SECURITY STANDARDS FOR PROOF-OF-IDENTITY DOCUMENTS

IDENTITY SECURITY

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[1] across consumer agencies. Document issuing agencies must acquire expertise essential to conduct third-line and electronic examinations.

[1] See Table (a) *Document Security Categories and Features* for definitions.

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.[2] 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 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

[2] *Biometrics Deployment of Machine Readable Travel Documents*. ICAO Document 9303, 2004

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**
Covert	• Security fibre paper or polymer/plastic card equivalent • Hidden image • Screen angle modulation • Security ink • Security threads	• Security fibre paper or polymer/plastic card equivalent • Hidden image • Screen angle modulation • Security ink	• Security fibre paper or polymer/plastic card equivalent • Screen angle modulation
Semi-covert	• High resolution printing processes • Security-type printing features	• High resolution printing processes • Security-type printing features	• High resolution printing process • Security-type printing feature
Overt	• Bearer's signature • Diffractive optically variable device (DOVD) • Digital facial image • Embossing • See-through register • Shadow/secondary image • Unique identifier • Watermark or polymer/plastic card equivalent	• Bearer's signature • Diffractive optically variable device (DOVD) • Digital facial image • Embossing • See-through register • Shadow/secondary image • Unique identifier • Watermark or polymer/plastic card equivalent	• Embossing • Optically variable ink • See-through register • Shadow/secondary image • Unique identifier • Watermark or polymer/plastic card equivalent
Integrated circuit	• Contact or contactless integrated circuit containing JPEG facial image, Public Key Infrastructure (PKI) and Basic Access Control (BAC)		

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.

	Features	**Recommended minimum features**
Covert	• Hidden image • Paper documents : Security fibres • Paper documents : Security threads • Plastic cards : Fluorescent printed areas embedded on card surface • Screen angle modulation • Security ink	Include two security inks including at least one taggant ink Include security fibre or security threads in paper documents Include two other 'covert' features
Semi-covert	• High resolution printing processes	Include at least three printing processes as detailed in the Security Features glossary[3]
	• Guilloche pattern • Latent image • Microprinting	Include all three of these printing features. Other additional printing features are also available for inclusion (see Security features glossary)
Overt	• Bearer's signature • Digital facial image • Embossing • Diffractive OVD (DOVD) • Paper documents : Watermark • Plastic cards : Watermark equivalent • See-through register • Shadow/secondary image • Unique identifier	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
Integrated circuit	• Contact or contactless integrated circuit containing JPEG facial image, including Public key infrastructure (PKI) and Basic access control (BAC)	Include an integrated circuit which incorporates a JPEG facial image

[3] 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.

	Features	Recommended minimum features
Covert	• Security ink • Screen angle modulation • Paper documents : Security fibre paper • Plastic cards : Fluorescent printed areas embedded on the card surface • Hidden image	Include one security ink Include at least two other 'covert' features
Semi-covert	• High resolution printing processes	Include at least two printing processes as detailed in the Security Features glossary
	• Micro printing • Guilloche pattern • Latent image	Include two of these printing features. Other additional printing features are also available for inclusion (see Security features glossary)
Overt	• Bearer's signature • Digital facial image • Embossing • Diffractive OVD (DOVD) • Paper documents: Watermark • Plastic cards: Watermark equivalent • See-through register • Shadow/secondary image • Unique identifier	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.

	Features	Recommended minimum features
Covert	• Hidden image • Paper documents : Security fibre paper • Plastic cards : Fluorescent printed areas embedded on card surface • Screen angle modulation	Include at least two 'covert' features
Semi-covert	• High resolution printing processes	Include at least one printing process as detailed in the Security Features glossary
	• Guilloche pattern • Latent image • Micro printing	Include at least one of these printing features. Other additional security printing features are also available for inclusion (see Security Features glossary)
Overt	• Embossing • Optically variable ink • Paper documents: Watermark • Plastic cards: Watermark equivalent • See-through register • Shadow image • Unique identifier	Include a unique identifier Include embossing Include at least one other 'overt' feature