



Department of the Premier and Cabinet
Government of Western Australia

**WESTERN AUSTRALIAN GOVERNMENT
OFFICE OF e-GOVERNMENT**

IDENTITY & ACCESS MANAGEMENT FRAMEWORK PROJECT

Action Plan (Draft Final V2.0)
15 September 2005

Prepared by
Convergence e-Business Solutions Pty Ltd



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

1. Introduction	1
2. Summary of Key WoWAG Survey Findings and Conclusions	2
2.1. Current Id&AM Maturity and Execution within WA Government Agencies	2
2.1.1. Awareness and Understanding	2
2.1.2. Strategy, Architecting and Approaches to Execution	2
2.1.3. Architecture/Composition of Id&AM Approaches	2
2.2. Sufficiency of Current Position as a Platform for Effective Transition to e-Government	3
2.3. Current Obstacles to a Cohesive WoWAG Id&AM Approach	3
2.3.1. Registration Policies and Processes	3
2.3.2. Information Management and Classification	3
2.3.3. User Identifiers	3
2.3.4. Credential Usage	3
2.3.5. Reliance on other Agency or Third Party Credentials	3
3. Framework – Proposed Approach	4
4. Key Framework Proposals	5
4.1. Trust Architecture/Model Selection	5
Businesses and other organisations “providing” government services	5
Businesses and other organisations as “users” of Government services	5
Individuals	6
4.2. Information Management	6
4.3. Entity Management	6
4.4. Authentication Management	7
4.5. Access Management	7
4.6. Shared Services	7
4.6.1. Registration Services	8
4.6.2. Credential and Credential Issuing Services	8
4.6.3. Credential Authentication Services	9
4.6.4. Permissions Management Services	10
5. WoWAG Priorities and Impact of Id&AM Framework	11
5.1. VoIP and Common Directory Scoping Study	11
5.2. Shared Corporate Services	11
5.3. Other Agency-Specific Initiatives	11
6. Action Programmes	12
7. Foundational Activities	13
7.1. Formalisation and Ratification of the Proposed Framework	13
7.1.1. Privacy and Public Policy Impact Assessment	13
7.1.2. Establish Governance Structure	14
7.1.3. Finalise Policy	15

7.1.4. Develop Forward Work Program and Budget.....	15
7.2. Establish WoWAG Id&AM Resources	15
7.2.1. Id&AM Strategy Template	16
7.2.2. Educational resources.....	16
7.2.3. Standards	16
7.2.4. Processes	16
7.2.5. Technology Architecture.....	17
7.2.6. Endorsed Technology Solutions	17
7.2.7. Assessment Models	17
8. Agency Consolidation.....	19
8.1. Uncover and Analyse Id&AM Components.....	19
8.2. Harmonise, Rationalise and Unify	19
8.3. Aggregate and Centralise	19
8.4. Architect	20
8.5. Justify, Budget and Plan	20
8.6. Cleanse	20
8.7. Educate and Train	20
8.8. Authorise	21
8.9. Automate.....	21
8.10. Evolve.....	21
8.11. Track, monitor, intervene, report, audit.....	22
8.12. Learn & Improve	22
9. Advancing Government-to-Government.....	23
10. Progressing G2B and G2C	24
11. Other Action Areas	26
11.1. WoWAG and Agency-cluster Initiatives	26
11.1.1. Shared Corporate Services	26
11.1.2. Shared Land Information Platform	26
11.1.3. Transport Executive and Licensing Information System	27
11.1.4. Criminal Justice Integration Project.....	27
11.1.5. Whole-of-Government Procurement Reform Project.....	27
11.2. OeG Focus Areas	27
11.2.1. Enterprise Architecture.....	27
11.2.2. Directories.....	28
11.2.3. Telecommunications Initiative.....	28
11.3. Legal	28
11.3.1. Legal Analysis.....	28
11.3.2. Privacy Act.....	28
11.3.3. Operational Legal Agreements	29
12. Proposed Schedule and Major Action Items.....	30
Attachment 1 – Summary of Proposed Approach.....	31
Attachment 2 - Id&AM Standards.....	38
Relevant Standards Bodies	38
Useful Standards for Access Control.....	39
Applicability to the Proposed WoWAG Framework.....	41

Security Purpose / External Technology Matrix 42
Id&AM Framework Infrastructure Protocols 43

Draft for Comment

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

1. Introduction

This document provides an Action Plan for the implementation of the Identity and Access Management (Id&AM) Framework across Western Australian Government agencies.

Understanding of this document relies upon a knowledge and understanding of the Framework as detailed in the separate *Identity & Access Management Framework* report.

The Framework seeks to achieve:

- improvements in security and service delivery, and reductions in the capital and operating costs associated with Identity and Access Management (Id&AM) environments; and
- a structure within which agencies can plan, architect and assess their approaches to Id&AM.

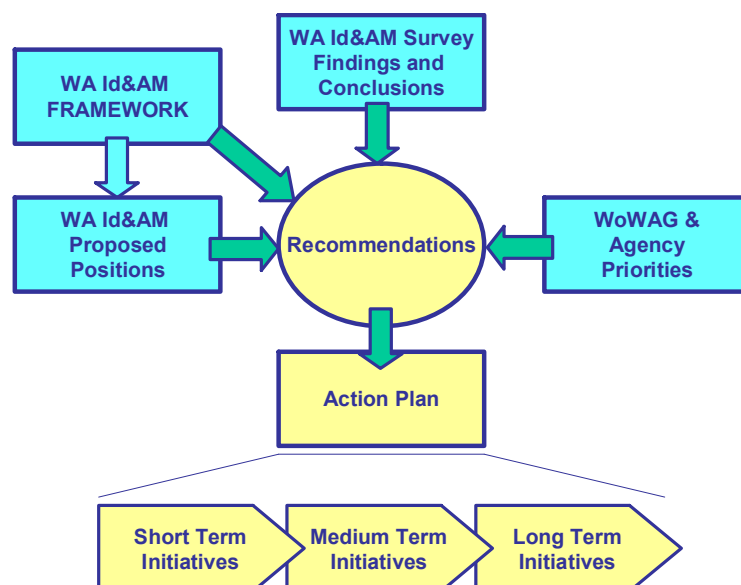
The Framework seeks to encourage approaches that:

- Improve the general usability, efficiency and integrity of the management of identities and related systems access for users and agencies.
- Share WA agency infrastructure and technologies where appropriate. This may be through operational sharing of existing infrastructure, deployment of new WoWAG Id&AM infrastructure, or replication of technology across agencies.
- Leverage existing WA agency policies and practices where available.
- Extend compatibility and alignment with other state and federal government Id&AM approaches particularly in respect to the use of identifiers and user registration processes.
- Ensure the protection of individuals' privacy.
- Align or move towards alignment with contemporary Id&AM standards and practices.
- Align with WoWAG Enterprise Architecture model.

The Framework also provides a structure within which agency cluster and whole-of-WA-Government positions and initiatives can be determined and assessed.

The Action Plan describes how the positions and approaches detailed in the Framework can be achieved when viewed against the Government's 'starting point' as detailed in the separate *Findings and Conclusions* report.

The context for and components of the Action Plan are shown below:



2. Summary of Key WoWAG Survey Findings and Conclusions

Major Findings and Conclusions that need to be addressed by the Government as a whole and individual agencies include:

2.1. Current Id&AM Maturity and Execution within WA Government Agencies

Whilst some major agencies, including DoJ, DLI and DoH have well articulated Id&AM strategies and are at various levels of maturity in execution, the overall level of maturity of Id&AM within key agencies is generally low in respect to both strategy and implementation.

With the exception of DLI and DoJ, this overall lack of maturity is particularly evident in agencies' dealings with external parties.

In particular:

2.1.1. Awareness and Understanding

Agencies rated their across-the-board level of awareness and understanding of Id&AM as low to medium in general, while rating that of their IT management as medium to high.

However the responses to aspects of the surveys, and the feedback obtained through the interview processes, would indicate that the multi-dimensionality of Id&AM is not fully understood even at the IT Management level, with agencies largely focusing on their insular business needs.

There is an almost universal requirement to raise awareness and understanding amongst agency executive and general management, as well as the requirement to raise skill levels among management and staff of the IT function.

2.1.2. Strategy, Architecting and Approaches to Execution

Few agencies have a holistic approach to Identity and Access Management. In most cases the issue is seen exclusively through the lens of IT security, and often tackled within an application-by-application context rather than being examined, planned and architected across the board.

Most agencies do not have an overarching Id&AM strategy that 'cuts through' the required business and technology layers. Nor do agencies take a WoWAG perspective when considering Id&AM.

2.1.3. Architecture/Composition of Id&AM Approaches

Embedding of Id&AM functionality

In general agency environments reflect the embedding of authentication and access control into each application albeit a limited number of agencies have initiatives in progress or on the drawing board that will see the gradual abstraction of authentication and access control from applications and their incorporation into infrastructure layer utility functions.

User-centric Profile and Provisioning and De-provisioning

The current, largely manual, non-integrated and non-workflow-based approaches to registration, enrolment and provisioning / de-provisioning of user credentials and access permissions impact on both the ongoing user management costs and the operational risks of ineffective administration.

Strategies relating to and the implementation of automated user management, and particularly provisioning and de-provisioning solutions remain in their infancy.

Standards

Awareness, understanding and use of emerging standards remain low in all but a few areas of government. Failure to adopt appropriate standards will hamper efforts in future to inter-operate and utilise federated or scheme-based approaches to authentication across agency-clusters or WoWAG.

2.2. Sufficiency of Current Position as a Platform for Effective Transition to e-Government

The current state of Id&AM within WA Government agencies appears to be hampering agencies' e-Government deployment plans. This flows from a lack of scalability and extensibility of existing Id&AM infrastructure, and the resultant costs of new developments. This is symptomatic of agencies' need or desire to "go it alone" rather than actively evaluating shared arrangements with other agencies.

There appears to be little evidence of a user-centric (whether business or citizen) approach to the planning and deployment of re-usable credentials. Few agencies have yet to explore opportunities to share or harmonise the following with other agencies:

- Processes (eg registration of prospective users).
- Infrastructure and solutions (eg authentication services and permissions management applications).
- Credentials (eg an agency accepting a user's authentication credential where this has been issued by another agency or non-WA Government organisation).

2.3. Current Obstacles to a Cohesive WoWAG Id&AM Approach

The following adverse findings on core elements of a contemporary WoWAG Id&AM regime need to be addressed:

2.3.1. Registration Policies and Processes

Development and adoption of standardised processes for the identification and registration of users is required as a first step in any transition to a whole of government Id&AM framework.

Improvements relate both to the requirement to achieve harmonisation within and across agencies as well as raising the standard/robustness of eg evidence-of-identity and other assurance checks.

Current agency processes have been developed to suit individual agency needs and demonstrate a range of rigour and completeness that differs markedly across agencies.

2.3.2. Information Management and Classification

In general agencies do not have a formal approach to information classification. Such an approach would provide a clear definition relating to 'ownership' and 'sensitivity', that, in turn, feeds through to application assurance level determinations and access control requirements.

2.3.3. User Identifiers

No policies or facilities are in place to ensure the uniqueness of identifiers for any category of users across agencies. This has the potential to compromise Id&AM across a portfolio as well as between agencies.

Even within many agencies, users (internal and external) have multiple identifiers.

2.3.4. Credential Usage

The selection of authentication credentials and their relationship to application risk is completed in a variety of ways across agencies. Whilst not an immediate issue due to the relatively low adoption of tokens or other authentication devices, the lack of a cohesive approach to credential selection, issuance and authentication will impact on user acceptance, operational efficiency and operational risk.

2.3.5. Reliance on other Agency or Third Party Credentials

There are few instances of agencies relying upon credentials issued by others.

The issue of shared credentials based upon federated or scheme based identity management models represents a major area of activity across many non-WA government sectors.

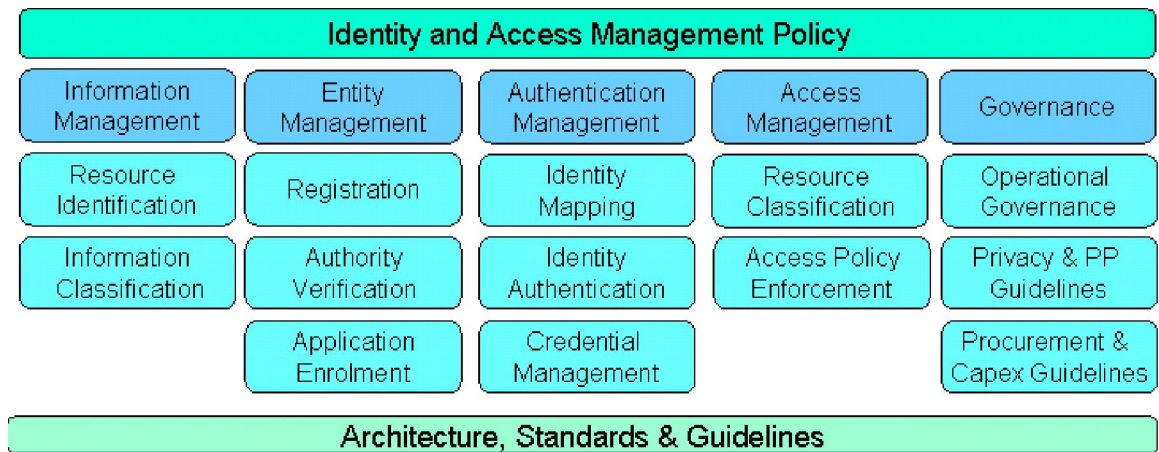
Agencies' ability to rely upon credentials issued by other parties represents a significant area of future benefit from the introduction of a WoWAG Id&AM regime. The benefit will apply to agencies, but more importantly to end users (particularly externals).

3. Framework – Proposed Approach

The Framework, as illustrated below, provides a basis for the development of an Id&AM Strategy and Implementation Plan for the WoWAG and within agencies. The Framework addresses the major pillars of:

- Information management
- Entity management
- Authentication management
- Access management.

The areas of governance, policies, standards and guidelines, are necessary to support and guide, and, where required, enforce compliance with the four major pillars of the Framework.



The Framework is exploded down to another level of detail in diagram 1 of section 2.2 of the Framework.

Clearly the Framework can be interpreted in a number of ways and consequently there are a number of ways that WoWAG and individual WA Government agencies might approach implementation and alignment with the Framework.

Attachment 1 (Summary of Proposed Approach) addresses this issue by proposing specific approaches to implementation at a WoWAG level and within agencies, covering internal and external users, and the issue of alignment across agencies.

4. Key Framework Proposals

4.1. Trust Architecture/Model Selection

For internal users¹ it is proposed that a “scheme” model be adopted whereby internal users would be issued with Identifiers that are unique within the WoWAG domain.

The introduction of the Shared Corporate Services HR environment, and associated clusters, enables the allocation of potentially persistent and unique identifiers to internal users, providing authoritative sources for identity information.

Key elements of a scheme-based approach are:

- The basis of registration should be consistent across government, including EOI requirements, and commonly required attributes such as qualifications, clearances etc.
- This information should be aggregated at a WoWAG level through a WoWAG Directory, and / or be replicated into individual user stores maintained at an agency or agency cluster level.

For external users, it is proposed that a hybrid approach be adopted recognising the diversity of the current and prospective user bases and the largely siloed nature of many agencies.

Key elements of this approach are presented below:

Businesses and other organisations “providing” government services

Where government outsources the delivery of various services to the private sector or NGOs (non-government organisations) there is a strong need to align the Id&AM treatment of these “external” users to the treatment of internal users as described above.

Identification and identifier requirements are identical to those for internal users excepting that it is unlikely that the issuance of a persistent identifier could be justified or required due to the close alignment of the individual with the service provider which may not be persistent over time.

However, requirements for uniqueness, registration integrity and potential storage within a WoWAG directory also apply for this user type.

Businesses and other organisations as “users” of Government services

Agency approaches should be based upon:

- Recognition, where practical and appropriate, of existing user credentials issued by, other WoWAG agencies, other government agencies or the private sector. Specifically, agencies should be positioned to utilise one or more of ABN-DSCs, ATO Certificates, HeSA Certificates and other high assurance credentials as might be issued by eg Australian banks in the future.
- When issuing agency-specific credentials, consideration should be given to enabling the use of this credential by other agencies either directly and/or in a federated manner. In the latter case the user is ‘directed’ to the relying agency after authentication by the issuing agency. The practicalities of this are non-trivial and will require active agency-cluster and/or WoWAG projects to work through the considerable detail involved.
- Where an identifier and credential needs to be issued by an agency, utilisation of the ABN as a primary identifier should be adopted where practical. This will be restricted to cases where a ‘business’ identifier suffices. In many instances where multiple users of a business each require individual credentials, the allocation of a sub-identifier in addition to the ABN will be required.

¹ WA Government employees and contractors that ‘act as employees’.

Individuals

It is proposed that further review be completed on the issues surrounding issuance of a WoWAG customer number, available to agencies via a central issuing facility.

The customer number would have the following characteristics:

- Be unique within the WoWAG.
- Be issued to individuals based on a consistent registration model, with potential for multiple customer numbers to be issued to the same individual, based upon customer choice.

Whereas the proposed 'customer choice' model above partly address some privacy impacts of a WoWAG customer number regime, the acceptability of this approach will need to be tested through a privacy impact assessment.

4.2. Information Management

It is proposed that agencies adopt a formalised approach to information/data identification and classification. This should be formalised within agencies':

- Information management practices and procedures.
- Application system analysis, design, build, test etc practices and procedures.
- Id&AM policy guidelines.

It is recommended that, as a basis for classification, agencies use:

- The framework provided in ISO-IEC 17799 – 2000, *Information technology code of practice for information security management* .
- The classification scheme outlined in Part C of the *Commonwealth Protective Security Manual (PSM)*.
- An agency-based or, ideally WoWAG extension of the PSM classification scheme to support the granularity necessary to support role-based access control within the WA Government context.

For the purpose of the Id&AM Framework the proposed implementation of the above encompasses the use of the classification categories only. Adoption of other aspects of eg the PSM will be guided by agencies' overall Enterprise Risk Management and ICT Security strategies.

4.3. Entity Management

Proposals for entity management aspects are contained within *Attachment 1 (Summary of Proposed Approaches)*.

In summary it is proposed that the entity management provisions of the Australian Government's AGAF be adopted.

Development of the necessary WoWAG policies and guidelines for implementation is required at a central level. This will need to consider the varying levels of entity checking that will be required from Agency to Agency.

As described in Section 5, the potential introduction of a WoWAG directory service, for internal parties at least, should be evaluated further, especially in the light of the proposed VoIP pilot program that seeks to initially introduce interoperable directory technologies across five agencies. This study will need to address the position and harmonisation of this directory vis-à-vis the proposed central identity store to be introduced as part of the Shared Corporate Services HR environment.

4.4. Authentication Management

It is proposed that:

- Authentication of users be progressively abstracted from application systems into an authentication layer of the architecture, and potentially utilise common WoWAG services to effect user authentication as described below. This will inevitably be a gradual process and may not be possible for some legacy applications. In such cases it is imperative that the proposed approach to Id&AM architecture be adopted when such applications are replaced/renewed.
- A formal WoWAG approach to the classification, selection and use of particular credentials (such as RSA SecureID, Rainbow USB Tokens, etc) be adopted, consistent with Australian Government AGAF guidelines, including the requirement that agencies select from the endorsed list only. This is intended to apply to tokens used for both internal and external users.
- The list of endorsed credentials be extended to include non-WA Government issued credentials such as ABN-DSCs, HeSA and ATO certificates, etc. The use of these will be dependent upon agencies evaluating the benefits and costs for themselves and the user populations.
- The classification of credentials align with the Application Assurance Level assignment categories prescribed in AGAF.

4.5. Access Management

It is proposed that:

- Access management be progressively abstracted from the application systems into an *access management layer* of the architecture. Access management should be abstracted from applications using a role-based access control (RBAC) approach. However permissions and alignment of these to roles will need to remain in applications.
- Abstraction be limited to medium grained access control (such as provided through group membership or operational role) with fine grained access/permissions-management, such as that requiring reference to specific user detail, remaining within application systems.
- Common approaches to access management be adopted across agencies. In particular it is proposed that agencies implement Assurance Level based access management provisions as systems are refreshed.

4.6. Shared Services

A major element to be considered in the implementation of a WoWAG Framework is the extent to which agencies 'go it alone' in implementation as opposed to utilising one or more elements of centralised or agency-cluster infrastructure.

Elements that are candidates for operational sharing include:

- **Registration Services**
Involving processes and facilities to support the registration of users, including:
 - EOI checking
 - Checking of other clearances (eg police, national-security)
 - Identifier assignment
 - (Potentially) credential issuance.
- **Credentials and credential issuing services**
Involving processes and facilities for the personalisation, issuance and activation of credentials.

- **Credential authentication services**
Involving processes and facilities to support:
 - Authentication of credentials issued by the requesting agency, another agency or a WoWAG service. This will require trust between agencies and MOU's.
 - Authentication of credentials issued by third parties such as ABN DSCs, ATO certificates, HeSA certificates, and bank issued credentials.
- **Permissions Management services**
Involving processes and facilities for the creation and enforcement of access rules for various internal or external identities.

It is proposed that:

4.6.1. Registration Services

Internal Users

Registration of internal users (including employees, contractors and service providers) through the Shared Corporate Services, Health and Police Clusters be aligned and implement the same practices for EOI and identifier issuance, ensuring that these remain unique across the Government.

Agencies that utilise Shared Corporate Services HR services are by definition utilising a shared services model for these services.

External Users

For businesses, where credentials of third parties or other agencies are unavailable or inappropriate, it is proposed that agencies complete all elements registration of users on their own behalf, applying consistent standards on EOI, EOI assurance, and provisioning.

Resultant Identifiers will be agency specific, but as proposed above the ABN should, where possible, form the basis of this identifier. In many instances where multiple users of a business each require individual credentials, the allocation of a sub-identifier in addition to the ABN will be required.

The potential role that could be played by the proposed Supplier Registry should be evaluated as soon as possible.

For individuals it is proposed, subject to further detailed analysis, that registration be effected through a shared services infrastructure whereby WoWAG identifiers would be issued to participating individuals.

The scope of this service would include:

- Minimum requirements for EOI to be completed by the registering agency.
- Allocation of an identifier by the shared service.
- Potentially, management of credential issuing to the user to support subsequent user authentication. It is envisaged that this would include passwords as well as stronger authentication mechanisms. In all such cases authentication would occur through the shared service.
- Management services to effect status changes of the identifier or authentication credential (lost, reset, suspend). These services could be accessed via a central support desk or through agency operated facilities.

4.6.2. Credential and Credential Issuing Services

Issuance of credentials, especially higher assurance credentials including mechanisms such as tokens or smart cards, is likely to be more effectively and efficiently achieved through a shared services model and this model is proposed for detailed consideration. Benefits accrue through operational and procurement cost savings, and an improved user experience as described below.

For many credential types, such as tokens and other non certificate based mechanisms, the relationship between the identifier (and identity) and the credential is achieved through a 'binding' process based on a token serial number or similar entry within a user store or directory. Hence the issuance of credential in itself is really just a 'minting' process.

As a consequence, a token issued by a central WoWAG service can be assigned to an identifier at any point in time, and in fact linked to multiple identifiers. In this way a user might utilise a single token for authentication of various connections to agencies, even though agencies might have assigned different identifiers to the user. This provides user convenience and cost savings to agencies.

The responsibility of the credential issuer includes:

- Management of the integrity of the issuance process.
- Provision of services to agencies to revoke and otherwise change the status of credentials.
- Provision of credential authentication services.
- Maintenance of accurate records of credential usage.

Moreover, it is proposed that a review be completed of existing agency issued tokens and related facilities with the view to rationalising both the issuance and authentication services.

It is not proposed or recommended that either individual agencies or WoWAG services be developed to issue PKI based certificates, In preference, where the use of certificates is deemed to be appropriate, existing certificates as issued under the Gatekeeper framework or particular instances such as ABN-DSC's, HeSA or ATO certificates be utilised.

4.6.3. Credential Authentication Services

Utilisation by a relying party of credentials issued by others can be effected through either:

- Direct access to a credential authentication service; or
- Indirect access through reliance on an assertion issued to the relying party by the credential issuer. Whilst this is the typical manner of implementation of federated identity architectures, it is not necessarily the most convenient in practice, especially in high volume environments and in environments where *transaction authentication* may also be required.

Direct Access

It is proposed, subject to further detailed analysis, that a WoWAG Authentication Service be established to support the authentication needs of all agencies, albeit that some agencies might elect for a range of reasons to implement their own service.

The WoWAG service would provide:

- Authentication brokering services for all accepted credential issuers and include:
 - Agency issued credentials intended for broader use; these could include tokens currently issued by various agencies for employee remote access.
 - Accepted tokens and certificates issued by other government jurisdictions and in particular ABN DSCs, ATO certificates and HeSA certificates.
 - Potentially, bank issued credentials.
- Fully centralised audit trails of all authentication activities.
- Be extensible to incorporate a range of token types and authentication mechanisms as they emerge.
- Be extensible to support authentication of transactions as well as identities.
- Support emerging standards such as SAML for the communication of authentication status information as required in a federated authentication model.

A WoWAG Authentication Service would clearly need to be implemented in a manner to ensure appropriate levels of security and availability.

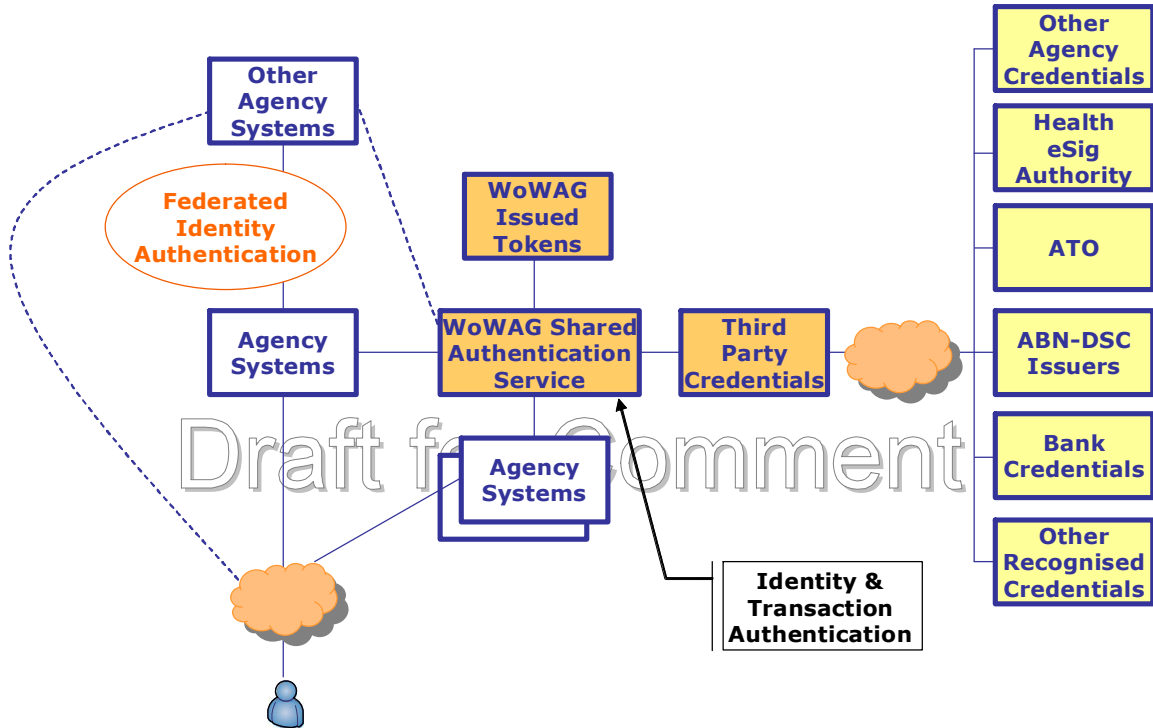
Indirect Access

For many joined-up-government applications, both internal and external, there is a need to pass-on authentication information to the next processor in the chain, rather than seeking re-authentication at each point.

This is best achieved through federated models and the passing of this secure authenticated ‘status’ between disparate systems.

Accordingly it is considered critical that agencies progress towards support for such ‘indirect access’ architectures in addition to the ‘direct’ authentication model proposed above.

A ‘strawman’ architecture to support credential and authentication services is shown below:



4.6.4. Permissions Management Services

Whilst technically feasible, and perhaps of some value to smaller agencies, it is not proposed that permissions management systems be provided as a shared service at this time largely due to the complexity of management of such a service and the unlikely WoWAG cost benefit of such an approach.

5. WoWAG Priorities and Impact of Id&AM Framework

The rollout of the Id&AM Framework will need to be cognisant of other major technology related initiatives underway within the WoWAG environment.

Some of these initiatives will benefit from an acceleration of Id&AM facilities whilst others have overlapping interest areas.

A key area, potentially impacting a number of initiatives, is consideration of a WoWAG policy and associated technology or implementation guidelines, for the implementation of directory technologies across agencies. This is discussed in more detail below.

5.1. VoIP and Common Directory Scoping Study²

This study considers the adoption of IP telephony across WA government agencies and recommends the completion of a pilot programme to assist in the formulation of a WoWAG approach to IP based telephony.

Fundamental to the proposed VoIP pilot is consideration of the directory approach to be used to support the VoIP operations and the study assesses a number of alternatives at both a specific technology levels and at an architectural level, albeit focused on the needs of VoIP and email needs.

Clearly investment in Directory infrastructure to support VoIP and related requirements should be cognisant of the broader context of Id&AM and the demands that this will potentially make on directories for the storage of information on users including identifiers, roles and permissions, and the authentication mechanisms, and the ability to support user de-provisioning across a range of application systems.

It is considered timely to escalate the current watching brief on directories within OeG to a formal project to assess the potential for a WoWAG approach to directory services addressing the needs of VoIP, Id&AM and independent agency initiatives. This work should run in parallel to, and interwork with the specific Id&AM action items described in Section 6 and beyond. This will particularly need to address the relationship between the directory and the WoWAG (internal user) identity store that is proposed as part of the Shared Corporate Services environment.

5.2. Shared Corporate Services

The proposed Id&AM Framework has been developed to leverage and depend upon initiatives underway within the Shared Corporate Services environment, and in particular the aggregation of HR services within a number of discrete agency clusters.

As discussed in Section 6, the successful implementation of the Id&AM Framework for internal users requires a consistent approach to registration and identifier allocation across clusters for government employees and contract for service parties.

It is not expected however that the Id&AM infrastructure implemented within various agencies will have any direct impact of the HR systems apart from the ongoing need for availability of HR information as the authoritative and current source of identity information by various related user stores or directories.

5.3. Other Agency-Specific Initiatives

A number of major agency initiatives were identified during the consultation process where application of the proposed Id&AM Framework would prospectively have some near term benefits at both a WoWAG and agency level.

Further definition of these specific opportunities will result from completion of the proposed Action Programmes and related activities as described in Sections 6 through 11 of this report.

² VoIP and Common Directory Scoping Study completed by CONSULTELE IT&T PTY LTD, August 2005

6. Action Programmes

The achievement of the above requires the initiation of a series of Action Programmes. These major clusters of related activities are outlined below in approximately the sequence in which they need to occur. Given the substantial variance in the strategic and operational maturity of Id&AM in agencies, and the divergence in the extent and urgency of agencies' Id&AM requirements, the sequence and timing can only be taken as indicative. It is highly probable that multiple Programmes will overlap within agencies and at a WoWAG level.

The proposed activity clusters are:

- **Foundational Activities.** These seek to achieve the acceptance of the Framework by all stakeholders, the establishment of the governance structures required to drive the implementation of the Framework at an agency and WoWAG level, and the development and deployment of the detailed 'resources' necessary to drive and support agency efforts.
- **Agency Consolidation.** This cluster recognises that while a small number of agencies have achieved an advanced level of strategic and/or operational maturity in relation to Id&AM, most agencies remain at a level that has the potential to compromise organisational integrity and hamper deployment of e-government applications.

This Action Programme outlines the activities that agencies will need to undertake in order to achieve an approach to Id&AM that is consistent with the Framework and can potentially support shared infrastructure and user-focused (eg scheme or federated trust model) initiatives.

- **Advancing Government-to-Government.** Improving Id&AM in cross-agency dealings and joined-up government initiatives is seen as a priority area by OeG. Early implementation of proposed Id&AM Framework initiatives for internal users will provide an environment where more structured and robust processes can be established to support and maintain cross agency interactions. This cluster identifies key activities required to achieve wide-spread deployment of harmonised/rationalised approaches to cross-agency dealings and joined-up-government initiatives.
- **Progressing G2B and G2C.** With few exceptions agencies currently operate siloed Id&AM architectures within and across agencies when dealing with businesses and citizens. There are considerable benefits in providing a single method of access to these external users across a range of application areas. This cluster outlines the activities required to identify and address these opportunities.
- **Other Action Areas.** This section examines other required areas for action at a WoWAG and OeG level including Shared Corporate Services, Enterprise Architecture, Directories and Legal issues.

The overarching *Summary of Recommended Approaches* (see Appendix 1) provides the guide to the end points that need to be achieved at an agency and WoWAG level, and should be referenced in relation to all of the Action Clusters.

A high level implementation schedule is provided in section 7.

7. Foundational Activities

7.1. Formalisation and Ratification of the Proposed Framework

The first cluster of activities seek to achieve:

- the acceptance of the Framework by all stakeholders;
- the establishment of the governance structures required to drive the implementation of the Framework at an agency and WoWAG level; and
- the development and deployment of the detailed 'resource kits' necessary to drive and support agency efforts.

7.1.1. Privacy and Public Policy Impact Assessment

Privacy and Public Policy issues are considered in depth in the Id&AM Framework (section 4.6 and Appendix H).

The privacy and public policy impacts of the Id&AM Framework are considerable. By definition Id&AM has much to do with human identities and entities. The Framework raises the possibility of:

- accumulation and/or exchange of elements of identifying or identified information; and
- imposition of effort on persons in relation to eg identification and other clearance processes, and obtaining and using authentication credentials.

The development of the Framework has involved considerable consultation with agencies, but not other stakeholders. Stakeholder analysis needs to be further developed, in order to ensure a full understanding of all segments of the population that have an interest in, or are affected by, the Id&AM initiative. Particular concerns include employees and contractors, small and micro-businesses, and citizens.

The absence of such consultation, and, in particular, a formal Privacy and Public Policy Impact Assessment (PPIA), will represent a significant project risk. Deferral of the PPIA to say a post Framework-ratification period would create the further project risk that participants may suspect that they are being asked to approve a *fait accompli*, without any realistic ability to influence the outcome. Stakeholder relations suffer in such circumstances.

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.

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.

In considering the privacy issues both in relation to the PIA and in the broad, the following activities are also recommended:

- Further consolidate the direct and indirect work that has been undertaken in these areas by the Information Commissioner, the Corruption and Crime Commission and the Auditor General.
- Extend the 'Privacy Impact' resources already prepared by OeG. In particular this should seek to:
 - o Ensure convenient access to sources of information on public policy issues that arise in the context of identity and access management.
 - o Where no sufficiently comprehensive or authoritative source can be located, develop and publish documents that consolidate the available information. This appears likely to be necessary at least in the case of privacy impacts.

- Ensure convenient access to sources of information, and where necessary develop and publish guidance for Western Australian government agencies, in relation to:
 - impact assessment methods, at least in relation to privacy, but possibly in relation to broader social impacts, or public policy impacts generally;
 - stakeholder analysis, which importantly also involves the segmentation of stakeholder groups, including agencies, employees and contractors, volunteers, business enterprises, associations, clients and citizens;
 - the discovery of appropriate representatives of and advocates for the various stakeholder segments; and
 - means for undertaking effective but efficient stakeholder consultation processes.
- Undertake consultations with the Victorian Privacy Commissioner, and/or the Australian Privacy Commissioner.
- Examine the results of recent work undertaken by other state governments – eg Queensland Government’s (smartcard) driver’s licence project.
- Evaluate the benefits to be gained from the development of formal (WA) privacy legislation. This issue is considered in further detail in section 11.3.2.
- Conduct one or more pilot impact assessments, in conjunction with the appropriate agency, program and/or project teams. Examples for consideration include the envisaged Western Australian Government (WAG) number, the consolidated employee record project, and the single supplier register.
- In relation to each such impact assessment, document the process, and publish that document and the resulting report, as openly-available exemplars.
- Mandate impact assessment as an element of the application of the Identity and Access Management Framework by agency, program and project teams. The guidance provided should make clear that the assessment process is to be scaled in order to reflect the potential harm and risks involved, and is to leverage off work previously undertaken by the Office for eGovernment and other projects.

7.1.2. Establish Governance Structure

Governance issues are considered at length in section 3.8 of the Framework.

The Framework outlines the reasons for and a proposed approach to governance of Id&AM both at a WoWAG and agency level.

Key bodies to be established include:

- **Whole-of-WA Government Id&AM Steering Committee** (WoWAG Id&AMSC). This could be a committee established with a ‘sunset’ provision.
- **Agency level Id&AM Steering Committees** (Id&AMSCs). For advanced agencies such a committee may not be required. Some agencies may already have in place a suitably structured committee which could take Id&AM on board as an additional area of oversight.
- **Id&AM Community of Practice** (CoP). Membership of ‘advanced’ agencies such as DOJ, DET, and DLI will be important to achieve rapid results from the CoP.

The earliest task of the WoWAG Id&AMSC will be to ratify the Framework.

Section 3.8 of the Framework also outlines the range of policy, standards and guideline issues to be resolved and the indicative balance between the WoWAG and agency positions on such matters. The WoWAG Id&AMSC working in conjunction with the Id&AM CoP should agree a timetable for the development and agreement of binding positions for WA Government in relation to:

- Identity & Access Management Policy.
- Identifiers and naming conventions.
- Identification standards/practices including EOI and clearances.
- Authentication credential assurance standards.
- Information classification standards.

- Legal and liability issues as outlined above and in section 11.
- Technology architecture, standards and protocols.

Attachment 1, *Summary of Recommended Approaches*, provides recommended positions in relation to these issues.

It is recommended that the WoWAG Id&AMSC and CoP also:

- Drive the examination of Shared Id&AM Infrastructure and Services.
- Contribute to OeG's development of a business case for Directories.

7.1.3. Finalise Policy

A proposed WoWAG Id&AM Policy is discussed in section 4.4 of the Framework and a recommended Policy is provided in Appendix G of the Framework.

The Policy is seen as an important artefact to raise awareness of the Framework and ensure compliance with the Framework over time.

OeG working in conjunction with the WoWAG Id&AMSC and the Id&AM CoP will need to:

- finalise the Policy;
- develop guidelines to assist agencies in its implementation;
- determine an appropriate timeframe for its implementation across government;
- determine compliance/reporting approaches; and
- determine processes for the maintenance of the Policy.

7.1.4. Develop Forward Work Program and Budget

The Action Plan describes a wide range of actions and provides a high level implementation schedule.

The actions necessarily translate into a range of program and project based initiatives. Each of these will have resource and funding implications at a WoWAG and agency level.

Program-based initiatives are seen as those that involve agencies in 'embedding' changes into key aspects of their existing approaches to Id&AM and the architectures and solutions that support these.

Project-based initiatives are seen as those that are discrete and may be commissioned at an agency or WoWAG level.

It will be important for OeG working in concert with the Id&AM Community of Practice to develop and maintain a detailed Forward Work Program for endorsement by the Id&AM Steering Committee. Such a document will be essential to identify resource and funding implications and the timing of these. Endorsement by the Id&AM Steering Committee should assist in supporting applications for funding at a WoWAG or agency level.

7.2. Establish WoWAG Id&AM Resources

To support the deployment of the Id&AM roll-out strategy, it is proposed that Id&AM Resources (eg kits) be developed that will provide agencies with valuable material to support the community, business, technology and operational transition to an integrated whole of government approach to Id&AM.

Most Resources will need to be maintained over time. An online rather than paper based medium will better suit this requirement as well as providing instant access across WA Government.

It is proposed that the Resources be developed by the Id&AM Community of Practice with assistance and support of OeG, agencies that have a high level of Id&AM maturity and the Procurement function of Treasury and Finance in relation to the proposed 'preferred technology solution schedule'.

In particular the following resources should be developed:

7.2.1. Id&AM Strategy Template

Section 4.1 of the *Findings and Conclusions* report highlights the disparities in the extent to which agencies have developed formal Id&AM and Authentication strategies.

Such strategies are essential to ensure that appropriate issues and investments are considered during business and technology lifecycles.

The Framework itself provides the major context and ‘headings’ for a strategy. Section 8 (*Agency Consolidation*) below outlines the major implementation steps that will need to be factored into an agency’s Id&AM strategy.

The development of a strategy template is recommended. This should be undertaken by OeG in concert with the Id&AM Community of Practice and agencies such as DOJ, DOH, and DET that already have mature and detailed surveys.

7.2.2. Educational resources

Section 4.2 of the *Findings and Conclusions* report highlights the extremely variable state of awareness and understanding of Id&AM across all sections of agency’s management and user communities.

The raising of awareness levels amongst executives, managers and other users, and the raising of skill levels amongst security and ICT staff is an essential pre-condition to the deployment of the advanced Id&AM approaches described in the Framework.

Resource kits should be developed to support executive management, business systems designers, systems architects, designers and builders, and operational risk managers.

The educational resources will focus on developing an understanding of the proposed Framework and its characteristics and optional approaches to implementation and operations.

It is expected that the educational resources will be enhanced over time to capture ‘case study’ style artefacts that can serve as signposts or benchmarks to future activities.

7.2.3. Standards

Section 4.15 of the *Findings and Conclusions* report shows the varying degree to which agencies have or are committed to the take-up of mature and emerging Id&AM standards.

Whilst there are a number of well established standards and conventions in use for Id&AM, the area is evolving rapidly and new standards are emerging. The achievement of interoperability (for eg cross-agency, WoWAG and other sectoral initiatives), systems flexibility and extensibility and the ‘future proofing’ of agency technology environments will depend upon the adoption of such standards.

Attachment 2 presents a comprehensive treatment of major standards activity currently in progress in the Id&AM area, along with details of relevant standards in terms of the proposed Framework.

As discussed in Attachment 2, ultimate selection of standards will be driven by application or infrastructure vendor support of the standards and their suitability for the task at hand.

A key component of the Standards Resource Kit will be a ranking of preferences for standards along with time or event driven objectives for the incorporation of these standards into agencies’ business systems.

7.2.4. Processes

Agencies have identified a wide variation in the manner in which they undertake similar processes within the Id&AM lifecycle (see Section 4.3 of the *Findings and Conclusions* report).

The *Processes* resource kit will provide pro-forma processes for agencies for a variety of Id&AM events.

Candidate areas for inclusion are (inter alia):

- Internal party registration.
- Credential issuance and revocation.
- Knowledge based authentication standards and processes as used in Enrolment.

- Determination and assignment of Roles.

The implementation of the Shared Services clusters will provide an excellent opportunity to develop these standardised processes.

7.2.5. Technology Architecture

Sections 4.10 and 4.12 of the *Findings and Conclusions* report illustrate the variation in agency Id&AM architectures. In most cases access management is still embedded in business applications impacting on scalability, visibility and usability.

The Id&AM architecture proposed by the Framework (see section 4.1 and Attachment 2 of this report) represents a starting point, but should be further developed.

The architecting and implementation experience possessed by the agencies with more mature Id&AM regimes (eg DoJ, DLI) will enable the development of a more fleshed out version of the architectural model that can assist the many agencies that are still at a level of Id&AM immaturity.

7.2.6. Endorsed Technology Solutions

Section 4.6, 4.13 and 4.16 of the *Findings and Conclusions* report illustrate the variation in agencies' technology environments.

The adoption of common technology platforms and solutions across government will drive procurement cost benefits and provide standardisation in areas where more detailed security and interoperability matters are of concern, as is the case in many Id&AM areas.

It is recommended that some formal endorsement process be implemented, potentially leveraging one or more of:

- Australian government initiatives and the Australian Government's Evaluated Product List (EPL);
- other government initiatives such as the US Government guide to credential evaluation (see www.nist.gov);
- programs offered by some standards groups which provide "reference models" through which vendors can certify their products as standards compliant.

Areas of particular importance are those technologies and products that:

- Interwork with other agency systems using standards based interfaces.
- Implement cryptographic processes as core elements of their operation, including:
 - User authentication tokens
 - Host authentication systems.

The outcome of this activity would be a list from which agencies could review and potentially select technology and products with some increased comfort as to their fitness for purpose.

It is not proposed that the use of particular products or technologies be mandated.

7.2.7. Assessment Models

It is proposed the Resource Kits include two *assessment models* to assist agencies in their development, planning and implementation of their Id&AM strategies.

Cost Benefit/Business Case Model

Section 4.7 and Appendix J of the Framework provide coverage of the requirement for and an approach to developing business cases in the area of Id&AM.

A more detailed model would be designed to assist agencies in the evaluation of alternate approaches to Id&AM implementation within their agency addressing both the cost and benefits elements of the evaluation.

Cost models would also provide a benchmark cost based on the use of shared services where these exist.

Benefit models would evolve over time and be based on quantitative information collected in WA Government Id&AM implementations.

Maturity Models

Section 4.9 of the Framework outlines an approach to the determination of the maturity of agency approaches to Id&AM in relation to both strategic/architectural and operational characteristics. The depiction of maturity based upon a number of 'spokes' allows agency management to determine where most effort should be directed to improve Id&AM approaches.

It is proposed that the maturity models, as outlined in the Framework, should be further developed to assist agencies determine their maturity in the deployment of Id&AM principles and the WoWAG Id&AM Framework in particular. This would require the identification of a range of evaluation criteria for each of the maturity 'categories' and the determination of how best to score agencies' positions in relation to these criteria.

Draft for Comment

8. Agency Consolidation

While a few WA Government agencies have achieved an advanced level of strategic and/or operational maturity in relation to Id&AM most are at a level that has the potential to compromise organisational integrity and hamper deployment of e-government applications³.

The achievement of agency-cluster and WoWAG objectives in the area of Id&AM will be severely hampered unless and until agencies reach a reasonable level of Id&AM maturity both at a strategy and operational level. Rectification of this position therefore needs to become an early and major focus of the Action Plan.

The Framework provides a firm basis to guide agencies deployment of Id&AM. In moving towards the achievement of the required level of maturity agencies will need to progress through the activities outlined below:

8.1. Uncover and Analyse Id&AM Components

The Framework identifies the key information, entity, process and systems components that need to be addressed in order to assure the efficacy of an agency's Id&AM approaches.

Agencies that do not have a mature approach to Id&AM will need to undertake appropriate discovery and analysis processes in relation to all:

- Identity stores (including clarification of their key purpose/s). These are likely to be found across all applications that contain directory information, including PABX directories.
- Internal and external identities and their associated authentication credentials and access permissions.
- Processes and policies/practices associated with user identification, hiring/firing and contracting.
- Types of roles and the permissions, authorities and delegations associated with such roles. This needs to be done across all applications and then mapped back to HR position roles.
- Authentication policies/practices and processes.
- Enterprise risk management and information security management systems plans and policies.
- Information management policies/practices and processes including how, when and where 'ownership' and classification of information is determined.
- Application assurance level determination policies/practices and processes.
- Technology/security standards in use and planned.

The above analysis will provide the agency with the empirical basis upon which to:

- Determine the degree of compliance (or non-compliance) with the Framework.
- Identify what components will require 'rectification' over time.

8.2. Harmonise, Rationalise and Unify

The policies/practices and processes for each of the categories listed in 8.1 above need to be harmonised to be internally consistent and consistent with WoWAG positions as outlined in the Framework (see summary in Attachment 1).

8.3. Aggregate and Centralise

Aggregation and centralisation of a number of Id&AM solution components has the potential to:

- Improve the integrity of Id&AM by removing redundancy of data and rules.
- Reduce technology and process costs.

³ See *Findings and Conclusions* report (section 5.1)

The data uncovered through the processes described in 8.1 above when compared with the models provided in the Framework should reveal opportunities for rationalising and centralising the following:

- Identity stores.
- Authentication solutions.
- Aspects of access control (eg application level access). This should aim for an RBAC approach.

8.4. Architect

It will be necessary to examine the business and technology aspects of the agencies enterprise architecture in order to develop:

- New business processes.
- Agency level governance regime for Id&AM matters.
- New solutions architecture including the abstraction of most aspects of Id&AM from an application to a middleware/utility level.
- Capacity to link into WoWAG Id&AM infrastructure eg identity stores and shared authentication platform/s for internals and externals.

The analysis undertaken in accordance with section 8.1 and 8.3 above provides the basis for determining the scope of this undertaking and the migration strategy.

Planning and design, and the buy-in from system owners, is critical to success and should not be underestimated.

8.5. Justify, Budget and Plan

Where changes are required agencies will need to develop a project plan and business case for the implementation of an enhanced approach to Id&AM. This will need to include:

- Capital and operating budgets.
- Evaluation of service provision alternatives (eg shared services).
- Cost of transition including systems re-engineering, data cleansing, and education and training (see sections below).
- Detailed project plan including key milestones.

The above will be driven by data emerging from the processes described in 8.4 above.

Section 4.7 and Appendix J of the Framework provide substantial guidance in relation to the development of Id&AM business cases.

8.6. Cleanse

As part of the implementation of a 'new' Id&AM approach agencies will have to cleanse identity, authentication and access stores to remove invalid users and access permissions and rationalize multiple (redundant) identities into one identity (eg using single identifiers).

This will necessarily involve information owners and custodians, application owners and potentially, the users themselves.

Agencies/WoWAG should seek to access the learnings from large scale initiatives in this area such as the Victorian Government's Project Rosetta and the NSW Department of Education's Student Directory project.

8.7. Educate and Train

On an upfront and ongoing basis it will be necessary for agencies to educate and train:

- Executives.
- Line Managers.
- All other staff and contractors.
- External users.

- Technical (including help desk) staff.
- Security staff.

Training will need to cover (as appropriate):

- key information management and Id&AM principles;
- revised processes;
- revised legal and contractual positions;
- revised architecture and solution stack;
- use of new provisioning, deprovisioning processes and, possibly, solutions;
- new authentication solutions.

8.8. Authorise

As part of the implementation of the 'new' Id&AM regime it will be necessary for agencies to:

- Appoint/re-affirm information and application owners.
- Determine roles and responsibilities of staff in relation to maintenance of identities and application access permissions.

8.9. Automate

The achievement of sustainable integrity and efficiency gains will necessitate that agencies:

- Create a 'first level' provisioning/deprovisioning solution that at least provides a form of 'enterprise user administration'.
- Define requirements for and acquire and install more integrated provisioning/deprovisioning solutions. The implementation of RBAC is seen as essential to the achievement of this.

8.10. Evolve

As the 'remediation' of agency Id&AM environments will inevitably be a long term exercise, the achievement of incremental benefits is essential. This requires agencies to focus on major applications and user bases at first before addressing lesser applications and user bases.

One approach could see agencies working to:

- Create aggregated identity stores for staff at an agency level and link into WoWAG identity stores to identify/authenticate other intra-WA Government users. This will require a Federated Services strategy using eg WS-Federation.
- Create aggregated identity stores for external users at an agency level. The implementation needs to be approached carefully as it can have significant security implications.
- Move towards simplified sign-on and then single sign-on for internal and then external users. The latter would in all probability require usage of a shared-service approach. As this requires that all applications authenticate to the same source significant application rework is involved.
An 'interim' approach proposed by DoJ sees the use of web services to pre-populate Identity information from the Meta-Directory into application authentication services (eg Basic or Forms authentication). This will be the most cost effective method of providing Pseudo Single Sign On.

Agencies will need to test the efficacy of implementations of each of the above and measure and report on progress to their Id&AMSC and ideally the WoWAG Id&AMSC as well.

8.11. Track, monitor, intervene, report, audit

Agencies will need to install comprehensive facilities to:

- Track and, where required, report upon provisioning and deprovisioning of all identities and authentication credentials. The intention is to enable:
 - Authorizing parties to regularly review applications and/or users for which they are responsible
 - Unusual activity patterns and attempted breaches
 - Reporting to agency executive.
- Provide ongoing measurement of the maturity of strategy and operations.

The activities required to complete the above will also need to be resolve 'who' and 'how' auditing is done for cross agency access.

8.12. Learn & Improve

The agency Id&AMSC will need to ensure that processes are in place to continually review, learn from and improve Id&AM approaches.

Draft for Comment

9. Advancing Government-to-Government

Improving Id&AM in cross-agency dealings and joined-up government initiatives is seen as a priority by OeG.

The progressing of improved and streamlined approaches to this:

- Will be dependent upon:
 - agencies consolidating and improving their own Id&AM positions using the approach detailed in section 8 above;
 - development of agreed WoWAG standards, protocols and best practices as outlined in section 7 above; and
 - initiation of project/s to define, architect, justify and implement cross-agency federated approaches to Id&AM.
- Should leverage WoWAG opportunities such as the pending move Shared Corporate Services and the OeG Directories initiative.

Agency-to-agency dealings have historically relied upon the dual registration of users – ie users in Agency A are registered into the systems of Agency A and those of other agencies to which they require access.

Whilst there has been some progress within more sophisticated agencies to adopt federated approaches⁴ to inter agency access, this situation remains a significant issue for both users and application providers. In particular it exposes both the accessing and accessed agency to operational risks resulting from the difficulty in managing and maintaining accurate registration and authority details for such users.

Early implementation of proposed Id&AM Framework initiatives for internal users (as outlined in sections 4 and 5 above) will provide an environment where more structured and robust processes can be established to support and maintain cross-agency interactions.

Necessary implementation steps include:

- Adoption of a single WoWAG Identifier for internal users, encompassing employees and contractors. It is proposed that this be affected through the Shared Corporate Services implementation and through equivalent initiatives in the other clusters. This is discussed in Section 11.1 below.
- Completion of Assurance Level requirements for key application systems that will likely require access from non-agency domiciled personnel.
- Alignment of user credentials across agencies such that an employee in one agency can authenticate her/his identity to the required level for access to other agency systems. This will require the development of Federated Services.
- The development and implementation of overarching MOU's to bind the parties (see section 11.3.3 for further coverage of this issue).

The implementation of these approaches will be dependent upon the requisite infrastructure (as discussed earlier) being in place. In essence this requires the implementation of abstracted identity and authentication processes as defined within the Framework. The extent of effort required to do this will depend on both the application systems and the underlying technology infrastructure.

Whilst not a necessary component for cross-agency dealings, the implementation of a WoWAG Internal directory would provide a powerful mechanism for implementing the necessary user identification and authentication processes required by these agency specific systems.

⁴ See section 4.2 and Appendix B of the Framework for an in-depth analysis of Trust Models including the Federated model.

10. Progressing G2B and G2C

With few exceptions agencies currently operate siloed Id&AM architectures within and across agencies when dealing with businesses and citizens.

As seen with DLI's Landgate initiative, there are considerable benefits in providing a single method of access to these external users across a range of application areas.

In a whole of government sense there are potentially substantial benefits in expanding this single view across multiple agencies.

However, more detailed review of these specific opportunities is required in order to assess these cases and priorities for providing a more holistic view of government to external users.

Accordingly it is proposed that more detailed work be completed, based around the Id&AM Framework, to:

- Investigate in more detail and assess agencies' current positions and future plans in regard to allowing access to network/web facing environments by external parties, the credentials used/planned and level of policy development guiding this access.
- Identify candidate agencies, or clusters of agencies, that offer opportunities of significant benefit to agencies and users through a consolidated or coordinated approach to identity management, and in particular a coordinated approach to identity authentication across a shared user base.
- Assuming that opportunities exist, various alternatives need to be assessed, in the context of the Id&AM Framework, for the sharing of:
 - **infrastructure and solutions** (including operational sharing and technology procurement) including:
 - User directory/s
 - Authentication Solutions/Service
 - Authentication 'hardware' eg cryptographic processors.
 - Delegated User Administration facilities (eg through portal)
 - Application Permissions Management Solutions
 - **Processes**, including
 - User outreach/awareness raising
 - Evidence of identity checks; qualification checks; authority checks; police clearances; etc
 - User registration and deregistration
 - Maintenance of user details
 - Help desk in relation to credentials
 - End-user agreements
 - **credentials** including the re-use of existing credentials.

Such sharing is largely independent of the trust model/s adopted by agencies as illustrated below.

The resultant approach may be specific to one or more nominated departments or clusters or potentially applicable across WoWAG.

Possible approaches are represented in the matrix below where the “ticks” represent various sharing opportunities:

Trust Models >>>	Siloed	Scheme/ Community	Centralised	Federated
Potentially Shared Components				
Infrastructure & Solutions	√	√	√	√
Processes	√	√	√	√
Credentials	X	√	√	√

The proposed work would be focused on examining each of the areas in which sharing of components appears to be possible. In particular this will seek to address:

- Whether and how sharing of one or more components might work.
- Operational, contractual/legal, risk management and commercial issues that would need to be resolved.
- Benefits to the agency (as an issuing and/or relying party).
- Benefits to external users.
- Extensibility to agencies beyond the cluster.

As foreshadowed previously and as discussed in more detail in section 11.1.5 below, the proposed Supplier Registry initiative has the potential to springboard the addressing of this matter and even to provide a key aspect of the infrastructure.

Draft for Comment

11. Other Action Areas

This section examines other required areas for action at a WoWAG and OeG level.

11.1. WoWAG and Agency-cluster Initiatives

11.1.1. Shared Corporate Services

The Id&AM Framework will leverage the implementation of the Shared Corporate Services (SCS) initiative through the introduction, subject to the proposed PPIA, of a WoWAG Identifier. This will be progressively adopted as the primary identifier within agency authentication portals, and ultimately where justified, within application systems across government.

The introduction of the WoWAG identifier will require some significant consideration in the design, implementation and operation of the HR systems within Shared Corporate Services, and in particular will require agreement upon (inter alia):

- The characteristics of the identifier – format, method of maintaining WoWAG uniqueness notwithstanding no single point of aggregation, level of persistence etc.
- The methods and basis of registration of employees and contractors.
- The methods by which the HR system issues associated credentials and the management of these credentials, including authentication.
- The synchronisation of the HR directories with agency based user stores or directories and the frequency and methods with which various status information changes are communicated.
- The methods of transfer of employees across clusters and the implications of this on relying systems in other agencies.

The role played by SCS as the 'outsourced' HR department of agencies and as the host of the agencies' HR applications is pivotal in relation to the identity and access management lifecycle for internal users (WA Government employees and contractors).

It will be necessary to resolve the following at an architecture, process, and possibly contract/service level:

- The role of the HR system within the Id&AM architecture. Of particular importance is whether or not the HR system is the authoritative source for identifying information for all internal users.
- The relationship between the SCS HR datastore instances (there being a number of these) and the WoWAG identity store recommended by this assignment, and whether the latter could be provided by the SCS.
- The extent and robustness of evidence-of-identity and other clearance checks (eg police, qualifications) undertaken by the SCS HR function and the liability associated with these.
- The timing, sequence, dependencies between HR processes and the establishment of user authentication credentials and (agency-level) access permissions.
- How Id&AM can be enabled for users across agencies' internal systems environments as well as the SCS system facilities – ie how can users achieve a single or simplified sign-on to both their agency and SCS systems?

11.1.2. Shared Land Information Platform

The Shared Land Information Platform (SLIP) is being developed, within the Landgate environment, on behalf of a consortium of agencies. SLIP is intended to connect to a range of agency systems and provide access to content for agency personnel and externals. While still at an early stage provides the following possibilities for the WA Government more broadly:

- Potential case study in relation to deployment of:
 - o A federated approach to identity and access management, and existing and emerging 'open' standards related to this (eg LDAP and SAML2).
 - o Digital rights management technologies and standards.

- Potential for other agencies to leverage authentication and permissions management infrastructure and solutions (including delegated administration management).
- Potential for other agencies to leverage credentials issued to business users.
- Potential to leverage inter-agency MOUs and user agreements.

11.1.3. Transport Executive and Licensing Information System

The Transport Executive and Licensing Information System (TRELIS) is a modernising, integration and consolidation of Western Australia's existing vehicle and driver databases into one database with the intention of providing data accuracy and integrity and delivering better customer service.

It has interfaces to a number of agencies including the Western Australian Police Service, the Department of Justice, the Insurance Commission of WA and the Department of Consumer and Employment Protection, and the Office of State Revenue.

A more detailed examination of TRELIS is considered worthwhile to determine:

- opportunities for leverage of infrastructure, processes and policies; and/or
- how and where TRELIS should be harmonised with the other Id&AM initiatives discussed in this Action Plan.

11.1.4. Criminal Justice Integration Project

The Criminal Justice Integration Project (CJIP) provides the following possibilities for the WA Government more broadly:

- A case study of an already implemented and operational, highly trusted joined-up government initiative.
- MOUs and User agreements.
- An advanced Id&AM architecture.
- Systems architecting and systems performance issues associated with 'abstracted' approach to Id&AM (eg single user ID and permission store).
- Experience in implementation of single/simplified sign-on.
- Experience in workflow approach to provisioning and deprovisioning.
- A design for and experience in role-based access control and the classification,
- Skilled personnel.

The capacity to share infrastructure and solutions with government more broadly while worthy of further exploration is not seen as particularly likely given the highly sensitive nature of the CJIP environment.

11.1.5. Whole-of-Government Procurement Reform Project

The development of the Supplier Registry should be leveraged as a unique 'infrastructural' opportunity for the Government to register and issue authentication credentials to a large number of suppliers (and by implication their staff) that could be used more broadly across other Government applications.

11.2. OeG Focus Areas

11.2.1. Enterprise Architecture

Section 4.10.2 of the Framework covers the suggested actions that agencies should take to factor Id&AM issues into their Enterprise Architecture (EA) approaches.

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

11.2.2. Directories

OeG is in the process of examining the feasibility of directories at an agency and WoWAG level. This initiative is cognisant of the Id&AM uses of directories that are possible, but is also examining other uses such as white and yellow pages.

The Framework calls for the implementation of a WoWAG identity store which would hold basic identifying information for all internal users, and, at their option, external users.

The development of the detailed requirements for this facility and the business case for its implementation should be addressed in conjunction with the OeG 'directories team' as this facility could undoubtedly meet most if not all of the requirements of Id&AM identity store and the additional functions sought by OeG. See also section 5.1 above.

11.2.3. Telecommunications Initiative

The Government is in the process of establishing WoWAG arrangements for an IP-based telecommunications network.

The introduction of a WoWAG Identifier and associated authentication mechanisms potentially provides a basis for the authentication of users seeking access to the planned WoWAG telecommunications infrastructure and services.

The extent to which a future WoWAG Directory, containing user identification and authentication information, could be used as, or is required by, the telecommunications initiative requires further analysis, once the detailed analysis phase of the Telecommunications project has been completed and Id&AM functions, especially authentication, determined. See also section 5.1 above.

11.3. Legal

A number of proposed actions are listed below:

11.3.1. Legal Analysis

A comprehensive review of relevant laws needs to be undertaken, by a lawyer who specialises in the area, including discussions with relevant Commissioners and agencies, the drafting of an issues paper, and review.

This will need to identify the impacts of the implementation of the Framework on issues including:

- Evidence
- Enforceability of contracts and declarations
- Privacy and other public policy issues
- Archiving statutes/regulations.

Each agency and each program that proposes to apply the whole-of-government Identity & Access Management Framework needs to conduct an agency- and/or program-specific analysis of relevant laws.

11.3.2. Privacy Act

Section 7.1.1 above has highlighted the need to consider the introduction of a Privacy Act in order to underpin aspects of the Government's administration of Id&AM, and to provide entities with a required level of assurance regarding Id&AM schemes.

11.3.3. Operational Legal Agreements

The move towards cross-agency and more federated forms of Id&AM, and, in particular, authentication, may lead to a plethora of bilateral MOUs between the agency issuing a credential and those agencies that rely upon it. Typically such MOUs cover issues relating to:

- responsibility for, robustness of and processes associated with user identification, registration and enrolment into applications;
- responsibility for, robustness of and processes associated with user deregistration;
- the nature of Agreements, if any that users have to sign before being provided access;
- liability for 'inappropriate access' and its consequences;
- reporting processes;
- responsibility to remedy breaches;
- connectivity and service level matters.

Two approaches make possible a rationalisation of this issue:

- Development of a scheme-based MOU in which all participants sign one MOU and agree to be bound to the conditions in relation to interactions with all other signatories of the MOU; or
- A boiler-plate MOU is developed which, while still entered into on a bilateral basis, reduces the requirement for bespoke development each time.

Of interest as well are User Agreements particularly those that require signing by users in eg Agency B who are accessing resources on the systems of Agency A.

Typically these cover user rights and responsibilities

- Reasonable use policies
- Confidentiality/privacy provisions
- Penalties for breaches
- Requirements to protect credentials.

Once again the development of boiler-plate agreements would reduce cost and effort.

Agencies and initiatives that are in a position to contribute useful exemplars of both of the above to this exercise include DoJ and SLIP.

12. Proposed Schedule and Major Action Items

The schedule below provides a high level view of possible timings for the Action Clusters listed in sections 7 through 11 above. A more detailed project plan will need to be developed as part of the Foundational Activities. This will require a harmonisation of detailed inputs from agencies and WoWAG initiatives.

	4Q05	1Q06	2Q06	3Q06	4Q06	1Q07	2Q07	3Q07	4Q07
Foundation Activities									
Agency Consolidation									
Advancing Government to Government									
Progressing G2B and G2C									
Other Action Areas									

Draft for Comment

Attachment 1 – Summary of Proposed Approach

Aspect	Priority	Proposed Approach	Similarities or Differences in Approach		Actions/Implications		Alignment / Consistency with
			Internal Users	External Users	WoWAG	Agency	
INFORMATION MANAGEMENT							
Data Classification	Low	Develop and implement data classification scheme	identical	Identical	Develop & maintain	Adopt where appropriate	Commonwealth Government Protective Security Manual (PSM)
ENTITY MANAGEMENT							
Identifiers	High	<p>Implement a uniform approach across Western Australian Government.</p> <p>Internal users to have an identifier that is unique across Government. Identifier is ideally persistent if user changes agency.</p> <p>Authoritative source for Internal users is HR systems.</p>	Identifier being agreed with Shared Corporate Services is primary identifier	<p>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.</p> <p>For business users, ABN is preferred identifier, potentially with subordinate identifier within business.</p> <p>For business, may accept other identifiers such as HeSA, and map to WoWAG Identifier</p>	Central Id number issuer.	Use central ID issuing service.	

Aspect	Priority	Proposed Approach	Similarities or Differences in Approach		Actions/Implications		Alignment / Consistency with
			Internal Users	External Users	WoWAG	Agency	
Registration	High	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 Banking Industry
Evidence of Identity (EOI)	High	Develop & continue to maintain best practice approach and align approaches with Credential Assurance Levels and Registration Levels. Consideration of inclusion of attributes such as 'Police checks' in record of EOI processing – i.e. to reduce duplication of processes.	Some variations in process and nature of evidence		Develop & maintain	Follow	Commonwealth Banking Industry
Enrolment	High	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. Need will exist until all applications migrate to single identifier usage	Some variations in process. Likely to persist indefinitely	Develop & maintain	Adopt and adapt	
User Clearance Levels	Low	Develop and implement user clearance level scheme. This is distinct from attribute verification which is dealt with in EOI above	identical	Identical Unlikely to arise	Develop & maintain	Adopt where appropriate	Commonwealth PSM
ID Mgt Role of Agency Meta-directories or agency user stores	High	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	

Aspect	Priority	Proposed Approach	Similarities or Differences in Approach		Actions/Implications		Alignment / Consistency with
			Internal Users	External Users	WoWAG	Agency	
AUTHENTICATION MANAGEMENT							
Credential Assurance Level	High	<p>Follow AGAF (Authentication Technique) model.</p> <p>Extend to develop detailed criteria along lines of US Gov 'Credential Assessment' approach incorporating Authentication Protocol</p> <p>Supported by recommendations in relation to:</p> <ul style="list-style-type: none"> - Evidence of Identity - Evidence of Record Ownership - Credentials/Tokens - Credential Issuer Reliance 	Identical	Identical	Develop & maintain	Follow WoWAG guidelines	Commonwealth
Credential Issuer Reliance Levels	Moderate	<p>Introduce notion of reliance level of credential issuer to support possible use by WA Government agencies of externally issued credentials.</p> <p>Also supported by the development of MOUs to apply between agencies issuing credentials to internal or external users.</p>	Identical	identical	Develop & maintain reliance evaluation criteria	Agencies to make own assessments based upon threat-risk factors.	
ACCESS MANAGEMENT							
Application Assurance Levels	Moderate	<p>Follow AGAF 1-4 level model.</p> <p>Develop more detailed procedures/criteria to determine assurance level.</p>	Identical	Identical	Develop & maintain	Follow WoWAG guidelines	Commonwealth

WA Office of e-Government – Identity & Access Management Framework Project

Aspect	Priority	Proposed Approach	Similarities or Differences in Approach		Actions/Implications		Alignment / Consistency with
			Internal Users	External Users	WoWAG	Agency	
Role-based Access Control	Moderate	Move to role-based access control to ensure scalability and efficacy of three-tier Id&AM architecture. 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	High	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	Moderate	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.	High	Develop and implement	Variation to reflect intra-dept reliance	Variation to reflect reliance on or by external credential provider	Develop & maintain	Adopt and adapt	
SHARED SERVICES							
ID Mgt role of WoWAG Directory	Moderate	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. 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	

Aspect	Priority	Proposed Approach	Similarities or Differences in Approach		Actions/Implications		Alignment / Consistency with
			Internal Users	External Users	WoWAG	Agency	
Registration Services	Low	Examine opportunities for sharing or using external service providers to complete registration processes	N/A	Use at agency option	Provider	User	
Authentication Services	High	Examine opportunities for sharing of authentication services and thereby credentials across agencies. 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	Low	Examine opportunities for Shared Services.	N/A	Use at agency option	Provider	User	

Draft for Comment

Aspect	Priority	Proposed Approach	Similarities or Differences in Approach		Actions/Implications		Alignment / Consistency with
			Internal Users	External Users	WoWAG	Agency	
ARCHITECTURE, STANDARDS AND GUIDELINES							
Architecture Model	High	Hybrid	Primarily Scheme based due to proposed single identifier and underpinning common MOUs	Primarily siloed. 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	High	Develop & continue to maintain standardised list and align approaches with Credential Assurance Levels. Support one, two and multiple factor approaches: <ul style="list-style-type: none"> - User-ID/Password - Shared Knowledge (KBA) - Shared Secrets - PKI (soft) - PKI (hard) - Challenge Response - Smart cards and other tokens - Biometric Supported by recommendations in relation to Credential Assurance Level.	identical	identical	Develop & maintain	Follow	Commonwealth (possibly banks to the extent that existing tokens could be leveraged).
Application Development Toolkits	Moderate	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	Moderate	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	Priority	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	

Draft for Comment

Attachment 2 - Id&AM Standards

This attachment provides an overview of contemporary standards and their use which it is envisaged will provide the basis of a WoWAG Id&AM Standards Resource.

Relevant Standards Bodies

Some of the industry standards bodies and other organisations currently most active in the access control area are:

W3C	The World Wide Web Consortium www.w3c.org
OASIS	Organisation for the Advancement of Structured Information Standards www.oasis-open.org
Liberty Alliance Project	Liberty Alliance Project www.projectliberty.org
IETF	The Internet Engineering Task Force www.ietf.org
RSA Laboratories (PKCS)	RSA Laboratories (research centre of RSA Security Inc.) Public-Key Cryptography Standards (PKCS) www.rsasecurity.com/rsalabs

Other standards organisations of importance include:

Standards Australia	Standards Australia Standards: Enterprise Risk Management; Information Systems security; PKI and many others www.standards.com.au
NIST	National Institute of Standards & Technology Is primary source of detailed US Government positions on security. www.nist.gov

Useful Standards for Access Control

The following list of standards is provided as a guide only⁵. Other standards not listed here may be more suitable in some environments.

Choice of standards within each agency will be influenced by support in available products, fit with requirements, and new and evolving standards work.

TLS (SSL, HTTPS)	Transport Layer Security (the successor to Secure Sockets Layer (SSL) and the S (secure) in HTTPS when used with HTTP) This is the protocol very commonly used to secure communications between a browser and a web-server. The protocol provides <ul style="list-style-type: none">• encryption of data for confidentiality,• message authentication for data integrity,• authentication of the web-server (this is optional but is normally used)• optional authentication of the user if client-certificates are used. When client-certificates are not used (the typical case), other types of authentication (eg passwords) are afforded protection by the encryption and data integrity of TLS. See www.ietf.org/rfc/rfc2246 (& RFC3546)
XML- Signature	“XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.” XML Signatures are most suited to web-services or thick-client interaction. The ability to include data by reference allows for significantly reduced message sizes where there is static data common to many transactions which must be included within the signed data (eg standard terms and conditions, policy, etc.) See www.w3.org/TR/xmlsig-core/
XML- Encryption	“XML-Encryption specifies a process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element, or XML element content. The result of encrypting data is an XML Encryption element which contains or references the cipher data.” XML Encryption is most suited to web-services or thick-client interaction. Considerable flexibility is provided, allowing encryption of only the sensitive portions of a message, which can significantly improve performance. See www.w3.org/TR/xmlenc-core/

⁵ DoJ note that many of these standards are either still in development (eg WS-Security, Liberty Alliance) or are still being refined (eg SAML, XACML) and at present are not without problems.

S/MIME S/MIME (Secure MIME) is the most commonly supported secure email standard. It provides for digital signing and/or encryption of data based on the MIME (Multipurpose Internet Mail Extensions) standards. S/MIME is most useful for unstructured human-to-human correspondence, or for machine-to-human correspondence. It can also be used for machine-to-machine transactions although XML-Signatures and XML-Encryption are considered more suitable and provide more flexibility.

See www.imc.org/ietf-smime/index.html

SAML **Security Assertion Markup Language**

“SAML is an XML framework for exchanging authentication and authorization information”

Although SAML also covers authorisation to some extent, its primary focus is on passing authentication information. The later XACML standard is a more complete protocol for passing authorisation information.

See www.oasis-open.org

XACML **Extensible Access Control Markup Language.**

XACML allows permissions policy *enforcement points* to query permissions policy *decision points*, which can in turn query other policy *decision points*. This allows for centralised permissions enforcement, and centralised, collaborative or devolved permissions management.

See www.oasis-open.org

WSS **Web Services Security**

(WS Security) WSS specifies message integrity and confidentiality for server-to-server messaging using SOAP (Simple Object Access Protocol www.w3.org/TR/soap/). It allows for a variety of authentication approaches including username + password, digital certificates, etc. Authentication information can be exchanged using either Kerberos (web.mit.edu/kerberos/www/) or SAML.

See www.oasis-open.org

Liberty Alliance Project

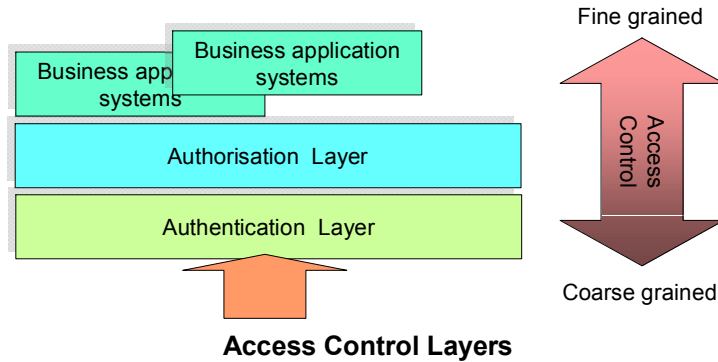
This consortium focuses on specifications and guidelines to support “Federated Identity Management”, building on available standards. Federated Identity Management means loosely-coupled authentication, authorisation and access control across organisational boundaries. The protocols and guides have a strong focus on preserving user privacy.

See www.projectliberty.org/

Applicability to the Proposed WoWAG Framework

The diagram, reproduced from section 3.5.2. (Access Policy Enforcement) of the Framework, illustrates that:

- access policy enforcement can be implemented over a number of architectural layers; and
- 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.



The applicable security standards available for consideration at each layer are:

Layer	Applicable security standards
Business application systems	Applicable standards will depend on the nature of the application. It is however seen as important that agencies define a model for their applications and ensure the applications comply to that model. The work undertaken by DoJ in this area will be helpful.
Authorisation	XACML (SAML) WS-Security Liberty Alliance
Authentication	SAML TLS with client certificates S/MIME XML-Signatures

Security Purpose / External Technology Matrix

The following table maps relevant standards mentioned above against security purpose for commonly used external communications environments.

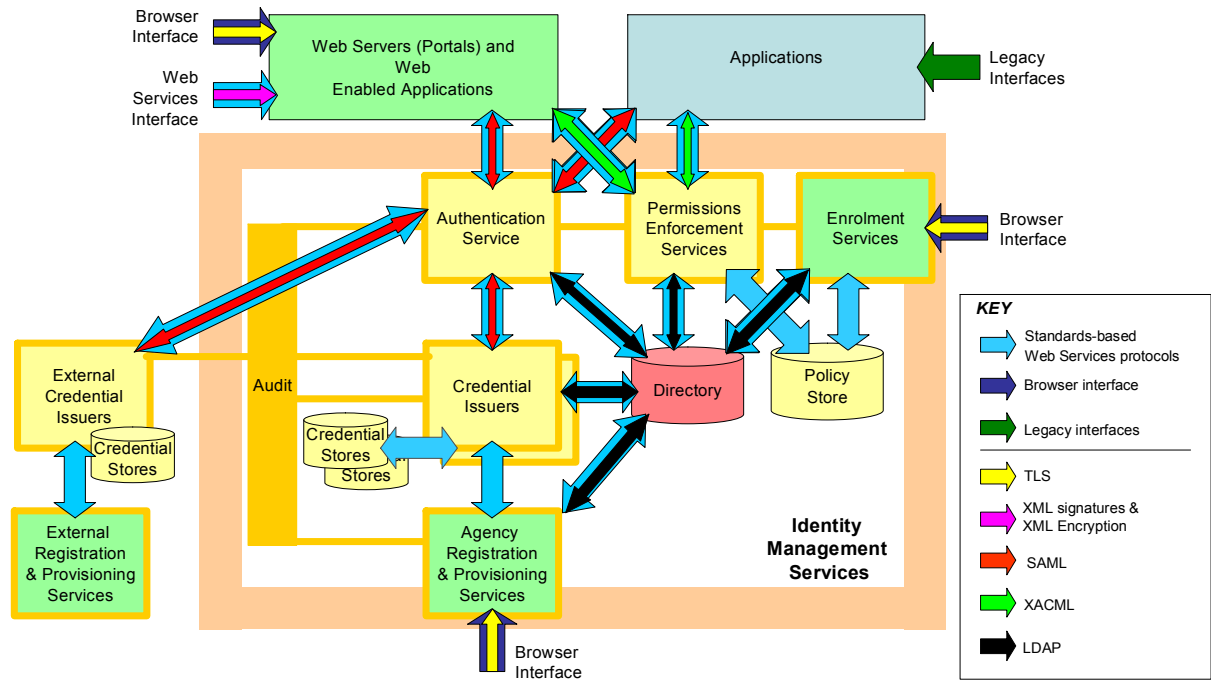
Note that there are other unlisted alternatives in each case. This table only covers protocols used between external systems and a service provider. It does not cover protocols used within the authentication and authorisation layers, or for communications between service providers and credential providers.

Security Purpose	Browser to Web-server	Email	Thick Client to Application	Web Services (server to server)
Authentication	TLS with client-certificates	S/MIME	XML-Signatures	XML-Signatures ⁶
Message Authentication (integrity)	TLS	S/MIME	XML-Signatures	XML-Signatures
Signing (non repudiation)	XML-Signatures (by using applet)	S/MIME	XML-Signatures	XML-Signatures
Confidentiality	TLS	S/MIME	XML-Encryption	XML-Encryption

⁶ DoJ notes: There is a fitness for purpose approach here. Not all business services will require this level of security for authentication. In fact many will only require Username/Password.

Id&AM Framework Infrastructure Protocols

The diagram (a reprise of the architecture diagram in Section 4.8.1 of the Framework illustrates indicative use of some of the standards/protocols within the authentication and authorisation technology and process architecture.



Architecture with overlaid Standards

Note that other protocols not shown here will also be needed across each connection at different or equivalent levels of the protocol stack.

For example, where SAML is shown:

- the protocol stack might be IP - TCP - HTTP - SOAP – SAML
- other web-services protocols may be used over SOAP in addition to SAML e.g. key exchange protocols, business process protocols (eg from the ebXML suite)
- other security protocols may be used at lower levels of the protocol stack to secure the connection between servers. eg
 - L2TP - IP - TCP - HTTP - SOAP – SAML, or
 - IP - IPSEC- TCP - HTTP - SOAP – SAML, or
 - IP - TCP - TLS - HTTP - SOAP – SAML.