Australian Government

Digital Transformation Office

National e-Authentication Framework

Management Summary

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

© Commonwealth of Australia 2009

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth.

Requests and inquiries concerning reproduction and rights should be addressed to the:

Commonwealth Copyright Administration,
Attorney General's Department,
Robert Garran Offices,
National Circuit,
Barton ACT 2600

or posted at http://www.ag.gov.au/cca

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Copyright: Department of Finance and Deregulation

Foreword

Australian citizens and businesses are increasingly conducting a wide range of transactions with government agencies using various delivery channels, including the internet and phone-based services. These transactions include obtaining general information, making applications and payments, lodging reports, receiving benefits, lodging tenders and providing services for government. As online transactions increase in frequency and significance, the risks associated with such transactions, particularly risks relating to identity can also increase.

The Department of Finance and Deregulation through the Australian Government Information Management Office (AGIMO) has developed the National Authentication Framework (NeAF) to provide a consistent, whole-of-government approach to managing identity related risks.

The NeAF combines two earlier publications – the Australian Government e-Authentication Frameworks for Business and Individuals into a single, coherent approach to the challenge of providing assurance to agencies as to the identity of parties with whom they are transacting.

In addition, the NeAF addresses the important issue of individuals and businesses being able to authenticate government websites with which they interact.

The Framework recognises and accommodates sectoral and whole of government initiatives through the re-use of existing authentication credentials and consideration of a variety of identity management frameworks as alternatives to traditional agency specific models.

Adoption of the NeAF across all tiers of government will minimise duplication of effort and achieve consistency of authentication approaches within and across jurisdictional boundaries, thereby

- maximising the efficiency and effectiveness of electronic service delivery by Australian government jurisdictions; and
- providing scope for reducing the costs to the community of interacting electronically with government.

The Framework is endorsed by the Australian Online and Communications Council (OCC) which operates as the peak ministerial forum across Australia on strategic approaches to information and communications technology issues. Membership includes senior ministers from state and territory governments and the President of the Australian Local Government Association (ALGA).

In endorsing the Framework, the Council agreed that jurisdictions will:

- comply with the principles of the National e-Authentication Framework; and
- accept and adopt as appropriate the Better Practice Guidelines as a means of providing greater consistency in the development and implementation of e-Authentication solutions across jurisdictions.

Ann Steward

Australian Government Chief Information Officer

Contents

Figures

Tables

Executive Summary

The National e-Authentication Framework (NeAF) replaces the Australian Government Authentication Frameworks for Business and Individuals (AGAF-B and AGAF-I). It has been developed as a national framework, addressing the needs of Commonwealth, State, Territory and local government agencies.

The NeAF is a better-practice framework intended to be adopted in a consistent manner by agencies, jurisdictions and sectors. Consistent application of the principles and elements of the Framework will facilitate the provision of fit for purpose authentication solutions thereby maximising the benefits both to agencies and the broader community.

In providing guidance on current and emerging models for the implementation of e-Authentication across agencies, jurisdictions and sectors the Framework supports the range of current initiatives to support connected government.

The scope of NeAF covers two aspects of authentication:

- electronic authentication of the identity of individuals and businesses; and
- authentication of government websites.

Central to the Framework is the concept of assurance levels. An assurance level is determined through a comprehensive risk assessment process that determines the severity of the impact of getting e-Authentication wrong. While the Framework notes that e-Authentication is one of the possible risk mitigation solutions that can be adopted to address identity related risks its focus is on answering the question:

> Do we have the correct party at the other end of the line – i.e. are they who they purport to be?

Implementation of e-Authentication solutions does not occur in isolation from other strategies and policy frameworks (both agency specific and “whole of government”) including agency identity and access management strategies, information and knowledge management strategies, information security policies, privacy management policies and systems development lifecycles.

To determine an agency’s assurance level and authentication requirements, the NeAF provides:

- principles to be applied by agencies in determining and implementing e-Authentication approaches
- a standardised set of (five) e-Authentication assurance levels and a recommended set of criteria for determining the level of assurance required for a particular e-transaction
- a standardised approach to determining the e-Authentication solution required to satisfy the e-Authentication assurance level; and
- a standardised approach to validating the e-Authentication approach selected.

1. Introduction and scope

Vision

A trusted electronic environment where the community can transact easily and securely with government.

1.1 Introduction

Electronic interactions between governments and individuals and businesses require that each party has confidence in the authenticity (of e.g. identity) and in some cases authority (e.g. position, role) of the other party.

Electronic authentication is the process that delivers (a level of) assurance of an assertion made by one party to another in an electronic environment. The National e-Authentication Framework (NeAF), which replaces the Australian Government Authentication Frameworks for Business and Individuals (AGAF-B and AGAF-I), is primarily concerned with the electronic authentication of identity of individuals and businesses. Other assertions include role, delegation and value.

e-Authentication is accomplished using something the user knows (e.g. password, secret questions and answers), something the user has (e.g. security token) or something the user is (e.g. biometric) or a combination of these.

1.2 Objectives

The objectives of the Framework are to:

- ensure that e-Authentication approaches are balanced between the underlying identity related transaction risk and the need for ease of use and affordability
- enhance community confidence in electronic dealings with government agencies
- provide consistency in e-Authentication approaches across agencies, jurisdictions and sectors to increase efficiency and enable:
  - reuse of credentials by the community where appropriate
  - sharing of infrastructure and solutions by agencies
  - extensibility of authentication schemes
  - increased trust in authentication and registration mechanisms
- provide agencies with the tools to determine the level of e-Authentication required and the related solution approaches; and
- ensure that due diligence is applied when determining e-Authentication approaches.

1.3 Scope

The scope of the NeAF encompasses:

- electronic authentication of the identity of individuals and businesses
- authentication of government websites.

The NeAF comprises:

- principles to be applied by agencies in determining and implementing e-Authentication approaches
- a standardised set of e-Authentication assurance levels and a recommended set of criteria for determining the level of assurance required for a particular e-transaction
- a standardised approach to determining the e-Authentication solution required to satisfy the e-Authentication assurance level; and
- a standardised five stage process to determine the strength of e-Authentication required and the e-Authentication approach to be adopted.

The NeAF also provides guidance on models for the implementation of e-Authentication solutions and planning standards for website authentication.

2. Principles and concepts

The implementation of NeAF requires an appreciation of:

- the key principles that are intended to guide an agency's application of NeAF; and
- the concepts of:
  - 'assurance levels' which represents the required degree of confidence of 'getting authentication right' as determined by the threats and risks associated with a transaction and the reciprocal level of robustness of the e-Authentication solution
  - e-Authentication solution components
  - e-Authentication implementation models.

2.1 Principles

The key principles that underpin the application of the NeAF by agencies are:

Transparency

e-Authentication decisions are made in an open and understandable manner involving consultation with relevant stakeholders.

Risk management

Selection of e-Authentication mechanisms is guided by the likelihood and consequences of identified threats being realised. These risks are articulated as part of the development and justification of e-Authentication mechanisms.

Consistency

A consistent approach to selecting e-Authentication mechanisms is applied by agencies and as a result, individuals and businesses can expect similar e-Authentication processes for transactions with equivalent assurance levels offered by different government agencies.

Interoperability

e-Authentication mechanisms are deployed in a way that facilitate interoperability and comply with relevant standards.

Responsiveness and accountability

Agencies respond to individuals' and business' needs and provide guidance on use of their electronic services and provide dispute handling processes. Agencies are accountable for determining and addressing agency-specific issues related to the e-Authentication approach adopted (e.g. liability).

Trust and confidence

The mechanisms used support electronic services and enable a balance between usefulness and security for government and individuals/businesses.

Privacy

Personal information is collected, used and disclosed in accordance with privacy laws or schemes in each jurisdiction.

Choice

When interacting electronically, individuals and businesses are able to use one or more electronic credentials to access services across multiple organisations.

Flexibility

Agencies support a range of fit for purpose e-Authentication approaches aligned to assurance requirements.

Cost effectiveness and convenience

e-Authentication processes are as seamless and simple as possible. Where appropriate, solutions that enable individuals and businesses to re-use existing e-Authentication credentials are adopted.

2.2 Concepts

These matters are discussed in greater detail in the Framework and in Volume 1 of the Better Practice Guidelines.

2.2.1 Assurance levels

NeAF provides for five levels of assurance (0 through 4).

The determination of the level of assurance (of e-Authentication) is based upon the application of long standing risk management and ICT security standards and policies[1].

These require the determination of the impacts of getting e-Authentication 'wrong'. This requires evaluation of:

- the nature of threats and associated risks e.g. inconvenience, financial loss and privacy and personal safety breaches
- the likely 'threat impact' calculated by multiplying the probability of occurrence. The probability is increased or reduced by taking into account risk mitigation factors other than e-Authentication.

The relationship between severity of 'threat impact' and the level of e-Authentication assurance required is illustrated in Table 1 below.

Table 1 NeAF Assurance levels

Threat impact	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Required e-Authentication assurance level	Level 0 – Null	Level 1 – Minimal	Level 2 – Low	Level 3 – Moderate	Level 4 – High

2.2.2 e-Authentication solution components

The components of e-Authentication solutions that determine their capacity to meet the assurance levels required for a transaction/s are, as illustrated in

[1] These include: AS/NZS 4360 – Risk Management Standard; ISM – Australian Government Information and Communications Technology Security Manual; Australian Government Protective Security Manual (PSM).

Table 2 below:

- the strength of the approach taken to register users
- the inherent strength of the authentication credential
- the robustness of the life-cycle management processes applied to the credential including agency information security practices.

Table 2 e-Authentication solution components

Strength of Registration					
4		Minimal	Low	Moderate	High
3		Minimal	Low	Moderate	Moderate
2		Minimal	Low	Low	Low
1		Minimal	Minimal	Minimal	Minimal
0	Null (0)	Pseudonymous Minimal	Pseudonymous Low	Pseudonymous Moderate	Pseudonymous High
	0	1	2	3	4

Strength of Authentication Mechanism

2.2.3 e-Authentication implementation models

The application of the NeAF principles across government is intended to result in the broad alignment of e-Authentication approaches.

Consistency of approach and implementation will open up opportunities for cross agency e-Authentication “schemes” to provide more convenient outcomes for individuals and businesses and more effective utilisation of resources by participating agencies.

The implementation contexts that influence the selection of e-Authentication models include:

- **Siloed** whereby agencies act in isolation on either an enterprise or application basis.
- **Sectoral (national and jurisdictional)** whereby industry sectors offer focused services on a sectoral level, crossing agency, jurisdictional and potentially private-public sector boundaries to provide users with a seamless interaction within the focus area.
- **Whole of government (portals for citizens and businesses)** whereby governments offer one or more portals or common access points to a range of government services with the intent of enabling users to readily access services largely transparently to the organisational distribution of these services within and across government agencies.
- **Agency clusters** whereby agencies with similar user bases provide portal based access and potentially work together to create a number of linked and interdependent workflows to support end user information or transactional needs.

There are a range of possible e-Authentication implementation models (see Better Practice Guideline Volume 3) to fit the above:

- **Siloed** where agencies implement and manage their own e-Authentication solutions.
- **Centralised** where multiple agencies utilise a general purpose e-Authentication service.
- **Federated** which allows for the portability of identity information across otherwise autonomous security domains. A variety of federated e-Authentication models are possible.

3. Identity e-Authentication Planning

The implementation of e-Authentication must factor in pre-existing strategies and frameworks, and should, in turn, be encompassed within agencies' systems development lifecycles.

These matters are discussed in greater detail in Volume 4 of the Better Practice Guidelines.

3.1 Identity and access management framework

An Identity and Access Management (IAM) framework integrates those factors required to control access by all classes of users to information (and some physical) resources as set out in Figure 1 below.

Figure 1 Identity and Access Management Framework

Identity and Access Management Policy				
Entity Management	Resource Management	Authentication Management	Access Management	Governance and Operations
Architecture, Standards and Guidelines				

3.2 e-Authentication strategy

Agencies should develop a strategic approach to e-Authentication to underpin the adoption of e-Authentication approaches that are consistent with the NeAF. Formulation of an e-Authentication strategy is primarily intended to develop a holistic view of all major transaction types and user bases and of the agency's e-Authentication requirements and probable e-Authentication approaches.

3.3 Privacy

Each agency must handle personal information as required by the applicable Commonwealth, state or territory privacy laws or schemes.

3.4 Systems architecture and systems development lifecycle

e-Authentication needs to be factored into agency systems development initiatives as well as into the periodic reviews of systems architectures undertaken by agencies. These activities should reference the e-Authentication strategy referred to in section 3.2 above to determine future e-Authentication requirements.

4. NeAF methodology

The Framework sets out a seven step process. The process is not linear. Rather, it is an iterative process and should be undertaken in the context of the agency's wider information security risk management processes.

The Framework recognises that a range of solutions (e.g. technology or business process based) may be in place that will mitigate identity related risk. However, where an agency determines that issuance of an authentication credential is an appropriate part of the solution to mitigate identity-related risk, the Framework provides guidance in relation to credential selection and management.

The Framework steps are:

1. Determine the business requirements

This includes identification of the electronic services to be provided, the target user base/s, the electronic delivery channels to be used, the assertions to authenticated, and privacy and public policy implications. This step also requires the identification of applicable whole of government information management and ICT security frameworks.

2. Determine assurance level requirements

This encompasses a comprehensive and multi-dimensional threat-risk assessment of identity related risks is used to determine an assurance level for a transaction (or transaction set).

3. Select the registration approach

This covers verification of the Subscriber's identity[2] to the required assurance level (as determined in step 2) prior to creating an e-Authentication credential.

4. Select the e-Authentication mechanism

This encompasses determining a combination of an authentication credential (e.g. password, biometric, digital certificate) and the credential lifecycle management system (issuance, activation, de-activation etc) that meets the required assurance level (as determined in step 2). Consideration should be given to re-use of credentials.

5. Select an implementation model

This covers selection of an approach to implementation designed to maximise usability and reduce cost and effort. Models include siloed (agency-specific), federated, and centralised. The use of trust services such as VANguard should also be considered.

6. Assess the business case and feasibility of the implementation model

This involves using *ICT Business Case Guide and Tools* to model costs and benefits to financially justify the implementation of the e-Authentication approach.

7. Review the e-Authentication solution

This encompasses validation the overall e-Authentication approach against Principles described in section 2.1.

[2] While the NeAF focuses on identity assertions a registration process can equally be used to verify other attributes such as role or position.

5. Authentication of government websites

5.1 Rationale

Authentication of government websites will increase trust levels for individuals and businesses in their on-line dealings with government. Stronger website authentication can reduce scope for attacks and reduce the incidence of identity theft, privacy breaches, fraud, contract disputes, unauthorised disclosure, and modification of information. Attacks on authentic web site content or web server files can lead to reduced confidence in the integrity of government information and reduce the effectiveness of online information initiatives.

For individuals and businesses, the level of assurance that can be placed in the authenticity of agency websites is dependent upon:

- user awareness and ongoing vigilance
- the robustness of agency website e-Authentication facilities; and
- associated agency detection and prevention initiatives that are aimed at reducing reliance on user involvement.

5.2 Planning principles for website authentication

A summary of the key principles to be applied to website authentication are:

- **Web server authentication** – a user should authenticate a government web site/server
- **User involvement in web site authentication** – user education is essential together with agency detection/prevention initiatives
- **Mutual authentication** – web site authentication should integrate with user authentication especially for higher assurance level applications
- **User credentials** – user credentials should be fit-for-purpose for the web site application
- **Web site credentials** – these need to provide base line security capabilities
- **Authentication techniques** – website authentication credential should be fit-for-purpose
- **Trusted channels** – trusted user interfaces should be provided
- **Client-side active content** – risks and benefits should be carefully assessed
- **Web site content** – content should be formally justified, accurate and current.

Full detail is provided in Better Practice Guidelines Volume 2.

6. Roles and responsibilities

Technical solutions alone will generally not be enough to satisfy practical e-Authentication requirements. e-Authentication necessarily involves management, business processes and cultural issues. Any e-Authentication solution will need to be supported by procedures that clearly define the responsibilities of the individual entities conducting online transactions.

6.1 Government roles and responsibilities

The Framework specifies a range of matters to which agencies should give due consideration including:

- considering the needs and expectations of individuals and businesses
- providing appropriate education and awareness services to end users
- providing leadership in e-Authentication practices
- delivering efficient and useful services online
- ensuring continuing reliability and quality of services.

6.2 Business and Citizens roles and responsibilities

Obligations of businesses and individuals interacting electronically with government will usually be set out in an agency’s terms and conditions and could include:

- provision of accurate evidence of identity and evidence of relationship information
- maintenance of the security of the credentials that are issued; and
- use of the credentials only for the purposes they are issued.