Australian Government

Digital Transformation Office

National e-Authentication Framework

Better Practice Guidelines – Vol 4 Positioning and Strategy

January 2009

Disclaimer

This document has been prepared by the Department of Finance and Deregulation (Finance) to provide information to government bodies in relation to the use of e-Authentication for government transactions.

While every effort has been made to ensure that the document is accurate, no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the document. This document should not be relied upon as legal advice. Users are encouraged to seek independent advice relevant to their own circumstances.

Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

ISBN 0 9758173 7 X

Department of Finance and Deregulation
Australian Government Information Management Office

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Copyright: Department of Finance and Deregulation

Contents

1. Introduction 4

2. Identity and Access Management 6

2.1 Introduction 6
2.2 IAM Lifecycle 6
2.3 Framework Overview 7
2.4 Identity and Access Management Policy 8
2.5 Entity Management 9
2.6 Resource Management 10
2.7 Authentication Management 11
2.8 Access Management 12
2.9 Governance and Operations 12
2.10 Architecture, Standards and Guidelines 13

3. e-Authentication Strategy 15

3.1 Introduction 15
3.2 Summary of strategy development process 15
3.3 Task Group 1 – Preparation 17
3.4 Task Group 2 – Analyse “As Is” Environment 18
3.5 Task Group 3 – Determine “To Be” Environment 19
3.6 Task Group 4 – Undertake a Gap Analysis 20
3.7 Task Group 5 – Develop Implementation Strategies and Priorities 21

Appendix 1: Risk and Security Policies and Standards 23

Introduction 23
Risk management 23
Information security 24
Identity Security 26

Appendix 2 – IAM Implementation Considerations 30

Assessing Identity and Access Management Maturity 30
Longer Term Identity and Access Management Planning 30

Appendix 3: Reference Documents 34

Figures

Figure 1: Identity and Access Management Lifecycle (showing information stores) 7

Figure 2: IAM Framework 8

Figure 3: IAM Conceptual Architecture (with standards overlay) 14

Figure 4: Developing an e-Authentication strategy – all tasks 15

Figure 5: Developing an e-Authentication strategy – Task 1 17

Figure 6: Developing an e-Authentication strategy – Task 2 18

Figure 7: Developing an e-Authentication strategy – Task 3 19

Figure 8: Developing an e-Authentication strategy – Task 4 20

Figure 9: Developing an e-Authentication strategy – Task 5 21

Tables

Table 1: IAM – Resources and Entity Types 8

1. Introduction

This volume forms part of the Better Practice Guidelines published to assist with agency implementation of the NeAF.

This volume:

- outlines a framework that agencies can use to examine the broader Identity and Access Management (IAM) requirements of which e-authentication is a part; and
- clarifies the positioning of NeAF in relation to risk management, information management and ICT security policies and standards.

A key driver for NeAF is the achievement of consistency in authentication approaches, across agencies and jurisdictions. This will increase efficiency and enable:

- re-use of credentials
- sharing of infrastructure and solutions; and
- extensibility of authentication schemes.

This requires that agencies have an overarching e-authentication strategy and implementation plan rather than applying the NeAF as and when new applications are being introduced by a particular business unit within an agency. An e-Authentication strategy is part of an agency's overall IAM Framework. This document will therefore provide an overview of the broader IAM environment as means of contextualising the development of an e-Authentication strategy.

Appendix 1: Risk and Security Policies and Standards to this volume provides an overview of relevant policies and standards.

Appendix 2: IAM Implementation Considerations provides further detail on implementation issues relating to development of an Identity and Access Management Framework.

Appendix 3: Reference Documents contains a list of reference documents.

This document is currently under review by the Digital Transformation Office.

2. Identity and Access Management

2.1 Introduction

The planning, implementation and operation of e-Authentication occurs within many contexts including enterprise risk and security management, systems planning, development and operation, and overarching Identity and Access Management (IAM).

Implementing e-Authentication solutions should be done within a well architected and orchestrated IAM framework. This section provides a high level framework for IAM. Appendix 2 provides guidance on the determination of the maturity of agencies IAM approaches and longer term planning for aggregated and/or federated IAM.[1]

For the purposes of this National e-Authentication Framework, IAM may be regarded as:

> *an integrated system of policies, processes, and technologies that enables agencies and the Government as a whole to facilitate and control users' access to applications and information resources while protecting confidential personal and business information from unauthorised users.*

When applied in a consistent and systematic way IAM underpins:

- identification of parties involved in government-related 'transactions' – employees, contractors, patients, organisations and locations
- authorised access to resources
- confidential transmission and receipt of private or sensitive information
- integrity of information transferred between parties; and
- traceability and audit of activity between transacting parties.

2.1.1 Benefits of improved IAM

The major goals of improved IAM are:

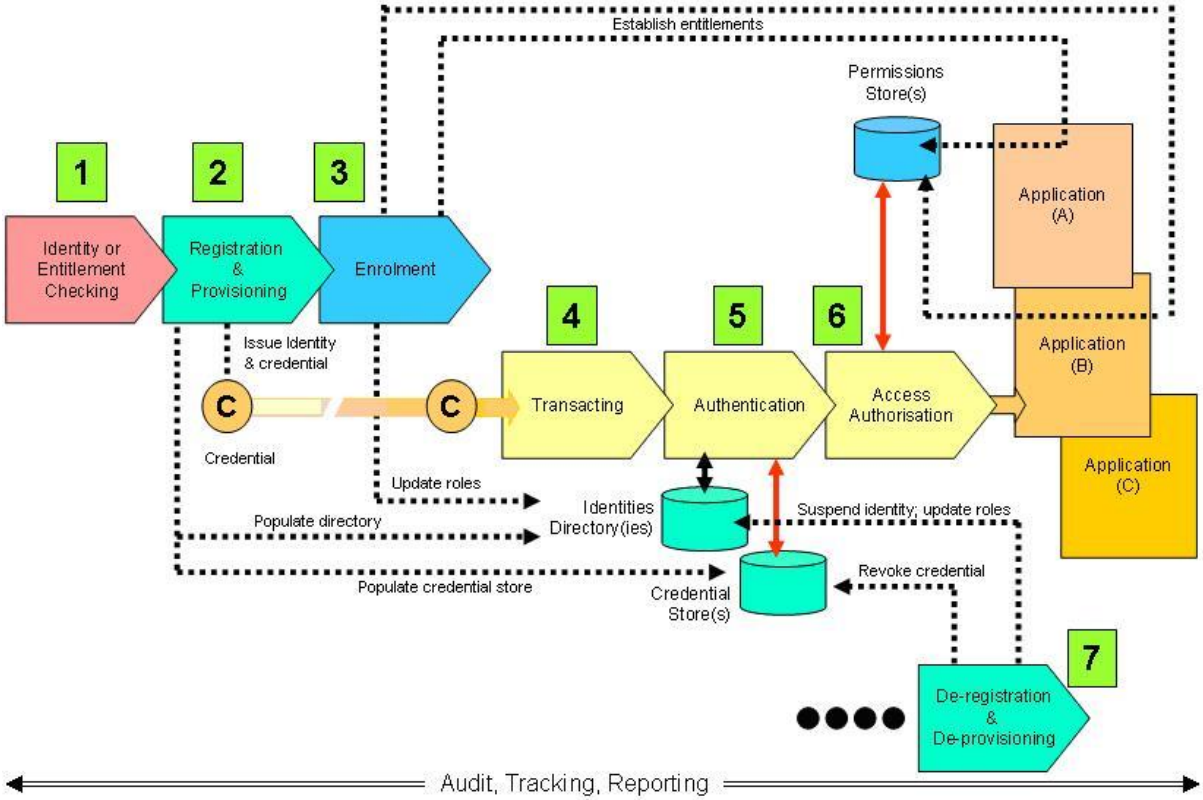
- improved productivity through the adoption of common solutions (including shared services and/or bulk licensing) and automation of manual 'access-related' processes
- better risk management through improved provisioning and de-provisioning, consistency of information classification and business processes, and improved support for less-well resourced agencies
- improved access by citizens in a consistent and 'efficient' manner
- improved access by the private sector leading to efficiency and industry development gains; and
- improved access to information based upon person rather than the organisation to which they belong.

2.2 IAM Lifecycle

Identity Management covers all policy, process and technology elements necessary to effectively service the Identity and Access Management lifecycle as illustrated below.

[1] Content in this section has been drawn from work undertaken by Convergence for the Governments of Victoria, South Australia and Western Australia.

Figure 1: Identity and Access Management Lifecycle (showing information stores)



2.3 Framework Overview

An IAM Framework is a distillation of legal, policy, process and technology factors that collectively determine how well organisations manage user identities and the resources to which those users may gain access. Each element of the IAM Framework can be found within one of more elements of an agency's operating environment including HR, ICT and customer/stakeholder management.

To enable agencies to implement the advanced service environments required by contemporary customer-focused and joined-up government initiatives and IAM Framework is necessary in order to provide a consolidated view of "identity" across the spectrum of agency business units.

The IAM Framework described is intended to provide unified coverage of:

- management of all entity types; and
- access by these entities to all types of resources.

This document is currently under review by the Digital Transformation Office.

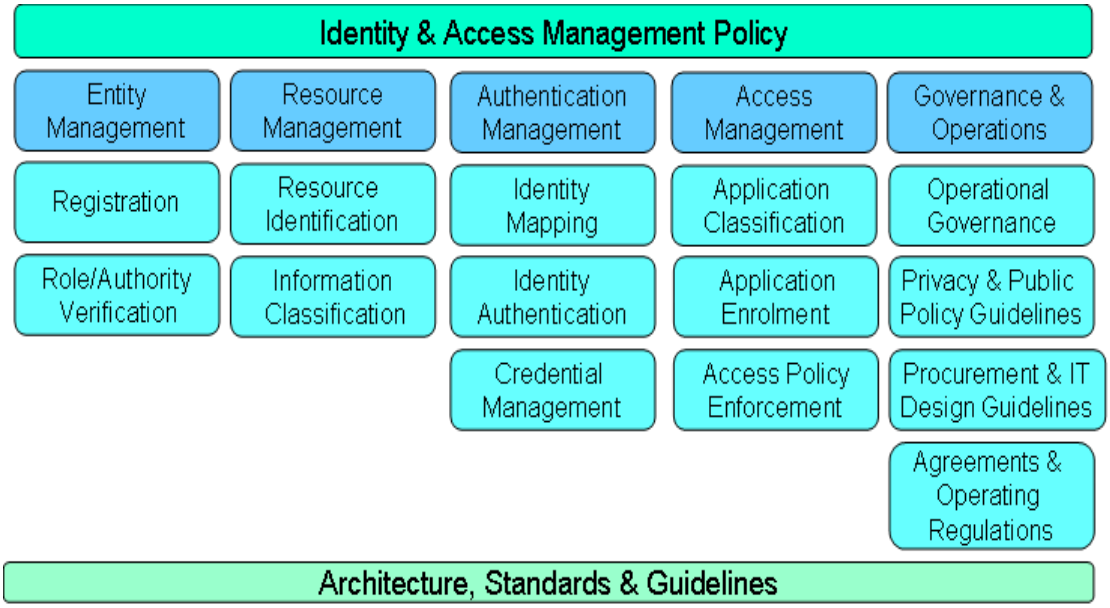
This scope is illustrated in Table 1 below.

Table 1: IAM – Resources and Entity Types

	Resource Types	
Entity Types	**System Resources**	**Physical Resources**
Internal Persons	√	√
External Persons	√	√
Automated Systems	√	√

The key pillars of the framework are illustrated below in Figure 2.

Figure 2: IAM Framework



A short description of each component of the framework and the 'target states' that agencies, agency-groups, sectors and whole-of-government initiatives should strive to achieve are detailed below.

2.4 Identity and Access Management Policy

Explanation

The IAM Policy 'pillar' is the minimum subset of principles, standards and practices that each agency undertakes to comply with, both within their agency and when interacting with other organisations. These cross-organisational contexts include agency-group, whole-of-government and sectoral. The fine detail of the policy may vary depending upon the context.

In general governments' goals are to achieve a consistent/interoperable policy environment across all agencies so as to ensure the:

- efficacy of the management of access to all government resources; and
- basis for interworking of identities across organisational boundaries to support the customer-centric and joined-up-government initiatives.

Target State

Agencies should develop and maintain a comprehensive, unified set of IAM policies covering the full lifecycle of the management of all entities including logical (i.e. systems) and as appropriate physical access. The policies should cover at least the following subjects:

- identification of entities (including evidence of identity) and determination of their 'roles'
- registration and enrolment of users in relation to establishment (and disestablishment) of credentials and resource access permissions
- the basis for classifying system applications, databases and other resources so that it is clear what level of assurance is required in order to allow user access to these
- authentication policies, compliant with the National e-Authentication Framework (NeAF)
- audit and reporting requirements and protocols; and
- approaches and protocols in relation to cross recognition of identities of outside entities (eg personnel of other agencies, vendors, etc).

The policies should be established and managed in concert with the following related policy areas:

- Human Resources: hiring, role assignment and modification, separation
- Vendor and Contractor lifecycle management, particularly the elements relating to personnel of these organisations
- Enterprise Risk Management as described by the AS/NZS4360 standard
- ICT/information Security as laid down by the governments' and agencies' Information Security Management frameworks and policies
- ICT Architecting and Management; and
- ICT Procurement.

2.5 Entity Management

Explanation

Entity Management refers to the whole of lifecycle management of entities that may gain access to Government resources (see particularly events 1, 2 and 7 in Figure 1 above).

Categories of human entities include staff, contractors, vendor/service provider staff, and customers (citizens and businesses).

Categories of non-human entities largely cover automated ICT systems that have a requirement to access information or physical resources; Supervisory Control And Data Acquisition (SCADA) systems are an example of the latter.

Target State

Agencies should:

- ensure the robustness of registration processes for all entities requiring access to government resources. Evidence of identity processes should follow the best practices set out in the National Identity Security Strategy and utilise, for high assurance levels, the resources of the national Document Verification Service[2]
- adopt, where practical, a role-based approach to determining the access permissions attributable to an entity/identity
- establish unified authoritative stores of identity information. It is anticipated that no more than two authoritative stores should exist:
  - one covering 'internal entities' such as agency staff, staff of other 'collaborating agencies', and contractors and service provider personnel who act in staff-like roles. Best practice suggests that the HR system should be the authoritative source
  - a second covering 'external entities' such as citizens, businesses, vendors
- implement automated provisioning/de-provisioning solutions; these should span the management of entities and their authentication credentials, as well as resource access management facilities.

2.6 Resource Management

Explanation

The key driver behind Identity Management is to ensure the authenticity and authority of people (or systems) that seek to gain access to Government resources. This requires that organisations have a robust and consistent approach to managing resources that is tightly coupled with the IAM lifecycle.

IAM is concerned with systems-based and physical resources.

Systems resources primarily consist of:

- information; and
- applications (ie computer programs) that create some form of outcome (eg HR, Payroll, Accounts Payable, Patient Health Records Management, etc).

The physical resources of most relevance are:

- premises or facilities to which access is controlled by some form of electronic access control; and
- operational systems that are computer controlled – e.g. SCADA systems controlling water pumps and sluices, electricity and telecommunications switching, traffic lights.

The appropriateness and completeness of information and asset management policies and practices are as important as identity management policies and practices in ensuring a robust approach to IAM.

Target State

Agencies should:

- uniquely identify each asset/resource so as to enable its effective management
- identify the owner/custodian for each asset/resource, and ensure that all decisions regarding the granting of access are made (directly or indirectly) by the owner/custodian

[2] Subject to availability and budgetary constraints.

- implement a resource access and assurance framework that dovetails effectively with the entity management approach described above. This should:
  - classify the resource based upon its intrinsic value/'sensitivity' and where necessary information security classifications contained in policy documents such as the PSM
  - identify all key aspects of the resource's lifecycle, and the associated controls and practices that should be associated with each 'event'
  - identify the matrix of entities/roles that are to be allowed to 'access' the resource and their related permissions
  - identify the tracking, auditing and reporting 'loop' necessary to ensure the effective ongoing management of this area
- in relation to the implementation of a consistent approach to the classification and control of all information, be guided by international standard, ISO-IEC 27002 – 2005 (Information technology code of practice for information security management).

Agencies must comply with government policies contained in the PSM and ISM (or their state and territory equivalents). Commonwealth agencies are required to comply with the Australian Government's Interoperability Frameworks and the Australian Government Architecture.

Other jurisdictions should consider using these frameworks as guidance in relation to ensuring the interoperability of information across organisations.

2.7 Authentication Management

Explanation

Authentication Management is the group of practices and processes that support the authentication of a user identity (see events 2, 5 and 7 in Figure 1 above). In an electronic environment, users are authenticated by presenting a credential when 'challenged' by the system.

Authentication credentials are re-usable. Once a user has been issued with a credential there should be scope for it to be used for multiple applications within an organisation or across multiple organisations. The emerging customer portals and single-entry points have an intrinsic requirement for this form of reusable authentication credential.

The implementation of customer-centric and joined-up government initiatives requires the implementation of a 'federated' approach to authentication across agencies. In principle this means that a user in Agency A, having been authenticated by that agency is able to gain access to information/ resources of Agency B using the same credential. See Volume 3 of the Better Practice Guidelines for detailed coverage of e-Authentication implementation models.

From a technology architecture perspective, effective authentication management requires that agencies 'abstract' authentication from individual application systems and manage authentication through a services layer.

Target State

Agencies should:

- implement authentication management as a 'services' layer and interface/integrate application environments with this facility
- adopt, where appropriate, a federated authentication approach to enable customers to be authenticated through portals and single-entry points. This is appropriate where staff need to collaborate with staff from other agencies, where case-management and equivalent cross-enterprise applications are warranted; and

This document is currently under review by the Digital Transformation Office.

- implement automated provisioning/de-provisioning solutions that span entity, authentication and access management.

2.8 Access Management

Explanation

Access management is concerned with the process of allowing or preventing authenticated users from accessing physical and systems resources. Access Management is concerned mainly with events 3, 6 and 7 in the IAM lifecycle as depicted in Figure 1.

Access management covers three key elements:

- the determination of the authentication assurance requirements relating to the application system or information to which access is requested
- the enrolment of users into applications, and subsequent un-enrolment; and
- the enforcement of the user access policy for the specific application or information resource.

Target State

Agencies must comply with relevant whole-of-government policies in relation to information security management (such as the Australian Government Information and Communications Technology Security Manual (ISM), the Commonwealth Protective Security Manual (PSM) for Commonwealth agencies) and privacy.

Agencies should:

- implement a consistent approach to determining assurance level requirements associated with resource types and user types. The approach should be consistent with:
  - national standard AS/NZS 4360 (Risk Management standard)
  - international standard ISO/IEC 27000 (IT Security standard)
- implement a role-based access control environment
- implement ‘first level’ access/permissions management as a ‘services’ layer and interface/integrate application environments with this facility; and
- implement automated provisioning/de-provisioning solutions to span entity, authentication and access management.

2.9 Governance and Operations

Explanation

The governance issues raised by the adoption of multi-organisational IAM (and e-Authentication) approaches require clear delineation of where strategy and policy decisions are made, implemented and enforced.

Better Practice Guidelines – Volume 3 provides further insight into the appropriate level at which governance related activities need to occur for various e-Authentication implementation models.

At issue is the extent to which the matters listed below have to be harmonised at multi-organisational (e.g. whole-of-government, whole-of-sector) level versus agency level:

- identifier schemes (eg for employees and customers) and naming conventions

This document is currently under review by the Digital Transformation Office.

- evidence of identity requirements
- authentication credential requirements
- conventions for classifying information resources
- business rules and legal/liability issues particularly where shared trust schemes are to exist between agencies or across government; and
- system interfaces and protocols, particularly in relation to shared trust environments.

The effective resolution of these matters, which will vary over time, requires that designated 'formal' governance structures exist at an agency, sector or whole-of-government (or sector) level.

There are a range of appropriate governance mechanisms (such as the Chief Information Officers Committee (CIOC)/Cross Jurisdictional Chief Information Officers Committee (CJCIOC) at whole of government level) which can be employed.

Other key matters that require addressing are ensuring that:

- individual privacy matters are identified and effectively dealt with
- agency and whole-of-government procurement arrangements embed the requirement for new application systems to comply with the IAM Framework and architecture
- agency IT design/development guidelines embed the requirement for new application systems to comply with the IAM Framework and architecture; and
- appropriate agreements and operating regulations are established between agencies (and possible non-government organisations) that will 'share trust' through e.g. federation of authentication credentials or sharing of authentication and permissions management facilities/services.

Target State

Agencies should:

- identify/establish an appropriate governance regime to oversight the required upfront and ongoing activities necessary to comply with the IAM Framework. This will ensure that appropriate IAM activity tracking and reporting is put in place to effectively support the governance
- ensure that IAM-related privacy management approaches are compliant with the *Privacy Act 1988* (Cth) or privacy regimes as appropriate
- implement procurement policies/guidelines that embed the key aspects of the IAM Framework and Architecture (when this has been developed)
- implement ICT design and development policies that embed the key aspects of the IAM Framework and Architecture (when this has been developed); and
- implement appropriate agreements with partners organisations when entering into agency-group or sector-based shared trust environments.

2.10 Architecture, Standards and Guidelines

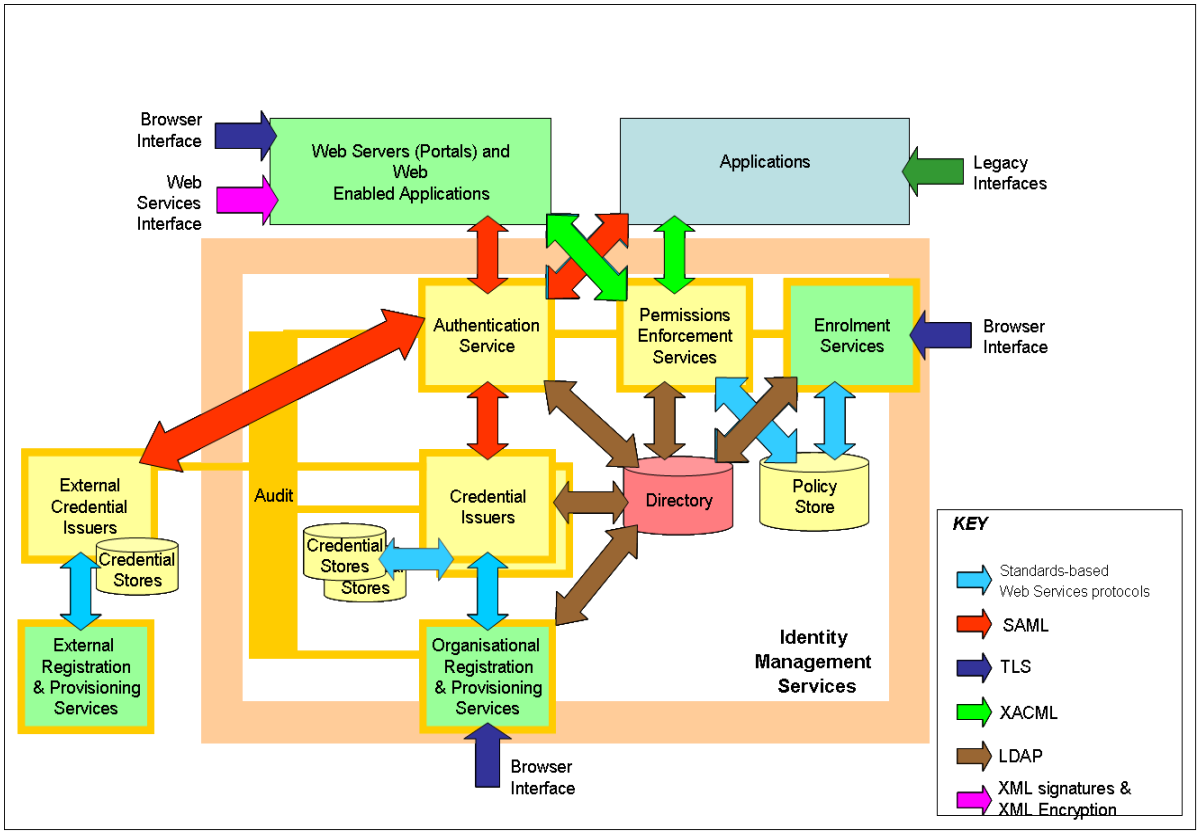
Explanation

An IAM architecture represents the detailed information and technology 'articulation' of key aspects of the IAM framework.

A high level IAM architecture is illustrated in Figure 3 below:

This document is currently under review by the Digital Transformation Office.

Figure 3: IAM Conceptual Architecture (with standards overlay)



The standards used in Identity management are described in five core categories:

- standards for profiles and services
- standards for Web Transport, session and security
- standards for tokens
- standards for policy and management; and
- standards for message security.

Guidelines and standards are essential to underpin the implementation of each element of the IAM Framework in order to support conformance and interoperability. Guidelines are particularly required where there are no national/international standards, or where these allow for 'flexibility' within individual implementations. Guidelines will be required for many of the subject matter areas referred to under the Governance pillar.

Target State

Agencies should:

- develop and maintain an IAM architecture[3] and procure and develop IAM solutions in accordance with this architecture; and
- implement a standards-based approach to IAM.

[3] A whole of government IAM Architecture is needed to provide a model against which agencies can develop their own architectures. Such a model architecture has yet to be developed.

3. e-Authentication Strategy

3.1 Introduction

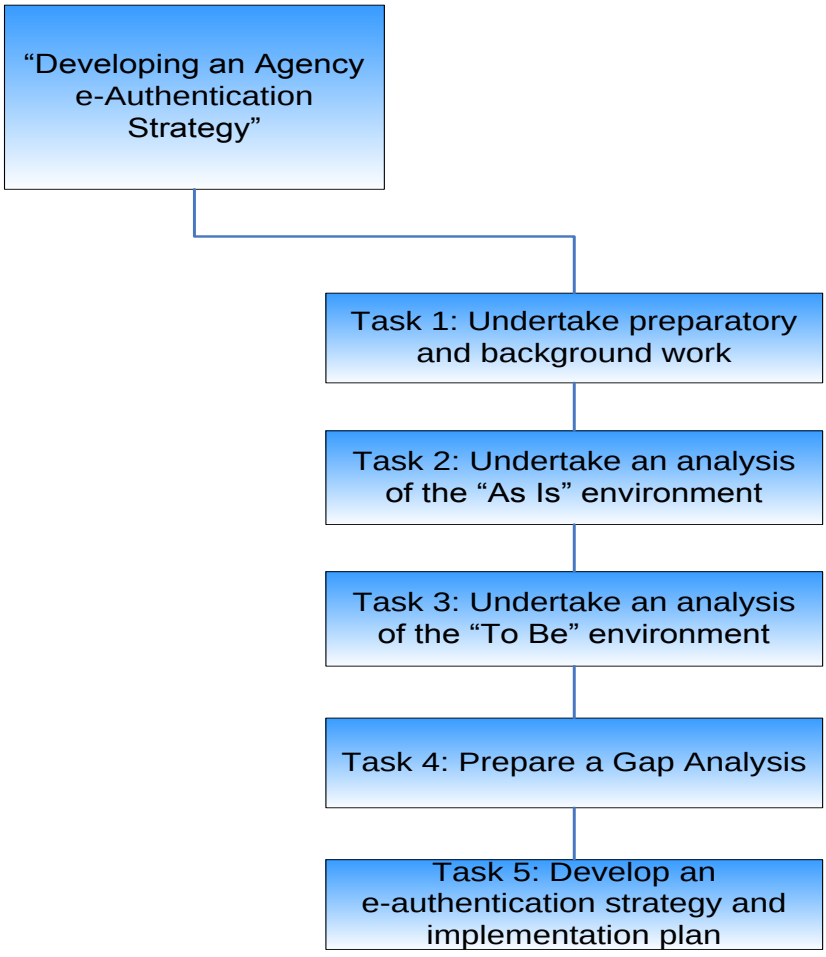
The goal of an e-Authentication strategy is to determine the short to medium term e-Authentication requirements of agency applications in order to allow for unified planning, development and deployment. This approach should minimise disruption, effort, cost and risk for users (individuals and businesses) and agencies. It will also focus on moving those services that most benefit stakeholders into an electronic environment.

This section provides a guide to the development of such a strategy.

3.2 Summary of strategy development process

Figure 4 below illustrates the task groups required in developing an e-authentication strategy.

Figure 4: Developing an e-Authentication strategy – all tasks



The approach to the preparation of an e-Authentication strategy follows the methodology frequently applied to organisational ICT strategies and involves five steps:

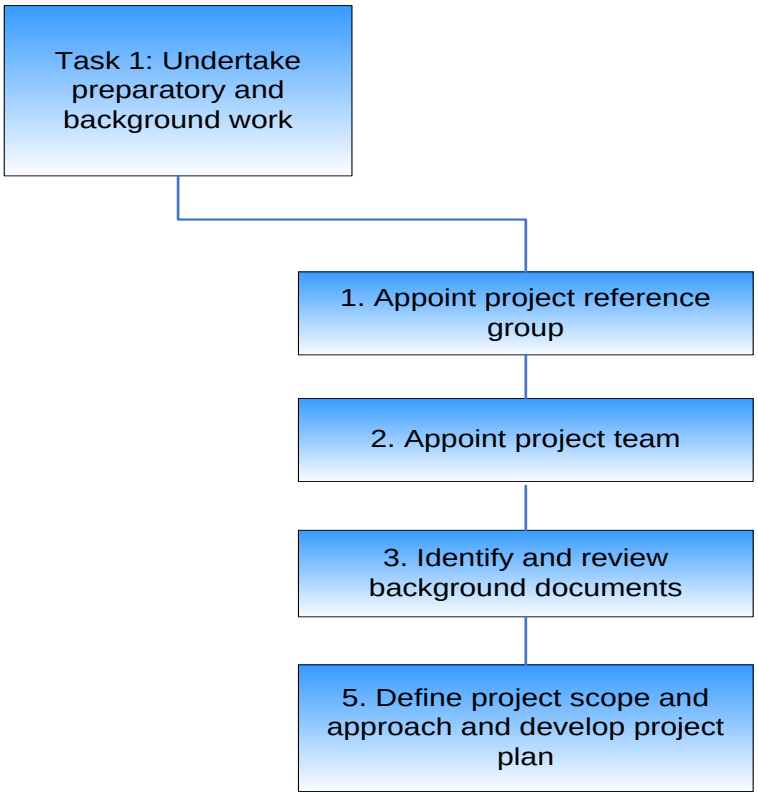
1. **Preparation:** Establishing project governance and the core project team. This step ensures that key participants familiarise themselves with core government and agency policy and strategy positions. Identify the business, technology, policy, legal and economic framework within which the e-Authentication strategy will be developed and tested.
2. **Analysis of the "As Is" environment.** Identify and analyse the existing state of core business services and the related ICT applications that most impact external stakeholders (individuals and businesses). Identify which applications would deliver most benefit to stakeholders if they were migrated into the electronic environment, including examination of key enabling ICT architectural and solutions capabilities, the current status of user registrations and any e-Authentication credentials that have either been issued by or which are accepted by the agency .
3. **Analysis of "To Be" environment.** Determine the e-Authentication requirements for core applications and external user groupings based upon application of the NeAF principles and processes.
4. **Gap analysis.** Identify the key gaps (and their magnitude) between the *As Is* and *To Be* positions for the core ICT applications for which electronic capabilities will be provided. Identify the required registration processes and e-Authentication solutions required to underpin and manage the envisaged e-Authentication scheme.
5. **Strategy development and implementation planning.**
    a. Identify a range of possible implementation models that will deliver the required applications, infrastructural and end-user capabilities required by the *To Be* position. This encompasses consideration of existing agency or external e-Authentication schemes. These may include multi-organisational collaborative e-Authentication schemes which should be evaluated based upon the benefit, cost and risk to the agency and the users.
    b. Prioritise implementation of e-Authentication based upon factors including degree of net positive impact for the agency and user, ICT and business priorities and existing commitments.

While the approach outlined below suggests that agencies consider all (but the most minor) actual and potential electronic transactions across all applicable (external individual and business) user bases, the scale of such an undertaking may be challenging, particularly for larger agencies. It is possible to take an application or application-cluster centric approach to determination of an e-Authentication strategy, without compromising the outcomes provided that the agency has well defined identity and access management policies and guidelines and architectural principles.

3.3 Task Group 1 – Preparation

Figure 5 below illustrates the key tasks involved in this stage.

Figure 5: Developing an e-Authentication strategy – Task 1



An outline of the key tasks is as follows:

1. **Appoint Project Reference Group**

This should encompass at least executives who have responsibility for:

- core external facing services
- ICT
- legal and privacy matters; and
- finance and administration

2. **Appoint Project Team**

This should include:

- senior representatives of business and technology owners/managers of core applications
- ICT security and enterprise risk management functions; and
- senior legal and privacy staff.

3. **Identify and review background documents**

Determine key government and agency policy positions that are relevant to the environment surrounding e-Authentication. This is likely to require the development of a synthesis of:

- core government information and ICT security policy positions security (eg PSM and ISM) and privacy assessment and management legal and policy positions

This document is currently under review by the Digital Transformation Office.

- NeAF policies and principles; and
- agency based documentation:
  - business strategies/plans and core policy planks
  - ICT strategic plan and development/maintenance schedule
  - ICT security policies (with guidelines and standards) where applicable
  - identity and access management plans, policies, guidelines
  - privacy management policies.

4. Define project scope and develop project plan

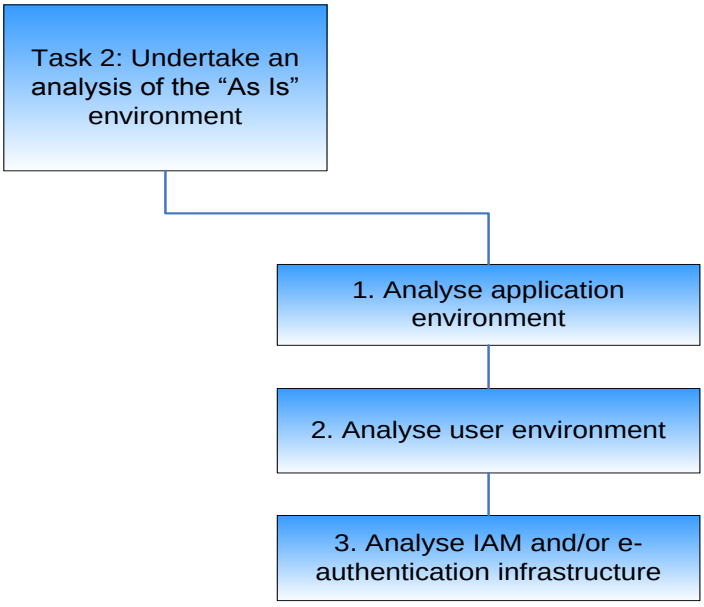
Given resource, time and budget constraints scoping may therefore be determined around key transactions undertaken by a particular group of users (e.g. intermediaries such as accountants or lawyers, or receivers of benefits from a particular assistance program).

A formal project plan and project resource schedule should be developed to ensure effective resource planning and management of expectations.

3.4 Task Group 2 – Analyse "As Is" Environment

Figure 6 below illustrates the key tasks involved in this stage.

Figure 6: Developing an e-Authentication strategy – Task 2



An outline of the key tasks is as follows:

1. Analyse application environment

- identify major applications for which electronic transactions are likely to be provided (based on scoping as above); and
- analyse external user registration, authentication and credential provision capabilities and identity/credential stores including how embedded/tightly coupled these capabilities are to the application.

2. **Analyse user user-groups environment**

- identify and stratify user (individuals and businesses) bases into logical clusters/groups and correlate these with the electronic applications identified in the previous step; and
- identify the status of existing user registrations with the agency and e-Authentication credentials that have either been issued by or which are accepted by the agency.

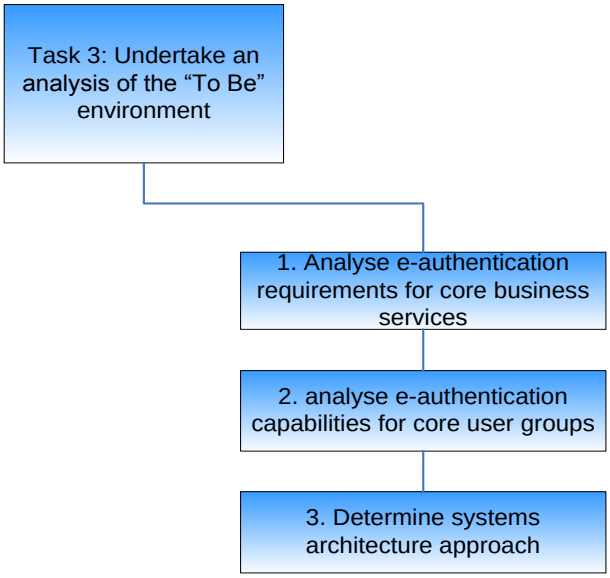
3. **Analyse infrastructure**

- Identity existing or planned IAM and/or e-Authentication solutions that are decoupled from applications.

3.5 Task Group 3 – Determine "To Be" Environment

Figure 7 below illustrates the key tasks involved in this stage.

Figure 7: Developing an e-Authentication strategy – Task 3



An outline of the key tasks is as follows:

1. **Conduct NeAF assessment of applications/transactions**

For major applications identified in Task Group 2 identify electronic transaction sets and conduct a NeAF assessment. This will reveal for each transaction the required:

- e-Authentication assurance level
- strength of registration
- strength of the e-Authentication mechanism; and
- credential management approach.

2. **Determine user groups e-Authentication capabilities**

Ascertain:

- whether user groups hold e-Authentication credentials from another 'trusted' agency, the strength of these relative to the e-Authentication assurance levels required by the agency's proposed applications, and whether such credentials have the possibility of being federated

This document is currently under review by the Digital Transformation Office.

- what suite of transactions will be required provide the necessary critical mass to encourage users to switch to the electronic environment; and
- the general level of ICT capability and maturity and Internet connectedness.

3. Determine user groups e-authentication capabilities

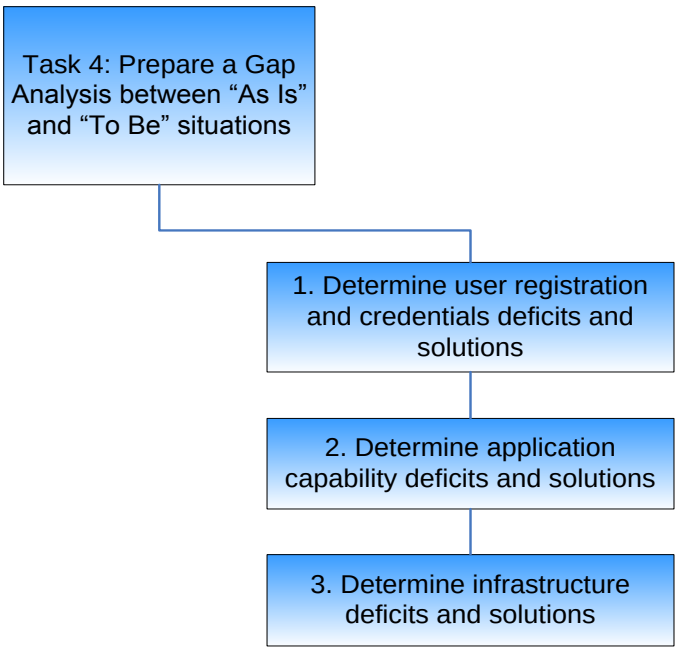
Develop an architectural model to efficiently and effectively manage the full e-Authentication lifecycle. Usually this will involve decoupling of e-Authentication functionality from applications, and its substitution with an infrastructural identity and access management solution that manages e-Authentication and first level permissions management on behalf of all or most applications. Such systems usually rely upon a unified store of identities, e-Authentication credential details and application permission rules.

3.6 Task Group 4 – Undertake a Gap Analysis

Based upon the comparison between the "*As Is"* and "*To Be"* positions, the agency should undertake a gap analysis. This analysis will deliver the 'to do' aspect of the e-authentication strategy.

Figure 8 below illustrates the key tasks involved in this stage.

Figure 8: Developing an e-Authentication strategy – Task 4



An outline of the key tasks is as follows:

1. Determine user registration and credentials deficits and solutions

For each user group determine an aggregated e-Authentication assurance level and from this determine:

- the new or additional registration processes that they will need to undergo. This will depend upon:
  - whether the users are already known customers to the agency and/or to another agency
  - the strength, currency and trustworthiness of the registration process.
- the new, refreshed or stepped-up e-authentication credentials they will need to be issued with.

This document is currently under review by the Digital Transformation Office.

2. Determine application capability deficits and solutions

For applications for which electronic transactions will be developed determine what actions will be required to support the infrastructure model identified in the previous steps. Necessary actions that may be identified include:

- cleansing of user identity stores and possibly linking to a central identity store
- re-engineering of applications to enable delegation of e-Authentication and possibly aspects of permissions management to an infrastructural solution; and
- modification of access control and other risk management facilities to address inherent strengths or weaknesses in the proposed e-Authentication solution approach.

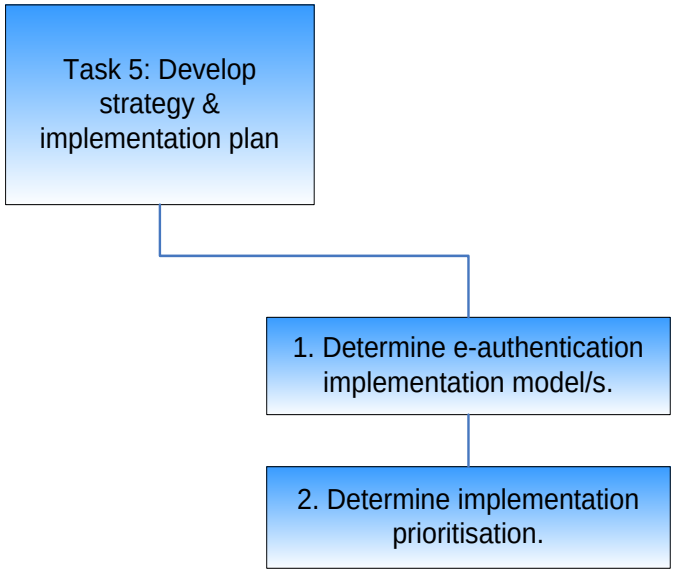
3. Determine e-authentication/IAM infrastructure capability deficits and solutions

For infrastructure it will be necessary to determine the acquisitions, development and changes necessary to provide the desired e-Authentication (or identity and access management) functionality.

3.7 Task Group 5 – Develop Implementation Strategies and Priorities

Figure 9 below illustrates the key tasks involved in this stage.

Figure 9: Developing an e-Authentication strategy – Task 5



An outline of the key tasks is as follows:

1. Determine Implementation Model(s)

Evaluate e-Authentication implementation and operational models (see Volume 2 of the NeAF Better Practice Guidelines).

The determination of possible implementation model(s) will be informed by:

- the service delivery model to e-Authentication model mapping described in section 6 of Volume 2 of the Better Practice Guidelines; and

- evaluation of the (whole-of-life) costs, benefits and risks of alternative models in relation to the agency and the user bases. The analysis of risks should particularly examine those related to individuals' privacy, security, continuity of service and agency legal liability.

2. Prioritise of development and deployment

This is likely to be heavily influenced by:

- demand from external users for electronic access to agency functions
- costs and benefits associated with the proposed online services
- maturity of online services capability of proposed users
- extent of existence of appropriately registered and credentialed user bases
- degree of difficulty, cost and risk associated with the required infrastructure enhancements and changes to application program environments
- suitability of agencies overarching information technology and telecommunications security capabilities; and
- status of agency application development, maintenance and replacement/refresh plans.

This document is currently under review by the Digital Transformation Office.

Appendix 1: Risk and Security Policies and Standards

Introduction

Appendices A and B of the Framework provide lists of laws, policies, standards and practices that agencies will need to consider in their application of NeAF.

The risk and security standards and policy positions provide guidance to agencies on how they should assess and address e-authentication threats and risks.

This section addresses the suggested positioning and relevance of the NeAF in relation to these key policies and standards, and vice versa.

Risk management

AS/NZS 4360

About

The Risk Management Standard AS/NZS 4360:2004[4] is intended to provide a "generic framework for establishing the context, identification, analysis, evaluation, treatment, monitoring and communication of risk". The treatment included in AS/NZS 4360 is intended to include all classes or risk including environment, business, personnel and premises, ICT.

The risk management process proposed by the standard is:

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

It stresses that risk management is an iterative process.

Positioning and relevance to NeAF

The majority of agencies use an AS/NZS 4360 based approach to identifying, analysing, treating etc risks including those applicable to the electronic applications which are the focus of NeAF.

NeAF does not seek to replace an AS/NZS 4360 based approach to risk management. This broader treatment of enterprise risks should continue. NeAF is interested in a small subset of risks, those applicable to e- Authentication.

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

This document is currently under review by the Digital Transformation Office.

Information security

AS/NZS ISO/IEC 27001:2005

About

ISO/IEC 27001:2005 represents the revision and redesignation of ISO/IEC 17799. In a similar vein, AS/NZS 27001:2005 represents the revision and redesignation of AS/NZS 7799. These standards provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). As such its focus is particularly on ICT, including the associated systems, people, processes and premises.

This standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. In particular, it describes best practice control objectives and controls in the following areas of information security management:

- security policy
- organisation of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity management; and
- compliance.

These control objectives and controls are intended to be implemented to meet the requirements identified by a risk assessment. The standard can be used in order to assess conformance by interested internal or external parties.

A range of related ISO/IEC standards are in place or under development including:

- ISO 27001:2005 – Information technology – Security techniques – - Specifications/Requirements
- ISO 27002:2005 – Information technology – Security techniques – Code of practice for information security management
- ISO 27004 (under development) – Information technology – Security techniques – Information security management measurements
- ISO 27005 (under development) – Information technology – Security techniques – Information Security Risk Management; and
- ISO 27006:2007 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.

Positioning and relevance to NeAF

The majority of agencies use AS/NZS 27001 (or AS/NZS 7799) as their common basis and practical guideline for developing organisational security standards and effective security management practices.

This document is currently under review by the Digital Transformation Office.

The resulting information security strategies, policies and practices require active consideration during the NeAF process in relation to:

- identifying other risk mediation solutions, other than e-Authentication; these will impact upon the e-Authentication assurance level
- determining the e-Authentication registration and credential approaches
- assessing the feasibility and suitability of the overarching e-Authentication solution.

Protective Security Manual

About

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

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

The PSM consists of eight parts:

- Part A – Protective security policy
- Part B – Guidelines on managing security risk
- Part C – Information security
- Part D – Personnel security
- Part E – Physical security
- Part F – Security framework for procurement
- Part G – Guidelines on security incidents and investigations
- Part H – Security guidelines on home-based work.

Positioning and relevance to NeAF

While compliance with the PSM is only mandatory for agencies of the Australian Government and other public and private sector organisations that hold national security classified information, aspects of it are being adapted and/or adopted by a range of State Governments.

The PSM applies to more than just information security, and therefore provides the broadest security or assurance context within which the NeAF is implemented.

Parts C and D are of particular significance to NeAF.

Part C sets up the classification system applied to both national and non-national security information. Under NeAF, as opposed to AGAF, agencies are required to take into account the security classification applicable to information that will be handled in the electronic transaction for which an e-Authentication approach is being sought.

Part D provides the framework and detailed policies and guidelines to be applied to vetting personnel who will have access to security classified information. This becomes relevant in determining the e-Authentication registration approach for certain categories of transaction that have an assurance level requirement of 4 (high) or above.

Australian Government Information and Communications Technology Security Manual – ISM

About

The Australian Government Information and Communications Technology Security Manual (ISM), produced by the Defence Signals Directorate (DSD), "represents the Australian Government recommended minimum security standard needed to secure Australian Government ICT systems."

ISM defines its positioning in relation to the PSM as follows:

> "The Commonwealth Protective Security Manual details the minimum standards for the protection of Australian Government resources (including information, personnel and assets) that agencies must meet in their operations.

This is complemented by the policies and guidance provided in this Australian Government Information and Communications Technology Manual which provides a framework to enable government to achieve an assured information and communications technology security environment."

In the latest iteration of ISM, DSD has adopted a "principles based approach to information security policy" and in particular those laid down by the Organisation for Economic Co-operation and Development (OECD) in section III of the OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*.

Positioning and relevance to NeAF

ISM is seen as being broadly applicable to Australian Government agencies and State and Territory agencies that hold or access national and non-national security information.

ISM provides coverage of all security matters associated with ICT. Its coverage of authentication in Chapter 6 of Part 3 is brief, and it is appropriate to see the detailed requirements of NeAF slotting in at this point.

Consideration of an agency's ISM based security frameworks, strategies and policies are essential in each of steps 2, 3 and 4 of the NeAF process.

Identity Security

AGAF relied significantly upon the EOI rules laid down under the AUSTRAC rules for identifying customers in the financial services sector. EOI requirements were described in relation to the number of points of identification required to meet registration assurance levels.

The development of the National Identity Security Strategy (see below) has modified governments' approaches to the determination of the strength of EOI. The NeAF requirements for EOI are based around this new framework.

National Identity Security Strategy

About

In 2007 the Australian and all State and Territory Governments agreed to the development of a National Identity Security Strategy (NISS). The NISS encompasses six elements that will provide a framework for strengthening national arrangements at each point along the identity security continuum.

These are:

- the Gold Standard Enrolment Framework (GSEF)
- security standards for proof-of-identity documents
- Gold Standard e-Authentication Requirements (GSAR)
- the national Document Verification Service (DVS)
- improving the integrity of identity data; and
- biometric interoperability.

Positioning and relevance to NeAF

The focus of the NISS is on is on ensuring applicants for Government documents that also may function as key documents for Proof of Identity (POI) [5] purposes are subject to a rigorous process of identification and verification. The implementation of the NISS will lead to strengthening of identity security in Australia which will benefit the integrity and robustness of electronic credentials issued under the NeAF.

The explicit positioning of the GSEF and GSAR are examined in detail below.

The positioning of other aspects of the NISS in relation to the NeAF is seen to be as follows:

- Wherever possible the DVS should be used to verify gold standard documents used as part of an EOI process for NeAF level 3 and 4 registration.
- Where applicable, electronic credentials should be produced and managed in accordance with the standards laid down by the *security standards for proof-of-identity documents* and *biometric interoperability* initiatives.
- The tenets of the *improving the integrity of identity data* initiative should be applied when developing an e-Authentication strategy and when devising e-Authentication solutions and schemes.

Gold Standard Enrolment Framework

About

The Gold Standard Enrolment Framework (GSEF) "specifies a premium, or "Gold Standard", approach for use by government agencies who enrol[6] individuals for the purpose of issuing government documents that also may function as key documents for POI purposes."

GSEF consists of:

- fourteen principles covering the areas of:
  - application of the Gold Standard
  - evidence used to identify the applicant
  - verification of POI credentials or information
  - interviewing the applicant
  - streamlined interaction after a Gold Standard enrolment
  - developments in technology

---

5 The NISS documents use the term "Proof of Identity" (POI). The NeAF (and Gatekeeper) use the term "Evidence of Identity" (EOI). The underlying meaning/definition of both is identical.

6 In this context the term "enrol" has the same meaning as the term "register".

- processes for Gold Standard enrolment; and
- exception conditions.

Attachment A to the GSEF is a Proof of Identity Framework that in effect replaces the previous AUSTRAC points based system for establishing evidence of identity and comprises:

- evidence of commencement of identity in Australia
- linkage between identity and person
- evidence of identity operating in the community; and
- evidence of residential address.

Positioning and relevance to NeAF

GSEF applies to the "enrolment of individuals for government documents that also may function as key documents for POI purposes" e.g. passport, driver's licence. As such the GSEF (and associated GSAR) represent a special case implementation of the NeAF.

NeAF is focused on electronic credentials provided to individuals that are used for electronic authentication purposes. These credentials will not in themselves function as key documents for EOI purposes. As a result, the GSEF is not mandatory for NeAF registration/enrolment processes, but:

- agencies will need to adopt a GSEF EOI framework (as per Appendix A to GSEF) in place of the former AUSTRAC points-based framework
- POI documents issued under GSEF may be regarded as being 'strong' and are therefore highly suitable for inclusion in the strong registration processes required by AGAF level 3 and above; and
- electronic identity 'documents may be issued under GSEF – e.g. e-passport, smart-card based driver license etc – which agencies may choose to use as an e-authentication credential for online access. See GSAR for further information.

Gold Standard Authentication Requirements

About

The Gold Standard Authentication Requirements (GSAR) is concerned with ensuring that "the person that an agency deals with is indeed the same person who originally registered for the service". GSAR is concerned with both physical and electronic authentication to suit the range of government service delivery channels.

Positioning and relevance to NeAF

The GSAR provides a "gold standard approach to electronic authentication" which should be applied "by government agencies where:

- the identity of an individual engaging in a transaction needs to be authenticated, and the authentication process is either wholly electronic or supported electronically
- an electronic credential issued as an output from the Gold Standard Enrolment Framework (GSEF) is employed in that authentication process; and
- the risks associated with the transaction require level 4 (high) assurance under the Australian Government e-Authentication Framework (AGAF)."

GSAR does not replace or supplant the NeAF. It provides directives regarding how GSEF credentials should be used within an e-Authentication environment.

The restrictions placed on the use of GSEF credentials for lower assurance levels (e.g. minimal and low) transactions and the retention of authentication audit trails should be noted. The former restricts agencies from issuing (or federating) a single credential to users that could be used for all levels of

interaction with that agency. The latter may impact on agency security/audit probity requirements that usually require retention of detailed records relating to electronic access to agency systems.

Gatekeeper EOI Policy

About

The Gatekeeper EOI Policy was revised and reissued in 2007 to bring it into line with the NISS POI framework and to formalise an extended set of registration models.

The new policy provides four models for individual and organisational registration:

- relationship model
- known customer model
- threat and risk assessment model; and
- formal identity verification model.

Positioning and relevance to NeAF

While the Gatekeeper framework is focused on PKI-based credentials which apply to NeAF assurance levels 3 and 4, the NeAF has adopted, more generally, its models and the EOI requirements.

Appendix 2: IAM Implementation Considerations

Assessing Identity and Access Management Maturity

Agencies' IAM maturity can be determined by examining a range of strategic and operational factors.

Strategic maturity is determined by whether the agency has appropriate:

- IAM strategy and implementation plan
- IAM architecture and systems migration strategy
- information and asset management strategy
- IAM governance framework
- comprehensive IAM policies
- IAM product and services strategy
- IAM standards and best practice; and
- appropriate skills and funding to operate, develop and remediate IAM environment.

Operational maturity is determined by whether the agency has:

- unified approach to IAM covering internal and external 'users' and physical and systems access
- information and asset management
- authoritative source of identity data
- rationalised IAM architecture
- automated provisioning and de-provisioning environment.
- compliance with the NeAF; and
- shared/federated authentication.

Longer Term Identity and Access Management Planning

The movement from agency "*As Is"* IAM positions to the "*To Be"* position outlined by this IAM framework will inevitably be a gradual and incremental process. The steps outlined below provide a series of tasks that agencies should plan into all appropriate projects and ongoing maintenance and operational activities.

Uncover/Analyse Existing Identity & Access Management Components

Agencies that do not have a mature approach to identity and access management will need to undertake an appropriate discovery and analysis process to determine their current capability in relation to all:

- identity stores/directories in use (including clarification of their key purposes)

This document is currently under review by the Digital Transformation Office.

- internal and external identities currently in place, and their associated authentication credentials and access permissions
- processes and policies/practices associated with entity identification, hiring/firing and contracting
- types of roles entities perform when using the business unit's applications and the permissions, authorities and delegations associated with such roles
- existing authentication policies/practices and processes
- enterprise risk management and information security management plans and policies; and
- formal enterprise-wide plans to move to federated identity and access management.

Without this baseline agencies will not be able to plan their migration to an aggregated/federated model.

A matrix of entity groups against the applications they access, or even application transactions they execute, broken down by assurance level and strength of registration and authentication is considered a critical requirement to inform decision-making.

Harmonise, Rationalise and Unify Components

IAM policies and processes need to be analysed to see where they can be rationalised, harmonised, and made consistent with the whole of agency or whole-of-government (or sector) approach as appropriate.

Aggregate and Centralise Components

As part of the above, opportunities to aggregate and centralise multiple identity and access management solution components should be explored. This may:

- improve the integrity of identity and access management by removing redundancy of data and rules; and
- reduce technology and process costs.

The information uncovered through the steps above should reveal opportunities for rationalising and centralising identity stores/directories, authentication solutions, and other aspects of access control (e.g. application level access).

Architect (a more aggregated/federated) solution

It will be necessary to examine the business (e.g. governance) and technology aspects of the agency's enterprise architecture in order to develop new business processes for identity and access management.

The analysis undertaken in the previous steps above will provide the basis for determining the scope of this undertaking and the migration strategy.

Justify, Budget and Plan

To implement the enhanced approach to identity and access management, business units will need to develop a project plan and business case. This will need to include:

- capital and operating budgets
- evaluation of service provision alternatives (e.g. shared services)
- the cost of transition to the new approach including systems re-engineering, data cleansing, and education and training; and
- a detailed project plan with key milestones.

This will be driven by information from the previous steps.

Cleanse Existing Identity and Access Management Components

As part of the implementation of a 'new' identity and access management approach business units will have to cleanse identity, authentication and access stores to remove invalid entities and access permissions and rationalise multiple (redundant) identities into one identity (e.g. using single identifiers).

This will necessarily involve application owners and custodians, and the entities themselves.

Educate and Train

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

- executives
- line managers
- all other staff and contractors
- external entities
- technical staff; and
- security staff.

Training will need to cover (as appropriate):

- the changes to identity and access management policies
- the revised identity and access management processes
- any change in legal and contractual positions; and
- any new provisioning, or de-provisioning processes and, possibly, new identity and access management solutions.

Authorise New Responsibilities

As part of implementing the new identity and access management regime it will be necessary for business units to:

- appoint/re-affirm application owners; and
- determine roles and responsibilities of staff in relation to maintenance of identities and application access permissions.

Implement for the Highest Priority Applications and Evolve Towards the Final Solution

As the 'remediation' of agencies' identity and access management environments will inevitably be a long term exercise, the achievement of incremental benefits is essential. This will require business units to focus on major applications and entity bases before addressing lesser applications and entity bases. One approach an agency may adopt is to:

- create aggregated identity stores for staff at a agency level and, where appropriate link into whole-of-government identity stores to identify/authenticate other intra-agencies within the same government
- create aggregated identity stores for external entities at an agency level
- move towards simplified log-in and then single log-in for internal and then external entities (the latter would probably require usage of a shared service approach).

Business units will need to test the efficacy of implementations of each of the above and measure and report on progress to agency management.

This document is currently under review by the Digital Transformation Office.

Track, monitor, intervene, report, audit

Business units will need to install comprehensive facilities to:

- track and, where required, report upon provisioning and de-provisioning of all identities and authentication credentials. The intention is to enable:
  - authorising parties to regularly review applications and/or entities for which they are responsible
  - unusual activity patterns and attempted breaches to be detected
  - appropriate reporting to be provided to the agency executive.
- provide ongoing measurement of the maturity of strategy and operations.

Learn & Improve

Business unit management will need to ensure that processes are in place to continually review, learn from and improve identity and access management approaches.

Appendix 3: Reference Documents

Reference Document/Source	Source and/or URL (where available)
Protective Security Manual	Australian Government Attorney-General's Department
Australian Government Information and Communications Technology Security Manual – ISM	Defence Signals Directorate http://www.dsd.gov.au/library/infosec/ism.html
National Identity Security Strategy including GSEF and GSAR	Australian Government Attorney-General's Department http://www.ag.gov.au/
Gatekeeper EOI policy	Australian Government Information Management Office http://www.gatekeeper.gov.au
AS/NZS 4360 – Risk Management Standard	Standards Australia
AS/NZS ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements	Standards Australia
ISO 27002:2005 – Information technology – Security techniques – Code of practice for information security management ISO 27004 (under development) – Information technology – Security techniques – Information security management measurements ISO 27006:2007 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems	ISO/IEC