Australian Government

Digital Transformation Office

National e-Authentication Framework

Better Practice Guidelines – Vol 2 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

Contents

CET11 – Checklist to analyse compliance with website authentication principles 4

CET12 – Transaction analysis checklist (for website authentication) 8

CET13 – Identifying user groups and their needs 9

Identify the user groups and their needs and capabilities 9

CET14 – Website mutual authentication analysis form 10

CET8 – ICT Investment Framework / Business Case Guide 12

CET10 – User impact assessment checklist 14

1. Access 14
2. Equity 15
3. Impositions 16

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

CET11 – Checklist to analyse compliance with website authentication principles

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

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

Principle	**Compliance**			**Notes**
	Yes	**No**	**N/a**	
Principle 1: Web server authentication A user should authenticate a government web site/server, since an unauthenticated web site/server can easily ask for confidential information from the user.				
Principle 2. User involvement in web site authentication Many solutions to web site authentication rely on user involvement to distinguish between trusted or untrusted sites. Some users (unsophisticated or unmotivated) cannot be relied upon for this purpose. Web site authentication solutions must extend beyond technology to include user education, and agency detection and prevention initiatives aimed at reducing reliance on user involvement. (These extensions may be best performed on a Whole of Government basis). Examples of agency initiatives to reduce reliance on user involvement include • the use of vendors or organisations – e.g. Anti-phising Working Group (APWG) – who scan email on the net to detect phishing attacks, and notify agencies of such attacks;				

Principle	Compliance			Notes
	Yes	No	N/a	
• the use of vendors who monitor domain name registrations to notify agencies of new registered names that could be potentially used for spoofing; • the implementation of appropriate protections for DNS servers; and • the implementation of appropriate protections for agency web site servers (e.g. to prevent hacking of authentic web site content) , including the use of firewalls, intrusion detection and prevention, digital hashes of web site content and monitoring of changes to digital hashes to identify any successful hacker attacks on the content of web pages. (There are also Common Criteria verified vendor products available to create a baseline of all web server files to detect and pinpoint changes and report them to the appropriate manager). Examples of subjects for user education (similar to the NetAlert initiative) include • how to verify/validate web site digital certificates; • where relevant, how to obtain, protect, and use authentication techniques (how to obtain credentials, how to logon, etc); • how to protect against attacks on the user's computer which could be used to compromise access to authentic sites (spyware, key stroke loggers, etc) using anti-spyware and anti-virus software, Windows firewall, etc; • how to identify and respond to spam emails (e.g. the SpamMatters initiative), and respond to broken image links; • how to use spam filtering, content filtering, popup blocking, and new protections as they emerge e.g. DomainKeys Identified Mail (DKIM); and				

Principle	Compliance			Notes
	Yes	No	N/a	
• how to apply security patches and updates, and so on.				
Principle 3: Mutual authentication Where user authentication is required by the government web site, web site authentication solutions should ideally integrate with user authentication mechanisms, so users are trained to use a single mutual authentication mechanism.				
Principle 4: User credentials Any user credentials used should be fit-for-purpose for the web site application. Where username/passwords are used, clear-text passwords must not be revealed during any phase of authentication, since an attacker can fool the user into completing any standard process. Where username/password authentication is inadequate, stronger alternatives such as digital credentials, secure tokens, smartcards, etc., should be considered. If a federated approach to authentication is to be adopted, either the credentials for all web sites will need to involve credentials which are strong enough to meet the most stringent requirement, or weaker credentials need to be disallowed by sites requiring stronger credentials (e.g. as provided for in the three different grades of Gatekeeper digital certificates).				
Principle 5: Web site credentials Gatekeeper Device certificates should be considered as the base level for any use of digital certificates for identifying government web sites.				
Principle 6: Authentication techniques The authentication mechanism used should be fit-for-purpose for the web site application. If a federated model for authentication is adopted, authentication mechanisms may need				

Principle	Compliance			Notes
	Yes	No	N/a	
to reflect the requirements of the web site requiring the highest protection.				
Principle 7: Trusted channels Use of channels such as SSL/TLS should use a Gatekeeper Device certificate at the web server, combined with user training on certificate verification, because an attacker can also offer a SSL/TLS channel using a self-signed certificate. In order to protect authenticating credentials against human man-in-the-middle attacks, strong cryptography must be an element of any solution. Trusted user interfaces for authentication must be at least based on a shared secret, communicated out of band, since all user interfaces are spoofable.				
Principle 8: Client-side active content The risks and benefits of active content technology on the client-side should be carefully assessed before it is implemented. User input should be validated at the web server, even if already validated by the active content of the user's browser.				
Principle 9: Web site content The content published by public government web sites should be formally justified (e.g. by the 'need to know' of the intended audience), formally approved, and formally managed. The NeAF includes coverage of information classified at Highly Protected and above. Public government web sites should not contain classified information. Where necessary, appropriately secured internal web sites (intranets) may be used for this purpose.				

CET12 – Transaction analysis checklist (for website authentication)

Description of specific part of the service or transaction	Number of Transactions	User Group	Number of Users	Is it necessary for the individual or business to determine the authenticity of the agency website?	User e-Authentication capabilities

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

CET13 – Identifying user groups and their needs

Identify the user groups and their needs and capabilities

User groups	Group demographics (size, location)	Rate each group's technology capabilities (H, M, L)	Rate each group's technology familiarity and security awareness levels (H, M, L)	Rate each group's cost profile

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

CET14 – Website mutual authentication analysis form

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

Transaction/Service Description:_____

Category of Harm	**Impact/Severity and Probability of Threat/Risk** **None, Minimal, Low, Moderate, High**				
	Phishing	**Pharming**	**Man-in-Middle** **Replay Attacks**	**Spyware**	**Other (describe)**
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[1] or other third party					
Financial Loss to Agency / service provider					
Impact on Government finances or economic and commercial interests					

[1] 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.

Category of Harm	**Impact/Severity and Probability of Threat/Risk** **None, Minimal, Low, Moderate, High**				
	Phishing	**Pharming**	**Man-in-Middle** **Replay Attacks**	**Spyware**	**Other (describe)**
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)	Insignificant, Minor, Moderate, Major, Severe
Mitigating Factors (specify nature of these)	e.g. user education, surveillance of and response to (phishing, pharming, etc)
Residual Risk (after taking into accounting mitigating factors)	Insignificant, Minor, Moderate, Major, Severe
Probability of Occurrence	Rare, Unlikely, Possible, Likely, Almost certain
Resultant weighted risk to be covered by e-Authentication	None, Minimal, Low, Moderate, High

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; and
- 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
    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 1. 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.

Table 1

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:

ICT Business Case Guide, Australian Government Information Management Office (AGIMO), 2006, located at http://www.finance.gov.au/budget/ict-investment-framework/business-case-guide.html

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

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

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?

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