Authentication of the Assertion that a person has the right to use a User-ID.<br>The effectiveness of the technique depends upon the assumption that the Password is known only by the appropriate Entity (and, in less secure schemes, also by the System conducting the Authentication).<br>If a Password is disclosed or shared, Accountability is compromised.<br>Synonyms/similar concepts are Passphrase, Personal Identification Number (PIN). |
| Permissions | A Capability, associated with an Identity, which enables Access to System Resources.<br>Authorisation and Privilege are used as synonyms for Permission.<br>See also Restriction. |

| TERM | DEFINITION |
|---|---|
| Permissions Management Infrastructure | The systems (hardware, software and networks) that enable the management of permissions in relation to user access to systems resources. |
| Permissions store | The systems-based repository that holds the authoritative records of valid user permissions. |
| PKI | Public Key Infrastructure.<br>The comprehensive set of measures needed to enable Public Key Technology to support the Authentication of Assertions. |
| Public Key Technology | Technology based on public key cryptography, that enables a message to be encrypted with one Key, and decrypted with another Key.<br>PKI is distinguished from secret-key (or symmetric) technologies, which use a single key that both parties must possess, and that therefore has to be communicated from whomever creates it to whomever needs it, and therefore has to be exposed to the risk of interception.<br>With public key technologies, on the other hand, one of the key pair can be kept securely by one party, and never exposed to the risk of interception by a third party. |
| Privacy | The interests that Natural Persons have in sustaining a 'personal space', free from interference by other people and organisations, and in controlling information about themselves.<br>It has multiple dimensions, including privacy of the physical person, privacy of personal behaviour, privacy of personal communications, and privacy of personal data.<br>A variety of privacy rights are conferred by international instruments, and by the laws of most jurisdictions.<br>The term is often used in a misleading manner by security specialists, as a synonym for what they also call ’data confidentiality’, or even to refer merely to the protection of the content of data during transmission. |
| Provisioning | The process (whether manual or automated) of supplying services to and enabling features for a subscriber, in this context, access permissions. |
| Registration | The process of establish a user’s Authentication Credentials.  This may involve eg requirement for production of Evidence of Identity and the issuing of one or more Credentials.<br>Multiple enrolments may occur after a user has been registered.<br>Although ‘registration’ and ‘enrolment’ are sometimes used as synonyms, a distinction is being drawn here between the two terms. |
| Risk | A measure of the likelihood of harm arising from a threat. |
| Risk Assessment | A process to determine the extent to which expenditure on safeguards is warranted in order to protect against identified threats. |
| Safeguard | A measure that:<br>– prevents a threatening event causing harm to an entity<br>– mitigates the harm caused by a threatening event, or<br>– enables detection and/or investigation of a threatening event. |

| TERM | DEFINITION |
|---|---|
| Single factor authentication | An Authentication process in which a single form of Evidence is used to authenticate the user.<br>In the case of Identity Authentication, this involves one of the following:<br>• an Identifier provided by the person;<br>• knowledge demonstrated by the person ('something you know');<br>• an act performed by the person (something you can do);<br>• a Credential provided by the person ('something you have');<br>• a Biometric surrendered by the person ('something you are' or something you do). |
| Shared information | Information known to the user and the party seeking to authenticate the user. This is often not information that has been specifically collected to enable authentication.<br>eg date/amount of last payment; address; date of birth |
| Shared secrets | Information specifically stored in order to enable authentication.<br>eg mother's maiden name; favourite colour; etc |
| Smart cards | A hardware token, usually taking the form of a credit-card sized plastic card with an embedded chip.<br>May be used as a hardware token to carry information for authentication including digital certificate. |
| Soft certificates | Digital certificate and associated private key stored on a user's computer. |
| Threat | A circumstance that could result in harm to an entity, for example, an earthquake, electricity failure, vandalism, malware (eg virus, trojan), software bug. A threat may be natural, accidental or intentional. |
| Threat assessment | A process to identify and examine the nature and implications of threats to an entity's assets. |
| Threatening event | An actual occurrence of a threat. |
| Token | A physical thing, issued as a Credential. A Token is likely to include security features intended to render it difficult to forge, and tying it in some manner with the particular Entity.<br>Examples include 'identity cards'(especially 'photo-id'), smartcards, one-time-password devices (eg RSA SecurID) and 'dongles'. |
| User-ID | A string of characters that is issued to an Identity, and is included within an Access Control List, and which thereby has Permissions, and is subject to Restrictions, in relation to Access to System Resources.<br>Also referred to as LoginID and User Name.<br>Normally used in conjunction with a Password or PIN, and possibly also a Token, in order to enable Authentication. |
| Vulnerability | The susceptibility of an entity to a threat, in the form of a weakness that may permit a threatening event to give rise to harm. Safeguards are intended to reduce vulnerabilities. However, they may also increase them, or may create new vulnerabilities. |
| Vulnerability Assessment | A process to identify and examine the nature and implications of the vulnerabilities of an entity's assets. |

| TERM | DEFINITION |
|---|---|
| WAGAF | The proposed Western Australian Government Authentication Framework.<br>The Framework covers the rules to be applied to authentication of entities when dealing with them online.<br>The Framework provides a risk management approach to authentication that aligns business needs and processes with appropriate authentication solutions and technologies. |
| WoWAG | Whole of Western Australian Government |

# Appendix B – Trust Models

## Purpose and Scope

This appendix details the broad characteristics of three authentication trust models in use today:

- Silo Model
- Scheme or Community Model
- Federated Model

The following does not address any issues of EOI (evidence of identity), except to the extent that the models recognize (to varying extents) that various strengths of EOI exist and might be appropriate operationally.

Nomenclature in this document does not necessarily comply with the draft Glossary.

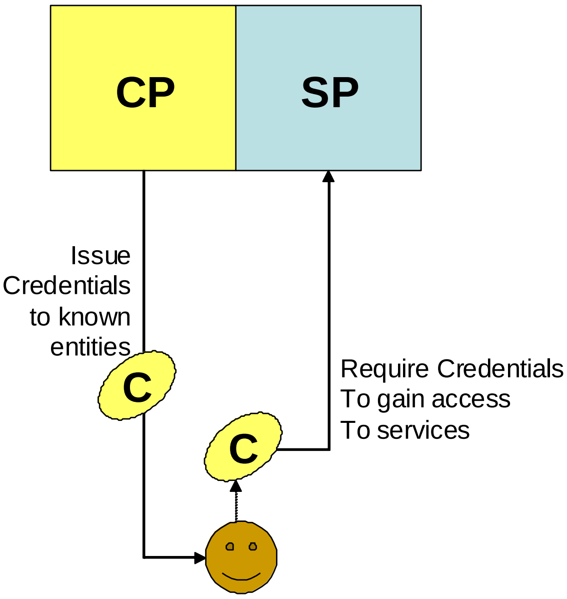
## Silo Model

Traditional online systems, as might be operated by a bank or airline, typically involve the service provider managing all aspects of:

- identification, registration, suspension and deregistration of users;
- provisioning and ongoing support of those elements required to connect online (user-id, passwords, tokens etc);
- authenticating users when they are connected;
- allocating and enforcing permissions to the user for access to business applications based on their underpinning business relationship; and
- maintaining a suitable level of auditability over operations.

In effect, these organisations are both "Credential Providers" (CP) and "Service Providers" (SP) to their customers for the purposes of their customers' dealings with the organisation.

The associated terms and conditions of use are often single purpose even within the organisation and it is not unusual for customers to have multiple online "identities" even for dealing with the one organisation. The different identification and authentication mechanisms used by banks today for Internet banking (user-id and password) versus access to funds at point of sale (account card and PIN) is an example of this.


CP
SP
Issue Credentials to known entities
C
C
Require Credentials To gain access To services

In government there are a number of examples of silo implementations including:

- ATO's digital certificate which is issued by the ATO for exclusive use of the ATO prospectively across a range of ATO applications.
- WA Government Landgate system that issues credentials for the sole use of Landgate users.

<u>Key Elements</u>

Key elements of a Silo Model are:

- As the relying party is also the issuer of the Identity and Credential, it has full knowledge of and total control over all elements of the identification, registration, issuance and management of the "identity".

- The authorized usage of the Identity/Credential is explicitly defined by the issuer of the "Identity /Credential" in Terms and Conditions of Use (T&Cs) and these are agreed to by the user. These conditions incorporate (amongst other things) the responsibilities and obligations of both parties when services are accessed using the Credential, and typically the duty of care in protecting the Identity/Credential. Whether a user really understands the implications of the T&Cs is arguable.
- There is typically no reliable way for third parties to leverage a silo identity. There are two elements to this;
  - the first being there is usually no way that the third party can validate the credential at time of presentment. This is true even in a PKI certificate-based scheme, as whilst the third party might be able to validate a signature, it cannot validate the current certificate status due to lack of access to the CRL (certificate revocation list) etc.
  - secondly, the third party doesn't have a business relationship with the Credential Provider that would give it the necessary recourse in case of disputes with the user.

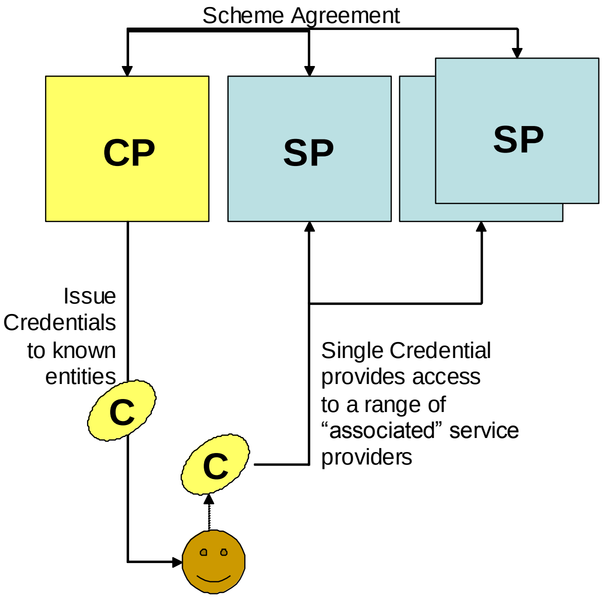
### Community or Scheme Models

The first progression towards a multi-use identity is the Community or Scheme model as depicted in Figure 2.

This model provides for multiple Service Providers utilising identities issued, usually by a single Credential Provider. There is a hybrid model where multiple Credential Providers may exist. Normally, in this case the Credential Providers will be bound by the rules of a 'scheme' that ensures equivalent levels of assurance as well as technical/operational interoperability.

Such a model must be underpinned by:

- A Scheme Agreement which defines the relationship between the Credential Provider and Service Providers addressing, amongst other things, warranties in respect to identity veracity, operational matters relating to identity and credential registration and validation services offered by the Credential Provider etc.
- Service Agreements between the end users and Credential Provider addressing registration and EOI, care of credentials, liability in the case of loss or miss-use etc.
- Service Agreements between the end-user and Service Providers which would encompass the provision of services, authorization of transactions etc


Scheme Agreement
CP
SP
SP
Issue Credentials to known entities
C
C
Single Credential provides access to a range of "associated" service providers

In practice these schemes might originate commercially where organisations align in order for one (or more) to leverage the pre-existing authenticated user base of another, or they might result from a true coincidence of interests where the "scheme" comes first and Credential Providers, Service Providers and customers enlist later. Traditionally the latter has been the more usual case.

Examples of the latter include:

- HIC's implementation of a PKI based scheme (HeSA [Health e-Signature Authority]) for use by participants in the healthcare sector. In this case Service Providers are also customers within the scheme, and the Credential Provider is CyberTrust, as the Certification Authority, based on registration effected by HeSA.. HeSA certificates are accredited under the Gatekeeper program.

- Identrus[20], as implemented in a single bank environment, where the bank issues certificates to its customers that can be used to authenticate these customers in their dealings with Service Providers (eg suppliers of goods and services) participating in the scheme.

  Importantly, the Identrus scheme is in fact a multi bank scheme, whereby there are multiple issuers, but all bound by the same over-arching scheme rules. In operation, Service Providers have an Agreement with a single bank (Credential Provider) who is a party to a broader Scheme Agreement (for Credential Providers). As such the bank warrants any Service Provider's claims against another bank (Credential Provider) in respect to veracity of identity etc.
- The ABN-DSC[21] within the Australian Australian Government's Gatekeeper program, provides an identity scheme which has many of the properties of a Scheme model, albeit there are a number of significant differences which tend to push it towards a more federated model as discussed later. Key differences between ABN-DSC and say Identrus include:
  - The ABN-DSC like Identrus has multiple instances of Credential Providers. However in the case of ABN-DSC there are differences between Providers in respect to their acceptance of liabilities (warranties) and service levels relating to revocation of credentials. A further difference has been the absence of a mechanism/facility that gives a single port of call to validate credentials potentially emanating from multiple Credential Providers. This point is being addressed in government by the creation of the BAF (Business Authentication Framework), a single point facility, that aims to resolve these differences.
  - ABN-DSC is not really a Scheme. Agreements between the Credential Provider and the Service Providers do not exist. Instead there are unilateral arrangements (CPS and CPs) imposed on any relying parties.

    Notwithstanding the above, for the purposes of this analysis, the ABN-DSC is considered a Scheme.

Key Elements

Key elements of a Scheme or Community Model include:

- Arrangements between all participant types (Credential Providers, Service Providers and Users) are consistent and understood.
- The notion of a single identity, usable with a range of Service Providers is supported. Unlike the silo model, the mapping of the "identity" to an individual Service Provider's knowledge of the identity (such as an internal reference number/key etc) is not necessarily implicit in the identity. Hence an "enrolment" or registration process may be necessary during the first connection to a Service Provider.
- "Opting in" to use the scheme in its all its breadth is implicit in usage. That is, a user will likely seek out "acceptors" of their Credentials in much the same way that a shopper might elect to use a MasterCard for payment having sought out a merchant that accepts that payment credential; the shopper understands the scheme, its rules and obligations, and receives a consistency in experience in respect to operations, resolution of disputes, loss of credential, cancellation of Agreement.
- Privacy elements are dealt with in the Scheme rules.

[20] A global bank-based online trust scheme - wee www.identrus.com

[21] Australian Business Number Digital Signature Certificate

- The notion of "identify once and transact often" is neither directly supported nor obstructed by the Scheme Model, however the consistency of authentication (and the underlying EOI etc) implicit in the scheme enables an authentication completed by one Service Provider to be recognised by another, relieving the end user with the need to re-authenticate as they complete business across the Internet.
  Explicit provisions for such recognition (including protocols to transfer authentication or identity information) could be provided for in the Scheme rules or could be provided for through bilateral agreements between Service Providers. Neither HeSA nor Identrus provide for this within their architectures.
- As there is a single Credential Provider in use, implementation issues of knowing where to go for authentication, what is the class of credential etc are avoided, and as such a gateway, direct, or hybrid mode of access to service Providers is possible. As discussed earlier, the government's current BAF initiative is intended to simplify any management of diversity in any case.

### Federated Model

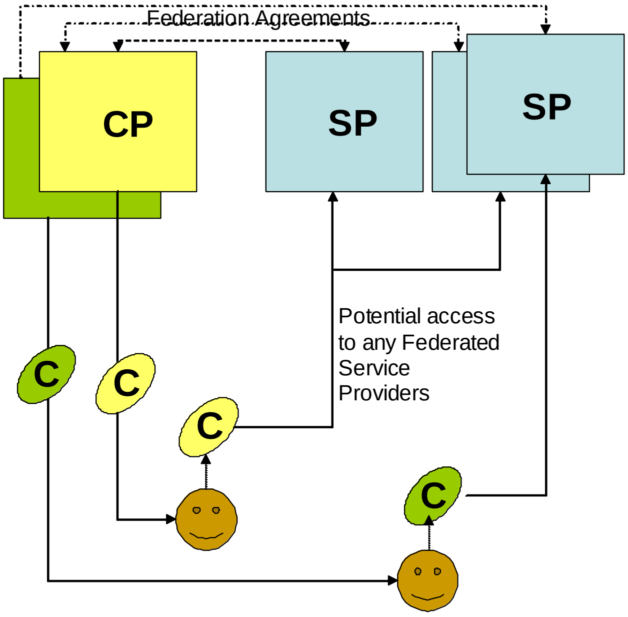
A Federated Model of identity management incorporates the following notions:

- There is more than one Credential Provider and each of these Providers issues identities and credentials that have an associated authentication "class" which relates to the strength of the identification process (EOI) and the strength of the authentication method used in the authentication process. For example, is the authentication method a user-id and a password, or a smart card based certificate created in a sterile environment.
- Service Providers (which may also be Credential Providers) "federate" with Credential Providers to enable Credential Providers to offer greater levels of service to their Subscribers (end users) and for service providers to gain access to large authenticated (potential) customer bases.
- Once Service Providers and Credential Providers have federated, Subscribers will be advised and offered the option of "opting in" so that they may utilize their "identity" when dealing with the newly federated Service Provider. The subscriber might or might not already have a relationship with this newly federated Services Provider. The principle advantage in the model is the ability of a subscriber to move between Service Providers, potentially without needing to re-authenticate along the way. This makes the model particularly relevant to "joined-up" government applications.
- In offering services to Subscribers a Service Provider will be able to offer services based on the authentication class of the Subscriber. Conceivably a subscriber might have credentials which are of different classes.

In a private sector environment it is expected that such arrangements could be quite fluid with Service Providers opting in and out of federations. These would likely be geared around some common interest with potential for incentives etc which could deliver something akin to dynamic loyalty programs.

In implementation, the following agreements are envisaged:

- Service Provider to Credential Provider which sets out the nature of the EOI and authentication methods used and associated commercial elements including confidentiality obligations, warranties, operational performance standards for revocation, validation etc of identities.



- Credential Provider to Subscriber Agreement which would be similar to the Scheme Model agreements but would be extended to accommodate rights and obligations of each party relating to the subscriber opting in to a federation offer from a Service Provider.
- Subscriber to Service Provider Agreements would again be similar to the Scheme Model, with extensions to accommodate federation.

Importantly, in its basic form there are no over-arching "scheme" rules with each act of federation being effected by bilateral arrangements between Service and Credential Providers and similarly, independent arrangements between Providers and the Subscribers. In practice it would seem necessary to have minimum standards for participation and some regime of classification for strength of identity etc.

Implementations of federated systems are in early stages with leadership in this area being provided by Liberty Alliance, a consortium of service providers, Credential Providers, technology companies and government agencies, based in the USA. Liberty's aim is the development of business and technology architectures and technology standards to support implementation. Companies such as PingId in the USA are working towards adding a particular legal framework to the model whose instance would really form an operational "scheme".

Individual technology approaches (outside the scope of Liberty) are operational in the field and are typically using SAML or Microsoft WS* standards.

<u>Key Elements</u>

Elements which are relevant in the context of government adoption of a federated approach are:

- The model supports multiple classes of identification and authentication and enables Service Providers (government agencies) to accept or reject these classes by federating or not.
- In theory the model (Liberty at least) is Credential Provider centric, with initial logon to the Credential Provider being part of the usual flow in order to gain the benefits of federation. In implementation this could well present some interesting issues and probably necessitates some sort of common gateway approach (as is being proposed/implemented by the national governments of Canada, the US and Ireland).
- Again within the Liberty scheme, the Credential Provider maintains the identity of the subscriber and relates this "identity" to Service Providers via an "alias" that is shared only with that Service Provider. As the subscriber federates with other Service Providers, a new and independent alias is utilised. The use of aliases resolved through Identity Mapping and a related enrolment program as for the Scheme Model in as much as there is no contextual or identity information passed to the Service Provider.
- This is not to say that in an alternate implementation of a federated model that a more meaningful identifier could not be passed around. The advantage of the use of aliases is that Service Providers cannot collude to aggregate information about a subscriber. It does however place a Credential Provider in a position of privilege.
- By the nature of the Liberty implementation model
  - single sign-on is supported
  - authenticate once and transact many characteristics are supported
  - pseudonymity is supported.

In considering options it is important to recognize that variations of the federated model (to that described above, which is Liberty Alliance oriented) could well be utilised which maintain the essential features of:

- Multiple Credential Providers and classes of EOI and authentication mechanisms in order that government agencies can better align their costs, convenience of user access and simplification of application development with their business risks.
- Users "opting in" to a federated environment; the issue here is really whether choosing not to opt-in effectively restricts the user from the services offered electronically (or at all).

# Appendix C – Identity Authentication Assurance

The WA Id&AM Framework proposes the definition of authentication assurance levels with the assurance level being a function of the respective strengths of the underpinning registration method and an associated authentication mechanism the latter being a product of credential strength and the authentication protocol used to verify the identity online.

This is shown in the matrix below matrix is shown below.

**Authentication Assurance Level Matrix**

| Strength of Registration of Entity, Identity, or Attribute | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 4 | Low (2) | Moderate (3) | High (4) | High (4) |
| 3 | Low (2) | Moderate (3) | Moderate (3) | High (4) |
| 2 | Low (2) | Low (2) | Moderate (3) | Moderate (3) |
| 1 | Minimal (1) | Low (2) | Low (2) | Low (2) |

**Strength of Authentication Mechanism**

The relationship between these elements is described in the following sections.

Key points are:

- The Authentication Assurance Level is a function of the strengths of the underpinning Registration Method and the Authentication Mechanism.
- There are two broad categories of Authentication Mechanisms:
- Credential based mechanisms which rely on the use of arbitrary “secrets” maintained by the user to facilitate the authentication.
- Authentication Mechanisms that don’t rely on “secret” information. These include knowledge based authentication mechanisms and biometrics.

For credential based authentication, as depicted in the diagram below, the strength of the Authentication Mechanism depends on the strength of the credential (password, hardware token, smart card etc, but not biometric) and the method or protocols deployed in its use. These elements are defined and described further below.

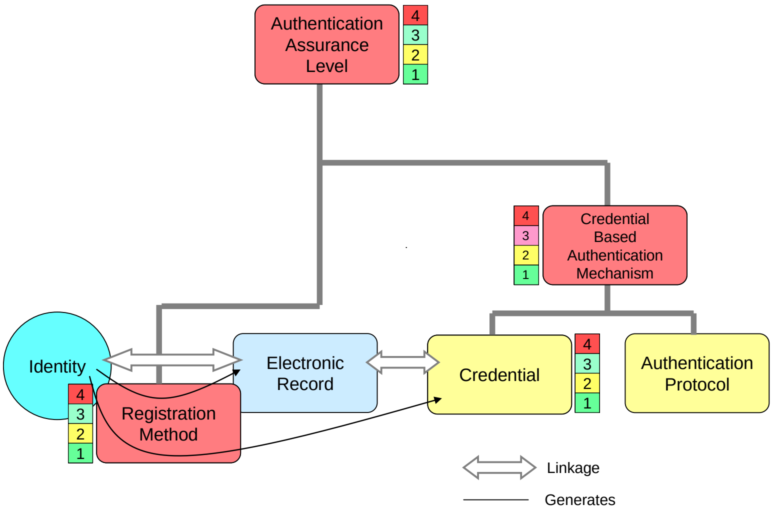
## Credential Based Authentication Mechanism Components

The diagram below shows the major components of a Credential Based Authentication Mechanism, highlighting the relationship between the registration method and the issued credential.

### Credentials

A credential is something used to authenticate a user’s identity. The user possesses the credential and controls its use through one or other authentication protocols. A credential incorporates a password, cryptographic key, or other form of secret. The form factor of the credential may be a physical device such as an RSA one time password token, a smart card, a code book, or simply the user’s knowledge of the secret.

A credential is linked to the registration method via an electronic record which underpins the linkage of the credential with the user or identity. A record may include digital certificates, a record in a database or directory, or other electronic records which can be accessed by the relying party to validate the linkage.



### Authentication Protocols

In considering the strength of various credentials it is critical to consider a number of elements in their implementation and usage collectively referred to as Authentication Protocols. These typically relate to various measures surrounding the credential which define and complement its usage or define its integrity in various contexts.

For instance, the assurance level which can be associated with the use of a password as a “something you know” type of credential is affected markedly by the method and confidentiality of the transfer of the password between the user and the relying party, the security over storage of the password at the relying party location, the methods deployed to verify the password and the overall policies of management of the password in regard to password change frequency, password lengths, password structure, password resetting etc.

For authentication mechanisms that utilize cryptographic elements, the protection of the secrecy of the cryptographic keys is a critical element in the assurance level that can be assigned to the authentication mechanism. In many cases a cryptographic token, such as a smart card or handheld device, can provide both a “something you have” factor as well as addressing the security of cryptographic keys and associated cryptographic processes which can be stored within or performed entirely within the device respectively.

The WA Id&AM Framework Action Plan incorporates authentication protocols for various credential-types and assigns related authentication mechanism assurance levels on the basis that the authentication protocols are adhered to within the implementation.

Where application developers develop their own authentication protocols involving the use of various credentials to meet specific business requirements or situations, these protocols should be formally evaluated.

## Credential Based Authentication Mechanisms

The following provides definitions and descriptions of common credential based authentication mechanisms, their usage protocols and characteristics.

All of the following utilize, in one way or another, secrets held by the user that can be validated by a relying party. Dependent on the credential type and authentication protocols adopted, these secrets may be created or generated by either the user or the relying party or the credential issuer.

Importantly, where there is an instance or suspicion of exposure of these secrets over time, the secrets can be quickly replaced and relying parties informed of the replacement, thereby mitigating the risks of persistent identity fraud.

### Passwords

The term ‘Password’ is used here to refer to a string of characters provided by the user during the authentication process.

Usage

A primary authentication credential to access electronic services.

Applicable across various channels (Internet, phone etc).

Assurance level is variable dependent on the protocols for generation, management, submission and verification of the password.

Characteristics

- Depends on users remembering the password, or (less securely) storing it in a form accessible to themselves and no-one else.
- Passwords are persistent for a period of time and reusable.
- Typically their structure and use are controlled by policies in respect to password length, password content and structure, change period etc.
- For online usage, passwords are typically transferred between the end user and the application encrypted using a protocol such as SSL
- The "secret" is disclosed as part of the authentication process.
- Passwords can be changed periodically and when deemed necessary (e.g. because of concern that they may have been compromised)

**Shared Secrets**

This refers to a process in which the party performing the authentication issues a series of prompts to which the user is required to respond.

Usage

A tenable but weak primary authentication credential to access electronic services

A secondary authentication credential to improve the strength of authentication during transaction processing.

Applicable across various channels (Internet, phone etc).

Assurance level is variable dependent on the protocols for collection, management and verification of the "secret" information.

Often used in lower assurance level situations as part of password reset and similar processes.

Characteristics

- Depends on users remembering the secrets, or (less securely) storing them in a form accessible to themselves and no-one else.
- Typically the secrets (and related prompts) are established by the user during a registration process, possibly by selection from a limited list of options. Examples include "first school", "favourite pet" etc.
- The question-answer selection and sequence should be varied.
- The exchange needs to be over a secure channel, e.g. using SSL to encrypt the sequence.
- The secret(s) is/are disclosed as part of the authentication process.
- Secrets can be changed periodically and when deemed necessary (e.g. because of concern that they may have been compromised).

**One time passwords**

A "one-time password" is a string of characters that is used once only. It offers the prospect of considerably higher assurance, but requires greater investment in infrastructure and processes.

Usage

A primary authentication credential for access to online services.

Applicable across various channels (Internet, phone etc).

Assurance level is variable, dependent on the protocols for generation, management, submission and verifying the password.

Characteristics

- The stronger forms of one time passwords (OTP) are typically generated at the user location and submitted to the application for authentication..
  In this case, the OTP is typically algorithmically generated using a cryptographic key (the secret) and other dynamic information such as time of day such that the OTP changes in discrete intervals over time, or in some other manner for successive authentication attempts.

OTP generation is typically performed entirely externally to the PC and in a separate user controlled hardware device (smart card, discrete portable electronic device) which protects the cryptographic keys and processes.

Unlike in the Shared Secret based authentication described above, the cryptographic keys which underpin this credential type and the generation of the OTP, are never exchanged between the user and the relying party during identity authentication processes.

Access to the hardware device may be protected by an access code or biometric, although some systems such as display devices require no authentication of the owner in order to retrieve the OTP.

Such devices typically, but not exclusively, utilize symmetric key encryption.

- Alternatively, OTPs can be generated by the central application and forwarded to the user by an alternate independent and secure channel such as:
- Paper based code book with OTPs listed by sequence or date.
- SMS message transmitted as a result of logon request.

In these instances, possession of the device / code-book is generally considered sufficient evidence of ownership, with no need for additional access codes.

Clearly methods that involve some form of protection against unauthorized access to the OTP, such as an access code, are stronger than those that rely only on possession of the display device, code-book or phone.

**Challenge-response**

This is a variation of the shared secrets approach, whereby the prompt and response are generated and authenticated with the aid of cryptographic tools.

Usage

A primary authentication credential for access to online services.

Applicable across various channels (Internet, phone etc).

Assurance level is variable dependent upon the methods of generation, management, submission and verification of the response.

Characteristics

Similar to one time password and relies on a secret (cryptographic key) held by the user in combination with selected “challenge” information. The resultant “response” is submitted to the application where it is verified.

The response is often generated in a separate hardware device (smart card, token). Access to the device would typically be via an access code or biometric.

The “challenge” data which is used to generate the “response” is typically generated at a central application system either randomly or contextually based on (say) message content in the case of message authentication. In the latter, the message would require some randomized or dynamic content, such as time of message receipt, or unique serial number, to avoid replay attacks.

Alternatively the challenge may be generated locally within the user system based on (say) message content. Advantages of this method include implicit support of digital signing (message authentication) as well as identity authentication. Moreover, unlike dynamic "time based" OTP's as described above, challenge-response authentication mechanisms result in "responses" that remain verifiable indefinitely.

Can utilize symmetric or asymmetric keys.

Challenge-response is the common mechanism for the use of asymmetric keys and certificates in authentication applications. SSL implements challenge – response as a core part of its authentication protocol.

## Non Credential Based Authentication Mechanisms

The authentication mechanisms described above utilize "secrets", held by the user, that have been established specifically for the authentication process and can be established and re-established as required as part of day to day operations with little or no affect on a user's dealings with other parties.

Other authentication mechanisms exist which instead rely on existing information in respect of the user. Most commonly, these mechanisms rely on knowledge of either biometric or behavioural information regarding the user. In other cases, the information may not be about the user, but about an organisation, attribute, event or transaction. The information which is either unchangeable or relatively static or "sticky", is held in a variety of repositories and is required for a variety of other reasons apart from authentication.

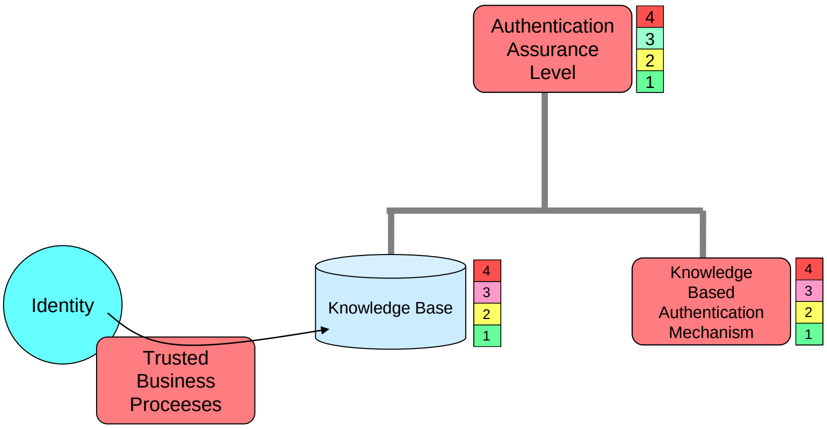
The information is thus vulnerable to being gained by an attacker, particularly if the information is frequently used.

Accordingly, whilst these mechanisms may be suitable, and necessary, for some elements of an authentication process, they are not by themselves considered suitable as mainstream online transactional or session authentication mechanisms.

### Knowledge Based Authentication

This refers to a process in which the user provides information to the party performing the authentication, most commonly in response to prompts. It is distinguished from password and other shared secret processes in that the information provided is knowable by other parties.

It is shown schematically below.


Authentication Assurance Level
4
3
2
1
Identity
Trusted Business Proceeses
Knowledge Base
4
3
2
1
Knowledge Based Authentication Mechanism
4
3
2
1

Usage

A primary authentication mechanism in an online registration or enrolment process for businesses and individuals.

Only limited use as a secondary authentication mechanism due to potential broad awareness of such knowledge amongst peers and associates and the extent of the information required to establish a (high) assurance level.

Attainable assurance level is variable based on extent to which the information is accessible by people other than the user.

Where the information relates to a human user, and especially where that user is acting as an agent for an organisation, the party performing the authentication may be constrained by privacy law and policies.

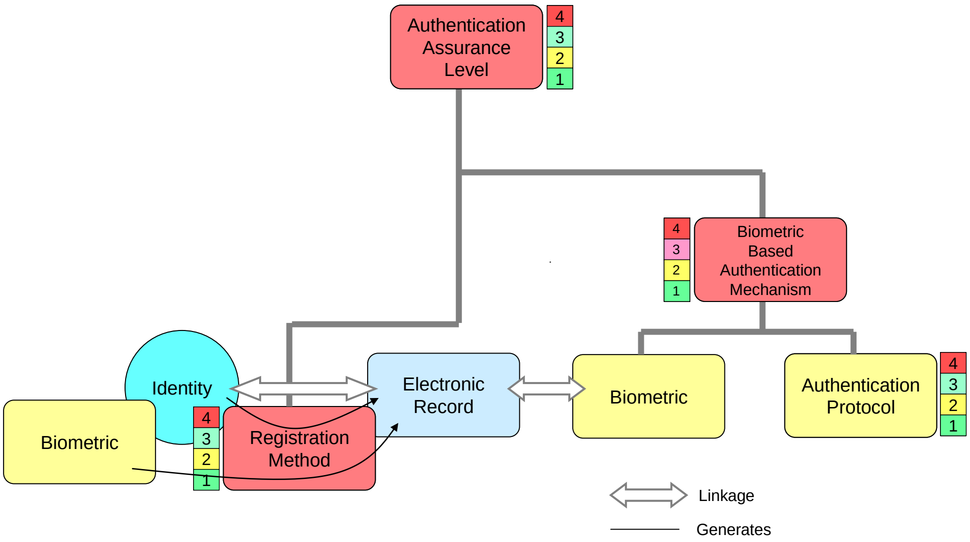
Characteristics

- Typically the knowledge request is based on information held by the relying party (and potentially others) in respect to prior dealings with the identity. This could include company number, address, date of birth of user, prior lodgement details, data describing the most recent transaction on the account, etc.
- Online validation is via a question answer sequence.
- It is desirable that the exchange be conducted over a secure channel, e.g. using SSL to encrypt the sequence.
- Knowledge is disclosed as part of the authentication process.
- Generally, some of the information used is static but some information changes, and additional items become available for use over time. The authentication protocol needs to provide for the refreshing of knowledge based questions when used as part of online authentication process.

### Biometrics

This refers to a process whereby a measure is taken of an attribute of a natural person's physical self, or of their physical behaviour, and compared against a previous measure of the same attribute. Examples include fingerprints, iris scans, hand geometry, and voice-prints.

The components of biometric based authentication are shown schematically below.



Usage

A primary means by which a person can protect a stored secret.

A potential means of performing human identity authentication based on some physical characteristics of the entity to which the identity assertion relates.

Due to the necessary "matching" elements of biometrics between a previous "sample" and a presented sample, the integrity of biometric authentication depends on the integrity and reliability of the biometric management and matching processes, in addition to the premise that the biometric-type is unique across the relevant population and as such represents a reliable authenticator of an identity assertion.

Increasingly, due to privacy and related issues, biometric authentication is being effected under the direct and sole control of the user and is being used (or proposed) as an alternative to user access codes, such as PINs, to provide access to smart cards or other hardware devices which are subsequently used to enable token based user authentication in the broader sense as described above.

Characteristics

- Biometrics have the advantage that they are not easily lost by the user, resulting in higher convenience and less help-desk support.
- Knowledge is static (you can't change your fingerprints), is not secret (your fingerprints are on your coffee cup), and knowledge is disclosed as part of the authentication process. If identity fraud occurs by spoofing a biometric, that biometric must be abandoned for that user. Spoofing attacks are comparatively easy for many types of biometrics.
- Due to the nature of the information being measured, perfect matching of a new reading and a previous sample is not possible, so a decision needs to be made if the match is "close enough". This means that there will be a percentage of false-positives (fraudulent access allowed) and false-negatives (legitimate user denied access). Biometric systems can typically be tuned to favour one or the other.
- Reliable authentication requires that the Relying Party can be sure that a real person is being read (not a severed finger, fake fingerprint, pre-recorded voice, contact lenses instead of iris, etc), that the biometric reader device is trustworthy, that information supposedly coming from the biometric reader has not been subverted during communications (eg replay of previous good read). Biometrics are thus generally unsuitable for remote authentication. They are most suitable where the reader device is being monitored and the reader device and all communications back to the relying party are under the control of the relying party.
- A significant percentage of the population will be unenrolable for any specific type of biometric eg some manual labourers have unreadable fingerprints, people may be missing limbs, unable to speak, etc.

### Multi-factor Authentication Mechanisms

Over many years the concept of identity authentication has been presented as having potentially three factors which are used together or separately to verify an identity assertion of an individual, and hence indirectly of an organisation.

These factors have been termed "something you know", "something you have" and "something you are".

Traditionally there has been a view that a combination of factors from two or three categories will provide stronger authentication than achievable from a single factor.

There are many examples of traditional two factor authentication in common use in government and industry today including the use of credit cards (something you have) initially along with signatures (a combination of something you know and something you have), and later the use of PINS (something you know). Without these two factors being present (as is the case for credit card transactions completed over the phone), issuing banks will not honour claims by merchants where disputes arise. Where they are present, issuing banks will honour such claims.

Whilst the use of multi-factor mechanisms for authentication has been adopted broadly in authentication of identity in online systems, the basis of the practice is really more to do with mitigating risk through the use of multiple independently assessable elements (within the risk context) to establish appropriate assurance levels, rather than strict adherence to the combination of the "know, have, are" factors – e.g. a combination of two or more 'what you know' factors may be used.

Increasingly changing threat and risk environments are resulting in the adoption of broader solutions geared at addressing these specific threats as they arise.

Many of these solutions involve the use of electronic and real time “out of band” communications using a separate communications channel (by phone say), between the authenticating party and the user much as might have been attained through traditional telephone call backs to confirm customer requests transferred by mail or fax and the use of physical mail for the distribution of PINs to cardholders.

It is a moot point whether these new multi-channel authentication approaches are “know, have, are”; the important thing is that the multiple security factors that are used to establish the required assurance level and provide protection against specific attacks and associated impacts are independent from one another.

**Accordingly, the concept of “factors” as traditionally described is considered as increasingly dated and can potentially lead to inappropriate or sub-optimal treatment of threats. A more structured approach using Threat and Risk Assessment methodologies is more likely to ensure selection of the appropriate authentication mechanisms (or combinations) and associated tokens (and protocols) for particular application requirements.**

## Appendix D - Commonwealth Government Protective Security Manual

The *Commonwealth Protective Security Manual* (PSM) was developed and is maintained by the Protective Security Policy Committee operating under the aegis of the Attorney-General's agency, in particular, the department's Protective Security Coordination Centre.

The PSM 'sets out the policies, practices and procedures that provide a protective security environment that is not only fundamental to good business and management practice, but essential for good government. It also lays down the procedures designed to ensure that *agencies and departments* approach protective security measures in a way that is consistent across government'.[22]

The PSM applies to more than just information security and therefore provides the broadest security or assurance context within which Id&AM may be implemented.

The PSM consists of eight parts:

- Part A – Protective security policy
- Part B – Managing security risk
- Part C – Information security
- Part D – Personnel security
- Part E – Physical security
- Part F – Security framework for competitive tendering and contracting
- Part G – Security incidents and investigations, and
- Part H – Home-based work.

A brief synopsis is provided below of the parts of the PSM that are particularly relevant to the overarching environment within which the AGAF is to be implemented.

**Part A** (protective security policy) of the PSM:

- requires that: 'each agency must create and maintain an appropriate security environment for the protection of its functions and official resources.'
- notes that:
  - '[in] practice, the day-to-day management of protective security arrangements in a Commonwealth agency is the responsibility of the agency head'
  - the legislative context (for protective security) includes the following Acts:
    - Crimes Act
    - Public Service Act
    - Agency-related Acts (e.g. Income Tax Assessment Act; Social Security Act)
    - Freedom of Information Act
    - Privacy Act
    - Archives Act
    - Occupational Health and Safety (Commonwealth Employment) Act
  - '[security] measures are sometimes expensive to implement and might have an impact on agency operations. Therefore, the government needs to be assured that protective security measures are only used when the risk warrants it and that any security measures used are appropriate to the identified risk'

[22] Excerpt from Foreword to the PSM 2000.

- requires that:
    - agencies develop ‘a security plan’
        - ‘[agencies] should implement audit trails on their IT systems, recording events subject to access control’
        - ‘[frequent] audits should be undertaken by the ‘information technology security adviser’ (ITSA) to ensure that agreed security measures are being followed’
    - recommends a governance structure encompassing an ‘agency security adviser’ (ASA) and an ITSA reporting to a ‘security executive’ who, in turn, reports to the ‘agency head’.

**Part B** (managing security risk) of the PSM:

- defines a **security risk** as ‘the likelihood and consequences of compromise of official resources’
- provides ‘a methodology to help the agency security adviser (ASA) or equivalent to identify, assess and treat security risk. The methodology is based on the principles of general risk analysis and risk management as outlined in the *Guidelines for managing risk in the Australian public service* (Australian Government Publishing Service, October, 1996) and the *Australian/New Zealand standard on risk management* (AS NZS4360:1999)’
- recommends a ‘security risk management process broken down into six basic steps:
    - gather information
    - identify the risks
    - analyse the risks
    - assess and prioritise the risks
    - treat the risks (and prepare the security plan)
    - monitor the risk environment and evaluate the security plan’
- highlights that the government has a series of policies that must ‘form part of every agency’s security criteria:
    - expectations about the care and confidentiality to be given to official information (for example, the *Public Service Act 1999* and associated regulations and the *Crimes Act 1914)*
    - the availability of official information to the public (the *Freedom of Information Act 1982*)
    - expectations about the collection, use and care of personal information (the *Privacy Act 1988)*
    - expectations about the well-being and personal security of staff (*Occupational Health and Safety (Commonwealth Employment) Act 1991*)
    - the measures and procedures agencies must adopt to protect official resources from fraud (Commonwealth fraud control policy)
    - the expectation that there will be a Commonwealth-wide system for providing appropriate protection to security classified information (Commonwealth protective security policy)’
- points out that ‘while the PSM provides some guidance on IT&T security, more detailed technical advice is available from Defence Signals Directorate (DSD) and from ACSI 33, ACSI 61 and ACSI 57’
- advises that ‘[to] lessen the adverse consequences of a risk, treatments should, where appropriate, include continuity plans. Continuity planning results in a set of planned procedures that enable agencies to continue or recover their services to the government and the public with minimal disruption over a given period, irrespective of the source of the disruption’

- recommends that 'the agency must conduct regular, preferably annual, evaluations of its security plan to determine whether or not the security objectives have been achieved. The agency must also consider whether they were achieved in the most cost-effective and efficient way'.

**Part C** (information security) of the PSM:

- states that 'The Commonwealth Government collects, receives and develops information to fulfil its functions (for instance, develop policy, establish programs and provide services). The government expects its agencies and contracted service providers who use and keep this information to recognise that it is a valuable official resource, that they do not own but hold on behalf of the Australian people'
- requires agencies to determine whether, 'particular information resources require protective security measures to ensure their:
  - confidentiality
  - integrity
  - availability'
- states that '[the] need for confidentiality is met by limiting the availability of information to authorised users for approved purposes. The confidentiality requirements for official information are determined by referring to the likely consequences of unauthorised disclosure'
- defines:
  - **integrity** as 'the assurance that information has been created, amended or deleted only by the intended authorised means'
  - **availability** as 'the desired state that allows authorised users access to defined information for authorised purposes at the time they need to do so'
- states that:
  - '[each] agency should have a general security policy. This security policy must be a formal document, available to all those who access the agency's resources. The information security policy should form part of the agency's general security policy and the agency's information management policy'
  - responsibility 'for making the decisions about what requires protection and what type of protection is most appropriate … must remain the responsibility of the manager with functional control of the resource'
- differentiates between systems where 'standard protection levels' are adequate and those requiring 'enhanced protection levels'
- outlines some protection options including:
  - 'procedural training and awareness for staff
  - attention to access control for authorised users
  - proper plans for day-to-day IT support and maintenance and back-up procedures, as well as formal continuity strategies
  - implementation of auditing procedures and data integrity checks
  - clear configuration control procedures
  - redundancy in system architecture (duplication of critical resources, alternative transmission paths)
  - correctness of basic operating system and other software
  - authentication, signing and sealing techniques and associated tools
  - virus checking'

- requires that 'all use of cryptography to protect Commonwealth information must be approved by DSD and must be implemented in accordance with DSD guidelines', and that '[cryptography] products are to be selected from the Evaluated Products List (EPL)'[23]
- defines:
    - three classes of information:
        - **Public Domain**
        - **Unclassified**
        - **Classified** – divided into national security and non-national security categories.
    - four categories of national security classifications:
        - **Restricted**
        - **Confidential**
        - **Secret**
        - **Top secret**
    - three categories of non-national security classifications – **In-confidence***,* **Protected** and **Highly-protected**. The PSM notes that 'very little information belongs in the Highly-protected category'
- specifies requirements for:
    - protecting classified information, including staff awareness, personnel security clearances, physical access controls and 'clear-desk policy'
    - controlling classified information, including registration systems, spot checks, accountable material, filing, control of IT&T systems, certification and accreditation of IT&T systems, handling and storage of cryptographic information, logical access controls, IT system audit trails, achieving clean systems and networks, and avoiding or handling viruses and other damaging software.

[23] Cryptography requirements related to PKI-based approaches to e-authentication are also covered under the government's Gatekeeper PKI framework.

# Appendix E – National and International Standards and Guidelines

Three documents are of particular note in relation to further broadening and deepening the overall risk management and IT security backdrop against which the Id&AM Framework needs to be implemented.

## E1. Risk Management Standard – AS/NZS 4360:1999

The Risk Management Standard AS/NZS 4360:1999[24] is quoted with approval by both the PSM and ACSI 33.

AS/NZS 4360 is intended to provide a 'generic framework for establishing the context, identification, analysis, evaluation, treatment, monitoring and communication of risk'. The authors advise that 'it should be read in conjunction with other applicable or relevant standards'.

The risk management process proposed by the standard is:

- establish the context
- identify risk
- analyse risk
- evaluate risk
- treat risk
- monitor and review, and
- communicate and consult.

It stresses that risk management is an iterative process.

The risk assessment process proposed by the WAGAF is consistent with AS/NZS 4360. The table below shows how the AGAF e-authentication assurance levels map onto the two axes of AS/NZS 4360 (likelihood and consequences).

| | **Consequences** | | | | |
|---|---|---|---|---|---|
| **Likelihood** | Insignificant | Minor | Moderate | Major | Catastrophic |
| Almost certain | Minimal | Low | Moderate | High | High |
| Likely | Minimal | Low | Moderate | High | High |
| Possible | Minimal | Low | Moderate | High | High |
| Unlikely | Minimal | Minimal | Low | Moderate | High |
| Rare | Minimal | Minimal | Low | Moderate | High |

**Mapping of WAGAF assurance level requirements onto AS/NZS 4360 risk matrix**

The WAGAF recommends that agencies review the AS/NZS 4360 approach when preparing to develop an e-authentication strategy.

## E2. Information security management – AS/NZS 7799.2:2003

The *Specification for information security management systems* AS/NZS 7799.2:2003[25] is intended to be read in conjunction with ISO/IEC 17799:2001 (see below).

This standard provides a model for establishing and managing (implementing, operating, monitoring, maintaining and improving) an effective information security management system (ISMS).

[24] Copyright: Standards Association of Australia, ISBN 0 7337 2647 X.

[25] Copyright: Standards Association of Australia, ISBN 0 7337 5011 7.

An ISMS is regarded as 'that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security'. The specification notes that '[the] management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources'.

Annexure A of AS/NZS 7799 details the 'control objectives and controls', divided into:

- A3. Security policy
- A4. Organisational security
- A5. Asset classification and control
- A6. Personnel security
- A7. Physical and environmental security
- A8. Communications and operations management
- A9. Access control
- A10. System development and maintenance
- A11. Business continuity management, and
- A12. Compliance.

Agencies should have a standards-based ISMS in place. In implementing the Id&AM Framework, agencies should review their ISMS to determine where control objectives and controls are involved in the e-authentication of business to government and/or where such control objectives and controls should be implemented within the ISMS.

## E3. Code of practice for information security management – ISO/IEC 17799-2000

The *Information Technology – Code of practice for information security management* (ISO/IEC 17799-2000)[26] is regarded by its authors as 'a starting point for developing organisation specific guidance' in relation to managing information security. Information security is defined as the 'preservation of confidentiality, integrity and availability of information'.

The code of practice provides substantial detail for each of the control objectives or controls listed in AS/NZS 7799.2:2003.

The following sections are seen as being particularly significant to implementing the Id&AM Framework:

- 4.2.1 Identification of risks from third party access
- 4.3.1 Security requirements in outsourcing contracts
- 5. Asset classification and control
- 8.7.3 Electronic commerce security
- 8.7.4 Security of electronic mail
- 8.7.6 Publicly available systems
- 9. Access control
- 12.1.4 Data protection and privacy of personal information
- 12.1.6 Regulation of cryptographic controls, and
- 12.1.7 Collection of evidence.

[26] Copyright ISO/IEC.

## Appendix F - Information Systems Security Context

### Scope definition

The purpose of the risk assessment process is to undertake analysis in order to devise a comprehensive and coherent security strategy and plan. This needs to be sculpted to the context. Hence the first step is to define the scope, with reference to:

- the set of stakeholders
- the proxies representing those stakeholders (there are checklists of possible stakeholders and proxies in AS/NZS 4360:1999 (p. 28) and in Appendix E)
- the interests of those stakeholders
- the degree of importance of security in a business's strategy, for example, in relation to business continuity, and the accessibility and/or secrecy of various categories of data
- the degree of importance of public visibility of assurance of the system's security, and
- the legal requirements to which the business and its stakeholders are subject, including contracts with customers and other parties, data protection and privacy statutes, intellectual property laws, occupational health and safety, the laws of evidence, and common law obligations such as the duty of confidence, and the duty of care inherent in the tort of negligence. In addition, the requirements of the PSM and ACSI 33 should be noted.

It is highly desirable that the scope definition be formalised, and that relevant executives be exposed to it and commit to it. This sets the framework within which the subsequent phases unfold.

### Threat assessment

A **threat** is a circumstance that could result in harm to an entity (for example, an earthquake, electricity failure, vandalism, software designed to cause harm, software bug). A threat may be natural, accidental or intentional.

Agencies need to do a stocktake of the information and processes involved, their sensitivity from the perspectives of the various stakeholders, and their attractiveness to other parties. This needs to be followed by an analysis of the nature, source and situation of threats.

The nature of the threats varies, and includes access to data by unauthorised persons, disclosure of data to others, or alteration or destruction of data.

The sources of the threats include several categories of entities:

- a person who is authorised to access the data, but for a purpose different from that for which they use it
- an intruder, who is not authorised to access the data, including:
  - an impersonator (that is, someone who has 'stolen' an identity)
  - an interceptor of data during a transmission
  - a 'cracker' who gains access to data within storage, and
- an unauthorised recipient of data from an intruder.

'Locations'/'events' within which threats may occur include:

- within manual processes, content and data storage
- within the physical premises housing system facilities
- within a business's computing and communications facilities, including:
- data storage, including:
  - permanent storage, such as hard disk, including high-level cache
  - transient storage, such as RAM, including low-level cache and video RAM

    - archival storage
- software that:
    - receives data
    - stores data (for example, a file handler or database manager)
    - renders data (for example, a viewer or player)
    - despatches data
    - enables access to the data in any of the above storage media (for example, disk utilities and screen-scrapers)
- transmission, including via:
    - discrete media (for example, diskettes, CD-ROMs)
    - electronic transmission over local area and wide area networks
- within other people's computing and communications facilities, for example
    - a workstation on a trusted network that is cracked by an intruder
    - a powerful computer that is cracked, and then used to crack one or more passwords on an organisation's computers
    - one or more weakly protected machines that are cracked and then used to launch denial of service (DOS) or distributed denial of service (DDOS) attacks against an organisation's servers or networks
- within supporting infrastructure, including electrical supplies, air-conditioning and fire protection systems.

## Vulnerability assessment

The term **vulnerability** refers to the susceptibility of an entity to a threat, in the form of a weakness that may permit a threatening event to give rise to harm. Safeguards are intended to reduce vulnerabilities.

The existence of a threat does not necessarily mean that harm will occur. For example, it is not enough for there to be lightning in an area for harm to occur. The lightning has to actually strike something that is relevant to the system. There also has to be some susceptibility within the system, such that the lightning strike can actually cause harm. The purpose of the vulnerability assessment is to identify all such susceptibilities to the identified threats, and the nature of the harm that could arise from them.

It is common for vulnerabilities to be countered by safeguards. For example, safeguards against lightning strikes on a facility may include lightning rods on the building in which the facility is housed. There may also be safeguards against threatening events occurring in situations remote to the system in question. For example, a lightning strike on a nearby electricity substation may result in a power surge or a power outage in the local facility. This may be safeguarded against by means of a surge protector and an Uninterruptible Power Supply (UPS).

Every safeguard creates a further round of vulnerabilities, including susceptibilities to threats that may not have been previously considered. For example, a UPS may fail because the batteries have gone flat and not been regularly inspected, or because its operation actually depends on the mains supply not failing too quickly, but it has never been tested in such a way that that susceptibility has become evident.

### Risk assessment

The term **risk** is used in many different senses (including as a synonym for what was referred to above as 'threat', 'harm' and even 'vulnerability'). But when security specialists refer to risk, they have a very specific meaning for it: a measure of the likelihood of harm arising from a threat.

Risk assessment builds on the preceding analyses of threats and vulnerabilities by considering the likelihood of threatening events occurring and impinging on a vulnerability. This is discussed in more detail in AS/NZS 4360:1999.

In most business contexts, the risk of each particular harmful outcome is not all that high. The costs of risk mitigation, on the other hand, may be very high. Examples of the kinds of costs involved include:

- the time of managers, for planning and control
- the time of operational staff and computer time, for regular backups
- the loss of service to clients during backup time
- additional media, for storing software and data
- the time of operational staff, for training
- duplicated hardware and networks, and
- contracted support from alternative ‘hot sites’ or ‘warm sites’.

Risks have varying degrees of likelihood and varying impacts if they do happen. It costs varying amounts of time and money to establish safeguards against threatening events or against the harm arising from a threatening event.

The concept of ‘absolute security’ is a fiction – it is in the nature of security that risks have to be managed. It is therefore necessary to weigh up the threats against the likelihood of risks happening and the degree of potential harm, and the cost of safeguards. A balance must be found between predictable costs and uncertain benefits in order to select a set of mitigation measures that lead to an acceptable level of residual risk appropriate to the need.

The aim of risk assessment is therefore to determine the extent to which expenditure on safeguards is warranted in order to provide an appropriate level of protection against the identified threats.

See Appendix A (Glossary) for the definition of risk assessment terms.

## Risk management strategy and security plan

There are a range of alternative responses for each type of threat, including:

- proactive strategies:
  - avoidance, for example, non-use of a risk-prone technology or procedure
  - deterrence, for example, warning signs, threats of dismissal, publicity for prosecutions
  - prevention, for example, physical and logical access control; surge protectors and backup power sources; quality equipment, media and software; staff training, assigned responsibilities and measures to sustain morale; staff termination procedures
- reactive strategies:
  - detection, for example, logging, exception reporting, fire and smoke detectors
  - recovery, for example, investment in resources, procedures or documentation, staff training, duplication (including hot sites and warm sites)
  - insurance, for example, policies with insurance companies, fire extinguishing apparatus, mutual arrangements with other organisations, maintenance contracts with suppliers, escrow of third-party software, inspection of escrow deposits
- non-reactive strategies:
  - tolerance, that is, ‘it isn't worth the worry’; ’cop it sweet’
  - graceless degradation, for example, being prepared to tolerate the consequences of a problem no matter how severe.

Devising a risk management strategy involves:

- selecting a mix of measures that reflect the outcomes of the preceding threat and risk assessments. The measures need to comprise:

    - technical safeguards. These are variously of a preventive nature, support the detection of the occurrence of threatening events, enable the investigation of threatening events, and monitor the environment for signs of possible future threatening events. Categorisations of technical safeguards are in AS/NZS 7799:2003 *Information security management - Specification for information security management systems*
    - policies and procedures. These are organisational features, in the form of structural arrangements, responsibility assignment and process descriptions
- formulating a security plan, whereby the safeguards and the policies and procedures will be put into place
- resourcing the security plan
- devising and implementing **c**ontrols to detect security incidents and investigate and address them, and to monitor whether all elements of the security plan are in place and functioning, and
- embedding audit processes in order to periodically evaluate the safeguards, the policies and procedures, the actual practices that are occurring, and the implementation of the planned controls.

**Security plan implementation**

The process of implementing a security plan must be well managed. Policies need to be expressed and communicated; manual procedures need to be variously modified and created to comply with the strategy and policy; and safeguards need to be constructed, tested and cut over.

Critically, implementing a security plan also requires developing staff awareness, educating them in the generalities, and training them in the specifics of the attitudes and actions required of them. This commonly involves a change in organisational culture, which must be achieved and then sustained.

### Security audit

No strategy is complete without a mechanism whereby review is precipitated periodically, the need for adaptation detected, and appropriate actions taken.

To be effective, an audit must be comprehensive, rather than being limited to specific aspects of security. It must follow through the entire organisation and its activities rather than being restricted to examining technical safeguards. Needless to say, this relies heavily on executives and managers committing strongly to the security strategy.

## Appendix G –Identity and Access Management Policy

### Statement of Policy

Western Australian Government agencies will use identified and approved Whole of Western Australian Government (WoWAG) standards and guidelines to ensure secure and appropriately authorised access by all internal and external users of government information technology facilities addressing requirements for identification and authentication of users, authorisation of access to particular information and assets and the auditability of this access.

### Policy Priority and Rationale

The key drivers for this policy are:

- The Government's recognition of the significant implications associated with inappropriate access to information, and the increasing risk of this happening, as network access is provided to increasing numbers of users, across increasingly wide and deep data sets and across organisational boundaries.
- The Government's recognition of the value of being able to join-up information across organisational boundaries to provide better outcomes to citizens and businesses in Western Australia, and its recognition of the significant security and privacy issues associated with this.
- From an implementation perspective, the Government's recognition that agencies are increasingly updating their ICT infrastructure and applications and that there is a current window of opportunity within which issues relating to standards, interoperability and the potential for shared services in the area of Id&AM needs to be decided.

The policy is underpinned by the following principles:

- Information is an asset and should be protected with the same care as physical assets.
- Information has custodians responsible for its safe keeping and appropriate use.
- Government is a trusted custodian of information.
- Government is responsible for security of information.
- Government is responsible for privacy and confidentiality of certain classes of information.
- Usage of information should be maximised to improve outcomes for citizens and businesses.
- Collection, processing, exchange, storage and archiving of information should be as efficient and cost-effective as possible.

In particular the Policy:

- Advocates minimum levels of integrity/robustness for departmental/agency approaches to identity and access management, designed to accommodate individual departmental/agency differences.
- Advocates adoption of a common framework, policies and practices to facilitate, where appropriate:
    - Interoperability/re-use/federation of authentication credentials
    - Interoperability/re-use of infrastructure and solutions
    - Common understanding across WA Government and its employees, contractors and outsourced service providers
    - Uniform and appropriate privacy protection for users' personal information
- Encourages best practice for identity and access management in relation to the attributes of:
    - Establishing trust and ensuring security
    - Fitness for purpose

- Cost effectiveness
- Efficiency
- Extensibility
- Interoperability

## Policy Purpose and Benefits

The purpose of this Policy is to establish consistent and appropriate approaches to identity and access management within Western Australian Government agencies/agencies to:

- Ensure completeness, integrity and robustness in agency approaches to Id&AM and thereby mitigate political, civil and commercial risks inherent in increased online access to government managed resources.
- Reduce costs of acquiring, developing, implementing and supporting Id&AM infrastructure, solutions and services through rationalisation and sharing of one or more of approaches, technologies and infrastructure.
- Provide an enabling environment to facilitate and support cost effective joined-up services.

Reduce overheads/effort and costs involved in provisioning and de-provisioning users, and in day to day user operations.

## Detailed Policy Statements

The Office of the e-Government intends to support the following policy principles by developing and maintaining agreed and approved consistent, standards-based Identity and Access Management (Id&AM) Implementation Guidelines for Western Australian Government *agencies and departments*.

These principles are provided within the context of a broader assessment of departmental and agency security needs as described in the ICT Security Policy and within cited industry standards including:

- Australian Standard for information security management - AS/NZS 7799.2 2003, Specification for Information Security Management.
- International Standard 17799:2001, “Code of Practice for information Security Management, which provides best practice guidance on security controls that should be considered for implementation within an organisation.
- Standards Australia handbook HB 231:2004 for ‘Information security risk management guidelines’

Specific Id&AM principles are:

### Identification

All users must be positively identified, to an agreed and defined level, prior to being granted access to government systems. In appropriate circumstances this process will need to include obtaining formal security clearances. Such checks may need to be refreshed on a regular basis depending upon the role played by the user.

### Registration

Registration processes must be implemented to ensure the integrity of the identification process and the process of providing authentication credentials to users.

Identified users (or identities) must be assigned an identifier that is unique within the application or network and be issued with a means of electronic identity authentication, such as a password or token.

The user’s Identifier will be used by the various access management systems to control, record and monitor a user’s access to applications.

### Application Classification

Agencies and departments, as application owners, must assess the potential impact within (and beyond) their application systems of reliance on a fraudulently presented identity, and from that assessment assign an application assurance level classification.

### Authentication

Agencies and departments must define identity authentication assurance level requirements for users seeking to access applications classified in the manner described above. These requirements might range from password, through to a range of commonly termed tokens or second factor authentication devices such as smart cards and password devices.

Authentication mechanisms will change over time based on technology changes and emergent threats and as such the suitability of authentication mechanisms must be continually monitored.

Strong passwords are a minimum requirement for all applications and tokens and other second factor authentication mechanisms are required for higher assurance level applications.

Other forms of authentication, including location of the user should also be considered within the overall application risk assessment.

### Access Rights

Access rights of users must only be granted where such access is required for the completion of the user's responsibilities as determined by the application owner.

Access rights must be removed when such access is no longer required to a particular application. Change of rights to one application must not impact on the integrity of other access rights held by the user.

### Roles

Access rights should preferably be managed through the definition of roles within business applications which define a logical grouping of application access rights specific to a role. These roles can then be assigned to one or more users.

### Group Access

In some situations, typically where access computers are shared amongst many users, there may be a requirement for users to share a single group identifier in order to streamline workflow.

Group identifiers should be supported only after a full assessment of the risks and supporting controls within the application and must not be used where the application assurance level requires more than password based authentication.

Assignment of a Group Identifier does not negate the need for Identification of all users.

### Administration

*User centric*

User access privileges must be reviewed regularly to ensure that access is still required by the user and that unanticipated combinations of access rights have not arisen.

*Application centric*

Access reviews must be completed regularly by application owners to ensure that those with access have the need for that access.

### Audit

Audit trails must be maintained detailing attempted and successful accesses to application systems.

Audit facilities must be generally robust and tamper-resistant for high assurance level applications.

An appropriate regime of reviewing audit trails and acting on suspected ‘abuses’ must be in place.

### Cross recognition of Identities

Where agencies and departments elect to “join-up” with other agencies or departments, and rely upon user identities registered and/or authenticated by these others, then formal agreements must be entered in respect to the obligations and liabilities of each department or agency in respect to the authentication, authorization and ongoing maintenance of the status of these users.

# Appendix H – Public Policy Framework – Context and Content[27]

## 1. Background

The effectiveness of the Id&AM Framework and Action Plan will be heavily dependent upon acceptance of the proposed approach to identity and access management by all relevant (intra-government and external) stakeholders.

This assignment has covered significant consultation with agencies of the Western Australian Government, but consultation with externals has been out of scope.

This Appendix considers the broader public policy issues which need to be satisfactorily addressed in order to ensure that the Id&AM can achieve broad acceptance by all stakeholder groups.

Key aspects of the WA context within which this document has been prepared are as follows:

- the Government is committed to a "citizen-centric approach ... focussed on the needs of Western Australians" (eGovernment Strategy, p.36);
- the Government needs to "actively engage with citizens. This engagement ... provides a vehicle for citizens to actively contribute to government decision-making at both the ministerial and agency levels" (eGovernment Strategy, p.36);
- "agencies need to create an environment that supports and encourages citizens (especially those who may be subject to 'digital divide' issues) to engage with government" (eGovernment Strategy, p.37);
- "2010 Vision: Citizens are able to actively participate in the governance of Western Australia through the use of e-government technology; ... and a whole-of-government platform for government service delivery enables citizen participation ..." (eGovernment Strategy, p.37);
- the scope of the Id&AM initiative is comprehensive. It is intended to encompass the following, probably in the priority order shown:
    - employees of WA Government;
    - individual contractors to WA Government agencies;
    - suppliers to WA Government agencies. There is a need to distinguish small and micro-enterprises from large and medium-sized business;
    - business partners of WA Government agencies;
    - citizens;
    - agents acting on behalf of any and all of the above;
- the Government delivers a very wide range of services;
- the Government performs many social control functions, which are a service to the community as a whole, but are perceived by individuals as constraints on themselves. In these contexts, identity management, and the data handling associated with it, are far less likely to be welcomed by individuals. Indeed, there are many circumstances in which individuals will feel 'put upon' by agencies, and will resist or even oppose the initiative;
- 'joined-up government' represents a promise in some contexts, and a threat in others. For example, the closer links among agencies that it entails also imply increased data-sharing, greater power by government over individuals, and cross-system enforcement;
- WA has some relevant legislation and specialist agencies in place, in particular the Freedom of Information Act and the Information Commissioner;
- there is at this stage no privacy legislation or Privacy Commissioner.

[27] Prepared for Convergence by Dr Roger Clarke, Xamax Consultancy Pty Limited – July 2005

## 2. Stakeholder and Public Policy Issues

Public policy issues are a critical aspect of the Id&AM Framework and Action Plan. There are very likely to be concerns felt among a variety of stakeholders. Moreover, lack of buy-in by stakeholders, reactions against its application by agencies and in whole-of-government projects, and negative perceptions of various aspects of the Framework, are all significant project risks.

Stakeholder analysis needs to be fully developed, in order to ensure a full understanding of all segments of the population that have an interest in, or are affected by, the identity and access management initiative. Particular concerns include employees and contractors, small and micro-businesses, and citizens.

Consultation with these stakeholder categories is best performed through a mix of focus groups and processes involving representatives of and advocates for the identified stakeholder segments. Effective consultation can only be achieved if participants have the opportunity to understand the nature of the proposal, and to provide comments, with a reasonable expectation that their comments will be reflected in the proposal as it is articulated.

Effective consultation is not a one-time event, but an ongoing process. The communications need to be institutionalised, through the phases of implementation and during the operation of the scheme.

The approach adopted needs to reflect the e-engagement work that has been undertaken in parallel with the early phases of the initiative.

The following are aspects of public policy that require consideration, and that may require specific action:

- service availability, accessibility and equity;
- human rights, including those of employees and contractors;
- the allocation of effort, cost and risks;
- freedom of information; and
- privacy.

## 3. Service Availability, Accessibility and Equity

Most agencies and programs are subject to specific statutes. In many cases, those statutes obligate the agency to perform certain functions, or to make certain services available to individuals. Some of these service obligations may be in conflict with the desire to authenticate identity. They may affect the agency's legal capacity to perform the actions involved in authenticating identity, or, conversely, the scheme could conceivably compromise the availability of those functions or services.

In addition, even though the Identity & Access Management initiative's purpose is to enhance services, there are various ways in which it may compromise service availability. For example, a health or emergency services worker under pressure may be unable to perform the actions necessary to gain access to an important database.

Anti-discrimination law may also be relevant. Access might depend on a mechanism that precludes a particular person from gaining access, or from gaining access under particular circumstances. Problems that might arise include where gaining access requires sight, or a device with a card-reader or a spare USB port, or a right thumb.

Issues arising from the design may extend beyond anti-discrimination to equity. Bases on which discrimination and equity issues might arise include:

- physical disability (e.g. of sight, mobility, or capacity to use a keyboard or mouse);
- mental disability (e.g. the inability to remember a username/password pair, or to carry a token);
- educational limitations (e.g. lack of understanding of username/password prompts, or what to do with a token);
- language barriers (e.g. insufficient English to understand instructions, even the instructions on how to contact an interpreter);

- location (e.g. in an institution, in a remote area, in a rural or regional area with outdated infrastructure or inadequate bandwidth, in another State or Territory of Australia, or in a foreign country); and
- lifestyle (e.g. aboriginals living a traditional lifestyle).

## 4. Human Rights, including of Employees and Contractors

It is easy to make presumptions about the government's authority to impose authentication mechanisms on employees and contractors, but it would be advisable to seek advice on the actual legal basis, and on what constraints exist.

All of the anti-discrimination and equity issues discussed in the previous section may be relevant.

Occupational health and safety law could be relevant, e.g. if a field-worker was unable to gain access to poisons information, or to guidance in relation to safe use of a device, as a result of authentication processes blocking the person's access to a government intranet.

There may also be provisions of industrial law that apply to some kinds of requirements that the scheme might impose, e.g. compulsory installation of equipment on a home-machine.

The question also arises as to the government's authority to impose some kinds of requirements on various categories of individuals. It would appear to be uncontentious to require that a person submit to reasonable requirements in order to authenticate themselves. But the interpretation of what is reasonable may not always be straightforward. An obligatory shared secret might be intrusive (even if the person were told that they could use any answer that they liked and could remember, whether it was true or not). Allocation of usernames and passwords could give rise to strings of characters that were offensive to the person concerned (e.g. a series of three sixes).

Further, the power to require submission to biometric measurement should not be assumed, because it could be interpreted by the courts as an interference with the physical person that is subject to common law, statutory or even constitutional protections.

## 5. The Allocation of Effort, Cost and Risks

An issue that may be of consequence is who is required to invest what efforts, and who is required to bear what costs. Examples of costs and effort include:

- undertaking evidence-of-identity and/or other clearance processes;
- obtaining authentication credentials that have a charge associated (eg digital certificates);
- having to upgrade computer equipment and/or software to enable the required level of security and authentication.

The Id&AM scheme might be designed to transfer effort or cost onto individuals or onto relying parties; or it might have that effect; or it might be perceived to have that effect. This could be particularly true for high assurance authentication schemes (eg those involving PKI and/or hardware tokens). In addition, the scheme might impose new responsibilities or onerous new obligations, on individuals or on relying parties.

Another concern is who bears what risks, both of a financial nature, and of a service-denial nature. There is likely to be concern among stakeholders to ensure an equitable distribution of risks and contingent liabilities.

## 6. Freedom of Information

In some jurisdictions, FoI has become ossified, with much greater efforts invested in preventing access rather than facilitating it.

The Internet has ushered in an era of greatly enhanced discoverability and access to, information of all kinds. This is bringing with it greatly increased expectations of unmediated, electronic access to government documents, or 'eFoI'.

The public is likely to expect that most such accesses will be as anonymous as looking up a document in a public library. Identity management will be relevant in a few areas, however.

These include:

- access by the persons or organisations to data about themselves;
- the publishing of documents and new versions of documents into open-access directories; and
- content ownership, and its migration over time as:
    - staff change;
    - position-titles change; and
    - agencies are re-named, merged, and disestablished.

## 7. Privacy

The most substantial public policy issue arising in relation to the Id&AM initiative is likely to be privacy. The following sub-sections trace the considerations through from the general to the specific.

### 7.1 'Authentication' versus 'Identity Management'

Attention is drawn to the advantages of an 'on-line authentication framework', as distinct from a more limited 'identity management framework'. The former actively encourages agencies and cross-agency projects to clarify what the assertions are that need to be authenticated. This is the approach being adopted by various governments, including the Australian and the New Zealand Governments. The ‘authentication’ component of the proposed WA Id&AM Framework highlights the requirement spelled out in detail in the AGAF to determine what ‘assertion’ is to be authenticated and not to automatically assume that this is ‘identity’.

The first benefit of this approach is that many transactions are found to involve a need for some assertion other than that of identity to be the appropriate focus, e.g. authentication of value, of attributes, of location, or of a principal-agent relationship and the associated delegation. The second benefit is that some are found to not require any authentication at all.

Apart from increasing the effectiveness of agency and project risk management, and avoiding unnecessary expense, this approach avoids unnecessary privacy-invasiveness.

### 7.2 The Concepts of 'Entity' and 'Identity'

An entity is something that exists in the real world.

An identity is a presentation of some underlying entity, such as that associated with some role the entity performs.

A fuller exploration of these terms is provided in section 1.2.1 of the Framework.

The clarification of ‘entity’ from ‘identity’ is important from a privacy perspective as requirements to authenticate ‘identity’ often make the un-required leap to ‘entity’.

A further challenge is that care must be taken in associating data with the correct thing, i.e. entity, identity or role. This is of especial concern where the data is sensitive, or the data could give rise to recriminations or reflect negatively on the person it is associated with.

### 7.3 The Concept of Privacy

Privacy is much-misunderstood, and much-misrepresented. It is therefore useful to quickly review the basic concept.

Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations.

But, rather than being only a single interest, it has several dimensions:

- **privacy of the person**, sometimes referred to as 'bodily privacy'. This is concerned with the integrity of the individual's body. Issues include compulsory sterilisation, compulsory immunisation, blood transfusion without consent, and compulsory provision of samples of body tissue, body fluids, and images of body parts, such as fingerprints, the face and the iris;

- **privacy of personal behaviour**. This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits and religious practices, but also political activities, both in private and in public places. It includes what is sometimes referred to as 'media privacy';
- •**privacy of personal communications**. Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations. This includes what is sometimes referred to as 'interception privacy'. A current serious issue in workplace privacy is uncontrolled employer monitoring of employees' email and web-usage; and
- •**privacy of personal data**. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is variously referred to as 'data privacy' and 'information privacy'. It is sometimes extended to 'informational self-determination', as in the German Constitution.

An important implication of the definition of privacy as an interest is that it has to be balanced against many other, often competing, interests. These include the following:

- the privacy interests of one person or category of people may conflict with some other interest of their own, and the two may have to be traded off (e.g. privacy against access to credit, or quality of health care);
- the privacy interest of one person or category of people may conflict with the privacy interests of another person, or another category of people (e.g. health care information that is relevant to multiple members of a family); and
- the privacy interest of one person or category of people may conflict with other interests of another person, category of people, organisation, or society as a whole (e.g. creditors, an insurer, and protection of the public against serious diseases).

Privacy Protection is a process of finding appropriate balances between privacy and multiple competing interests. Because there are so many dimensions of the privacy interest, and so many competing interests, at so many levels of society, the formulation of detailed, operational rules about privacy protection is a challenging exercise.

So-called privacy laws are in most cases focused exclusively on information privacy. This was a natural consequence of the rise in public concerns that has been, and continues to be, driven by fears about the power of computers and information technology. But many of the impacts of these technologies now extend beyond mere information, to affect the behaviour, and even the bodies, of individuals, particularly employees and contractors.

### 7.4 Privacy Law

Consideration of the public policy implications of the Id&AM initiative is complicated by the absence of any comprehensive privacy law in Western Australia. The Freedom of Information Act 1992 provides data subject access and correction rights, but (valuable though this is) it represents about one-tenth of a comprehensive information privacy law, and does not address broader issues of physical, behavioural and communications privacy.

Trust by employees and citizens alike is dependent upon appropriate, enforceable, and enforced privacy protection laws being enacted.

Detailed examination is needed of the existing framework of instructions, policies and MoUs among agencies. Detailed examination is also needed of alternative models, in particular:

- recent implementations of OECD-Guideline laws, of which the Information Privacy Act 2000 (Vic) is the best exemplar; and
- combined Information and Privacy Commissioner laws, exemplars of which include the Information Act 2002 (NT) and the Freedom of Information and Protection of Privacy Act 1990 (Ontario).

The elements of such laws include a framework that establishes rights and responsibilities, a statutory privacy regulator or 'watchdog' office, and principles to enable the regulator to guide agencies and to mediate and arbitrate on complaints of unjustified invasion of privacy by agencies.

Considerable care is needed in formulating, or selecting, or customising, a set of principles. Existing sets suffer a range of deficiencies, and many are greatly dated.

On the basis of those analyses, a privacy protection model needs to be selected, and legislation prepared to give it effect, in a manner appropriate to the needs of Western Australian citizens.

A number of existing statutes include provisions that at least incidentally, and in some cases intentionally, provide some forms of privacy protection. These include:

- the Freedom of Information Act 1992, at http://www.austlii.edu.au/au/legis/wa/consol%5fact/foia1992222/;
- the Spent Convictions Act 1988, at http://www.austlii.edu.au/au/legis/wa/consol%5fact/sca1988222/;
- the Telecommunications (Interception) Western Australia Act 1996, at http://www.austlii.edu.au/au/legis/wa/consol%5fact/twaa1996540/; and
- the Surveillance Devices Act 1998, at http://www.austlii.edu.au/au/legis/wa/consol_act/sda1998210/;
- the Corruption and Crime Commission Act 2003, at http://www.austlii.edu.au/au/legis/wa/consol%5fact/cacca2003338/;
- the Parliamentary Commissioner Act 1971, at http://www.austlii.edu.au/au/legis/wa/consol_act/pca1971301/;
- the Consumer Affairs Act 1971, at http://www.austlii.edu.au/au/legis/wa/consol%5fact/caa1971174/;
- the Health Services (Conciliation and Review) Act 1995, at http://www.austlii.edu.au/au/legis/wa/consol%5fact/hsara1995365/;
- the State Records Act 2000, at http://www.austlii.edu.au/au/legis/wa/consol%5fact/sra2000156/.

Aspects of the common law are also relevant, in particular the law of confidence, but also the tort of passing off. It is also possible that a tort of privacy may be emergent in Australian law.

In general, each agency and each program is subject to additional specific statutes, many of which have provisions that directly or indirectly relate to privacy.

There may be aspects of the law of the Commonwealth which may be relevant to the Framework. The Privacy Act (Cth) might be applicable to some agencies of the Western Australian Government, depending on the scope of the scheme, the definitions of agency and similar terms employed under W.A. law, and under the Privacy Act (Cth), and the extent and nature of outsourcing used by W.A. Government agencies. The Telecommunications Act (Cth) and the Telecommunications (Interception) Act (Cth) could also be relevant.

## 7.5 Consultations with Privacy Regulators

Detailed discussions are highly advisable, in order to draw on available experience. The matter is complicated by the absence of any specialist privacy regulator in Western Australia.

The Victorian scheme is more up-to-date, and the Commissioner is well-established and experienced. Consultation with this Office would be likely to be valuable.

The Australian Privacy Commissioner is still new, and the nature of the federal agencies the Office regulates is very different from that of Western Australian agencies. Nonetheless, some benefit would be likely to be gained from consultation.

## 7.6 Particular Sensitivities of Persons-At-Risk

It is important that the analysis not be limited to existing laws, because public concerns may go well beyond them. A particular aspect of this is the needs of people who face physical risks if their personal data is disclosed, especially their physical location or data that may result in disclosure of their physical location.

Categories of such 'persons at risk' include:

- people who are under the direct threat of violence, including:
  - people concealing themselves from previous criminal associates;
  - victims of domestic violence;
  - protected witnesses;
  - people under fatwa;
- celebrities, notorieties and VIPs, including:
  - politicians;
  - entertainers and sportspeople;
  - people 'in the public eye', such as lottery-winners;
- people in security-sensitive roles, such as national security operatives, undercover police, prison warders, and staff in psychiatric institutions.

### 7.7 The Commonwealth P.I.A.

The Australian Government eAuthentication Framework (AGAF), at http://www.agimo.gov.au/infrastructure/authentication/agaf, included a Privacy Impact Assessment (PIA) process, that was conducted as an integral part of the project as a whole. A considerable amount of information arising from that process is of relevance to the W.A. Identity & Access Management initiative. See Appendix G1.

The Commonwealth PIA is useful, but it can only inform this project to a limited extent. There are considerable differences between the Commonwealth and W.A. contexts. For example:

- the scope of the NOIE project was e-Authentication of many different categories of assertion whereas the W.A. project is concerned with Identity & Access Management;
- the scope of the Australian Government excludes employees and contractors, whereas the W.A. project focuses on them;
- a PIA was an intrinsic part of the NOIE project, whereas it has not yet been performed for the W.A. project;
- the PIA consultative process for NOIE did not include people from W.A.

### 7.8 The Need for a P.I.A. for the W.A. Identity & Access Management Initiative

The Government needs to initiate a Privacy Impact Assessment (PIA) in relation to the emergent model. This needs to encompass detailed consultations with representatives of and advocates for the interests of affected population segments.

The entire scope of privacy interests needs to be kept within view during the PIA. Of especial concern are the interests of persons-at-risk, the ability to use pseudonyms, and the ability to protect sensitive personal data, including not only data relating to obviously sensitive matters such as health, counselling, discipline and criminal investigations, but also data that may only be sensitive for only a proportion of people, such as contact-details.

The benefits that can be gained from a PIA include the following:

- early appreciation of stakeholders' perspectives;
- constructive suggestions:
  - to avoid negative impacts;
  - to improve the design;
- early warning of future problems;
- avoidance of re-work and retro-fit;
- pre-countering of public criticism.

The work undertaken for NOIE conveyed a number of critical messages about the nature and importance of a PIA as part of the W.A. whole-of-government project:

- a PIA is more process than product, and requires active involvement of all relevant parties, and incorporation of ideas and language into an emergent design;
- a PIA gauges the acceptability of various features to affected parties. That cannot be achieved if no proxies for the affected parties are engaged;
- a PIA harnesses proxies for affected parties in a constructive search for alternative approaches, and for ways in which negative impacts can be avoided. If there are no proxies involved, there is no constructive search;
- a PIA achieves some form of acceptance or agreement from representatives and advocates of affected parties. If they're not involved, it isn't possible to gain their commitment;
- a PIA involves consultation, based on sharing of information. This is an implication of the Government's commitment to a citizen-centric approach, and of the e-engagement guidelines;
- a PIA commences early, in order to maximise involvement, avoid suspicion, and minimise the cost of re-working;
- a PIA involves multiple phases, such that shared understanding increases, and with it commitment;
- a PIA for identity management alone is more liable to invoke negative responses from affected parties than is a broader authentication framework that includes assertions other than of identity;
- a PIA reduces the likelihood that public opposition and misinformation campaigns will be conducted at a later stage, and, even if they are, it reduces their credibility.

Further information is provided in a companion document called 'PIA Guidelines'.

Consideration needs to be given to the scope of the assessment. It could be specifically a Privacy Impact Assessment. Alternatively it could be a broader social impact assessment, in which case it would cover other public policy matters, especially access and equity. A further scoping issue is whether the PIA/SIA is to focus on people generally, including employees and contractors; or whether at least those issues arising in respect of public service employees should be defined to be outside-scope, and pursued through other, established channels.

## 8. Conclusions

The implementation of the Identity and Access Management Framework gives rise to public policy issues in such areas as service availability and accessibility; the allocation of effort, costs and risks; and privacy.

These represent potential vulnerabilities, because the positive image of the initiative could be diluted, and negative public perceptions could arise. These could be harmful to the willingness of Western Australians to adopt the scheme, and to the eagerness of agencies to apply it.

Specific actions are needed within the Action Plan to address these issues.

In addition, guidance needs to be provided to agency, program and project teams as to how to address these issues when applying the Framework.

The e-Government Strategy's emphasis on citizen participation represents a commitment to interaction with stakeholders, and the Guidelines for Community Engagement provide a basis for consultative processes to ensure balanced application of the Framework.

## Appendix H1 – Relevant Aspects of the Australian Government Framework

A comprehensive Privacy Impact Assessment was completed as part of the NOIE Authentication Framework development.

A considerable number of findings from that assessment are of relevance to the W.A. Identity & Access Management initiative:

- privacy expectations are considerably broader than the limited set of principles and the limited set of rights, and the very limited set of sanctions, that are expressed in the Information Privacy Act;
- stakeholder representatives and advocates perceived some benefits of identity management for consumer/citizens; but they felt concern that those benefits need to be balanced against some fairly substantial disbenefits;
- it is very important to carefully analyse or segment the categories of affected people, because the impacts, the trade-offs, and the appropriate solutions to problems, all vary considerably among the different categories;
- there is considerable scepticism about nominal choice not translating into actual choice, but into effective compulsion;
- there was enthusiasm for the inclusion within the Australian Government authentication scheme of assertions other than identity;
- serious concerns were felt about individuals' rights to their commonly-used name being compromised because an agency, or the government as a whole, had previously registered someone else with the same name;
- the silo model has always been, and remains, the most significant single privacy protection. Hence any movement away from the silo model is at great cost to privacy;
- concern was expressed that the federated model is merely a distributed form of the centralised model, and hence is just as privacy-intrusive, and just as unacceptable as the centralised model;
- 'joined-up government' is being sold as a service, but there is a distinct feeling that it will be delivered as an imposition;
- there is scepticism that any case has been made for 'joined-up government' (and evidence in both the Australian and Victorian government contexts is consistent with that view);
- there are strong preferences for standards, norms and best practice guidelines, rather than for common services and infrastructure;
- there is a great deal of angst about the pre-registration / enrolment process;
- biometrics are regarded with enormous suspicion;
- there is common agreement that enhancements in the authentication of documents and tokens would be 'a good thing';
- public interest representatives and advocates are very suspicious of cost/benefit analyses that are performed from the perspective of governments and agencies alone, without factoring in the impacts and costs facing consumer/citizens.

## Appendix I – Excerpt from University of Massachusetts 'Data Security and Classification Guidelines'

Campus standards regarding data security and classification shall require that University data classifications are adhered to. Five levels of data classification have been established. The data classifications DO NOT apply to correspondence or memorandum EXCEPT when the correspondence/memorandum contains other than unclassified data.

The data classifications determine how the data will be secured, managed, retained, and disposed of. Dissemination of University data to external sources is dictated by the Family Educational Rights and Privacy Act of 1974 (as amended), 20 U.S.C. 1232g, and the regulations promulgated thereunder, 34 C.F.R., Part 99; the Massachusetts Fair Information Practices Act, M.G.L. c66A, and the Massachusetts Public Records Act, M.G.L. c. 66, section 10.

Assignment of data into the following classifications shall be performed in accordance with the requirements of the foregoing laws.

- Unclassified - data that does not fall into any of the other data classifications noted below. This data may be made generally available without specific data custodian approval.
- Operational Use Only - data whose loss, corruption or unauthorized disclosure would not necessarily result in any business, financial or legal loss BUT which is made available to data custodian approved users only.
- Private - data whose disclosure would not result in any business, financial or legal loss BUT involves issues of personal credibility, reputation, or other issues of personal privacy.
- Restricted - data whose loss, corruption or unauthorized disclosure would tend to impair the business or research functions of the University, or result in any business, financial, or legal loss.
- Confidential - data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts.

Campus procedures regarding data security and classification shall require that data, regardless of medium and/or form, will be:

- identified as to its classification (i.e. Unclassified, Operational Use Only, Private, Restricted or Confidential);
- accessed, used and disposed of in a manner commensurate with the data's classification and with University Records Management, Disposition and Retention Polices/Guidelines/Schedules and Campus procedures;
- made secure against unauthorized creation, updating, processing, outputting, and distribution;
- appropriately secured and not accessible to non-approved users when not in use.

Campus procedures regarding data security and classification shall require that:

- Aggregates of data should be classified as to the most secure classification level (e.g. when data of mixed classification exist in the same database, file, report, etc., the classification of that database, file, or report should be that of the highest level of classification).
- Databases containing Operational Use Only, Private, Restricted or Confidential data should be secured. Extracts of Operational, Private, Restricted or Confidential data should be secured at the same level as the file/database from which the data was extracted.
- Reports containing Operational Use Only, Private, Restricted or Confidential data should be disposed of properly. Paper and microfiche/film should be shredded. Disks/ hard drives should be erased so as to be irretrievable.

**Data Access and Use**

Undefined or unclear guidelines or procedures shall not be construed to imply access authorization.

Campus procedures regarding data security and classification shall require that:

- only authorized users have access to University data;
- access to data other than unclassified data is denied unless the user has obtained explicit approval by the data custodian;
- access to data classified as Private, Restricted or Confidential should be based on legal requirements or on a need to know; job function; or course requirement basis;
- access to data is given to authorized users. This access should not be shared, transferred or delegated (e.g., authorized users should not log on, access data and then let others use that data);
- vendors, read, understood and will comply with the University Data Security and Classification Guidelines and Campus procedures;
- authorized users act in a manner which will ensure the data they are authorized to access is protected from unauthorized access, unauthorized use, invalid changes (e.g., putting a Q in a grade field), destruction, or improper dissemination;
- authorized users will use their access to University data for approved purposes only;
- authorized users logoff University computer systems if they will not be accessing data for an extended time;
- authorized users will not use University applications and their data in illegal activities;
- authorized users are prohibited from viewing or accessing data, in any medium and/or form, for which they are not approved;
- classified data are not copied without prior approval;
- authorized users understand the data they are accessing and the level of protection required;
- authorized users set file protections correctly when they create or copy a file;
- authorized users periodically "refresh" downloaded data to ensure they are working with accurate, up-to-date data.

## Appendix J – Business Case – Costs and Benefits

Deriving a number of the business case 'values' will be based upon the quantification of costs and benefits. An examination of the major areas of cost and benefit are detailed below. Further data provision by agencies is required to enable the quantification of these.

### Costs

Key **upfront cost** categories are listed below together with a brief explanation of each.

An estimated level of costs is provided for Whole-Of-WA-Government. The ratings are intended to convey the following levels of cost:

Low : $hundreds of thousands to low $millions;

Medium : $ low millions to $10 million

High: $ tens of millions.

The opportunity to reduce costs by collaboration and rationalisation across agencies is also indicated.

| Area of Cost | Estimated Level of Cost | Collaboration / Rationalisation Opportunities |
|---|---|---|
| **Awareness Raising, Education and Training**<br>Development and deployment of awareness raising and training courses for executives, technical staff and end-users. | Low | Development could be undertaken once for WoWAG with execution taking place at agency level. |
| **Privacy Impact Assessment**<br>Conducting of a PIA of the Id&AM | Low | Opportunity cost of not doing this is extremely high as community could reject proposed approaches. |
| **Policies and Procedures**<br>Definition of mutually agreed and accepted authentication and authorisation policies and procedures based around the proposed I&AM Framework. | Low | Development could be undertaken once for WoWAG with tailoring/personalisation taking place at agency level. |
| **Existing Technology Platforms**<br>The re-engineering costs associated with 'connecting' agency applications with access management solutions. | High | Opportunities for savings from WoWAG purchasing (of solutions / services) and shared learnings across agencies. |
| **Existing Data Stores**<br>The costs of data cleansing associated required to harmonise / rationalise 'user IDs' in a single agencies and multi- agency context. | High | Opportunities for savings from WoWAG purchasing (of solutions / services) and shared learnings across agencies. |

| Area of Cost | Estimated Level of Cost | Collaboration / Rationalisation Opportunities |
|---|---|---|
| **New Technology Platforms and Solutions**<br>The cost of solutions (eg authentication management, authorisation/permissions management, provisioning) and the associated costs of implementation and integration. | Medium to High | Potential for consolidation around a single infrastructural solution as per the Canadian and US Governments.<br>WoWAG purchasing approach for multiple solutions will also deliver savings. |
| **Security / Audit / Validation**<br>The cost to validate the efficacy of the harmonised/rationalised environment including development of 'Trusted Credentials Validation Methodology'. | Medium | Opportunities for savings from WoWAG purchasing (of solutions / services) and shared learnings across agencies. |
| **Legal Costs**<br>Examination of the legal issues associated with 'shared credentials' including liability and privacy issues.<br>Development of standardised MOUs to be exchanged between issuers of trust and relying parties. | Low | Development could be undertaken once for WoWAG with tailoring/personalisation taking place at agency level. |

Key **ongoing costs** relate to:

| Area of Cost | Order of Magnitude | Collaboration / Rationalisation Opportunities |
|---|---|---|
| **Education and Training**<br>Development and deployment of awareness raising and training courses for executives, technical staff and end-users. | Low | Ongoing development and maintenance of materials can be undertaken at a WoWAG level. |
| **Community Consultation and Application-level PIAs**<br>As policies and approaches change it will be necessary to get community input. | Low | The inclusion of community stakeholders in WA ID&AMSC and/or in Community of Practice will reduce cost-time of these activities. |
| **Policies and Procedures**<br>Maintenance of policies and procedures, and some possible audit/QA functions. | Low | Ongoing development can be undertaken at a WoWAG level. |
| **Existing Technology Platforms**<br>Ongoing enhancement and licensing costs. | Medium | WoWAG purchasing will reduce this cost. |

| Area of Cost | Order of Magnitude | Collaboration / Rationalisation Opportunities |
|---|---|---|
| **Existing Data Stores**<br>Ongoing alignment costs. | Low | Opportunities for shared learnings across agencies. |
| **New Technology Platforms and Solutions**<br>Ongoing enhancement and licensing costs. | Medium to High | WoWAG purchasing and/or shared infrastructure will reduce this cost. |
| **Security / Audit / Validation**<br>Cost of periodic security audits and reviews. | Medium | WoWAG purchasing and/or shared learnings will reduce this cost. |
| **Legal Costs**<br>Cost of 'personalisation' of MOUs to be exchanged between issuers of trust and relying parties. | Low | WoWAG purchasing and/or shared learnings will reduce this cost. |

## Benefits

Key quantifiable benefits are listed below. The categories of data that will need to be collected to achieve the computation of benefits in dollar terms are provided.

| Value Category | Benefit | Data required for computation |
|---|---|---|
| Direct Customer/User | Avoidance of application for multiple credentials | 1. Audience categories and sizes.<br>2. Extent to which users need to apply for multiple credentials.<br>3. Time costs for user applications for credentials. |
| Government Financial | Reduction in cost of infrastructure and operational services for provision of online access to externals. | 1. Fully implemented and deployed cost of platforms per agency.<br>2. Deployed cost of WoWAG infrastructure (as an alternative).<br>3. Cost of registration, provisioning and de-provisioning of users and estimated reduction in levels due to consolidation. |
| Government Operational/ Foundational | Reduction is usage of non-electronic delivery channels. | Cost of non-electronic service delivery and percentage of this that will be saved. |