Australian Government

Digital Transformation Office

National e-Authentication Framework

Better Practice Guidelines – Vol 1 Identity e-Authentication

January 2009

Disclaimer

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

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

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

ISBN 0 9758173 7 X

Department of Finance and Deregulation
Australian Government Information Management Office

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Copyright: Department of Finance and Deregulation

Contents

FIGURES

TABLES

1. Introduction

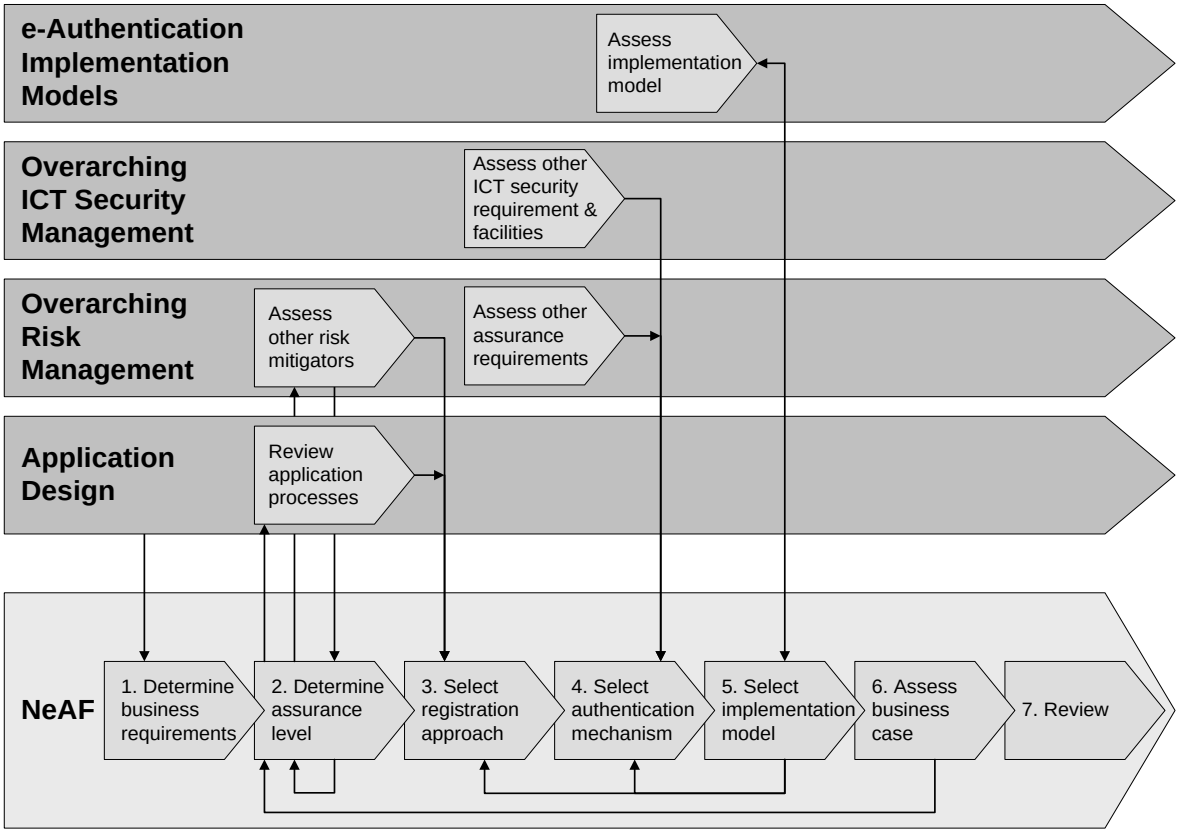
This volume provides guidance on the usage of NeAF for the determination of e-Authentication approaches where the assertion to be authenticated is the identity[1] of users of government online services.

A set of supportive *Checklists, Explanations and Templates* is provided as a separate document.

1.1. Background

The standardised NeAF process for determining the strength of e-Authentication required and the e-Authentication approach to be adopted is illustrated in Figure 1 below.

Figure 1: NeAF process



This figure illustrates that determining 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 overarching risk management and information security management regimes.

1 Note that assertions other than identity are also able to be addressed using the NeAF.

1.2. Purpose

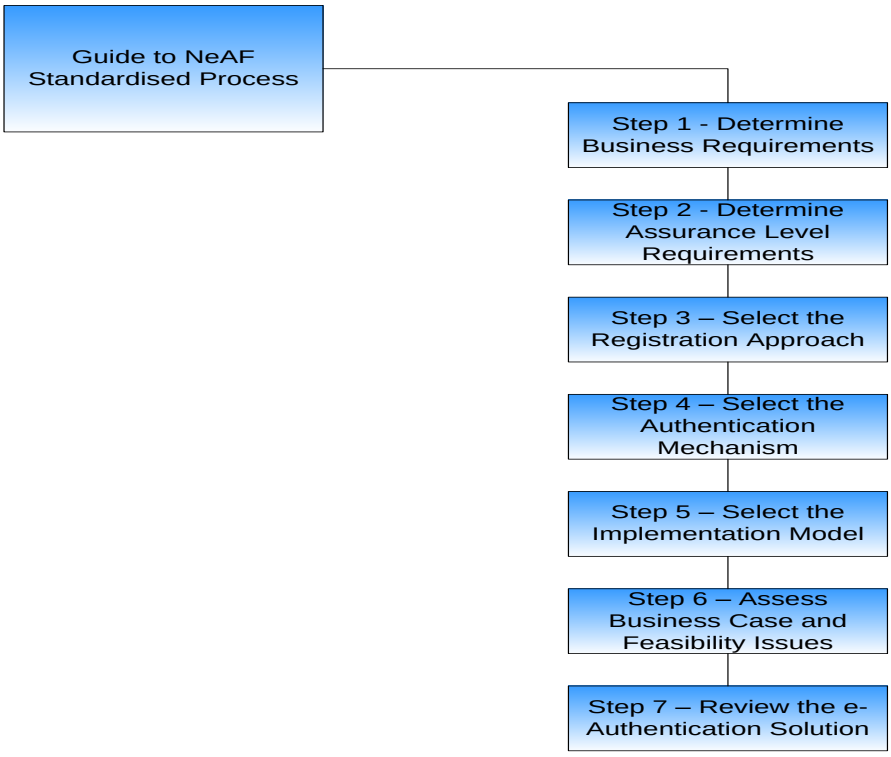
The volume will assist agencies to:

- **identify the business requirements for e-Authentication of their users, including assessing relevant privacy and public policy implications**
- **determine the assurance levels for e-Authentication**
- **select an appropriate registration approach for that assurance level**
- **determine an e-Authentication mechanism for that assurance level**
- **select an implementation model** for their approach to e-Authentication
- develop a business case and feasibility for their approach to e-Authentication
- review their e-Authentication solution.

1.3. Process Summary

Figure 2 below illustrates the steps required for the determination of e-Authentication requirements and development an e-Authentication solution.

Figure 2: Methodology



Preparation: Prior to the commencement of the project, an initial preparation step must be undertaken to establish project governance and the project team, ensuring that key participants familiarise themselves with applicable government and agency policy and strategy positions and identify the business, technology, policy, legal and economic framework within which the

e-Authentication approach will be developed and tested[2]. This lays the groundwork for the subsequent project activities.

The methodology for the project itself involves seven steps:

1. **Determine Business Requirements:** Consider a range of factors, in particular whether the transaction or transaction cluster under consideration requires authentication of a user's identity.
2. **Determine Assurance Level Requirements.** Apply a standardised risk management approach to the determination of threats and risks associated with the transaction or transaction cluster. The determination of the e-Authentication assurance level, which guides the selection of the e-Authentication solution, is dependent upon assessing the residual risk associated with the transaction – i.e. that remaining after other risk mitigation controls have been applied.

> An online Risk Assessment Tool is provided as an adjunct to the Better Practice Guidelines to assist with this process – contact AGIMO authentication@finance.gov.au.

3. **Select the Registration Approach.** Registration is the act of establishing the digital identity in the agency's authoritative identity register/directory and associating an e-Authentication credential with that identity. The registration approach is dependent upon the e-Authentication assurance level required, and the nature of the intended user-base. Three categories of users are considered: known customers (i.e. known either to the agency or, possibly, to another agency), unknown users who need to be identified, and pseudonymous users.

Consideration should be given at this stage to existing whole of government or sectoral authentication solutions that would allow end-users to re-use existing credentials. Consideration could also be given to the scope for use of non-authentication based solutions to mitigate identity related risks

4. **Select the Authentication Mechanism and Credential Management Approach.** The mechanism represents the technology base for the user's credential[3]. The credential management approach relates to the level of trust in the environment and processes associated with creating, issuing, managing and revoking user credentials.
5. **Select the e-Authentication Implementation Model.** A spectrum of implementation approaches are possible, ranging from agency or application centric siloed approaches through to centralised whole-of-government or whole-of-sector schemes. These are differentiated by a range of convenience, cost, usability and risk factors (see Volume 3 of the Better Practice Guide).
6. **Assess the Business Case and Feasibility of the e-Authentication Implementation Model**. This involves using *ICT Business Case Guide and Tools*[4] to model costs and benefits to financially justify the implementation of the e-Authentication approach.
7. **Review the e-Authentication Solution.** Test the proposed e-Authentication solution against the NeAF's e-Authentication principles.

---

2 If an e-Authentication Strategy has been developed, along the lines of that proposed in Volume 4 of the *Better Practice Guidelines*, this will already have addressed most issues and devised appropriate responses.

3 The term 'technology' is used here in a general sense, as it may represent everything from a user's memory (e.g. for a password) through to an electronic token.

4 See http://www.finance.gov.au/budget/ict-investment-framework/business-case-guide.html.

2. Preparation

2.1. Purpose

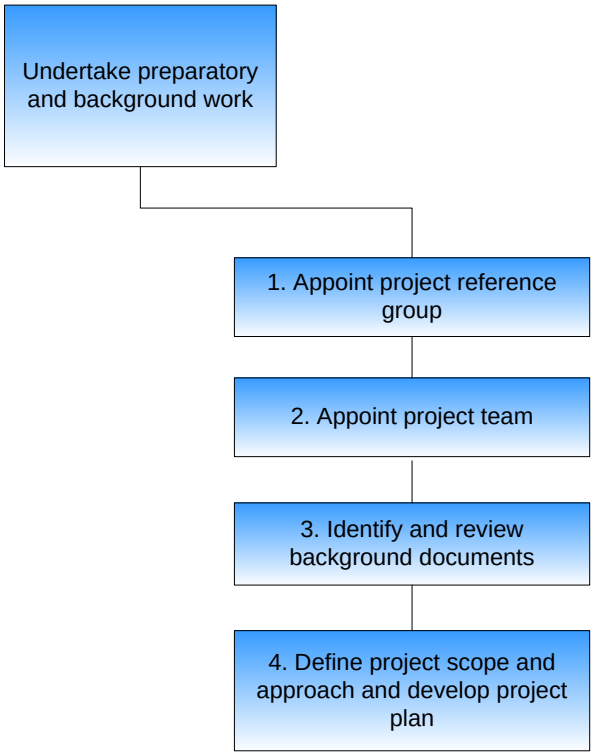
This step involves the establishment of the project reference group and team, the gathering together of pre-existing intelligence, and project planning.

The tasks mirror those outlined for the preparation of an e-Authentication Strategy (see BPG Volume 4), however it is anticipated that the scale, formality and timeframes will be significantly lower.

2.2. Overview of Methodology

Figure 3 below illustrates the key tasks involved in this stage.

Figure 3: Tasks covered in initial Preparation



2.3. Tasks

An outline of the key tasks is as follows:

1) Appoint project reference group

This should encompass at least executives who have responsibility for:

- The service/s for which electronic transactions are to be deployed
- ICT
- Legal and privacy matters; and
- Finance and administration.

2) Appoint project team

This should include:

- senior representatives of business and technology owners/managers of the proposed electronic transactions
- ICT security and enterprise risk management functions; and
- senior legal and privacy staff.

3) Identify and review background documents.

Determine government and agency policy positions that are relevant to e-authentication[5] including:

- core government information and ICT security policy positions (e.g. PSM and ISM) and the legal and policy positions pertaining to privacy assessment and management
- NeAF policies and principles; and
- agency based documentation:
  - business strategies/plans and core policy principles
  - ICT strategic plan and development/maintenance schedule
  - ICT/Information security policies (with guidelines and standards) where applicable
  - identity and access management plans, policies, guidelines
  - privacy management policies.

4) Define project scope and develop project plan

The scope of the project will encompass consideration of:

- enterprise scope – is the scope restricted to a single business unit or organisation, or is it enterprise-wide or even multi-organisational in scope
- scope of transactions – some or all transactions related to a given application or cluster of applications; and
- scope of user-base – all users of the specified transactions or only particular user-groupings.

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

[5] If an e-Authentication Strategy has been developed then few if any of the documents described above will be required.

It is suggested that at the start of the project an agency takes a copy of *CET1-Checklist to Analyse Compliance with NeAF Principles*, and uses that throughout the process to inform all actions and assessments. The final Step of this process is to review project objectives against these principles, and it is suggested that the principles are introduced early in the process to prevent any major departures.

3. Step 1: Determine the Business Requirements

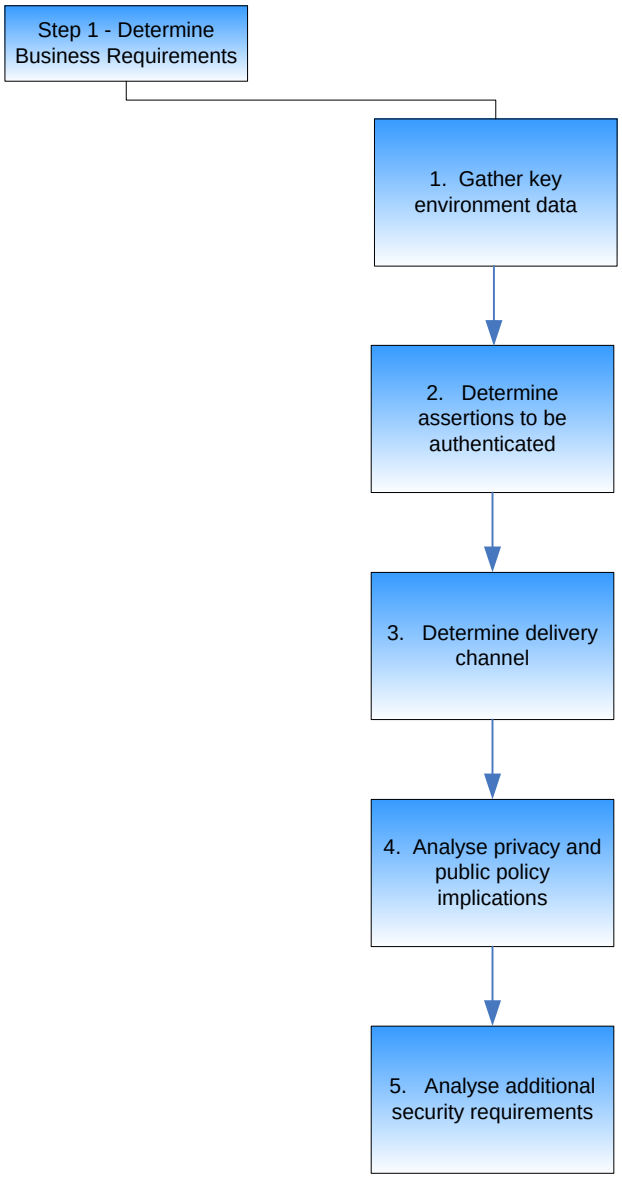
3.1. Purpose

The major objective of Step 1 is to identify key contextual factors that will need to be considered throughout the remaining steps of the evaluation.

3.2. Overview of Methodology

Figure 4 below shows the tasks involved in determining the business requirements for e-Authentication that are covered in Step 1.

Figure 4: Tasks covered in 'Determine Business Requirements' Step



3.3. Tasks

1) Gather key environment data

To analyse its e-Authentication needs and design e-Authentication measures, an agency will need to gather information on:

- the volumes of relevant transactions. This is necessary to determine business case, logistics and system sizing
- the categories of direct users, (including, staff, contractors, staff and contractors of partner organisations, customers, etc.) and number of such users. This is necessary to assess the capability (technical, economic, etc) of users to conduct electronic transactions and to understand and harness the e-Authentication approach/s evaluated
- other agencies involved in servicing the user base/s for the same or similar purposes, and the status of their online initiatives. This will assist in determining the e-Authentication implementation model to be adopted – e.g. it may be possible to use a federated approach if users have an existing e-authentication credential from another agency
- the categories of indirect users, and number of users (that is, people or organisations that are affected by the system, even if they do not use it). This is necessary to determine the scope and size of implementation efforts including process re-engineering, publicity/outreach
- the number of locations involved. This will assist with the sizing and scoping of the solution, as well as being necessary for costing purposes
- other security requirements – see task 5 below.

CET2-Transaction Analysis Checklist may be used to catalogue the results of the above.

2) Determine the assertions to authenticate

Differing electronic transactions will require the authentication of differing assertions. An assertion is a statement that declares that one or more alleged facts are true. Common assertions include identity, role, value and agency. Other assertions may include location, qualification, age, membership, nationality, etc.

The NeAF is primarily concerned about identity related assertions as they represent the most common assertions to be authenticated in electronic services.

> While the NeAF process is suited to the determination of assurance level requirements and some aspects of the e-authentication solutions for non-identity based assertions, the registration approaches and implementation models are explicitly tailored for identity-based authentication.

Identity e-authentication is driven by the need to ensure that the requesting party:

- has proper rights to access the requested information; and
- has the proper authority to complete the requested transactions.

In many ways the first need is more critical insofar as once information has been divulged it cannot be readily retrieved (although its use can potentially be suppressed), whereas there are generally mechanisms (technical and commercial) to unwind executed transactions.

Transactions that have one or more of the following profiles are seen as requiring authentication of identity:

- The proposed transaction involves:
  - collection of personal information
  - disclosure of personal information
  - collection of organisational information; or
  - disclosure of organisational information.
- The transaction requires personal attestation because the person, either on behalf of themselves an organisation or another person, is:
  - making a claim or application for funds or services; or
  - submitting a return or declaration which requires attestation.
- It is necessary to determine whether the user is an already established user for the sake of having a persistent 'conversation' in which non-public information is to be exchanged – e.g. whistleblower hotline, or anonymous health or welfare advice line. In this case no personal identifying information is collected, but a pseudonym will need to be chosen, and authenticated in subsequent interactions

The approaches to registration and e-authentication will depend upon the nature of the assertion to be authenticated. The most common instances are registration of individuals:

- as themselves
- as representatives of organisations; or
- as representatives of other individuals.

CET3-Checklist to help determine whether identity e-Authentication is required may assist an agency determine whether the electronic service requires identity e-authentication.

3) Determine delivery channel/s

The main electronic service delivery channels are telephone and computers[6]. Computers may be used on internal networks which may be secure, or across insecure external networks such as the internet. Different e-Authentication solutions are likely to be required for each. Agencies will generally be required to facilitate multiple delivery channels and thus be required to support a number of authentication solutions (not all necessarily electronic in nature). In such circumstances the agency will also have to ensure that mechanisms are in place to coordinate users having multiple credentials, each for a different channel.

The nature of the delivery channel will determine the suitability of the e-Authentication mechanism.

Agencies can use *CET4-Checklist to analyse Delivery Channels* to collect the information needed to decide how the proposed delivery channels are best served by e-authentication.

4) Identify privacy and user impact implications

This step represents a preliminary privacy and user impact review. During this step agencies should determine whether any privacy and user impact issues are likely to arise in relation to e-authentication.

6 While facsimile also represents an example of an electronic channel, e-authentication is more problematical in that a facsimile is essentially an electronic version of a paper based document hence authentication would rely on confirmation of the sending machine and the signature (or other "identifier" on the transmitted document.

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

Privacy issues include:

- whether the nature of the transaction warrants the authentication of identity, particularly where the form of identity to be authenticated is tightly coupled with a human entity. Privacy principles require that personal information not be collected unless the information is necessary for agency functions or activities
- whether and to what extent personal information will be collected as part of the registration process. Also, what aspects of this information will be stored, for how long and under what security and governance regimes.
- the extent to which audit trails covering user activities will be collected, stored, and used; and
- Whether identifiers will be allocated to users and the extent to which these will be used across applications and, in some cases, across organisational boundaries.

The assessment of privacy issues will be framed by the *Privacy Act 1988* in the case of Australian Government agencies, and various jurisdictionally-based acts and/or policy positions for state and territory governments.

CET1-Checklist to Analyse Compliance with NeAF Principles, and in particular the checklists applying to NeAF principles 6-8 will assist in this regard.

Early consideration of these issues is intended to guide considerations made during the entire NeAF process. In the final step of this process – Review the e-Authentication Solution – a more formal consideration of these issues will have to be undertaken.

5) Identify additional security requirements

A number of security requirements in addition to authentication may apply to the transaction under evaluation. These may include:

- the requirement for confidentiality of information passing across the electronic channel
- ensuring the integrity of transactions or instructions submitted via the electronic channel; this is often referred to as transaction authentication and aims to assure that the transaction or instruction has not been modified maliciously, or accidentally whilst in transit; and
- the requirement to limit as far as is possible the ability of the user to repudiate a transaction.

While e-Authentication does not provide a solution to these requirements, it may be possible to leverage the underlying e-Authentication processes and technologies to assist with a solution.

Whilst NeAF focuses predominantly on the authentication of the identity of the subscriber, some e-Authentication mechanisms may also provide levels of assurance in respect to other security attributes, as well as support confidentiality of exchanged information.

As such the broader authentication requirements of the channel, beyond identity authentication, should be considered when selecting an identity authentication mechanism.

The ultimate use of identity authentication credentials for broader purposes, including the support of confidentiality, should be considered as part of the credential selection process and as an element of overall delivery channel security design.

The final column of *CET2 – Transaction Analysis Checklist* may be used to capture this information.

4. Step 2: Determine the Required Assurance Level

4.1. Purpose

The objectives of the tasks described in this part are to determine the level of assurance required for an electronic transaction (or cluster of transactions). This translates directly into the assurance level required for authenticating a user.

4.2. Overview of Methodology

Figure 5 below shows the tasks involved in evaluating the transaction assurance levels required.

Figure 5: Tasks covered in the 'Determine Assurance Level' step

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

4.3. Who should undertake the risk assessment?

The risks associated with electronic transactions span business and technology areas. Agencies should assess risks on a group basis, with groups encompassing key stakeholders such as:

- business application owners
- security policy and operational staff
- legal staff
- privacy advisers and other 'customer-advocacy' type staff; and
- solution architects.

4.4. Tasks

The first step in determining the assurance level is to undertake a Threat/Risk Assessment for each transaction. A standards-based (AS/NZS 4360) risk assessment approach is required, where agencies examine the threats and risks associated with the proposed transaction together with the mitigating factors or safeguards that will reduce the likelihood or consequences associated with the risks.

A synopsis of one such approach to assessment is detailed below:

1) Establish or refine the risk management strategy

In general, agencies will already have a risk management strategy that applies to the business processes in question. If so, this needs to be reviewed, and possibly refined; and if not, a risk management strategy needs to be established.

Agencies can adopt alternative approaches to each threat, including:

- **proactive strategies**, such as avoidance, deterrence and prevention;
- **reactive strategies**, such as detection, recovery and insurance; or
- **non-reactive strategies**, such as tolerance and 'graceless degradation'.

Accepting a non-reactive strategy means an agency will bear the cost of the residual risk. This approach is rational if the cost of possible losses the agency is willing to countenance is appropriately balanced against the savings delivered by, for example, not implementing expensive safeguards, or migrating users to lower cost electronic channels.

Devising a risk management strategy involves selecting a mix of measures that reflect the outcomes of the preceding threat and risk assessments. These measures are likely to include technical safeguards, policies and procedures, a documented security plan, resources to implement it, controls to detect security incidents and resolve these, and audit processes.

2) Determine the type of threats

Agencies need to evaluate the threats associated with incorrect or invalid e-authentication.
In evaluating the threat, mitigating factors and existing safeguards should be ignored.

Agencies should consider a wide range of threats. These include the actions of internal and external users, persons with vested personal or financial motives to compromise information or commit fraud, hackers etc. Accidental and intentional threats should be treated separately.

Table 1 below contains a list of suggested categories of harm. These are intended to provide guidance rather than be prescriptive, and an agency may wish to add to or delete from the list to suit particular agency circumstances.

Table 1: Categories of Harm and Description of Impacts/Consequences

Category of harm	Description of impacts
Financial	Financial loss by any party
Performance	Adverse impact on the performance of any party's functions
Productivity	Adverse impact on the productivity of any party
Public confidence	Adverse impact on the confidence with which any party regards the relevant business processes
Reputation	Adverse impact on the reputation of any party
Health and safety	Adverse impact on the health or safety of any person
Confidentiality	Inappropriate access to or dissemination of confidential data relating to any party
Privacy	Adverse impact on the privacy of any person, their behaviour, their communications or their personal data
Disciplinary or corrective actions	Impacts that adversely affect the agency by causing or resulting in disciplinary or corrective actions
Regulatory and legislative compliance	Impacts that adversely affect the agency's ability to comply with regulations and legislative requirements
Fines and legal penalties	Impacts that adversely affect the agency by causing or resulting in fines or legal penalties

Agencies should record the type of threats associated with each business process or transaction in *CET5-Risk Analysis Form.*

3) Assess the likelihood and consequences of threats

Key risk areas associated with electronic transactions with individuals and businesses can be grouped under the following headings:

- fraud/theft
- privacy breach (deliberate or accidental)
- public safety breach; or
- repudiation of transactions.

Certain classes of transaction, particularly those associated with classified information (whether national security classified or not), involve additional risks including potential compromise/breach of national security.

Determining the consequences of threats requires an identification of the associated risks, as outlined above, coupled with an assessment of the probability of occurrence and the seriousness of the consequences from the perspective of all stakeholders. Agencies should undertake this cataloguing and assessment on a group basis, with all key stakeholders represented in making the final evaluation.

It is important that agencies consider the impacts of all of the following:

- **single instances**, that is, one-off accidents or 'attacks', usually on a small scale and impinging upon or exploiting weaknesses in agency processes
- **systemic accident or serial abuse**, which involves multiple single instances over a period of time. While the consequences of each instance may be small, the cumulative impact may be significant; and
- **large-scale accident or mass attack**. The impacts of some kinds of accidents may result in very substantial harm, for example, the loss of a complete disk, or the theft of an off-site backup containing all data in readily accessible format. A mass attack involves deliberate large-scale attack (for example, for fraud purposes), undertaken so rapidly that after-the-fact processes will not provide an effective remedy. Such attacks may exploit both weaknesses in agency processes and the inherent anonymity, speed and ease of replicating online systems.

Some of the questions agencies should ask are:

- Who are the likely internal and external parties who may constitute a threat? This could include dissatisfied clients or disgruntled or unethical employees.
- How many users will have access to online systems through each type of delivery channel? For example, access may be via secure networks internally, but via insecure networks such as the Internet externally. How many of these users could be parties who may constitute a threat?
- How many transactions are expected to flow through the system each day? How many of these could come from a party who may be a threat?
- How attractive is the online system to a party who is a threat? What could they do through the system (use or misuse) that could have an adverse impact on the agency, or may further the ends of the user?
- How skilled are the parties who constitute a threat likely to be? How easy would it be for them to achieve something that would have an adverse impact on the agency, or may further the ends of the user?
- On balance, considering all the factors above, what is the consequence of the threat occurring, and how frequently is the threat likely to occur?

Record the likelihood and consequences of threats associated with each business process or transaction in *CET5-Risk Analysis Form.*

4) Assess existing risk mitigation factors

The term **mitigation factors** refers to all aspects of the process, infrastructure and context that tend to reduce the probability of the threat occurring, or reduce the consequences of the threat should it eventuate.

Some mitigating factors are accidental or incidental. For example, there may have been no known instances of a threatening event, or there may be a lack of motive for attackers (e.g. the online system may not be attractive to them).

Mitigating factors that are designed into the infrastructure or processes are referred to as **safeguards**. Safeguards may be strategic in nature (for example, hiring staff with appropriate educational background) or tactical (for example, inspecting logs after a suspicious incident).

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

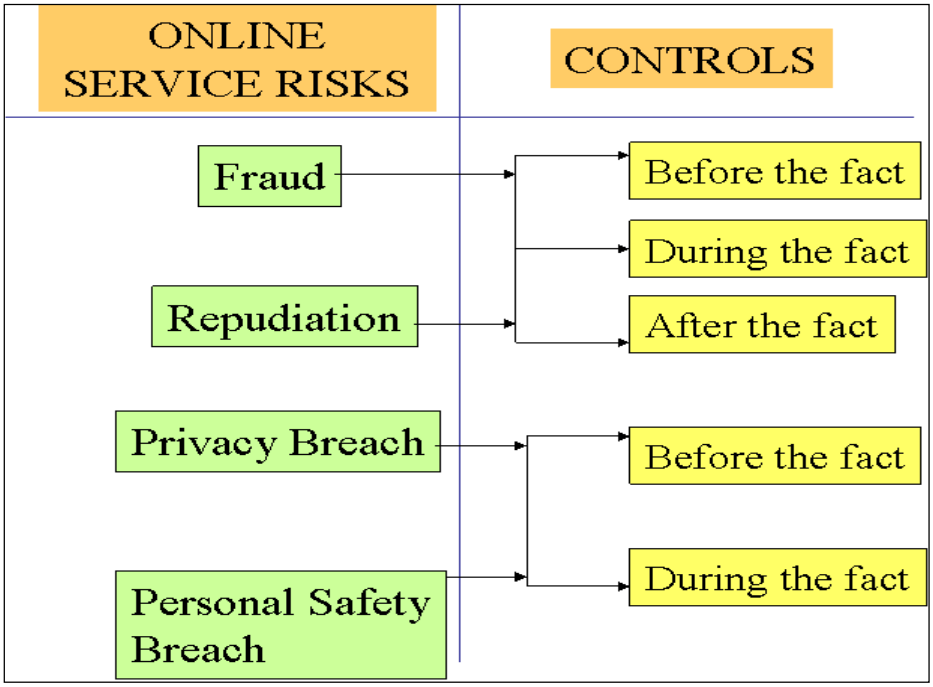
It is important to consider risk mitigation factors in order to avoid complex or costly e-Authentication arrangements that cannot be warranted on the basis of risk assessment, or the need to ensure user confidence.

Staged and complimentary controls

Agencies can mitigate risks by implementing control measures at different stages of the transaction lifecycle – before, during and after the fact. Before-the-fact controls include e-Authentication. During-the-fact controls include those implemented via access control (authorisation or permissions management) applications and via the business logic in applications. After-the-fact controls include processes to detect, analyse and remedy errors or transgressions (possibly through legal action).

Figure 6 below is illustrative of the three types of controls in association with certain (not all) classes of online risks.

Figure 6: Risk categories and types of controls



Defence in Depth

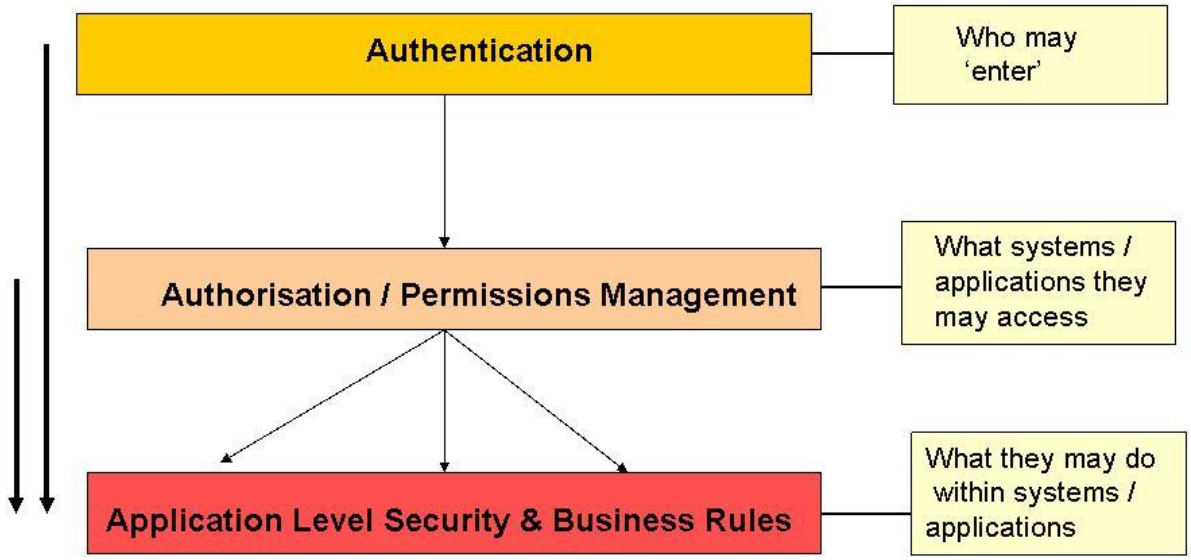
While individual safeguards are important, it is important for agencies to adopt a defence in depth approach. This entails having a set of safeguards in such a manner that the failure or compromise of one does not leave assets directly vulnerable to harm. Two metaphors are used to describe the most effective form of complementary safeguards. One is the 'onion skin' notion, invoking the idea of successive layers that have to be peeled off before the heart is exposed. The other is 'defence in depth', implying that if the perimeter defences are breached, there are further defence layers behind them.

By way of example, e-Authentication can be seen to be only one of three levels of system control applied to address risk issues.

Behind e-Authentication lie access control (also called permissions management), and security mechanisms at the level of the individual application, including the specific business rules specified in the application requirements. This is shown in Figure 7.

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

Figure 7: Defence in depth – multilayered controls



Safeguards

Among the most important safeguards are computer-based and manual checks and balances that are imposed on the transaction life cycle to reduce the likelihood of threatening events occurring, enable their early detection, or reduce the harm arising from them.

Examples of safeguards include:

- checks of the internal consistency of data in an incoming message
- checks of incoming data against data already held in an agency's database
- reconciliation between bank statements of funds received and amounts submitted in messages
- controls embedded as business rules within applications
- informed user (particularly customer) consent, including acknowledgement of the importance of protecting e-Authentication credentials; and
- continual reinforcement of the importance of protecting e-authentication credentials through user education, warnings or notices displayed for each online session.

Safeguards that can be used to combat single-instance accidents and attacks, and systemic accident or serial abuse, include:

- implementing challenge-response questions for important transactions (for example, change of address and bank account details)
- informing users of:
  - the number of recent accesses and date of last access
  - access attempts (on their 'accounts') using invalid passwords
  - important categories of transactions (for example, change of name or address, bank account) that require verification by means of 'out-of-band' channels, such as post or SMS
- validating bank account names with banks (for example, should be same name as user or payment nominee)
- blocking suspicious or unusual transactions during the event, based on rules derived from patterns of dealings; and
- detecting and re-confirming transaction combinations associated with known errors or attacks (for example, change of bank account followed by immediate request for advance payment).

Safeguards that provide defence against large-scale accidents and mass attacks include:

- implementing active monitoring of transaction patterns and automatic or operator-initiated intervention or suspension of a user's capacity to transact
- blocking suspicious or unusual transactions during the event, based on rules derived from patterns of dealings; and
- detecting and re-confirming transaction combinations associated with known errors or attacks (for example, change of bank account followed by immediate request for advance payment).

Safeguards in relation to health and safety include:

- limiting transactions that can be conducted through particular channels
- requiring stronger e-Authentication for particularly sensitive data (for example, challenge-response using knowledge-based approach or one-time password)
- masking the presentation of information via online channels by removing identifying information or the use of pseudonyms; and
- implementing additional controls at the e-authentication, permissions management and application levels in relation to categories of persons-at-risk, i.e. individuals whose physical safety may be at risk if information about them is subject to unauthorised access.

Special safeguards necessary in relation to privacy include:

- obtaining informed consent from all users before:
  - providing an e-Authentication credential to a user
  - enabling a nominee or agent to act on behalf of a user
- reinforcing (and being seen to reinforce) sound practices across the user base through education campaigns and reinforcing the message during all user online login processes
- masking the presentation of information via electronic channels by removing identifying information or the use of pseudonyms – this can be widely applied or based on user choice; and
- informing users of:
  - the number of recent accesses and date of last access;
  - access attempts using invalid passwords
  - important categories of transactions (for example, change of name and address, bank account) using 'out-of-band' channels, such as post or SMS.

Agencies can use particular safeguards to guard against unjustified repudiation of transactions, in particular by:

- maintaining full transaction audit trails (e.g. date-time, IP address) for sufficiently long periods so they are available if needed to support legal processes; and
- periodically or randomly introducing a second e-Authentication factor (e.g. challenge-response using shared knowledge questions).

Record the mitigating factors associated with each threat/risk in *CET5-Risk Analysis Form.*

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

5) Assess assurance level required to cover residual risk

An online Risk Assessment Tool is provided as an adjunct to the Better Practice Guidelines to assist with this task – contact Finance at authentication@finance.gov.au.

The end point of the transactions process above is the assessment of the residual risks that e-Authentication will be required to address. The required e-Authentication assurance level is assessed by identifying the severity of the consequences of getting e-Authentication wrong. This uses the risk assessment criteria detailed in Table 2 below[7].

Note – the list of Consequence Type's in Table 2 is just a sample list of standard consequences. However in many cases, residual risks may broadly fall into the types listed below. Please add or remove consequence types where not relevant.

[7] Based upon the risk assessment table in the Queensland Government Authentication Framework (QGAF).

Table 2: Illustrative consequences and severity

Consequence Type	**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 no significant impact	Measurable impact, breach of regulations or commitment to confidentiality	Release of information would have a significant impact	Would have major consequences to a person, agency or business
Financial loss to any client of the service provider[8] or other third party	No loss	Minimal	Minor	Significant	Substantial
Financial Loss to Agency / service provider	None	Minimal < 2% of monthly agency budget	Minor 2% – < 5% of monthly agency budget	Significant 5% – < 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	Agency business or service delivery impaired in any way	Agency business halted or significantly impaired for a sustained period[9]
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

8 The amounts to be considered are suggested as: Minimal <$50, Minor $50-<$200, Significant $200-<$2000 and Substantial >$2,000, but these figures here 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 to something more akin to the figures used for financial loss to the service provider. If multiple clients will suffer the loss, the impact level should be adjusted accordingly to reflect the total losses to clients.

9 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 necessary to map this against the likelihood of this occurring in order to finally determine the assurance level to be applied. This applies the approach proposed by AS/NZS4360. The result is illustrated in Table 3 below.

Table 3: Indicative assurance level requirements based upon likelihood and consequences

	Threat Impact/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 threat consequence and likelihood used for this table should be informed by the *CET5-Risk Analysis Form*, and the definitions derived from the agency's risk management framework. The online Risk Assessment Tool (contact Finance at authentication@finance.gov.au) may also be used to catalogue application, transaction and user-type profiles and compute assurance level requirements.

Table 2 can be used to inform the consequence assessment. The following descriptions may inform the likelihood assessment:

- **Rare:** May occur in exceptional circumstances, e.g. less than once in 10 years.
- **Unlikely**: May occur at some time, e.g. once or more in 10 years.
- **Possible**: Should occur at some time, e.g. once or more in 3 years.
- **Likely**: Will probably occur in most circumstances, e.g. once or more in 1 year.
- **Almost certain**: Is expected to occur in most circumstances, e.g. more than once in 1 month

The information security classification level associated with the information that will be 'exchanged' during the transaction[10] 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 section 3.104 of ISM available at http://www.dsd.gov.au/library/infosec/ism.html

6) Determine the required e-authentication assurance level

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.

[10] Agencies are referred to the PSM and ISM for authoritative policies in this regard.

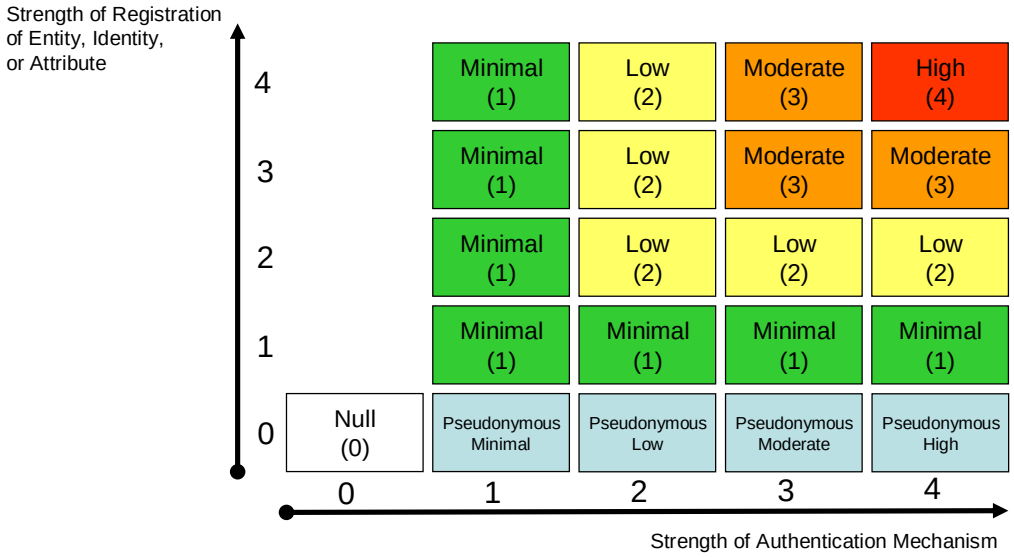
At this stage, stakeholders need to review their judgement based on the unique factors associated with the agency's business, the nature of the user base, the overall environment and the transaction aspects. It is important to consider the guidance contained in the PSM:

> "…[security] measures are sometimes expensive to implement and might have an impact on agency operations. Therefore, the government needs to be assured that protective security measures are only used when the risk warrants it and that any security measures used are appropriate to the identified risk."

The required e-Authentication assurance level may effectively narrow down the choices available for strength of registration and strength of e-Authentication mechanism, as show in Figure 8 below.

Any constraints of this nature will need to be carried forward into the following steps.

Figure 8: Identity Authentication Assurance Matrix



5. Step 3: Select Registration Approach

5.1. Introduction

Registration is the establishment of a unique identity record and allocation of an e-Authentication credential to a user. A registration process is required where a user does not yet possess a credential. Registration can encompass evidence of identity (EOI) and/or evidence of relationship (EOR) processes.

Enrolment is the process whereby specified applications are configured to use a particular credential to authenticate a user. Multiple enrolments may occur after a user (individual or business) has been registered. See section 4 of the NeAF Framework document.

The registration approach will be determined by:

- The nature of the assertion to be authenticated. The most common instances are registration of individuals:
  - as themselves; or
  - as representative for an organisation; or
  - as representative for another individual.
- The assurance level required, as determined in Step 3 above, including any constraints on strength of registration arising from this assurance level (see *Section Determine the required e-authentication assurance level* above).
- Whether the user is to be identified – i.e. whether there is to be a determinable connection between the entity (individual) and the credential. An alternative, which is increasingly adopted in portals and online service points, is for the user to be allocated a pseudonymous credential.
- Whether the individual (subscriber) is already a known customer of the agency. Two variations emerge for known customer subscribers:
  - the subscriber has no pre-existing e-Authentication credential; or
  - the subscriber 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; and
  - the credential lifecycle management process employed by that agency
- The nature and significance of privacy and other public policy issues identified during Step 1.

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

5.2. Core reference documents

The following are core reference documents for this task:

- Schedules A1 and A2 of the *NeAF Framework* provide detailed guidance on registration processes to be followed in various situations.
- *National Identity Security Strategy:*
  - Gold Standard Enrolment Framework (which includes the Proof of Identity (POI) Framework)
  - Gold Standard Authentication Requirements.
- *Gatekeeper EOI Policy (which has adopted the POI Framework)*

5.3. Purpose

The objectives of the tasks are to determine the appropriate approach to the registration of the user. This requires establishment of:

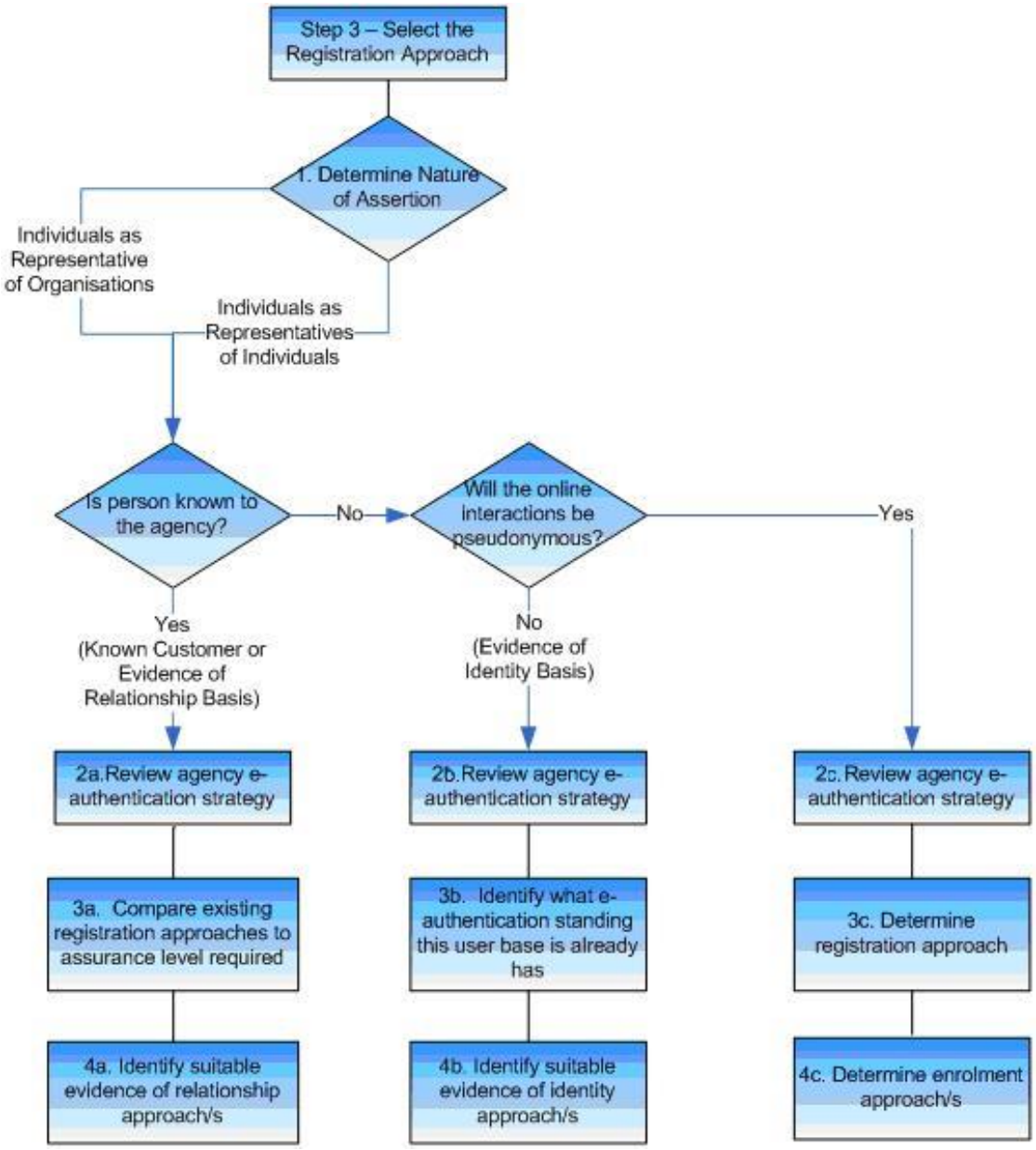
- whether the registration involves Evidence of Identity, Evidence of Relationship (known-customer) or pseudonymous approaches
- which registration approaches are suitable to provide the required level of assurance
- what existing registration approaches might be used. This needs to be examined in an agency, cross-agency and/or whole-of-government context
- what the preferred default approach will be.

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

5.4. Overview of Methodology

Figure 9 below shows the tasks involved in selecting registration approaches.

Figure 9: Tasks covered in the 'Determine Registration Approach' step



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

5.5. General Tasks

1) Determine the nature of the assertion to be authenticated

Registration involves verifying the subscriber's identity[11] or other attribute to an understood assurance level prior to creating and issuing an e-Authentication credential for the subscriber.

The selection of the registration approach 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 organisations; and
- registration of individuals as representatives of other individuals

Registration approaches will also be determined by the nature of the relationship with the users. Specifically the nature could be:

- a customer already known to the agency
- a new customer to the agency
- a new customer to the agency but who is known to another agency; or
- a pseudonymous user.

The initial analysis of this should have been undertaken during Step 1, and be described in *CET3-Checklist to help determine whether identity e-Authentication is required.*

2) Review agency e-authentication strategy

Where an e-authentication strategy has been developed, as recommended in *Better Practice Guidelines – Volume 4*, this should be reviewed to identify critical factors early in the process of selecting registration mechanisms, including:

- where registration fits within the agency's overall security strategy
- areas of particular risk and difficulty within the agency
- high level estimates of costs, benefits and risks associated with the registration requirements
- governance and reporting requirements
- areas of existing registration and enrolment use within the agency; and
- the recommended implementation plan for a registration system within the agency.

The strategy may well have identified (or at least pre-identified) possible registration approaches.

5.6. Tasks related to known customer

If a known customer approach is to be adopted the following tasks should be followed:

1. **Determine whether EOI collected as a result of pre-existing registration approaches provides the underlying required level of assurance.** Reference should be made to *NeAF Framework* Schedule A1 – 'Evidence of Identity' basis. If EOI is not sufficiently strong to meet the constraints determined in *Section Determine the required e-authentication assurance level*, it will be necessary to devise an approach to upgrade (refresh) EOI for the determined user base.
2. **Identify registration approach.** Reference should be made to *NeAF Framework* Schedule A1 – 'Evidence of Relationship' basis. For known customers the registration approach could rely upon

[11] This Guideline focuses on identity assertions. However it is equally applicable to other assertions or attributes (e.g. position, title etc)

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

matching pre-existing information held by the agency to answers to challenges provided by the customer. Agencies will need to determine:

a. The channel/s to be used to undertake EOR registration processes. Options include telephone/call centre and/or online.

b. How to authenticate the customer. A template that suggests a structured and weighted approach is provided through the *CET6-EOR Risk matrix*. Agencies will need to determine their own questions/challenges, and the weightings that they wish to give these.

5.7. Tasks related to new (identified) customer

If the intended user is unknown to the agency and the assurance level requirements are such that identification is necessary the following tasks should be followed:

1. **Determine whether registration has already been undertaken to a required level of assurance by another trusted agency**. If agreed between the agencies, this may enable re-use of the credentials issued by the other agency for the registration purposes of your agency.
2. **Determine documentary evidence required to establish level of assurance**. Reference should be made to *NeAF Framework* Schedule A1 – 'Evidence of Identity' basis.
3. **Identify registration approach.** Agencies will need to determine the channel/s to be used for EOI registration processes. Options include telephone/call centre and/or online. The EOI process could be undertaken by a trusted third party (e.g. an accredited PKI registration authority such as Australia Post).

5.8. Tasks related to pseudonymous customer

Pseudonymous Registration 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' myaccount ; and
- 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 e.g. for purposes of completing and amending a whistleblower's report.

Both of the above require the capturing of sufficient user provided information to enable a unique and persistent relationship to be established by the user. The information must be user determined and may be entirely fictitious. The information will be important where e.g. the user needs to have a password reset (if this is the nature of the credential provided). The user may or may not select their own user-ID, dependent upon the agency's system capabilities to handle this approach.

In the case of pseudonymous registration for a portal or online service point, it is then necessary to bind the pseudonymous credential with known instances of the user on target agency sites. The robustness of the enrolment process will have to be determined by the individual agencies who will allow access to their systems based upon the credential issued by the portal or online service point. It is most appropriate that these agencies run through a process akin to 'registration of known customers' as detailed in Section 5.6. Tasks related to known customer above.

6. Step 4: Select Authentication Mechanism

6.1. Introduction

Components that define an e-Authentication mechanism are:

- An authentication credential (Credential) which is something tangible that is controlled by the subscriber that could incorporate one, or a combination of, something the subscriber knows, has in their possession, or something the subscriber is. These attributes are termed **factors**.
  - Examples of factors include traditional passwords, one time passwords, digital signatures and a biometric measure such as a fingerprint. These factors may also be contained within hardware devices such as USB tokens or smartcards. The combination of the factor and its container is also often referred to as the Credential.
- 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.
  - As an example, an enrolment process with an appropriate credential (User ID and password) may be undermined by poor credential management and usage. For example, if there are no rules built into the online system to enforce strong passwords, a user may choose as a password the word 'password' itself. Similarly, if strong passwords are written down, they may be readily compromised. To mitigate this risk, agencies should implement training and awareness programs for users on the appropriate protection of credentials.
- A full risk assessment of the strengths and weaknesses of the authentication mechanism should be undertaken including, as appropriate, risks arising from the behaviour of the credential holder.

6.2. Core reference documents

The following are core reference documents for this task:

- Schedules B1 (credential assurance levels) and B2 (credential management and usage) of the *NeAF Framework*.
- *National Identity Security Strategy* – security standards for proof-of-identity documents.

Additional information sources that will be important in certain contexts include the:

- DSD Evaluated Products List
- Gatekeeper policies and criteria for PKI.

6.3. Purpose

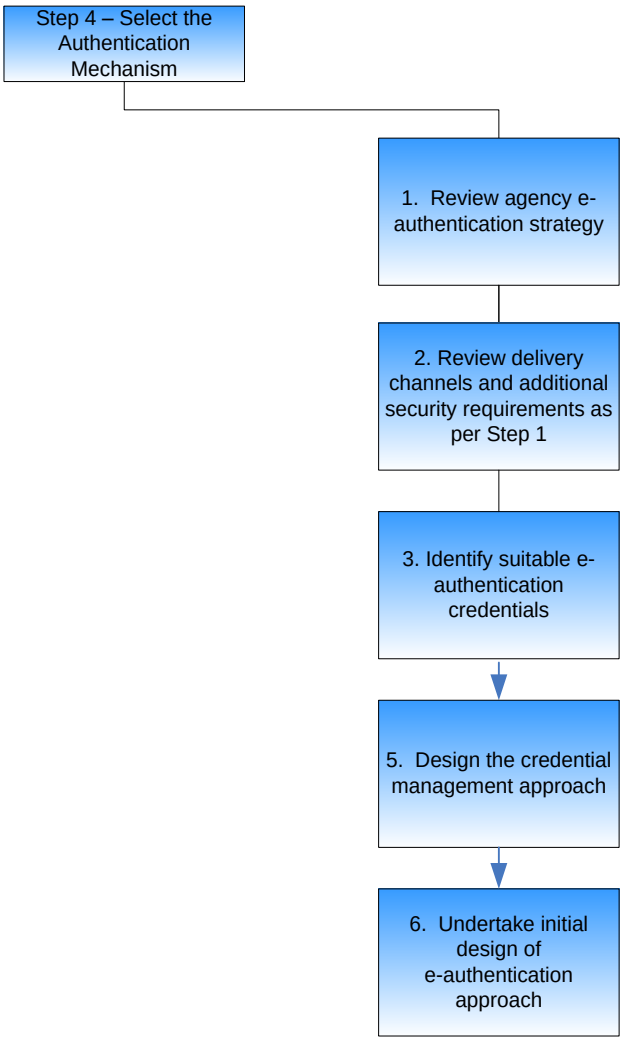
The objectives of the tasks described in this step are to determine the appropriate e-Authentication credential mechanism and lifecycle management approach.

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

6.4. Overview of Methodology

Figure 10 below shows the tasks involved in evaluating the appropriate e-Authentication credential mechanism and lifecycle management approach.

Figure 10: Tasks covered in the 'Select e-Authentication Mechanism' step



6.5. Tasks

1) Review agency e-Authentication strategy

Where an e-Authentication strategy has been developed, as recommended in the *Better Practice Guidelines – Volume 4*, this should be reviewed to identify critical factors early in the process of selecting e-Authentication mechanisms and credential management approaches.

The strategy may well have identified possible e-Authentication mechanisms and credential management approaches, for the transactions under consideration as well as the intended user groups.

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

2) Review delivery channel/s and additional security requirements

Delivery channel/s

In Step 1, agencies will have determined the intended electronic delivery channel/s.

These will influence the selection of the e-Authentication mechanism e.g.

- if telephone is a delivery channel the e-Authentication mechanism may have to be one of: PIN, password provided verbally to an operator, speech processing system, or voice biometric
- if online/web is the delivery channel then all of the mechanisms identified in Schedule B1 represent possible candidate mechanisms.

If a single credential is required to support multiple channels the choice of mechanism may be restricted e.g. to a PIN or password.

Finally, if the review of risks associated with each delivery channel has led to a high required assurance level (see section 4.6 above), the constraints imposed on the strength of registration and authentication mechanism may limit the choices of authentication mechanism that are available.

Additional requirements

In Step 2, a number of additional requirements may have been identified as applying to the transaction/s under evaluation. These may have included:

- the requirement for confidentiality of information passing across the electronic channel
- ensuring the integrity of transactions or instructions submitted via the electronic channel (often referred to as transaction authentication) with the aim of assuring that the transaction or instruction has not been modified maliciously or accidentally whilst in transit; and
- the requirement to limit as far as is possible the ability of the user to repudiate a transaction.

As indicated in Step 2, while e-Authentication does not provide a complete solution to these requirements, it may be possible to leverage the underlying e-Authentication processes and technologies to assist with that solution. As such the broader authentication requirements of the channel, beyond identity authentication, should be considered when selecting an identity authentication mechanism.

Specific credential usage opportunities are described in Schedule B1 of the *NeAF Framework*.

The ultimate use of identity authentication credentials for broader purposes, including the support of confidentiality, should be considered as part of the credential selection process and as a major element of overall delivery channel security design.

If already completed in Step 2, agencies can use the *CET2–Transaction Analysis Checklist* to decide what additional requirements apply to the transaction, and where e-Authentication might be leveraged to provide solutions.

3) Identify suitable e-authentication credential/s

The selection of a credential type should be based upon the following factors:

- capacity to meet the required e-Authentication assurance level, as illustrated in Schedule B1 of the *NeAF*, including any constraints on the strength of authentication mechanism (see Determine the required e-authentication assurance level)

- capacity of the credential selected to:
  a. suit the delivery channel/s identified in the previous task; and
  b. meet the additional requirements (e.g. transaction confidentiality and/or non-repudiation) identified in the previous task. This is not an essential requirement, as other complimentary technological and/or process approaches may be more appropriate to meet these additional requirements.

Schedule B1 of the *NeAF Framework* is intended to provide guidance to agencies. It cannot, and should not, be used by agencies to fully determine the decision appropriate in every circumstance. Each agency will therefore need to consider aspects of its business processes and their context, and judge whether variations are needed. Particular factors of importance may include:

- credentials that the user community commonly possesses
- credentials that the agency's infrastructure already supports
- credentials that would be easily understood and used by the user base and that could be supported easily
- credentials used by other government agencies; and
- credentials provided by other trusted third parties such as banks.

Agencies can use the information in Schedule B1 of *NeAF* to develop an initial list of potential e-authentication mechanisms.

The accompanying *CET7-e-Authentication Approach Analysis* form may assist in collating the suggested information.

4) Design the credential management approach

A credential management approach should now be identified that supports the selected credentials and registration approach. This credential management approach must meet the required assurance levels for the e-Authentication mechanism selected.

Factors to be considered and resolved in this step are:

- credential generation
- credential issuance and activation
- activated credential management, including re-activation
- credential verification; and
- authentication event logging.

See Schedule B2 of *NeAF* for guidance on possible credential management techniques and their link to required assurance levels.

5) Undertake initial design of the e-authentication approach

By selecting one or more appropriate e-Authentication approaches, agencies can start to do the detailed design. The purpose of this task is to deliver a sufficient description:

- to enable impact analysis to be conducted; and
- once the decision is confirmed, to enable the design and implementation to move forward.

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

In articulating a design an agency needs to consider:

- a description of the registration and/or enrolment process to be applied (using information collated in Step 4). A registration process is required where a user does not yet possess a credential. An enrolment process is where a user has a pre-existing credential and is then enrolled to use this for one or more specified applications, and
- a more detailed description of the e-Authentication process outlined in the tables on mapping e-Authentication approaches to risk assurance levels in Schedule B of the National e-Authentication Framework document.

During the process the agency should commence with a critical assessment of the overall e-Authentication solution including the issues covered in the step above i.e.:

- ease of registration and credential collection/delivery, installation and use for users
- ease of implementation by the agency, including consideration of credentials that agency infrastructure already supports
- credentials used by other government agencies that could be federated (see 7. Step 5: Select Implementation Model)
- credentials that the user community commonly has and the likelihood that users will be able to use this credential with other agencies
- whole of life costs to users and the agency.

These matters will be further considered in Steps 6, 7 and 8.

7. Step 5: Select Implementation Model

7.1. Purpose

This step examines which e-authentication model best suits the agency's immediate and medium term online services goals. The selection of an appropriate model can have the following positive impacts on an agency and its user base:

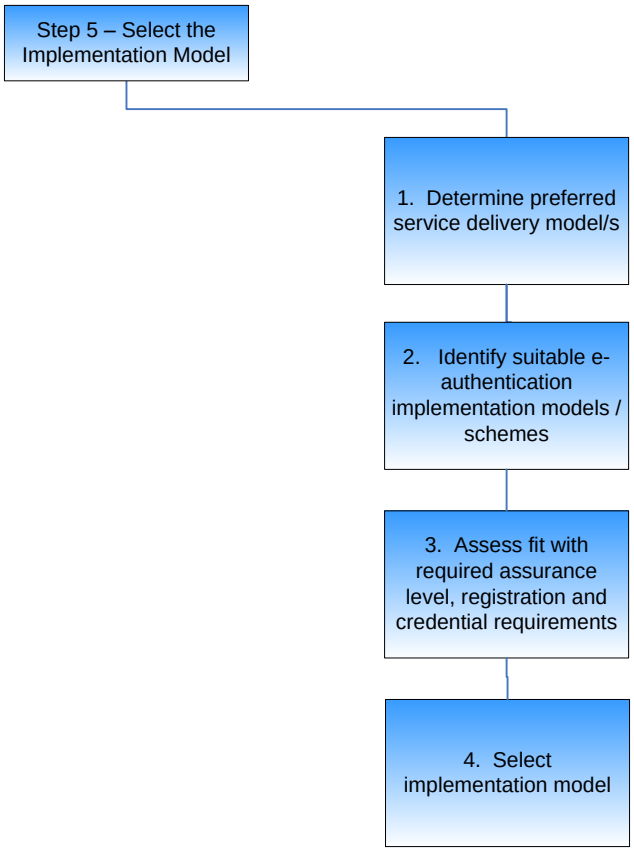
- reduce whole of life costs of implementing and operating an e-Authentication approach for both the agency and users; or/and
- increase usability and critical mass for the user base/s; or/and
- provide support for customer-centric or joined-up government service delivery models.

The key information resource supporting this step is Volume 3 (e-Authentication Implementation Models) of the Better Practice Guidelines.

7.2. Overview of Methodology

Figure 11 below shows the tasks involved in selecting an e-Authentication implementation model.

Figure 11: Tasks covered in the 'Select Implementation Model' step



7.3. Tasks

1) Determine preferred service delivery model

Service Delivery Models, in the context of this guide, are models of the business processes used to deliver services to clients.

The emergent service delivery models described below are aimed at:

- enabling increased user centricity – allowing users greater choice in how they deal with government – e.g. reducing the number of e-Authentication credentials they choose to hold
- decreasing users' need for awareness of the distribution of various business service delivery facilities across government agencies, and changes in this distribution over time through machinery of government changes
- improving the efficiency of electronic government services delivery through reuse of core infrastructure
- retaining, and potentially enhancing, agencies' abilities to implement a risk based approach to user authentication.

A core determinant for the selection of e-Authentication models is the preferred service delivery model. These include:

- **Agency** or business unit or application centric.
- **Sectoral** (e.g. health, education). These can be jurisdictionally based or national, with the latter becoming increasingly dominant.
- **Whole of government**. Here the desire is to provide individuals and businesses with a single window into access to government services. The electronic articulation of these models takes the form of portals.
- **Agency clusters**. Here a range of agencies that have a collective focus and shared responsibility for services and/or outcomes come together virtually to share information and, at times, transactions. Prominent examples are the state and territory government multi-party land information systems and justice-cluster applications.

Agencies should determine which service delivery model they wish to pursue. While agency-centric (siloed) service delivery models are the default, these increasingly run counter to overarching government service delivery strategies.

2) Identify candidate e-Authentication implementation models and schemes

Table 4 below provides an indicative mapping of the suitability of various identity authentication models to the service delivery models.

Table 4: Rating suitability of e-Authentication Models to Service Delivery Models

e-Authentication Models	Service Delivery Models		
	Sectoral	Agency Cluster	WoG
Siloed			
Centralised	✓✓✓ (1)	✓ (1)	
Federated- (SSO) Portal	✓✓ (2)	✓ ✓ (2)	✓ ✓ (2)
Federated Peer to Peer Portal		✓✓ (4)	✓ ✓ ✓ (3)
Federated Portal PLUS		✓ ✓ ✓ (5)	✓✓✓ (5)
Federated Authentication Services			✓✓✓ (6)

In the above diagram the number of ticks in the cells provides a relative measure of suitability, whilst the number in brackets refers to the explanatory note below.

Notes

1. Benefits through a single identifier used across the participating agencies.
2. Benefits through a single point of access with a credential.
3. Benefits through increased openness and user choice in use of particular credentials.
4. Benefits through increased openness and user choice in use of particular credentials. Agency overheads through increased operational complexity.
5. Potential benefits through user authorised synchronisation of identity related information across participating agencies.
6. Benefits through implicit separation of users' affairs across agencies without the loss of user benefit of single credential usage.

In addition to identifying candidate models, where possible agencies should identify actual or planned e-Authentication schemes or services e.g. AGOSP, National Authentication Service for Health.

3) Assess fit with requirements identified in Steps 3 to 5

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

- assurance levels determined in Step 3
- registration approach/s determined in Step 4; and
- e-Authentication credential and credential management solutions identified in Step 5.

In practice, selection by agencies or collectives of agencies of the most appropriate authentication model/scheme for their business applications and service delivery models will be determined by a range of issues and influences including:

- identifiers and their usage
- user centricity in respect to credentials
- privacy considerations and implications

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

- visibility by agencies of the authentication method or processes
- Registration Assurance Levels
- agency 'onboarding' processes for subscribers
- potential extensibility to a fully federated identity management environment
- extensibility in respect to technology / discipline and standards advances
- extensibility to support authentication of complementary attributes including document and transaction authentication
- supportability of other government and private sector issued credentials
- model maturity and deployed base, including international experience; and
- legal, contractual and governance requirements and implications.

See Table 1 of Volume 3 of *the Better Practice Guidelines* for a detailed explanation of these factors.

In the event of a mismatch between the candidate models/schemes and the requirements identified by Steps 3–5 above a number of paths are possible:

- reassess assurance level requirements and/or registration processes and/or credential solutions by revisiting Steps 3–5
- negotiate changes to an existing scheme to gain compliance with requirements identified through Steps 3–5; or
- evaluate the issues associated with establishing a new scheme based upon the preferred implementation model.

4) Select implementation model

The previous step should have refined the implementation model, and hopefully scheme, choices down to no more than two.

The implicit scoring undertaken in the previous task may well have identified a better or preferred fit to one model/scheme.

In addition the following issues should be evaluated:

- **Existing user credentials**. Which model/scheme is most closely linked with or extensible to existing user e-Authentication credentials?
- **User capability**. Which model/scheme best fits with user capabilities? e.g. in terms of systems literacy, computing platform, network bandwidth.
- **Cost**. Which model will have the least whole-of-life costs. Commonly this will involve the comparison of an agency or application centric siloed model with one or more models that provide a greater degree of aggregation or sharing with other applications within an agency or across organisational boundaries.
- **Speed of implementation**. Which model will enable more rapid implementation?
- **User outreach and onboarding and ongoing support**. Which model/scheme will enable the most effective and cost efficient approach?
- **Provision of a critical mass**. Which model/scheme will provide most useful functionality without which users may not migrate to an electronic channel?
- **Privacy protection** – Which models allow for the ease of simplified or single signon to a range of applications within an agency or across multiple agencies, and yet still allow greater de grees of pseudonymity?

8. Step 6: Assess the Business Case and other Feasibility Issues

As agencies complete the authentication steps outlined earlier in this volume, they will gather the information necessary to develop a high-level cost-benefit analysis.

In undertaking this analysis, the NeAF recommends that agencies use the *ICT Business Case Guide* methodologies (see the *CET8-Business Case Guide*):

1. Step 1: Review Environment and Identify Business Need
2. Step 2: High Level Options Analysis
3. Step 3: Detailed Options Analysis.

Some aspects of this are covered below.

8.1. Costs

The following table briefly identifies the key upfront cost categories, together with opportunities to reduce costs through collaboration and rationalisation across agencies.

Table 5: Upfront costs

Area of upfront cost	**Collaboration/rationalisation opportunities**
Education and training Development and deployment of awareness raising and training courses for executives, technical staff and end-users	Development could be undertaken once for whole-of-government, with execution taking place at agency level.
Policies and procedures Definition of mutually agreed and accepted e-authentication policies and procedures, including the development of an e-authentication assurance level profiles for all transactions	Development could be undertaken once for whole-of-government, with tailoring or personalisation taking place at agency level.
Existing technology platforms The re-engineering costs associated with connecting agency online systems with e-authentication mechanisms	There are opportunities for savings from whole-of-government purchasing (of solutions or services) and shared learnings across agencies.
New technology platforms and solutions The cost of e-authentication solutions and the associated costs of implementation and integration	There is potential for consolidation around a shared infrastructural solution. Whole-of-government purchasing approach for multiple solutions will also deliver savings.

Area of upfront cost	Collaboration/rationalisation opportunities
Security, audit or validation The cost to validate the efficacy of the e-authentication environment	There are opportunities for savings from whole-of-government purchasing (of solutions or services) and shared learnings across agencies.

The following table identifies the key ongoing costs, together with opportunities to reduce costs.

Table 6: Ongoing costs

Area of ongoing cost	Collaboration/rationalisation opportunities
Education and training Development and deployment of induction training, and ongoing awareness raising and training courses for executives, technical staff and end-users	Ongoing development and maintenance of materials can be undertaken at a whole-of-government level.
Policies and procedures Maintenance of policies and procedures, and some possible audit or QA functions	Ongoing development can be undertaken at a whole-of-government level.
Existing technology platforms Ongoing enhancement and licensing costs	Whole-of-government purchasing will reduce this cost.
New technology platforms and solutions Ongoing enhancement and licensing costs	Whole-of-government purchasing and/or shared infrastructure will reduce this cost.
ICT Operations and Development Costs of incremental operations and user help desk staff, computer room utilities, ongoing e-Authentication mechanism updates, hardware maintenance, telecommunications	Whole-of-government hosting and/or shared help desk and systems hosting, and shared development will reduce this cost.
Security, audit or validation Cost of periodic security audits and reviews	Whole-of-government purchasing and/or shared learnings will reduce this cost.
Legal costs Cost of personalising MOUs to be exchanged between issuers of trust and relying parties (if appropriate)	Whole-of-government purchasing and/or shared learnings will reduce this cost.

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

8.2. Benefits

The following table identifies the key quantifiable benefits, together with the data required to achieve the computation of benefits in dollar terms.

Table 7: Benefits

Value category	Benefit	Data required for computation
User benefits	Higher trust in electronic systems, and higher utilisation (reduction in costs of manual alternatives)	1. User categories and sizes 2. Cost of manual processes and electronic processes **to the user** 3. Estimate of increased uptake of electronic processes.
Government operational or foundational benefits	Reduction in use of non-electronic delivery channels	1. User categories and sizes 2. Cost of manual processes and electronic processes **to the agency** 3. Estimate of increased uptake of electronic processes.
Government financial benefits	Reduction in cost of infrastructure and operational services for providing electronic access to externals, as a result of any whole of government initiatives	1. Fully implemented and deployed cost of platforms per agency 2. Deployed cost of whole-of-government infrastructure (as an alternative)

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

9. Step 7: Review proposed e-authentication solution

9.1. Purpose

By completing the steps outlined earlier, agencies would have determined the preferred registration and e-Authentication approaches to make up the e-authentication solution.

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

This should give consideration to whether the proposed solution meets the ten principles detailed in Section 1.6 of the *NeAF* document, these being:

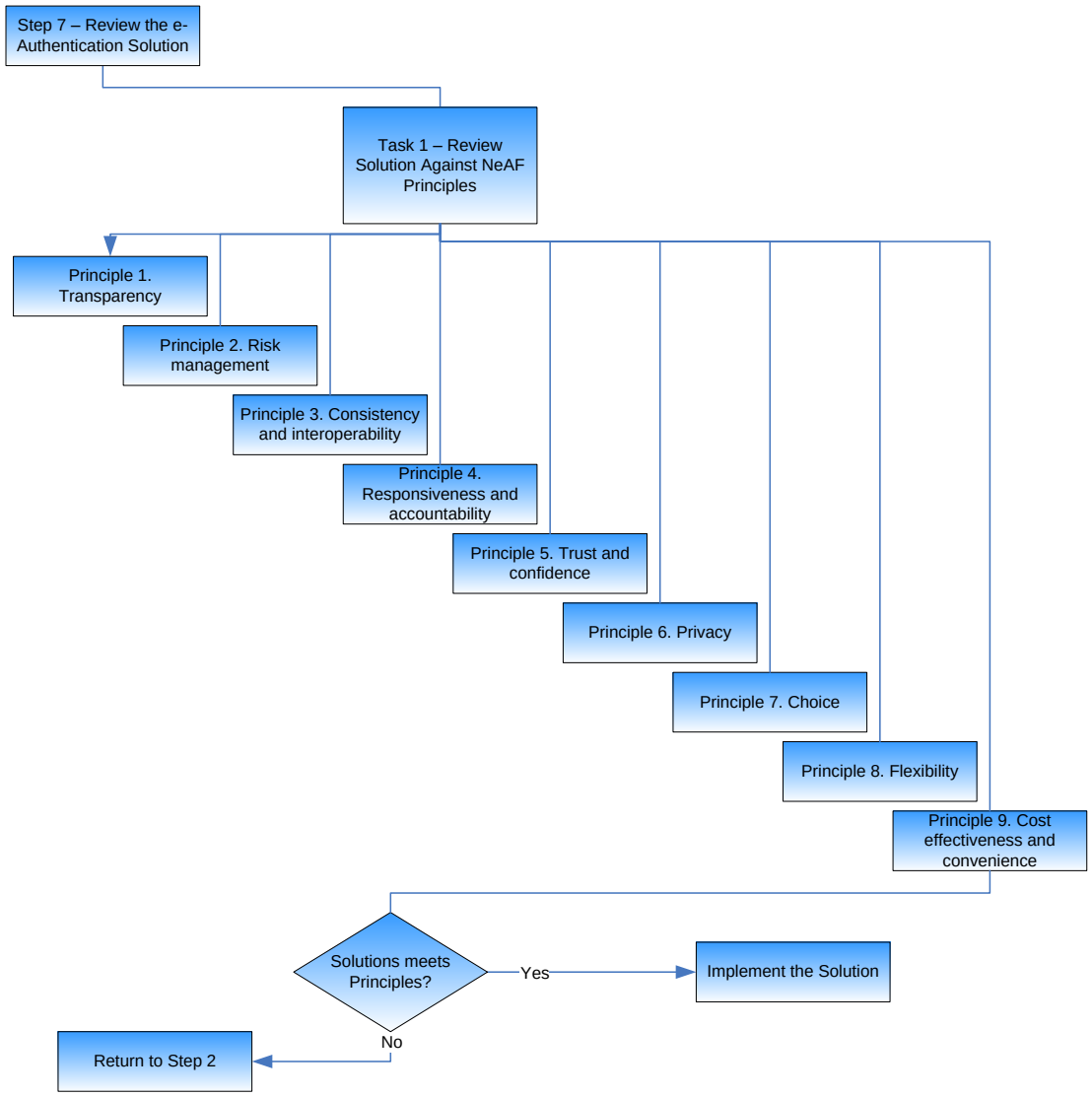
- Principle 1. Transparency
- Principle 2. Risk management
- Principle 3. Consistency
- Principle 4. Interoperability
- Principle 5. Responsiveness and accountability
- Principle 6. Trust and confidence
- Principle 7. Privacy
- Principle 8. Choice
- Principle 9. Flexibility
- Principle 10. Cost effectiveness and convenience

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 costs issues associated with the necessary implementation and operational model.

9.2. Overview of Methodology

Figure 12 below shows the tasks involved in reviewing the intended e-Authentication solution.

Figure 12: Tasks covered in the 'Review e-Authentication Solution' step



9.3. Tasks

1) Review Solution Against NeAF Principles

In ensuring the e-Authentication approach selected through the *NeAF Framework* process is the best solution, the NeAF provides a set of principles against which to validate it.

The ongoing application of the NeAF principles across government agencies will result in the broad alignment of e-Authentication approaches across government agencies and applications throughout Australia.

This should give consideration to whether the proposed solution meets the nine principles detailed in section 1.6 of the *NeAF Framework*, these being:

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

Transparency

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

Risk management

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

Consistency

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

Interoperability

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

Responsiveness and accountability

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

Trust and confidence

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

Privacy

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

Choice

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

Flexibility

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

Cost effectiveness and convenience

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

Agencies should review the selected e-Authentication approach against each of the Principles to validate it. Where an approach does not comply with any of the NeAF Principles, the agency should:

- identify what parts of the approach are causing the non-compliance
- identify the results of the non-compliance using a threat/risk assessment approach, thus identifying the likelihood and consequences of any negative outcomes
- assess whether parts of the approach must be changed to comply with the Principle or whether other risk treatments could be used
- return to Steps 2, 3 and 4 of this Guide to change the approach if necessary.

Use CET1-Checklist to Analyse Compliance with NeAF Principles to help collate the suggested information.

2) Determine feasibility of e-authentication approach

Agencies now need to review the analysis conducted in the previous Steps. Based on an assessment of the relative positives and negatives, agencies then decide on the feasibility of the registration and e-Authentication approaches identified in Steps 4 and 5 and a course of action including, but not limited to:

- moving to a fuller design of the e-Authentication approach and a project plan for its implementation, or
- revisiting Step 3 to reassess risks and the nature and extent of other risk mitigation factors, and/or
- revisiting Steps 4 or 5 to determine other possible approaches to registration or e-Authentication, and/or
- undertaking further work (for example, through focus groups, surveys) to more fully test user attitudes, competencies and technology capabilities, and in particular, their responses to one or more ‘straw man’ e-Authentication scenarios, and/or
- undertaking further work to assess alternative process and technological approaches within an agency, including assessing shared solutions, and/or
- shelving further work on this transaction pending more favourable agency and/or user circumstances emerging.

Agencies should determine whether a proposed approach to e-Authentication is feasible from a business and agency perspective. If feasible, commence a more detailed design and implementation plan for the e-Authentication approach. If not feasible in its current form, revisit the tasks outlined in Steps 3 and 4 of this guide to see whether negative issues can be overcome by re-assessing and re-scoping the approach.