

Department of Finance and Deregulation
Australian Government Information Management Office

National e-Authentication Framework

Better Practice Guidelines – Vol 1
Checklists, Explanations and Templates

January 2009

Disclaimer

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

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

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

ISBN 0 9758173 7 X

Department of Finance and Deregulation

Australian Government Information Management Office

© Commonwealth of Australia 2009

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

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

Commonwealth Copyright Administration,

Attorney General's Department,

Robert Garran Offices,

National Circuit,

Barton ACT 2600

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

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Copyright: Department of Finance and Deregulation

Table of Contents

CET1 - Checklist to analyse compliance with NeAF principles	1
Principle 1. Transparency	1
Principle 2. Risk management	2
Principle 3. Consistency and interoperability	3
Principle 4. Responsiveness and accountability	4
Principle 5. Trust and Confidence	5
Principle 6: Privacy	7
Principle 7. Choice	8
Principle 8. Flexibility	9
Principle 9. Cost effectiveness and convenience.....	10
CET2 – Transaction analysis checklist.....	1
CET3 - Checklist to help determine whether identity e-Authentication is required	1
CET4 - Checklist to help analyse delivery channels.....	1
CET5 - Risk analysis form.....	1
CET6 - Evidence of relationship risk matrix	1
CET7 - e-Authentication approach analysis form*	1
CET8 - ICT investment framework / business case guide.....	1
CET9 - Privacy law compliance checklist	1
CET10 - User impact assessment checklist	1
1. Access.....	1
2. Equity.....	3

CET1 - Checklist to analyse compliance with NeAF principles

This Checklist provides a set of questions to answer to assist in the determination compliance with the NeAF Principles.

For each question tick the yes/no/na box, and then detail why that answer was selected. In general 'yes' answers are what is expected in order to be compliant with the NeAF Principles.

Principle 1. Transparency				
e-Authentication decisions will be made in an open and understandable manner involving consultation with relevant stakeholders.				
Question	Yes	No	N/a	Description
Stakeholders Mapping: have all stakeholder groups been identified along with representatives or advocates?				
Disseminating information: have draft approaches or selection documents been communicated to stakeholders with sufficient timeframes for review and comment?				
Involving stakeholders: have stakeholder views been canvassed during this process or an appropriate prior process?				
Consideration: Have the results of the consultation processes been collated and given due consideration?				
Agreements: where stakeholders have or should have a vote in the selection process, were those stakeholders able to participate?				

Principle 1. Transparency				
e-Authentication decisions will be made in an open and understandable manner involving consultation with relevant stakeholders.				
Question	Yes	No	N/a	Description
Transparency: Has feedback been provided to stakeholders on a regular basis?				
Documentation: Has the process been documented?				

Principle 2. Risk management				
Selection of e-Authentication mechanisms will be guided by the likelihood and consequences of identified risks. These risks will be articulated as part of the development and justification of e authentication mechanisms. Risk assessment and management are conducted in accordance with the Australian and New Zealand Standard, AS/NZS: 4360.				
Question	Yes	No	N/a	Description
Has a threat assessment been undertaken to collate and categorise authentication and related security threats?				
Have the likelihood and consequences of those threats been detailed?				
Have the current risk treatments been identified, and thus residual risk been detailed?				
Has the risk assessment and management plan been communicated to stakeholders?				

Principle 2. Risk management

Selection of e-Authentication mechanisms will be guided by the likelihood and consequences of identified risks. These risks will be articulated as part of the development and justification of e authentication mechanisms. Risk assessment and management are conducted in accordance with the Australian and New Zealand Standard, AS/NZS: 4360.

Question	Yes	No	N/a	Description
Has the risk assessment and management plan been reviewed by risk and authentication specialists?				
Has the e-Authentication approach selected process been explicitly based on this risk assessment?				

Principle 3. Consistency and interoperability

Government agencies will apply a consistent approach to selecting e-Authentication mechanisms, so individuals and businesses can expect similar e-Authentication processes for transactions with similar assurance levels offered by different government agencies. Agencies should also deploy e-Authentication mechanisms that are consistent with the Australian Government Technical Interoperability Framework.

Question	Yes	No	N/a	Description
Has the selection process considered existing registration instances and e-Authentication mechanisms currently in use within the target user group/s?				
Has the selection process considered the varying implementation models as outlined in BPG Volume 3?				

Principle 3. Consistency and interoperability

Government agencies will apply a consistent approach to selecting e-Authentication mechanisms, so individuals and businesses can expect similar e-Authentication processes for transactions with similar assurance levels offered by different government agencies. Agencies should also deploy e-Authentication mechanisms that are consistent with the Australian Government Technical Interoperability Framework.

Question	Yes	No	N/a	Description
Where existing registration and e-Authentication mechanisms are currently in use with the target user group/s by your agency or other agencies, are you leveraging those mechanisms?				
Is the implementation model consistent with the Australian Government Technical Interoperability Framework?				
Does the approach and implementation model comply with the relevant whole-of-government agreed policies and standards (including those shown in NeAF Appendices A and B)?				
Has the agency provided details of its 'solution' to other relevant agencies to enable potential re-use by those agencies?				

Principle 4. Responsiveness and accountability

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

Question	Yes	No	N/a	Description
Have user needs been detailed based on consultation with and/or submissions from users or their representatives/advocates, whether during this process, or pre-existing?				
Have measures or KPI's been set to measure whether user needs are met?				
Have monitoring and reporting mechanisms been devised to ensure that the agency is accountable for meeting the business needs?				
Have user guides, training and education programs been developed to be implemented with the e-Authentication approach for agency staff, end users, and where appropriate, partners?				
Are suitable user advice and assistance facilities available via web and phone?				
Have dispute resolution systems been devised for the approach?				

Principle 5. Trust and Confidence

The mechanisms used will support electronic services and should be useful and safe for government and individuals/businesses.

Question	Yes	No	N/a	Description
Has the selected approach been assessed in terms of security risks (data privacy, integrity, and non-repudiation)?				
Will the selected approach save time, cost, and/or inconvenience for the user?				

Principle 5. Trust and Confidence				
The mechanisms used will support electronic services and should be useful and safe for government and individuals/businesses.				
Question	Yes	No	N/a	Description
Will the selected approach provide any additional functions or benefits for the user?				
Will the selected approach save time, cost, and/or inconvenience for the agency?				
Will the selected approach enable users/agencies to undertake transactions that could not previously be undertaken?				
Is compliance with best practice policies and procedures being monitored in the implementation of the approach?				
If required, has a User Impact Assessment been undertaken?				

Principle 6: Privacy

Personal information will be collected only where necessary for the processes being undertaken. Agencies should conduct an internal Privacy Review for all new e-Authentication initiatives and the extension of existing services that go beyond their original scope. Some jurisdiction’s legislative and/or policy environment may require that a formal and independent Privacy Impact Assessment (PIA) is conducted for new large scale e-Authentication initiatives that involve the collection, processing and storage of high levels of personal information.

It should also be noted that at the Commonwealth level, a PIA is not a statutory obligation but considered good privacy practice. Not every project will need a PIA, though if it involves significant amounts of personal or sensitive information, it is likely to benefit from a PIA. To assist agencies and organisations, the Office of the Privacy Commissioner (Cth) has produced a PIA guide, which is available on its website (see <http://www.privacy.gov.au/publications/piao6/index.html>). The Information Privacy Principles should also be referenced in this analysis – see <http://www.privacy.gov.au/publications/ipps.html>.

Question	Yes	No	N/a	Description
Has the agency carefully determined whether it is necessary to authenticate identity or whether some alternative assertion can be authenticated?				
Have particular approaches been adopted for user groups who may be ‘at risk’?				
Has the NeAF BPG privacy checklist been completed for the project?				
If required, has a Privacy Law Review been undertaken?				
If required, has a Privacy Impact Assessment been undertaken?				

Principle 6: Privacy

Personal information will be collected only where necessary for the processes being undertaken. Agencies should conduct an internal Privacy Review for all new e-Authentication initiatives and the extension of existing services that go beyond their original scope. Some jurisdiction’s legislative and/or policy environment may require that a formal and independent Privacy Impact Assessment (PIA) is conducted for new large scale e-Authentication initiatives that involve the collection, processing and storage of high levels of personal information.

It should also be noted that at the Commonwealth level, a PIA is not a statutory obligation but considered good privacy practice. Not every project will need a PIA, though if it involves significant amounts of personal or sensitive information, it is likely to benefit from a PIA. To assist agencies and organisations, the Office of the Privacy Commissioner (Cth) has produced a PIA guide, which is available on its website (see <http://www.privacy.gov.au/publications/piao6/index.html>). The Information Privacy Principles should also be referenced in this analysis – see <http://www.privacy.gov.au/publications/ipps.html>.

Question	Yes	No	N/a	Description
Has the EOI Requirement Checklist been completed to ensure that Evidence of Identity is necessary?				

Principle 7. Choice

Individuals and businesses will be able to choose whether to use multiple or (where available) aggregated electronic credentials to access services across multiple organisations.¹

Question	Yes	No	N/a	Description
Has the suitability of the alternative				

¹ Note that while individuals and businesses retain the right to choose whether to interact electronically with government the limitation of the choice principle here reflects the narrower context within which the principle of choice applies in relation to e-Authentication.

Principle 7. Choice				
<p>Individuals and businesses will be able to choose whether to use multiple or (where available) aggregated electronic credentials to access services across multiple organisations.¹</p>				
Question	Yes	No	N/a	Description
Implementation Models described in BPG Volume 3 been evaluated?				
Will users be able to use different credentials when accessing services from different/other government agencies?				
Will users be able to use a multi-agency or whole-of-government credential to access these services?				
Will users be able to select different credentials or registration approaches to get access to this service?				
Have users been consulted on their preferences for choice of credential and registration approach for this service, and leveraged use with other services?				

Principle 8. Flexibility				
<p>The NeAF will support diverse e-Authentication approaches aligned to assurance requirements. Agencies can choose the most appropriate e-Authentication approaches on the basis of risk, information classification, public policy and privacy issues.</p>				
Question	Yes	No	N/a	Description
Have multiple e-Authentication approaches been assessed for their applicability?				
Has the assessment approach				

Principle 8. Flexibility

The NeAF will support diverse e-Authentication approaches aligned to assurance requirements. Agencies can choose the most appropriate e-Authentication approaches on the basis of risk, information classification, public policy and privacy issues.

Question	Yes	No	N/a	Description
identified and ranked risk, information classification, user impact and privacy issues for each shortlisted approach?				
Has the selection process detailed the criteria, weighting and scores that resulted in the selection of an approach?				

Principle 9. Cost effectiveness and convenience

e-Authentication processes will be as seamless and as simple as possible. Individuals and businesses will not have to engage in cumbersome and expensive e-Authentication processes for simple or low risk transactions. Where there are benefits to individuals and the use complies with government security and risk management practices it will be desirable for government to implement systems that will give individuals and businesses the option of using e-Authentication processes for multiple government services.

Question	Yes	No	N/a	Description
Have the other agencies with whom the user base also interacts been identified, their requirements-mapped, and their existing approaches been compared?				
Have existing e-Authentication infrastructures and solutions been considered?				

Principle 9. Cost effectiveness and convenience

e-Authentication processes will be as seamless and as simple as possible. Individuals and businesses will not have to engage in cumbersome and expensive e-Authentication processes for simple or low risk transactions. Where there are benefits to individuals and the use complies with government security and risk management practices it will be desirable for government to implement systems that will give individuals and businesses the option of using e-Authentication processes for multiple government services.

Question	Yes	No	N/a	Description
Has a business case been prepared for the selected approach, including consideration of the case for the users?				
Does the selected approach provide the least cost/effort burden on the user among approaches that met the assurance level?				
Is the approach, or elements of the approach, and existing approach being utilised by the users with other agencies?				
Has the approach been offered to other agencies with whom the user interacts?				

CET2 – Transaction analysis checklist

Description of specific part of the service or transaction	Number of Transactions	User Group	Number of Users	Is it necessary to know the identity of any persons, roles or businesses accessing that service?	User e-Authentication capabilities	Other security requirements – confidentiality, integrity, non-repudiation

CET3 - Checklist to help determine whether identity e-Authentication is required

Is identity authentication required?					
Transaction	User group	Information that can only be released to specific identities	Transactions that require knowledge of identity	Are the users already “Known Customers” of the agency?	Can the users be representatives of organisations or other individuals?

--	--	--	--	--	--

CET4 - Checklist to help analyse delivery channels

Analysis of the delivery channels in place and proposed					
Description of delivery channel	Is it a channel already used by the user group?	Are there any other authentication mechanisms for this channel within the Agency?	Are there any specific technology requirements for users of this channel?	Are there any authentication mechanisms for other Agency channels that can be used in this channel?	What other security technologies need to be used in the channel?

CET5 - Risk analysis form

Use this form to evaluate the risk associated with each business process or transaction.

Transaction Description: _____

Category of Harm	Describe Nature of Threat	Severity of Threat/Risk None, Minimal, Low, Moderate, High
Inconvenience to any party		
Risk to any party's personal safety		
Release of personally or commercially sensitive data to third parties without consent		
Financial loss to any client of the service provider ² or other third party		

² 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 or 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.

Category of Harm	Describe Nature of Threat	Severity of Threat/Risk None, Minimal, Low, Moderate, High
Financial Loss to Agency / service provider		
Impact on Government finances or economic and commercial interests		
Damage to any party's standing or reputation		
Distress caused to any party		
Threat to government agencies' systems or capacity to conduct their business		
Assistance to serious crime or hindrance of its detection		

Summary Risk and Probability Assessment	
Aggregate Threat/Risk (based upon highest risk noted above)	None, Minimal, Low, Moderate, High
Mitigating Factors (specify nature of these)	

Residual Risk (after taking into accounting mitigating factors)	None, Minimal, Low, Moderate, High
Probability of Occurrence	Rare, Unlikely, Possible, Likely, Almost certain
Resultant weighted risk to be covered by e-Authentication	None, Minimal, Low, Moderate, High

CET6 - Evidence of relationship risk matrix

*** See Rules and Key at the end of the Tables

				Parties with potential access to user information held on agency files					
Question/ challenge for user	Matching Rules	Evidence of Relationship Challenge Group	POR points	Ex- Part- ner	Family	Friend s	Age nts	Hacke r	Risk Score
Category 1: Primary identifying information – used to identify customer record in agency									
Customer Identifier	Exact match	Identify record	1						9
Name (surname, given names)	Exact match for surname and primary given name	Identify record	1						15
Date of Birth	Exact match	Identify record	1						
Contact address	Exact match	Identify record	1						
etc									

				Parties with potential access to user information held on agency files					
Question/ challenge for user	Matching Rules	Evidence of Relationship Challenge Group	POR points	Ex- Part- ner	Family	Friend s	Age nts	Hacke r	Risk Score
Category 2: General demographic information – used to demonstrate association of customer record with customer									
One or more phone numbers	Match designation (eg home, office, mobile) and number	Associate record with registrant	1						
Street address	Match designation (eg home, office) and detail	Associate record with registrant	1						
Postal address	Exact match	Associate record with registrant	2						
Own, Mother's, Partner's maiden name	Must match if this record exists on customer record		3						
Partner, spouse, dependents names	Must match if this record exists on customer record		4						

				Parties with potential access to user information held on agency files					
Question/ challenge for user	Matching Rules	Evidence of Relationship Challenge Group	POR points	Ex- Part- ner	Family	Friend s	Age nts	Hacke r	Risk Score
etc									
Category 3: Agency dealing information – used to associate customer with record if required assurance level is 3 or 4									
Date of last lodgement		Associate record with registrant	5						
Amount of last claim or payment		Associate record with registrant	5						
Previous, next reporting or lodgement date		Associate record with registrant	5						
etc									
Category 4: Original evidence of identity documents presented									
Australian passport		EOI	5						
Australian drivers licence		EOI	2						

				Parties with potential access to user information held on agency files					
Question/ challenge for user	Matching Rules	Evidence of Relationship Challenge Group	POR points	Ex- Part- ner	Family	Friend s	Age nts	Hacke r	Risk Score
Birth certificate		EOI	3						
Household accounts – supplier name and account numbers		EOI	2						
etc									

KEYS/RULES:

******NB: THESE ARE ONLY INTENDED TO BE ILLUSTRATIVE – AGENCIES SHOULD DETERMINE THE RULES AND WEIGHTINGS FOR THEIR SITUATION**

1. Risk scores assigned to likelihood of knowledge of customer related information

Almost certain	Likely	Possible	Unlikely
4	3	2	1

The risk score is determined by adding the score for each of the five ‘party’ categories.

2. Points assigned to risk scores for Proof of Relationship

The principle applied here is that the higher the risk rating, the lower the reliance that can be place of the

Risk Score	Evidence of Relationship Points
5	10
6-10	7
11-15	5
16-19	2
20	0

3. Points required to meet NeAF Registration Assurance Levels

NeAF Assurance Level	Evidence of Relationship Points Required
Minimal (Level 1)	2

Low (Level 2)	5
Moderate (Level 3)	7
High (Level 4)	10

CET7 - e-Authentication approach analysis form*

E-Authentication approach	Transactions this has been applied to	Strength of registration	Strength of authentication mechanism			Notes
			Technology strength	Credential process management strength	Composite strength	

* This represents a catalogue of existing issued authentication credentials

CET8 - ICT investment framework / business case guide

The ICT Business Case Guide is intended to assist agencies in developing solid Business Cases for investments with significant ICT components to ensure that the recommended course of action:

- contributes to the achievement of Government objectives as reflected in Agency Outcome statements (which are outlined in the agency's Portfolio Budget Statement)
- aligns with the agency's ICT strategic direction and the Government's e-Government Strategy
- is robustly costed and takes into account all relevant costs over the life cycle of the proposal
- provides value for money
- maximises net benefits compared to alternative options
- identifies the risks associated with the initiative and indicates how these will be managed.

The Guide should be used by agency officials who are putting together a Business Case for Budget or internal approval purposes. It provides a framework for evaluating any investment decision or ongoing program with a significant ICT component. The methodology provides for a consistent approach across agencies. While the key principles of the business case should be applied to all relevant capital proposals, they should be applied sensibly and in recognition of the size, sensitivity and risk of the proposal.

A Business Case provides the Government with the information it needs to make a fully informed decision on whether funding should be provided and/or whether an investment should proceed. It should evaluate viable alternatives to reach the desired solution, explain how it delivers value for money, outline resourcing requirements and describe impacts on stakeholders. Most importantly, a Business Case should provide an analysis of the cost, benefits, risks and other important Qualitative information required to evaluate an investment.

A Business Case should fulfil the following key objectives:

- outline the Business Case need
- provide important background and supporting information to contextualise the investment
- describe how the investment aligns with government policy, agency policy and the Responsive Government: A New Service Agenda, 2006 e-Government Strategy, including its four strategic priorities:
 1. meeting user’s needs
 2. building connected service delivery
 3. achieving value for money; and
 4. enhancing public sector capability.
- provide a robust estimate of whole-of-life costs of the investment
- provide a robust estimate of financial benefits of the investment
- provide an estimate of non-financial benefits of the investment
- describe the approach, including timelines, resources, procurement and governance
- provide a rigorous assessment of inherent risks, including how they are likely to impact on the investment and strategies for mitigating them; and
- provide options for the consideration of Government.

Developing a Business Case involves five critical steps, which are outlined in Table 2. It describes the analysis to be conducted, the subsequent outputs and its relation to the Business Case section. Each step in the ICT Business Case Guide comprises the major components of the Business Case content.

Business Case Development Step	Description	Business Case Section
Step 1 Review Environment and Identify Business Need	Assess your current environment to identify the need and context for the investment (include your agency, ICT and Government context).	Identify the Need
Step 2 High-level Options Analysis	Conduct a high-level review and outline of all options that could potentially deliver the desired solution for your agency.	High-Level Options Analysis
Step 3 Detailed Options Analysis	Perform a rigorous analysis of costs, benefits and risks based on options chosen for further analysis in Step 2.	Detailed Options Analysis
Step 4 Develop Appendices to Business Case	Prepare additional information such as the Technical Report, Project Management Plan and Governance Plan etc. (this will depend on the size and risk profile of your proposed investment).	All Appendices
Step 5 Undertake Quality Assurance and Develop Executive Summary	Review your draft Business Case to ensure it is consistent with your agency, Government and ICT strategies, estimates have been quoted correctly and for quality assurance purposes. Develop a concise and illustrative snapshot of the Business Case including mandatory content requirements.	All Sections Executive Summary

The implementation of the NeAF lends itself to applying the methodologies and tools contained in the ICT Business Case Guide. It is recommended that agencies use the ICT Business Case Guide and its related tools to undertake the feasibility analysis on e-Authentication solutions. The Guide is structured in line with the Business Case Template and Evaluation Methodology that must be completed when submitting a Business Case to a range of stakeholders, including Finance. Agencies will find Template that link directly to the Business Case Tool, an Excel®-based application.

The Guide provides a step-by-step account of key considerations and actions necessary to compile the data and supporting information the Government requires to assess a Business Case. Agencies can also use these tools when preparing inter-agency Business Cases for other stakeholders.

Reference: Further information can be found at

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

CET9 - Privacy law compliance checklist

The following Privacy Law compliance (PLC) checklist is framed as a series of questions, most of which are capable of being answered with either a 'yes' or 'no'. In practice, however, agencies should document the explanation and analysis that underpin the answers in order for the report to be a useful decision making tool.

The checklist covers privacy issues raised by both:

- the establishment and use of an e-Authentication approach within the NeAF, and
- the application with which the individual will use the e-Authentication approach.

The purpose of this broader scope for the Privacy Law compliance is that:

- the nature of the privacy concerns raised by the application will be an element in determining whether a digital certificate is the appropriate technology to be used, and
- it will determine, in light of the privacy concerns that the e-Authentication approach raises, whether the use of that e-Authentication approach is still justified.

The checklist is a sample only. It is by no means exhaustive and is intended as a starting point to stimulate discussion of the process and analysis that an agency may undertake to assess privacy risks. The questions are phrased to clearly identify areas of privacy concern. If the answer to a question is 'no', the Privacy Law compliance report should document:

- the reasons, and any legal exceptions or logical exceptions that justify the e-Authentication approach not meeting the privacy concern expressed in the question
- what could be done to make the answer 'yes', and
- if the answer is to remain 'no', what procedures are in place to mitigate the possible effects of the identified risk.

Where there are no legal exceptions permitting deviation from the privacy requirements imposed by law or by binding policy (for example, Gatekeeper

privacy requirements), an agency must take steps to amend the e-Authentication approach or surrounding process so that the answer becomes ‘yes’.

PLC 1 – Use of the e-Authentication approach	Yes	No
Are all four features offered by PKI (e-Authentication, integrity, non-repudiation and confidentiality) necessary for the application? If not, what alternative technology options could be used to provide the necessary features without requiring individuals to procure and use digital certificates?		
PLC 2 – Description of application and e-Authentication approach		
Describe the important features of the application, including the following:		
<ul style="list-style-type: none"> ▪ List the project name for the proposed application, the name of the agency responsible and any agencies involved in the project. 		
<ul style="list-style-type: none"> ▪ Describe the use of digital certificates in plain, non-technical language. 		
<ul style="list-style-type: none"> ▪ Describe the drivers for developing the application and using the e-Authentication approach, including any new needs the application will address and any public benefits it will provide. 		
PLC 3 – Personal information to be collected		
List and describe the personal information (information about an identifiable individual) to be collected in the course of using the application, including:		
<ul style="list-style-type: none"> ▪ identifying information such as the individual’s name or any identifying number assigned to the individual 		
<ul style="list-style-type: none"> ▪ attribute or eligibility information such as the educational, medical, criminal, employment or financial history of the individual 		
<ul style="list-style-type: none"> ▪ evidence of identity information 		
<ul style="list-style-type: none"> ▪ sensitive information³ 		
<ul style="list-style-type: none"> ▪ biometric information 		
<ul style="list-style-type: none"> ▪ categories of individuals or groups the personal information will concern – and the classes of personal information collected for each category 		
<ul style="list-style-type: none"> ▪ any third-party personal information that may be collected. 		

³ If a definition is required, one is included in Section 6 of the Privacy Act 1988.

PLC 4 – Method of collection	Yes	No
<p>Will personal information be collected in using the e-Authentication approach, or in the application, be collected only from the individual to whom the information relates?</p> <p>If no:</p>		
<ul style="list-style-type: none"> ▪ Why can the personal information not be collected from the individual concerned? Why must it be collected from alternative sources? 		
<ul style="list-style-type: none"> ▪ Is the personal information being collected by lawful and fair means? 		
<ul style="list-style-type: none"> ▪ Is the personal information to be collected on one occasion only (that is, not ongoing)? 		
PLC 5 – Purpose, use and disclosure		
Limits on collection	Yes	No
<ul style="list-style-type: none"> ▪ Is the personal information relevant and necessary for using the application? 		
<ul style="list-style-type: none"> ▪ Is there a statutory power, authority or requirement for the agency to collect and use the personal information? 		
<ul style="list-style-type: none"> ▪ Will the information collected not intrude to an unreasonable extent on the personal affairs of the individual (especially evidence of identity information)? 		
<ul style="list-style-type: none"> ▪ Can information be collected in a de-identified (anonymous) or pseudonymous manner? 		
<ul style="list-style-type: none"> ▪ Are individuals given the option of acquiring the services without having to provide some or all of the personal information sought? 		
Purpose	Yes	No
<ul style="list-style-type: none"> ▪ Is personal information obtained in using the e-Authentication approach, or in the application, used exclusively for the purposes made known to and consented to by the individual? 		
Secondary use	Yes	No
<ul style="list-style-type: none"> ▪ If the agency finds a secondary use that can be made of data already collected, is the use consistent with uses notified to or consented to by the individual? ▪ If no: 		
<ul style="list-style-type: none"> ▪ Can an individual opt not to consent to the secondary use and still be entitled to receive the services offered using the original application? 		

Consent	Yes	No
<ul style="list-style-type: none"> ▪ Will notice of the following information be given to the individual at or before collection: 		
<ul style="list-style-type: none"> ▪ The purpose for which the personal information is being collected 		
<ul style="list-style-type: none"> ▪ The collection of the personal information is authorised or required by or under law 		
<ul style="list-style-type: none"> ▪ The people, bodies or agencies to which the collecting agency usually discloses personal information of the kind being collected 		
<ul style="list-style-type: none"> ▪ The individual asked at or before collection to consent to the collection and use of the personal information 		
<ul style="list-style-type: none"> ▪ Uses that the agency considers 'consistent' with the primary purpose (for example, audit trails of transactions) also made known to the individual 		
Disclosure	Yes	No
<ul style="list-style-type: none"> ▪ Is personal information involved in using the e-Authentication approach, or in the application, disclosed to any third party other than those whom the individual has been notified as potential recipients of the personal information? ▪ If no, does some exception under law apply? 		
<ul style="list-style-type: none"> ▪ Is the recipient's use of the personal information limited to the purpose for which it was collected? Will the recipient disclose the personal information to third parties? 		
<ul style="list-style-type: none"> ▪ Will personal information disclosed to third parties be protected from privacy risks to the standard proposed to protect it? 		
PLC 6 – Choice		
Using the e-Authentication approach, use in personal information, multiple certificates/identities	Yes	No
<ul style="list-style-type: none"> ▪ Do agency customers have a choice about whether to use the e-Authentication approach? 		
<ul style="list-style-type: none"> ▪ Can clients choose what use is made of their personal information? 		
<ul style="list-style-type: none"> ▪ Do clients have a choice regarding whether they can hold multiple identities? ▪ Are suitable protections in place if a client wishes to use only one identity? 		

Anonymous/pseudonymous	Yes	No
<ul style="list-style-type: none"> Are anonymous and pseudonymous options made available to clients involved in the application, where appropriate? 		
<ul style="list-style-type: none"> Can clients use substitute services via other means (that is, without using the application) and thereby reduce (or eliminate) the personal information they are required to supply? 		
PLC 7 – Storage		
Security	Yes	No
<ul style="list-style-type: none"> Does the level of security provided in using the e-Authentication approach, or in the application, match the potential harm caused by breaches of privacy? 		
<ul style="list-style-type: none"> Is the individual able to generate their own credentials? 		
<ul style="list-style-type: none"> Are individuals given information about the importance and available means of maintaining credential security? 		
<ul style="list-style-type: none"> Will security measures be reviewed over time to address new potential security hazards (e.g. changes to technology)? 		
Retention and destruction	Yes	No
<ul style="list-style-type: none"> Will a retention policy or destruction schedule be developed which requires retention of personal information only for the period required for use? 		
<ul style="list-style-type: none"> Is personal information de-identified as soon as possible? 		
PLC 8 – Data quality	Yes	No
<ul style="list-style-type: none"> For the purpose for which it is used, will the personal information collected in using the e-Authentication approach, or in the application, be up to date at all stages and on all occasions that it is used, relevant, accurate and complete. 		
<ul style="list-style-type: none"> Will records be maintained of the date of the last update of the personal information held and used by the agency, and the source of updates to personal information? 		
<ul style="list-style-type: none"> Will updates and modifications to personal information be disseminated to all third parties to whom personal information has been disclosed? 		
PLC 9 – Access and correction	Yes	No
<ul style="list-style-type: none"> Can the individual ascertain whether the agency has records that contain personal information, the nature of that information and the steps that individual should take to access their record? 		

<ul style="list-style-type: none"> ▪ Will the costs incurred in accessing personal information be reasonable? 		
<ul style="list-style-type: none"> ▪ Can the data or records about an individual be updated as a result of an individual seeking correction of personal information? 		
<ul style="list-style-type: none"> ▪ Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed? 		
PLC 10 – Potential for aggregation of personal data	Yes	No
<ul style="list-style-type: none"> ▪ Does the manner in which digital certificates are issued, managed and used for the application prevent the use of an individual’s public key as an identifier to link, match or cross-reference personal information about that individual held in different databases? 		
PLC 11 – Public register information		
Certificate revocation lists (CRLs)	Yes	No
<ul style="list-style-type: none"> ▪ Can a subscriber revoke their own certificate? 		
<ul style="list-style-type: none"> ▪ Will steps be taken to ensure that no comprehensive log of CRL accesses is kept? 		
Public key directories	Yes	No
<ul style="list-style-type: none"> ▪ Is it really necessary, by design, for user certificates to be publicly accessible in a directory? ▪ Does the agency ensure that detailed histories of directory checks are not created by the application or by the directory manager? 		
<ul style="list-style-type: none"> ▪ Will steps be taken to restrict directory searches to single specific searches only? 		

CET10 - User impact assessment checklist

1. Access

Use this checklist to analyse the access impacts on individuals and businesses.

Quantify potential access issues					
What bandwidth is required for the e-Authentication approach?	What computer level is required for the e-Authentication approach?	What features might prevent physically impaired users from using it?	Will the e-Authentication approach require specific hardware, software or Operating System?	Rate the access ability for individuals and small, micro and home-based businesses (H, M, L)	Describe any geographic requirements for the approach

--	--	--	--	--	--

2. Equity

Use this checklist to analyse the equity impacts on individuals and businesses.

Quantify potential equity issue					
What channels are available for the user to access?	What disadvantages would the individual or business suffer by using other channels?	What incentives or disincentives?	What special user groups could be unduly affected?	Rate effect on those groups (H, M, L)	Describe any additional imposts on individuals and businesses

3. Impositions

Use this checklist to analyse the impositions on individuals and businesses.

Quantify potential imposition					
User group	What travel requirements could this group be subject to?	What tokens or credentials could this group need to carry?	What will this group need to remember?	What complex security requirements will this group have to meet?	What liability or legal requirements will be placed on individuals or staff or owners of businesses?

Quantify potential imposition					
User group	What travel requirements could this group be subject to?	What tokens or credentials could this group need to carry?	What will this group need to remember?	What complex security requirements will this group have to meet?	What liability or legal requirements will be placed on individuals or staff or owners of businesses?