

Report to the Council of Australian Governments  
on the elements of the National Identity Security Strategy

April 2007

## TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>1</b>
<b>THE GOLD STANDARD ENROLMENT FRAMEWORK.....</b>	<b>3</b>
<b>SECURITY STANDARDS FOR PROOF-OF-IDENTITY DOCUMENTS .....</b>	<b>11</b>
<b>GOLD STANDARD e-AUTHENTICATION REQUIREMENTS.....</b>	<b>19</b>
<b>THE NATIONAL DOCUMENT VERIFICATION SERVICE.....</b>	<b>37</b>
<b>IMPROVING THE INTEGRITY OF IDENTITY DATA.....</b>	<b>45</b>
<b>BIOMETRIC INTEROPERABILITY .....</b>	<b>51</b>

## INTRODUCTION

Identity security is a critical concern to Australian, State and Territory governments who have responsibility for Australia's national security, revenue protection and law enforcement. False identities underpin terrorist and criminal activity, undermine border and citizenship controls, and efforts to combat terrorist financing and financial crime. Identity theft is also a major invasion of privacy and a serious concern to the Australian community. It is essential to Australia's security and economic interests that the identities of persons accessing government or commercial services, benefits, official documents and positions of trust, can be accurately verified.

Identity security is a whole-of-government cross-jurisdictional issue. Developing and implementing the National Identity Security Strategy (the Strategy) will require a comprehensive and collaborative effort between and within jurisdictions.

Recognising these concerns, the National Identity Security Coordination Group (NISCG) has given significant consideration to responses which will achieve the elements of the Strategy. The NISCG has mapped out six elements which will provide a framework for strengthening national arrangements at each point along the identity security continuum.

Substantial work has been completed by the NISCG working groups on the six elements. Jurisdictions recognise the value of the work done to date, and that this Strategy provides a guide for the development of jurisdictions' own identity security frameworks. It is noted that the NISCG working groups will continue to develop the work program in accordance with the Inter-Governmental Agreement (IGA) on the Strategy.

This report provides a snapshot of the work to date on the six elements of the Strategy. It is intended as a guide for organisations who want to improve their current identity security arrangements and they are not mandatory.

This report complements the IGA that was tabled separately and signed at the Council of Australian Governments' meeting of 13 April 2007.

The six current elements of the Strategy, outlined in this report, will form the basis for the continuing work of the NISCG.

# THE GOLD STANDARD ENROLMENT FRAMEWORK

## 1. Introduction

The issue of identity security was addressed by the Council of Australian Governments (COAG) Special Meeting on Counter-Terrorism on 27 September 2005. The resulting communiqué noted that “The preservation and protection of a person's identity is a key concern and right of all Australians”, and heads of government agreed to the development and implementation of a National Identity Security Strategy (NISS).

This Framework is intended to operate in conjunction with other elements of the NISS, such as efforts to improve the security of identity documents, authentication standards, biometric interoperability, the integrity of identity data holdings, and procedures for document verification.

The Framework's prime focus is on ensuring applicants for government documents that also may function as key documents for proof of identity (POI) purposes are subject to a rigorous process of identification and verification. The Framework provides a comprehensive approach to the establishment of identity by individuals. It does not address other enrolment considerations such as eligibility and entitlement.

In 2004 the Standing Committee of Attorneys-General endorsed use by agencies of a POI Framework (at Attachment A). The POI Framework may be read in conjunction with this report.

The Framework and the processes embedded in it are intended for use by government organisations at this time, but could serve as a benchmark for private sector customer identification and verification processes. While the Framework does not directly apply to processes employed by agencies when registering and enrolling individuals for government benefits and services, it could however be referenced as appropriate within the broader personal identification frameworks that apply to such enrolment processes.

The National Identity Security Coordination Group will provide the ongoing governance necessary to maintain and develop the Framework in light of policy, legislative and technological developments, and changes in the environment and risk criteria for credentials<sup>1</sup> which will occur over time.

## 2. Purpose

Secure enrolment is a pre-requisite to building an identity security system of high integrity. Accordingly, it is necessary that sufficiently high quality processes are put in place to register, enrol and issue key POI credentials to individuals and for these processes to be embraced and applied consistently by relevant credential issuing agencies.

---

<sup>1</sup> Credential is a generic term that can apply to both paper documents and non-paper based objects such as smartcards and other tokens.

As credentials used as POI play an important role in the community, the issuing of such credentials is a high risk process requiring a high integrity enrolment approach to reduce the risk of identity crime. Adherence to the Framework would enable greater consistency in the registration of identity details and enhance public confidence in government enrolment and registration processes.

### **3. Scope**

The Framework specifies a premium, or “Gold Standard”, approach for use by government agencies who enrol individuals for the purpose of issuing government documents that also may function as key documents for POI purposes. This Framework provides a firm foundation for other elements of the NISS, but does not include efforts to improve the security of identity documents, authentication standards, biometric interoperability, the integrity of identity data holdings, and procedures for document verification.

This framework is not intended to apply to the issuance of birth certificates at or near the time of birth.

### **4. Principles for Gold Standard Enrolment**

#### **Application of the Gold Standard**

**Principle 1:** *The Gold Standard will define a high quality approach to enable the consistent and robust enrolment of individuals and give a strong assurance of individuals’ identities. The use of the Gold Standard will also underpin other measures to enhance identity security under the NISS.*

**Principle 2:** *The Gold Standard should be applied in circumstances where the consequences flowing from registering a false identity are high and a high level of confidence in establishing a person’s identity is required. It should be used when issuing key POI credentials or for national security checking purposes.*

**Principle 3:** *Gold Standard enrolment will need to adhere to relevant privacy principles and privacy regimes.*

#### **Evidence used to identify the applicant**

**Principle 4:** *Gold Standard enrolment will need to establish evidence of a person’s commencement of identity in Australia. In most cases, this will involve verifying a person’s name and gender as registered with a Registrar of Births, Deaths and Marriages or, in the case of people born overseas, the Department of Immigration and Citizenship as the basis for issuing key POI credentials.*

**Principle 5:** *Gold Standard enrolment will need to establish evidence of a person’s identity operating in the community. In most cases, this will involve verifying a person’s ‘social footprint’ from credentials or other information establishing a person’s use of identity in Australia over time.*

**Principle 6:** *Gold Standard enrolment will need to establish evidence of a linkage between the applicant and the claimed identity. This will usually involve the presentation of government-issued POI credentials embodying photographic or biometric identity features. These credentials might also be used to establish commencement and use of identity under Principles 4 and 5 above.*

### **Verification of POI credentials or information**

**Principle 7:** *POI credentials and other information provided by the applicant to satisfy Principles 4 to 6 should be verified with the relevant issuing authority or other authoritative source.*

### **Interviewing the applicant**

**Principle 8:** *An enrolling agency should conduct a face-to-face interview when issuing government documents that also may function as key documents for POI purposes.*

**Principle 9:** *An enrolling agency should bind the applicant to the identity recorded on the POI credential that is issued by taking a photograph or a biometric of the applicant. This will ensure that the agency can subsequently check to whom the POI credential was issued.*

### **Streamlined interaction after a Gold Standard enrolment**

**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.*

**Principle 11:** *An enrolling agency should only issue a key POI credential when the claimed identity has been sufficiently validated in accordance with Gold Standard enrolment procedures.*

**Principle 12:** *A key POI credential issued as a result of a Gold Standard enrolment could be used to streamline enrolments with other agencies.*

**Principle 13:** *Where an enrolling agency already possesses information verifying a client's identity to the equivalent of a Gold Standard (a known customer), that identification process may be used to streamline further enrolment for a new key POI credential. A 'known customer' should however be required to provide evidence confirming their identity in accordance with Principles 7-9 above.*

### **Developments in technology**

**Principle 14:** *Gold Standard enrolment principles will be revised in the future to incorporate developments in biometric technology.*

## **5. Processes for Gold Standard enrolment**

Gold Standard enrolment should include the following processes:

### **5.1 The application stage**

- lodgement of the application;
- initial assessment of the application to confirm it has been correctly completed and contains sufficient information to enable verification of the applicant's claimed identity as per Principles 4 to 6;
- recording the details of POI credentials or information presented by applicants;
- verification of key POI credentials or information. Verification can take place prior to the interview;
- noting the applicant's record with the verification result(s).

### **5.2 Pre-interview assessment**

- On the basis of information provided by the applicant the enrolling agency will check its identity register for an existing enrolment to ensure the applicant is not already enrolled.
- The enrolling agency will assess whether the applicant:
  - has already been enrolled to a Gold Standard;
  - is likely to achieve Gold Standard verification of their identity;
  - is likely to need additional assistance to identify themselves to the Gold Standard level.
- There are several ways in which an applicant may be able to satisfy the Gold Standard principles. A principle may be satisfied by either reference to a registration in an appropriate identity register, a credential that evidences that registration, or rigorous enquiries and detailed checks which satisfy the same requirement.
- Where an agency is satisfied that an applicant has already been enrolled to a Gold Standard then an abbreviated face-to-face interview process may be implemented.

### **5.3 The interview**

- Where the applicant attends a face-to-face interview with the agency or its nominated representative, the applicant should provide at that interview:
  - the original application form (if not already submitted);

- original POI credentials or verifiable information providing evidence of their commencement, use and linkage of identity;
- explicit consent to verify the credentials or information provided.
- The applicant may be required to have biometric detail recorded during the interview (e.g. a photograph) that will bind the applicant to the claimed identity.
- The interviewing officer should check the originals of any POI credentials or information submitted to ensure:
  - the credentials or information satisfy Principles 4 to 6;
  - that there are no physical signs of tampering of any credentials;
  - the applicant's name is on every credential. Where the POI credentials bear a different name then the linkage between that POI credential, the name to be registered and the applicant must be clearly established;
  - the applicant's date of birth is on at least one of the credentials;
  - a recognisable photograph of the applicant is on at least one of the credentials;
  - the applicant's signature is on at least one of the credentials;
  - the applicant's address is on at least one of the credentials;
  - if required, that none of the credentials have expired.

#### **5.4 Verification of credentials and/or information**

- The enrolling agency should verify POI credentials if not already undertaken.
- The enrolling agency retains a copy of the POI credentials or information presented. This process could be optional if the POI credentials are electronically recorded and verified.
- The original POI credentials are returned to the applicant.
- Key information provided by the applicant will need to be verified. Verification may be performed by reference to an appropriate identity register or other authoritative source.

#### **5.5 Post application**

- The enrolling agency should conduct follow-up investigation of individuals presenting unverifiable credentials or information;

- The enrolling agency should conduct follow-up investigation of individuals presenting credentials which have been recorded as lost or stolen;
- The enrolling agency should review enrolments which exhibit risk<sup>2</sup> and investigate anomalies to ensure the integrity of the information that has been recorded;
- The enrolling agency should integrate enrolment processes with critical post enrolment mechanisms, such as:
  - establishing secure and reliable processes for registering change of name, gender or address, and for credential re-issuing processes;
  - cancelling credentials where appropriate to do so;
  - establishing reliable processes for the identification of expired credentials;
  - ensuring, where necessary, that appropriate internal controls around segregation of duties exist for staff involved in the issue of POI credentials;
  - ensuring processing staff hold suitable clearances;
  - ensuring secure storage processes exist for scanned credentials and biometric data.
- issue the new credential or token of high integrity with regard to:
  - ensuring only authorised staff issue the credential;
  - security around the issue and collection of the credential.

## **6. Exceptions**

### **6.1 Circumstances**

Although a high proportion of the Australian population will be able to meet the requirements of a Gold Standard enrolment, some applicants may face genuine difficulty in identifying themselves in some circumstances.

Circumstances can occur when an individual does not possess, or is unable to obtain, the necessary information or evidence of commencement or use of identity in Australia to meet the Gold Standard (e.g. some homeless persons or some persons with mental health issues).

When an applicant is unable to provide the necessary POI credentials or verifiable information an enrolment process may entail:

---

<sup>2</sup> Risk refers to the enrolling agency's risks identified in their risk assessment framework and fraud control plan.

- lodgement of an application;
- verification of the applicant's claimed identity with authorised referees<sup>3</sup>;
- a face-to-face interview with the applicant;
- the applicant may be required to have biometric detail recorded (e.g. a photograph);
- the enrolling agency will be required to confirm the identity details by:
  - contacting referees who are authorised to perform the confirmation and obtaining from them the assurance that the individual is who they say they are;
  - if necessary, undertaking specific enquiries with persons and organisations associated with the applicant;
  - if the applicant is an established customer of appropriate agencies the claimed identity might be verified directly with those agencies.

Where commencement or use of identity cannot be established to a Gold Standard, it may be appropriate for the enrolling agency to issue the applicant a service-only credential.

## **6.2 Service - only credential**

To varying degrees, all agencies have a minority of customers or clients who have difficulty meeting POI requirements even though they have a legitimate and legal entitlement to certain services or payments. These individuals generally do not have or are unable to obtain the necessary credentials, and/or are unable to provide sufficient information within relevant timeframes to enable enrolment to occur with a high level of confidence about the identity of the applicant.

Enrolling agencies could consider issuing a temporary credential where appropriate to allow the applicant to receive relevant services.

A service only credential would have limitations:

- it would lapse after a limited period of time, either when the individual is able to enrol to the Gold Standard, or when the registration expires;
- it would be issued for the sole purpose of doing business with the enrolling agency;
- it would not be accepted as a key POI credential by another agency.

---

<sup>3</sup> An authorised referee is a person or organisation that holds a position of trust in the community and is known and listed by the enrolling agency to perform the function of a referee.

**ATTACHMENT A**

**PROOF OF IDENTITY FRAMEWORK**

<b>Objective</b>	<b>Documents Satisfying the Objective</b>
<p><b>A</b> Evidence of commencement of identity in Australia  (Mandatory for all agencies)</p>	<ul style="list-style-type: none"> <li>• Birth certificates</li> <li>• Record of Immigration Status:               <ul style="list-style-type: none"> <li>➤ Foreign Passport &amp; current Visa</li> <li>➤ Travel Document &amp; current Australian Visa</li> <li>➤ Certificate of Evidence of Residence Status</li> <li>➤ Citizenship Certificate</li> </ul> </li> </ul>
<p><b>B</b> Linkage between Identity and Person  (Photo &amp; signature)</p>	<ul style="list-style-type: none"> <li>• Australian Drivers Licence (current &amp; original)</li> <li>• Australian Passport (current)</li> <li>• Firearms Licence (current &amp; original)</li> <li>• Foreign Passport</li> </ul>
<p><b>C</b> Evidence of Identity Operating in the Community  (Could be another Category A or B document)</p>	<ul style="list-style-type: none"> <li>• Medicare Card</li> <li>• Change of Name Certificate – Non Standard POI – (for marriage or legal name change – showing link with previous name/s)</li> <li>• Credit or Account Card</li> <li>• Centrelink or DVA card</li> <li>• Security guard/Crowd control Licence</li> <li>• BDM Issued Marriage Certificate</li> <li>• Tertiary ID Card</li> </ul>
<p><b>D</b> Evidence of residential address  (Used only to provide evidence of residential address if not provided by a Category B or C document)</p>	<ul style="list-style-type: none"> <li>• Utilities notice</li> <li>• Rent details</li> </ul>

# SECURITY STANDARDS FOR PROOF-OF-IDENTITY DOCUMENTS

## 1. Introduction

The Council of Australian Governments (COAG) addressed the issue of identity security at a Special Meeting on Counter Terrorism on 27 September 2005. The resulting communiqué noted that “The preservation and protection of a person's identity is a key concern and right of all Australians”. Accordingly, heads of government agreed to the development and implementation of a National Identity Security Strategy (NISS).

The NISS has a number of key elements, which aim to strengthen national arrangements at each point along the identity security continuum. A key element of the NISS involves enhancing the security features on key proof of identity documents, including the use of biometric identifiers where appropriate, to reduce the risk of forgery.

This report on Security Standards for POI documents identifies and recommends a set of security standards, with the aim of reducing the risk of forgery or unauthorised alterations of documents. It outlines a system of categorisation of available security features based on assessed risks and levels of confidence.

The standards proposed in this report refer to the security features and do not reflect on the legal purpose of any document or the integrity of underlying systems. The standards are intended as a guide for organisations who wish to consider improving their technical security features used for key documents and are not mandatory.

## 2. What is a POI document?

- A POI document is a document issued by a government body to a person for a specific legal purpose, and which is widely accepted in the community to establish the identity of the holder.
- The term document covers not only traditional paper documents such as birth, marriage or change-of-name certificates, but also includes, for example, passports, drivers' licences or other physical tokens relating to a personal identity.
- Documents may be paper-based or polymer/plastic cards, including 'smartcards'.

## 3. Document security categories

Security features which can be applied to key POI documents have been categorised in three groups: **high**, **medium** and **standard**. It is the responsibility of each document issuing agency to apply these standards in accordance with their own policy priorities, security risk assessments and legislation.

The selection of the appropriate security category for document(s) issued, may be based on the following factors:

- Effectiveness, practicality and fitness for purpose;
- Risk management;
- Technical reliability and durability;
- Interoperability, including reference to electronic verification processes;
- Privacy protection;
- Compliance with relevant Australian and international standards; and
- Cost effectiveness.

Documents requiring the highest level of protection are those carrying the greatest potential damage consequences (e.g. to public safety and public revenue) of the counterfeiting or unauthorised alteration of the document.

The categories' descriptive nomenclature refers to the *security features* included in each category. They are not intended to reflect on the legal purpose of any document or the integrity of underlying data systems.

#### **4. Document security features**

Each category contains a mixture of security features and reflects a range of production costs. A 'high risk' POI document (for instance, a passport) justifies a higher expense for protection than a document carrying a lower risk.

Perfect document security is an unattainable goal. Security measures must be regarded as reducing the risks of forgery or unauthorised alteration or misuse, not eliminating those risks. POI documentation is only one part of a continuum of identity authentication measures. Security features alone cannot guarantee the integrity of a POI document. Unless all other links in the chain are sound (e.g. the legitimacy of the underlying data, the reliability of the issuing process and the presentation of the document by its legitimate holder), there will be the possibility of fraud. POI documents having advanced security features but weak identity processes (e.g. where a photograph is incorporated without sufficient checks to ensure it is not that of an impostor) actually increase the risk of fraud as the document has a high-integrity appearance and is likely to be more widely accepted as evidence of identity than a seemingly less secure POI document.

A comparative overview of security features is at table (a) following. The specifications for the features are at tables (b), (c) and (d).

The tables specify the *minimum* recommended range of features for each nominated category. Agencies may increase the number or type of features in their POI documents.

However, care should be taken in selecting additional features for documents. An inappropriate combination of security devices can negate their benefit. For example, intaglio printing over a watermark will make the watermark difficult to see. Over-complexity may introduce a problem with useability. The inspection procedure may be difficult to remember and harder to perform.

The security features allow for defence-in-depth. No single feature is sufficient. A range of features allows for different levels of inspection. Some provide only moderate security but provide easily identifiable visual or tactile features for easy checking. Others provide better security but may require more time/equipment to check.

## **5. Training**

Examiners must be aware of the security features incorporated into documents which assist in detection of fraudulent documents. It is essential that information on specific document security features is available to first and second-line examiners<sup>4</sup> across consumer agencies. Document issuing agencies must acquire expertise essential to conduct third-line and electronic examinations.

## **6. Biometric interoperability**

Biometrics can be defined as measurable physical characteristics or personal behavioural traits used to recognise the identity, or verify the claimed identity, of a person.<sup>5</sup> The principle biometrics in wide use in Australia are fingerprint (principally law enforcement agencies), facial recognition and signature recognition. In this Report, facial (visual/physiological) and signature (visual/behavioural) recognition have been considered. Newly emerging technologies may bring a wider range of techniques to the forefront in the next few years.

As the public typically interacts with service providers across a number of agencies at all levels of government, it is essential that should a digital facial image be embedded in the integrated circuit (chip) of the POI document, the chip be of a common non-proprietary specification. This provides biometric interoperability and will allow agencies to read the facial image on the chip.

The recommended minimum specification for a facial image stored on a chip is a JPEG image at 300 DPI, used in the current Australian passport.

Guidance for agencies on a broad range of emerging biometric technologies will be provided in the *Australian Government Biometrics Framework (AGBF)*, being developed by the Australian Government Information Management Office (AGIMO). Until the AGBF is completed, the *Australian Government Smartcard Framework* will provide a standardised approach (not standards-based) to using a facial biometric/signature. It is understood these are likely

---

<sup>4</sup> See Table (a) *Document Security Categories and Features* for definitions.

<sup>5</sup> *Biometrics Deployment of Machine Readable Travel Documents*. ICAO Document 9303, 2004

to be based on the International Civil Aviation Organisation (ICAO) standards as a minimum requirement.

## **7. Availability of technology and supply process**

The security printing industry has well established practices for ensuring the security of technologies used in the production of security documents. The supply processes for these technologies are tightly controlled to minimize the risk of unauthorised people gaining access to these technologies and processes.

The controlled availability requirement should be applied to each component or segment of the POI document manufacturing and supply process. Selection of security features should be dominated by these considerations. The strategy here is based on selecting features and technologies that are not available to the general public through normal commercial channels. For the high category features especially, the choice of papers, inks, printing techniques, optically variable device foils and data storage algorithms should be tightly specified to be as distinct from conventional public technologies as possible.

## **8. Standards review**

The security features recommended in this report should be reviewed at least every three years to keep pace with developments in technology and patterns of fraud. Increased sophistication in counterfeiting techniques may require features to be downgraded or removed. New features may also become available.

**Table (a) Document Security Categories and Features**

**Covert** represents the third line of document inspection. A specialist may be required to conduct a detailed in-depth examination of a document using special equipment and knowledge.

**Semi-covert** represents the second line of document examination. A trained employee using simple equipment such as a magnifying glass, ultra-violet light, infra-red lamp, etc.

**Overt** represents the first line of document examination undertaken by a trained employee using sight and/or touch

	Security category		
	High	Medium	Standard
<b>Covert</b>	<ul style="list-style-type: none"> <li>• Security fibre paper or polymer/plastic card equivalent</li> <li>• Hidden image</li> <li>• Screen angle modulation</li> <li>• Security ink</li> <li>• Security threads</li> </ul>	<ul style="list-style-type: none"> <li>• Security fibre paper or polymer/plastic card equivalent</li> <li>• Hidden image</li> <li>• Screen angle modulation</li> <li>• Security ink</li> </ul>	<ul style="list-style-type: none"> <li>• Security fibre paper or polymer/plastic card equivalent</li> <li>• Screen angle modulation</li> </ul>
<b>Semi-covert</b>	<ul style="list-style-type: none"> <li>• High resolution printing processes</li> <li>• Security-type printing features</li> </ul>	<ul style="list-style-type: none"> <li>• High resolution printing processes</li> <li>• Security-type printing features</li> </ul>	<ul style="list-style-type: none"> <li>• High resolution printing process</li> <li>• Security-type printing feature</li> </ul>
<b>Overt</b>	<ul style="list-style-type: none"> <li>• Bearer’s signature</li> <li>• Diffractive optically variable device (DOVD)</li> <li>• Digital facial image</li> <li>• Embossing</li> <li>• See-through register</li> <li>• Shadow/secondary image</li> <li>• Unique identifier</li> <li>• Watermark or polymer/plastic card equivalent</li> </ul>	<ul style="list-style-type: none"> <li>• Bearer’s signature</li> <li>• Diffractive optically variable device (DOVD)</li> <li>• Digital facial image</li> <li>• Embossing</li> <li>• See-through register</li> <li>• Shadow/secondary image</li> <li>• Unique identifier</li> <li>• Watermark or polymer/plastic card equivalent</li> </ul>	<ul style="list-style-type: none"> <li>• Embossing</li> <li>• Optically variable ink</li> <li>• See-through register</li> <li>• Shadow/secondary image</li> <li>• Unique identifier</li> <li>• Watermark or polymer/plastic card equivalent</li> </ul>
<b>Integrated circuit</b>	<ul style="list-style-type: none"> <li>• Contact or contactless integrated circuit containing JPEG facial image, Public Key Infrastructure (PKI) and Basic Access Control (BAC)</li> </ul>		

**Table (b) High Category Security Documents**

**Covert** represents the third line of document inspection. A specialist may be required to conduct a detailed in-depth examination of a document using special equipment and knowledge.

**Semi-covert** represents the second line of document examination. A trained employee using simple equipment such as a magnifying glass, ultra-violet light, infra-red lamp, etc.

**Overt** represents the first line of document examination undertaken by a trained employee using sight and/or touch.

	<b>Features</b>	<b>Recommended minimum features</b>
<b>Covert</b>	<ul style="list-style-type: none"> <li>• Hidden image</li> <li>• Paper documents : Security fibres</li> <li>• Paper documents : Security threads</li> <li>• Plastic cards : Fluorescent printed areas embedded on card surface</li> <li>• Screen angle modulation</li> <li>• Security ink</li> </ul>	Include two security inks including at least one taggant ink Include security fibre or security threads in paper documents Include two other 'covert' features
<b>Semi-covert</b>	<ul style="list-style-type: none"> <li>• High resolution printing processes</li> </ul>	Include at least three printing processes as detailed in the Security Features glossary <sup>6</sup>
	<ul style="list-style-type: none"> <li>• Guilloche pattern</li> <li>• Latent image</li> <li>• Microprinting</li> </ul>	Include all three of these printing features. Other additional printing features are also available for inclusion (see Security features glossary)
<b>Overt</b>	<ul style="list-style-type: none"> <li>• Bearer's signature</li> <li>• Digital facial image</li> <li>• Embossing</li> <li>• Diffractive OVD (DOVD)</li> <li>• Paper documents : Watermark</li> <li>• Plastic cards : Watermark equivalent</li> <li>• See-through register</li> <li>• Shadow/secondary image</li> <li>• Unique identifier</li> </ul>	Include DOVD. See Security features glossary on the effects to be included in the DOVD device Include either watermark or see-through register Include at least four other 'overt' features
<b>Integrated circuit</b>	<ul style="list-style-type: none"> <li>• Contact or contactless integrated circuit containing JPEG facial image, including Public key infrastructure (PKI) and Basic access control (BAC)</li> </ul>	Include an integrated circuit which incorporates a JPEG facial image

<sup>6</sup> Security Standards for Proof of Identity Documents, Report of the Working Group, 12 October 2006

**Table (c) Medium Category Security Documents**

**Covert** represents the third line of document inspection. A specialist may be required to conduct a detailed in-depth examination of a document using special equipment and knowledge.

**Semi-covert** represents the second line of document examination. A trained employee using simple equipment such as a magnifying glass, ultra-violet light, infra-red lamp, etc.

**Overt** represents the first line of document examination undertaken by a trained employee using sight and/or touch.

	<b>Features</b>	<b>Recommended minimum features</b>
<b>Covert</b>	<ul style="list-style-type: none"> <li>• Security ink</li> <li>• Screen angle modulation</li> <li>• Paper documents : Security fibre paper</li> <li>• Plastic cards : Fluorescent printed areas embedded on the card surface</li> <li>• Hidden image</li> </ul>	Include one security ink Include at least two other 'covert' features
<b>Semi-covert</b>	<ul style="list-style-type: none"> <li>• High resolution printing processes</li> </ul>	Include at least two printing processes as detailed in the Security Features glossary
	<ul style="list-style-type: none"> <li>• Micro printing</li> <li>• Guilloche pattern</li> <li>• Latent image</li> </ul>	Include two of these printing features. Other additional printing features are also available for inclusion (see Security features glossary)
<b>Overt</b>	<ul style="list-style-type: none"> <li>• Bearer's signature</li> <li>• Digital facial image</li> <li>• Embossing</li> <li>• Diffractive OVD (DOVD)</li> <li>• Paper documents: Watermark</li> <li>• Plastic cards: Watermark equivalent</li> <li>• See-through register</li> <li>• Shadow/secondary image</li> <li>• Unique identifier</li> </ul>	Include a DOVD. See Security features glossary on the effects to be included in the DOVD Include a unique identifier Include digital facial image Include the bearer's signature Include at least one other 'overt' feature

**Table (d) Standard Category Security Documents**

**Covert** represents the third line of document inspection. A specialist may be required to conduct a detailed in-depth examination of a document using special equipment and knowledge.

**Semi-covert** represents the second line of document examination. A trained employee using simple equipment such as a magnifying glass, ultra-violet light, infra-red lamp, etc.

**Overt** represents the first line of document examination undertaken by a trained employee using sight and/or touch.

	<b>Features</b>	<b>Recommended minimum features</b>
<b>Covert</b>	<ul style="list-style-type: none"> <li>• Hidden image</li> <li>• Paper documents : Security fibre paper</li> <li>• Plastic cards : Fluorescent printed areas embedded on card surface</li> <li>• Screen angle modulation</li> </ul>	Include at least two 'covert' features
<b>Semi-covert</b>	<ul style="list-style-type: none"> <li>• High resolution printing processes</li> </ul>	Include at least one printing process as detailed in the Security Features glossary
	<ul style="list-style-type: none"> <li>• Guilloche pattern</li> <li>• Latent image</li> <li>• Micro printing</li> </ul>	Include at least one of these printing features. Other additional security printing features are also available for inclusion (see Security Features glossary)
<b>Overt</b>	<ul style="list-style-type: none"> <li>• Embossing</li> <li>• Optically variable ink</li> <li>• Paper documents: Watermark</li> <li>• Plastic cards: Watermark equivalent</li> <li>• See-through register</li> <li>• Shadow image</li> <li>• Unique identifier</li> </ul>	Include a unique identifier Include embossing Include at least one other 'overt' feature

## **GOLD STANDARD e-AUTHENTICATION REQUIREMENTS**

### **1. Introduction**

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 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 (NISS). The key elements of the NISS 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 NISS, 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 POI purposes. Tokens, documents or credentials that are established with an electronic binding to an identity<sup>7</sup> during the Gold Standard enrolment process 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 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.

### **2.1 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 AGIMO for

---

<sup>7</sup> 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.

the AGAF to be found online at:

[http://www.agimo.gov.au/infrastructure/authentication/agaf\\_b/glossary/v](http://www.agimo.gov.au/infrastructure/authentication/agaf_b/glossary/v)

### 3. Scope

The GSAR will describe a gold standard for electronic identity authentication<sup>8</sup> 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**

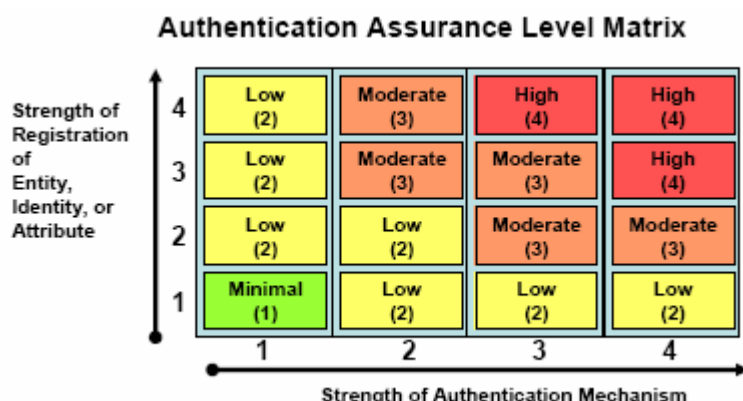
Level 1	Level 2	Level 3	Level 4
Minimal assurance	Low assurance	Moderate assurance	High assurance
Minimal risk posed by transaction; therefore, little requirement for confidence in the assertion	Low risk posed by the transaction; therefore, some confidence in the assertion is required	Moderate risk posed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

<sup>8</sup> 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, these 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 POI 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<sup>9</sup> 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.

---

<sup>9</sup> 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).

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

AGIMO is working on developing guidance on mutual authentication under the auspices of the AGAF and this guidance should be available in 2007.

## **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.<sup>10</sup> 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.

---

<sup>10</sup> In this context the GSEF will define the appropriate way in which credentials are bound to an individual.

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

### **6.2.1 Step 1 – GSEF**

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 2 – 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:

### **Something you have:**

- 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 personal identity number (PIN).
- A protected cryptographic key contained in software.

### **Something you know:**

- 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.

### **Something you are:**

- 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 3 – 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 4 – 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”<sup>11</sup> 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](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.

**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.

---

<sup>11</sup> 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.

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 to assess which appropriate kinds of assurance mechanisms are required. As a general rule, agencies should choose the lowest level in the AGAF 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**

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:

[www.agimo.gov.au/infrastructure/authentication/agaf\\_i/overview\\_and\\_principles](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. 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 GSAR applies only to situations which require the electronic authentication of identity through the use of a 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 two 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.

### **Something they have:**

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

### **Something they know:**

This may be a 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.

### **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 assessment (PIA) 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.

## **12. References**

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

*Gatekeeper Framework*, AGIMO (Department of Finance and Administration), 2006;  
[www.gatekeeper.gov.au](http://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](http://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](http://www.dsd.gov.au/library/infosec/acsi33.html)



# THE NATIONAL DOCUMENT VERIFICATION SERVICE

## 1. Introduction

Identity security is an issue of critical concern to Australian, State and Territory governments and the private sector. It is essential to Australia's security and economic wellbeing that the identities of citizens, legitimate residents and visitors seeking access to government or commercial services, benefits, official documents and positions of trust, can be accurately verified in order to prevent the use of false identities and the assistance they provide to terrorists, people-smugglers and in the commission of economic or other crime.

Improving procedures for verifying the integrity of key identity documents is a critical element of the National Identity Security Strategy. It complements efforts to improve the security of identity documents, client registration and enrolment procedures, authentication standards, biometric interoperability, and the integrity of identity data holdings.

This report supports the establishment of a National Document Verification Service (DVS) as a key component in efforts to enhance procedures for verifying the integrity of key identity documents. It is intended that the DVS be accessible to all Australian, State and Territory government document issuing agencies to strengthen and enhance existing proof of identity (POI) processes and systems.

## 2. Background

The genesis of the DVS lies in a "Feasibility Study for a Document Verification Service" jointly conducted in 2003 by relevant Australian Government, State and Territory government agencies. The study found that POI processes could be significantly strengthened and registrations/enrolment of persons for high value transactions made less open to fraud if agencies were able to confirm the personal information appearing on key POI documents. It recommended that a DVS should be implemented in a measured and staged manner taking account of key agencies' ability to incorporate the necessary functionality with their existing business and information technology systems.

Development and implementation of a national DVS to combat the misuse of false and stolen identities was endorsed by the Council of Australian Governments (COAG) at its Special Meeting on Counter-Terrorism on 27 September 2005 as part of a comprehensive National Identity Security Strategy to better protect the identities of Australians.

A prototype DVS was trialled from February to June 2006, limited to the Department of Foreign Affairs and Trade and the Department of Immigration and Citizenship (formerly known as the Department of Immigration and Multicultural Affairs) checking POI documents offered by individuals seeking

Australian passports and citizenship.<sup>12</sup> An evaluation of the prototype demonstrated its technical feasibility; that secure connectivity had been achieved using dedicated lines; and that verification of the data is viable in an online environment.

### **3. Overview**

#### **3.1 Vision**

The DVS is pivotal to the introduction of more rigorous and accurate national identity security measures. In particular it will strengthen and support client enrolment and registration processes by providing agencies with greater certainty of the identity of prospective clients.

#### **3.2 Objective**

The DVS will enhance the integrity of agencies' POI procedures by providing an assurance that a person is establishing eligibility with verifiable documents. It is envisaged that the DVS will become an accepted and integral part of an agency's POI procedures by minimising:

- a) the registration and subsequent use of false identities, and
- b) the occurrence of multiple enrolments for fraudulent purposes.

The DVS will enable authorised agencies to verify the detail on key POI documents that clients provide when registering or enrolling for benefits or services, and possibly as part of an application to receive an identity document. It will also help ensure the documents are not recorded as being lost or stolen, cancelled, amended or replaced.

#### **3.3 What is the DVS?**

The DVS will be a secure, national, real time, on-line system accessible to all authorised Australian Government, State and Territory agencies, and potentially by the private sector.

It is intended that the DVS allow participating agencies to verify that:

- a document was in fact issued by the document issuing agency claimed on its face
- the details recorded on the document correspond to those held in the document issuing agency's register
- the document is still valid (i.e. has not been cancelled or superseded), and
- the document has not been lost or stolen.

---

<sup>12</sup> POI documentation checked was restricted to Passports, Citizenship certificates and ACT/NSW Birth Certificates and Driver's Licence.

## **4. Benefits**

### **4.1 A national approach**

A national approach to document verification represents a major advance in combating identity crime. It is expected that a significant proportion of identity theft, particularly that of an opportunistic nature, may be deterred by community awareness of the operation of the DVS.

### **4.2 Benefits to government**

The need to correctly establish the identity of individuals is one that exists across Australian, State and Territory government service provision, with agencies being highly reliant on the integrity of key POI documents for establishing clients' identities. Use of the DVS will improve public confidence in the integrity of government registers and the accountability measures used by government to protect public revenue and expenditure.

The DVS will provide a wide range of agencies with a high integrity means of verification, offering greater certainty of the identity of prospective clients. When integrated into government enrolment processes, use of the DVS will allow agencies to:

- replace the need for cumbersome and expensive manual processes that allow only a small fraction of applications to be verified
- conduct more checks on key POI documents during enrolment, providing greater confidence in the identity of those to whom services are provided
- integrate the verification response into their enrolment and business processes to gain further efficiencies
- verify POI documents issued by agencies in a different jurisdiction, and
- avoid the need for separate negotiations for access with a variety of document issuing authorities.

### **4.3 Benefits to the public**

Citizens' trust in government is critically affected by the standard of its information handling. The DVS will enhance accurate confirmation of an individual's identity, reducing the likelihood of identity theft and providing reassurance that governments can carry out their functions efficiently while respecting privacy.

A further benefit to the individual is the increased speed of approval of benefits and services, through a more robust and faster enrolment process. An individual applicant can also have greater confidence in the security of their information as it is being processed.

## **5. Implementation**

### **5.1 How the DVS will operate**

It is intended that the verification process consist of the following steps:

- A person presents their POI documents to an agency in support of their application for a benefit or service.
- The individual authorises the agency to undertake checks to verify the documents.
- Details on the identifying document such as name, date of birth, official registration number of the document, or other identifying features are entered into a computer system linked to the DVS.
- The information is sent via a secure communications pathway to the document issuing agency where an automated check of the agency's register will verify whether the information provided is identical to the information on the document.
- If the information provided matches the information held by the issuing agency, a YES response is transmitted to the inquiring agency informing them that the document has been verified; otherwise, a NO response is returned indicating that the document details were not verified.

The DVS processes will be complemented by checks by the service delivery agency on the authenticity of the documents presented, according to agreed security standards for POI.

### **5.2 Operating principles**

It is proposed that the following operating principles form the basis for development of the DVS.

- The DVS will replace current verification practices but will not change the way in which agencies deal with personal information.
- Document issuing agencies will maintain ownership and control of their data and systems.
- The DVS will provide a means of verifying that the document being checked has identical information to the document originally issued.
- The DVS will only seek to verify information from the POI document with the issuing agency. It will not retrieve any information held by the issuing agency.
- The function of the DVS is not to store information, but to act as a conduit for the verification of information that is already held by issuing agencies.

- Information sent to or from the DVS will be transmitted using secure, encrypted methods of communication.
- An inquiring agency will not base any decision to grant enrolment for a benefit or service solely on the basis of a positive response from the DVS.
- An inquiring agency will not reject a POI document on the basis of a single negative response from the DVS.
- A response received from the DVS will only be used for the purpose of verifying information included on a POI document.
- Standards and protocols will govern the administration, access to and use of the DVS.
- The National Identity Security Coordination Group will provide high level oversight and guidance to the development and implementation of the DVS.

The DVS will maintain a high level of responsiveness to requests to ensure that it meets the needs of the user.

### **5.3 The importance of national identity data capture**

The full participation of Australian, State and Territory governments and document issuing agencies is critical to the success of the DVS. Without national coverage, criminals will be able to exploit weak links in the identity verification process.

Records kept and maintained by agencies relating to the beginning and end of identity are of critical importance in improving personal identification systems in Australia.

Rollout of a DVS will require access to electronic data held by agencies responsible for issuing key POI documents such as the Australian Government Department of Foreign Affairs and Trade and Immigration and Citizenship, and all State and Territory Roads Traffic Authorities and Registrars of Births, Deaths and Marriages.

Currently not all birth, fact of death, arrivals or citizenship registration information is captured electronically. The availability of such electronic data is critical to the operation and effectiveness of the DVS. Therefore back capture of this data to agreed common dates is required.

Recognising the need for national electronic data availability, the Parties agree to work towards the electronic capture of birth, fact of death, arrivals and citizenship data and to give consideration to a common date from which records would need to be captured.

## **5.4 Financial arrangements**

The implementation of the DVS will strengthen the integrity of Australian, State and Territory government agency enrolment processes. While the benefits of this are not quantifiable, it will make Australian, State and Territory government agencies less open to fraud, resulting in a reduction in lost revenue for Australian, State and Territory governments.

Some States and Territories charge for access to registration data which would need to be accessed for the effective operation of the DVS. Achievement of the full benefits offered by the DVS through fast access and streamlined administration will require agreement on a financial regime to enable future access.

Recognising the common interest in removing obstacles to the effectiveness and comprehensiveness of the DVS, the Parties agree to work towards finalising a mutually agreeable financial regime for access and use.

## **5.5 Indemnity**

It is not expected that there will be any claims against a data issuing agency for possible losses resulting in liability arising from the operation of the DVS. There are two reasons for this:

- 1) The key operating principles of the DVS that:
  - An inquiring agency shall not base any decision to grant enrolment for a benefit or service solely on the basis of a positive response from the DVS, and
  - An inquiring agency shall not reject a POI document on the basis of a single negative response from the DVS.
- 2) The DVS will not introduce any risks additional to those already posed by current verification processes.

In view of this, and recognising that as a general principle risks should be borne by those best placed to manage them, the Parties agree not to require indemnity from liability arising from their participation in the DVS.

## **5.6 Privacy impacts**

Implementation of a national DVS will involve ongoing consultations with the Office of the Privacy Commissioner (Cth) and State and Territory privacy officials to ensure that national oversight and accountability arrangements take account of cross-jurisdictional and public sector flows of information.

The Commonwealth will prepare a Privacy Impact Assessment for the DVS which will outline the privacy implications and strategies to manage these.

## **5.7 Future development**

The scope and functionality of the DVS has been designed to take into account emerging policy and technological initiatives relating to identity security. Due consideration will also need to be given to how the DVS will complement, or operate in relation to any new initiatives and the opportunities those initiatives may provide to enhance the service.

The potential for expansion of the DVS to certain industries such as the banking sector is also an area for future consideration, following implementation by government agencies and appropriate consideration of key issues such as privacy, risk management and user access arrangements.

## **6. Conclusion**

Australia relies on a range of documents that a person may use to identify themselves. A DVS will improve the reliability and integrity of these documents as part of a national approach to improving identity security.

Once established, there is substantial scope to further enhance the capability of a DVS by adding other potential Australian, State, Territory or private document issuers. Over time, it may be possible to extend the scope of the DVS to include access by sensitive areas of the private sector, such as the financial and transport sectors, subject to suitable safeguards.

The development of the DVS will be an integrated and iterative process, incorporating future identity security initiatives, and making best possible use of new technological solutions. Such linkages will help in future-proofing Australia's identity security strategy against emerging vulnerabilities.



## **IMPROVING THE INTEGRITY OF IDENTITY DATA**

### **1. Background**

#### **1.1 The need for improved integrity of identity data**

All governments require information about individuals to take informed decisions about those individuals and to carry out their activities more broadly. Many government agencies collect information on the identity of individuals to:

- ensure that an individual seeking access to government services has an entitlement to those services, and
- prevent fraud and consequent loss of government revenue, breaches of privacy, or risk to the public.

While governments need to collect identity information, their information needs vary, as do their methods of processing and recording identity data.

Variations in the processing and recording of identity data between agencies, and changes over time can result in excess, redundant or false identity records. Inaccurate identity records undermine governments' ability to properly allocate entitlements, collect revenue, provide services effectively and efficiently, and comply with privacy obligations.

Improving the integrity of identity data holdings is a key element of the National Identity Security Strategy. It complements efforts to improve the security of identity documents, client registration and enrolment procedures, authentication standards, biometric interoperability, and systems for verifying the integrity of key identity documents.

In particular, improvements to the integrity of agency identity data holdings are necessary to ensure the effective operation of the national Document Verification Service (DVS). The existence of multiple, incorrect or fraudulent registrations in key agency data holdings will compromise the efficient working of the DVS, and could lead to a compounding of fraudulent identity information.

Improving the integrity of data holdings will also complement efforts to improve registration procedures for government documents that also may function as key documents for proof of identity (POI) purposes. It will help to ensure that existing identity data can be relied on when a person enrolls for new key POI documents.

### **2. Methods for improving integrity of identity data**

Data cleansing and data-matching are two tools for improving the integrity of identity data holdings.

Data cleansing is generally single-agency focused, and aims to ensure that only one registration exists for each individual identity. Methods of data

cleansing vary, and are rapidly evolving in tandem with developing information technology solutions.

Commonly used methods include:

- internal file matching – comparing an agency’s customer register with itself to remove or flag excess customer registrations. These internal checks can help ensure the uniqueness of each identity registered on the database, foster an environment where false identities are more readily detected, and improve the scope for data-matching with other agencies;
- checking of other names – a process in which separate records in an individual’s married, maiden names or other known names are identified and linked using information such as birth data already held on the database, and
- checking of deceased persons – a process in which individual identity records are checked against existing agency records or records of deceased persons such as the National Fact of Death database to remove these records from the database, or mark them appropriately.

Data-matching is generally multi-agency focused, and enables the large-scale comparison of information to align recorded identities with the individuals to whom they relate. This is relevant both to cleansing existing identity databases and to improving the recording of new identities.

Cross-agency data-matching can be used to detect fictitious or ‘created’ identities, and stolen identities. It provides a means of accessing and aligning key identity details that will pinpoint a fraudulent or stolen record. Systematic analysis of the composite information collected for the matched records can identify inconsistencies that characterise identity theft or fraud. For example, anomalous address and contact details between a fraudulent record and the legitimate records on other databases may point to a stolen identity.

### **3. Privacy implications**

Individuals have a clear interest in the information about them held by government being correct, and in that information is being used only for defined purposes. The privacy impacts of identity data-matching processes will be a product of the design of those processes, and the consequences of particular choices need to be understood.

Poor quality identity data, and the absence of processes to improve that quality, reduce the ability of agencies to ensure that identity data is accurate, complete and kept up-to-date. Efforts to improve the integrity of identity data through data-matching and data cleansing can reduce the significant risks to privacy resulting from identity theft and fraud.

It is vital that data cleansing and matching protocols ensure that individuals are informed of the uses and disclosures that will be made of their personal

information and that the consent of those individuals be sought where appropriate.

It should also be recognised that there are circumstances in which individuals may not wish personal information to be shared between agencies despite the benefit of reduced risk of identity theft and fraud. This may be for various reasons, but particularly in situations where the inadvertent improper use or disclosure of personal information, such as residential address, by an agency may have serious ramifications for the individual (e.g. domestic violence situations).

#### **4. Interoperability issues**

Information technology options for data cleansing and matching are rapidly evolving. In-house solutions may involve agencies building applications to suit their specific requirements, while proprietary software products, designed to provide more generic solutions, are also available. However, there are currently no best practice solutions to guide government agencies in Australia wishing to employ identity data-matching.

Databases are designed to meet the individual business needs of agencies, and will reflect the differing levels of importance an agency attributes to the various elements of an individual's personal information. For example, individual identity information collected by the Australian Passports Office will reflect the primary purpose of ensuring a person's commencement of identity in Australia by reference to birth or citizenship data, and any change of name information. Identity information collected by the Australian Electoral Commission will reflect a stronger emphasis on current address and any movement data.

Such decisions will affect the capacity for cross-agency data-matching. For example, an individual may be recorded in multiple agency databases, but be unable to be identified through data-matching because of differences in the way key details such as names are recorded. Improving the chances of correctly matching such records requires steps to standardise the recording of commonly held details or the establishment of standards for data-matching to overcome data and field inconsistencies between information holdings.

Differing protocols for recognising and recording 'change of name' in Australia can also affect data integrity. For example, a woman who adopts her husband's surname following marriage may be registered in different agency databases under both names, particularly where the person's married name has not been formally registered. Without a formal linkage between these differing names, data-matching and data cleansing will be made more difficult.

Particular issues arise in the biometric context. For example, the increasing trend towards use of smartcard technology for key identity documents places greater emphasis on the 'readability' of biometric features such as a person's photograph or signature. The capacity to match such information will become increasingly important over time, and will only be possible if standard formats are adopted for the capture of such information.

## 5. Evolving legal environments

All government agencies are subject to privacy and secrecy legislation of general application in addition to agency-specific legislation. The legal environments of individual agencies will vary, but in every case those legal environments will affect the extent to which those agencies can engage in identity data-matching.

Privacy regimes seek to preserve the ability of individuals to determine what happens to their personal information, and to have government agencies focus on the level of personal information actually needed to perform their legitimate functions. Secrecy provisions serve to protect the operations of government and to support public confidence that government agencies handle information appropriately, which in turn affects the quality of information individuals are prepared to disclose to government.

Agency-specific legislation may place statutory limitations on the collection, use and disclosure of personal identity information. For example, taxation legislation places specific limitations on the disclosure of tax file numbers for identification purposes.

Legal environments are also evolving in response to the increasing risks of identity theft and fraud in the e-commerce environment and to emerging national security threats. For example, phishing is the practice whereby a fraudster pretending to be from a legitimate organisation sends misleading emails requesting personal and financial details from individuals. Phishing is increasingly affecting all realms of e-commerce including government services.

In addition, threats to national security from terrorism have placed a heightened priority on the need for governments to verify the identity of citizens. False identities underpin terrorist and criminal activity and have the potential to undermine border and citizenship controls and efforts to combat terrorist financing and financial crime. It is essential to Australia's security and economic interests that records of the identities of persons accessing government services, benefits, official documents and positions of trust are accurate and up to date.

In this new environment, it is important that privacy values and identity security goals be seen as part of the same continuum rather than existing in opposition to each other. Legislative frameworks should allow the articulation and defence of all legitimate interests in a co-ordinated way that both brings existing processes into a coherent approach and also guides the construction of future additions.

## **6. Future-proofing**

The environment in which government operates has changed over recent decades as a result of improved information and communications technologies to require greater and faster responsiveness to the needs and expectations of citizens. E-government and the provision of services online are relatively new phenomena, as are the linkages of agencies at each level of government and between levels of government.

Although not necessarily technology-specific, present regimes regulating data-matching, privacy and secrecy in most jurisdictions were constructed against the background of a much more limited computing environment where government was not so closely interconnected. It is timely to revisit those regimes to see if they most efficiently and effectively reflect contemporary policy choices, the present needs of government and the expectations of citizens.

The increasing interconnectedness of government within and across levels, and individuals' increasing interaction with government based on needs rather than a knowledge of the organisational structure of the bureaucracy, suggest that greater use needs to be made of the possibilities offered by information and communications technologies. These possibilities include greater use of identity data-matching.

The challenges facing government increasingly cross over structural and political boundaries – terrorism and organised crime are examples particularly relevant to identity data. Future measures will increasingly require a co-ordinated national approach encompassing statutory and other regulatory regimes, work processes, information technology solutions and engagement with the private sector.

## **7. Next steps**

Action to improve the integrity of identity data held by governments in Australia could include:

- (i) ensuring that identity data held by agencies is accurate, complete and up-to-date
- (ii) reviewing statutory regimes dealing with privacy and secrecy to identify inconsistencies and opportunities for improving efficiencies in identity data management
- (iii) working collaboratively to develop national best practice guidelines for identity data collection and identity data-matching, including developing standards for processes to support identity data-matching
- (iv) reviewing identity data recording systems and procedures and examining the scope for improved consistency of identity recording to facilitate identity data-matching across government agencies

- (v) working collaboratively to develop a common approach to identity data-matching, including:
  - (a) establishing a common approach to privacy and secrecy and the relationship between them
  - (b) establishing the factors to be considered in determining whether or not identity data-matching is appropriate in a particular situation
  - (c) establishing the factors to be considered in determining whether or not it would be appropriate to extend data-matching activities to involve private sector organisations
  - (d) where identity data-matching protocols require the concurrence of a particular agency before an identity data-matching exercise can proceed, streamlining the necessary consultation and authorisation procedures
  - (e) considering creating a standing authorisation for identity data-matching for non-commercial government purposes
- (vi) in order to assist in combating terrorism and organised crime, working collaboratively to identify circumstances where a standing authorisation for identity data-matching may be appropriate after consulting with relevant privacy commissioners, either on an on-going or case-by-case basis, and taking necessary measures to give effect to such an authorisation
- (vii) in order to assist in combating terrorism and organised crime, identifying particular aspects of identity data management in Australia as priority areas for national action
- (viii) at the request of the Commonwealth, consider cooperating in data-matching activities involving parties other than Australian Government agencies

## BIOMETRIC INTEROPERABILITY

### 1. Background

#### 1.1 Biometric systems

Biometrics are automated means of recognising a person through the measurement of distinguishing physiological or behavioural traits.<sup>13</sup> The range of measurable characteristics that are distinctive of individuals has increased over the last two decades and is likely not complete yet. Currently recognised biometrics include:

Biometric	Features used
Fingerprint recognition	Unique finger ridge detail and pore structure
Hand or palm recognition	Vein structure, measurement of fingers and palm
Iris or retina recognition	Iris pattern, vein structure
Face recognition	Relationship of specific facial features (eyes, nose, mouth)
Voice recognition	Tone, timbre, speech pattern
Signature recognition	Pressure and speed differentials

Traditionally, identity verification has relied on something you know, such as a password or personal identification number (PIN), or on something you have, such as a smart card or access device. Biometrics offer the advantage of being based on the unique physical characteristics of an individual. This means there is nothing to carry or remember, and much less possibility that a biometric identifier could be used without the individual's knowledge and permission. To provide even stronger authentication mechanisms, biometrics can also be used in combination with other authentication mechanisms, such as passwords, digital certificates and smart cards.

Biometrics provide the "what you are" factor in multi-factor authentication approaches and can, in combination with "what you know" and "what you have" factors provide strong authentication. For example, a photograph on the surface of a smartcard, or stored in the chip, can provide strong binding of the relevant identity to the card so that ownership of the card cannot be authenticated by another identity.

Biometric details are initially captured during an enrolment process and are then stored for later comparison. These details can be stored in a database and also on a computer chip for subsequent inclusion in another credential, such as a smart card or a passport.

Individuals presenting to obtain a service or access to something will have their biometric information read by a sensor and that data compared with the

<sup>13</sup> *Biometrics Deployment of Machine Readable Travel Documents* ICAO Document 9303, ICAO 2004.

stored values. A successful match between the 'live' and the stored biometric data confirms the identity of the individual and the desired activity is permitted.

Biometrics systems are not infallible nor can be employed in every situation or on every occasion. Matching is based on probability, and biometrics have varying rates of false positive and false negative matches. Due to physical or environmental reasons, individuals may be incapable of having a particular biometric 'template' recorded at enrolment or later when presenting for a service. Further, given that all biometrics have some reliance on our physical selves, some remain fixed while others change over time.

## **2. Privacy and community acceptance**

Biometrics have the capacity to be both privacy enhancing (e.g. when used to provide security against unauthorised access to another's personal information) and privacy invasive (e.g. when used to monitor an individual's movements or activities). The impact of biometrics on privacy will largely depend on the uses to which they are put.

At the very least, biometric data will typically fall within the definition of personal information in statutory privacy regimes and government agencies must deal with it accordingly. In particular, agencies need to ensure that they comply with their privacy regimes in pursuing biometrics as a solution for the authentication or identification of individuals. Toward this end, agencies should consult with Australian, state and territory government privacy commissioners as appropriate prior to considering the use of biometric data in identity security projects.

Some individuals may regard biometrics as inherently invasive of individual privacy because they identify people by sampling a part of their body or behaviour. Additionally, some types of biometrics may be regarded by different members of a user population as more or less invasive, and this may be connected to the degree of physical intrusion or the reasonable ability to refuse to supply a biometric.

Most forms of biometrics will only work if users are willing to voluntarily submit a part of their body or behaviour for authentication or identification. While face recognition may be regarded by some as less invasive because it is done from a distance, the use of 'face in the crowd' facial recognition may be regarded as involuntary surveillance.

Other factors, in addition to privacy, will affect user attitudes and acceptance. The attitudes of the particular user population, and variations within that population, will be another important consideration. Biometric systems will usually need to be able to recognise people of all racial groups and ages in the user population. However, it is possible that individuals with particular cultural or religious beliefs may not be willing to voluntarily access premises or systems protected by certain types of biometrics.

Consideration also needs to be given to ensuring that people with a range of disabilities will be able to access premises or systems protected by

biometrics. Provision should also need to be made for individuals for whom the use of biometrics is not appropriate. It is likely that in any given user population there will be individuals who due to physiological or cultural reasons will not be able or willing to use biometrics. Alternative service channels may need to be provided.

### **3. Standards and interoperability**

Currently there is little interoperability between biometric systems produced by different vendors, even those utilising the same biometric characteristic. The biometrics market has been characterized by a mixture of open and proprietary standards with intense competition for market space between some proprietary standards and similar open standards. Consequently there are new biometrics approaches and products being currently developed and this will likely continue for some time.

Although governments and some segments of the biometrics industry have been pursuing standardisation, a major driver for innovation in the industry as a whole has been the development of intellectual property rights (IPR) for biometrics products (including algorithms, software and hardware) in order to either dominate a biometrics sector or to license the relevant IPR. This, combined with the market share already obtained by some proprietary standards, has a tendency to work against any trend towards increased interoperability.

In order to assist Australian participation in all types of activities around the globe, the Australian Government has a preference for co-operating on international standards rather than developing purely local standards. International efforts to standardise biometrics have been led by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Civil Aviation Organisation (ICAO).

In each country, national representatives participate in the development of international standards through technical committees established to deal with particular fields of technical activity. The ISO and IEC have established a Joint Technical Committee on Information Technology which in June 2002 established a Subcommittee on Biometrics, SC37. Australia's involvement in SC37 is being driven by the Australian Government, in particular through the passports area of the Department of Foreign Affairs and Trade (DFAT).

Standards Australia represents Australia on the ISO and the IEC. It recently formed a dedicated committee, IT-032, to address standardisation in the field of biometric and identification technologies and applications. The committee's work includes Harmonized Biometric Vocabulary, Biometric Testing and Reporting, Cross-Jurisdictional and Societal Aspects, driver licences and passports. The committee will also contribute to the Joint Technical Committee's SC37 biometrics area of work.

Within Australia, individual agencies are recognised as having particular expertise in the implementation of specific biometric applications: CrimTrac for

fingerprint technology; DFAT for facial recognition; the Department of Immigration and Citizenship for iris technology; and Centrelink for voice recognition.

The Australian Government Information Management Office (AGIMO) began work on an Australian Government Biometric Framework in 2005. That work has been incorporated into this Report, and a number of agencies have offered to provide reference material through the National Identity Security Strategy Authentication Working Groups, managed by AGIMO.

#### **4. Next Steps**

Action to improve biometric interoperability could include:

- (i) nominating particular agencies as national centres of expertise and reference points for particular biometric technologies
- (ii) exploring the potential for development of national systems, including common tendering processes for biometric applications to promote economies of scale
- (iii) reviewing legal and privacy issues associated with biometric applications
- (iv) improving linkages to international biometric standard setting processes, and
- (v) publishing the above materials under the title of an Australian Government Biometric Framework, to be hosted by AGIMO on its public website (for public material) and on Govdex (for secure material).