GOLD STANDARD e-AUTHENTICATION REQUIREMENTS -
AN ELEMENT OF THE NATIONAL IDENTITY SECURITY STRATEGY

COAG has endorsed the Gold Standard e-Authentication Requirements (GSAR) Document as a national best practice guide. Implementation is a matter for each jurisdiction.

1. Introduction and Overview

Accurate authentication is necessary to ensure the person that an agency deals with is indeed the same person who originally registered for the service. Authentication may be conducted in a variety of ways and the degree of verification required will usually depend on the value of the service. A variety of authentication means may be used including face to face authentication and e-authentication.

This Report largely deals with Gold Standard e-Authentication Standards. For face to face authentication, credentials issued under the Gold Standard Enrolment Framework (Report 1) will provide a photographic or biometric link between the individual presenting and the credential itself. For example, a photographic image might appear on the face of the credential itself and perhaps in a microchip attached to the credential. This linkage provides a high degree of assurance regarding the individual and contributes to the authentication process. Additionally, the authenticity of the credential itself can be verified with the issuing agency. Combined, these two measures contribute to a strong and efficient authentication procedure. Further information on dealing with face to face authentication is provided at Section 9.

Government agencies are increasingly seeking to transact with individuals using electronic means such as the internet. To transact electronically, individuals may be required to use a 'gold standard' or high integrity proof of identity document, token or credential ('credential') to establish that they are who they say they are.

Where there are potentially substantial consequences if the wrong person completes a transaction with government, the use of a gold standard credential may need to be supported by strong mechanisms to electronically authenticate the identity of an individual. Without strength in both these aspects, there will be a weakness in the process that will undermine the identity security process as a whole.

The Gold Standard e-Authentication Requirements (GSAR) describe a gold standard approach to electronic authentication. This approach should be applied by government agencies where:

- the identity of an individual engaging in a transaction needs to be authenticated, and the authentication process is either wholly electronic or supported electronically;
- an electronic credential issued as an output from the Gold Standard Enrolment Framework (GSEF) is employed in that authentication process; and
- the risks associated with the transaction require Level 4 (high) assurance under the Australian Government e-Authentication Framework (AGAF).

2. Background

The GSAR is one of a number of documents being prepared by the Australian Government in partnership with State and Territory Governments as part of the National Identity Security Strategy (the Strategy). The key elements of the Strategy are to:

- Develop a standard framework for Proof of Identity (POI) and Enrolment Processes;
- Increase security standards on POI documents;
- Establish a Document Verification Service (DVS);
- Improve the integrity of Identity Data; and
- Develop authentication standards.

As an element of the Strategy, a GSEF has been developed. The GSEF provides a supporting basis for the development of premium enrolment processes by agencies issuing high integrity government documents, tokens or credentials, that also function as key documents for proof of identity (POI) purposes. Tokens, documents or credentials that are established with an electronic binding to an identity[1] during the gold standard process of enrolment are subject to these requirements. These electronic tokens, documents or credentials, which are an output of the GSEF, will be referred to throughout the GSAR as "GSEF credentials". It is important to understand that the GSAR only applies to the use of GSEF credentials in e-authentication.

These gold standard e-authentication requirements will complement the high quality of a GSEF credential. Used together, they will achieve a high level of assurance in the authentication process in the electronic environment.

The GSAR will draw upon a standardised application of policies, including those contained in the Australian Government e-Authentication Framework (AGAF), the Australian Government Smartcard Framework, and the Gatekeeper Framework. This allows the GSAR to provide a simpler narrative of the requirements and to 'future proof' it as the other frameworks and guidelines evolve.

Terminology

The GSAR uses a number of technical terms that may not be familiar to some readers. Some of the key terms are explained in footnotes. Readers needing further assistance with terms could refer to a glossary prepared by the Australian Government Information Management Office (AGIMO) for the Australian Government e-Authentication Framework (AGAF) to be found online at:
http://www.agimo.gov.au/infrastructure/authentication/agaf_b/glossary/v

[1] These could include smartcards, documents containing an electronic chip (such as an e-passport), electronic tokens (such as a USB stick), or digital certificates. They are capable of storing digital information.

3. Scope

The GSAR will describe a gold standard for electronic identity authentication[2] in transactions which require the e-authentication of identity through the use of a GSEF credential. The GSAR covers claims of an individual's identity. It does not cover other claims such as financial value, an individual's qualifications, or the delegated authority to conduct transactions. Therefore, the gold standard for e-authentication using a GSEF credentials outlined in the GSAR only applies in particular circumstances. These are where the consequences of a false claim of identity in a transaction are such that they require an e-authentication mechanism that achieves an assurance of identity specified in the AGAF as being assurance level 4. The four levels AGAF has identified are outlined below.

Figure 3.1 – The four AGAF assurance levels

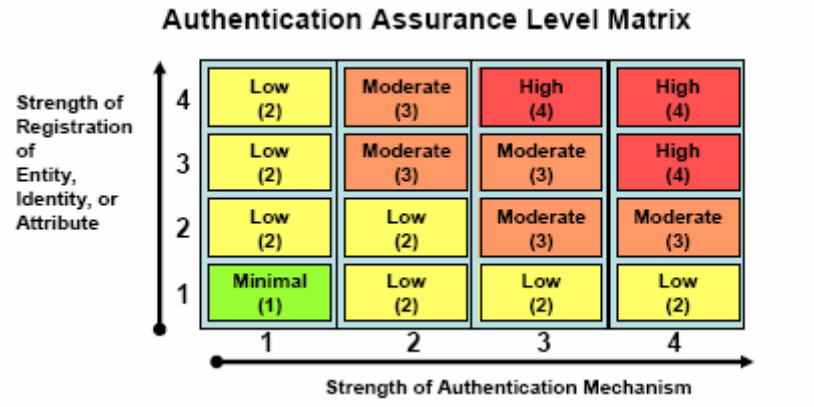
Level 1	Level 2	Level 3	Level 4
Minimal assurance	Low assurance	Moderate assurance	High assurance
Minimal risk posed by transaction; therefore, little requirement for confidence in the assertion	Low risk posed by the transaction; therefore, some confidence in the assertion is required	Moderate risk posed by the transaction; therefore, moderate confidence in the assertion is required	High risk posed by the transaction; therefore, high confidence in the assertion is required

It should be noted that in this figure the term 'risk' refers to the risk rating derived by considering both the likelihood and the consequences of that event according to the Risk Management Standard AS/ANZ 4360.

To achieve level 4 assurance generally under the AGAF, an agency needs a combination of a credential that has been established by a strong enrolment process and a strong e-authentication process. Figure 3.2 below shows this relationship.

[2] Identity e-authentication is the process of testing a statement or claim that a particular entity is appropriately using an identity, in order to establish a level of confidence in the statement or claim's reliability (AGAF Discussion Paper, December 2005, Glossary, p 46.)

Figure 3.2 – Registration with authentication relationship



Sourced from the AGAF (2005).

The GSAR is not intended to cover transactions that involve issuing a further GSEF credential. The circumstances covered by the GSAR, therefore, would not include such events as use of an old passport to authenticate identity in the process of issuing a new passport. However, they would include a process where, for example, an e-passport is used to authenticate identity in an electronic transaction.

The GSAR is primarily intended to deal with electronic interactions. It should not, however, be seen as representing a position that e-authentication is superior (or inferior) to face-to-face authentication, or that e-authentication is always appropriate or preferable.

Nothing in the GSAR is intended to replace or supersede the requirements of the *Australian Government's Protective Security Manual* or the *Australian Government Information and Communications Technology Security Manual*.

3.1 When should level 4 assurance apply?

The AGAF indicates that level 4 assurance is required where substantial damage might arise from a claim being accepted as true when it is actually false. The AGAF lists such damage as including:

- Risk to any party's personal safety
- The release of personally or commercially sensitive data to third parties
- Substantial financial loss to any party
- Substantial damage to any party's standing or reputation
- Substantial distress being caused to any party
- Significant threat to government agencies' system or agencies' capacity to conduct their business
- Assisting a crime or hindering its detection

- Substantial inconvenience to any party.

Examples of transactions requiring level 4 e-authentication assurance could be where the GSEF credential is being used to:

- access personal health information, such as a health record, via a website portal;
- access financial information
- make a claim for a substantial benefit or entitlement in an electronic environment
- transmit funds electronically either to an individual from an agency or from an individual to an agency.

Determining what is 'substantial' in these circumstances will depend on the specific business environment of the agency. That determination should be informed by an assessment of the risks associated with an agency's transactions. The onus remains with agencies to maintain a risk-based approach to e-authentication as described in the AGAF. The GSAR only applies if a risk assessment identifies a high risk transaction and a GSEF credential is to be used in the transaction.

Therefore, there are clear circumstances that the GSAR does not cover, which include:

- e-authentication using a GSEF credential where the assurance level required is lower than AGAF assurance level 4, that is the risk associated with the transaction is assessed as moderate or lower; or
- authentication in circumstances that do not involve the use of a GSEF credential in an electronic transaction.

In addition, the GSAR does not address the nature of the information, privilege, benefit or entitlement an individual might obtain once e-authentication is complete, or the consequences of where the result of the e-authentication process is that the identity of the person presenting the credential is not authenticated.

3.2 What channels does the standard apply to?

The requirements outlined in the GSAR cover any electronic channel that could, either now or in the future as technologies develop, support the use of a GSEF credential by an agency in an e-authentication.

3.3 Privacy

The GSAR recognises the intrinsic role that privacy considerations, including consumer choice, play in achieving a high level of assurance. This is so even where high risk electronic transactions are involved. Designing a system that enables consumers to choose the e-authentication mechanism should facilitate a high level of take up of these options and avoid the risk of accumulating personal information in ways that create security risks, or threat of fraud. The privacy aspects of this gold standard are discussed further in section 10 of the GSAR.

4. What does e-authentication of identity rely on?

Broadly speaking e-authentication relies on one or more of the following factors:

- Something the individual knows, such as a password or other information that is also known to the agency (a shared secret);
- Something that an individual has, such as a proof of identity document, card or token;
- Something that an individual is, such as a fingerprint or a facial image.

Some of these factors are more effective than others in securing a particular element of an e-authentication process. For the purpose of the GSAR at least two factors must be used in the e-authentication process. The GSEF credential itself can be considered to be the something an individual has factor.

5. How is a high level of trust achieved in an electronic environment?

5.1 The chain of trust

Once an individual is issued with a GSEF credential there are a number of points in the e-authentication process that need to be secured or managed to reach a high level of assurance (a gold standard) that the person using the GSEF credential is who they claim they are. These points form a chain of trust.

The e-authentication mechanism for an assurance level 4 transaction must be capable of meeting electronic security threats as they currently apply and as they evolve in the future. Current threats include:

- Eavesdropping
- Replay attacks
- Online guessing
- Active network attacks
- Malicious host software
- Man-in-the-Middle attacks

In order to meet these threats, the agency authenticating an identity needs to be assured to a high level, consistent with the technology available, that each of the chain of trust links (bindings) has been addressed. These links are:

1. The GSEF credential has been issued by the agency authorised to issue it, i.e. not fake (binding the item to the issuer);

2. The GSEF credential is current and has not been revoked e.g. because it is lost or compromised, there has been a change of name, or because the GSEF credential was an interim credential;
3. The GSEF credential being used for the electronic transaction belongs to the entity[3] using it (binding the item to the person using it) – this is because a validly issued credential might be in the hands of someone other than the person to whom it was issued;
4. The GSEF credential relates to the identity of the person using it. This link sometimes needs to be considered separately because an entity can have more than one identity, but no identity should relate to more than one entity. Depending on the circumstances an agency may need to check a claim at entity level or at the identity level or both. For example, if a biometric is used to test an entity, it may not be necessary to test the identity;
5. The GSEF credential is not tampered with before it is used in the electronic environment, either to make it look like it belongs to someone other than the person to whom it was issued, or to alter some aspects of identifying information about that person – in a smartcard situation by changing the chip in card, or changing the data on the chip;
6. Any information on the GSEF credential being transmitted electronically is not being tampered with either to make it look like it belongs to someone other than the person to whom it was issued, to alter some aspects of identifying information about that person, or to otherwise enable "man in the middle" attacks;
7. The information on the GSEF credential cannot be viewed by anyone other than the relying party while it is being transmitted;
8. Mutual authentication is established, where possible and dependent on technology. The individual who is seeking to conduct an electronic transaction using a GSEF credential needs to be assured that the agency with which they are transacting electronically is who they claim they are. Without this assurance, the individual could be giving a whole range of identity information to an organisation that is not entitled to receive it and may have intentions to use the information for fraudulent purposes. This could compromise the whole security of the e-authentication process.
9. Where there is an operational requirement, non-repudiation of the claim is supported, i.e. it is very difficult for parties to claim "that was not me".

Electronic identity authentication at assurance level 4 using a GSEF credential should have mechanisms to the extent that effective technology is available to ensure acceptable levels of security at all these links in the process. Strong authentication must be coupled with the corresponding appropriate level of encryption for the information in storage and whilst travelling across untrusted networks (e.g. the Internet). ACSI 33 provides further advice on this issue.

In the case of mutual authentication in the online environment, use of impersonation strategies by those with malicious intent is a rapidly emerging threat of which 'phishing' and man-in-the-middle attacks are early signs. Agencies will have to give consideration

[3] For the purposes of authentication an entity can be described as a natural person, a legal person or an artefact such as a hardware device. An identity is a presentation, or a representation, of an entity (AGAF 2005).

to implementing technologies, as they become available, that adequately address these threats.

6. Approaches to e-authentication using a GSEF credential at level 4 assurance

6.1 Introduction

In the electronic environment, ensuring the strength of all links in the chain of trust and achieving level 4 assurance is highly dependant on a robust approach to e-authentication. There are a number of possible approaches, though agencies should select approaches that are appropriate to the channel or channels they propose to use and which accord with their particular business requirements.

Credentials should be 'bound' to the issuer and user through approved methods of authentication[4]. Bindings establish who issued a credential and provide assurance with regard to the authority of an individual to use the credential. Agencies will need to ensure that the mechanisms address all the links in the chain of trust to a sufficient level of security.

As Figure 3.2 indicates, obtaining a level 4 assurance requires combining a GSEF level 4 registration assurance process with a level 3 or 4 authentication mechanism:

This means that authentication mechanisms that satisfy level 3 or 4 assurance requirements, as defined in the AGAF, fall within the scope of the GSAR. It will be up to agencies to determine the required strength of the authentication assurance process.

The following section provides a step-by-step process for identifying possible approaches an agency can take to reach a gold standard. Implementation details, such as hardware and software specifications, lifecycle management, security methods, threat responses and exception handling are not discussed. The adequacy of approaches will evolve over time with the advent of new and improved technologies, frameworks and standards. Agencies are responsible for ensuring that the approach to implementation recognises the importance of securing the transaction.

The section below is intended to assist agencies to understand the complex relationships between the nature of the GSEF credential, channels, mechanisms, factors and mitigation strategies, while defining minimum standards and promoting flexibility. It is thought that the options below will alter over time, as e-authentication is a dynamic field in which solutions come and go according to the emergence of new technologies, solutions and threats.

6.2 Designing an e-authentication scheme

A fundamental requirement of the GSAR is that it make use of the GSEF credential and the information it contains. This use constitutes the first step therefore in any gold standard e-authentication process. How a GSEF credential is capable of being used depends on the channels and mechanisms that an agency decides to employ, and the

[4] In this context the GSEF will define the appropriate way in which credentials are bound to an individual.

information contained on the credential. The following points describe the steps required to achieve gold standard e-authentication.

6.2.1 Step 1 – GSEF credential.

An e-authentication process commences when a GSEF credential is read electronically in order to extract an identifier stored upon it. This identifier can be 'freely' available, perhaps as a simple numeric value, but more commonly it is in the form of a digital certificate. The 'freely' available identifier is subject to many of the risks that apply to non-digital identifiers, while the digital certificate is protected from such risks

6.2.2 Step 1 – Select factors and associated mechanisms

To reach a gold standard e-authentication a minimum of two factors must be used. Factors can be described as something you have, something you know, or something you are.

Having determined the factors, the authentication mechanism(s) must be selected. It is the mechanism that 'binds' or associates an individual with a credential. Mechanisms can be defined as follows:

<u>Something You Have.</u>

- A protected cryptographic key contained on a hardware device, such as a smartcard or USB token.
- One-time password generator: A token that generates a password that can be used for one transaction. For the GSAR this device must be secured with a PIN.
- A protected cryptographic key contained in software.

<u>Something You Know.</u>

- PIN or password: Mutually known ongoing PINs or passwords.
- Secret questions: A set of questions and answers known only to the individual and agency concerned.
- Recent transaction information: Information such as the amount of a previous utility bill.

<u>Something You Are</u>

- A biometric representation. A representation of a physical or physiological attribute of an individual such as a facial image biometric, voice or fingerprint.

6.2.3 Step 2 – Delivery of mechanisms

Once mechanisms are chosen, thought should be given to the delivery or collection of the mechanism. It is recommended that a GSEF credential should not be delivered by the same system as its activation or binding mechanism. For example, if a GSEF

credential is provided through the mail system the related PIN should be provided through another delivery system; perhaps by SMS. Risk analysis should be undertaken by agencies when deciding collection and delivery options.

Delivery systems may include:

- Post
- Phone Authority
- SMS
- Online

Different delivery systems have differing levels of risk, and agencies are advised to seek advice as to suitability according to their business needs.

Ideally the mechanisms would be provided and/or recorded at the same time as the GSEF credential is provided. Of course, some mechanisms, such as recent transaction information, are iteratively developed. Using 'late binding', where the mechanism is provided after identity has been authenticated, requires that agencies assure themselves that the individual to whom the mechanism is associated is the individual to whom the credential was issued.

6.2.4 Step 3 – Consolidating the elements

The final step in designing the scheme is to consolidate the individual elements of the intended approach and ensure that they collectively provide a sufficient level of assurance as to the validity of the claimed identity. This section provides examples of potential approaches that may be suitable. However, responsibility for determining the level of assurance that is required, and the mechanisms necessary to meet that level, rests with individual agencies.

The authentication process for online transactions must combine a something you have factor with either a something you know factor or something you are factor. The GSEF credential can be considered to be the something you have factor.

As examples, the following scenarios would achieve a gold standard in e-authentication:

- A customer presents a GSEF credential that contains a cryptographic key into a reader or a USB port on a home computer and the card is activated through a biometric analysis, e.g. a fingerprint scan.

- A customer presents a GSEF credential that contains a cryptographic key into a reader on a home computer and the card is activated through the application of a PIN.

- A customer presents a GSEF credential in the form of a one-time password generator. They enter a PIN to generate a password and use that password to log in.

- To access a service a customer enters a PIN to activate a 'soft' certificate (the GSEF credential) that is stored on their PC.

6.2.5 Specific Guidance for a Public Key Infrastructure (PKI) approach

If the GSEF credential is utilising a private key associated with a digital certificate (e.g. in the case of a smartcard, USB token or "smart" SIM card) then the GSEF credential including the private key may be regarded as one factor and a password or biometric required to activate the key as the second factor. In such an approach the following applies:

- For Australian Government agencies, the digital certificate must be issued by a Gatekeeper accredited Certification Authority (CA) in accordance with Gatekeeper policy (including in particular CA compliance with the *Privacy Act 1988*);
- The certificate must operate with a fully functional Key Pair (or Key Pairs) to provide both authentication and confidentiality;
- The private key must be obfuscated/encrypted within the GSEF credential and able to be activated only by means of either a "strong"[5] password known only to the cardholder or a biometric;
- The GSEF credential itself, if it is a hard token, must be listed on the Defence Signals Directorate Evaluated Product List at an appropriate assurance level - see (http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html);
- The private key should be generated by the credential holder on the GSEF credential;
- The authenticating agency should ensure both mutual authentication and the provision of a secure communications channel for the transaction; and
- The private signing key must not be backed up or escrowed.

Further information on PKI and Gatekeeper can be found at http://www.agimo.gov.au/infrastructure/gatekeeper

7. Key principles to maintain the security and effectiveness of level 3 and 4 assurance mechanisms

An approach that provides level 4 assurance must be designed to address high levels of risk. The identification of risk and the associated requirement for level 4 assurance in a transaction remains the responsibility of an agency. Such approaches may be complex and expensive to implement. It will therefore be critical for agencies to ensure that they take steps to maintain the security and effectiveness of their approaches. The following are key principles for maintaining the security and effectiveness of level 3 and 4 assurance mechanisms.

[5] A strong password can be defined as one that involves an increased level of complexity. A recommended approach for passwords is contained at paragraph 3.6.11. of the September 2006 release of ACSI 33.

Principle 1

Level 3 or 4 assurance e-authentication mechanisms should only be used with a GSEF credential when the circumstances require them to be used.

The effectiveness of level 3 and 4 assurance e-authentication mechanisms will be best maintained when their use is limited to those circumstances where the assessed risks require them to be used. If government agencies use these mechanisms beyond these circumstances and, therefore, cause them to become widespread, they will become increasingly attractive as targets for security attacks.

Agencies should assess the severity of the impact on each party or otherwise of a failure in the e-authentication process and then refer to the AGAF framework to assess which appropriate kinds of assurance mechanisms are required. As a general rule, agencies should choose the lowest level in the AGAF framework consistent with the identified level of risk.

Assessment that a transaction requires level 3 or 4 e-authentication assurance should be conducted in accordance with the AGAF and Australian and New Zealand Standard on Risk Management, AS/NZ:4360.

Principle 2

Level 3 or 4 assurance e-authentication mechanisms should operate in such a way that no detailed history of client transactions are created or used by the agency, except to the extent that this is required for system maintenance or evidentiary purposes.

The security and effectiveness of level 3 or 4 e-authentication assurance processes will also be best maintained if they collect or generate only the minimum personal information necessary for the mechanism to operate. This makes the mechanism less vulnerable to security breaches. This includes that they will be less attractive for malicious security attacks.

Principle 3

To the extent possible level 3 or 4 assurance mechanisms should be designed to accommodate client choice.

The security and effectiveness of level 3 or 4 assurance mechanisms will be best maintained if its users trust and are willing and able to use them. Choice is often a key ingredient in generating trust in a new channel. Users will be less likely to take steps that might compromise the system if they have the greatest level of choice and control possible in relation to the mechanism. Economic considerations will be important in this decision, as are the needs of individuals to feel that they have some choices and are not being unnecessarily constrained. The decision should be based on a strong culture of customer service and convenience.

Notwithstanding this, the GSAR is, by definition, intended to apply to a small number of high risk transactions and therefore this may restrict the choices that an agency is able to offer a user if the user wishes to access the services electronically.

8. AGAF principles to apply in selecting level 3 or 4 e-authentication assurance mechanisms for individuals

AGAF for Individuals identifies nine principles that are to be used to guide the development of e-authentication approaches. The principles are:

- Transparency;
- Risk management;
- Consistency and Interoperability;
- Responsiveness and accountability;
- Trust and security;
- Privacy;
- Choice;
- Diversity;
- Cost-effectiveness and convenience.

The principles are described in the AGAF for Individuals, Overview and Principles, available at:

http://www.agimo.gov.au/infrastructure/authentication/agaf_i/overview_and_principles

All nine principles apply to any approach that is intended to provide level 4 assurance for individuals. Four of these principles are of special relevance and this section provides additional guidance on their application in the context of the GSAR.

8.1 Consistency and interoperability

The AGAF suggests that government agencies should apply a consistent approach to selecting e-authentication mechanisms that address similar risks to facilitate the outcome that individuals can expect similar e-authentication processes for transactions of similar risk.

Having a consistent approach to selecting and implementing e-authentication mechanisms is important to maintaining the security of a level 4 assurance process because it creates a more predictable environment for the user. This enables them to more easily identify abnormalities including attempts at fraud, for example, phishing. It also has the added benefit of improving user experience.

8.2 Agency choice and flexibility

The gold standard e-authentication requirement does not provide an infallible approach to e-authentication using a GSEF credential. It indicates several approaches to e-authentication that an agency might use with a GSEF credential transaction that requires a level 4 assurance. In choosing a particular option an agency will need to consider where in the trust chain risks relating to the particular transaction will arise and which option is most likely to address them.

8.3. Identification of risks and customer safety

In selecting the e-authentication process, the risks to all parties, especially to the agency and the individual using the GSEF credential will be identified, and reasonable steps taken to ensure that all parties are aware of them.

The e-authentication process must anticipate the possibility of failure, and have mechanisms in place for addressing it, both from the point of view of ensuring business continuity, and from the consumer perspective. Where an e-authentication mechanism fails in a transaction requiring level 4 assurance, the consequences for individuals will be significant. It is, therefore, particularly important that an individual presenting the GSEF credential can do so without undue fear of having to bear the burden of dealing with the consequences of error or failure. In particular, due process must ensure the party is treated with respect and treated as if "innocent until proven guilty". Agencies will therefore need to consider the issue of 'false negatives' in defining and scoping the implementation of their e-authentication schemes.

8.4 Providing for exceptional circumstances

Agencies should ensure, unless constrained by operational circumstances, that they include a non-electronic channel for individuals to use to authenticate their identity if they do not have access to electronic channels.

9. Face to Face and Telephonic Authentication

9.1 Scope

The *Gold Standard e-Authentication Requirements* (GSAR) applies only to situations which require the electronic authentication of identity through the use of a *Gold Standard Enrolment Framework* (GSEF) credential. The following procedures apply for face to face authentication of existing customers and clients of an agency using a credential issued or registered by that agency. It does not apply to the use of a GSEF credential in a POI, registration or enrolment process. Where an individual has not been issued a GSEF credential, the full enrolment procedures contained in the GSEF will apply.

Principle 10 of the GSEF provides guidance on the elements surrounding face to face authentication for individuals who have been issued a GSEF credential.

Principle 10: *An enrolling agency should in most cases enrol a person to a Gold Standard only once. Future authentication by that agency should rely on the POI*

credential issued by the agency. A full enrolment process may however be necessary depending on the integrity and currency of the POI credential.

9.2 Face to Face Authentication of Existing Customers and Clients

Authentication of existing customers and clients of an agency using a GSEF credential that has been issued by that agency should be based upon a minimum of 2 factors: something they have – their possession of the GSEF credential itself – and at least one other authentication factor (something they know or something they are) both of which can be accommodated by the GSEF credential itself.

1. *Something they have*:

   In the situation of face to face authentication for the GSAR, this will be the GSEF issued credential.

2. *Something they know:*

   This may be a Personal Identification Number (PIN) or password known only to the individual and the issuing agency. Where the PIN or password is contained on the GSEF credential it will need to be protected by sufficient encryption to prevent it being read by unauthorised persons. Alternatively, the something they know may also be a set of questions and answers known only to the individual and agency.

3. *Something they are:*

   This should be a biometric identifier – most likely a photograph of the individual printed on the surface of the credential or contained in the credential's integrated circuit chip. In most cases a visual match to the biometric on the credential should be sufficient. However in high risk transactions, agencies may consider re-checking the biometric identifier against system held data.

9.3 Telephonic Authentication of Existing Customers and Clients

Situations will arise – in remote localities for example – where the identity of an existing customer or client needs to be authenticated over the telephone. In these circumstances, authentication may be achieved by

using a *Something they know'* factor, plus a voice recognition '*Something they are'* biometric identifier.

10. Privacy and data protection

In implementing an e-authentication mechanism that provides level 4 assurance agencies will need to identify and address the particular privacy issues that arise in relation to the mechanism chosen. Privacy is discussed in general terms in the AGAF, and more specifically in other relevant documents including those relating to the Australian Government Smartcard Framework and the Gatekeeper Framework. Agencies should refer to the latter two documents when seeking privacy guidance around the use of smartcards and PKI respectively.

A common thread running through these documents is that agencies should carry out a privacy impact (PIA) assessment before choosing and implementing an e-authentication mechanism in accordance with the PIA privacy guidelines released by the Office of the Privacy Commissioner in August 2006.

11. Governance mechanisms

For security purposes and to achieve high level trust in the selected level 3 or 4 e-authentication approach, conscious implementation of detailed governance processes is essential. These processes should be documented and responsibilities for managing and monitoring of processes clearly identified. Processes should establish that:

- the approach and its implementation are working as intended;
- this gold standard is being complied with; and
- customer orientated processes for handling failures are successful.

Agencies implementing an e-authentication process that requires level 4 assurance should check using both internal and external audit mechanisms on a regular basis to provide assurance that risk, including security and privacy remain appropriately managed.

References

Australian Government e-Authentication Framework, AGIMO (Department of Finance and Administration), 2005; www.agimo.gov.au/infrastructure/authentication/agaf

Australian Government Smartcard Framework, AGIMO (Department of Finance and Administration), 2006; www.agimo.gov.au/infrastructure/smart_cards

Gatekeeper Framework, AGIMO (Department of Finance and Administration), 2006; www.gatekeeper.gov.au

Australian Government Protective Security Manual, Attorney-General's Department, *2005;* www.ag.gov.au/agd/WWW/protectivesecurityhome.nsf/Page/Protective_Security_Manual

Australian Government Information and Communications Technology Security Manual, Defence Signals Directorate, September 2006; *www.dsd.gov.au/library/infosec/acsi33.html*