Australian Government

Digital Transformation Office

National e-Authentication Framework

Executive 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

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Vision

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

Introduction

The Australian Government in its 2006 *e-Government Strategy, Responsive Government: A New Service Agenda* stated that:

> *"Through effective use of technology, the government will improve its structures and processes. Online, electronic and voice-based services will be fully integrated into government service delivery. Electronic delivery will underpin all other delivery channels, ensuring a consistent base to all activities and providing consistent service no matter how government is approached."*

The business conducted over these channels ranges from providing general information to users of government services, receiving applications and payments to accepting the lodgement of reports and tenders and providing benefits to citizens and businesses.

Frequently these transactions require that each party has confidence in the identity, and in some cases the authority, of the other party. Without this assurance unauthorised transactions may be executed, sensitive information may be released to unauthorised personnel or individuals or businesses may be subject to fraudulent activity by web sites masquerading as legitimate government entities.

The ***National e-Authentication Framework*** (NeAF) will assist agencies, jurisdictions and sectors in ***authenticating the identity*** of the other party to a desired level of assurance or confidence. The NeAF encompasses the electronic authentication (e-Authentication) of the identity of individuals and businesses dealing with the government, on one side of the transaction, as well as the authentication of government websites on the other side. The NeAF positions e-Authentication within the broader context of an agency's approach to identity and risk management and provides guidance on developing the processes and technology required to provide the desired level of confidence.

e-Authentication is effectively 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.

While the Framework supports an agency-specific model where each agency develops its own, separate, technology solution, it recognises and accommodates broader sectoral and whole of government e-Authentication initiatives. These are supported through the re-use of existing authentication credentials and consideration of a variety of identity management frameworks. 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. This will maximise the efficiency and effectiveness of electronic service delivery by Australian government jurisdictions as well as 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, which operates as the peak ministerial forum across Australia on strategic approaches to information and communications technology issues.

Objectives

There are five key objectives of the NeAF:

1. to ensure that approaches to e-Authentication of identity balance the ***underlying risk*** with the need for ***ease of use*** on behalf of both parties
2. to enhance ***community confidence*** in electronic dealings with government agencies
3. to provide ***consistency in government processes*** for e-Authentication of identity in order to increase efficiency and maximise the ease-of-use for all parties involved
4. to provide government agencies with the ***tools to determine the most appropriate approach*** to the e-Authentication of identity; and
5. to ensure that ***due diligence is applied*** when determining these authentication approaches.

Structure

The NeAF comprises a set of ***principles***, a standardised set of ***assurance levels***, and a standardised ***approach and process*** for determining assurance levels and related e-Authentication solutions. It provides guidance on **models** for the implementation of e-Authentication solutions and planning standards for **website authentication**.

Principles

The NeAF identifies a set of key principles that are to be applied by government agencies as they develop systems for e-Authentication. These principles are:

1. ensure transparency for all parties
2. take a standard approach to risk management
3. strive for consistency across government agencies
4. maximise the interoperability between different systems
5. be responsive and accountable to end-users
6. balance trust, security and ease of use
7. respect the privacy of all individuals
8. provide end-users with an appropriate choice of authentication mechanisms
9. be flexible in supporting a range of approaches to electronic authentication
10. ensure solutions are both cost effective and convenient.

e-Authentication Assurance Levels and Solutions

e-Authentication represents the process that delivers (a level of) assurance of the assertion of identity made by a user. The level of assurance required will be dependent upon the level of risk[1] associated with the transactions that the user will undertake, and the mitigating factors, other than e-Authentication that will reduce this risk. A range of assurance levels are possible. In NeAF five assurance levels are prescribed, calibrated from minimal through high.

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

Table 1 Threat Impact and Authentication Assurance

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

Achieving the required assurance level for the e-Authentication solution is then a function of the strength of the registration and enrolment processes on the one hand, and the strength of the user's e-Authentication credential (e.g. userid+password, biometric) and its on-going management on the other. This is illustrated below in Table 2.

Table 2 Identity Authentication Assurance Matrix

Strength of Registration	Strength of Authentication Mechanism: 0	1	2	3	4
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

[1] The level of risk derives from the impact of a threat, and the likelihood of its occurrence. Impact has two dimensions: severity and extent. Severity measures the impact of a single instance (e.g. financial loss, inconvenience, embarrassment, injury, death), while extent measures the number of probable instances (e.g. single user/client versus all users/clients).

Methodology

The Framework identifies a seven-step process for assessing the strength of authentication demanded by the transaction, the technology components that will provide the desired authentication strength, and the business processes that are required to achieve this level of authentication.

This is an iterative process that takes into account existing controls, the possible consequences of incorrectly authenticating the parties to the transaction and the likelihood of these consequences eventuating. The process is undertaken in the context of the agency's wider information security risk management processes.

The Framework requires that the agency:

- Identify the requirements of the electronic service that is to be delivered, the nature of the user base/s, the desired electronic delivery channel/s, and the specific details that are to be authenticated as well as the privacy and policy implications of the process.
- Ascertain the assurance level requirements by undertaking a comprehensive analysis of the threats and risks associated with the transaction.
- Determine the most appropriate means to register the client of the service including collection and/or verification identity or other information.
- Select the mechanism for authenticating the end-user identity (or other attribute) and the processes that must be applied to assure integrity and robustness throughout its lifecycle.
- Determine the most appropriate e-Authentication implementation model, including assessing the re-use of existing systems and processes.
- Assess the business case and feasibility of the implementation model.
- Review the e-Authentication solution to ensure that the key principles have been addressed and the overall costs and benefits to the agency and its client groups understood and managed.

Roles and responsibilities

Technical solutions alone will generally not be enough to satisfy practical

e-Authentication requirements. e-Authentication also 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.

The NeAF 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; and
- ensuring continuing reliability and quality of services.

The NeAF also considers the obligations of businesses and individuals interacting electronically with government. These will usually be set out in an agency's terms and conditions and would include:

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