



**Australian Government**

**Department of Finance and Deregulation**

Australian Government Information Management Office

# National Smartcard Framework



**December 2008**

## Disclaimer

This document has been prepared by the Department of Finance and Deregulation (Finance) to provide information to government bodies in relation to the use of smartcards for government transactions.

While every effort has been made to ensure that the document is accurate, no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the document. This document should not be relied upon as legal advice. Users are encouraged to seek independent advice relevant to their own circumstances.

Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

Department of Finance and Deregulation

Australian Government Information Management Office

© Commonwealth of Australia 2008

ISBN (online): 0 9758173 6 1

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the :

Commonwealth Copyright Administration,

Attorney General's Department,

Robert Garran Offices,

National Circuit,

Barton ACT 2600

or posted at <http://www.ag.gov.au/cca>

## Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Copyright: Department of Finance and Deregulation

# Foreword

Smartcards are emerging as an important technology in the public and private sectors. Smartcards have the potential to improve service delivery and user convenience and increase security against identity theft and fraud.

The National Smartcard Framework (the Framework) will allow consistent approaches to the implementation of smartcard technology by agencies in all Australian jurisdictions. It assists agencies deploy smartcards and allows for common policies and technologies with technical interoperability between smartcard deployments. The Framework is based on Australian Government and international standards, including those from the International Standards Organisation (ISO).

For citizens, smartcards have the capacity to increase the trust and confidence in engaging in online transactions with government with the knowledge that their smartcard provides enhanced protection of personal information. Additionally, smartcard technology offers users the scope to hold multiple credentials on the one smartcard thus enabling them to interact with a number of agencies. This Framework aims to ensure that the experience of citizens is as simple as possible when using smartcards.

The Framework is endorsed by the Australian Online and Communications Council (OCC) which is the peak ministerial forum across Australia on strategic approaches to information and communications technology issues. In endorsing the Framework, the Council agrees that jurisdictions will:

- comply with the principles of the National Smartcard Framework
- accept that the Smartcard Handbook, the Implementation Models and Checklists, the Smartcard Project Design Guide and the Framework Implementation Specifications form better practice guidance documents.

The Framework's principles will help agencies make best use of agreed standards, and smooth the path towards more comprehensive future standards and toolsets. These principles centre on preserving the business objectives of original smartcard issuers, protecting cardholder privacy, ensuring security of multiple applications and giving due consideration to interoperability at the design stage.

Ann Steward  
Australian Government Chief Information Officer  
Chair, Cross Jurisdictional Chief Information Officers Committee

# Contents

Foreword	iv	
1. Introduction	4	
1.1 Intended audience	5	
1.2 Scope		5
1.3 Structure of the Framework	5	
1.3.1 Outline of the sections	5	
1.4 Governance	8	
1.5 Contact details	9	
2. Vision and principles	10	
2.1 A vision for and benefits of the Framework	10	
2.1.1 Interoperability of the Framework	11	
2.1.2 Benefits of the Framework	11	
2.2 Principles	13	
Principle 1: Interoperability	13	
Principle 2: Privacy and data protection	13	
Principle 3: Risk management	14	
Principle 4: Security and trust	16	
Principle 5: Choice and flexibility	17	
2.3 Business approach	18	
2.4 Information approach	18	
2.5 Technology approach	19	
3. Communities of practice	20	
3.1 Establishment of a CoP	21	
3.1.1 Roles of CoPs	22	
3.2 Governance	23	
3.3 Examples of CoPs	24	
3.3.1 Telecommunications	25	
3.3.2 Commercial	25	
3.3.3 Transport	25	
3.3.4 Border control	27	
3.3.5 Health and human services	28	
3.3.6 Access control	29	

4.	Interoperability architecture	31
4.1	Technical interoperability	31
4.1.1	What does “technical interoperability” mean?	31
4.1.2	Levels of interoperability	32
4.1.3	Standards of interoperability	33
4.1.4	Establishing interoperability	33
4.1.5	Interoperability with other sectors of the economy	33
4.2	Standards and policies	34
4.2.1	International standards	35
4.2.2	Australian Government standards	37
4.2.3	Industry and vendor standards	40
4.2.4	Interoperability standards developed using existing CoPs	41
4.3	Interoperability under ISO/IEC 24727	43
5.	Functional considerations	43
5.1	Framework Implementation Specifications (FIS)	43
5.1.1	Management of FIS	43
5.1.2	FIS functional requirements	44
5.1.3	Further information on FIS	44
5.2	Card lifecycle considerations	44
5.3	The chain of trust	46
5.4	Security and protection requirements	48
Appendix 1: List of shortened forms		38
<hr/>		
List of figures and tables		
Figures 1: Structure of the Framework		6
Figure 2: Interoperability interface from Australian Government Technical Interoperability Framework		11
Figure 3: Roles of CoPs		22
Figure 4: Examples of CoPs		24
Figure 5: CoP case study		27
Figure 6: Agency program framework		34
Figure 7: Smartcard lifecycle model		45
Table 1: Levels of interoperability		32
Table 2: Description of international standards		35
Table 3: Australian Government standards		36

# 1 Introduction

The National Smartcard Framework (the Framework) aims to facilitate consistent implementation of smartcard technology by agencies at all levels of Australian government. It will assist agencies that intend to deploy smartcards and allow for the adoption of common policies, business processes and technologies that facilitate interoperability between smartcard deployments.

The benefits arising from such deployments include:

- improved service delivery through harnessing the added convenience and functionality that smartcards can provide
- reduced costs of smartcard deployments; and
- increased security of government information and resources.

Deployments of the Framework will also provide a range of benefits to citizens and businesses including:

- more streamlined interaction with governments
- enhanced protection of information
- scope for functionality to be extended without additional registration processes; and
- the potential for personalisation of information held on the smartcard.

Smartcards are an important enabling technology in a variety of online, offline and hybrid applications in the public and private sectors. A smartcard deployment involves a number of levels that shall be considered before the technology can be implemented. These include:

- defining the business requirements that are to be met
- establishing the rules and processes that will govern the use of the smartcard
- designing the information that is to be available on the smartcard; and
- selecting the technology to be used, including the smartcard itself, card readers, communication methods, applications and interfaces to back-end systems.

Deployments may be concentrated on a closed group of cardholders, such as staff of an agency that wishes to use smartcards to control access to buildings and systems, or a wider group, such as all the users of a particular transport network. The deployment of smartcards in either case represents a significant investment and therefore it is critical that this technology is applied efficiently and effectively.

## 1.1 Intended audience

The Framework is aimed at government agencies deploying smartcards, and third-party service providers engaged to deliver smartcard solutions on their behalf. These agencies are known as “card authorities” in this Framework.

It should be read by:

- policy makers responsible for introducing smartcards for delivery of services
- business and information system managers who are required to implement or acquire smartcard-enabled services; and
- technical architects involved in implementing new forms of information technology (IT) service delivery.

## 1.2 Scope

This Framework is one of a number of frameworks developed to support interoperable business applications across all Australian governments. It supports the blueprints for connected government described in e-government strategies published at different levels of government. Additionally, the Framework fits within a broader range of policy documents covering service delivery, authentication, identity management and interoperability. Further explanation of these card lifecycle considerations is found in Section 5.2.

Agencies should read this Framework in conjunction with their own jurisdictional frameworks and consult within their own governance structures as to how the Framework is to be implemented. Interoperability also relies on the policies, protocols and patterns agreed by specific communities of practice (CoPs), which may operate across jurisdictions or business domains. CoPs, and the wider community of interest (Col) concept, are both defined in Section 1.4 and described in more detail in Section 4.

In order to use a consistent language when describing the different business, information and technical layers, this Framework uses the Australian Government Interoperability Frameworks. This is a set of interrelated frameworks developed to assist Australian Government agencies in making the transition to connected and shared modes of operation. Detailed explanation of the Interoperability Frameworks can be found at <[www.finance.gov.au](http://www.finance.gov.au)>.

## 1.3 Structure of the Framework

Figure 1 indicates how the Framework is organised.

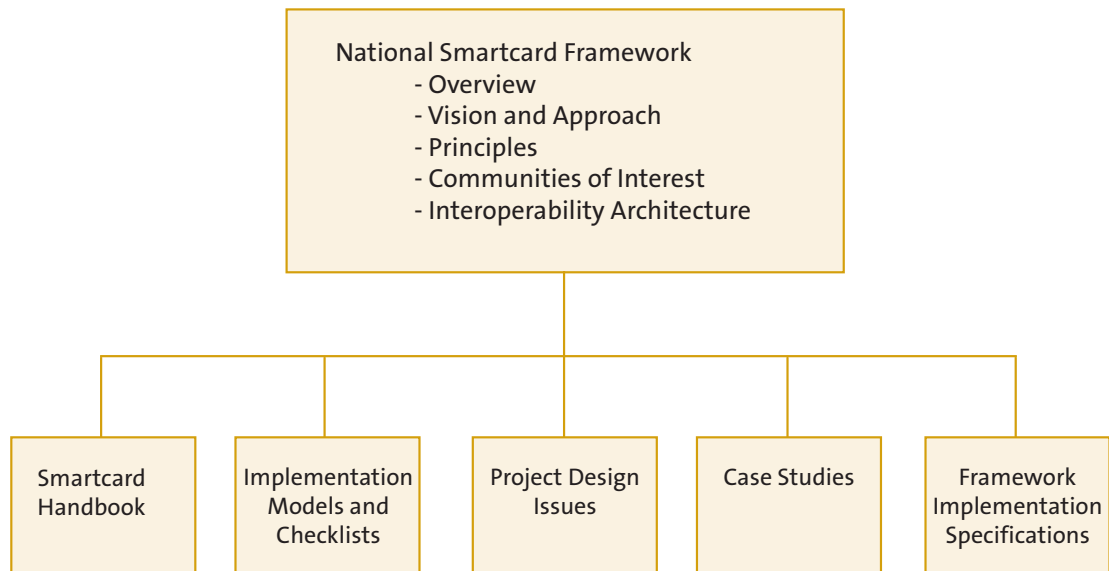


Figure 1: National Smartcard Framework Structure

To complement the Framework, a suite of online supporting documents will be available to assist agencies in planning and implementing smartcard deployments. The suite will include:

- Smartcard Handbook
- Implementation Models and Checklists
- Smartcard Project Design Guide
- Case Studies; and
- Framework Implementation Specifications (FIS)

It is expected that case studies will be provided by CoPs as smartcard deployments occur. These supporting documents will be online at <http://www.finance.gov.au/e-government/>.

## Outline of sections

### National Smartcard Framework (the Framework)

1. Introduction - outlines the concept of smartcard deployments and how the Framework and its supporting material is structured.
2. Vision and principles - articulates a set of uniform principles for smartcard deployments by Australian governments and considers the benefits the Framework will provide.
3. Communities of practice - includes a description and examples of CoPs and their business requirements.
4. Interoperability architecture - includes a discussion of what is meant by interoperability and the standards which assist in achieving it.
5. Functional considerations - offers suggestions around smartcard specific issues relating to the lifecycle of a card, and security and trust.

Appendix A: Glossary and bibliography - defines the terms and language used in the Framework.

### Framework support documentation

- Smartcard Handbook - is a guidance document providing an overview of smartcard technology, including a plain-English description of smartcard technologies, the technology “stack”, and how smartcards can deliver certain benefits in certain environments.
- Implementation Models and Checklists - includes various models for the implementation of smartcard projects and a series of checklists that can be used as tools at different stages of a deployment.
- Smartcard Project Design Guide - provides guidance at the project management level in important areas such as privacy, security and technology selection.
- Case Studies - includes a selection of domestic and international deployments to assist readers in assessing some of the issues that have arisen in smartcard implementations.
- Framework Implementation Specifications (FIS) - allow for the sharing of functional specifications and reference models relating to smartcards implemented by a specific CoP. This will enhance interoperability and re-usability between agencies and third-party providers while protecting intellectual property. The concept and use of FIS is introduced in Section 5: Functional considerations.

## 1.4 Governance

The Framework has been prepared by the Australian Government Information Management Office (AGIMO) in collaboration with agencies in all Australian jurisdictions. It has been endorsed as a National Smartcard Framework by the Online and Communications Council, after consideration by the Australian Government's Chief Information Officers Committee and the Cross Jurisdictional Chief Information Officers Committee. These committees have been informed by their appropriate working groups, with additional advice from specialist technical reference groups. The Australian Local Government Association has also been consulted in the development of this Framework.

Within the context of this Framework, "government" refers to all levels of government within Australia; that is, Commonwealth, states and territories, and local governments. In endorsing the Framework, governments agreed that - except where the business requirements within a jurisdiction indicate that adaptation may be necessary - they will:

- accept the principles of the National Smartcard Framework
- follow, as a minimum, the technical specifications included in the Framework; and
- use the supporting documentation (Smartcard Handbook, the Smartcard Implementation Models and Checklists, the Smartcard Project Design Guide, Case Studies, and FIS) as better practice guidance documents.

In this Framework the following terms are defined in alignment with the Standards Australia definitions as stated in HB162-2002:

"shall" is used where there is a requirement to be strictly followed in order to conform to the document and from which no deviation is permitted

"should" is used to indicate that - among several possibilities - one is recommended as particularly suitable, without mentioning or excluding others, or that a certain possibility or course of action is deprecated but not prohibited

Governments have agreed that CoPs will be the vehicle through which the governance and assurance model will operate. The Australian Standard on Knowledge Management (HB 189-2004) defines a CoP as a group which develops competence and good practice in a defined area. Within the context of this Framework, a CoP is defined as:

an agreed population of card authorities (also referred to as members) with policy and operational responsibility for defined smartcard deployments.

In addition to the members of a CoP, it is recognised that a wider group of stakeholders will have an interest in and require input to the design and development of a smartcard deployment. These may include cardholders, vendors, card issuers, service providers, relying parties and even other CoPs. Together, these parties make up a community of interest (Col). CoPs should consult their wider Col when designing the deployment. However, the members of the CoP have the responsibility for making policy and operational decisions regarding the architecture of the deployment at the business, information and technical layers as described in the Australian Government Interoperability Framework.

Further guidance on CoPs and Cols is included in Section 4 of the Framework.

All technologies evolve, and frameworks need to be continually updated. All governments will continue to be consulted as this Framework evolves and their agreement sought to ensure that their smartcard deployments align with the Framework. This will help achieve maximum economies of scale, critical mass, and convenience for members of the public and businesses.

Existing smartcard implementations are not required to comply retrospectively but, where practicable, any extension or replacement of an existing deployment shall comply with the Framework to the greatest extent possible.

This Framework and supporting material are managed by cross-jurisdictional working groups. Details about these groups can be found through the Department of Finance and Deregulation website at <<http://www.finance.gov.au>>.

## 1.5 Contact details

Inquiries should be forwarded to <[smartcard@finance.gov.au](mailto:smartcard@finance.gov.au)>.

## 2 Vision and principles

### 2.1 A vision for and benefits of the Framework

The vision for the Framework is to ensure governments in Australia adopt a consistent approach to using smartcard technology. The benefits will be enhanced privacy and security of cardholder information, greater convenience in accessing government services and increased protection of government-issued smartcards and related systems. The Framework will enable agencies to design and deploy business process improvements, and create efficiencies and cost reduction through smartcards.

The marketplace for security and authentication technologies is dynamic, with demand drivers evolving rapidly in response to real-life threats and risks, quickly decreasing costs, and some technologies maturing. Expectations of authentication, on the part of agencies, businesses and the general public, are becoming very sophisticated. Smartcards are thought by many to offer special advantages in certain security settings. Historically, however, implementations have been constrained by the relatively high cost of smartcard technology and infrastructure.

In light of global trends and changing costs, smartcards will become steadily more important in Australia. This Framework seeks to facilitate clear thinking about implementation issues associated with new technologies, to help governments and their agencies understand the business case for smartcards, and to promote standardisation and uniformity for the shared benefit of all government agencies and their clients.

The Framework and its supporting materials:

- articulate a minimum set of requirements to optimise smartcard interoperability
- set minimum standards for all government smartcard technologies against which interoperable solutions may be specified and procured, with shared cost savings
- describe additional functionality - such as multiple applications, digital certificates, digital photographs, biometrics and interface options - and how agencies can customise deployments while still promoting interoperability; and
- outline considerations for agencies when designing smartcard deployments.

The intended benefits of the Framework are to:

- increase service delivery options for individuals and businesses accessing government services
- increase citizens' trust in transactions and confidence in using government-deployed smartcards
- increase consistency and interoperability of smartcard deployments

- increase the opportunity for re-use of valuable technical and information resources to the greatest possible extent
- increase economies of scale through maximum possible standardisation and uniformity in the application of smartcards
- reduce the total cost of implementation of smartcard deployments for all agencies; and
- increase the necessary technical and management capabilities in the public and private sectors to create new applications and to migrate to new technologies.

### 2.1.1 Interoperability in the Framework

One of the objectives of the Framework and the supporting material is to define common business and functional requirements and standards that will facilitate interoperability between smartcard deployments. In establishing this objective, it is recognised that for smartcard implementations to be interoperable, there needs to be alignment at the business, information and technical layers.

In the Australian Government Technical Interoperability Framework, interoperability is defined as:

the ability to transfer and use information in a uniform and efficient manner across multiple organisations and information technology systems. It underpins the level of benefits accruing to enterprises, government and the wider economy through e-commerce.

The following diagram shows how interoperability can be achieved. The Alignment Domain is where CoPs and CoIs sits along with the appropriate standards referenced in this Framework that will assist in achieving interoperability.

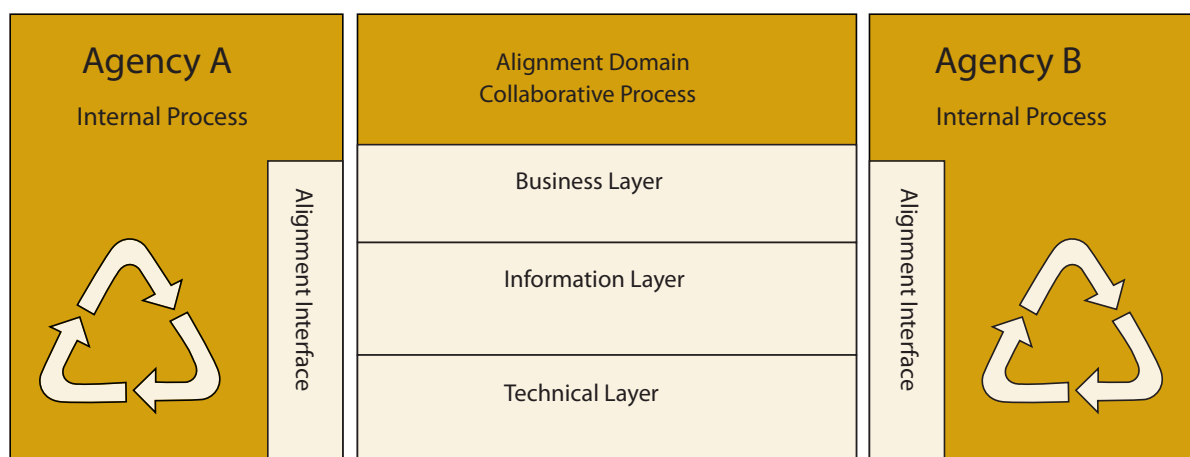


Figure 2: Interoperability interface from Australian Government Technical Interoperability Framework

Interoperability is more than just the flow of information between agencies and the connection of IT systems. It requires a collective mindset, an understanding of how each collaborating agency operates and the development of arrangements which effectively manage business processes that cut across organisational boundaries. To achieve interoperability, it is imperative for the business and information layers to be aligned before consideration is given to technology choices.

Within the smartcard context there is a need for the alignment of business processes to allow different jurisdictions or lines of business to interact, and agreed data specifications and technical infrastructure that is able to recognise all other components and provide an end-to-end business transaction. The responsibility for designing the smartcard deployment to meet these requirements rests with the CoP.

### 2.1.2 Benefits of the Framework

By following this Framework across all government smartcard deployments, governments and users will see a number of significant shared benefits. This Framework will enable:

- Lower unit cost of smartcards. This has been a major issue, with smartcards often costing several dollars each. Even a large deployment of smartcards in Australia represents a relatively small market by international standards. In this context, adopting a Framework-compliant smartcard optimises the per-unit price that can be offered.
- Lower total cost of ownership. Using the Framework will ensure high degrees of uniformity and shared business requirements and infrastructure. These are characteristics that can lead to large-scale managed service options, with the potential to reduce total cost of ownership. One example is the development of an optical variable device (OVD) that may be used in multiple deployments, hence saving considerable costs on the design and production of an OVD on subsequent deployments.
- Confidence of cardholders and users in smartcard based systems. As smartcards are deployed in accordance with the Framework, citizens, businesses and other government agencies will have confidence in the ability of the system to provide security, privacy protection and usability for all stakeholders.
- Capability building. This will be achieved through:
  - a stronger Australian skills base - collaborative approaches build our capability to deliver new technology by developing a pool of skilled people knowledgeable in the core technologies
  - faster rollout of each new project through the ability to share ideas and lessons learnt -
  - collaboration facilitates greater cooperation and re-use between projects, less time spent revisiting strategic decisions and policy settings, and better access to commercial solutions
  - greater acceptance of smartcards by citizens as they gain familiarity with and understanding of smartcards through education and consistency of design of deployments

- developing a competitive Australian market for smartcard products and services that attracts quality vendor support, and fosters competition and innovation.
- Greater flexibility and ability to adopt innovation throughout government. By working collaboratively and developing best practice and continuous improvement processes, governments will be able to respond to changes in citizens' expectations and technology.

## 2.2 Principles

The following principles provide the foundation through which governments will deploy smartcards in a consistent manner. In accordance with the agreement detailed in Section 1.4: Governance, all government smartcard deployments shall conform to these principles and minimum standards, unless there are business requirements to do otherwise.

### Principle 1: Interoperability

Interoperability is best managed by communities of practice (CoPs) that bring together smartcard authorities for the purpose of delivering a business outcome

As defined in Section 4, CoPs are responsible for interoperability within their CoP and for determining whether there is a need for interoperability with another CoP's smartcard deployment.

Regardless of the technical approach that is taken to interoperability, there are a number of requirements that apply to all government smartcard deployments:

- Government issuers of smartcards shall consider interoperability and re-use issues when developing business requirements. Card authorities should consider whether they should enable re-use of the technological and information resources represented by their smartcards. The authority or the CoP, should clearly document their vision for interoperability and re-use and specify the scope of any re-use they support.

Card authorities should also consider existing arrangements between current holders of non-smartcard cards and third parties who rely on printed information available on the face of the existing card. The implications in changing access to that information should be considered.

If interoperability and re-use is to be allowed, the business objectives of the issuer of the smartcard shall not be hampered by any subsequent addition of extra functionality to those cards. Any third-party applications which would seek to interoperate in any way with the card, shall have the permission of the issuer and that of the cardholder where applicable, to do so. (Refer to Principle 2: Privacy and data protection, below).

Importantly, interoperability does not automatically mean that any given smartcard is usable by any other government agency or third party. This principle, in a sense, preserves the "business ownership" of a smartcard by the card authority that first invested in its deployment. It also helps to protect against compromise of smartcard users' privacy should other agencies seek to make use of the original deployment.

- Any parties who would seek to re-use or interoperate with a government-issued smartcard shall engage with the issuer (and with members of the relevant CoP where applicable) before deploying new applications or adding extra functionality to cards. The issuer, and the CoP where appropriate, shall ensure that its vision for re-use is clearly scoped and specified.
- Levels of interoperability. The need for interoperability is recognised as the reason behind the creation of a CoP. There may also be a business reason for the smartcards from two or more CoPs being able to interoperate. However, it is recognised that the level of interoperability between smartcard deployments will vary depending on the business need and it is the responsibility of the CoP to determine that level. A table describing the levels of interoperability is at 4.1.2.

## Principle 2: Privacy and data protection

Card authorities shall take measures to safeguard the privacy of personal information and the confidential data of businesses, and protect government data.

Privacy and data protection - provision of assurances by means of law, technology design and industry practice that personal information will be collected, exchanged and used fairly and in full compliance with applicable privacy laws or schemes and regulations - are important issues to be considered from the outset of any smartcard deployment.

For any smartcard deployment to be successful, the expectations of the community around privacy and data protection shall be met. To do this, the privacy legislation and regulations shall be complied with and a comprehensive communications plan should be developed to ensure that potential cardholders understand the ways their information will be protected.

This Framework aims to work within the legal framework for the protection of personal information within particular jurisdictions:

- card authorities shall have a comprehensive privacy policy and make the policy available to all members of the CoP. The privacy policy shall comply with the requirements of the privacy regime in their particular jurisdiction
- card authorities shall comply with relevant jurisdictional privacy schemes. At the Australian Government level, agencies deploying smartcards shall comply with the Privacy Act 1988 (Commonwealth) and its regulations. Card authorities in other jurisdictions shall comply with their relevant privacy regimes; and
- in accordance with relevant legislation and privacy and identity security policies within applicable jurisdictions, card authorities shall undertake a privacy impact assessment:
  - at relevant points in the design of a smartcard deployment, including initial design and final design stage
  - whenever the functionality of a smartcard system is to be altered, particularly by adding new applications to the card scheme or secondary use of the data, the issuer shall ensure a privacy impact assessment is undertaken.

- card authorities shall ensure that the information is protected by reasonable security safeguards to protect it from loss, misuse, or unauthorised access, modification or disclosure
- card authorities shall ensure that any contracted service provider that is provided with any personal data is obligated to protect that data appropriately in accordance with their agency's requirements; and
- in protecting personal or business information contained on the cards, smartcard deployments should be designed to enhance privacy or confidentiality by removing information from human readable forms, requiring authorisation for access and including audit trails.

Further information on privacy and data protection is provided in the Smartcard Project Design Guide.

### Principle 3: Risk management

Card authorities shall undertake a risk management approach when designing and implementing a smartcard scheme.

In the development of a smartcard solution, CoPs shall consider the principle of risk management as being integral to the formulation of their policies and plans.

Card authorities in the various jurisdictions should take into consideration the requirements set out in their risk management and security guidelines. For example, Australian Government agencies shall comply with the Protective Security Manual , part b - Guidelines on Managing Security Risk.

CoPs shall ensure that every smartcard deployment is subject to a risk management plan (RMP). A risk treatment plan (RTP) shall be developed for each deployment. The risk assessment and treatment strategy contained within those plans should be consistent with the risk management guidelines set out in the following documents published by Standards Australia and available via <[www.saiglobal.com](http://www.saiglobal.com)>

- Australian Standard AS/NZS 4360 "Risk Management" (current edition)
- SAA HB 436 "Risk Management Guidelines - Companion to AS/NZS 4360"
- SAA HB 231 "Information Security Risk Management Guidelines".

CoPs implementing a smartcard deployment shall undertake formal threat and risk assessments, taking into account the following key considerations, where relevant:

- compliance with Commonwealth and state and territory legislation and regulations including, but not limited to, legislation and regulations relating to public administration, public record management, archival obligations, financial administration, management and audit, freedom of information, and privacy

- compliance with enforcement legislation and regulation including, but not limited to, legislation and regulation relating to law enforcement, anti-terrorism Acts, evidentiary requirements and electronic signatures
- compliance with sector-specific legislation including, but not limited to, legislation and regulations relating to health, education and transport
- identification and resolution of any conflicts between the requirements of Commonwealth and state legislation and regulations
- identification of the business risks to the CoP and the controls in place to mitigate risks to acceptable levels; and
- protection of the rights and identity of citizens.

When smartcards are being considered in an e-authentication context, the National e-Authentication Framework (NeAF) can provide agencies with assistance. The NeAF is a transparent risk management framework designed to assist agencies in determining appropriate authentication approaches and mechanisms for government services delivered electronically.

Awareness is an essential element of risk management, and information security requires attention at all levels. Security awareness should therefore be aimed at managers, users and information system practitioners. Awareness and understanding is essential to implement information security policies and to ensure that related controls are working properly. Managers, users and others with access to information resources cannot be expected to comply with policies they are unaware of or do not understand. Similarly, if they are not aware of the risks associated with their information resources they may not understand the need for and support compliance with policies designed to reduce risk.

## Principle 4: Security and trust

Card authorities shall take a comprehensive approach to security and take measures to build trust within the community of interest (CoI).

Protecting the security of a smartcard implementation and creating an environment in which all transacting parties, including the cardholder, operate within a 'chain of trust' is crucial to the effective operation of a smartcard scheme. A smartcard deployment that is not perceived as being secure is unlikely to be trusted. In such circumstances the utility of the smartcard will be reduced.

CoPs shall take a holistic view of security. Some of the possible security issues that shall be taken into consideration when designing smartcard deployments are:

- the security of all card applications shall be protected against intended or accidental corruption of application code and data, account hijacking, and eavesdropping on card functions. This means that all system components, including terminals, communications links and back-office systems, shall be appropriately protected

- where possible and appropriate, information shall be split between the card and the rest of the system in a way that compromising the integrity of either does not breach overall security
- unauthorised access to a particular card shall not justify the effort required to gain that access
- hacking into a single card or card reader shall not jeopardise the security of the entire system
- the physical security of the card shall be complemented by appropriate accounting and audit measures
- the likelihood of the information held on the card being compromised and the potential maximum impact on the card holder and issuer shall be minimised; and
- management systems shall provide for timely blocking of cards suspected of being involved with security breaches.

Other parts of the Framework and supporting materials explore security in more detail - both the general security strengths of smartcards as well as their security peculiarities. Agencies should consult with the Defence Signals Directorate, or equivalent jurisdictional bodies, if in any doubt.

## Principle 5: Choice and flexibility

Efficient and effective service delivery is optimally achieved through a Framework that provides agencies and their clients with a degree of choice and flexibility.

Frameworks such as this represent a significant balancing act between the desire for card authorities' autonomy in managing business requirements and risks locally, and the ideal of maximum standardisation and uniformity across CoPs. This balance is recognised in the agreement that all Australian governments will comply with the requirements of the Framework except where their business requirements indicate that adaptation may be required.

Consequently this Framework respects an agency's individual business requirements and recognises that some customisation may be required to meet the needs of each agency's specific circumstances, even within a CoP. While the Framework requires adherence to recognised industry standards and actively promotes efforts to achieve interoperability, it does not mandate a one-size-fits-all solution. In fact, complete adherence to the Framework may not be cost effective in some cases, such as small, localised smartcard deployments.

The ideal is to set standards as high up the technology "stack" as possible, so all smartcard deployments converge towards a common set of building blocks, tools and skills, while allowing sufficient room for customisation on a project-by-project basis. The Framework embodies certain decisions regarding this balancing act, and attempts to make those decisions explicit in the discussions that follow. Card authorities, governments and CoPs are encouraged to only deviate from these decisions through their own customisation where necessary to meet their own explicit business needs. Over time, as fully mature interoperability standards emerge from the smartcard industry, the balance will become easier and gradually less customisation will be required.

## 2.3 Business approach

Smartcards are an enabling technology that can be used to fulfil a business requirement. After the requirement has been fully identified and a range of technical solutions have been considered, if smartcards are selected as the most suitable solution only then should the deployment go ahead.

The business approach for the Framework is based on the concept of CoPs which will lead to interoperability between government smartcard deployments where appropriate and encourage re-use of components and other materials. The Framework recognises that it is essential to create aligned business processes as the first stage in developing an interoperable smartcard deployment.

The use of this Framework will:

- guide the establishment of CoPs that bring together card authorities from different governments or agencies that have a common interest in deploying an interoperable smartcard
- create a consistency of approach in designing and implementing smartcard deployments
- enhance interoperability within and between CoPs deploying smartcards by adopting appropriate standards at the international and domestic level; and
- increase efficiency and effectiveness by the re-use of appropriate applications and other components.

The analysis of core business requirements for this Framework and supporting material has focused on providing strong infrastructure guidance, whilst leaving business considerations to CoPs. Further guidance on aligning business considerations can be found in the Australian Government Business Process Interoperability Framework at <<http://www.finance.gov.au>>.

## 2.4 Information approach

The Australian Government Information Interoperability Framework describes information interoperability as:

the ability to transfer and use information in a uniform and efficient manner across multiple organisations and information technology systems.

In the smartcard context, information will be exchanged across systems using smartcards as the enabling technology. It is essential that information is aligned in a way that allows it to be shared without breaching its integrity or the privacy and protection regulations that attach to it.

This Framework does not prescribe how information should be handled but leaves it to CoPs to determine what information will need to be exchanged and how they are going to handle its alignment. The Information Interoperability Framework will assist CoPs by providing principles that underpin sound information management and establish the concepts, practices and tools that will drive the successful sharing of information within and between smartcard deployments. It can be found at <<http://www.finance.gov.au>>.

## 2.5 Technology approach

The aim of the Framework at the technology layer is to:

- identify interfaces that allow for interoperability within and between smartcard deployments; and
- increase efficiency and effectiveness by the re-use of suitable components and other materials.

The Framework concentrates on the technology layer as the decisions about the business and information layers will need to be made on a deployment-by-deployment basis. Once the business and information layers are aligned, the technology layer becomes less complex but does still need careful consideration to ensure interoperability.

There are standards available that support interoperability and re-use. However, they do not guarantee interoperability unless all members of the CoP agree as to how they will implement all parts of the smartcard system and adopt the relevant sections of the standards. In particular, International Organisation for Standardization / International Electrotechnical Commission (ISO/IEC) 24727 has been developed to facilitate interoperability at its application layer to allow smartcards to operate across different deployments. In the Australian context this may apply to smartcards providing similar functions across a number of jurisdictions or offering several different functions that cross lines of business.

ISO/IEC 24727 mandates the following capabilities:

- a common application interface for a broad range of card types
- discoverability of a smartcard's capability and applications, and automatic configuration of the middleware layer in ISO 24727 stack to support the particular card and applications; and
- the ability to swap or select different authentication protocols depending on application business requirements (e.g. changing from PIN to shared-secret card authentication).

### 3 Communities of practice

A community of practice (CoP) is a group that comprises smartcard authorities committed by formal agreements to implementing a particular business requirement. Its role is crucial in terms of providing interoperability. It provides agreed protocols and specifications beyond technical standards for that CoP so that specific government smartcard deployments satisfy not only individual agency requirements but also broader government strategic objectives.

The members of the CoP have the responsibility for making policy and operational decisions regarding the smartcard deployment. They may be driven by legislative or policy requirements that require the enabling technology of smartcards. The community will be bound by an agreed set of rules. Such rules could be in the form of an explicit membership agreement, or they could be enshrined in legislation.

In addition to the CoP, a broader group may exist that are stakeholders in the smartcard deployment. These will form a community of interest (Col), which may consist of cardholders, card issuers, card-relying parties, card vendors, service providers, privacy advocates and other government agencies that may have an interest in the deployment.

Within the public sector, a variety of Cols already exist. Most of these fall within lines of business. For example, there are Cols relating to driver licences, e-passports, government staff identity cards, higher education, clinical health services, health and social services, and transit services. Some of these groups are now becoming CoPs as they undertake smartcard deployments.

It is acknowledged that a card authority may belong to more than one CoP. For example, a licensing authority within a jurisdiction may be part of several CoPs - such as a cross-jurisdictional CoP to ensure interoperability of the licence across state boundaries, and a CoP consisting of all licensing authorities within their jurisdiction such as driver licences, marine licences and industry licences. There may also be a need for interoperability with other, as yet unidentified, CoPs.

The same agency may also be a member of several Cols where it does not have responsibilities for decision-making regarding the smartcard deployment but still have an input into the design of the deployment to ensure its own requirements are considered.

Agencies should develop their business cases taking into account whether their smartcard deployment will be required to be:

- interoperable within an existing Col
- interoperable within a new Col
- interoperable across a number of Cols
- not interoperable; and
- not potentially damaging to other systems (as a minimum).

When doing this, agencies should also consider the level of interoperability that will be required as described in Section 4: Interoperability architecture. This will ultimately influence the scope of

the CoP. In some instances, a high degree of interoperability may be required. In others, the main interoperability requirement may only be that a credential issued by one party is capable of being recognised by another or even just that it does not cause adverse effects when read by a terminal belonging to a different CoP. It is also possible that the smartcard may not need to interoperate at all with other systems. This is usually the case in transit-card deployments.

When considering a smartcard deployment, any CoP should consider all stakeholders that are part of the Col currently using existing systems, whether they are directly involved in the management of the systems or are peripheral users; for example, relationships between the cardholder and another unknown party. In non-smartcard applications, much of the information is available on the face of the card. As digital aspects are introduced, it is important to consider all ways the information on the existing card is used.

### 3.1 Establishment of a CoP

A CoP can be established where the following conditions are met:

- there is a pre-existing working relationship between the members of the CoP, or a new opportunity to work collaboratively has been identified
- there are shared benefits to all parties
- there are no adverse privacy or security implications arising from the relationship; and
- it is legally and actually possible to create a relationship of trust between the members.

Whether a new CoP is being considered or created, existing CoPs are considering a new member, or an existing CoP is considering the need to interoperate with another existing CoP, a detailed business analysis should be undertaken. This analysis should include:

- an environmental scan of the existing environment (a checklist is included in Implementation Models and Checklists available separately to this document)
- a determination of the policy and business drivers
- identification of existing and emerging stakeholder groups and end users that may make up the associated Col; and
- the anticipated usage of smartcards.

Members of the CoP should negotiate and agree the terms and conditions under which the community will operate. The CoP should clearly define the business requirements that relate specifically to that community prior to deciding how technical interoperability will be achieved. This task is dependent on input from each member to ensure that the business requirements contained are expansive and robust.

Section 5: Functional considerations includes a description of the Framework Interface Specifications (FIS) concept. FIS are reference models and specifications that can be re-used to support smartcard deployments. They may include business and functional requirements, use case models and

detailed technical specifications that facilitate interoperability and re-use within and between deployments. A key activity for CoPs is to determine what FIS, if any, are necessary for them.

The Implementation Models and Checklists document contains a number of checklists that provide agencies with an indication of the issues that should be considered when establishing a CoP and any associated Col.

### 3.1.1 Roles of CoPs

CoPs should develop a set of specifications that cover all levels of the architecture for a smartcard deployment, from the performance domain to detailed technical specifications, to ensure interoperability across lines of business or jurisdictions. The diagram below illustrates the levels at which a CoP shall operate.

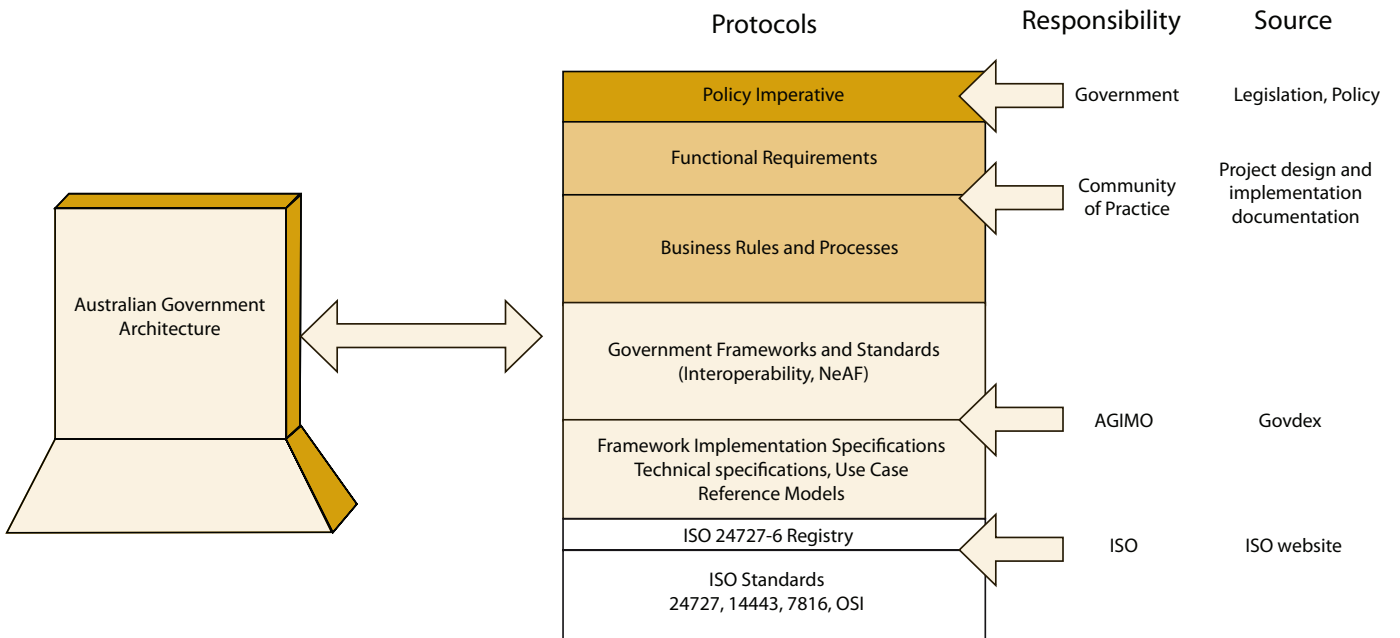


Figure 3: Roles of CoPs

Architectural frameworks exist to establish a common language and structure to assist in developing a solution to business requirements. They should take into consideration all aspects of the environment, from the policy impetus through the business processes, services to be delivered, information structure and technology. Using the Australian Government architecture terminology as an example, the levels at which a CoP should operate in order to achieve a successful smartcard deployment are:

- Performance domain - establishment of a CoP through a memorandum of understanding or other mechanism which binds the members to an agreed set of outcomes and policy requirements.
- Business and service domains - preparation of detailed business and functional requirements specifications to ensure that all policy and business requirements are able to be met across the CoI.
- Data domain - development of an agreed logical data structure to ensure interoperability at this level.
- Technical domain - definition of infrastructure requirements including physical cards, readers, communications, applications, both on and off card, security protocols and card management systems in accordance with recognised standards as appropriate.

Assistance in preparing these is available in the Implementation Models and Checklists and the Smartcard Project Design Guide that support this Framework.

Once the smartcard deployment is underway, it is important that the CoP undertakes testing for interoperability at the business, information and technical levels to ensure that interoperability has been achieved.

## 3.2 Governance

Each CoP has responsibility for establishing an appropriate governance regime and for managing compliance with the terms of the CoP. Members of CoPs will be responsible to the “parent” government in which they operate in accordance with existing accountability arrangements.

### 3.3 Examples of communities of practice

Using the terms of the Australian Government Architecture (AGA), CoPs can exist within business areas or service domains. They may also cross lines of business and/or combine business requirements and services.

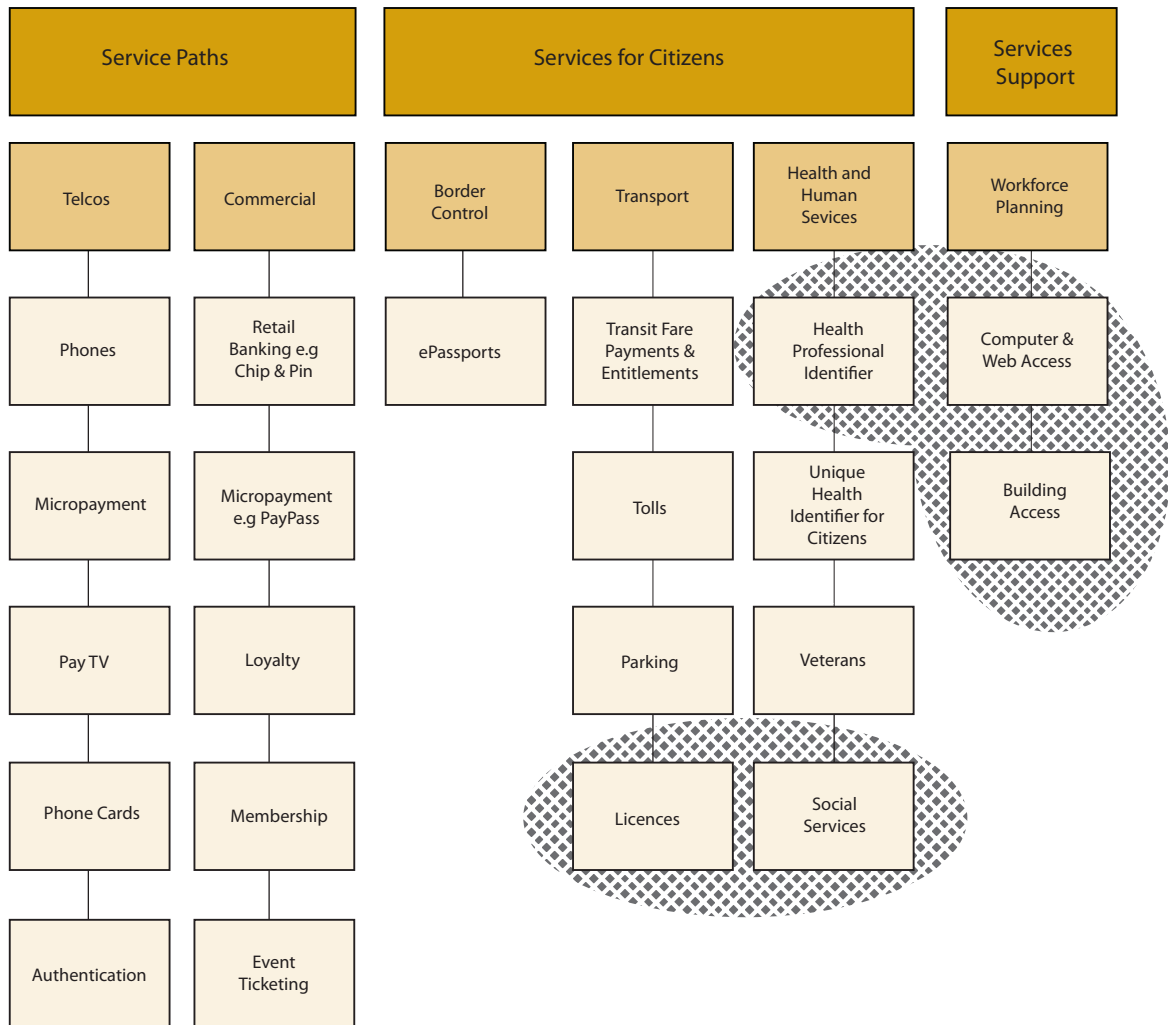


Figure 4: Examples of CoPs

As shown above there may be linkages between CoPs. For example, a health professional identifier card may also be used as a staff identity card and an access control card within a particular health service.

The following descriptions of CoPs, and the business requirements they need to fulfil in deploying smartcards, may assist when establishing a new CoP:

### 3.3.1 Telecommunications

Telecommunications CoPs are some of the largest users of smartcard technologies. Up to now the business requirements for this CoP have been fairly simple, including:

- high number of Integrated Circuit Card (ICC) in Subscriber Identity Module Identification (SIM ID)
- low level of security on operation; and
- low-level evidence of identity at registration.

As members of the CoP consider moving into Near Field Communications (NFC), these requirements will become more complex.

### 3.3.2 Commercial

Some important features of CoPs in the commercial sector that may be relevant to e-Government smartcard system design include:

- a strong and clearly bounded CoP
- potential worldwide interoperability
- that the prime organisation does not issue cards but provides multiple services, including specification and compliance management, business rules, operational oversight, transaction switching and international hot-listing
- the achievement of physical interoperability in part by mandating low-level ISO physical, electrical and logical interface standards
- the use of secure card readers/terminals
- the importance of secure processes when issuing cards and readers; and
- outsourcing of bulk issuance to trusted third parties.

The business considerations of this CoP that are relevant to government smartcard deployments are:

- high-integrity evidence of identity on registration; and
- high level of security for all transactions.

### 3.3.3 Transport

There are several distinct lines of business within this business area where CoPs may exist.

## Transit

Transit smartcard schemes (for automatic fare collection and concessional travel) are largely but not exclusively government-sponsored around the globe, including in Australia. Some important aspects of these CoPs are:

- a clearly bounded CoP
- use of low level ISO standards to achieve physical card-to-reader compatibility
- the likely use of significant proprietary back-end software elements
- use of ICCs with limited features
- requirement for high-speed throughput at the reader, which may require purpose-built readers
- complex interactions between issuers, service providers and cardholders
- outsourcing of issuance processes to trusted third parties
- support for both anonymous and personalised cards, determined by cardholder preferences and use-case needs
- use of embedded Secure Access Modules (SAMs) to protect card keys in front-end devices
- use of symmetric cryptographic keys as compared to public keys for card access; and
- need for transition planning from older technologies, such as paper ticket and magnetic stripe to chip-based technologies.

Within Australia, a number of transit smartcard projects have been initiated at state and local government levels. There are many other examples from around the world, such as the Oyster Card in London which is now required to become interoperable with the standards of the Integrated Transport Smartcard Organisation (ITSO) in the UK.

## Driver licenses

Policy and functional requirements for driver licences are strong considerations for a CoP in this line of business. Some of the business requirements are:

- a high level of interoperability across jurisdictions
- high-integrity registration and card-issuance processes, including the need for strong evidence of identity
- strong policy guidelines concerning use of cards for purposes other than as a driver credential
- robustness of card electronic and OVD security features, including anti-cloning and anti-counterfeiting measures

- that OVDs and other graphical elements provide first-stage credential verification capability
- different access rights to data on the ICC or on the back-end according to levels of authority of interrogator
- consideration of the use of public key methods for card authentication and access control
- being able to read the card at different types of service points (e.g. registry offices) and in the field (e.g. police checking of licenses in the field), potentially using varying hardware and software platforms; and
- consideration of other potential uses of the smartcard outside the intended use that may hinder acceptance of the card if not met.

#### SLIP: A COMMUNITY OF PRACTICE FOR DRIVER LICENCES

The Queensland Government has decided to transition its driver licence to a smartcard driver licence. To address platform-related interoperability issues across all jurisdictions, the Smartcard Licence Interoperability Protocol (SLIP) working group, chaired by Queensland Transport and reporting to the Austroads Registration and Licensing Task Force, has been established. The working group comprises representatives from Austroads, each state and territory, and the Commonwealth Department of Transport and Regional Services. It will assess and (where appropriate) recommend the adoption or modification of existing or developing national and international smartcard interoperability standards – thereby avoiding duplication of effort, minimising costs and reducing risk.

While other Australian jurisdictions may not currently have plans to implement smartcard driver licences, all have acknowledged the importance of ensuring continued mutual recognition and interoperability of driver licences (and supporting infrastructure) when Queensland makes the transition. This is to ensure that driver licences can continue to be used in an open “virtual” environment (for core driver licence information held on the smartcard chip), in the same way that information is currently accessed in an open “physical” environment (i.e. on the face of the licence). For example, following the introduction of the New Queensland Driver Licence (NQDL), any police officer in Australia would be able to access standard licence information stored on the Queensland licence chip. If other Australian jurisdictions move to a smartcard platform for their licences, they will be able to read driver licensing information from each other’s smartcards.

Figure 5: CoP case study

#### 3.3.4 Border control

Some important aspects of this CoP are:

- the requirement for a very clear privacy policy covering:
  - data collection
  - protection against loss, misuse or unauthorised access
  - modification or disclosure and destruction
  - any supplementary use of the identity token or instrument

- the need to determine if the smartcard instrument is an identity credential or is likely to be used as one
- the need for coherent cardholder education on the correct use and care of the token
- the requirement for a high-integrity enrolment and cardholder database management program
- the need for very strong anti-cloning and anti-counterfeiting controls
- the need for cross-border or cross-jurisdictional cooperation, including protocols for information exchange and card or token usage, along with common technical card-authentication methods
- the need for revocation agreements, including the ability to disseminate revocation lists in a timely manner, or to provide access to an online revocation database; and
- the potential requirement for granting different access privileges to different data fields or memory areas on the card chip.

### 3.3.5 Health and human services

There are various potential uses of smartcards for the delivery of health care and other human services within e-government. Some considerations for such a CoP are:

- a customer-centric focus to core deployment activities such as registration and card use; consideration should be given to all customer groups, particularly marginal groups such as the elderly and Indigenous Australians
- the development of a clear value proposition for all stakeholders, including government, the public and providers
- the development of a comprehensive privacy policy; in particular, the provision of customer choice and consideration covering data collection, protection against loss, misuse or unauthorised access, modification or disclosure, and destruction, and for any supplementary use of the identity token or instrument
- the deployment of a registration process leveraging existing government frameworks, such as the Australian Government Gatekeeper PKI Framework and the National Identity Security Strategy
- impacts on the business processes of healthcare professionals, such as doctors and pharmacists; in particular, how smartcards may impact on consultation times and how smartcard infrastructure, such as hardware and software, is deployed and managed
- the use of smartcards, including consumer and provider cards in healthcare settings, to provide an appropriate authentication mechanism to access electronic health services
- the use of smartcards and public key infrastructure (PKI) to implement claiming solutions
- the need for a high level of interoperability across jurisdictions; and
- the need for card anti-cloning and anti-counterfeiting controls.

### 3.3.6 Access control

An important current and future use of smartcards within government is for computer and building access control. Apart from this Framework, CoPs developing smartcard deployments for access control should take into consideration the National Identity Security Strategy (NISS), a discussion on which is accessible at <<http://www.ag.gov.au>>. The Australian Government's Identity Management for Australian Government Employees (IMAGE) framework also provides guidance on developing a smartcard for access control for employees. This can be found at <<http://www.finance.gov.au>>.

#### Agency computer access control (logical access)

The business requirements for access smartcard deployments include that a smartcard should:

- operate in support of, and in conjunction with, potentially complex infrastructure
- have a strong, unique two-factor (card plus e.g. PIN) authentication
- have authentication processes that are closely aligned to an authorisation system which defines permitted access to applications and data on an individual cardholder basis
- include a need for effective suspension, reactivation and revocation mechanisms both at authorisation and authentication levels
- allow, in some cases, complex transition plans for migration from older authentication schemes
- have the ability to manage identity management subsystems incorporating biometric capture that are likely to be part of the system design; and
- offer certificate-based public key cryptographic methods suitable for card authentication processes.

## Agency building access control (physical access)

Factors affecting a building access smartcard include the considerations that:

- building access authentication may only require single-factor (card authentication only)
- card readers may be under video surveillance
- access control authentication methods can vary across a broad spectrum of cryptographic capability
- Optically Variable Devices (OVDs) - which change colour when viewed from different angles - and other physical card security features are likely to play a significant security role in building access authentication
- current back-end infrastructure, including door access controllers, is likely to be specific to the application and proprietary to a given vendor
- building access smartcard systems shall have effective suspension, reactivation and revocation mechanisms; this includes a help desk for the reporting of lost, stolen and damaged cards; and
- conditions of tenancy and shared premises may significantly constrain options.

## 4 Interoperability architecture

This section provides guidance for CoPs seeking to build interoperable solutions. It is intended for technical architects and offers an overview of the path that will assist in achieving interoperability. It is important to note that compliance with standards and this Framework will not guarantee interoperability. Smartcards systems shall be designed to meet the level and extent of interoperability determined by the CoP.

### 4.1 Technical interoperability

#### 4.1.1 What does “technical interoperability” mean?

For the purpose of this Framework, smartcard technical interoperability is defined as information technology systems, cards, middleware and devices complying with the Framework that are able to recognise the other technical elements involved in an end-to-end business transaction and participate in the business transaction without limitation, other than that specified by business requirements.

This means that, for example, business transactions can occur within various operating policies and administrative procedures with:

- separate IT systems (including software, hardware and firmware); and
- various generations and types of cards and terminals but still provide a seamless, end-to-end transaction for the cardholder and relying parties.

## 4.1.2 Levels of interoperability

The table below outlines the different levels at which interoperability may be required. Each CoP will determine the level of interoperability required between the members of the CoP as part of its functional requirements and also whether there is a need for interoperability with other CoPs.

Level	Definition	Functions	Layer at which alignment is required to achieve interoperability
0	Interoperability only at the physical card level, meeting ISO 7816 and/or 14443	Able to: <ul style="list-style-type: none"> <li>meet card physical format requirements</li> </ul>	Technical layer only
1	Interoperability at the data level where freely available, on-card data can be read	Able to: <ul style="list-style-type: none"> <li>insert physical card into standard card reader</li> <li>read freely available data without authenticating the card</li> </ul>	Technical layer Information layer
2	Interoperability at the authentication level where the card can be identified as a validly issued card	Able to: <ul style="list-style-type: none"> <li>insert physical card into standard card reader</li> <li>read freely available data</li> <li>authenticate the card</li> </ul>	Technical layer Information layer Business layer
3	Interoperability at the application level, where the reader is permitted to access restricted data, or off-card applications	Able to: <ul style="list-style-type: none"> <li>insert physical card into standard card reader</li> <li>read freely available data</li> <li>authenticate the card</li> <li>validate reader to the card to enable access to restricted data or applications</li> </ul>	Technical layer Information layer Business layer
4	Full interoperability at all levels where the reader has permission to alter data that is loaded on the card	Able to: <ul style="list-style-type: none"> <li>insert physical card into standard card reader</li> <li>read freely available data</li> <li>authenticate the card</li> <li>validate reader to the card to enable access to restricted data or applications</li> <li>change applications on the card</li> </ul>	Technical layer Information layer Business layer

Table 1: Levels of interoperability

### 4.1.3 Standards and interoperability

The Framework has been based on international and Australian standards. The development of standards (both international and domestic) ensures that agencies have a choice of compliant smartcard devices and middleware vendors to facilitate interoperability. However, it should be pointed out that even compliance with standards will not provide interoperability. It is necessary for the CoP to define the individual stack models and physical characteristics required to ensure interoperability.

At the time of publication of this Framework, a particular challenge for implementers of smartcard systems is that it is not yet technologically possible to achieve interoperability across the range of different contact and contactless formats. This problem is largely a function of the incompleteness of standards and the divergence in card form factors that is inevitable at this stage in the evolution of the technology. The Framework acknowledges this fact, and that it will take time for the industry to achieve full interoperability, particularly across form factors. The supporting material aims to help agencies through this period by flagging particular interoperability pitfalls, and by promoting interoperability within and between deployments in the short to medium term through the work of the CoPs.

### 4.1.4 Establishing interoperability

All Australian governments recognise the need for smartcard deployments to be interoperable where appropriate.

A decision by an agency to introduce smartcard technology can represent a significant investment in both time and money. Long-term and short-term problems, both within and across jurisdictions, can occur if an individual agency proceeds without appropriate consideration of broader issues.

Conceptually, interoperability is best achieved through the use of standards. With complex technologies, however, setting standards involves a sometimes difficult balancing act between global and national interests in interoperability and uniformity, and local interests in flexibility, autonomy and containing direct costs. Moreover, international smartcard standards are still evolving, and there is ongoing migration of proprietary or private standards into the public domain. Finally, the Australian system of government and public administration recognises the benefits that flow from a federal system and, in the case of the Australian Government, a devolved governance structure.

As a result of these factors, interoperability is best achieved, in the short to medium term, through placing responsibility on CoPs. While CoPs are responsible for establishing the appropriate level of interoperability, all governments have agreed that they will comply with the requirements of the Framework, except where the business requirements within a jurisdiction indicate that adaptation may be required.

### 4.1.5 Interoperability with other sectors of the economy

Today's multi-application-capable smartcards represent flexible computing resources that can, in principle, be re-used beyond their respective issuing agencies in a variety of ways, with significant savings in cost, time and end-user overheads. Additional data and/or applications could be loaded onto cards for new business purposes, provided they do not unduly interfere with the

issuer's original objectives. Further, data can sometimes usefully be shared between old and new applications - subject, of course, to privacy considerations discussed in detail elsewhere in this Framework. Also, with careful coordination between agencies, it may be possible for certain card applications to be shared, or put to use with differing back-end systems.

Smartcard deployments within agencies that involve financial applications should also look at interoperability with commercial banking systems, especially via the Europay, MasterCard and VISA (EMV) specification. Business agreements may need to be established for public and private applications to comply with both the financial and government smartcard requirements.

## 4.2 Standards and policies

This Framework relies on existing and emerging standards at the international and Australian levels. In this section, the standards that are particularly important to creating interoperability between smartcard deployments are listed. This is not an exclusive list. Technical architects involved in designing smartcard schemes should become familiar with these standards as a minimum. In addition there may be other standards that are relevant to the business requirements, information structure or technical solutions that need to be understood and applied.

The following figure illustrates the relationship between these standards and government programs.

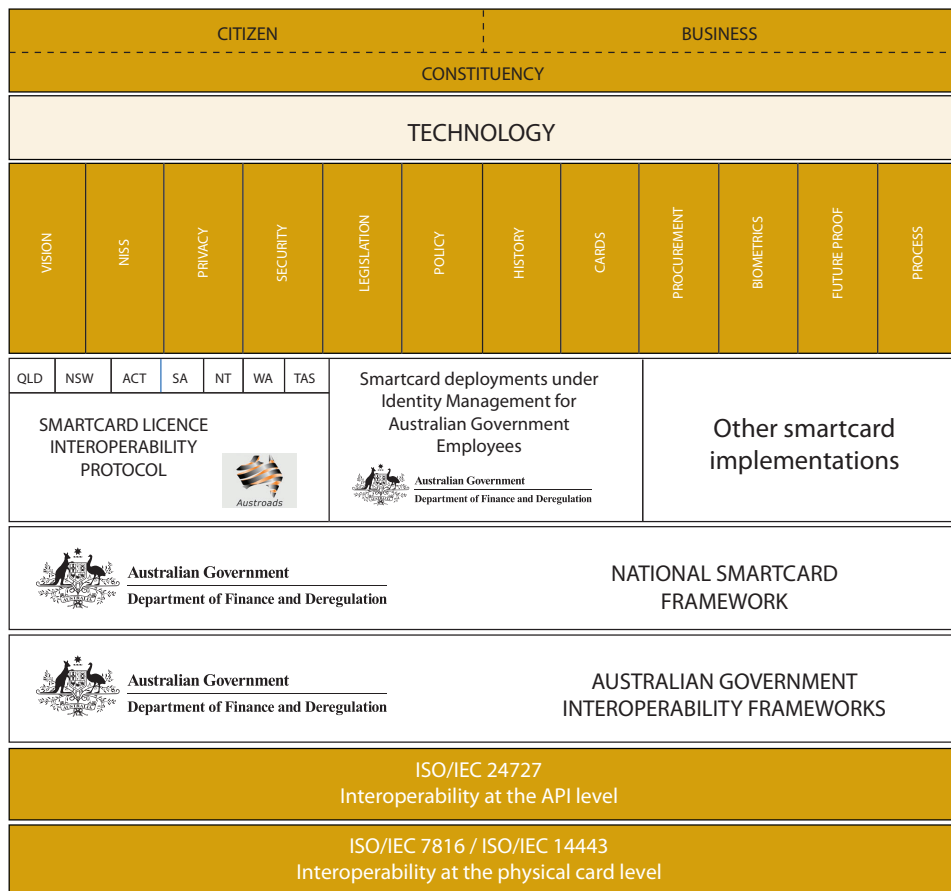


Figure 6: Agency program framework

## 4.2.1 International standards

This Framework adopts the following specific ISO/IEC smartcard standards:

1. ISO/IEC 7816 Identification cards -- Integrated circuit(s) cards with contacts
2. ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards
3. ISO/IEC 24727 Identification Cards -- Integrated circuit card programmin interfaces

Note that there are a number of other international standards that are referenced by these standards or are relevant to a particular industry, but it is not within the scope of this Framework to discuss every international standard.

Name of standard	Description
ISO/IEC 7816: Identification cards -- Integrated circuit cards with contacts	<p>The standard focuses predominantly on smartcards. It describes the physical aspects, such as the location of the ICC contacts, and low-level communication and commands for cards. There are 15 parts:</p> <ul style="list-style-type: none"> <li>• Part 1: Physical characteristics</li> <li>• Part 2: Dimensions and location of the contacts</li> <li>• Part 3: Electronic signals and transmission protocols</li> <li>• Part 4: Organisation, security and commands for interchange</li> <li>• Part 5: Registration of application providers</li> <li>• Part 6: Inter-industry data elements for interchange</li> <li>• Part 7: Inter-industry commands for Structured Card Query Language (SCQL)</li> <li>• Part 8: Commands for security operations</li> <li>• Part 9: Commands for card management</li> <li>• Part 10: Electronic signals and answer to reset for synchronous cards</li> <li>• Part 11: Personal verification through biometric methods</li> <li>• Part 15: Cryptographic information application.</li> </ul>
ISO/IEC 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards	<p>The standard describes two types of contactless smartcards, type A and type B. It describes the physical requirements for contactless cards including radio frequencies. There are four parts:</p> <ul style="list-style-type: none"> <li>• Part 1: Physical characteristics</li> <li>• Part 2: Radio frequency power and signal interface</li> <li>• Part 3: Initialisation and anti-collision</li> <li>• Part 4: Transmission protocol.</li> </ul>

Table 2: Description of international standards - continued on next page

Table 2 continued: Description of international standards

Name of standard	Description
<p>ISO/IEC 24727: Identification cards - - Integrated circuit card programming interfaces</p>	<p>This draft standard is a set of programming interfaces for interactions between integrated circuit cards and external applications to include generic services for multi-sector use.</p> <p>The standard can be used by implementations desiring interoperability among diverse application domains.</p> <p>This standard is consistent with ISO/IEC 7816 and ISO/IEC 14443 and aims to provide clarity for implementations seeking interoperability.</p> <p>There are six parts:</p> <ul style="list-style-type: none"> <li>• Part 1: Architecture</li> <li>• Part 2: Generic card interface</li> <li>• Part 3: Application interface</li> <li>• Part 4: Application Programming Interface (API) administration</li> <li>• Part 5: Testing procedures</li> <li>• Part 6: Registration authority procedures.</li> </ul>

## 4.2.2 Australian Government standards

The Framework interacts with a number of other frameworks and standards which have been developed for use in the Australian Government context and should be considered in conjunction with these.

Please note that not all Australian Government standards are used by other jurisdictions. In some cases, jurisdictions may have adapted or merely recognised the Australian Government standards as useful guidance documents.

The major interactions are listed in the table below.

Name	Description
National e-Authentication Framework (previously known as the Australian Government e-Authentication Framework)	<p>This framework aims to provide enhanced confidence in electronic dealings between Australian governments and their clients, whether they are individuals or businesses by:</p> <ul style="list-style-type: none"> <li>• enhancing privacy of personal information stored or transmitted in relation to their electronic dealings</li> <li>• ensuring minimum levels of conduct in relation to their electronic dealings</li> <li>• ensuring a fitness-for-purpose approach that matches authentication approaches to the underlying risk of transactions, and encompasses consideration of privacy and public policy, logistical, usability and economic factors</li> <li>• facilitating consistency in authentication approaches across agencies and jurisdictions to increase efficiency</li> <li>• facilitating interoperability to enable: <ul style="list-style-type: none"> <li>- re-use of credentials</li> <li>- sharing of infrastructure and solutions</li> <li>- extensibility of authentication schemes.</li> </ul> </li> </ul> <p>This framework is managed by AGIMO and is available from &lt;<a href="http://www.gatekeeper.gov.au">www.gatekeeper.gov.au</a>&gt;.</p>
Gatekeeper PKI Framework	<p>This is the Australian Government's strategy for the use of public key infrastructure (PKI) as a key enabler for the delivery of online government services.</p> <p>This framework is managed by AGIMO and is available from &lt;<a href="http://www.finance.gov.au">www.finance.gov.au</a>&gt;.</p>

---

Identity Management for Australian Government Employees (IMAGE)

IMAGE offers better practice guidance on identity management for Australian Government employees and contractors. It outlines the “look and feel” of a standardised government staff identity card, which may be a smartcard. The aim of IMAGE is to increase trust, improve interoperability and enhance mobility for public sector employees.

This document is managed by AGIMO and is available from <[www.finance.gov.au](http://www.finance.gov.au)>.

---

Australian Government Interoperability Framework

This framework addresses the information, business process and technical dimensions of interoperability in the Australian Government and sets the principles, standards and methodologies that support the delivery of integrated and seamless services. The components are:

- at the business layer, National Service Delivery Improvement Strategy and Business Process Interoperability Framework
- at the information layer, National Information Sharing Strategy (currently being developed) in conjunction with Information Interoperability Framework
- at the technical layer, Technical Interoperability Framework.

This framework is managed by AGIMO and is available from <[www.finance.gov.au](http://www.finance.gov.au)>.

---

National Identity Security Strategy (NISS)

The key objectives of the strategy are:

- improving standards and procedures for enrolment and registration for the issue of proof of identity documents (PoI)
- enhancing the security features on PoI documents to reduce the risk of incidence of forgery
- establishing mechanisms to enable organisations to verify the data on key PoI documents provided by clients when registering for services
- improving the accuracy of personal identity information held on organisations’ databases
- enabling greater confidence in the authentication of individuals using online services
- enhancing the national interoperability of biometric identity security measures.

The National Identity Security Strategy is available from the Attorney-General’s Department at <[www.ag.gov.au](http://www.ag.gov.au)>.

---

---

Protective Security Manual (PSM)

The PSM is designed to assist agencies with their protective security arrangements, and includes principles, standards and procedures for the protection of government personnel, infrastructure and information.

The purpose of the minimum standards prescribed in the PSM is to facilitate and promote a consistent approach to security across all agencies.

Access to the PSM is restricted to government agencies. Agencies may provide engaged contractors with the sections of the PSM required to meet contractual obligations.

For all inquiries regarding the PSM, please email <[psm@ag.gov.au](mailto:psm@ag.gov.au)>.

---

Australian Government Information and Communications Technology Security Manual (ISM)

ISM provides policies and guidance to Australian Government agencies on how to protect their ICT systems.

Australian Government agencies are required by the PSM to comply with ISM. Agencies shall consider the security implications of their ICT systems and devise policy and plans to ensure the systems are appropriately protected.

The ISM is available from the Defence Signals Directorate at <[www.dsd.gov.au](http://www.dsd.gov.au)>.

---

### 4.2.3 Industry and vendor standards

There are many independent developments of smartcard platforms and standards by vendors and industry. It is difficult to list all developments around the world. Some platforms that are widely known throughout the world are<sup>1</sup>:

1. GlobalPlatform
2. Java Card
3. MULTOS
4. Federal Information Processing Standard (FIPS 201) and Personal Identity Verification of Federal Employees and Contractors (PIV)

#### GlobalPlatform

GlobalPlatform provides a suite of smartcard specifications, together with market and application-specific configurations. The entire smartcard infrastructure is covered: cards, devices and systems. These technical documents offer a dynamic and complete technology platform for the development of smartcard programs.

GlobalPlatform also makes available test plans, suites and tools for self-testing of products for compliance to the GlobalPlatform Specifications.

More information on GlobalPlatform can be found at [www.globalplatform.org](http://www.globalplatform.org).

#### Java Card

Java Card technology is a leading open, interoperable smartcard platform that enables smartcards and other resource-constrained devices to securely run Java technology-based applications. Java Card supports cross-platform and cross-vendor applet interoperability of multiple communication interfaces, each capable of running with independent co-resident applications. More information on Java Card is available from Sun Microsystems at [java.sun.com/javacard](http://java.sun.com/javacard).

#### MULTOS

MULTOS is a smartcard operating system that allows multiple software applications to reside separately and securely on a smartcard. The operating system isolates each application so they do not interfere with each other.

To ensure its openness and to further advance its adoption into all smartcard-related markets, the control of the MULTOS specification is contractually invested in the MULTOS Consortium. The MULTOS Consortium is a group of international blue chip organisations whose objective is to promote MULTOS as the smartcard industry standard across all market sectors.

More information on MULTOS can be found at [www.multos.com](http://www.multos.com).

---

<sup>1</sup> This section on vendor-specific technologies does not indicate any endorsement or recommendation of the technology by the Department of Finance and Deregulation or the Australian Government. Government agencies shall still adhere to their procurement requirements when selecting a vendor.

## FIPS and PIV

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the US Department of Commerce. NIST is the primary US Federal agency responsible for the deployment of government standards for the US Government. Some NIST standards are recognised worldwide, such as the FIPS suite of standards, which includes important identity and smartcard standards; namely the PIV standard.

The PIV Standard consists of:

- NIST Special Publication 800-73: Interfaces for Personal Identity Verification
- NIST Special Publication 800-76: Biometric Data Specification for Personal Identity Verification
- NIST Special Publication 800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification.

Another NIST publication that is particularly relevant to smartcard deployments is:

- NIST Special Publication 800-53: Cryptographic Modules.

More information on NIST and PIV is available at <[www.csrc.nist.gov](http://www.csrc.nist.gov)>.

### 4.2.4 Interoperability standards developed by existing CoPs

There are a number of programs that set requirements for specific smartcard environments:

- The International Civil Aviation Organisation (ICAO) has established the requirements with respect to e-Passports
- The Smart Licence Interoperability Protocol (SLIP) working group has set interoperability requirements for driver licences; and
- The National Transport and Ticketing Working Group of the Australian Transport Council (ATC), a coalition of public transport ticketing operatives within the six state governments, has developed an open-architecture standard for contactless smartcard transit ticketing.

Agencies need to consider the implications of these specifications, where appropriate, when developing their requirements.

### 4.3 Interoperability under ISO/IEC 24727

The ISO/IEC 24727 standard allows for its components to interact with and be deployed in various combinations, known within the ISO/IEC 24727 standard as “stack models”. The ISO/IEC 24727 components that make up the stack models are described in more detail in the Implementation Models and Checklists that accompany this Framework.

While ISO/IEC 24727 has been developed to facilitate interoperability of smartcards, there are many different stack models that can be selected. In order to actually achieve interoperability, a CoP will need to select the most appropriate stack model for their deployment.

## 5 Functional considerations

There are a number of functional considerations that are specific to smartcard deployments that should be considered when designing the technical solution. One tool that will assist CoPs to develop deployments that can interoperate within the CoP or with other CoPs are Framework Implementation Specifications (FIS), which are introduced below.

Functional considerations that should also take precedence when developing the smartcard deployment include specific requirements that arise from the smartcard lifecycle, the issues surrounding the chain of trust required to ensure the integrity of the smartcard, and security and protection - particularly relating to authentication protocols.

This section introduces these considerations and points the technical architect to sources of further information.

### 5.1 Framework Implementation Specifications (FIS)

In order to achieve interoperability between implementations within and between CoPs, it is important for them to document the functional components of the system and make these specifications available to other members of their CoP. This will allow other agencies to determine how the system has been designed and to develop their applications in accordance with the specifications. This document introduces the concept of FIS as explicit specifications that describe a set of generic functional requirements.

The benefit of FIS is that any application developed from them should be distinctly recognisable by other applications and/or cards, therefore facilitating interoperability and also increasing the potential for applications to be re-used across smartcard schemes.

FIS should be modular to allow each CoP to determine the touchpoints where interoperability is required within and across that community.

FIS will be developed by agencies implementing a smartcard and are separate from this Framework. To facilitate sharing with members of the CoP, card authorities are encouraged to provide a copy of their FIS to AGIMO so that they can be made available to other CoPs through a secure website.

#### 5.1.1 Management of FIS

AGIMO will develop a management strategy for FIS that will be available at <http://www.finance.gov.au/>.

The strategy will be based on an electronic library where FIS will be offered for re-use and be made available to appropriate potential users once they have registered their interest with AGIMO. The protection of intellectual property rights of the creator of the FIS will be the responsibility of the FIS developer. AGIMO's responsibility is to maintain a repository for the publication of each FIS.

### 5.1.2 FIS functional requirements

All FIS shall meet the following functional requirements as a minimum. A FIS shall:

- be capable of being implemented within smartcard systems complying with this Framework
- not rely on a specific card-operating system
- ensure that all edge interfaces external to a FIS application shall be:
  - defined in other FIS
  - definable via the ISO/IEC 24727-3 API
  - defined as ISO/IEC 24727-2 commands at the GCI.
- ensure that any complying FIS applications shall be capable of being discovered when implemented on smartcards complying with ISO/IEC 24727-2 and 3 (in order to simplify application discovery); and
- ensure that all FIS specifications should be interface-neutral, wherever possible. This is dependent upon sufficient time being available for the card to complete the transaction. It is expected that some applications will specifically require either contact or contactless cards due to practical operational requirements.

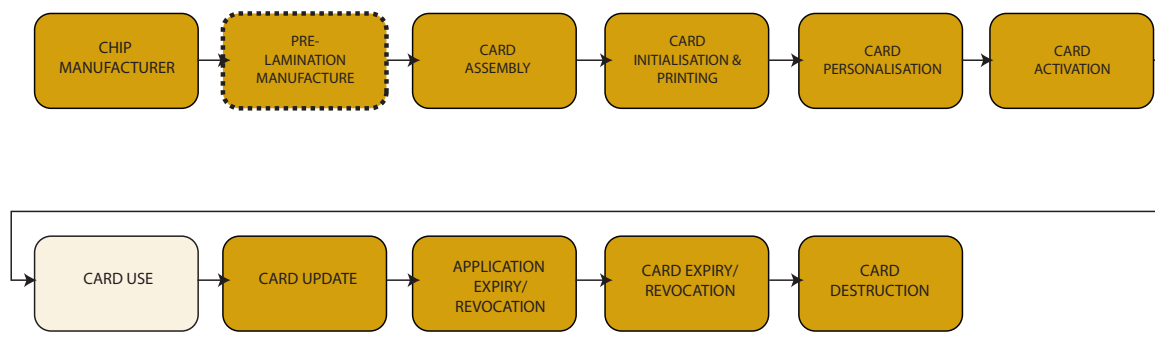
### 5.1.3 Further information on FIS

Further information on the current status of FISs will be available at <http://www.finance.gov.au/e-government>.

## 5.2 Card lifecycle considerations

Processes shall be developed by the CoP and put in place to ensure the integrity of any changes to the smartcard at any point in its lifecycle. The lifecycle of a smartcard can be broken down into four parts:

- acquisition of custom cards
- card personalisation and activation
- change of functionality
- card revocation



CARD LIFECYCLE MODEL

Figure 7: Smartcard lifecycle model

A typical smartcard lifecycle model is depicted above. The lifecycle phases are as follows:

- Chip manufacture - creation of the chip or chip module at a “silicon foundry”. Post-processing at the foundry might include the embedding of unique chip IDs and cryptographic keys or passwords used to deny unauthorised access to the chips during transport to a card assembler
- Pre-lamination manufacture - for contactless cards, the chip or chip module is typically embedded in a “pre-laminate”, which also carries the antenna, the latter bonded to the chip module. Pre-laminate manufacturers may operate independently of chip makers and card assemblers, and should not require security access to the chip contents
- Card assembly - embedding of the contacted chip module or contactless pre-laminate in the final smartcard carrier. Bulk printing may occur during this phase, or be deferred until card initialisation. Other surface features, such as signature panels and optical security devices, may be applied at this stage. Card assemblers should not require security access to the chip contents
- Card initialisation and printing - the next lifecycle phase typically involves electronic initialisation or loading of the smartcard chip memory with initialisation data and loadable on-card applications. Keys may also be generated or injected at this point, and the initialisation process may also include printing
- Card personalisation - as the next step before the card is transferred to the cardholder, personal data or ID-related printing may be applied to the card. Note that initialisation and personalisation may be subsumed in the one operation
- Card activation - depending on the card system’s issuance requirements, the card may require to be presented to the system for final activation before normal use is permitted. A back-end database entry may also be used to activate the card
- Card use - cardholder use of the card in the intended business processes

- Card update - in some systems, the card contents will be updated through a distinct card management process. This might include loading of new applications, certificates or keys, or the revocation of old ones
- Application expiry/revocation - on-card applications may have an explicit expiry date or may be revoked before expiry is reached. In a multi-application environment, one application may be revoked or expire independently of other applications. Temporary application suspension may also be used as an administrative measure
- Card expiry/revocation - cards may have an explicit expiry date or may be revoked or temporarily suspended by the system before expiry is reached. Due to the finite data retention period of some types of card memory (Flash and Electrically Erasable Programmable Read-Only Memory (EEPROM), it is desirable that cards be removed from circulation before they fail through natural attrition (such failure may result in unpredictable behaviour). Project planners shall consider how expiry, revocation and suspension can best be used in the specific project context. Likewise, they shall decide which of these processes will involve a card-access operation as distinct from a back-office administrative action.
- Card destruction - even where a card has been electronically deactivated, some deployments will require that revoked cards be destroyed; for example, to prevent unauthorised parties masquerading as an authorised stakeholder using the card graphics, noting that it is infeasible to enforce the destruction requirement for lost or stolen cards. Defective or wasted card stock shall be destroyed to prevent misuse.

### 5.3 The chain of trust

The chain of trust in a smartcard deployment is essential to ensure the integrity of the card. It represents the management of the card in the initial stages of the card's lifecycle, from the different stages in the manufacture, through to loading applications and data onto the chip and issuing to the correctly registered user.

One of the most crucial requirements for any smartcard implementation is to achieve adequate binding between the various elements which make up the chain of trust in the credential. The "links" within this chain of trust will depend on the nature of the smartcard. For example, for smartcard schemes that rely on verifying the identity of a cardholder, binding should be to the "commencement of that identity", i.e. an event such as birth or citizenship, and the document that relates to the particular event.

The issue of binding a person to the chain of trust via some form of registration process and associated business rules has not been addressed in the Framework. CoPs are directed to their own jurisdictions and cross-jurisdictional requirements in determining what is required in this regard.

CoPs shall develop processes that will ensure the chain of trust when designing their smartcard deployment. Further guidance on the chain of trust can be found in the Implementation Models and Checklists and the Smartcard Project Design Guide at <http://www.finance.gov.au/e-government/security-and-authentication/smartcard-framework.html>

## 5.4 Security and protection requirements

Smartcards allow a range of cryptographic protections to be designed into any particular card and system. These can range from no protection at all, to extremely strong symmetric, asymmetric or even custom algorithms. This Framework does not recommend the use of custom algorithms but requires that CoPs shall define an appropriate mix of protections so that their deployment is fit for purpose.

As part of their risk threat plan, CoPs should consider the following security and protection possibilities:

- unauthorised knowledge of asymmetric private keys
- unauthorised knowledge of chip symmetric keys
- authentic trusted asymmetric keys
- unauthorised knowledge of secure messaging (session) keys
- logical chip data has not been changed
- access to protected data; and
- key management and key distribution requirements.

Further guidance on these issues can be found in the Smartcard Project Design Guide.

# Appendix 1: Acronyms

AGA	Australian Government Architecture
AGIF	Australian Government Interoperability Frameworks
AGIMO	Australian Government Information Management Office
ALGA	Australian Local Government Association
ATC	Australian Transport Council
AWG	Authentication Working Group
CIOC	Chief Information Officer Committee
CoI	community of interest
CoP	community of practice
EEPROM	Electrically Erasable Programmable Read Only Memory
EMV	Europay, Mastercard and Visa
FIPS	Federal Information Processing Standard
FIS	Framework Implementation Specifications
ICAO	International Civil Aviation Organisation
ICC	Integrated Circuit Card
ICT	information and communication technology
IEC	International Electrotechnical Commission
IMAGE	Identity Management for Australian Government Employees
ISM	Australian Government Information and Communications Technology Security Manual
ISO	International Standards Organisation
IT	information technology
ITSO	Integrated Transport Smartcard Organisation
NeAF	National e-Authentication Framework
NFC	Near Field Communication
NISS	National Identity Security Strategy
NIST	National Institute of Standards and Technology (US)
NSF	National Smartcard Framework
NQDL	New Queensland Driver Licence
OCC	Online and Communications Council
OVD	optical variable device
PIN	personal identification number
PIV	Personal Identity Verification
PKI	public key infrastructure
PoI	proof of identity
PSM	Protective Security Manual
RMP	risk management plan
RTP	risk treatment plan
SAM	Secure Access Modules
SCQL	Structured Card Query Language
SIM ID	Subscriber Identity Module Identification
SLIP	Smart Licence Interoperability Protocol
SRG	Smartcard Reference Group
WGA	Working Group on Authentication