Australian Government
Department of Finance and Deregulation
Australian Government Information Management Office

National e-Authentication Framework

January 2009

National e-Authentication Framework

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

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 are made to obtain general information, make applications and payments, lodge reports, receive benefits, lodge tenders and provide services for government. As online transactions increase in frequency and significance, the risks associated with such transactions – particularly risks relating to identity – may also increase.

The Australian Government Information Management Office (AGIMO) of the Department of Finance and Deregulation 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 Framework for Business and Australian Government e-Authentication Framework for Individuals (AGAF-B and AGAF-I) – into a single, coherent approach to the challenge of providing assurance to agencies as to the identity of parties with whom they are transacting.

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

The NeAF 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 NeAF 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). The OCC meets annually to discuss policy issues relating to the information economy with a focus on online and communications issues.

In endorsing the NeAF, the OCC agreed that jurisdictions will:

- comply with the principles of the National e-Authentication Framework
- 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

Table of contents

List of Figures

List of Tables

List of Acronyms

AGAF	Australian Government e-Authentication Framework
AGAF-B	Australian Government Authentication Framework for Business
AGAF-I	Australian Government Authentication Framework for Individuals
AGIMO	Australian Government Information Management Office
AGOSP	Australian Government Online Service Point
AISEF	Australasian Information Security Evaluation Facility
ALGA	Australian Local Government Association
CAPTCHA	Type of challenge-response test to ensure that the response is not generated by a computer
CMP	Public Key Infrastructure Management Protocol
C-R	Challenge-response
CRL	Certificate revocation List
DSD	Defence Signals Directorate
DVS	Document Verification Service
EOI	Evidence of identity
EOR	Evidence of relationship
GSEF	Gold Standard Enrolment Framework
HSM	Hardware security module
ICT	Information and communication technology
IP	Internet Protocol
ISM	Australian Government ICT Security Manual
IT	Information technology
IVR	Interactive Voice Response
LDAP	Lightweight Directory Access Protocol
NeAF	National e-Authentication Framework
NISS	National Identity Security Strategy
OASIS	Organisation for the Advancement of Structure Information Standards
OCC	Online and Communications Council
OTP	One-time password
PAD	Personal Authentication Device
PIN	Personal identification number
PKAF	Public key Authentication Framework
PKI	Public key infrastructure

PoI	Proof of identity
PSM	Protective Security Manual
SAML	Security Assertion Mark-up Language
SBR	Standard Business Reporting
SDLC	Systems Development Life Cycle
SMS	Short Message Service
SOA	Service-oriented architecture
SSL/TLS	Secure Sockets Layer / Transport Layer Security
XBRL	An XML-based open standard language
XML	EXtensible Markup Language

Executive summary

The National e-Authentication Framework (NeAF) replaces the Australian Government Authentication Framework for Business and Australian Government Authentication Framework for 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 NeAF 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 NeAF 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
- authentication of government websites.

Central to the NeAF 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 NeAF 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 questions "Do we have the correct party at the other end of the line?" and "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
- a standardised approach to validating the e-Authentication approach selected.

1. Introduction

Vision

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

1.1. Background

In 2003 the Australian Government developed and adopted the *Australian Government e-Authentication Framework* (AGAF). The key drivers for the AGAF were the establishment of better practices to promote minimum standards of assurance for the growing range of online government transactions, and facilitating consistency in authentication approaches across agencies. The latter was seen to offer the opportunity for greater levels of "sharing" of e-Authentication elements (e.g. one or more of processes, infrastructure and / or credentials) across agencies and user bases.

The AGAF was initially applied within Australian Government agencies to their online dealings with **business**. It has also been adopted by most state and territory governments.

During 2006 work was undertaken to make the AGAF suitable for use by governments in their electronic interactions with **individuals**. This project also examined a range of additional matters, including website authentication and privacy-enhancing technologies.

In June 2007, the Online and Communications Council (OCC) requested the development of the AGAF into a National e-Authentication Framework (NeAF) to improve the consistency of approaches being taken by governments to electronic service delivery. While the NeAF is intended as a better practice framework, to be adopted – and where appropriate, customised – by agencies, jurisdictions and sectors, it is expected that all jurisdictions will comply with the principles that underpin its application.

The drivers for the development of the NeAF were to minimise duplication of effort and achieve consistency of e-Authentication approaches across jurisdictional boundaries that in turn will maximise the efficiency and effectiveness of electronic service delivery to the community across all tiers of government.

1.2. Objectives

The objectives of the NeAF 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 and jurisdictions to increase efficiency and enable

  - re-use 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 when and what type of e-Authentication is required; and
- ensure that due diligence is applied when determining e-Authentication approaches.

1.3. Scope

The NeAF focuses on:

- electronic authentication of the identity of individuals and businesses including their agents or representatives; and
- electronic authentication of government websites.

Where appropriate it can be applied to:

- electronic authentication of assertions other than identity
- electronic authentication of transactions, addressing integrity and non-repudiation requirements
- cross-organisational electronic authentication (e.g. between government agencies within or across jurisdictions, to include private and public sector initiatives)
- electronic authentication of non-human entities; and
- electronic authentication of individuals to support physical access controls.

1.4. Overview

The Australian Government, in its *2006 e-Government Strategy, Responsive Government: A New Service Agenda* (the Strategy) 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.[1]

The NeAF contributes to the achievement of the objectives of the Strategy by facilitating a consistent approach by agencies across all tiers of government to the management of unacceptable identity-related risks for the purpose of facilitating secure and easy interaction with government. It will guide agencies in determining:

[1] See http://www.finance.gov.au/publications/2006-e-government-strategy/vision-for-2010.html.

- the level of authentication required based on an assessment of the risk of interactions with their end users (i.e. businesses or individuals); and
- an electronic authentication-solution approach that will enable end users to build trust and confidence in electronic transactions with government.

This document positions e-Authentication within the broader identity and risk management context for agencies and describes the processes by which the e-Authentication risk assessment is undertaken. It provides sufficient detail for the reader to be informed of the range of issues to be addressed in each stage of the identity authentication process. More-detailed explanation of the processes involved and their application is contained in the Better Practice Guidelines.

The NeAF as a whole has a number of target audiences:

- the **Management Summary** is directed to agency heads, chief executive officers and chief information officers
- the NeAF is directed primarily to Chief Technology Officers and business line and technical areas responsible for agency policy with respect to the development of online services (including privacy, information management and information security); and
- the **Implementation Models and Better Practice Guidelines** are targeted primarily at those responsible for the design, development and implementation of online government services, and external risk and security advisers engaged by agencies.

In adopting the NeAF, agencies should consider the following:

- the requirements of different client groups (in terms of the useability of authentication solutions and balancing the reduction of the red tape burden on both individuals and business) should be balanced against the importance of ensuring the appropriate level of identity assurance for transactions
- identity assurance is multi-dimensional, and selection of an appropriate e-Authentication credential must be the outcome of a comprehensive risk assessment process
- each e-Authentication credential type has inherent strengths and weaknesses that should be assessed in the context of the overall risk assessment process for the particular transaction
- as e-Authentication credentials function as only one element of an information security system, the likelihood and consequence of identity-related risk should not be treated in isolation as their effectiveness is only as good as their implementation and the associated business processes; and
- agencies shall reference authoritative policy documents such as the Australian Government Protective Security Manual (PSM) and the Australian Government ICT Security Manual (ISM) for the Commonwealth, and relevant security policies that apply in states and territories. This NeAF does not replace these policies.

1.5. What is e-Authentication?

Electronic authentication (or "e-Authentication") is the process of determining the degree of confidence that can be placed in assertions that a user or identity is who and/or what they purport to be. Assertions include identity, role, delegation and value. The National e-Authentication Framework (NeAF) is primarily concerned with the electronic authentication of identity.

Electronic transactions are considered to be across a number of channels, including:

- internet or web-based
- telephone IVR; and
- facsimile transmissions.

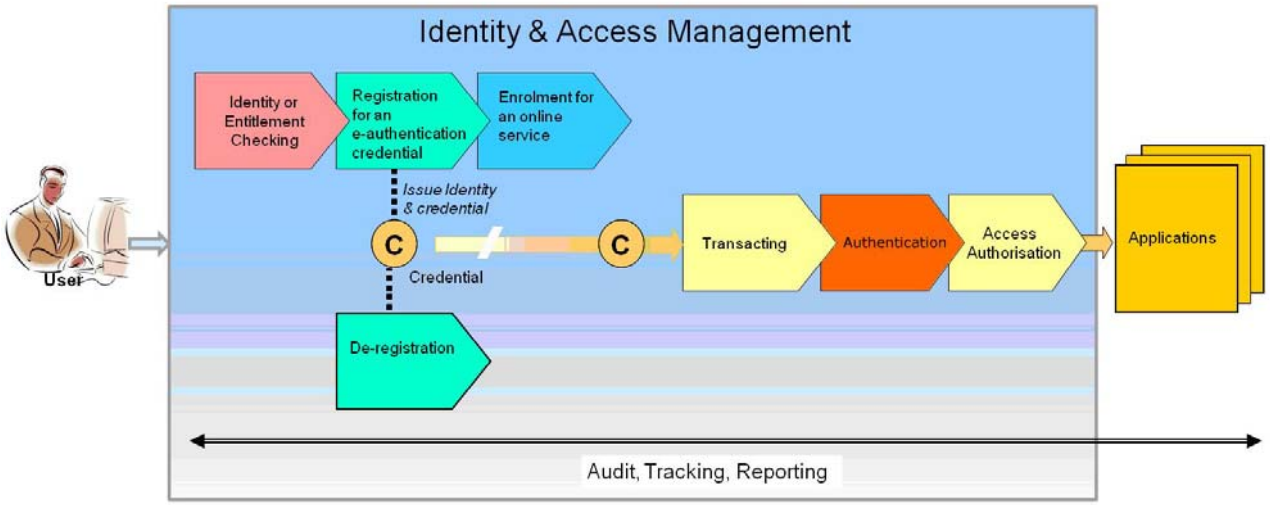
e-Authentication is accomplished using something the user knows (e.g. password, secret questions and answers), something the user has (e.g. security token) or something the user is (e.g. biometric), or a combination of these.

Determining the appropriate authentication approach requires that a balance is struck between the level of risk that is acceptable and the desired user experience. High-risk systems, applications and information require stronger forms of authentication that more accurately confirms the user's digital identity as being who they claim to be, as opposed to a low-risk application where the confirmation of the digital identity is not as important from a risk perspective.

Authentication is not the same as authorisation, which addresses the permissions or privileges granted to an end user to access particular systems, receive particular services or lodge particular reports etc. The issue of authorisation is not addressed in the NeAF.

e-Authentication is part of the broader identity and access management systems as shown in Figure 1 below.

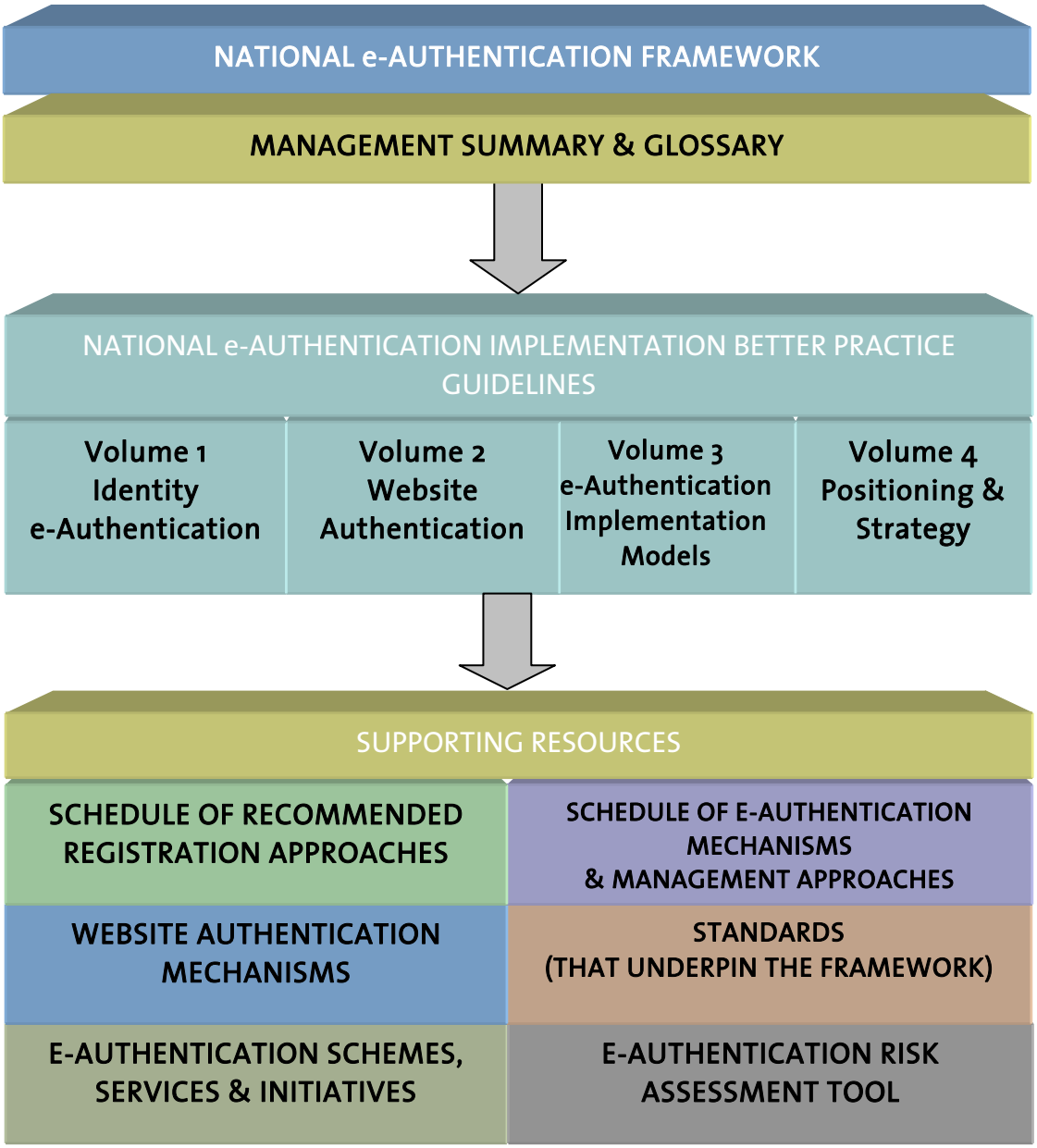
Figure 1: Identity and Access Management lifecycle



1.6 Structure

The NeAF consists of this document and associated guidelines as well as the supporting standards and procedures that provide guidance in their implementation.

Figure 2: NeAF structure



1.7 Principles and terminology

This section provides a checklist of fundamental principles that will guide agency implementation of the NeAF and a summary of the major terms used in this document.

The checklist below is expressed as a series of aspirational statements that are designed to provide agencies with a “benchmark” against which their application of the NeAF can be checked.

1.8 NeAF application 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 businesses' 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 (i.e. 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.

1.9 Terminology

The meaning of key terms within the NeAF context is provided below.

Table 1: Definition of key NeAF terms

Term	Meaning (within NeAF document set)
AISEF	Information technology (IT) security-testing laboratories that are accredited to conduct IT security evaluations for conformance to the Common Criteria for Information Technology Security Evaluation, International Standard ISO/IEC 15408-1:2005 and ISO/IEC 15408-2/3: 2008.
Assertion	The attribute that the relying party wishes to authenticate. These can include: entity, identity, value, role or delegation.
Assurance level	The level of trust that is required from e-Authentication and/or the level of trust related to a particular approach to e-Authentication.
Credential	The "technology" used by a user for authentication (e.g. user-id+password, shared information, smartcard, public key infrastructure (PKI) etc.)
Credential management	The "lifecycle" approach associated with a credential including creation, initialisation, personalisation, issue, maintenance, cancellation, verification and event logging.
Document Verification Service (DVS)	The national DVS is an Australian Government initiative to improve identity security, combat identity crime and protect the identities of Australians from being used for illegal purposes.
e-Authentication	The process that delivers (a level of) assurance of an assertion made by one party to another in an electronic environment. Under the NeAF the focus is on the assurance of identities of individuals and businesses.
e-Authentication approach	The collective of e-Authentication elements selected and implemented by an agency including the approach to registration and enrolment and the authentication mechanism selected.
e-Authentication mechanism	The combination of the credential and the credential management approach.
e-Authentication scheme	A formalised, usually contractually-bounded, community approach to e-Authentication that identifies all key players including registration authority, credential issuer and verifier, subscribers and relying parties, and all business rules associated with the assessment and containment of risk.
Enrolment	The act of binding an e-Authentication credential to a known instance of a user within an IT resource context (e.g. network, website, application system) in order to enable access by the user.
Entity	The person or "subject" (e.g. corporations, trusts, superannuation funds, incorporated associations) associated with a digital identity. An entity may have multiple digital identities.
Evidence of Identity (EoI)	Evidence (usually in the form of documents) presented to verify the identity of an entity (person or organisation).
Evidence of Relationship (EoR)	Evidence (e.g. in the form of shared knowledge/secrets, or documentary) used to substantiate that the presenting party has an existing relationship with the relying party (i.e. is already the "owner" of a digital identity on the relying party's system). (In some existing government authentication schemes this is referred to "proof of record ownership".)

Term	Meaning (within NeAF document set)
Identification	A claim or statement of identity (of an individual or business).
Identity	The representation of an entity, particularly within an information and communication technologies (ICT) context. An entity may be represented as "themselves" or as a representative, role, delegate etc.
National Identity Security Strategy (NISS)	NISS is an Australian Government initiative to improve identity security, combat identity crime and protect the identities of Australians from being used for illegal purposes.
One-time password (OTP)	An OTP is a password that is changed each time it is required.
Public Key Infrastructure (PKI)	PKI is a set of processes and systems that support the requirements of public key (or asymmetric) cryptographic security.
Registration	The processes associated with the initial creation of an electronic identity for a user. Registration usually encompasses EOI and/or EOR processes.
Subscriber	The entity that "applies for", is issued with and uses an e-Authentication credential.
Token	A hardware device (e.g. smartcard, mobile phone) that stores authentication information and may be able to perform programmatic functions (e.g. encryption).

2. Identity e-Authentication planning (see Better Practice Guidelines Vol. 4)

2.1 Introduction

A strategic approach to e-Authentication will underpin the adoption of e-Authentication approaches that are consistent with NeAF, supporting a more rapid deployment and use of e-Authentication credentials at the least cost and effort to agencies, individuals and businesses. A strategic approach will also enable consideration of relevant connected government initiatives.

Development of an agency e-Authentication strategy will:

- develop a bird's eye view of the agency's e-Authentication requirements in the context of the agency and government's overall approach to information security
- highlight areas of particular risk and difficulty, including requirements to change processes and systems
- determine the costs, benefits and risks associated with the e-Authentication requirements
- develop an implementation strategy including:
  - determining awareness-raising, training and change-management requirements for agency personnel and users
  - determining appropriate governance and reporting approaches
- allocate responsibility and resources for implementation.

An agency e-Authentication strategy needs to take both a top-down and bottom-up view. The top-down view relates to the overall information security management policies, approaches and architectures of an agency, and the governance and reporting approaches required to provide the requisite level of corporate assurance. A top-down approach shall also factor in existing government identity-related policies and frameworks.

The bottom-up view relates to the matrix of user bases, transaction sets and e-Authentication approaches. These need to be captured and correlated, with the intelligence gained being used to map out an agency's general approach to e-Authentication. It is important that this activity is informed by discussions with users and collaboration with other agencies that deal with the same user bases.

2.2 Identity and access management

e-Authentication strategies are best determined within the context of an overarching identity and access management framework that provides a unifying approach to the management of access to information – and, in some cases, physical resources (e.g. premises) – and informs conformance across the areas illustrated in Figure 1 above.

2.3 Systems architecture and systems development lifecycle

e-Authentication requirements should be factored into agencies' periodic reviews of systems architectures. ISO/IEC 15288:2008 Systems engineering - System Life Cycle

Processes can provide useful guidance to agencies. It is essential that e-Authentication requirements are identified in the earliest stage of this lifecycle and carried forward to ensure that a suitable and robust approach is engineered into all necessary aspects of the solution, the surrounding processes, and the testing, training, deployment and operations.

2.4 Privacy

The Commonwealth and each state and territory regulate the collection and handling of personal information either by legislative or administrative regimes. Agencies shall ensure that implementation meets all relevant regulatory and administrative requirements for their jurisdiction, as well as community expectations.

2.5 Risk management

2.5.1 Introduction

As part of the systems development lifecycle[2], agencies will evaluate and resolve a range of information security threats, vulnerabilities and consequences. Mitigation strategies are typically designed to reduce either the likelihood of a threat occurring or to reduce the consequences (i.e. impact) in the event it does occur.

Typically this will be done by following risk management methods and applying information security treatments such as those codified in organisational policies and national and international standards (e.g. AS/NZS 4360: 2004 Risk Management and AS/NZS ISO/IEC 27001:2006 Information technology - Security techniques - Information security management systems – Requirements; and AS/NZS ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management), in government policy directives such as ISM[3] and the PSM[4].

The determination of an appropriate approach to e-Authentication does not occur in isolation. It is usually generated by other processes (e.g. application development) and is positioned within the overarching risk management and information security management regimes of an agency.

---

[2] Systems Development Life Cycle (SDLC) – see industry standards: AS/NZS 15288 – System Life Cycle Processes Standard, or ISO/IEC 15288 – System Life Cycle Processes Standard

[3] Australian Government ICT Security Manual, located at http://www.dsd.gov.au/library/infosec/ism.html.

[4] Australian Government Protective Security Manual, located at http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(PSM2005).

2.5.2 Types of electronic transactions

Typically electronic transactions undertaken by individuals or businesses with government fall into five main categories:

- enquiries
- information provision or instruction
- declarations
- statements; and
- financial transactions.

The nature and extent of threats and risks associated with these categories of electronic transactions will vary according to the sensitivity of the information to be exchanged, the value of the transaction and/or the legal issues associated with the transaction.

2.5.3 Electronic transaction risk treatment

Risk mitigation solutions to electronic transactions seek to treat the following for security risks:

1. **Authentication:** Do we have the correct party at the other end of the line – i.e. are they who they purport to be?
2. **Data integrity:** Can we detect if information has been altered while in transit?
3. **Confidentiality:** Can we ensure that information while in transit remains confidential?
4. **Non-repudiation:** Can we prove that a given identity submitted or approved or signed the received information? [5]

The objective of this NeAF is to address the first of these questions.

2.5.4 Classes of risk treatments

Agencies mitigate threats by implementing control measures at different stages of the electronic transaction lifecycle. These controls can be classed as:

- before the transaction
- during the transaction; and
- after the transaction.

e-Authentication is essentially a "before the transaction" risk mediation treatment that contributes to the security of electronic transactions.

---

[5] The Gatekeeper PKI Framework defines non repudiation as: "Evidence, verifiable by a third party that a Transaction has been sent/authorised by the purported sender."

3. NeAF methodology (see Better Practice Guidelines Vol 1)

The NeAF 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 NeAF recognises that a range of solutions (e.g. technology or business process-based) are possible to mitigate an identity related risk.

However, where an agency determines that issuance of an authentication credential is an appropriate solution to mitigate an identity-related risk, the NeAF provides guidance in relation to credential selection and management.

The NeAF steps are:

1 determine the business requirements

2 determine the assurance level requirements

3 select the registration approach

4 select the e-Authentication mechanism

5 select an implementation model

6 assess the business case and feasibility of the implementation model; and

7 review the e-Authentication solution.

Step 1: Determine the business requirements

This step is usually undertaken as part of the "requirements definition" phase of a business and systems project that is seeking to develop online services.

Some of the key business requirements to be determined (and not in any particular order) in the context of a comprehensive risk assessment process are listed below.

- clearly identify the services to be provided, information to be accessed and the user community
- what assertion or assertions are to be authenticated? In general this will be identity, but other assertions such as entity, role, delegation and value may need to be authenticated in addition to, or in place of, identity.
- what electronic delivery channel is to be used: telephone (landline or mobile), facsimile and/or computer or some combination?
- what privacy implications are inherent in the proposed transaction, and/or what privacy issues need to be satisfied in the determination of the need for and type of e-Authentication approach?
- what additional transaction assurance or security requirements exist (i.e. data integrity, confidentiality, non-repudiation) and is it possible/appropriate to leverage the underlying e-Authentication processes and technologies?

Step 2: Determine the assurance level requirements

This step involves two parts. Firstly, a comprehensive and multi-dimensional assessment of identity-related threats and risks to determine an assurance level for a

transaction (or transaction set). The end point of this process is the identification of the residual identity-related risks that e-Authentication (or alternative mitigation strategy) will be required to address. While the NeAF explicitly focuses on identity-related threats, agencies need to be sensitive to the range of other threats relevant to the determination of an e-Authentication solution.

Secondly, assessment of the required e-Authentication assurance level by identifying the severity of the impacts of getting e-Authentication wrong. Tables 2, 3 and 4 (below) provide a more-detailed summary of the risk assessment process that ultimately generates the authentication assurance level. An online risk assessment tool is provided to assist with this task: contact Finance at authentication@finance.gov.au. (Note: Agencies should consider the nature of the information and its classification that is entered into this tool.)

Assurance levels

Assurance levels are used to describe the level of importance of getting e-Authentication right and the resultant level of robustness of the required solution.

The NeAF determines assurance levels based upon the assessment of the threats to agencies and/or end-users of getting e-Authentication wrong.

Table 2: NeAF assurance levels

No assurance	Minimal assurance	Low assurance	Moderate assurance	High assurance
Level 0	**Level 1**	**Level 2**	**Level 3**	**Level 4**
No confidence is required in the identity assertion.	Minimal confidence is required in the identity assertion.	Low confidence is required in the identity assertion.	Moderate confidence is required in the identity assertion.	High confidence is required in the identity assertion.

Table 3 below provides an indicative description of possible consequences and their respective severities. The consequences listed each have inherent levels of seriousness; hence, in some cases only the higher or highest levels of severity are acceptable. These threats also have more than one dimension of severity, such as the number of individuals or businesses that are impacted.

The table should be interpreted across each row where the scale of severity increases from “Insignificant” to “Severe”. Examples of the nature of that severity are provided. It is not intended that the table be used to compare or equate the severity of different consequences (i.e. “threaten life directly” does not equate to “substantial inconvenience” despite the fact that both are rated as “Severe”).

Table 3: Illustrative consequences and severity

Consequence	Severity				
Consequence rating	**Insignificant**	**Minor**	**Moderate**	**Major**	**Severe**
Inconvenience to any party	No inconvenience	Minimal inconvenience	Minor inconvenience	Significant inconvenience	Substantial inconvenience
Risk to any party's personal safety	No risk	No risk	No risk	Any risk to personal safety	Threaten life directly
Release of personally or commercially sensitive data to third parties without consent	No impact	Would have little impact	Measurable impact, breach of regulations or commitment to confidentiality	Release of information would have a significant impact	Would have severe consequences to a person, agency or business
Financial loss to any client of the service provider[6] or other third party	No loss	Minimal	Minor	Significant	Substantial
Financial loss to Agency / service provider	No loss	Minimal < 2% of monthly agency budget	Minor 2% to < 5% of monthly agency budget	Significant 5% to < 10% of monthly agency budget	Substantial • 10% of monthly agency budget
Impact on government finances or economic and commercial interests	No impact	No impact	Cause financial loss or loss of earning potential	Work significantly against	Substantial Damage
Damage to any party's standing or reputation	No damage	No damage	Minor: short-term damage	Limited long-term damage	Substantial long-term damage
Distress caused to any party	No distress	No distress	Minor: short-term distress	Limited long-term distress	Substantial long-term distress
Threat to government agencies' systems or capacity to conduct their business	No threat	No threat	No threat	Agency business or service delivery impaired in any way	Agency business halted or significantly impaired for a sustained period[7]
Assistance to serious crime or hindrance of its detection	Would not assist in or hinder detection of unlawful activity	Would not assist in or hinder detection of unlawful activity	Prejudice investigation or facilitate commission of violations that will be subject to enforcement efforts	Impede investigation or facilitate commission of serious crime	Prevent investigation or directly allow commission of serious crime

Source: AS/NZ 4360 – Risk Management 2004

[6] The amounts to be considered are suggested as: Minimal <$50; Minor $50 to <$200; Significant $200-<$2000; and Substantial • $2,000. These figures are guidelines only based on impact on an "average" individual. Where the client is known to be a corporation of other similar entity, these figures would need to be adjusted upward. If multiple clients will suffer the loss, the impact level should be adjusted accordingly to reflect the total losses to clients.

[7] The period here may vary from agency to agency – some agencies may be able to endure a halt in business for a number of days without serious impact on the government or society. Others more directly involved in public safety and similar services would be less tolerant of outages.

While the above process determines the consequences of getting e-Authentication wrong, it is also necessary to map the likelihood of this occurring in order to finally determine the assurance level to be applied. An indicative mapping of consequences versus likelihood is illustrated in Table 4 below.

Table 4: Indicative assurance level requirements based upon likelihood and consequences

	Consequences				
Likelihood	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Nil	Low	Moderate	High	High
Likely	Nil	Low	Moderate	High	High
Possible	Nil	Minimal	Low	Moderate	High
Unlikely	Nil	Minimal	Low	Moderate	Moderate
Rare	Nil	Minimal	Low	Moderate	Moderate

The information security classification level associated with the information that will be "exchanged" during the transaction (agencies are referred to the PSM and ISM for authoritative policies in this regard) will be a consideration in assessing the consequences of a particular threat being realised.

Information classified at "X-in-Confidence" and above can only be transmitted across an unclassified network such as the internet under certain circumstances. Further guidance on this matter can be found in the ISM available at http://www.dsd.gov.au/library/infosec/ism.html.

While the adoption of higher-assurance e-Authentication solutions may represent one solution to mitigate threats in relation to classified information the application of alternative risk mitigation approaches will need to be considered.

These could take the form of increased levels of application-based access control, or the limitation of the nature of sensitive information revealed or exchanged, or the exclusion of categories of "at risk" users from the proposed online community.

At the completion of this step agencies should revisit the risk management plan for possible decision points. Questions to ask include:

- Are existing information security strategies adequate to mitigate identified risks?
- Are the identified risks acceptable in terms of the agency's "risk appetite"?
- Is an e-Authentication solution still appropriate?

If the determination is made to continue with the development of an e-Authentication solution then the next stage in the process is to determine the nature of the registration process to be implemented.

Step 3: Select the registration approach

The registration approach will be determined by:

- the nature of the assertion to be authenticated
- the assurance level required
- whether the subscriber is already a known customer of the agency; two variations emerge:
  - the subscriber is a known customer but has no pre-existing e-Authentication credential
  - the subscriber is a known customer and has a pre-existing e-Authentication credential
- whether the subscriber has already been issued a credential by another government agency, in which case a range of additional factors will have to be considered including:
  - the registration process used by that agency
  - the credential lifecycle management process employed by that agency
- the nature and significance of privacy and other public policy issues identified during Step 1.

Further detail is contained in Schedule A of this document.

Registration involves verifying the subscriber's identity or other attribute to an understood assurance level prior to creating an e-Authentication credential.

The approach to registration will depend upon the nature of the assertion to be authenticated. The most common instances are:

- registration of individuals (as themselves)
- registration of individuals as representatives of businesses; and
- registration of individuals as representatives[8] of other individuals.

Three approaches are most commonly used:

[8] While an element of the registration process will include ensuring that the individual has the appropriate authorisation to act on behalf of another individual, the emphasis here is on ensuring the individual's identity.

- **Evidence of identity (EoI)** basis, which requires individuals to present a range of documentation to validate their claim to identity. Recommendations regarding the number and types of documents are contained in a range of authoritative government identification schemes, including those associated with the National Identity Security Strategy (NISS), and the Gatekeeper PKI Framework.[9] Agency risk management strategies should contain contingencies to cover the "failure" of EoI approaches.
- **Evidence of relationship (EoR), or "known customer"** basis, which requires individuals to establish they have an existing relationship with the agency. In most circumstances, the establishment of the original relationship would have encompassed an EoI process. This approach to registration usually involves the presentation of documentary or knowledge-based evidence that relates to the context of the relationship between the subscriber and the relying party.
    - A further option is that an individual may present to an agency with a credential issued by another agency[10] – in other words the individual is "known" to that second agency. This is an important consideration from the perspective of credential re-use which can deliver efficiency gains to both agencies and end-users.
- **Pseudonymous registration**, which does not require a user to go through either an EoI or EoR process to obtain an e-Authentication credential. Two variants of this approach exist:
    - Those in which a pseudonymous e-Authentication credential having been created is then linked through an EoR enrolment process to known instances of the user with one or more agencies e.g. AGOSP and DHS's *myaccount*.
    - Those in which the pseudonymous e-Authentication credential is not linked with pre-existing instances of the user on the agency's system. Here the purpose of the credential is to enable a persistent conversation between the user and the agency; for example, for purposes of completing a passport application.

Step 4: Select the e-Authentication mechanism

The strength, or assurance level, of an e-Authentication solution depends upon

- the strength of the registration process; and
- the strength of the e-Authentication mechanism, which, in turn, depends upon:

---

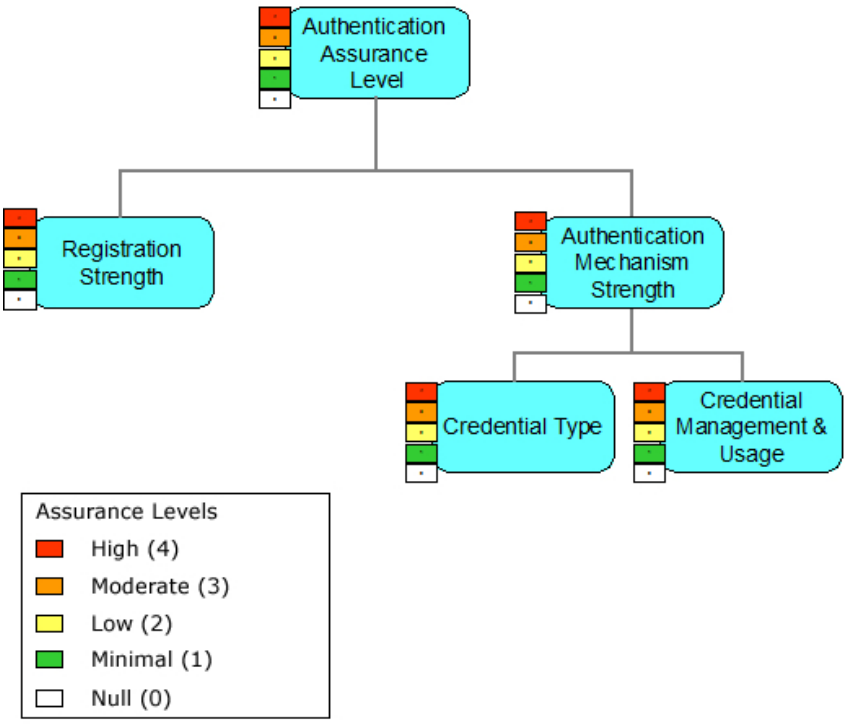
9 Situations may arise in which an individual is unable to present the required document set due to; for example, having never applied for or been issued with defined identification documents, or having lost these, or having a cultural predisposition to not retain/carry documents. Surrogate approaches to conducting EoI will have to be devised to suit these circumstances; for example, requiring another individual who does have the requisite level of EoI documentation to vouch for the identity (or related attributes) of the applying individual.

10 See Australian Standard AS 4860 Knowledge Based Identity Verification for further detail.

- the strength of the credential type
- the credential management and usage strength.

This is illustrated in figure 3 below.

Figure 3: e-Authentication solution components



Authentication mechanisms are the means by which subscribers authenticate themselves electronically.

Components that define an authentication mechanism are:

- An authentication credential (the Credential), which is something tangible controlled by the subscriber that could incorporate one or a combination of attributes:
  - something the subscriber knows
  - something the subscriber has in their possession
  - something the subscriber is.

These attributes are termed “factors”.

- The methods of management and usage of the credential over its life time.

These methods will incorporate processes around generation of the credential, its distribution to the subscriber, its activation and its ultimate usage within a broader authentication protocol established between the subscriber and a relying party.

A description of common credential types and factors influencing their inherent strength is at Schedule B, later in this document.

In selecting an authentication mechanism agencies should consider the following.

- As an "authentication mechanism" is an amalgam of the credential type and the credential management approach, it is necessary to select the appropriate strength of each of these in order to meet the e-Authentication assurance level required:
  - lifecycle management of the credential may also be interpreted to include the registration business processes
  - care should be taken to ensure that, in determining the appropriate authentication mechanism, a full assessment of the strengths and weaknesses of the solution is undertaken including, as appropriate, risks arising from the behaviour of the credential holder.
- Existing authentication mechanisms/schemes.

Selecting a credential

Credential types

Credentials may be categorised as:

- **single-factor**, such as a password, an unprotected one-time password (OTP) device, or a simple code book; and
- **multi-factor** (i.e. two or more), such as a PIN-protected smartcard or PIN-protected OTP device, password-protected digital certificate or a biometric protected token. A multi-factor credential requires multiple factors of different types (something you know, something you have, or something you are) to be present in order to generate an authentication code which is presented to the relying party for verification.

The selection of a credential type should take into consideration the following:

- the strengths (and weaknesses) of particular credential types relative to the level of assurance required (see Schedule B1, of this document)
- the ease of use of the credential by the intended client group (if the credential type is not easy to use then the intended objective of increasing community take-up of electronic transactions will not be achieved; thus, a balance between identity assurance and ease of use is a major consideration in the selection of the authentication solution)
- whether a pre-existing credential is already in the hands of the intended subscriber base (this may be a credential already issued by the agency or a credential issued by another organisation); and
- if required, the capacity of the credential selected to meet the additional requirements (e.g. transaction confidentiality and/or non-repudiation) identified in Step 1 (above). Note that other complementary technological and/or process approaches (e.g. VANguard, see Appendix C) may be more appropriate to meet these additional requirements.

Credential management

In addition to the intrinsic credential characteristics the strength of an authentication mechanism depends on the management and usage of the credential. Credential management processes affect authentication mechanism strength and would typically be documented in arrangements between credential issuers and relying parties.

It should be noted that the behaviour of the credential holder has the potential to adversely affect the strength of the assurance provided by the credential itself as well as agency-based management processes. These threats need to be factored into many decision-making processes regarding the choice of authentication mechanism.

End users should be provided with adequate information (and training, if necessary) regarding use and procedures to safeguard their credential to minimise the risk of fraudulent use.

The strengths and weaknesses of an authentication mechanism determine its suitability for use within various contexts.

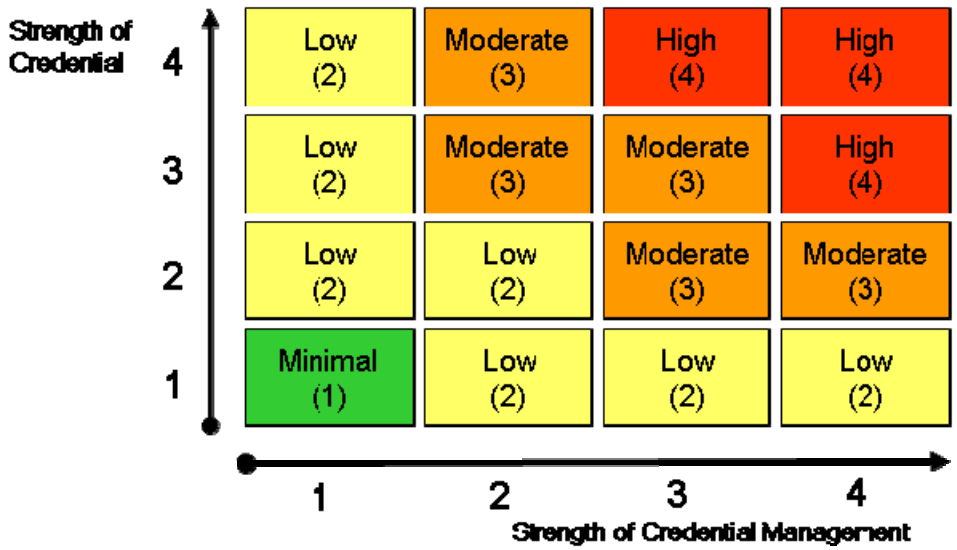
Factors to be considered and resolved in this step are:

- credential generation
- credential issuance and activation
- ease of use by credential holders, including possible inappropriate credential holder behaviours
- activated credential management, including re-activation
- credential verification; and
- authentication event logging.

If reliance is placed on a credential issued by another agency then consideration will have to be given to the strengths and weaknesses of the lifecycle management processes in place within that agency.

Table 5 below maps the inherent strength of the credential against the strength of the lifecycle management process. Note that the assurance levels reflected in the table are indicative only.

Table 5: Authentication mechanism attributes to meet assurance level



Step 5: Select an implementation model (see Better Practice Guidelines Vol 3)

A spectrum of e-Authentication implementation approaches are possible, ranging from agency or application-centric approaches to centralised whole-of-government or whole-of-sector schemes.

This requires agencies to determine whether and how the models/schemes will fit with the:

- assurance levels determined in Step 2 (above)
- registration approach/s determined in Step 3 (above); and
- e-Authentication credential and credential management solutions identified in Step 4 (above).

This step should also consider the extent to which re-use of existing credentials and infrastructure is appropriate for the agency's particular requirements

This step should also include consideration of the use of intermediating trust-broker services (e.g. VANguard, see Appendix C).

Authentication implementation models are differentiated by a range of factors, including functional distribution across participants, privacy environments, legal frameworks and governance models.

Emerging implementation contexts and service delivery models

e-Authentication implementation models are required to address the emerging needs of a range of government service delivery models that are aimed at:

- enabling increased user-centricity – allowing users greater choice in relation to the number of e-Authentication credentials they choose to hold and (subject to agency requirements) how they choose to use these credentials

- efficiency improvements in the delivery of government services electronically through re-use of core infrastructure
- promoting agencies' abilities to implement a risk-based approach to user authentication; and
- decreasing users' need for awareness of the distribution of various business support functions across government agencies, and changes in this distribution over time.

NeAF and implementation models

The application of the NeAF principles across government will result in the broad alignment of e-Authentication approaches. This will provide consistency across participating agencies of:

- the treatment of application assurance needs and associated authentication risk mitigation approaches across agencies
- implementation of end-user registration and credential-provisioning processes, for various assurance levels across agencies and across user segments; and
- selection and utilisation of e-Authentication credentials and e-Authentication mechanisms for various assurance levels as required by application systems.

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.

Identity authentication implementation model components

Contemporary identity authentication implementation models are described by and differentiated by a range of factors including:

- the distribution of the authentication-related roles and functions across the various operating participants
- the treatment of identifiers within the models and the related privacy implications and controls (for example, some models mandate the use of a single identifier linked to the authentication credential to be used for access to all applications and agencies, whereas other models enable discrete application or agency specific identifiers to be linked to a credential); and
- the legal frameworks and governance regimes which underpin the models.

Trust-broker services

While both the federated and centralised e-Authentication implementation models may be characterised as providing "trust-broker" services, such services may be provided independently of the implementation model/scheme and may therefore be available as a verifier service between the credential issuer and the relying party (see Appendix C).

Step 6: Assess the business case and feasibility of the e-Authentication 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. A three-step approach is recommended:

Step 1: Review the environment and identify business need

Step 2: Carry out a high-level options analysis

Step 3: Carry out a detailed options analysis.

Step 7: Review the e-Authentication solution

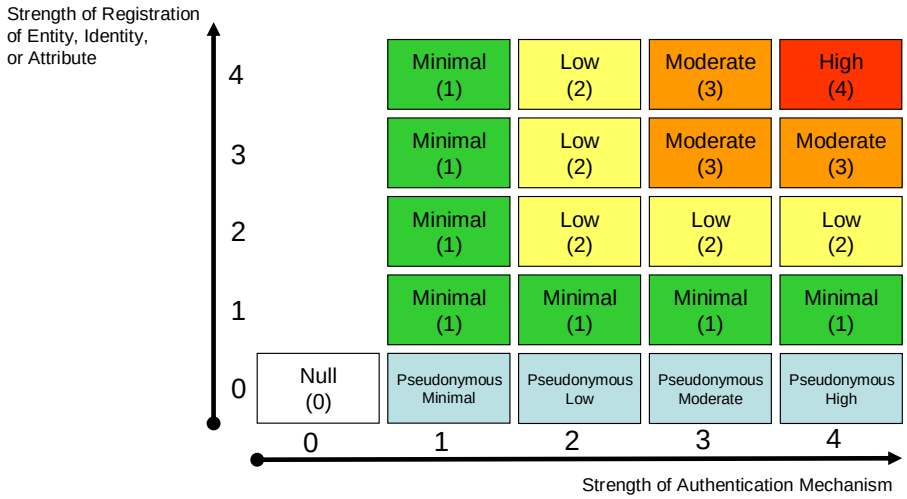
Once an e-Authentication solution has been selected, it is necessary to validate it.

Validation should encompass:

- consideration of whether the selected registration approach and authentication mechanism provide the required e-Authentication assurance level as illustrated in Table 6 below; and
- consideration of whether the proposed solution meets the 10 principles detailed in Section 1.8 of this document.

In addition, where the e-Authentication solution includes the use of a pre-existing credential it will be necessary to analyse the legal, process, technology and cost issues associated with the necessary implementation and operational model.

Table 6: NeAF – solution element-mapping for assurance levels



4. Authentication of government websites (see Better Practice Guidelines Vol 2)

4.1 Rationale

Authentication of government websites will increase trust levels for individuals and businesses dealing electronically with government.

The capacity to authenticate a government website becomes increasingly important as electronic services are developed using a service-oriented architecture (SOA) approach, particularly where there is a reliance upon locating and utilising web services through service instance directories.

4.2 Website authentication planning principles

The following is adapted from a range of vendor-developed (e.g. Google and Microsoft) position papers submitted to the World Wide Web Consortium (W3C, see <www.w3.org>) and from prior documents developed for AGIMO.

Web server authentication

A user should authenticate a government website/server, since an unauthenticated website/server can ask for confidential information from the user for unknown purposes.

User involvement in website authentication

Many solutions to website authentication rely on user involvement to distinguish between trusted or untrusted sites. Some users (unsophisticated or unmotivated) cannot be relied upon for this purpose.

Website authentication solutions should extend beyond technology to include user education, and agency detection and prevention initiatives aimed at reducing reliance on user involvement. (These extensions may be best performed on a government-wide basis.)

Mutual authentication

Where user authentication is required by the government website, website authentication solutions should ideally integrate with user-authentication mechanisms so that users are trained to use a single mutual-authentication mechanism.

User credentials

Any user credentials used should be fit for purpose for the website application.

Website credentials

Gatekeeper compliant device certificates should be considered as the base level for any use of digital certificates for identifying government websites.

Authentication techniques

The authentication mechanism used should be fit for purpose for the website application. If a federated model for authentication is adopted, authentication mechanisms may need to reflect the requirements of the website requiring the highest protection.

Trusted channels

Use of channels such as SSL/TLS should use a Gatekeeper-compliant device certificate at the web server, combined with user training on certificate verification. In order to protect authenticating credentials against human man-in-the-middle attacks, strong cryptography should be an element of any solution. Trusted user interfaces for authentication should be at least based on a shared secret, communicated out of band, since all user interfaces are spoof able (i.e. where an entity successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage).

Client-side active content

The risks and benefits of active content technology on the client-side should be carefully assessed before it is implemented. User input should be validated at the web server, even if already validated by the active content of the user's browser.

Website content

The content published by public government websites should be formally justified (e.g. by the "need to know" of the intended audience), formally approved, and formally managed.

4.3 Website authentication framework

The application of the NeAF approach requires that:

- agencies determine the assertion that the individual or business would be seeking to authenticate. In most cases this would be the identity of the agency, but other possibilities could include the "role" or "function" of the agency or the authenticity of a particular web-service instance (e.g. "customer eligibility checking" service) posted on the agencies' website
- agencies determine the assurance level required. The tests would apply the amended NeAF criteria, that is:
  - degree of inconvenience to any party
  - degree of risk to any party's personal safety
  - possibility of releasing of personally or commercially sensitive data to third parties
  - degree of financial loss to any party
  - degree of damage to any party's standing or reputation
  - degree of distress being caused to any party
  - extent of threat to government agencies' systems or capacity to conduct business
  - whether this would assist a crime or hinder its detection
  - extent of threat to government classified information and related assets.
- agencies determine the website authentication approach

- agencies assess the privacy and public policy implications of the proposed approach
- agencies assess the business case and other feasibility issues associated with the proposed approach; and
- agencies revisit Step 3 (above), based upon the results of Step 4 and/or Step 5.

5. 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. Management will need to promote an organisational culture that encourages awareness of e-Authentication as well as the development of good practices as a business priority.

5.1 Government roles and responsibilities

Government agencies will, consistent with the principles that underpin the NeAF:

- consider the needs and expectations of individuals and businesses
- provide appropriate education and awareness services to end users
- provide leadership in e-Authentication practices
- deliver efficient and useful services online
- ensure continuing reliability and quality of services
- manage the permissions of users who conduct transactions with government
- apply appropriate e-Authentication mechanisms and assurance levels
- collect personal information only when needed for the business process being undertaken
- provide a means of e-Authentication to parties involved in transactions so that they can confirm their identity when needed
- establish systems to control access and use of resources; and
- establish and maintain records and robust audit processes for access and permissions.

5.2 Businesses' and citizens' roles and responsibilities

Businesses and citizens will need to comply with the terms and conditions of the agency services with which they are engaging. Such requirements could include at a minimum:

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

Appendix A: NeAF legal and policy framework

In applying the NeAF, agencies will need to assess the impact of national and jurisdictional laws, regulation and policies, the most relevant ones being:

Legislation and regulation

- Privacy
- Information security
- Electronic transactions and evidence
- Record-keeping.

Government policies and references

- e-Government strategies
- Interoperability frameworks
- Privacy schemes
- Information security policies
- Identity security policies
- Authentication frameworks (PKI, smartcards etc.).

Appendix B: NeAF standards and practices foundation

In applying the NeAF, agencies will need to assess the applicability of international, national and industry/sectoral standards and practices, the most relevant ones being:

1. **Risk management**
    a. AS/NZS 4360:2004 Risk Management
    b. AS/NZS ISO/IEC 16085:2007 Information technology – Systems and software engineering – Life cycle processes – Risk management.
    c. 27005:2008
2. **Information technology security**
    a. AS/NZS ISO/IEC 27001:2006 (also AS/NZS ISO/IEC 27001) – Information technology – Security techniques – Information security management systems – Requirements
    b. ISO/IEC 27002:2005 – Information technology – Security techniques – Code of practice for information security management
    c. ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management
    d. ISO/IEC 27006:2007 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
    e. ISO/IEC 27000 Information technology – Security techniques – Information security management system – Overview and vocabulary (under development)
3. **e-Authentication technologies/methods/approaches**
    a. Evaluated Products List – Defence Signals Directorate
        i. http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html
    b. PKI:
        i. Information technology – Public Key Authentication Framework (PKAF) related Standards – General - PKAF architecture – AS4359.1.1-2002
        ii. Health informatics – Public Key Infrastructure – AS ISO 17090 (1,2,3)-2003
        iii. X.509 PKI certificates – RFC 4210 Internet X.500 Public Key Infrastructure Management Protocol (CMP) see http://www.ietf.org
    c. Knowledge-based Identity Authentication
        i. AS 4860-2007 – Knowledge-based identity authentication – Recognising Known Customers
    d. Service Oriented Architectures
        i. Organisation for the Advancement of Structured Information Standards (OASIS) see http://www.oasis-open.org.

ii. Web Services – Security, Trust, Federation etc.
see http://www.oasis-open.org

e. Directory Services

i. X.500 Information Technology – Open Systems Interconnection – The Director: Overview of Concepts Models and Services
see <http://www.itu.int>

ii. Lightweight Directory Access Protocol (LDAP)

f. Security Assertion Mark-up Language SAML (See http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security) – Cross-domain authentication and authorisation.

Appendix C: Current government e-Authentication initiatives

AGOSP single sign-on (via the enhanced <http://www.australia.gov.au>)

Single sign-on will be one of the many new services offered by the enhanced http://www.australia.gov.au (hereafter simply australia.gov.au) website. "Single sign-on" is a term used to describe the process that enables people to use a single australia.gov.au credential (e.g. username and password combination) to access a range of government accounts and services.

Currently, it is quite common for people to have several accounts across a large number of agencies, each with their own credential. Single sign-on enables people to create an australia.gov.au credential and, if they choose, associate their agency accounts with this credential.

Importantly, having an australia.gov.au single sign-on credential does not mean agency accounts are linked to one another. Rather, the australia.gov.au single sign-on allows people to have the convenience of using a single credential, while still maintaining separate agency accounts and identities. Agency records are not linked, neither is the information within these accounts shared.

The australia.gov.au single sign-on will be completely optional, and users can continue to access agency services directly.

The australia.gov.au single sign-on will be implemented using a whole-of-government authentication hub. This hub will use meaningless but unique number associations to create links between an australia.gov.au credential and an agency account in a privacy-protecting manner.

VANguard e-Authentication Services

VANguard is an existing whole-of-government service delivered by the Department of Innovation, Industry, Science and Research. VANguard is a key enabler in meeting the e-Government Strategy (AGIMO 2006) for business-to-government transactions.

VANguard is positioned as an authentication service provider, including serving the role as a trust broker. VANguard enables an agency to accept a business user's digital credential that has been issued by another organisation and then direct that credential to VANguard for e-Authentication.

VANguard verifies the digital signature and validates the digital certificate using an appropriate certification authority within a secure environment.

VANguard supports business by allowing business users to conduct transactions securely with government agencies (federal, state or local) using a range of digital credentials including Australian Taxation Offices certificates and VeriSign Australia Gatekeeper certificates.

VANguard provides a range of secure e-Authentication services comprising:

> **User authentication**: Real-time authentication of business users is provided via VANguard's authentication web page. Agencies redirect their business users to this web page at the time of log-in to be authenticated. This service enables agencies to obtain a digital signature to facilitate business user access to a secure web site or application.

Signature verification: This service enables agencies to have PDF forms or XML-based content signed by business users and verified by VANguard. Agencies send signed PDF forms or signed XML-based content to VANguard for verification of a business user's digital signature.

User non–repudiation: This service enables agencies to have browser-based content signed in real-time by business users and validated by VANguard. Agencies redirect their business users to VANguard's authentication web page when they require a business user to digitally sign the content of a transaction.

Single sign-on: Real-time authentication of business users across multiple agencies is provided via VANguard's authentication web page. An agency redirects the business user to VANguard's authentication web page at initial log-on to be authenticated. Business users can then access other nominated agencies' secure websites without the need to present their digital credential again. This service enables agencies to obtain a single digital signature to facilitate business-user access to multiple secure websites.

Timestamping: VANguard's timestamping service provides independent, verifiable electronic evidence of the date and time of an electronic transaction. This service enables agencies to gain an authoritative and defensible timestamp for a business transaction and to securely store the transaction record.

Security token service: This service enables agency systems and business systems to conduct secure online transactions. Agencies and businesses obtain security tokens from VANguard to enable authentication. VANguard has undertaken high-level design of this service and is investigating its feasibility.

Standard Business Reporting (SBR) program

SBR is a multi-agency initiative that will simplify business to government reporting by:

- making forms easier to understand
- using accounting/record keeping software to automatically pre-fill government forms; and
- introducing a single secure way to interact on-line with participating government agencies

Government agencies participating in the SBR program include the Australian Treasury, Australian Bureau of Statistics (ABS), Australian Prudential Regulation Authority, Australian Securities and Investments Commission, Australian Taxation Office (ATO) and all state and territory government revenue offices.

SBR is focusing on financial reporting first, since this set of forms affects most businesses. Some examples of forms include the ATO's Business Activity Statement and the ABS' Quarterly Business Indicators Survey.

Major work being undertaken in the lead-up to the 2010 SBR implementation include:

- the standardisation of reporting terms
- development of a reporting taxonomy using XBRL (XBRL is an XML-based open standard language specifically designed to improve electronic communication of financial data)
- the standardisation of relationships between accounting terms and information reportable to government
- the mapping of reporting rules and relationships to a business's account within their record-keeping system
- the development of SBR core services
- connecting government agency systems to the core services; and
- education and two-way communication with business, software developers and business intermediaries.

Schedule A: Registration approaches

Schedule A1: Registration of individuals and individuals as representatives of organisations.

Registration strengths will vary depending on whether the particular e-Authentication solution is operating as part of a closed community of interest or as part of a wider federated identity implementation. Reliance on initial registration processes (and therefore issued credentials) will require the relying agency to have a good understanding of the registration models employed.

The guidance provided below is indicative only.

Registration basis	Registration requirements by registration strength			
	Level 1	Level 2	Level 3	Level 4
Evidence of identity (EoI) basis	None	Provision of images of documents from the Gatekeeper EoI Policy PoI Framework Policy: – One Category B document – Two Category C documents	"General" Gatekeeper requirements	Gold Standard Enrolment Framework (GSEF)[11] "High-assurance" Gatekeeper requirements
Known customer basis	None	Evidence of existing relationship with agency. Activation of credential requires successful responses (by the user) to agency challenges regarding shared information.	"General" Gatekeeper requirements	Not Applicable

[11] The GSEF is an element of the National Identity Security Strategy see http://www.ag.gov.au.

Schedule A2. Registration of authorised representatives

Authorised representatives may act on behalf of either individuals or businesses. Registration models for authorised representatives may follow all or only some of the following steps:

The guidance provided below is indicative only.

Registration basis	Registration requirements by registration strength			
	Level 1	Level 2	Level 3	Level 4
Evidence of identity (EoI) basis for individual to be represented (Principal)	Not applicable	Provision of images[12] of documents from the Gatekeeper EoI Policy, PoI Framework Policy: – One Category B document – Two Category C documents	"General" gatekeeper requirements	GSEF "High-assurance" Gatekeeper requirements
EoI basis for representative	Not applicable	Provision of images of documents from the Gatekeeper EoI Policy, PoI Framework Policy: – One Category B document – Two Category C documents	"General" Gatekeeper requirements	GSEF "High-assurance" Gatekeeper requirements
Evidence of authority to act as a representative	Not applicable	Activation of representative credential requires successful responses to two shared information challenges in respect to the Principal	Provision of legally enforceable document attesting to the authority	Face-to-face provision of legally enforceable document attesting to the authority

[12] Agency discretion should apply in relation to acceptance of an "image of a document" or the original of that document

Schedule B: Authentication mechanisms

Standard credential types

Memorised password (either issuer-provided or subscriber-generated)

A traditional password or secret that is shared between the credential issuer and the subscriber.

User-supplied shared information (also referred to as "shared secret")

This credential is a set of challenges and responses typically established by the subscriber and managed by the credential issuer. They typically take the form of a question to which the answer is a "secret" held by the subscriber.

Context-specific shared information

Context-specific shared information differs from the user-supplied shared information in that the challenge is based on information pertaining to the relationship between the relying party and the subscriber.

Code book

A code book may be held on a physical or electronic device and may be accessed sequentially or via a challenge mechanism (coordinates in a matrix, page reference etc.) to provide an authentication code. This authentication code can be strengthened by the introduction of a diversification method based upon a shared secret or other means.

Pre-registered origin

A pre-registered origin of the subscriber connection can be provided through caller-id, IP addresses and potentially other means.

Call back to pre-registered address

Out-of-band credentials provide for the delivery of a secret to a subscriber for subsequent presentation to the verifier. Examples of out-of-band channels include telephone voice channel/IVR, mobile SMS and email.

Software cryptographic credential (soft certificate)

Software cryptographic credentials involve the storage of a cryptographic key, usually based on public key cryptography, within software on the subscriber's connecting device (e.g. a personal computer) and protected by a password. The cryptographic key (once unlocked by the password) is used to generate an authentication code.

One-time password (OTP) device

An OTP device is a specialised hardware device that displays an OTP which is calculated within the device based on a secret shared with the credential issuer. OTP devices may require a PIN to be submitted to activate the device to generate an OTP.

Challenge–response device

A challenge–response (C-R) device is a hardware token that generates a password/ passcode based upon information keyed into the device which is provided by the organisation/application seeking to authenticate the user. C-R devices may require a PIN to be submitted to activate the device to generate the response.

CAPTCHA

A CAPTCHA is a type of challenge–response test used to ensure that the response is not generated by a computer. This is sometimes referred to as a reverse-Turing test.

Grid authentication

Grid authentication provides organisations a means to implement simple, effective, two-factor authentication by leveraging a security grid card. Users receive a security grid that contains a series of numbers and letters in easily marked columns and rows. These security grids can be delivered to users as credit card-sized cards, or printed on the backs of access badges, credit or ATM cards, or even printed on billing statements and other confidential communications.

Hardware cryptographic device (hard certificate)

A hardware cryptographic device is a specialised device that generates an authentication code cryptographically based on data input to the device. Input information may be "challenge" information provided by the relying party, transactional information, or hash information. The input data can be entered through a device keypad or through a computer interface such as a USB port or smartcard interface. Typically these devices are PIN-protected.

Biometric credentials

Biometrics (as authentication credentials in themselves) are considered unsuited to the authentication of external parties where the biometric capture facilities are outside the direct governance and control of relying party government agencies.

The exception to this is voice authentication, which is maturing rapidly as basic authentication method.

Biometrics might also play an important part as a second or third factor relating to use of a hardware cryptographic device, such as a smartcard, as a means of gaining access to the device within the subscriber's environment.

Hybrid subscriber authentication mechanisms

The term "hybrid authentication mechanisms" refers to the use of two or more credentials in combination in order to increase the effective level of strength of the authentication process. The credentials can be of the same factor or different types of factors.

As a general rule, increasing strength across levels can only be achieved by combining credentials of different factors. In other words combining two "what you know" credentials may not be sufficient to increase authentication strength across levels whereas the combination of a "what you know" credential and a "what you have" credential would be sufficient.

Notwithstanding the above, an increase in the authentication process assurance within a level can be achieved by combining like factor credentials (e.g. two "what you know" credentials), and such approaches are being used increasingly in adaptive and context-based authentication methods within industry and government.

Adaptive authentication mechanisms

Adaptive authentication mechanisms are typically very structured in their use of various credentials, based on dynamic risk assessment, including consideration of location of the subscriber, time since last visit, consistency with prior interaction patterns etc. As such, the benefits and appropriateness of this approach need to be determined within the specific business context and an overarching threat and risk assessment of the business system.

Schedule B1: Credential strength

Note that the information provided in this Schedule is **indicative** only and should be used as input to an agency's overall e-Authentication assessment.

Note: The strength of these credentials may be reduced over time as a result of developments in technology. Regardless of the strength, there are vulnerabilities with each credential type, and agencies should research and factor into risk assessment.

Credential	Factors	Use	Variables affecting strength of credential	Strength of credential			
				Level 1	Level 2	Level 3	Level 4
Memorised password	Know	Subscriber authentication	Ability to guess: – password length and character set – password lifetime – invalid-password strategies – password storage – password entry tools	✓ The probability that an attacker can guess a valid authentication code over the lifetime of the credential is less than xx	✓ The probability that an attacker can guess a valid authentication code over the lifetime of the credential is <yy Credential issuer blocks subscriber account after successive invalid submissions	×	×
User-supplied shared information	Know	Step-up authentication. Credential management e.g. PIN reset on OTP device	Size of information set Invalid-response strategies	✓ The probability that an attacker can guess a valid authentication code over the lifetime of the credential is less than xx	✓ The probability that an attacker can guess a valid authentication code over the lifetime of the credential is less than yy Credential issuer blocks subscriber account after successive invalid	×	×

Credential	Factors	Use	Variables affecting strength of credential	Strength of credential			
				Level 1	Level 2	Level 3	Level 4
					submissions		
Context-specific shared information	Know	Step-up authentication Credential management e.g. PIN reset on OTP device Enrolment	Predictability of shared information by known parties. Invalid-response strategies	✓	✓ Credential issuer blocks subscriber account after successive invalid submissions	×	×
Code book	Know Have	Subscriber authentication	Physical security of Code book Ability to guess: – code length and character set – code book lifetime – invalid-code strategies	✓ The probability that an attacker can guess a valid authentication code over the lifetime of the credential is less than xx	✓ The probability that an attacker can guess a valid authentication code over the lifetime of the credential is less than yy Authentication code diversification through shared secret Credential issuer blocks subscriber account after successive invalid submissions	✓ The probability that an attacker can guess a valid authentication code over the lifetime of the credential is less than zz. Authentication code diversification through shared secret.	×
Pre-registered origin - caller-id	Have	Subscriber authentication	Management of changes to pre-registered addresses	✓	×	×	×

Credential	Factors	Use	Variables affecting strength of credential	Strength of credential			
				Level 1	Level 2	Level 3	Level 4
- IP address							
Call back to pre-registered address: voice SMS OTP email OTP	Have	Subscriber authentication	Management of changes to pre-registered addresses Evidence of subscriber's custody of the address/channel	✓	✓	✓ When combined with memorised password.	×
Voice biometric	Are	Subscriber authentication	Technology maturity	✓	✓	×	×
Software cryptographic credential Symmetric key	Know (Have)	Subscriber and transaction authentication	Management of keys in software Key length and algorithms Credential passcode policy Invalid-code strategies Key rollover strategies	✓	✓	✓ Each authentication requires PIN entry. Clear text keys destroyed after use. Algorithm complies with xx standards. Credential issuer blocks subscriber account after successive invalid submissions.	×
Software cryptographic credential	Know (Have)	Subscriber and transaction authentication	Management of keys in software Key length and	✓	✓	✓ Cryptographic processor shall comply with xxx.	×

Credential	Factors	Use	Variables affecting strength of credential	Strength of credential			
				Level 1	Level 2	Level 3	Level 4
Asymmetric keys		Non repudiation	algorithms Credential passcode policy Invalid-code strategies Certificate rollover strategies			Each authentication requires PIN entry. Clear text keys destroyed after use. Algorithm complies with xx standards. Credential issuer blocks subscriber account after successive invalid submissions.	
ne-time password (OTP) device	Know Have	Subscriber authentication	Algorithm used and data used in OTP generation – time- or event-based Length of time OTP is valid Key length Tamper-resistance of device PIN activation required Invalid-code strategies	✓	✓ Cryptographic processor shall comply with zzz Time- or event-based algorithm No PIN required Credential issuer blocks subscriber account after successive invalid submissions.	✓ Cryptographic processor shall comply with xxx. Time-based algorithm with OTP valid for less than two minutes only. PIN activation of device through integrated keypad. Device locks after multiple invalid PIN entries Credential issuer blocks subscriber account after successive invalid submissions.	

Credential	Factors	Use	Variables affecting strength of credential	Strength of credential			
				Level 1	Level 2	Level 3	Level 4
						Credential issuer completes symmetric key cryptographic functions in hardware security module (HSM) with keys not exposed outside of HSM.	
Hardware cryptographic device Symmetric Key	Know Have Are	Subscriber and transaction authentication	Algorithm Key length Tamper-resistance of device PIN activation required Invalid-code strategies	✓	✓ Device cryptographic processor shall comply with xxx Variable data input through device key pad PIN or biometric activation of device through integrated keypad Device locks after multiple invalid PIN /biometric entries Credential issuer blocks subscriber account after successive invalid submissions	✓ Device cryptographic processor shall comply with xxx. Variable data input through device key pad. PIN or biometric activation of device through integrated keypad. Device locks after multiple invalid PIN /biometric entries. Credential issuer blocks subscriber account after successive invalid submissions. Credential issuer completes symmetric key cryptographic functions in HSM with keys not	✓ Device cryptographic processor shall comply with xxx. Variable data input through device key pad. PIN or biometric activation of device through integrated keypad. Device locks after multiple invalid PIN /biometric entries. Credential issuer blocks subscriber account after successive invalid submissions. Credential issuer completes symmetric key cryptographic

Credential	Factors	Use	Variables affecting strength of credential	Strength of credential			
				Level 1	Level 2	Level 3	Level 4
						exposed outside of HSM. The HSM should comply with nnn.	functions in HSM with keys not exposed outside of HSM. The HSM should comply with nnn.
Hardware cryptographic device Asymmetric key	Know Have Are	Subscriber and transaction authentication Non-repudiation	Algorithm Key length Tamper-resistance of device PIN activation required Invalid-code strategies	✓	✓	Device cryptographic processor shall comply with xxx. PIN or biometric activation of device. Device locks after multiple invalid PIN /biometric entries. Credential issuer blocks subscriber account after successive invalid submissions.	Device cryptographic processor shall comply with nnn. PIN or biometric entry required through independent (from personal computer) device interface – e.g. reader PIN PAD for smartcards. Device locks after multiple invalid PIN /biometric entries. Credential issuer blocks subscriber account after successive invalid submissions.

Schedule B2: Credential management and usage

Note that the information provided in this Schedule is **indicative** only and should be used as input to an agency's overall e-Authentication assessment.

Processes	Variables affecting strength of mechanism	Strength of authentication mechanism			
		Level 1	Level 2	Level 3	Level 4
Credential generation	Credential / key generation techniques			Cryptographic keys should be generated using Hardware Security Modules (HSM) selected from the DSD Evaluated Products List.	Cryptographic keys should be generated using Hardware Security Modules (HSM) selected from the DSD Evaluated products List.
Credential issuance and activation	Method of delivery of credentials to subscribers Method of activation of credential		Credentials should be delivered to subscribers through a secure channel	Credentials should be delivered to subscribers through a secure channel. Credentials should be delivered to subscribers in a locked state.	Credentials should be delivered to Subscribers through a secure channel incorporating evidence of receipt. Credentials will be delivered to Subscribers in a locked state
Activated credential management — revocation — re-issuance — suspension — unlocking	Time lapse between advice of loss of a credential and reflection of this in verifier and credential-issuer systems			Revoked credentials should be reflected in CRL or similar method within xx minutes of authenticated request for revocation by the subscriber. Locked credentials should require an unlock code to reset the PIN.	Revoked Credentials should be reflected in CRL or similar method within yy minutes of authenticated request for revocation by the subscriber. Locked credentials should require a cryptographically generated single use, and credential specific unlock code to reset the PIN.
Credential verification	Method of storage of		Passwords and	Credential issuer completes	Credential issuer completes

Processes	Variables affecting strength of mechanism	Strength of authentication mechanism			
		Level 1	Level 2	Level 3	Level 4
	passwords and cryptographic keys by the credential provider		cryptographic keys should be held by the credential issuer in a salted and hashed state. Communications between a relying party, the verifier and the credential issuer should be through a protected channel	symmetric key cryptographic functions in HSM with keys not exposed outside of HSM. Communications between a relying party, the verifier and the credential issuer should be through a protected channel with cryptographically-based cross authentication of the communicating parties.	symmetric key cryptographic functions in HSM with keys not exposed outside of HSM. Communications between a relying party, the verifier and the credential issuer should be through a protected channel with HSM-based cross-authentication of the communicating parties.
Authentication event logging	Methods of protection of event logs against tampering		All credential lifecycle events should be logged Log files should be retained for xx years	All credential lifecycle events should be logged. All authentication events should be logged. Log file records should be cryptographically protected against modification, deletion and addition of log file records. Log files should be retained for yy years.	All credential lifecycle events should be logged. All authentication events should be logged. Log file records should be cryptographically protected, using an HSM, against modification, deletion and addition of log file records. Log files should be retained for yy years.