



Australian Government

Department of Finance and Deregulation

Australian Government Information Management Office

Identity Management for Australian Government Employees Framework (IMAGE)

April 2008

Version 1.0

Department of Finance and Deregulation

Australian Government Information Management Office

© Commonwealth of Australia 2008

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>

Contents

| | | |
|-------|--|----|
| 1 | Introduction | 1 |
| 1.1 | What is IMAGE? | 1 |
| 1.2 | Principles | 2 |
| 1.3 | Benefits | 3 |
| 1.4 | Governance and management | 3 |
| 1.5 | Issuance of IMAGE compliant credentials | 4 |
| 2 | Employee and Contractor Identity Data Management | 5 |
| 3 | Registration Process for Employment | 7 |
| 3.1 | Evidence of identity check | 7 |
| 3.2 | Police records check and character check | 7 |
| 4 | Common Credential | 9 |
| 4.1 | Physical card requirements | 10 |
| 4.1.1 | Standards | 10 |
| 4.1.2 | Printed material | 10 |
| 4.1.3 | Tamper proofing and resistance | 11 |
| 4.2 | Physical characteristics and durability | 12 |
| 4.3 | Visual card characteristics | 13 |
| 4.4 | Required IMAGE compliant card elements | 15 |
| 4.4.1 | Restrictions | 15 |
| 4.4.2 | Front of the IMAGE compliant card | 15 |
| 4.4.3 | Back of the IMAGE compliant card | 25 |
| 4.5 | Optional IMAGE compliant card elements | 26 |
| 4.5.1 | Front of the IMAGE compliant card | 27 |

| | | |
|-------|--|----|
| 4.5.2 | Back of the IMAGE compliant card | 27 |
| 4.5.3 | Card design guidance | 28 |
| 5 | Visitor Credentials | 29 |
| | Glossary | 30 |
| | Annotated References | 32 |
| | Information Privacy Principles | 36 |
| | Principles for Gold Standard Enrolment | 42 |

1 Introduction

Identity management within the Australian Public Service is essential for trust between government agencies with regard to the authentication of their employees¹. Government agencies are responsible for establishing and managing the identity life cycles of their employees. Identity management enables agencies to ensure that issues such as employee authentication, provision of physical and logical access, data protection, data security, employee data sharing, and privacy are addressed in order for agencies to deliver trustworthy services to the Australian community.

The Identity Management for Australian Government Employees (IMAGE) Framework, established in 2006, is designed to achieve standardisation and transparency in the policies and practices relating to staff identity and identity management across the Australian Government. The implementation of the IMAGE Framework, including design specifications for a staff card, will assist government agencies to

- implement uniform authentication of its employees,
- establish standardised identity management practices, and
- implement a whole of government staff card for identification, and physical and logical access.

Establishing rigorous, consistent and transparent identity management practices across agencies for all employees will encourage trust between government agencies, and also between government agencies and the Australian community. Other benefits including cost savings and efficiency gains through more streamlined processes, which improved identity management processes will facilitate.

IMAGE is consistent with both the connected government² philosophy and the devolved management accountability under the *Financial Management and Accountability Act 1997* and the *Public Service Act 1999*.

1.1 What is IMAGE?

IMAGE is an Australian Government initiative to achieve standardisation in employee identification and identity management. The aim is to promote trust between government agencies in staff identification processes employed by each government agency. IMAGE was developed in consultation with Australian Government agencies, under the auspices of the Secretaries Committee on Information and Communication Technology (SCICT), the Business Process Transformation Committee (BPTC), the Chief Information Officers' Committee (CIOC) and its Authentication Working Group (AWG).

¹ Employees for the purposes of IMAGE, refers to ongoing employees, non-ongoing employees and contractors

² <http://www.connected.gov.au/>

IMAGE is based on a standardised set of business processes for identity management and the issue of secure credentials for physical and logical access. The IMAGE Framework highlights the critical issues for agencies to address when managing identity and access for employees.

IMAGE should be implemented in conjunction with the requirements specified in the following government publications:

- Protective Security Manual (PSM)
- Australian Government Information and Communications Technology Security Manual (ACSI 33)
- Australian Government e-Authentication Framework (AGAF)
- National Smartcard Framework
- National Identity Security Strategy (NISS)

It is recommended that Australian Government agencies align with the IMAGE Framework when reviewing or upgrading their identification or access systems.

1.2 Principles

IMAGE requires agencies to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes the following levels of identity assurance based on the principles from the Australian Government e-Authentication Framework (AGAF) for Business:

- **Transparency** – implement policies and practices in an open and understandable manner
- **Risk management** – conduct a risk assessment of the authentication processes in place and map identified risks to the applicable assurance level
- **Consistency** – promote a consistent set of requirements to facilitate management and movement of employees across the Australian Government
- **Trust and confidence** – promote consistent application of existing government policies and procedures
- **Privacy** – comply with the Information Privacy Principles under the *Privacy Act 1988*
- **Cost-effectiveness** – standardise and streamline relevant administrative processes and produce economies of scale for an identification and access token

1.3 Benefits

IMAGE is expected to deliver the following benefits in the longer term:

- Potential cost savings through more streamlined processes and management of identities of employees in one or more system.
- Efficiency gains through reducing the paperwork burden on employees and agencies.
- Better management of trusted identities across the Australian Government.
- Increased acceptance of established identity data by developing a relationship of trust through the use of common credentials.
- Improved confidence in the identity and character of employees throughout the APS, and subsequently improved trust in the services delivered to the Australian community.

1.4 Governance and management

IMAGE has been developed around existing Australian Government policies. As an Australian Government initiative, it falls under the governance arrangements of the Secretaries Committee on ICT (SCICT) and its subordinate committees:

- Chief Information Officers Committee (CIOC)
- Business Process Transfer Committee (BPTC)

Strategic issues will be dealt with by the SCICT, business process issues will be referred to the BPTC and technical issues referred to the CIOC.

The Department of Finance and Deregulation (Finance), through AGIMO (Australian Government Information Management Office), will work with the Australian Public Service Commission (APSC) and the Protective Security Coordination Centre (PSCC) to ensure that IMAGE continues to accurately reflect the PSM and the *Public Service Act 1999*, as well as any changes to the applicable legislation and regulatory environment³.

IMAGE is intended to be a dynamic framework, capable of amendment as necessary to ensure it remains relevant. Finance, through the Authentication Working Group (AWG) will review IMAGE on an annual basis.

Proposals to amend the Framework are welcomed and should be forwarded to the Government Authentication Team at image@finance.gov.au.

³ Introduction of IMAGE does not impact upon an agency's requirement to comply with other relevant legislation relating to employment in the Australian Government.

1.5 Issuance of IMAGE compliant credentials

An important goal of IMAGE is for agencies to eventually implement a common government employee credential. This credential would be in accordance with the design specifications of IMAGE, and in line with relevant government policy for proof of identity, security, and identity data management. This framework provides agencies with a procedure for reaching this goal.

The IMAGE compliant card is the physical staff identification credential that allows an employee to identify themselves as an Australian Government employee or contractor and, depending on individual roles and permissions, access buildings and systems within an agency. Verification of an individual's identity and completion of a character check are fundamental components of identity management within IMAGE. These are the foundations upon which physical and logical access and control systems are established.

An IMAGE compliant card is issued to an individual for the following reasons:

- the recruitment of an individual to the APS;
- the physical movement of an employee, whether ongoing or non-ongoing, from one agency to another;
- the hiring of a contractor to an agency within the APS.

The card must be de-registered when the following occurs:

- the retirement of an employee
- extended leave taken by an employee
- the termination of an employee's employment
- the death of an employee or contractor
- the expiry of a contractor's contract
- the termination of a contractor's contract
- the suspension of an employee or contractor whom is under investigation

Where there is a machinery of government change that involves the movement of employees either between Australian Public Service (APS) agencies, or into or out of the APS, the Public Service Commissioner's powers to move employees under s.72 of the Public Service Act 1999 will not be affected by agencies' policies on the adoption of IMAGE.

2 Employee and Contractor Identity Data Management

This section provides guidance to Australian Government agencies on managing employee identity data within and between agencies. Identity management under the IMAGE Framework is the management of the identity life cycle of an employee. This document refers to minimum requirements for acceptable data management policy and practice, and directs agencies to appropriate government legislation and policy when creating, storing, transferring, protecting and managing employee and contractor personal information in systems, directories or applications of Australian Government agencies.

To access further information detailing these minimum requirements, agencies should refer to the following publications.

- *The Privacy Act 1988* (Cth) – Australian Government agencies are required to deal with personal information in accordance with the *Privacy Act*, in particular the Information Privacy Principles (IPPs)⁴. The IPPs are set out in Section 14 of the *Privacy Act* and direct how Australian Government agencies should collect, use, disclose and store personal information. The *Privacy Act* also obliges Australian Government agencies to require contracted service providers to act in accordance with the IPPs. Further information about the IPPs can be obtained from your agency Privacy Contact Officer or at the website of the Office of the Privacy Commissioner⁵.
- Protective Security Manual (PSM) – The PSM details the minimum standards for the protection of Australian Government resources (including information, personnel and assets) that agencies must meet in their operations. It provides guidance for developing and maintaining an appropriate security environment in agencies through sound risk management principles.
- Australian Government Information and Communications Technology Security Manual (ACSI 33) – The PSM requires agencies to comply with ACSI 33 for the protection of information held on government information and communications technology (ICT) systems. This manual provides guidance to government agencies for the effective security of their ICT systems, including information pertaining to individuals.
- *The Archives Act 1983* – Under the *Archives Act 1983*, Commonwealth records must not be destroyed or otherwise disposed of unless authorised disposal arrangements are in place.

This Framework should be used in conjunction with the recordkeeping policies and standards promulgated by the National Archives of Australia⁶ and in accordance with legislative and regulatory requirements surrounding data storage, privacy, employment and contracting in the APS. Agency Records Managers should be consulted for advice

⁴ The IPPs are reproduced in Attachment C

⁵ <http://www.privacy.gov.au>

⁶ See the *Recordkeeping* section of the National Archives of Australia's website at <http://www.naa.gov.au/recordkeeping/default.html> for more information

on creating, keeping, and managing records within a specific agency. IMAGE recordkeeping systems should not operate in isolation from an agency's existing recordkeeping policy environment or from its information management strategic framework.

The benefits of the IMAGE framework will be more readily demonstrated where agencies

- adopt employee identity data management policies and procedures across government to help build trust,
- handle employee identity data in a consistent and secure way to enable easier and more efficient exchange and processing of employee identity data, and
- prevent function creep in the use of employee data.

Agencies that adopt these requirements as a minimum will help facilitate government-wide mobility of employee identity data and information.

For government agencies implementing IMAGE, the agency's associated policies and procedures must detail how the agency will

- collect employee identity data
- store and archive employee identity data (electronic and non-electronic)
- dispose of employee identity data
- access employee identity data
- transfer employee identity data (electronic and non-electronic), and
- protect personal privacy.

These will encourage better practice in data management and at the same time enable greater trust and mobility of information within and between agencies. They have been designed to help agencies consider all aspects of employee identity data management and develop appropriate policies and practices. Agencies may of course choose to further enhance the effectiveness of their data management practices by implementing additional processes.

In accordance with advice from the Office of the Privacy Commissioner, agencies should ensure there is a Privacy Contact Officer within the organisation and appropriate resources are supplied to him or her.

All agencies should conduct a privacy impact assessment when planning any implementation of IMAGE.

3 Registration Process for Employment

Registration is the process by which an employee is issued with a credential. In almost all cases, the employee will be required to present proof of identity documentation at the initial registration process.

The initial registration process adopted by government agencies should ideally include both an evidence of identity check and character, including police records, check.

3.1 Evidence of identity check

IMAGE recommends that agencies comply with the Principles set out in the Gold Standard Enrolment Framework (GSEF) in order to achieve uniformity in recruitment processes across the Australian government.

The GSEF, developed by the Attorney General's Department as part of the National Identity Security Strategy⁷, focuses primarily on ensuring that applicants for Government documents that also function as high integrity proof of identity documents are subject to a rigorous process of identification and verification. The GSEF incorporates rigour in both the documents used to establish identity and in the process by which a new credential is issued (i.e. a face-to-face process).

The GSEF comprises of a set of Principles and provides a comprehensive approach to the establishment of identity of individuals. Attachment A to the GSEF provides a 'Proof of Identity Framework' outlining the appropriate proof of identity credentials an agency could accept⁸.

3.2 Police records check and character check

Agencies should comply with the minimum requirements for conducting character and police records in accordance with the *Public Service Act 1999*. The *Public Service Act* provides that suitability requirements and conditions of engagement must be met before a person is unconditionally appointed to the APS. These conditions may include security and character checks (subsection 22(6)). For agencies conducting security clearances for their employees, they may choose to conduct a more rigorous process than outlined in the PSM depending on their business requirements.

⁷ The Report to the Council of Australian Governments on the elements of the National Identity Security Strategy can be found at http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_ReporttotheCouncilofAustralianGovernmentsontheelementsoftheNationalIdentitySecurityStrategy-April2007

⁸ Attachment D of this document outlines the Principles contained in the GSEF.

As part of an Australian Government employee's engagement with a new agency, the employee is asked to provide the agency with written consent to conduct a police records check. Once consent is granted, the Australian Federal Police (AFP), through CrimTrac, will conduct a police records check on the individual based on the information supplied during the application stage of the GSEF. The AFP will send the results of the police records check directly to the issuing agency.

All agencies should ensure their clearance policies and assessment criteria are published on agency websites. This will assist agencies that are gaining or providing access to an employee from another agency to determine the adequacy of the policies and processes of the departed/home agency relative to their own requirements. Where parity of procedure is determined, agencies may decide to rely upon police records checks conducted by departed/home agencies. Alternatively, where agencies are unable to satisfy themselves as to parity of procedure, new checks may be initiated.

Agencies should ensure that their policies and procedures in relation to police records checks and character checks adhere to:

- anti-discrimination law⁹
- the *Public Service Act 1999*
- the *Public Service Commissioner's Directions 1999*, and
- the *Privacy Act 1988*, in particular the Information Privacy Principles.

⁹ For more information, see the Human Rights and Equal Employment Opportunity Commission (HREOC) Discussion Paper on Discrimination in Employment on the Basis of Criminal Record at http://www.humanrights.gov.au/human_rights/criminalrecord/discussion.html#toc5

4 Common Credential

This section sets out the baseline design specifications for an IMAGE compliant employee identification card, which also accommodates agency-specific requirements.

The baseline design specifications of the IMAGE compliant card include some of its physical characteristics, such as its dimensions (width and height), thickness, and aspects of its general appearance. The physical appearance of the card should balance the need to have it recognised as an Australian Government employee identification card, while providing the flexibility to support individual agency requirements.

The use of commercially available card holders and carriers can provide flexibility for agencies to individualise their cards, rather than altering the common elements of the physical appearance of the card. For example, where agencies are required to protect the identity of their staff, the card sleeve or holder can be printed with opaque panels to obscure the full name of the employee from public view.

The objectives of the common credential are to

- ensure consistency in the appearance of Australian Government employee identification cards, and
- improve the level of confidence in employee and contractor identity information across the Australian Public Service.

4.1 Physical card requirements

References to the IMAGE compliant card in this section pertain to the physical characteristics only. References to the front of the card apply to that side of the card that contains the electronic contacts.

4.1.1 Standards

Compliance with applicable International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards is required. The IMAGE compliant card must also comply with the physical characteristics described in ISO 7810¹⁰, ISO 10373¹¹, ISO 7816¹² for contact cards, and ISO 14443¹³ for contactless cards. These open standards are established so independent implementations based on them should be interoperable. Additionally, where testing for card durability, the standards specified in ANSI 322¹⁴ must be satisfied.

4.1.2 Printed material

The printed material must not rub off during the life of the IMAGE compliant card. Printed material must not interfere with the contact and contactless integrated chip cards (ICCs) and related components, or obstruct access to machine-readable information.

Printing methods

An agency can choose from several commonly accepted printing methods to personalise IMAGE compliant cards. Such methods include standard dye-sublimation printing, reverse dye printing, thermal transfer printing, and laser etching. The printing method selected will determine the quality and durability of the end product. Tradeoffs can include production costs and levels of maintenance and support. Various vendors offer different models of printers. ID card printers can vary in cost, quality, and capability.

¹⁰ ISO/IEC 7810 is the international standard for physical characteristics of identification cards.

¹¹ ISO 10373-6 is the international standard for test methods for proximity identification cards.

¹² ISO 7816-3 is the international standard for electronic signals and transmission protocols of IC cards with contacts. It defines the characteristics of the signals used to communicate with a smartcard.

¹³ ISO 14443 is the international standard for contactless smartcards operating at 13.56 MHz in close proximity with a reader antenna; it sets communications standards and transmission protocols between card and reader to create interoperability for contactless smartcard products.

¹⁴ ANSI 322 is the American National Standards Institute's standard for card durability test methods.

Lifespan

The IMAGE compliant card should be valid for no more than 5 years. Every card will experience normal wear and tear associated with usage. It is estimated that, with normal usage, the useful life of a new card is 3–5 years. It is to be expected that a certain percentage of cards will need to be replaced before their normal end-of-life. Additionally, cardholders will use their cards with different frequencies; the more frequently a card is used, the more likely it is to wear out. Agencies should inform and educate cardholders on the proper use and storage of their cards. This will reduce replacement costs due to re-issuance of cards before their normal end-of-life.

For agencies requiring digital signature certificate storage on the IMAGE compliant card, end-of-life for keys and certificates should pose no problem. Public Key Infrastructure (PKI) keys and certificates can be revoked, and new keys and certificates installed on the card independent of card lifespan.

Agencies should ensure that the card life is not shorter than the life of the digital certificate installed on the card, as card replacement will necessitate revocation and reissue of keys and certificates, thus resulting in increased costs.

4.1.3 Tamper proofing and resistance

For the purpose of this Framework, a tamper-evident security feature must be incorporated into the card body to reduce risks associated with counterfeiting, tampering and to provide visual evidence of attempts to tamper with an IMAGE compliant card. Tamper-evident security features can be incorporated into the IMAGE compliant card either by printing or by incorporation into the card laminate.

Agencies are strongly encouraged to review their requirements and incorporate appropriate security features commensurate with identified threats and risks. Examples of security features include:

- optical varying structures
- optical varying inks
- laser etching and engraving
- holograms
- holographic images
- watermarks.

One security feature commonly implemented on identity cards is a hologram. Holograms are either generic, meaning the image is non-specific and therefore available to the general public; or customised, meaning the image is of something specific, such as a corporate or agency logo. Custom holographic images are often registered or trademarked to deter unauthorised use. Customised holograms can be more expensive to produce, and the lead times for graphic design may be longer; but they can provide a greater level of security than generic holograms.

All tamper-evident and anti-counterfeiting methods must comply with the following requirements.

- The security features are implemented in accordance with durability requirements specified in ISO/IEC 7810.
- The security features are free from defects.
- The security features do not obscure printed information on the IMAGE compliant card.
- The security features do not impede access to machine-readable information on the IMAGE compliant card.

Agencies should work closely with their card vendors and systems integrators to evaluate which security methods are most suitable. Agencies may also want to consider a combination of security features to achieve a higher level of confidence in the IMAGE compliant card.

4.2 Physical characteristics and durability

The physical characteristics and requirements of the IMAGE compliant card are listed below.

- The card may carry a contact and a contactless ICC interface. As many agencies will have business imperatives that dictate use of alternative access and authorisation mechanisms may have existing access and authorisation legacy systems that need to be accommodated in the short term, it is not mandatory that agencies use the ICC capability for their specific access and authorisation requirements. However this functionality is considered desirable in the longer term, and economies of scale will dictate a lower per-unit cost for a common card across the whole of government.
- The card body structure must consist of card material(s) that satisfy the card characteristics in ISO 7810 and the test methods in ANSI 322. Although the ANSI 322 test methods do not currently specify compliance requirements, the tests will be used to evaluate card material durability and performance.
- The card will be 685.8 to 838.2 micrometers thick (before lamination).
- The card will not be embossed.
- Decals must not be adhered to the card.
- The card must be worn without physically altering it by using various commercially available card holders and carriers.
- The card material must be able to withstand the effects of the temperatures required to apply a polyester laminate on one or both sides of the card by commercial off-the-shelf (COTS) equipment. The thickness added due to a laminate layer must not interfere with the smart card reader operation. The card material will allow production of a flat card after lamination of one or both sides of the card.

4.3 Visual card characteristics

The primary colour for the background of the front of the IMAGE compliant card will be white. The information on an IMAGE compliant card will be in visual printed and electronic form. This section covers placement of visual printed information; not information stored in electronic form, such as stored data elements, and other possible machine-readable technologies.

To achieve a common appearance yet provide agencies with flexibility to augment the card with agency-specific requirements, the card will contain required and optional printed information. Required and optional items will generally be placed as described and depicted. Printed data must not interfere with machine-readable technology.

An IMAGE compliant card will require inclusion of certain elements on both the front and the back of the card. These elements are identified by zone. Table 1 and Table 2 list the required and optional zones on the front and back of the IMAGE compliant card. The requirements for each element are described in the following sections.

| Required (Y/N) portrait | Required (Y/N) landscape | Zone | Description | Data format |
|-------------------------|--------------------------|------|----------------------------|---|
| Y | Y | 1 | Photograph | Minimum 300 dpi Dimensions (including border) 0.75 ratio: <ul style="list-style-type: none"> ▪ 33 x 44mm (minimum) ▪ 37.5 x 50mm (maximum; landscape only) |
| N | N | 2 | Photo border | Black, maximum 1mm thickness |
| N | N | 3 | OVD Foil | Dimensions: 15 x 15mm |
| N | N | 4 | Agency-specific zone | Agency discretion; however if an employee's surname is not printed in Zone 6, Zone 4 must be used for this purpose |
| N | N | 5 | Employee status (colour) | Agency discretion for colour and layout (border or base strip) |
| N | N | 5 | Contractor status (colour) | Blue (PMS 292) must be used to identify contractors Agency discretion for layout (border or base strip) |
| Y | Y | 6 | Employee/Contractor name | Agency options for layout |
| N | N | 7 | Agency-specific zone | Agency discretion |

| Required (Y/N) portrait | Required (Y/N) landscape | Zone | Description | Data format |
|-------------------------|--------------------------|------|---------------------------|--|
| Y | Y | 8 | Commonwealth Coat of Arms | Conventional 3A solid design Dimensions: <ul style="list-style-type: none"> 15mm wide (portrait) 20mm wide (landscape) |
| N/A | N | 9 | Agency-specific zone | Agency discretion |
| N/A | N | 10 | Agency-specific zone | Agency discretion |
| Y | Y | | Expiration date | A required element, must feature in an agency-specific zone. |

Table 1. IMAGE compliant card physical elements (card front)

| Required (Y/N) | Zone | Description | Data format |
|----------------|------|------------------------------|--|
| Y | 1 | Australian Government Design | In-line strip design Minimum Dimensions: Maximum Dimensions: 82 mm long Permitted branding options: <ul style="list-style-type: none"> Australian Government logo Australian Government logo accompanied by Agency Name Australian Government logo accompanied by agency-specific approved co-branding |
| Y | 2 | Reserved space for ICC | |
| N | 3 | Agency-specific zone | Agency discretion |
| Y | 4 | Serial Number | Minimum 5 pt/Arial/normal font |
| N | 5 | Agency-specific text area | Return Address recommended |
| N | 6 | Agency-specific text area | Counterfeit, alter, or misuse warning recommended |

Table 2. IMAGE compliant card physical elements (card back)

Agencies should demonstrate an internally consistent approach to all agency-specific implemented elements. For example, an agency should choose either a portrait view card or a landscape view card for their IMAGE implementation, not a combination of both. Similarly contractor status should be denoted by either a coloured border or a coloured strip, not both.

4.4 Required IMAGE compliant card elements

There are seven required elements that should be printed on an IMAGE compliant card.

1. Commonwealth Coat of Arms (front of card)
2. Photograph of the IMAGE compliant card holder (front of card)
3. Full name of the IMAGE compliant card holder (front of card)
4. Employee or contractor status of the IMAGE compliant card holder (front of card)
5. Expiration date of the IMAGE compliant card (front of card)
6. Australian Government branding (back of card)
7. Agency issued Serial Number (back of card)

The requirements for each visual element are described below. The placement and formatting for each required element is shown in Figure 1 and Figure 2.

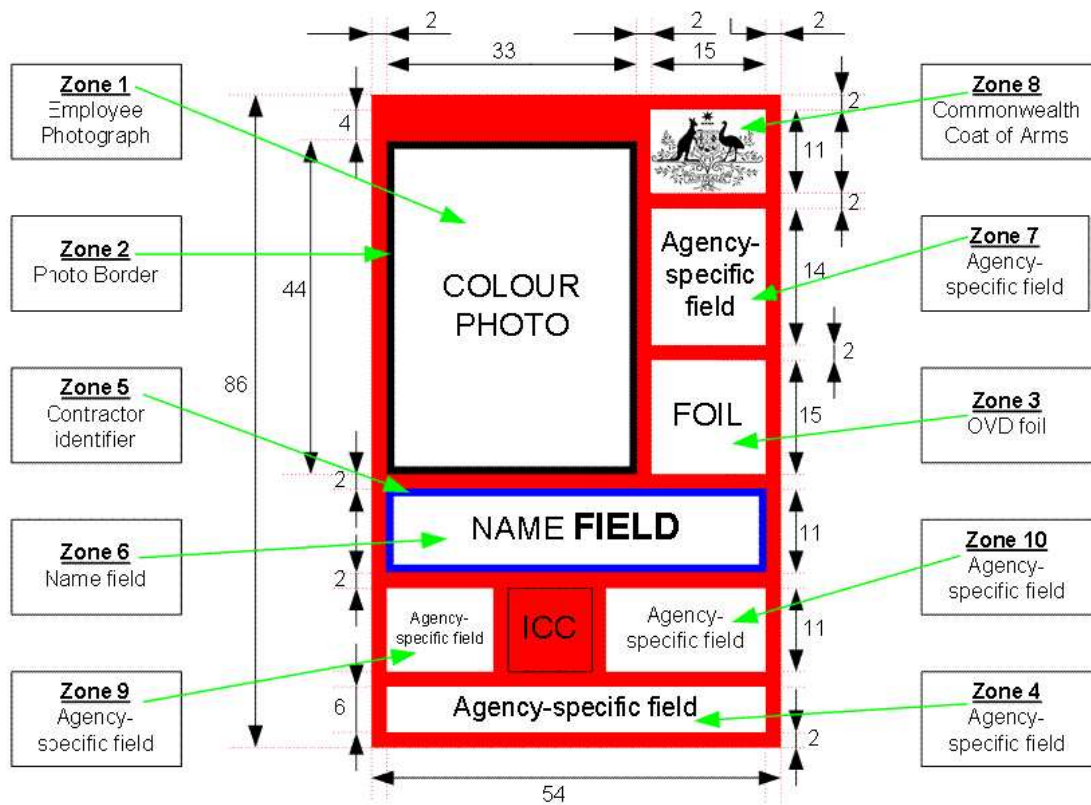
4.4.1 Restrictions

Areas marked “reserved” should not be used for printing. These are visually distinguishable in the following diagrams as the red shaded areas.

The terms “Australian Government” and/or an agency’s departmental or organisational name must not be printed on either face of the card except as part of the official Australian Government brand applied to the back of the card.

4.4.2 Front of the IMAGE compliant card

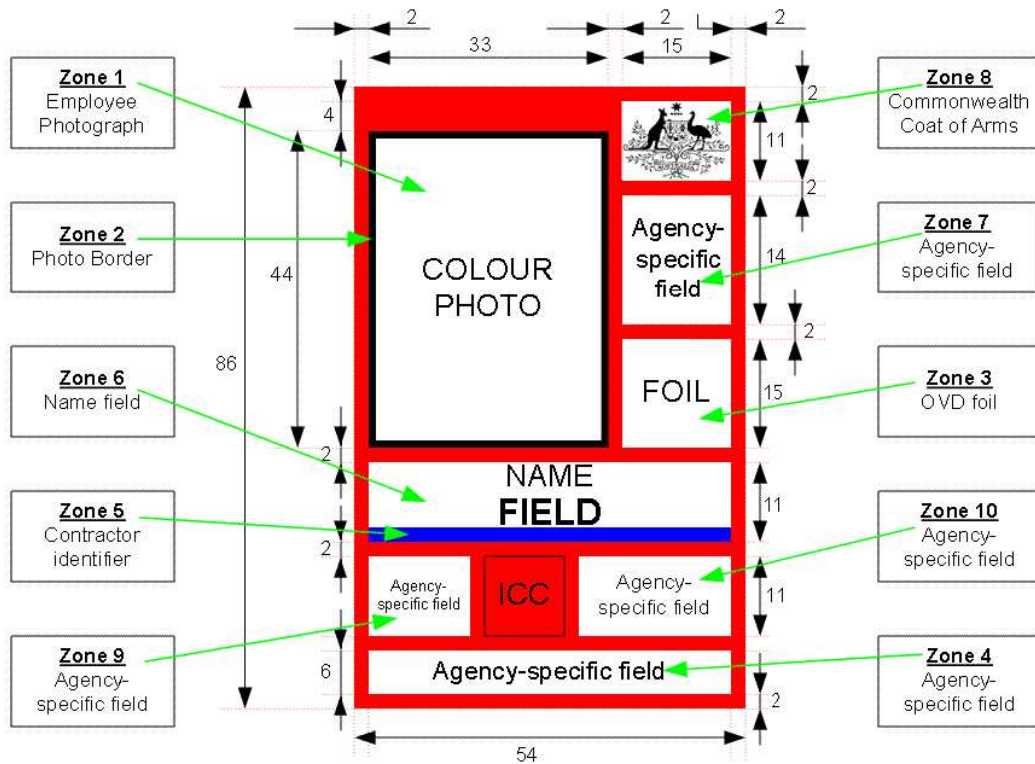
The following pages depict various design options for an IMAGE-compliant card.



Key: Reserved area. No printing is permitted in this area.

Notes: All measurements around the figure are in millimetres.
 All text is to be printed using Arial-font.
 Unless otherwise specified, the recommended font size is 5 pt normal weight for data labels (also referred to as tags) and 6 pt bold for actual data

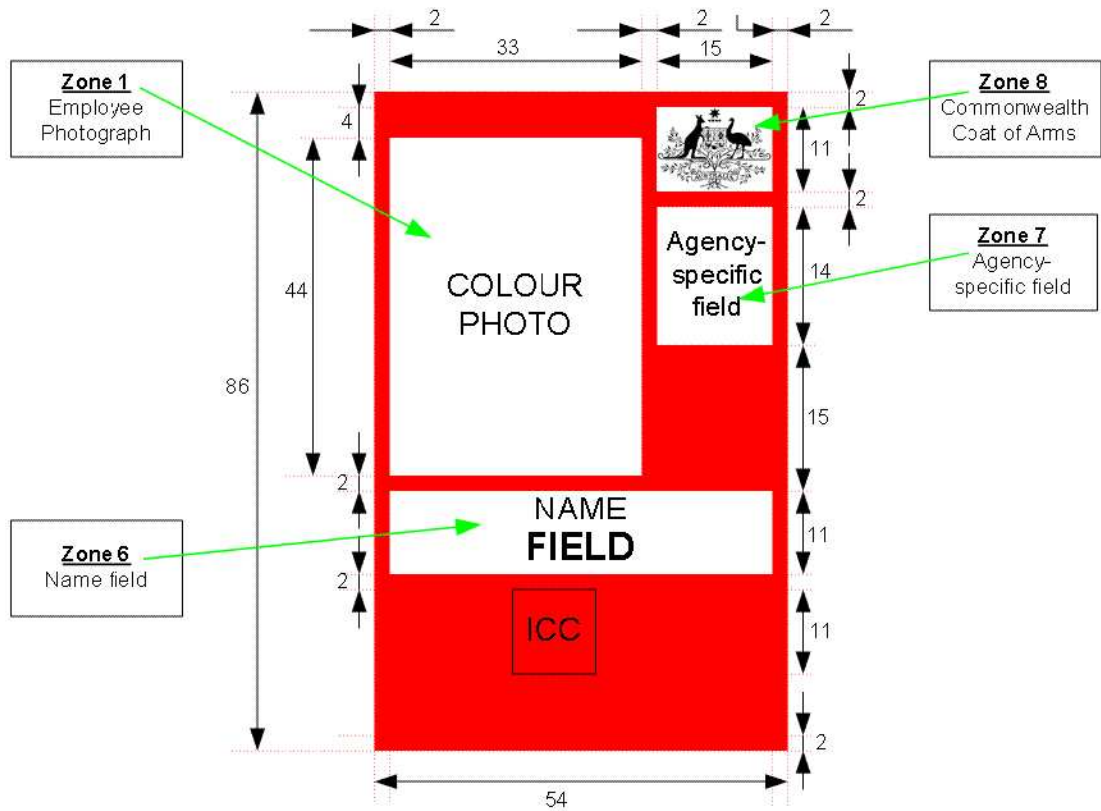
Figure 1. Card front – portrait view: printable areas, required and optional data




Key: Reserved area. No printing is permitted in this area.

Notes: All measurements around the figure are in millimetres.
 All text is to be printed using Arial-font.
 Unless otherwise specified, the recommended font size is 5 pt normal weight for data labels (also referred to as tags) and 6 pt bold for actual data.

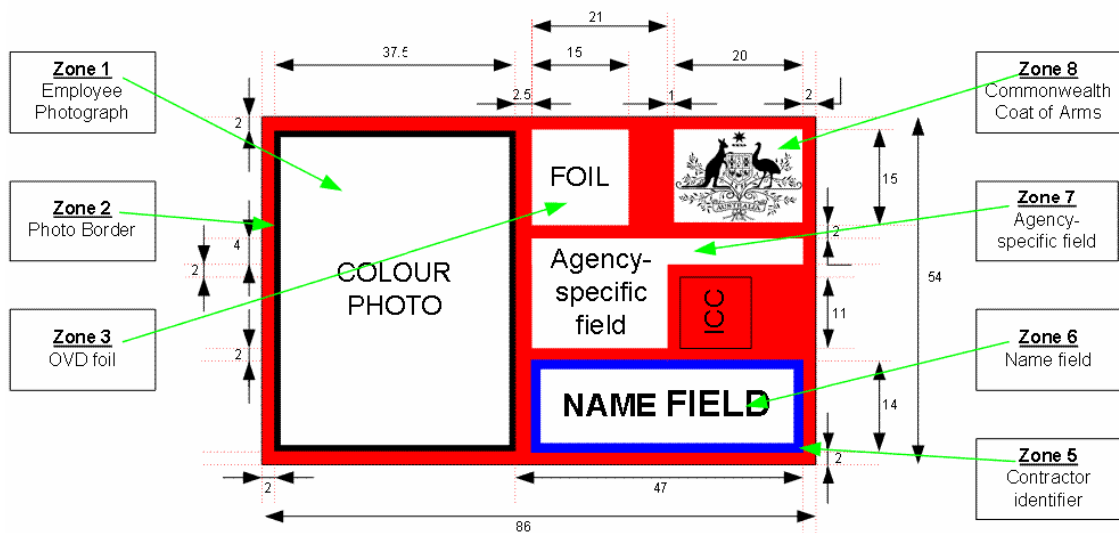
Figure 2. Card front – portrait view: printable areas, required and optional data



Key:  Reserved area. No printing is permitted in this area.

Notes: All measurements around the figure are in millimetres.
 All text is to be printed using Arial-font.
 Unless otherwise specified, the recommended font size is 5 pt normal weight for data labels (also referred to as tags) and 6 pt bold for actual data

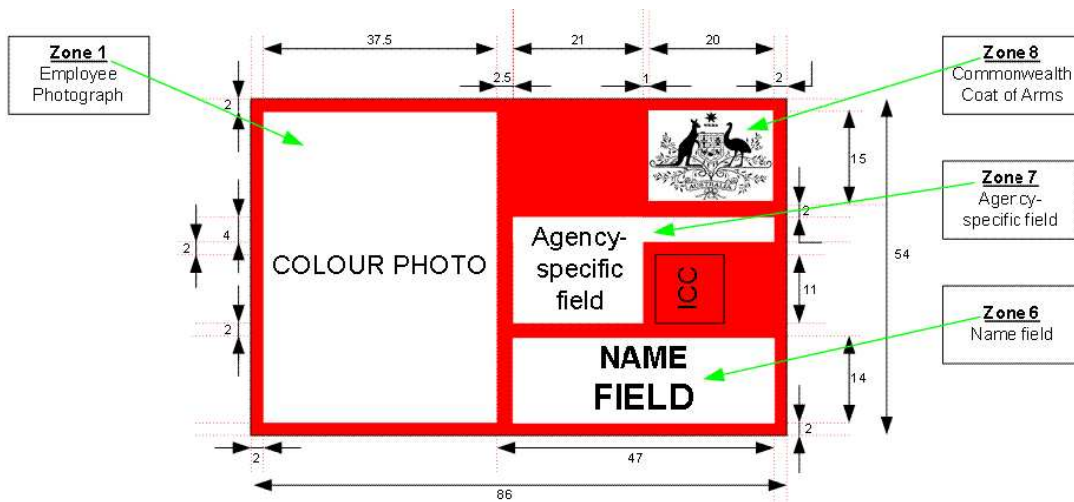
Figure 3. Card front – portrait view: printable areas, required and optional data




Key: Reserved area. No printing is permitted in this area.

Notes: All measurements around the figure are in millimetres.
 All text is to be printed using Arial-font.
 Unless otherwise specified, the recommended font size is 5 pt normal weight for data labels (also referred to as tags) and 6 pt bold for actual data

Figure 4. Card front –landscape view: printable areas, required and optional data



Key:  Reserved area. No printing is permitted in this area.

Notes: All measurements around the figure are in millimetres.
All text is to be printed using Arial-font.
Unless otherwise specified, the recommended font size is 5 pt normal weight for data labels (also referred to as tags) and 8 pt bold for actual data

Figure 5. Card front –landscape view: printable areas, required and optional data

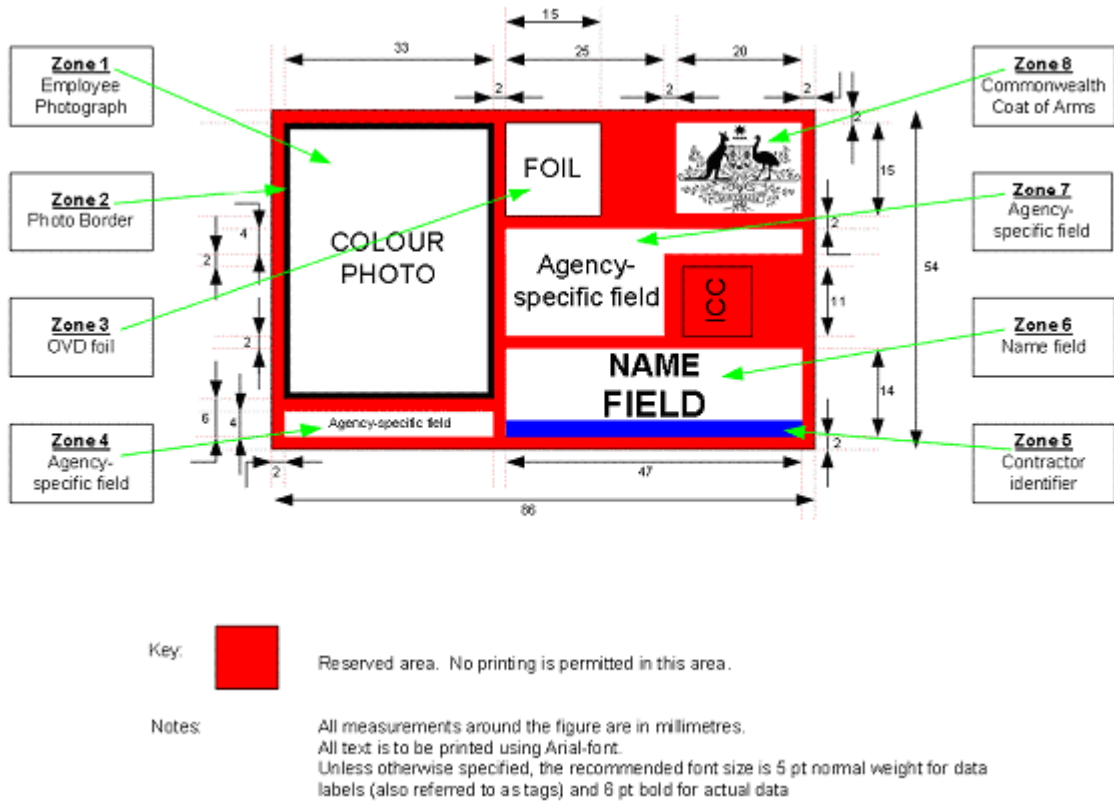
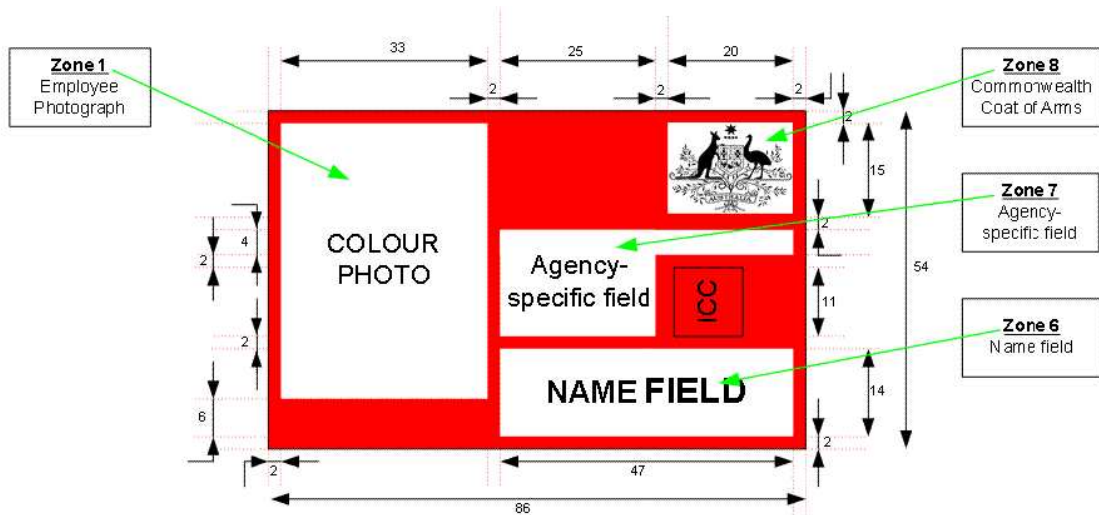


Figure 6. Card front –landscape view: printable areas, required and optional data



Key: Reserved area. No printing is permitted in this area.

Notes: All measurements around the figure are in millimetres.
 All text is to be printed using Arial-font.
 Unless otherwise specified, the recommended font size is 5 pt normal weight for data labels (also referred to as tags) and 6 pt bold for actual data

Figure 7. Card front –landscape view: printable areas, required and optional data

Zone 1 – Photograph

A photograph of the person to whom the card has been issued should be placed in Zone 1 and be a full front-facing pose, from the top of the head to the shoulders. The resolution required for compliance is a minimum of 300 dpi and comply with the ICAO recommended specifications. The recommended dimensions are for a 0.75 aspect ratio (width divided by height). Portrait view cards are recommended to use dimensions of 33 x 44mm including a photo border. Landscape view cards are recommended to use dimensions of a minimum 44 x 33mm and maximum 37.5 x 50mm including photo border. The background for the photograph should follow recommendations in SP 800-76¹⁵.

Zone 6 – Name

The cardholder's first name (or pseudonym when applicable under law) should be printed in Zone 6 in as large as practicable Arial font. Agencies may scale font size down to cater for length of names. Bold font is recommended for surnames. Agencies may print names on one line or two. If two lines are used for printing, an employee's first name should be printed on the top line. Names may be written in any practicable combination of lower case and capital letters subject an internally consistent approach being adopted for all employees within an agency.

For portrait view cards, agencies may choose to print an employee or contractor's first name only in Zone 6. Where this option is chosen, agencies must print the employee or contractor's surname in Zone 4.

Zone 5 – Employee/ Contractor status

Employee / Contractor status is identified by a coloured border or strip, around or at the base of Zone 6. This border or strip is located in Zone 5. Blue (PMS 292) must be used to identify contractors in Australian Government agencies. White is preferred for identifying employees (i.e. the absence of a colour strip or border), however agencies have discretion in the use of colours to denote employee status. Agencies may determine the dimensions of Zone 5, provided that both consistency is maintained for all cards, and that no part of an employee or contractor's name is obscured.

Zone 4 – Agency-specific zone

This area is available at agency discretion. However, in cases where the cardholder's first name only is printed in Zone 6, Zone 4 must be used for the printing of the cardholder's surname. Surnames should be printed in bold in as large a font size as practicable.

¹⁵ National Institute of Standards and Technology 2006, Biometric Data Specification for Personal Identity Verification, Special Publication 800-76 – Information Security, US Department of Commerce. This publication describes technical acquisition and formatting specifications for the biometric credentials of the Personal Identity Verification system.

Zone 11 – Commonwealth Coat of Arms

The Commonwealth Coat of Arms must be located in Zone 8. The recommended design for use is the Conventional 3A Solid design. For portrait view cards, the dimensions for the Coat of Arms must be a minimum 15 mm wide; for landscape view cards the dimensions must be 20mm wide. A 2mm boundary surrounds the zone to prevent crowding of the Coat of Arms. Agencies should source a graphic of the Commonwealth Coat of Arms directly from the Department of Prime Minister and Cabinet.

Expiry Date

Agencies must include the date of card expiration on the front of the card. No specific zone is designated for the expiry date, however it should be in one of the provided 'agency-specific' zones (Zones 4, 7, 9 or 10¹⁶) Agencies may choose any practicable layout of the expiration date, e.g. ddmmyy; mmmyyyy.

¹⁶ Zones 9 and 10 are only available on portrait view cards

4.4.3 Back of the IMAGE compliant card

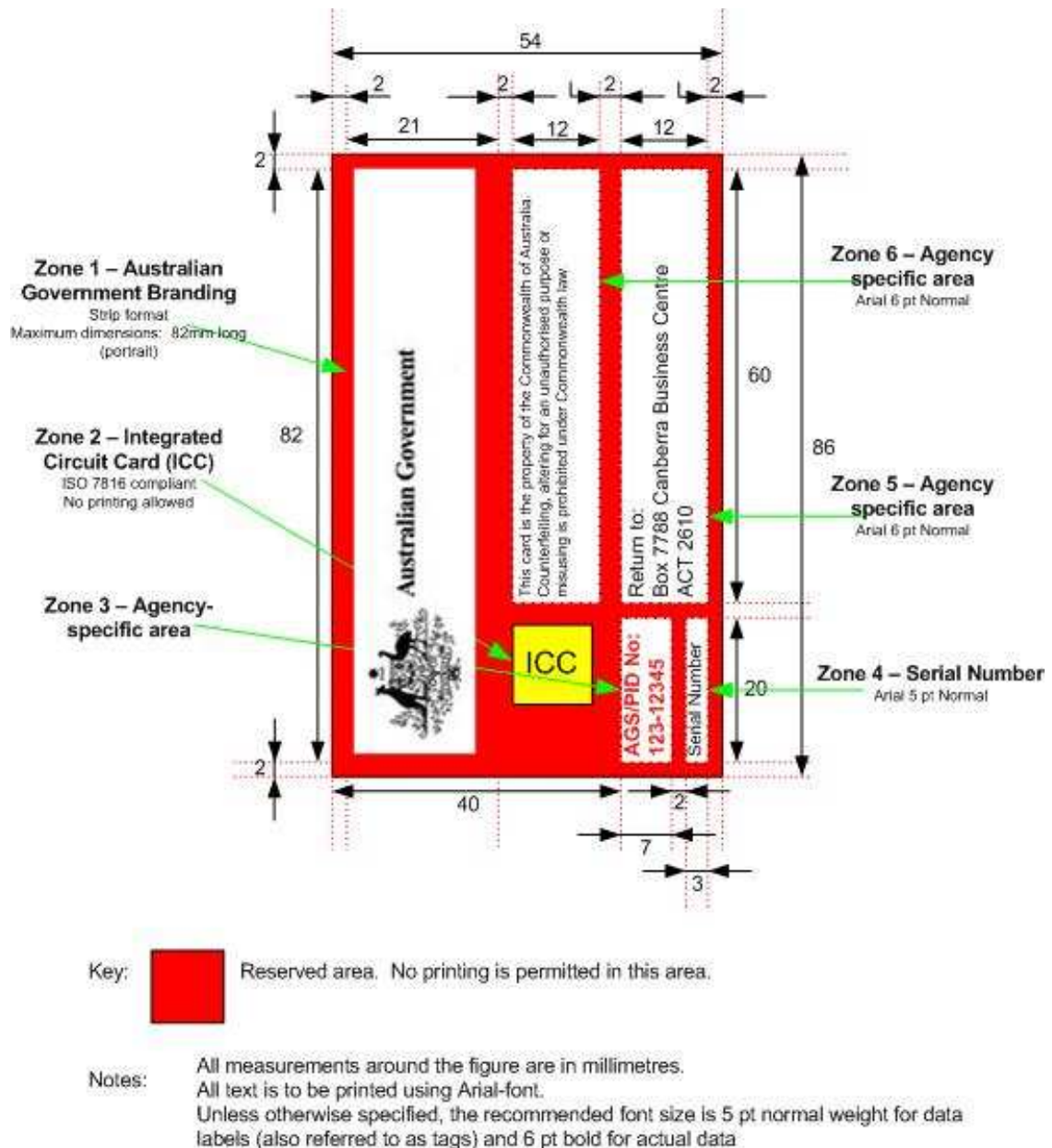


Figure 2. Card back – printable areas, required and optional data

Zone 1 – Australian Government design

Australian Government branding¹⁷ must be located in Zone 1 of the back of the card. Branding must be presented in the 'in-line strip' design. There are three permitted options.

1. Australian Government logo
2. Australian Government logo accompanied by Agency Name
3. Australian Government logo accompanied by agency-specific approved co-branding

Use of Australian Government branding must comply with the Design Guidelines, available on the Department of Prime Minister and Cabinet's website. The maximum dimension of this zone is 82mm wide (landscape view).

Zone 4– Agency issued Serial Number

A unique credential serial number should be printed on the card in this zone. The number should be formatted in accordance with individual agency requirements. Individual agencies should discuss with their card manufacturers when, in the card issuance process, the Australian Government Serial Number should be placed on the IMAGE compliant card. The dimensions of this zone are 20 x 3 mm.

4.5 Optional IMAGE compliant card elements

Several optional data elements can be implemented on both the front and back of an IMAGE compliant card. These optional elements allow individual agencies to tailor IMAGE compliant cards to meet their specific needs and provide additional security features. For example, optional card elements that can provide additional levels of assurance include the cardholder's signature, and the cardholder's physical characteristics (that is, height, weight, eye colour, hair colour).

Individual agencies may find it useful to identify what items are included on their current identity credentials and what items are currently recognisable to security personnel. Agencies can then decide what optional elements to implement. While each additional item placed on a card may make it more difficult for the card to be used illegally, agencies should note that card management also becomes more complex with each additional item placed on the card.

For the front of the card, zones 2, 3, 4, 7, 9 and 10¹⁸ are designated areas for optional card elements. For the back of the card, zones 3, 5 and 6 are designated areas for optional card elements.

¹⁷ Use of the Australian Government design must be in accordance with the Design Guidelines, released by the Department of Prime Minister and Cabinet. These guidelines are available at http://www.dpmc.gov.au/guidelines/docs/design_guidelines_PMC.pdf

4.5.1 Front of the IMAGE compliant card

Zone 2 – Photo border

Agencies may choose to surround the photograph of the employee with a black border of a maximum 1.0mm thickness. The border must not obscure the photograph of the employee in any way.

Zone 3 – Optical Variable Device (OVD) Foil/Security Device

An OVD foil may be applied to the card. The dimensions of this element must be 15 x 15 mm.

Zone 4 – Agency-specific zone

This area is available at agency discretion. However, in cases where the cardholder's first name only is printed in Zone 6, Zone 4 must be used for the printing of the cardholder's surname. Surnames are recommended to be printed in bold in as large a font size as practicable.

Zone 7 – Agency-specific zone

This area is available for use at agency discretion.

Zone 9 – Agency-specific zone

This area is available for use at agency discretion (for portrait view only).

Zone 10 – Agency-specific zone

This area is available for use at agency discretion (for portrait view only).

4.5.2 Back of the IMAGE compliant card

Zone 3 – Agency-specific text area

This area is optional for agency specific purposes. However, agencies may choose to print their employee's AGS number in this zone of the card. The dimensions of this space are 20 x 7 mm.

¹⁸ Zones 9 and 10 are only available to portrait view cards

Zone 5 – Agency-specific text area

This area is optional for agency specific purposes. However for those agencies that choose to include a return address on the card in cases of lost cards, this information must be printed in this zone. The dimensions of this zone are 60 x 12 mm.

Zone 6 – Agency-specific text area

This area is optional for agency specific purposes. However agencies may choose to print a message conveying that the card is the property of the Commonwealth agency and warning against counterfeiting, misuse or unauthorised alterations. For those agencies that print this warning, it must be located in this zone. The dimensions of this zone are 60 x 12 mm.

4.5.3 Card design guidance

Agencies implementing their own IMAGE cards should follow the following design guidance to ensure consistency of design while maintaining a unique agency IMAGE card:

- A 2mm perimeter around card edge should be maintained
- A minimum 2mm border should separate all zones **except Zones 2 and 5 (on the front of the card)**
- For the front of the card zones 4, 6, 7, 9, and 10, have no pre-determined measurements **provided** the 2mm border restrictions are maintained
- For the front of the card, portrait view, zones 3, 7 and 8 should always align to the left
- For the front of the card, landscape view, zones 3, 6 and 7 should always align to the left
- All text should be printed in Arial, unless otherwise specified in a minimum 6pt normal font

5 Visitor Credentials

IMAGE is not prescriptive in relation to Visitor Credentials and is sufficiently flexible to accommodate a range of agency business requirements. However, it is important that the physical appearance of agency Visitor Credentials are sufficiently different to the physical appearance prescribed for the IMAGE compliant card.

Accordingly, agencies should ensure Visitor Credentials are clearly marked with the name of the agency to make them agency specific, and to further minimise the potential for confusion with the IMAGE compliant card.

Glossary

| | |
|-------------------------------|--|
| ACSI 33 | Australian Government Information and Communications Technology Security Manual |
| character check ¹⁹ | The processes that enable an agency to ensure a prospective employee is a suitable person to be engaged as an APS employee, or for specific duties. The agency head can determine that checks should be made, for example, through a police records check, or an enquiry with any relevant professional licensing or registration board or another APS agency or other employer, to determine whether the person has a criminal conviction or criminal charges that are pending, an inquiry by a professional licensing or registration body is pending, and/or there have been any findings that the employee breached the APS Values or a misconduct investigation was pending at the time the person ceased employment. |
| contactless ICC module | Integrated circuitry embedded into a flat, plastic body that can be machine read over short distances without need for physical contact with a card reader. |
| contractor | An individual for whom a contract exists between the agency (or agencies) and themselves, directly; or a person who is employed as a contracted service provider to an agency (or agencies) via the organisation that employs or contracts them. |
| credential | A token that provides evidence of a person's right to confidence or authority. |
| embedded antenna | Antennas directly integrated into a credential. In most cases, this antenna is matched to the building access system and cannot be used in other applications. |
| employee | Australian Public Service employees |
| EOI | evidence of identity |
| ICC | integrated chip card – integrated circuitry embedded into a flat, plastic body |
| IEC | International Electrotechnical Commission |
| IMAGE Framework | Identity Management for Australian Government Employees Framework |
| IMAGE compliant card | Australian Government Staff Identification Credential |

¹⁹ *Conditions of engagement*, Australian Public Service Commission, 2005.

| | |
|------------------------------|--|
| information security | Protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability. |
| information system | A discrete set of information resources organised for collecting, processing, maintaining, using, sharing, disseminating, or disposing of information. |
| IPP | Information Privacy Principles, located in <i>The Privacy Act 1988</i> |
| ISO | International Organisation for Standardisation |
| machine-readable information | Information encoded in a form that can be scanned or sensed by a machine or computer and interpreted by hardware and/or software. |
| micrometer | 1/1000 of a millimetre |
| PDF | Portable Data File |
| PDF barcode | A sequence of vertical bars and spaces that can become a compressed, portable data file. |
| personal information | Any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, name, ethnicity, gender, home address, telephone number, physical description, education, medical/employment history, and/or financial matters. It includes statements made by, or attributed to, the individual. |
| PSM | Australian Government Protective Security Manual 2005 |

Annotated References

Administrative Functions Disposal Authority 2000, National Archives of Australia

The Administrative Functions Disposal Authority that authorises disposal of records, in whatever format, relating to common administrative functions carried out by most Commonwealth agencies. The Authority is issued in accordance with Section 24 of the Archives Act 1983. The Administrative Functions Disposal Authority can be found at http://www.naa.gov.au/Images/AFDA_tcm2-666.pdf

Archives Act 1983 (Cwth)

The Archives Act 1983 was in part established to prevent the unauthorised disposal (including destruction) of Commonwealth records and to provide provisions for public access to those Commonwealth records more than 30 years old. Information about the Archives Act 1983 and the National Archives of Australia's standards and guidelines for recordkeeping in the Commonwealth can be found at <http://www.naa.gov.au/records-management/index.aspx>

Australian Government e-Authentication Framework (AGAF)

The AGAF comprises a set of principles for e-authentication for the whole-of-government. It is based on four assurance levels that are matched to the risk associated with a transaction. The AGAF comprises two parts: the AGAF for Business and the AGAF for Individuals. There is a range of resources available on the AGIMO website to help implement the AGAF. The AGAF can be found at http://www.agimo.gov.au/infrastructure/authentication/agaf_b

Australian Government Information and Communications Technology Security Manual (ACSI 33)

The ACSI 33 provides policy and guidance to complement the Protective Security Manual. The advice is designed to enable government agencies to achieve an assured information technology security environment. ACSI 33 ensures there is a minimum standard for information and communication technology security that can be applied consistently across government agencies. The ACSI 33 can be found at <http://www.dsd.gov.au/library/infosec/acsi33.html>

Australian Government Protective Security Manual 2005 (PSM)

The Attorney-General's Department issues the Australian Government Protective Security Manual (PSM). It is the principal means for disseminating Australian Government protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for protecting official resources. The revised PSM provides minimum mandatory standards in protective security for all Australian Government agencies and contractors and their employees performing services for and on behalf of the Australian Government. These minimum standards ensure a consistent approach to protective security within and between agencies. An overview of the contents of the PSM can be found at

<http://www.ag.gov.au/www/agd/agd.nsf/Page/RWPE30AA68A4D5313EACA2571EE000AAF9F>

Employees and contractors will need to liaise with their relevant Agency Security Advisor to access to the PSM as it classified as Security-In-Confidence.

Australian Public Service Commission, Conditions of Engagement booklet

The Conditions of Engagement booklet provides agencies with advice on exercising an agency head's discretion to impose conditions upon the initial engagement of an APS employee in relation to, for example, citizenship and character checks.

Australian Public Service Commission, *Ongoing Employment – Recruitment and Related Issues*

The *Ongoing Employment – Recruitment and Related Issues* booklet provides guidance on recruitment and selection for both engagement and subsequent promotion and movement within the APS. It includes a brief discussion of pre-employment checking and a sample letter and instrument of engagement.

This booklet is part of a series of guides the Commission issued to complement the *Public Service Act 1999*. Agencies can access the latest information through www.apsc.gov.au.

APS Employment Database Manual Version 3 (2005)

The APS Employment Database Manual describes, in detail, APSED reporting. It describes processes and what data is collected, as well as the codes, definitions, intended usages and interpretations needed for data comparability. Where possible the definitions are derived from the Public Service Act 1999 and supporting documentation. The APS Employment Database Manual can be found at <http://www.apsc.gov.au/apsed/apsedmanual.pdf>.

Commonwealth legislation and regulations

Commonwealth legislative and regulatory instruments that affect employment, security and privacy have been enacted. Those that are particularly relevant to IMAGE are listed below.

- Administrative Appeals Tribunal Act 1975
- Administrative Decisions (Judicial Review) Act 1977
- Crimes Act 1914
- Disability Discrimination Act 1992
- Equal Employment Opportunity (Commonwealth Authorities) Act 1987
- Equal Opportunity for Women in the Workplace Act 1999 (Consolidation version)
- Freedom of Information Act 1982
- Occupational Health and Safety (Commonwealth Employment) Act 1991
- Privacy Act 1988
- Public Service Act 1999 and instruments made under that Act
- Public Service Regulations 1999 (Consolidation version)
- Public Service Commissioner's Directions 1999 (Consolidated version)
- Sex Discrimination Act 1984
- Superannuation Act 1990 (Consolidation version)
- Superannuation Act 1976 (Consolidation version)
- Superannuation Guarantee (Administration) Act 1992
- Workplace Relations Act 1996
- These Acts can be accessed through www.comlaw.gov.au

Freedom of Information Act 1982 (Cwth)

The object of the Freedom of Information Act 1982 is to extend, as far as possible, the right of the Australian community to access information in the possession of the Australian Government. It does this by making available to the public, information and documents in the possession of Ministers, agencies and public authorities (limited only by exceptions and exemptions necessary for protecting public interests and the private and business affairs of people in respect of whom information is collected and held by agencies and public authorities). It also provides the right to bring about amendment of records containing personal information that is incomplete, incorrect, and out of date or misleading. The FOI Act is available at <http://scaleplus.law.gov.au/html/pasteact/0/58/top.htm>.

As well, the Attorney-General's Department website has general information about freedom of information at http://www.ag.gov.au/agd/WWW/agdhome.nsf/Page/RWP1EC54688BED58170CA2570770_01D10FF#5

Human Rights and Equal Opportunity Commission (HREOC)

The HREOC's responsibilities include education and public awareness, discrimination and human rights complaints, human rights compliance, and policy and legislative development. Details on HREOC can be found at www.humanrights.gov.au. The discussion paper on discrimination in employment based on criminal record can be found at http://www.humanrights.gov.au/human_rights/criminalrecord/summary.html.

National Identity Security Framework

The National Identity Security Strategy, developed by the National Identity Security Coordination Group is a Council of Australian Governments initiative providing a framework for strengthening identity security at a national level. The Strategy consists of six elements designed to achieve this purpose and provides a guide for the development of jurisdictions' own identity security frameworks. The Report to the Council of Australian Governments on the elements of the National Identity Security Strategy can be found at http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_ReporttotheCouncilofAustralianGovernmentsontheelementsoftheNationalIdentitySecurityStrategy-April2007

Privacy Act 1988 (Cwth)

The Privacy Act 1988 protects the privacy of individuals. It contains 11 Information Privacy Principles that are the baseline privacy standards government agencies need to comply with in relation to personal information kept in their records. The Privacy Act and information is available at <http://www.privacy.gov.au>.

Standards

ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards. ISO is a non-governmental organization that forms a bridge between the public and private sectors. Many of its member institutes are part of the governmental structure of their countries, or are mandated by their government, while other members are from the private sector, having been set up by national partnerships of industry associations. More information about international standards can be found at <http://www.iso.org/iso/home.htm>

The American National Standards Institute (ANSI) is the organisation responsible for the US standards and conformity assessment system. Further information about ANSI can be found at <http://www.ansi.org>

Information Privacy Principles

The Information Privacy Principles (IPPs), reproduced below, have been extracted from Section 14 of the Privacy Act 1988. Further information about the IPPs can be obtained from your agency Privacy Contact Officer or at the website of the Office of the Privacy Commissioner²⁰.

Principle 1 – Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
 - (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
 - (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2 – Solicitation of personal information from individual concerned

Where:

- (a) a collector acquires personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

- (c) the purpose for which the information is being collected;
- (d) if the collection of the information is authorised or required by or under law – the fact that the collection of the information is so authorised or required; and
- (e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

²⁰ <http://www.privacy.gov.au>

Principle 3 – Solicitation of personal information generally

Where:

- (a) a collector acquires personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector:

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

- (c) the information collected is relevant to that purpose and is up to date and complete; and
- (d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4 – Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

- (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
- (b) that, if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5 – Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:
 - (a) whether the record-keeper has possession or control of any records that contain personal information; and
 - (b) if the record-keeper has possession or control of a record that contains such information:
 - (i) the nature of that information;
 - (ii) the main purposes for which that information is used; and
 - (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.
3. A record-keeper shall maintain a record setting out:
 - (a) the nature of the records of personal information kept by or on behalf of the record-keeper;
 - (b) the purpose for which each type of record is kept;
 - (c) the classes of individuals about whom records are kept;
 - (d) the period for which each type of record is kept;
 - (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
 - (f) the steps that should be taken by persons wishing to obtain access to that information.
4. A record-keeper shall:
 - (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and
 - (b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6 – Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7 – Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:
 - (a) is accurate; and
 - (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.
2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

- (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
- (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;
- (c) the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8 – Record-keeper to check accuracy etc. Of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9 – Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10 – Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:
 - (a) the individual concerned has consented to use of the information for that other purpose;
 - (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
 - (c) use of the information for that other purpose is required or authorised by or under law;
 - (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
 - (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.
2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11 – Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
 - (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
 - (b) the individual concerned has consented to the disclosure;
 - (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
 - (d) the disclosure is required or authorised by or under law; or
 - (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under Clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

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.

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.