Australian Government

Digital Transformation Office

National e-Authentication Framework

Better Practice Guidelines – Vol 2
Website 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

© 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

FIGURES

INDEX OF TABLES

1. Introduction

1.1. Objectives

Enabling the authentication of government websites is seen as important to increase trust levels for individuals and businesses dealing with government electronically.

As shown in Figure 1, there are some fundamental questions that must be answered for any online initiative in government to be trusted.

Figure 1: Fundamental Questions Requiring Answers in e-Authentication

1. Can the website trust this user? **2. Is the traffic between the parties secure?** **3. Can the user trust this website?**

The major objectives of Volume 2 are to use the NeAF to develop and implement an e-Authentication approach for authentication of Government websites – i.e. to satisfy Question 3 in Figure 1 above.

Questions 1 and 2 are addressed by the NeAF and Volumes 1, 3 and 4 of the Better Practice Guidelines.

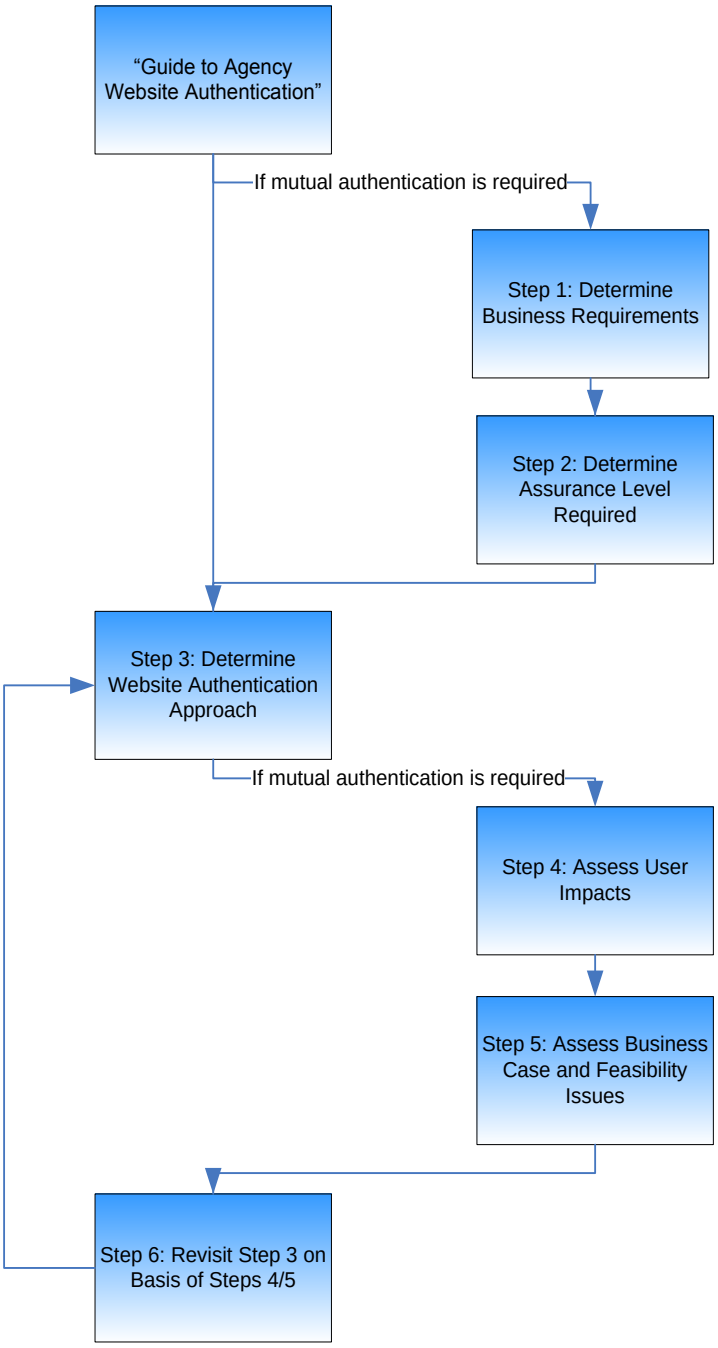
This volume should assist agencies to:

- identify the business requirements for e-Authentication of their website(s)
- determine the assurance levels for that authentication
- determine the authentication approach for their website(s)
- assess the privacy and public policy implications of their approach to authenticating their website; and
- assess the business case and feasibility of their approach to authenticating their website.

1.2. Summary of Steps

Figure 2 shows the six steps involved in utilising the NeAF to identify the authentication approach of an Agency's website.

Figure 2: Steps covered in Volume 3



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

1.3. Background

1.3.1. Why Website Authentication

Enabling the authentication of government websites is seen as important to increase trust levels for individuals and businesses dealing with government electronically.

The impact of poor website authentication can be felt in many ways. Some of the potential impacts are:

- **Identity theft –** Users may become the victims of identity theft through providing personal information to a spoofed 'government' web site
- **Fraud –** Users or service providers may be subject to one-off or ongoing phishing fraud
- **Reduced consumer confidence, trust, service take-up –** Users may be reluctant to migrate to e-services owing to fear of identity theft and other security breaches
- **Privacy breaches –** Personal information may be disclosed without user consent; or
- **Liability –** Agencies, organisations and third party service providers may become liable for loss resulting from their role in a security or privacy breach.

Further detail on the rationale for providing e-Authentication of government agency websites to users is provided in Section 5 of the *NeAF Framework* document.

For more detail on the types of attacks that can be used against users of websites, see the *Guide to Website Attacks* in Attachment 1.

1.3.2. Planning principles for website authentication

The planning principles for website authentication provided below have been adapted from a range of vendor-developed (e.g. Google and Microsoft) position papers submitted to the World Wide Web Consortium W3C, and from prior documents developed for Finance. These principles should be considered when using NeAF to inform the implementation of website authentication, and they are:

- Principle 1: Web server authentication
- Principle 2. User involvement in website authentication
- Principle 3: Mutual authentication
- Principle 4: User credentials
- Principle 5: Web ite credentials
- Principle 6: Authentication techniques
- Principle 7: Trusted channels
- Principle 8: Client-side active content
- Principle 9: Website content

CET11- Checklist to Analyse Compliance with Website Authentication Principles provides detail on each principle and provides a form for noting level of compliance.

It is important to note that agencies will usually be significantly reliant on some user involvement to distinguish between trusted or untrusted sites.

As a consequence:

- agency website initiatives should extend beyond technology to:
  - include user education

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

  - encompass policies to help employees and business/groups to use web authentication properly to reduce the risk of intentional and inadvertent misuse
- agencies should initiate detection and prevention initiatives aimed at reducing reliance on user involvement.

Examples of subjects for user education (similar to the NetAlert initiative) include:

- using browser help information to better understand web site security e.g. Internet Explorer Help topics such as “How to decide if you can trust a website”, and “How to know if an online transaction is secure”
- using browser security settings, including:
  - the use of trusted and restricted Internet sites
  - how to ensure warnings about untrusted content are displayed
  - how to ensure prompts are displayed when web sites attempt to use restricted protocols for active content
- how to verify/validate website digital certificates
- for mutual authentication, how to obtain, protect, and use authentication techniques (how to obtain credentials, how to logon)
- how to protect against attacks on the user’s computer which could be used to compromise access to authentic sites (examples include spyware, key stroke loggers) using anti-spyware and anti-virus software, Windows firewall
- 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
- how to apply security patches and updates.

Examples of agency initiatives to reduce reliance on user involvement include:

- the use of vendors or organisations (e.g. the Anti-Phishing Working Group) who scan email on the net to detect phishing attacks, and notify agencies of such attacks
- 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[1]; and
- the implementation of appropriate protections for agency web site servers (e.g. to prevent hacking of authentic website 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.)

1.3.3. Assurance framework

Indicative web site assurance levels and criteria are provided in Table 3 on page 15. This provides a guideline only and should be used as input by agencies in their risk assessment processes. Additionally, there are several caveats associated with this schedule:

- The words ‘realised threat’ in the example descriptions provided in Table 3 are generic, and include (for example) a failure to meet confidentiality, integrity, and availability requirements of information or services delivered (or initiated) by the web site, whether as a result of force majeure

[1] See NIST, Guidelines on Securing Public Web Servers, Version 2, September 2007, http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf.

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

organisational shortcomings, human error, technical error, or deliberate acts of internal or external parties. (Actual risks must be assessed and rated in detail by the agency itself, i.e. Table 3 should not be used as it stands.)

- The words ‘minimal’, ‘minor’, ‘significant’ and ‘substantial’ are relative, and differences in agency purpose, size, threats, and risks will mean their meaning is agency-specific. For example, a ‘minor’ financial loss for one agency may be a ‘significant’ financial loss for another, or a ‘substantial’ loss for a client of an agency. Agencies should develop their own criteria for the interpretation of these assessments.

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

2. Step 1: Determine Mutual Authentication Business Requirements

This first step is required if mutual authentication is to be used. If website authentication only is under consideration, then agencies can go directly to 4. Step 3: Determine the Web Site Authentication Approach under Figure 2. Mutual authentication includes technologies such as keypad personalisation and browser chrome enhancements (described in Attachment 2: Bibliography), which augment user authentication and concurrently assist with website authentication. The design of the user authentication mechanism is a prerequisite to the design of the website authentication enhancements.

The major objectives of Step 1 are to do an initial scoping of the approach to mutual authentication for a website (or cluster of websites), and plan how to undertake the remaining processes described in this Volume. Agencies will analyse the users of the website, assess the purposes for which they use the website, analyse the information and transactions available on the website, and describe what could happen if the information was lost, altered or stolen or transactions incorrectly entered into (e.g. with a bogus or spoof site).

The first step is therefore to ensure that there are up-to-date descriptions for all relevant electronic business processes and information stores accessible through the relevant website(s). Experience suggests that relying solely on formal documentation such as application descriptions and procedures manuals is likely to be inadequate as these may be out of date.

In order to set the stage for analysing mutual authentication needs and designing mutual authentication measures, an agency will need to gather information, including statistics (or at least estimates) on:

- the types and volumes of relevant electronic business processes and exceptions
- the categories of direct users, (including, staff, contractors, staff and contractors of partner organisations, customers, etc.) and number of users
- the categories of indirect users (that is, people or organisations that are affected by the system, even if they do not use it e.g. those represented by agents and guardians) and number of such users
- the number of locations involved
- other relevant characteristics.

Use *CET12-Transaction Analysis Checklist* to collate information regarding transactions and user groups.

Agencies should consider the capability of each user group to use the mutual authentication approach, including familiarity with online systems, the equipment they are using, the bandwidth of their connection and their familiarity with English. This information will be used in Step 4 *Assess User Impacts*.

Use *CET13-Identifying User Groups and their Needs* to collate further user group information.

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

3. Step 2: Determine the Assurance Level Required

If mutual authentication is under consideration, it is important that Step 1 produces clear descriptions of the information and business processes that will be provided through the website.

Building on that work, this task involves assessing the significance of each of the information stores and transactions, in particular, whether there are serious consequences to both user and agencies if the system is compromised, i.e. data is accessed, deleted, changed or stolen, or fraudulent transactions are entered.

The objectives of the processes described in this step are to determine the level of assurance required for users of a particular electronic transaction or usage of a website, and therefore what assurance level is required in the mutual authentication mechanism. These objectives are met through undertaking a Threat/Risk Assessment and an Information Classification.

This is a critical step because the solution options for mutual authentication are limited, and their fit to assurance levels will have a high bearing on their availability as an option.

Agencies should undertake this cataloguing and assessment on a group basis, with all key stakeholders represented in making the final evaluation. Threat/risk assessments for transaction identity authentication mechanisms can be used as inputs into this process where those transactions are provided by the website under review.

The following table 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

Category of harm	Description of impacts
Financial	Financial loss by any party
Performance	Adverse impact on the performance of any business's functions
Productivity	Adverse impact on the productivity of any business
Public confidence	Adverse impact on the confidence with which any party regards the relevant business processes
Reputation	Adverse impact on the reputation of any business as well as that of the agency
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 business
Privacy	Adverse impact on the privacy of any person

Category of harm	Description of impacts
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

When assessing the impact of a threat, agencies should use their own risk impact matrix. An example is provided in *Better Practice Guide Volume 1, Step 5 – Assess assurance level required to cover residual risk*.

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 website or user processes – generally targeted at a single user;
- **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**. Where the impacts of some kinds of accidents may result in very substantial harm, for example, a large scale phishing attack on Australian email addresses affecting large numbers of users of a particular agency website. 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.

Use *CET14- Website Mutual Authentication Analysis Form* to complete a risk assessment for each business process or transaction. Include for each category of harm:

- a description of each threat identified
- a description of the consequences that would arise if each of those threats eventuated
- an assessment of the seriousness of the consequences, rated as Insignificant, Minor, Moderate, Major or Severe
- an assessment of the likelihood of 'attack'.

  In completing this action, agencies should refer to *Attachment 1: Current Attacks on Websites.*

The next step is to assess the mitigating factors – the 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 common risk mitigation factors for mutual authentication include:

- before the fact: user education, antivirus/antispam/antispyware software
- during the fact: informing users of recent activity; and
- after the fact: monitoring unusual activity, consider multi-factor e-Authentication approaches for user identity.

Continue completion of *CET14 – Website Mutual Authentication Analysis Form* noting mitigating factors for each identified threat.

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. Note that this strategy may or may not include risks to the users of an agency website.

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 and/or the users 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, or treatments, 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 investigate and address them, and audit processes[2].

Review existing risk management strategy or develop a risk management strategy if none exists.

Agencies need to evaluate the probability of each kind of threatening event occurring, and the residual risk, which is what remains after applying mitigating factors to the intrinsic risk.

This task involves agencies quantifying or qualifying that residual risk.

Finalise completion of *CET14 – Website Mutual Authentication Analysis Form* including information about the likelihood of the harm arising (Almost certain, Likely, Possible, Unlikely, or Rare – see *Better Practice Guidelines Volume 1, Step 5*).

The final task for agencies is to use the information developed during the Threat/Risk Analysis to determine which of the four assurance levels the mutual e-Authentication process will need to satisfy in order to mitigate the residual risk.

Note that e-Authentication solutions may not always be the most appropriate form of risk mitigation.

[2] For greater detail on developing a risk management plan, agencies should refer to the Risk Management Standard AS/NZS 4360, and the ANAO Better Practice Guide on Risk Management.

Table 2: Illustrative consequences and severity

Criteria	Assurance levels			
	Minimal	**Low**	**Moderate**	**High**
	Level 1	**Level 2**	**Level 3**	**Level 4**
Inconvenience to any party	Minimal (A realised threat to information or services delivered or initiated by the web site will cause minimal or minor inconvenience)	Low (A realised threat to information or services delivered or initiated by the web site will cause significant inconvenience)	N/A	N/A
Risk to any party's personal safety	No (A realised threat to information or services delivered or initiated by the web site will have no impact on personal safety)	No (A realised threat to information or services delivered or initiated by the web site will have no impact on personal safety)	No (A realised threat to information or services delivered or initiated by the web site will have no impact on personal safety)	Yes (A realised threat to information or services delivered or initiated by the web site will have a significant impact on personal safety)
Release of sensitive personal or commercial data to third parties.	No (The information or services delivered or initiated by the web site do not collect, provide or use any personal or commercially sensitive data)	No (The information or services delivered or initiated by the web site do not collect, provide or use any personal or commercially sensitive data)	Yes (The information or services delivered or initiated by the web site collect, provide or use personal or commercially sensitive data)	Yes (The information or services delivered or initiated by the web site collect, provide or use personal or commercially sensitive data)
Financial loss to any party	Minimal (A realised threat to information or services delivered or initiated by the web site will cause minimal financial loss)	Minor (A realised threat to information or services delivered or initiated by the web site will cause minor financial loss)	Significant (A realised threat to information or services delivered or initiated by the web site will cause significant financial loss)	Substantial (A realised threat to information or services delivered or initiated by the web site will cause substantial financial loss)
Damage to any party's standing or reputation	No (A realised threat to information or services delivered or initiated by the web site will cause no damage to a party's standing or reputation)	Minor (A realised threat to information or services delivered or initiated by the web site will cause minor damage to a party's standing or reputation)	Significant (A realised threat to information or services delivered or initiated by the web site will cause significant damage to a party's standing or reputation)	Substantial (A realised threat to information or services delivered or initiated by the web site will cause substantial damage to a party's standing or reputation)
Distress being caused to any party	No (A realised threat to information or services delivered or initiated by the web site will not cause any distress)	Minor (A realised threat to information or services delivered or initiated by the web site will cause minor distress)	Significant (A realised threat to information or services delivered or initiated by the web site will cause significant distress)	Substantial (A realised threat to information or services delivered or initiated by the web site will cause substantial distress)
Threat to agencies' systems or capacity to conduct their business	No (A realised threat to information or services delivered or initiated by the web site will not impact on an agency's systems or capacity to conduct business)	No (A realised threat to information or services delivered or initiated by the web site will not impact on an agency's systems or capacity to conduct business)	Moderate (A realised threat to information or services delivered or initiated by the web site will have a moderate impact on an agency's systems or capacity to conduct business)	Significant (A realised threat to information or services delivered or initiated by the web site will have a significant impact on an agency's systems or capacity to conduct business)
Assistance in commissioning serious crime or hindering its detection	No (A realised threat to information or services delivered or initiated by the web site will not assist in the commission of a serious crime, or will not hinder its detection)	No (A realised threat to information or services delivered or initiated by the web site will not assist in the commission of a serious crime, or will not hinder its detection)	Yes (A realised threat to information or services delivered or initiated by the web site will assist in the commission of a serious crime, or will hinder its detection)	Yes (A realised threat to information or services delivered or initiated by the web site will assist in the commission of a serious crime, or will hinder its detection)
Extent of threat to government classified information and related assets	No (A realised threat to information or services delivered or initiated by the web site is not a threat to government classified information and related assets)	No (A realised threat to information or services delivered or initiated by the web site is not a threat to government classified information and related assets)	No (A realised threat to information or services delivered or initiated by the web site is not a threat to government classified information and related assets)	Yes (A realised threat to information or services delivered or initiated by the web site is a threat to government information and related assets.

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

While the above process determines the consequences of getting mutual authentication wrong, it is also necessary to map 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

	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 consequences and likelihood used for this table should be those derived from the agency's risk management framework.

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."

4. Step 3: Determine the Web Site Authentication Approach

4.1. Website authentication mechanisms

If mutual authentication is required, then agencies should also refer to Volume 1 for guidance. This volume largely deals with the enhancements to authentication of users that improves website authentication.

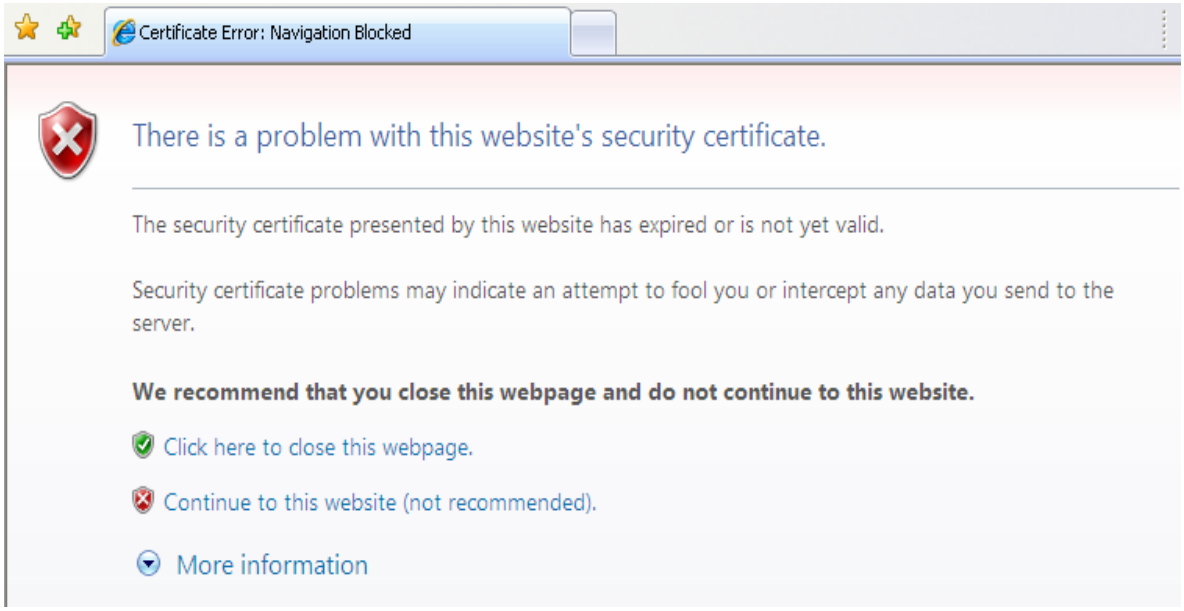
If mutual authentication is not required, then some of the website authentication mechanisms described below are no longer relevant. For example, keypad personalisation and browser chrome enhancements are used to augment user authentication mechanisms, and these will no longer be relevant.

The sample Website Authentication Mechanisms schedule (see *Schedule 1*) provides an indication of the strength of each mechanism, and should guide agencies in the selection on appropriate mechanisms to authenticate the website. At the basic level, use of SSL/TLS with a Gatekeeper compliant Device certificate may be appropriate up to assurance level 4. This may be complemented by locked cookies and domain-name strengthening. (The Gatekeeper compliant certificate, combined with user training on certificate verification, is used to help overcome the issue of spoofed sites offering SSL/TLS channels using a self-signed certificate.)

The use of SSL/TLS in conjunction with a Gatekeeper compliant Device certificate (acting as the web server credentials) is desirable even in cases where mutual authentication is not an issue. In this case, SSL/TLS is not being used because of its encryption capabilities, but rather as a mechanism to present the web server certificate for verification by the user's browser.

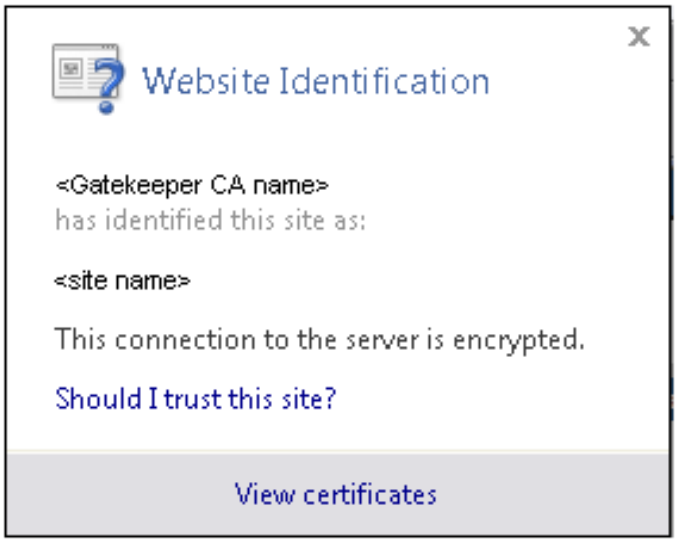
If there are security concerns with this certificate the browser will present warnings to the user. An Internet Explorer example is provided below:

Figure 3: Example website certificate warning message



If there are no security concerns, the user can still click on the relevant symbol (e.g. the lock in Internet Explorer) which will allow the user to check the certificate and/or access Help information on whether to trust the site or not. An example of a typical Internet Explorer message displayed to the user in this case is shown below:

Figure 4: Example website identification message



If SSL/TLS is also being used to meet an encryption objective e.g. as part of mutual authentication, then the requirements of the Australian Government ICT Security Manual (ISM) should be followed, i.e.

- agencies should not use versions of SSL prior to version 3.0; and
- agencies permitting SSL or TLS through their gateways should implement:
  - a product that decrypts and applies content filtering to SSL traffic; and/or
  - a whitelist specifying the external addresses to which encrypted connections are permitted, with all other addresses blocked.

As SSL and TLS do not protect data during storage, there is usually a greater risk that data will be accessed while stored at either end of the communication path, where SSL/TLS does not protect it.

- Agencies should review and mitigate this risk where appropriate; possible solutions include encryption of all or part of the data and/or positioning the data in a zone that is decoupled from Internet access.

4.2. Assessment criteria

Authentication approaches are assessed based on criteria outlined in Table 4.

Table 4: Website authentication mechanism assessment criteria

Assessment Criteria	Description
A. Ease of use	This criterion assesses whether the Website Authentication (WA) approach can be used and understood by ordinary consumers.
B. Cost	This criterion compares the costs to both the agency and website users of the WA approaches being considered.
C. Effectiveness	This criterion assesses whether the WA approach is effective against common forms of attack. Sub-criteria include: • effectiveness against phishing; • effectiveness against pharming; • effectiveness against Man-in-the-middle and Replay Attacks; and • vulnerability to further attack. (Many WA approaches are themselves vulnerable to further attacks – there is the potential that a WA approach helps to eliminate on security risks but enables another one.)
D. Suitability for whole-of-government	This criterion assesses suitability for a Whole of Government approach to WA. Sub criteria will include: • alignment or integration with approaches to individual authentication; • ability to enable consistent user experience and interfaces across services and agencies; • ability to be used across a diverse range of services and channels; and • compliance with government policies (e.g. in relation to DNSSEC requirements).
E. Support / maturity	This criterion assesses the maturity of the approach and whether or not it was sufficiently supported. Sub criteria include: • organisational maturity; • technological maturity; • level of openness of the approach; • level and availability of industry support; and • number of existing or planned implementations.

Assessment Criteria	Description
F. Responsiveness	This criterion assesses whether the approach can assist / enable timely responses to attacks or vulnerabilities. Sub criteria include: • ability to identify and measure attacks and breaches; • ability to alert consumers of attacks and breaches; and • ability to issue alerts across whole of government.

4.3. Assessment criteria rating methodology

A set of ratings have been developed to allow a comparable assessment of the technologies considered in this report. It should be emphasised that such criteria based numerical ratings should not be read in isolation, but rather in conjunction with the description of each website e-Authentication technology, given the variety of technologies considered.

Table 5: Website authentication approach – criteria rating

Rating	Classification	Notes
-	Criteria not applicable to this technology	
0	Not compliant	Technology does not provide for this criterion.
1	Minimal compliance with assessment criterion	Can be used in an approach that has a higher level of compliance Immature approach/technology Proprietary, limited industry/open source support
2	Moderate compliance with assessment criterion	Provides basic/limited support Some commercial or open source implementations Maturing – some industry support/standards
3	Significant compliance with assessment criterion	Industry standard approach Successful large-scale commercial and open source implementations Approach largely delivers capability with some gaps
4	Fully compliant with assessment criteria	Approach is designed from the ground up to provide this capability Many successful large-scale commercial and open source implementations across multiple industries including government

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

The sample Website Authentication Technology Assessment Schedule (see *Schedule 2*) uses the above scoring approach. This sample can be used in conjunction with an agency's own analysis to identify possible authentication approaches that meet both the required level of assurance and also meet all of the identified criteria.

Typically, more than one approach may be suitable. In such cases, agencies will need to make a selection, taking into account factors such as usability, cost and current agency support.

In choosing a default website authentication approach, it is important not to demand unnecessarily high assurance. Higher assurance approaches are generally more costly and less convenient for users. Feedback from business focus groups[3] is that they believe government often demands unnecessarily strong security that is not commensurate with business norms.

Agencies should select the most suitable website authentication approaches from the list developed in this Step, by applying the following criteria:

- meets required assurance level; and
- complies with the assessment criteria that are determined to be important for the agency and the users.

[3] The feedback was obtained as part of the *Privacy and public policy impact assessment* undertaken by the Australian Government Information Management Office (AGIMO) of the Department of Finance and Deregulation during June 2004.

5. Step 4: Assess the User Implications

In general a Privacy Impact Assessment is not required, as this should be done as part of the determination of the User e-Authentication approach.

Due to the complexity of some of the potential mutual authentication solutions, and the strong need for user education as a key part of the solution for mutual authentication, a User Impact Assessment should be undertaken to uncover any potential problems with the selected approach.

An agency needs to perform this task only if it determines that a consultative user impact assessment is necessary e.g. where:

- preliminary assessment has concluded that there may be a considerable impact on a user group
- relevant representative organisations or advocates have expressed concerns about the proposal
- the categories of user groups have not previously used substantial or onerous mutual authentication processes
- user groups are not represented by associations experienced in using mutual authentication; or
- willing engagement of the user or other organisations is necessary for the project to succeed.

Schedule 2-Website authentication – technology assessment schedule provides an assessment of a range of usability and other impacts of different mutual authentication mechanisms.

5.1. Factors to consider

The three key factors to consider are:

- **Access**. This has to do with the general issue of physical and electronic access to services/technologies, but also covers the key issue of the usability of technology for less technology-literate users and users with disabilities
- **Equity**. This has to do with ensuring, as far as is possible, equivalence in service delivery for all eligible categories of users; and
- **Imposition**. This has to do with the imposition of cost and/or effort on users.

The *CET10 – User impact assessment checklist* provides a structured basis for undertaking this task.

In general governments are committed to provide accessible service approaches. See http://www.finance.gov.au/e-government/service-improvement-and-delivery/publication-guidelines/accessibility.html

Agencies can use the following checklist to decide whether access may be an issue:

- Will users from any geographic location be able to use the online service through the proposed mutual authentication approach?
- Will users with physical impairments be able to use the online service through the proposed mutual authentication approach?
- Will the proposed mutual authentication approach prevent any specific group of users from accessing the online service?

See also http://www.w3.org/WAI/intro/accessibility.php

Agencies may need to take particular care with categories of users that are the subject of government policy, such as regional, rural and Indigenous users.

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

6. Step 5: Assess the Business Case and other Feasibility Issues

This step is only likely to be required in the case of mutual authentication. Website authentication on its own is a relatively simple and straightforward task, and is unlikely to justify the overhead of a formal business case.

As agencies undertake the mutual authentication tasks outlined above, it will be important to gather the information necessary to develop a high-level cost-benefit analysis.

In undertaking this exercise, the NeAF recommends that agencies use the *ICT Business Case Guide* methodologies (see *CET8 – ICT Investment Framework / Business Case Guide* for greater guidance). For the mutual authentication mechanism it will be suggested to utilise the complete process from the Guide:

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

In undertaking Tasks 2 and 3, agencies should consider the relative costs and benefits of different approaches to website authentication as well as considering the 'null' case – i.e. not providing any form of website authentication.

6.1. Costs

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

Table 6: 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 mutual e-authentication policies and procedures, including the development of a mutual e-authentication assurance level profile 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 websites with mutual e-authentication mechanisms	There are opportunities for savings from whole-of-government purchasing (of solutions or services) and shared learning across agencies.

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

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

Table 7 identifies the key ongoing costs, together with opportunities to reduce costs.

Table 7: Ongoing costs

Area of ongoing cost	Collaboration/rationalisation opportunities
Education and training Development and deployment of 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 staff, computer room utilities, ongoing web site content updates, hardware maintenance, telecommunications	Whole-of-government hosting and/or shared 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 learning will reduce this cost.
Legal costs Cost of personalising MOUs to be exchanged between issuers of trust and relying parties	Whole-of-government purchasing and/or shared learning will reduce this cost.

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

6.2. Benefits

Table 8 identifies the key quantifiable benefits, together with the data required to achieve the computation of benefits in dollar terms.

Table 8: Benefits

Value category	Benefit	Data required for computation
User benefits	Reduction of identity theft caused through spoofing, phishing or pharming	1. Audience categories and sizes 2. Cost of average identity theft 3. Average incidence of identity theft.
Government financial benefits	Reduction in cost of infrastructure and operational services for providing online access to externals	1. Fully implemented and deployed cost of platforms per agency 2. Deployed cost of whole-of-government infrastructure (as an alternative).
Government operational or foundational benefits	Reduction in use of non-electronic delivery channels	Cost of non-electronic service delivery and percentage of this that will be saved.

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

7. Step 6: Review the Website Authentication Approach

Agencies need to determine the feasibility of the mutual authentication approaches identified in Step 4. Possible outcomes of this process are:

- moving to a fuller design of the mutual authentication approach and a project plan for its implementation, or
- revisiting Step 2 to reassess risks and the nature and extent of other risk mitigation factors, and/or
- revisiting Step 4 to determine other possible approaches to mutual 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' mutual 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 website pending more favourable agency and/or user circumstances emerging.

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

Agencies should also revisit *CET11- Checklist to Analyse Compliance with Website Authentication Principles* to determine their degree of compliance with the Website Authentication Principles.

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

Schedule 1: Website authentication mechanisms

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

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

Website Authentication Mechanism	**Use**	**Implementation issues, Standards, Suitability for Use**	**Variables Affecting Strength of Mechanism**	**Indicative Assurance levels**			
				Level 1	**Level 2**	**Level 3**	**Level 4**
SSL/TLS	Provides both client and server authentication, and communication encryption.	Vulnerabilities well understood. Implementations can eliminate man-in-the-middle attacks e.g. by using Gatekeeper compliant Device Certificates at the servers.	Assurance level of server certificate, user training.	✓			✓ if Device cert used
Gatekeeper compliant Device Certificates	Provides stronger authentication (based on Gatekeeper PKI) of web servers using SSL/TLS.	See above. Requires obtaining a device certificate from a Gatekeeper accredited CA. (Can also be used with Gatekeeper compliant certificates for the client side).	See above.	✓ when used in conjunctions with SSL/TLS – see above			
Browser Chrome Enhancements	Complimentary technology. Relies on users to authenticate web sites, aided by plug-in tools.	Requires implementation of plug-ins by user on every computer they use, and operation often requires significant user involvement.	User training, motivation and sophistication.	✓			

Website Authentication Mechanism	Use	Implementation issues, Standards, Suitability for Use	Variables Affecting Strength of Mechanism	Indicative Assurance levels			
				Level 1	Level 2	Level 3	Level 4
Trusted Password Windows and Dynamic Security Skins	Complimentary technology. Relies on users to authenticate web sites, and may be aided by plug-in tools.	May requires implementation of plug-in by user, and operation requires user involvement.	User training, motivation and sophistication.	✓			
Trust Marks	Trust marks or seals are installed on government web sites.	Requires web site to meet trust mark / seal requirements (can be costly). Must implement as dynamic trust mark to be effective. Requires training of users to not ignore broken images. May require installation of browser extensions.	User training on not ignoring broken images.	✓			
Domain Name Strengthening	Authenticates URL of legitimate web sites.	Can be used with other approaches e.g. SSL/TLS with Gatekeeper compliant Device certificate to provide. a high level of assurance. Requires training of users to not ignore broken images.	Assurance level of server certificate, user training in certificates and not ignoring broken images.	✓ depending on technologies implemented in conjunction with			
Locked cookies	Complementary technology. Browser cookies used for SSL/TLS authentication are bound to the originating server's public key.	Implemented in conjunction with SSL/TLS (see above). Locked cookies are transparent to the user and do not require any server-side changes.	As for SSL/TLS with Gatekeeper compliant Device certificate.	✓ when used in conjunctions with SSL/TLS and Gatekeeper compliant Device certificate – see above			

Website Authentication Mechanism	Use	Implementation issues, Standards, Suitability for Use	Variables Affecting Strength of Mechanism	Indicative Assurance levels			
				Level 1	Level 2	Level 3	Level 4
White lists of trusted sites and authentication toolbars	Complimentary client side technology.	Requires user installation of any toolbar, and maintenance of white lists, user involvement.	Accuracy of white list, user training.		✓		

Schedule 2: Website authentication – technology assessment schedule[4]

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

Solutions	Findings Summary	A. Ease of Use	B. Cost	C. Effectiveness	D. Suitability for Whole-ofGovt	E. Support / Maturity	F. Responsiveness
SSL	SSL is an established technology which remains valuable for encryption, but its ubiquitous use has made it a primary target for spoofing attacks, and its authentication vulnerabilities are now well known.	✓	-	✓	✓✓✓	✓✓✓	✓
Gatekeeper compliant Device certificates	Gatekeeper compliant Device certificates provide significant assurance, especially in high level transactions involving experienced users who can assess the certificate, but still rely on (and suffer the problems of) delivery technologies like SSL.	✓	-	✓✓	✓✓✓	✓✓✓	✓
Keypad Personalisation Techniques	Keypad personalisation can be an effective technique and may be more easily understood by users than other similar technologies. However it is currently only used in limited types of applications.	✓✓	-	✓✓✓	✓✓	✓✓	✓✓

[4] Source: Galexia – AGAF(I) Task 3: Website Authentication

Solutions	Findings Summary	A. Ease of Use	B. Cost	C. Effectiveness	D. Suitability for Whole-ofGovt	E. Support / Maturity	F. Responsiveness
Challenge / Response Mechanisms	Challenge/response approaches to authentication provide an effective architecture for authentication but are vulnerable to well established security threats at the communications layer.	✓✓✓	-	✓✓	✓	✓✓✓	✓✓
Smartcards	Smartcards may provide a useful method for authentication if deployed in an appropriately secure infrastructure.	✓	-	✓✓	✓✓	✓✓	✓✓
Federated Identity Management Systems	Federated technologies are likely to form a significant part of government IT development over the coming decade and provide attractive features for authentication.	✓✓	-	✓✓✓	✓✓✓	✓✓✓	✓✓✓✓
Secure Remote Password Protocol (SRP)	SRP is effective in preventing the disclosure of passwords during transit. However, it only deals with this limited (although important) aspect of authentication and leaves many other issues unaddressed.	✓✓✓	-	✓✓	✓	✓✓	✓✓
Delayed Password Disclosure (DPD)	DPD addresses an important shortcoming in the SRP protocol, but in a user intensive way which is not well suited to large scale authentication applications.	✓✓✓	-	✓✓	✓	✓	✓✓

Solutions	Findings Summary	A. Ease of Use	B. Cost	C. Effectiveness	D. Suitability for Whole-ofGovt	E. Support / Maturity	F. Responsiveness
Browser Chrome Enhancements	Browser chrome enhancement software provides security (although somewhat variably) against the types of social engineering attacks used to circumvent conventional technical solutions. However, to remain effective it cannot be standardised.	✓✓✓	-	✓✓	✓	✓	✓✓
Trusted Password Windows and Dynamic Security Skins	The trusted window effectively addresses security issues around spoofed login window software. However for the approach to provide mutual authentication, the user has the burden of remembering different images for each website.	✓✓✓	-	✓✓	✓✓	✓	✓✓
Shared Secrets	Shared secret techniques form an important basis for many mutual authentication schemes, but require careful design and appropriate complementary technologies to make them effectively secure.	✓✓✓	-	✓✓	✓✓	✓✓✓	✓✓
Trust Marks	Trust marks are traditionally designed to provide assurance to users regarding the site's policies and security. They are capable of providing authentication but rely heavily on user intervention.	✓✓	-	✓	✓✓✓	✓✓✓	✓

Solutions	Findings Summary	A. Ease of Use	B. Cost	C. Effectiveness	D. Suitability for Whole-ofGovt	E. Support / Maturity	F. Responsiveness
Domain Name Strengthening	Domain name strengthening addresses the major weakness of most authentication technologies – social engineering attacks based on simple website imitation. If deployed on a wide scale and combined with certificate based technology (for example, Gatekeeper), it provides a high level of assurance.	✓✓✓	-	✓✓	✓✓	✓	✓✓✓✓

Attachment 1: Current Attacks on Websites

This attachment outlines some of the attacks Internet users are subject to which have caused website authentication to become a prominent issue.

Phishing

Phishing involves an attempt by a fraudulent party to obtain confidential personal data from Internet users through the creation and use of communications (primarily emails) that are deliberately designed to appear as if they have been sent by legitimate and reputable businesses and financial institutions.[5] Users are lured by these communications to a congruently designed ("spoofed") website where they are prompted to provide confidential data such as usernames and passwords. The data obtained as a result of the phishing attack can thus be used by its architects to facilitate the commission of identity theft.

Phishing is becoming an increasingly prominent form of identity theft. The Australian Computer Emergency Response Team (AusCERT) handled 2000 online identity theft incidents (which include phishing and Trojan-based attacks) during the 12-month period between April 2005 and March 2006. This represented an increase of 27 per cent over the preceding year.[6] The Anti-Phishing Working Group (APWG) detected 11,796 phishing websites during May 2006.[7] This represents an increase of over 8,000 compared with the corresponding figure for the same month in 2005.

Why does Phishing work? There is a good explanation in *W3C – Limits to Anti-Phishing*:[8]

1. The unmotivated user is not willing or not able to put in the effort to distinguish trusted services from untrusted services. Trust indicators in browsers are currently subtle, requiring users to parse URI syntax. Many users mistake the presence of HTTPS as a sign that a website is legitimate. Also, the trust indicators in the browser are easily spoofed.
2. The adversarial attacker is capable of creatively countering any static security measure with a response. Phishing attacker can forge links, impersonate domains, spoof browser chrome, and create simulated browsers. Attackers can implement or spoof HTTPS.
3. Further, in a successful phishing attack, the user trusts a phishing site and is willing to pass authenticating credentials to the phishing site. The attacker can replay these credentials to the server. HTTPS may be used by the attacker and / or service provider, but since the user trusts the attacker, HTTPS does not protect against this man-in-the-middle attack.
4. We assume phishing attackers have not compromised the OS or browser. If the attacker has already compromised the OS or browser, phishing attacks, which gain the cooperation of the user, are unnecessary.
5. Service adoption for an anti-phishing technology faces two challenges to adoption, the users and the service providers.

---

5 Black P, *Catching a phish: protecting online identity*, Internet Law Bulletin, Vol 8 No 10, 2006, page 133.

6 Australian Computer Emergency Response Team, 200*6 Australian Computer Crime and Security Survey*, 2006, http://www.auscert.org.au/render.html?cid=3000&it=2001, page 22.

7 Anti-Phishing Working Group, *Phishing Activity Trends Report*, May 2006, http://antiphishing.org/reports/apwg_report_May2006.pdf, page 2.

8 Nelson J and Jeske D, *Limits to Anti-Phishing*, W3C Workshop on Transparency and Usability of Web Authentication, 2006, http://www.w3.org/2005/Security/usability-ws/papers/37-google.

6. By definition, the unmotivated user won't expend effort on anti-phishing. Various anti-phishing proposals require some action by the user, for example setting a site-specific secret or carrying a hardware token. Some solutions ask users to memorize longer passwords or secondary passwords. Users have to learn to use the new devices correctly and must be willing to expend the effort. Users want to roam between computers with no extra effort. Unmotivated users will not adopt complex anti-phishing solutions.
7. Further, service providers are cost-sensitive. Service providers recognize the financial impacts of phishing. The service provider is motivated, but significant barriers exist to the adoption of any new authentication technology. They have collectively invested billions of dollars in stateless HTTP infrastructure. Solutions that suggest new stateful protocols require big investments to upgrade existing stateless infrastructure. Software development is also very expensive. Solutions that employ new popup windows or otherwise modify the existing login processes face tremendous challenges. Any solution which does not seamlessly integrate with the existing HTML FORM tag further requires UI redesign and product implications. The costs to service providers must not be understated.

Attempting to educate users as to how to best detect emails that link to spoofed websites is unlikely to entirely negate the opportunity for phishing to be used as a means of facilitating identity theft. This is because the techniques involved in the commission of phishing attacks are constantly evolving. The latest types of phishing attacks do not make use of spoofed websites. Instead, they cause the end-user to connect to a proxy server that in turn connects to the real site the user actually intends to visit. The real site is thus displayed to the user, but they are typically not able to detect that their communications are being routed through a proxy. The fraudulent party behind the phishing scam can then act as a man-in-the-middle, using the proxy server to monitor and, where desired, modify communications that are made (more information about man-in-the-middle attacks is available in a later section).[9]

The use of a proxy server that is interposed between a client and the real website they intend to visit makes it difficult to educate end-users as to the precise indicia they should use to govern their judgment as to whether they are being subjected to a phishing attack, particularly where those indicia focus upon the content of a website itself as the means of detecting an attack.

Pharming

Pharming involves a fraudulent party interfering with the domain name resolution process – this is used to map a URL requested by an Internet user to the corresponding IP address.

Pharming can take one of two forms:

- Firstly, a DNS server can be hijacked and its data modified such that when a user enters the URL of a legitimate organisation's website, the server maps the domain name to the IP address of a spoofed website.[10]
- The second form relies on the fact that an end-user's computer will store the IP addresses of certain commonly accessed domains so that the DNS server does not need to be contacted when the IP addresses for these domain names is required. A fraudulent party can in some circumstances compromise the end-user's system so that it points to the IP address of a spoofed website.[11]

---

9 Infidel Incorporated, *Phishing 2.0: Next Generation Attacks Makes Current One Time Password Technologies Obsolete*, 2005.

10 Keizer G, *Possible Domain Poisoning Underway*, TechWeb, 4 March 2005, http://www.techweb.com/wire/security/60405913.

11 de la Cuadra F, *Pharming – a new technique for Internet fraud*, eChannelLine Canada, 7 March 2005, http://www.crime-research.org/news/07.03.2005/1015.

In either case, the result is that the end-user believes they are visiting a legitimate website when they have in fact been forwarded to a fraudulent site.

Pharming is becoming an increasingly common technique for directing Internet users to fraudulent websites for the purposes of procuring confidential data. This is primarily because 'social engineering' techniques such as phishing attacks are more readily capable of detection by end-users, particularly as they become more accustomed to these types of attacks occurring.[12]

Man in the middle and Replay Attacks

Man-in-the-middle and replay attacks take place in circumstances where two parties (X and Y) on the Internet attempt to communicate with each other, and a third party interposes themselves between X and Y such that they are (without the knowledge of either party) able to read and modify communications made between X and Y.[13]

In a replay attack, the fraudulent party uses data they have obtained by eavesdropping on the communications between X and Y (for example, authentication credentials) to assume the identity of either of X or Y, at a later date.

Man-in-the-middle and replay attacks both highlight the necessity for the encryption of confidential data prior to transmission over the Internet. The use of SSL does not necessarily prevent these attacks – often the client is not required to authenticate itself to the server, meaning that the server can be deceived as to the identity of the party with whom it is communicating.

Man in the Browser Attacks

A new threat is emerging that attacks browsers by means of Trojan horses. The new breed of new Trojan horses can modify the transactions on-the-fly, as they are formed in browsers, and still display the user's intended transaction to them. Structurally they are a man-in-the-middle attack between the user and the security mechanisms of the browser. Distinct from Phishing attacks which rely upon similar but fraudulent websites, these new attacks cannot be detected by the user at all, as they are using real services, the user is correctly logged-in as normal, and there is no difference to be seen.

The WYSIWYG concept of the browser is successfully broken. No advanced authentication method (PIN, TAN, iTAN, Client certificates, Secure-ID, SmartCards, Class3 Readers, OTP) can defend against these attacks, because the attacks are working on the transaction level, not on the authentication level. PKI and other security measures are simply bypassed, and are therefore rendered obsolete.[14]

---

12 Roberts P, *DNS pharming attacks target .com domain*, ARNnet, April 2005, http://www.arnnet.com.au/index.php/id;1857419881;fp;2;fpid;1.

13 Wikipedia, *Man-in-the-middle attack*, 2006, http://en.wikipedia.org/wiki/Man_in_the_middle.

14 Concepts against Man-in-the-Browser Attacks *Philipp Gühring* *pg@futureware.at* Date: 2006–06–16 Update: 2006–09–12

Spyware

Spyware refers to software covertly installed on an end-user's machine that then proceeds to monitor and collect information about the user's activities.[15] More malignant versions may perform tasks such as redirecting users and stealing and distributing confidential information belonging to the user.[16]

Despite the availability of software utilities to detect and remove many types of spyware, it has become an extremely troublesome issue for Internet users. A 2004 survey of US Internet users revealed that 80 per cent of respondents' computers were infected with spyware, with close to 90 per cent of those respondents being unaware of the spyware's presence. Another study found that 85 million spyware programs were installed on the computers of a sample of Internet users, a clear indication of the magnitude of the problem.[17]

[15] Webopedia, *What is Spyware?*, 2005, http://webopedia.com/TERM/s/spyware.html.

[16] BBC News, *US moves to rein in spyware*, June 2004, http://news.bbc.co.uk/1/hi/technology/3818057.stm.

[17] Commonwealth of Australia, *Senate – Official Hansard,* 12 May 2005, http://www.aph.gov.au/hansard/senate/dailys/ds120505.pdf, page 5.

Attachment 2: Bibliography[18]

Domain Names

Gabrilovich E and Gontmakher A, *The Homograph Attack*, February 2002, http://www.cs.technion.ac.il/~gabr/papers/homograph_full.pdf.

GeoTrust, Identity Verification: Verified Domain™, 2005.

Government Standards and Guidelines for web sites

AGIMO, *The Guide to Minimum Website Standards*, April 2003, http://www.agimo.gov.au/archive/mws.

Office of the Federal Privacy Commissioner, *Guidelines for Federal and ACT Government Websites*, March 2003, http://www.privacy.gov.au/internet/web/index.html.

Public Key Infrastructure (PKI)

Gatekeeper – the full set of Gatekeeper documentation – http://www.finance.gov.au/e-government/security-and-authentication/gatekeeper/documents.html

Hall, K, *Vulnerability of First-Generation Digital Certificates and Potential for Phishing Attacks and Consumer Fraud*, April 2005, http://www.geotrust.com/resources/white_papers/pdfs/SSLVulnerabilityWPcds.pdf.

Marchesini, J and Smith, S, *Virtual Hierarchies – An Architecture for Building and Maintaining Efficient and Resilient Trust Chains*, May 2002, http://www.cs.dartmouth.edu/~sws/pubs/ms02.pdf.

Microsoft, *How CA Certificates Work*, 2003, http://technet2.microsoft.com/WindowsServer/en/Library/0e4472ff-fe9b-4fa7-b5b1-9bb6c5a7f76e1033.mspx?mfr=true.

Tumbleweed Communications, *Digital Certificate Validation in Public Key Infrastructures (PKI), and the Online Certificate Validation Protocol (OCSP)*, 2003, http://tumbleweed.com/pdfs/tmwd_certvalidation_in_pki_wp.pdf.

Secure Socket Layer (SSL)

Adelsbach, A, Gajek, S and Schwenk, J, *Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures*, Horst Gortz Institute for IT Security, 2005, https://www.a-i3.org/content/category/7/51/130/.

IBM, An overview of the SSL handshake, 2005.

IBM, How SSL provides authentication, 2005.

[18] Full references have been provided where possible. Where a reference does not contain a link to the material, this is because it is no longer available or cannot be accessed online.

Miller, R, *SSL's Credibility as Phishing Defense Is Tested*, March 2004, http://news.netcraft.com/archives/2004/03/08/ssls_credibility_as_phishing_defense_is_tested.html.

Transport Security Layer Working Group, *The SSL Protocol Version 3.0*, 1996, http://wp.netscape.com/eng/ssl3/draft302.txt.

Ye, EZ, Yuan, Y and Smith, S, *Web Spoofing Revisited: SSL and Beyond*, Dartmouth College Department of Computer Science, February 2002, http://www.cs.dartmouth.edu/~pkilab/papers/tr417.pdf.

Trustmarks

Archer, P, *The QUATRO approach to Transparency and Usability of Web Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/04-quatro-trust/.

Consumer and Business Affairs Victoria, Department of Justice, *Web Seals Of Approval*, January 2002, http://www.consumer.vic.gov.au/CA256902000FE154/Lookup/CAV_Publications_Computers_Internet_Discussion_Papers/$file/WebSealsFinalReport.pdf.

GeoTrust, True Site™: Identity Assurance for Web Sites, 2004.

PCWorld, *VeriSign Redesigns Trust Mark Seal,* November 2003, http://www.pcworld.com/news/article/0,aid,113264,00.asp.

Quatro, *How to make your trustmark machine-readable using the Quatro system*, May 2006, http://www.quatro-project.org/files/file/howto.htm.

Rosenberg J, *True Site™: Helping on-line companies create trusted brands so their site visitors feel confident enough to stay and pay*, GeoTrust, November 2001 http://www.northost.net/SecurityAndIdentity/TrueSiteWP.pdf.

The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, *Web Seals: A Review of Online Privacy Programs*, September 2000, http://www.privacy.gov.au/publications/seals.html.

Ullrich, J, Coded Trust Seal.

VeriSign *VeriSign Unveils Newly Designed Security Trust Mark To Aid Consumers In Identifying Safe Web Sites To Shop This Holiday Season,* 2003.

VeriSign, *The VeriSign Secured™ Seal Research Review,* 2006, http://www.VeriSign.com/static/013506.pdf.

Web Authentication Commentary

Alves-Foss, J, *Provably Insecure Mutual Authentication Protocols: The Two-Party Symmetric-Encryption Case*, Centre for Secure and Dependable Software, University of Idaho, October 1999.

Bakker, B, *Mutual Authentication with Smart Cards*, USENIX, 1999, http://www.usenix.org/events/smartcard99/full_papers/bakker/bakker.pdf.

Dreymann, DT, *Cert*,*ifiedEmail*™ – *a New Trustworthy Messaging Class,* W3C Workshop on Transparency and Usability of Web Authentication, 2006, http://www.w3.org/2005/Security/usability-ws/papers/38-goodmail.

Evers, J, Phishers come calling on VoIP, CNET, July 2006, http://news.cnet.com/2100-7349_3-6092366.html.

Fette, I, Sadeh, N and Cranor, L, *Web Security Requirements: A Phishing Perspective*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/13-cmu-requirements.

Financial Services Technology Consortium, *Financial Industry Recommendations and Requirements for Better Mutual Authentication*, June 12 2006.

Fraser, N, *The Usability of Picture Passwords,*Tricerion, 2006, http://www.tricerion.com/files/285_Usability_of_picture_passwords.pdf.

Gajek, S and Schewnk, J, *Reversed Responsibilities: Browser Authentication instead of Server Authentication,* W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/09-dortmund-reverse/.

Hardmeier, S, *The Phishing Filter: Fighting the Modern Day Con Artist*, Microsoft, 10 November, 2005, http://www.microsoft.com/windows/ie/community/columns/phishing.mspx.

Hirsch, F and Le Van Gong, HA, *Approaches to Simplify Server Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/07-nokia-and-sun/.

IBM developerWorks, *The cranky user: What you can do about phishing,* January 2006, http://www-128.ibm.com/developerworks/web/library/wa-cranky60.html.

IEEE Security and Privacy, *The TIPPI Point: Towards Trustworthy Interfaces*, July 2005, http://www.cs.dartmouth.edu/~sws/pubs/ss05a.pdf.

Infidel Incorporated, *Phishing 2.0: Next Generation Attacks Makes Current One Time Password Technologies Obsolete*, 2005.

Jakobsson, GM and Myers, S, *Stealth Attacks and Delayed Password Disclosure*, AI3, 2006, https://www.a-i3.org/content/view/69/104/.

Jones, MB, *The Identity Metasystem: A User-Centric, Inclusive Web Authentication Solution,* W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/28-jones-id-metasystem/.

Keizer, G, *5 Tools To Bulletproof Firefox*, InformationWeek, 14 July, 2006, http://www.informationweek.com/shared/printableArticle.jhtml?articleID=190400479.

Linn, J, Kaliski, B, Nyström, M and Yung, M, *Applying Context to Web Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/03-rsa-context/.

Mysore, SH, *Web Authentication Today and For Tomorrow,* W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/25-mysore-webauth-today-tomorrow/.

National Consumers League, *A Call for Action: Report from the National Consumers League Anti-Phishing Retreat*, March 2006, <http://www.antiphishing.org/reports/200603_NCL_Phishing_Report.pdf>.

Nelson, J and Jeske, D, *Limits to Anti-Phishing*, W3C Workshop on Transparency and Usability of Web Authentication, 2006, http://www.w3.org/2005/Security/usability-ws/papers/37-google.

Nielsen, J, *User Education Is Not the Answer to Security Problems,* October 2004, http://www.useit.com/alertbox/20041025.html.

Rivest, LR, *Separable Identity-Based Ring Signatures: Theoretical Foundations For Fighting Phishing Attacks*, February 2005, http://theory.lcs.mit.edu/~rivest/AdidaHohenbergerRivest-SeparableIdentityBasedRingSignatures.pdf.

Rotondi, D, *A Server Authentication Procedure Proposal,* W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/06-rotondi-authentication/.

Rubinoff, S and Steinberg, J, *Key Human Factors Issues Surrounding Consumer Two Factor Authentication and Mutual Authentication*, Green Armor Solutions, 11 July 2006.

Saikos, G, *Improving Internet Trust and Security,* W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/33-staikos-improving-trust/>.

VeriSign, *VeriSign Enhances Online Transaction Security With Mutual Authentication Solutions Leveraging Microsoft Internet Explorer 7 and "InfoCard"*, February 2006, https://press.verisign.com/easyir/customrel.do?easyirid=AFC0FF0DB5C560D3&version=live&prid=216742&releasejsp=custom_97.

Wade. C, *Financial Industry Requirements for Better Mutual Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/15-wade-financial.

Wright. KL, *W3C Workshop on Transparency and Usability of Web Authentication*, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/21-wright-position.

Zurko. ME and Wilson. D, *Using History, Collaboration, and Transparency to Provide Security,* W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/19-zurko-history/.

Zurko, ME, *User-Centered Security: Stepping Up to the Grand Challenge*, IBM Software Group, 2005, http://www.acsac.org/2005/papers/Zurko.pdf.

Other Authentication Technologies

Bellare, M, *Attacks on SHA-1*, OATH, March 2005, http://www.openauthentication.org/pdfs/Attacks on SHA-1.pdf.

Chou, N, Ledesma, R, Teraguchi, Y, Boneh, D and Mitchell, JC, *Client-side defense against web-based identity theft,* Stanford University Computer Science Department, February 2004, http://crypto.stanford.edu/SpoofGuard/webspoof.pdf.

Close, T, *Petname Tool: Enabling web site recognition using the existing SSL infrastructure*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, http://www.w3.org/2005/Security/usability-ws/papers/02-hp-petname/.

Cloudmark, *Cloudmark Anti-Phishing Services*, 2006, <http://www.cloudmark.com/releases/docs/ds_anti-phishing_10470406.pdf>.

Cloudmark, *Cloudmark Automated Feedback System Helps Service Providers & Customers Combat Messaging Threats*, May 2006, http://www.cloudmark.com/press/releases/?release=2006-05-30-01.

Dhamija, R and Tygar, JD, *The Battle Against Phishing: Dynamic Security Skins*, Symposium On Usable Privacy and Security, July 2005, http://cups.cs.cmu.edu/soups/2005/2005proceedings/p77-dhamija.pdf.

Digital Resolve, *Trusted Server™ Technology*, 2006, http://www.digital-resolve.net/solutions/trusted_server.html.

Entrust, *Securing What's at Risk: A Common Sense Approach to Strong Authentication*, 8 November 2005, <http://www.entrust.com/resources/download.cfm/22313/>.

Green Armor Solutions, *Identity Cues Two Factor™ & Two Way Authentication*, 2005, http://www.greenarmor.com/DataSheets/Identity%20Cues%20Two%20Factor%20Data%20Sheet.pdf.

Herzberg, A, *TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks*, September 2004, http://eprint.iacr.org/2004/155.pdf.

Howarth, F, *Deploying psychology in the fight against phishing*, Bloor Research, 15 July 2005, http://www.greenarmor.com//DataSheets/Identity%20Cues%20Two%20Factor%20Data%20Sheet.pdf.

Iconix, *How eMail ID Works*, 2005, http://www.iconix.com/learnmore.php.

MacFarland, A, *Iconix Truemark Authentication Service Add More Trust into E-Business*, The Clipper Group (Navigator), December 2005, http://www.clipper.com/research/TCG2005078.pdf.

Merritt, R, *Crack in SHA-1 code 'stuns' security gurus*, EETimes, February 2005, http://eetimes.com/news/latest/showArticle.jhtml?articleID=60402150.

Neuman, BC and Theodore, T, *Kerberos: An Authentication Service for Computer Networks*, Institute of Electrical and Electronics Engineers, September 1994, http://gost.isi.edu/publications/kerberos-neuman-tso.html

Open Authentication Initiative, *Mutual OATH: HOTP Extensions for mutual authentication*, December 2005, http://openauthentication.org/pdfs/draft-mraihi-mutual-oath-hotp-variants-00.pdf.

Open Authentication Initiative, *OATH Reference Architecture Release 1.0*, 2005.

Open Authentication Initiative, *OATH Roadmap*, November 2005, http://openauthentication.org/pdfs/OATH Public Roadmap 2006.pdf.

PhishCops, How Does PhishCops™ Work?, 2005.

Phoenix Technologies, *Phoenix SPEKE – Strong Authentication for Devices, Networks, and Data*, 2006, http://www.phoenix.com/NR/rdonlyres/04BD87B1-F01A-449E-AE1E-743A7399A3C0/0/SPEKE_ds.pdf

RSA Security, *Protecting Against Phishing by Implementing Strong Two-Factor Authentication*, 2004.

Sestus Data Corporation, *PhishCops™ White Paper*, 2006.

Tricerion, Account Hijacking Prevention with the Tricerion Strong Mutual Authentication (SMA) Server, 2005, http://www.tricerion.com/downloads/984_Tricerion_SMA_-_Account_Hijacking_Protection.pdf.

Tricerion, *Tricerion SMA Product Description*, 2006, https://secure.tricerion.com/downloads/978_Tricerion_SMA_Product_Description.pdf.

Wi-Fi Planet, *Technology for a Secure Mobile Wireless LAN Environment: Evolution, Requirements, Options*, 30 January 2002, http://www.wi-fiplanet.com/tutorials/article.php/965471.

WiKID, *WikID Mutual Authentication*, 2006, http://www.wikid.com/technology/mutual_authentication/.

WiKID, *WiKID releases HTTPS Mutual Authentication*, October 2005, http://www.wikidsystems.com/WiKIDBlog/categories/Mutual Authentication.

Willoughby, M, *OATH Swears Authentication is the Next Big Thing*, Digital ID World, January 2005, http://magazine.digitalidworld.com/Jan05/Page34.pdf