



Australian Government

Department of Finance and Deregulation

Australian Government Information Management Office

National Smartcard Framework



December 2008

**Implementation Models
and Checklists**

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

Contents

1	Introduction	2
1.1	Industry Sectors/Usage Models	2
1.1.1	Banking & Commercial	3
1.1.2	Public Transport & Road-Related Usage	4
1.1.3	Access Control	6
1.1.4	Identity Credentials and Border Control	7
1.1.5	Health & Human Services	7
1.1.6	Education Sector	8
1.1.7	Telecommunications	8
2	Some Model Building Block Decisions	9
3	Deployment Framework	14
3.1	General	14
3.2	Design & Operational Verifications	16
4	Community of Practice Checklists	18
4.1	Environmental Scan	14
4.2	Developing Terms and Conditions for a CoP	19
4.3	New CoP entrant to an established CoP	20

1 Introduction

The Australian Government Information Management Office (AGIMO), within the Department of Finance and Deregulation (Finance), fosters the efficient and effective use of information and communications technology (ICT) by Australian Government departments and agencies. AGIMO provides leadership in defining and driving government-wide ICT strategy, standards and technical architecture.

The National Smartcard Framework (the Framework) is one of a number of frameworks and strategies developed to support interoperable whole-of-government business applications. The Framework should be read in conjunction with other Australian Government frameworks, including the Attorney-General's Department's National Identity Security Strategy, AGIMO's Australian Government Interoperability Framework, National e-Authentication Framework, Better Practice Guide to Authorisation and Access Management, and the Gatekeeper PKI Framework (for use where public key technologies are implemented with smartcards).

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

- Smartcard Handbook
- Implementation Models and Checklists (this document)
- Smartcard Project Design Guide
- Case Studies, and
- Framework Implementation Specifications (FIS).

It is expected that case studies will be provided by Communities of Practice (CoP) as smartcard deployments occur. These supporting documents will be available at <http://www.finance.gov.au/e-government/>

1.1 Industry Sectors/Usage Models

Smartcard system planners should decide which industry models apply to their specific requirements. Figure 1 below provides a representative depiction of these models¹.

¹ Only a sampling of the boxes shown in Figure 1 are expanded in the text

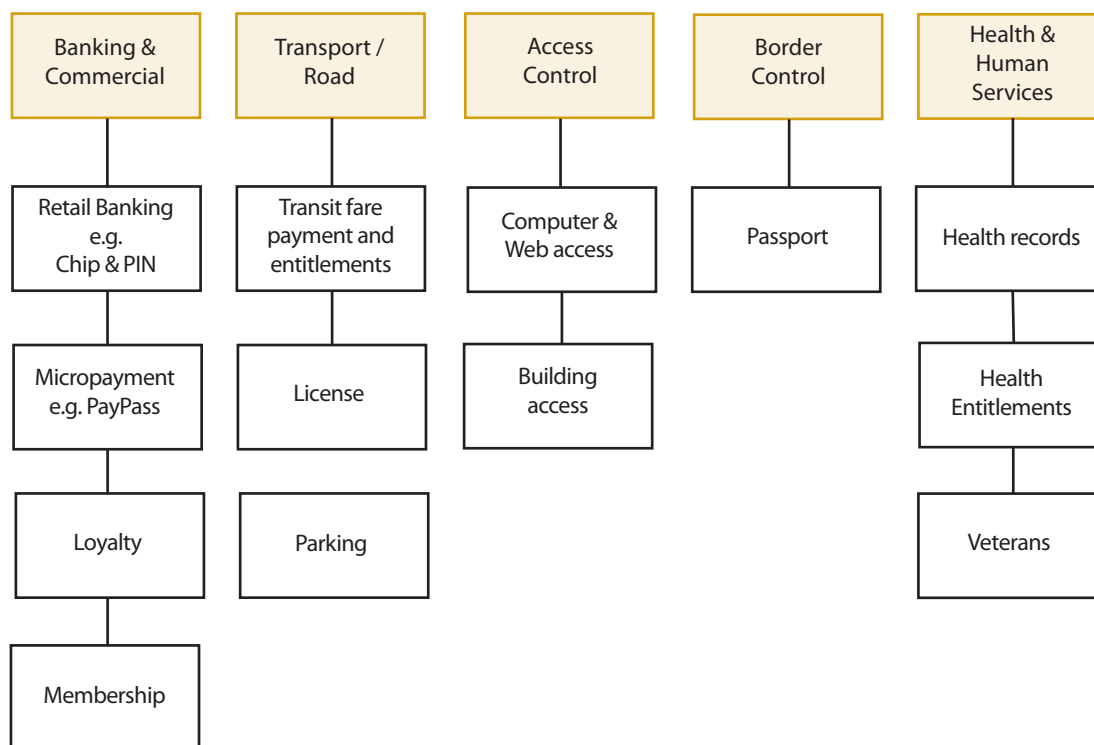


Figure 1: Industry Sector Models

1.1.1 Banking & Commercial

Banking and commercial cards system models serve as useful examples rather than specific models for e-Government in Australia. Applications of this type include Chip and PIN for debit and credit cards used in retail banking, the best example being the EuroPay, MasterCard VISA (EMV) specifications.

Contactless micro-payment models using EMV components have also entered the market relatively recently, the primary examples being PayPass (MasterCard), payWave (Visa) and ExpressPay (American Express).

Some important aspects of the banking smartcard model may be relevant to e-Government smartcard system design²:

- a strong and clearly bounded community of interest
- potential world-wide interoperability, with regional card issuers operating at a tier below the peak issuing body

² This is not an exhaustive list

- the peak issuer not issuing cards per se, but providing multiple services including specification and compliance management, business rules, operational oversight, transaction switching, and international hosting
- achieving front-end interoperability in part by mandating low level ISO physical, electrical and logical interface standards
- the development of a comprehensive peer-reviewed technical design, including security architectural models
- the use of purpose built secure reader-terminals, and the consequent need to secure the reader issuance processes as well as card issuance processes
- the enforcement of an approved evaluation program for readers, and the conduct of rigorous audits over participating issuers
- due to market size, the availability of multiple smart card chip suppliers targeting the same application; and
- outsourcing of bulk issuance to trusted third parties.

1.1.2 Public Transport & Road-Related Usage

Public transport and road-related smartcard models expand into multiple sub-models to meet different policy and business requirements

Transit

Internationally, transit smartcard schemes for automatic fare collection and concessional travel are largely but not exclusively government-sponsored. Some important aspects of this model (each scheme will implement important variants) include the following:

- a clearly bounded CoP (government and transport providers) at inception, but with potential to embrace additional applications, for example, commercial rights extensions that may be unique to each transit scheme owner
- the potential for regional interoperability (e.g. ITSO in the UK) but also demonstrating where commercial and delivery timeline imperatives may mitigate against early interoperability between separate projects
- use of low level ISO/IEC standards to achieve card to reader compatibility, but in contrast, the likely use of significant proprietary back-end software elements
- the ability to deliver a rich service set with low-end chips
- the existence of complex interactions between issuers, service providers and cardholders

- the potential outsourcing of issuance processes to trusted third parties
- issuance of cards to children as well as adults
- support for both anonymous and personalised cards, determined by cardholder preferences and use-case needs
- the use of purpose-built reader terminals to meet performance and operator functionality criteria
- the use of embedded Security Application Modules (SAMs) to protect card keys in front-end devices
- the almost exclusive use of symmetric cryptographic keys for card access; and
- the need for transition planning from older technologies (paper and magnet tickets) to chip-based technologies.

Driver Licences

Smartcard system models for driver licences incorporate important features such as the following:

- high integrity cardholder enrolment and issuance processes, including need for strong evidence of identity
- strong policy guidelines concerning use of cards for purposes other than driver credential
- robustness of card electronic and graphical security features (including anti-cloning and anti-counterfeiting measures) crucial to the viability of business cases
- graphical elements that provide first-level credential verification capability in the absence of the ability to interrogate the card chip
- the possibility of carrying a digital cardholder photo in addition to or in place of a printed photo
- potentially, the need for different access rights to on-card electronic data for different parties
- attractive environment for the use of Public Key methods for card authentication and access control; and
- the ability to read the card at 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.

1.1.3 Access Control

An important current and future use of smart cards in the Australian e-Government context is for computer and building access control. Key aspects of such usage models are outlined below.

Agency Computer Access Control

- targeted at both local workstation and remote computer access
- operates in support of and in conjunction with potentially complex infrastructures
- strong unique two-factor (card plus e.g. password or Personal Identification Number (PIN)) authentication is the generally preferred model
- authentication processes must be closely coupled with and enabled by an authorisation system which defines permitted access to applications and data on an individual cardholder basis
- system must have effective suspension, reactivation and revocation mechanisms both at authorisation and authentication levels. This must include a help-desk for the reporting of lost and stolen cards
- in some cases, complex transition plans are required for migration from older authentication schemes
- a sophisticated card management system is likely to play a central role in card issuance
- identity management subsystems incorporating photo-capture are likely to be part of the system design
- middleware is likely to play a significant role in interfacing on-card applications to system capabilities
- certificate-based public key cryptographic methods are highly suited to card authentication processes; and
- card graphics may play a significant supplementary security role.

Agency Building Access Control

Some important aspects of this card usage domain are as follows:

- building access authentication
- readers may be under video surveillance

- access control authentication methods can vary across a broad spectrum of cryptographic capability with advanced methods being rare and costly to implement
- card graphics (photos, colour-coding of access rights) are likely to play a significant supplementary security role to building access authentication
- back-end infrastructure including door access controllers is likely to be specific to the application and proprietary to a given vendor; and
- as with computer access, a building access smartcard system must have effective suspension, reactivation and revocation mechanisms. This includes a help-desk for the reporting of lost and stolen cards.

1.1.4 Identity Credentials and Border Control

Some important aspects of this card usage domain are as follows:

- the requirement for very clear policy guidelines for data collection, use and destruction, and for any supplementary use of the identity token or smartcard instrument
- the need to determine if the smartcard instrument constitutes legal proof of identity, or is only evidence of identity to be weighed with other factors in identity verification
- 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 co-operation, 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 on-line revocation database; and
- the potential requirement for granting different access privileges to different data fields or memory areas on the card chip.

1.1.5 Health & Human Services

There are various potential uses of smartcards for the delivery of health care and other human services within e-Government. Some important aspects of this card usage domain are as follows:

- the requirement for very clear policy guidelines for data collection, use and destruction, as well as for approved card usage
- the requirement for a high-integrity enrolment and cardholder database management program
- the need for very strong card anti-cloning and anti-counterfeiting controls
- the need for strong anti-fraud measures at business process level due to use of cards to facilitate money transfers
- the potential requirement for granting different access privileges to different data fields or memory areas on the card chip
- the potentially strong benefit from the use of Public Key methods to authenticate and protect access to card information or to back-end information, predicated on the presentation of the card; and
- the possibility of coupling health sector cards to funds transfer processes (payments of prescribed fees and making of service-related Electronic Funds Transfer (EFT) payments).

1.1.6 Education Sector

Smartcard applications already exist in some countries for student attendance cards, library borrowers' cards, and limited stored-value cash replacement purses for the purchase of on-campus services. Campus applications are sometimes seen as a good match for co-issuance with the public transport sector.

1.1.7 Telecommunications

The largest single smartcard chip application around the globe is for Global System for Mobile communications (GSM) mobile phone Subscriber Identity Modules (SIMs). While government is unlikely to become an issuer of SIMs, the rapid growth of mobile payment and related applications based on multi-application SIMs and the emergence of Near Field Communications (NFC) technology are strong predictors of the role of the mobile phone as a smartcard substitute. Smartcard system planners should be aware of the potential uses of this technology, as well as the many issuance questions that will arise if it is adopted for an e-Government application.

2 Some Model Building Block Decisions

There are few examples of 'one size fits all' approaches within industry sectors, let alone across differing applications within an industry sector. Figure 1-2 depicts in schematic form a range of significant decision continuums and dichotomies facing smartcard system planners and designers. This discussion serves mainly to alert system planners to issues needing to be considered during the early planning phases of a project.

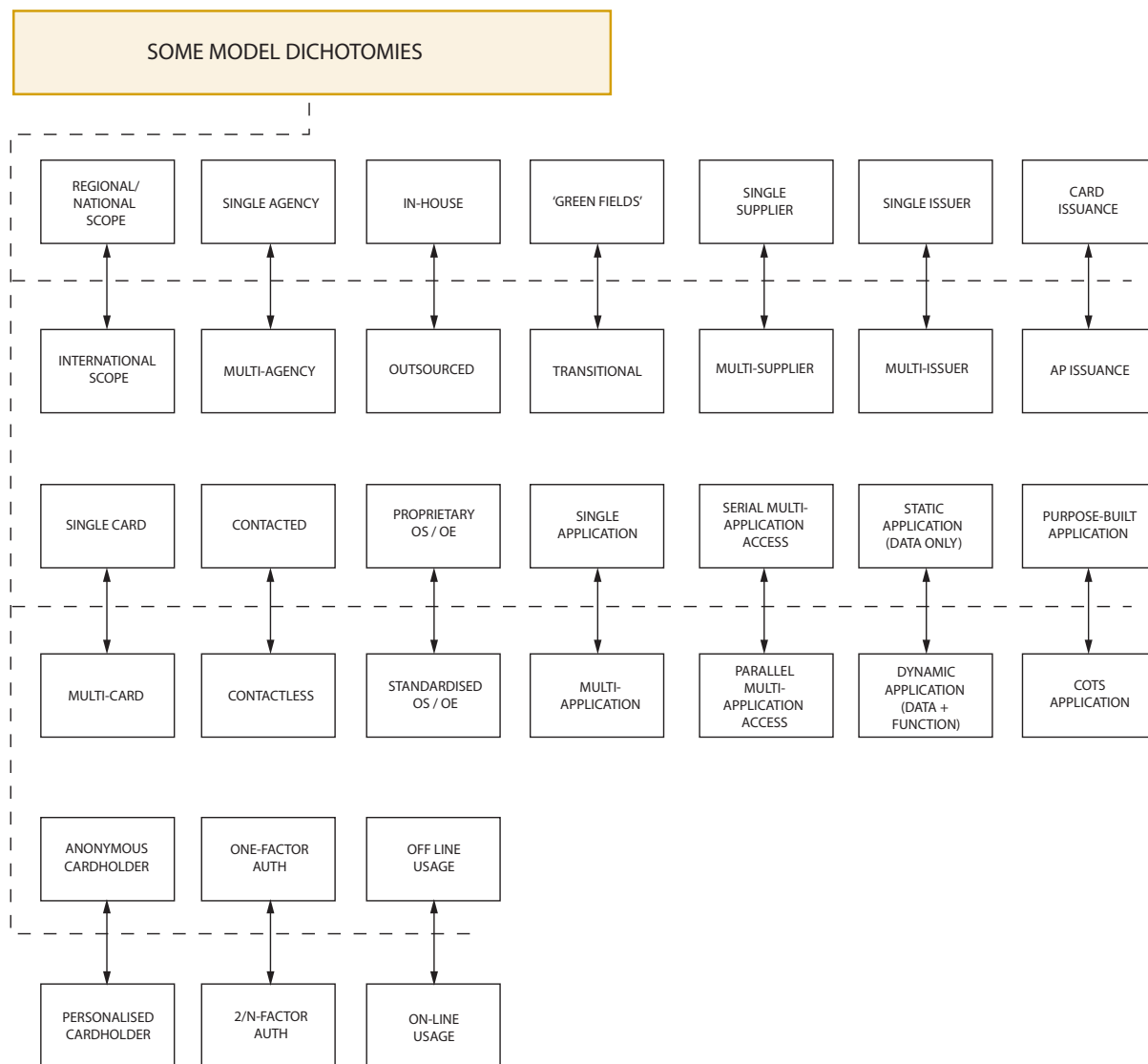


Figure 2: Decision Spectra

- Regional, National, or International Scope - different smartcard deployments will have differing geographical aspirations. Some, such as in-house state government departmental use, will be entirely regional. Transit smartcard schemes may be regional, or may aspire to multi-region or national interoperability. Other deployments – for example border control – may aspire to international interoperability.
- Agency Scope - an agency must determine whether its solution is destined for internal use only or whether some degree of interoperability with other agencies is necessary, desirable, and viable. Experience in Australia and elsewhere suggests that the broad objective of federated card usage can become significantly complicated once detailed design decisions about data definitions, data sharing and the allocation of access rights need to be taken. That is, the benefits of a federated approach are more likely to be apparent at the conceptual stage, while the costs of such an approach may only be revealed at detailed technical consultation stage.
- Service Source – a rigorous cost-benefit analysis must be completed before a decision can be taken to outsource all or part of a given smartcard deployment. Outsourcing of card issuance and long-term management may be commercially attractive for a large cardholder base, but prohibitive for small rollouts. Security or privacy concerns may also mandate that services be delivered in-house even though it would otherwise be commercially attractive to outsource. Some projects will also require a mixed model: for example, outsourced bulk issuance and ad hoc in-house issuance.
- New and Legacy Systems – Some smartcard deployments are ‘green-field’ with no constraints arising from prior business practices. Many - for example computer access – may require integration of new card-based methods with older methods for a transitional period. This can be further complicated by the natural transition of other technologies within an agency. Smartcard planners may need to adapt deployment methods and milestones to a moving technical infrastructure baseline.
- Supplier Diversity – Compatible general-purpose technologies are usually available from multiple suppliers, but compatible purpose-specific technologies are less likely to be. Standardisation efforts such as ISO/IEC 24727 are seeking to remove this obstacle from smartcard interfacing, but specific use cases may still demand solutions only available from one, or a very limited number of vendors.
- The Issuer Dimension – Security applications within government are likely to involve a single smartcard issuer. However applications such as transit may attract multiple issuers. Transit provides an obvious example of multi-issuance where a transit operator may issue its own cards but also allow its transit application to be issued by a banking institution, most commonly co-branded with a traditional credit card application.
- Application issuance – Card system planners must also consider the dichotomies of card and application issuance, and in some cases such as biometrics, even the possibility of different issuers for different application elements (e.g. one party issuing the overall application business logic with another issuing biometric signal processing drivers). Security, liability and other factors will be inputs to the decision making and design process.
- Card Types – Many smartcard programs will issue a single card type, but some smartcard programs may find a significant benefit in issuing different cards for different purposes or

contexts. Card 'type' differences may be in the graphical design of card printing, chip type (e.g. limited use chips versus complex use chips), or chip carrier (standard ID-1 format versus SIM format versus various other packaging or embedding options).

- Card (and Reader) Interfaces – card system planners need to carefully consider the appropriateness of available card interfacing models. The primary dichotomy is between contactless and contacted interfaces (although dual interface cards will be applicable in some contexts). Inputs into the decision making process will include such issues as reader cost, reader integration within computer or terminal platforms, reader power consumption, reader operating environment and card life expectancy. In rare cases, an additional interface might be added to a card to allow their use with an agency's existing proprietary building access control readers.
- Card Operating Systems and Environments – on the surface, a decision to select a chip technology based on proprietary operating systems or operating 'environments'² may seem at odds with the general framework principles of seeking openness and contestability. However, there are clear instances, particularly in cost-sensitive arenas such as transit and dedicated building access control, where use of a card with standardised physical and electrical interfaces, but a purpose-specific operating system or environment, are warranted. It should also be noted that the ISO/IEC 24727 aims to render the question of operating system or environment irrelevant from the application programmer's perspective: the responsibility for the low level detail is shifted from the system implementer to the card and middleware vendor community.
- Single or Multi Application – smartcard system planners must determine whether their requirements fit within a single application or multi-application context. Clarity is needed regarding what is meant by the term 'application'. In differing schemes this may mean one or more of the following:
 - the software functionality of the smartcard
 - the software functionality of the terminal/reader; and
 - the overall service delivery context including front and back end-processes.

It is also important to note that a multi-application environment can be delivered:

- on one card type or on multiple card types
- on a single card through the use of separate or overlapping datasets contained within the same (non-firewalled) files or memory structures and sharing the same access control variables (keys, PINs passwords etc)
- on a single card using firewalled logical or physical partitions; and
- on a single card with one card data set but variable terminal/reader behaviour based on business context.

Planners must therefore make multiple functionality, and cost-benefit decisions before arriving at a design solution.

Transit system designers for example, may select the second approach above with application segregation provided by terminal business rules only, whereas a government agency implementing an access control program would be more likely to select the third approach because of the level of cryptographic or access-controlled firewalling demanded by the project threat and risk assessment.

It is important to acknowledge that where an agency has a single specific purpose for a smartcard deployment, that a single application design may be much more cost effective approach than embedding the single application in a multi-application design. Nonetheless, as multi-application cards and middleware become more pervasive, the cost benefit gap may narrow significantly.

- **Atomic or Co-dependent Multi-Applications** – Multi-application system planners must decide on the relationship between multiple applications on the card platform, i.e. whether each supported application is atomic, or whether there are co-dependencies. For example, a card supporting an on-card biometric verification application and a separate digital signature application might be used atomically in some cases, but in some cases designers may wish to enable the digital signature function to be conditional to the biometric verification result. If the dependency rules are to be enforced, then a trusted path must be provided between the two applications. This could be achieved by sequentially accessing each application and relying on the front or back-end business rules to securely bind the two types of card access. Alternatively, the trusted path might be provided inherently through an on-card inter-application semaphore system allowing one application to access the results of use of another application without going off card. Another example could be where a service provider has distinct applications on card and also needs to access a common stored-value purse.
- **Passive or Active Card Applications** – System planners must determine whether their requirement is to use the card as an essentially static storage medium or whether the card is required to effect application-related computations.
- **Bespoke or COTS Applications** – System planners must decide whether their business processes can be satisfied using commercially available off-the-shelf (COTS) card applications, or whether their business rules demand either modifications of an existing COTS application, or a purpose-built application. Such a decision cannot be taken without a rigorous business requirements analysis, followed by a correlation of those requirements with market offerings. Simple applications such as PIN-activated digital signatures, and authenticated data storage are readily available, but applications with complex data access control arrangements or special cryptographic procedures may necessitate bespoke development.
- **Static or Dynamic Authentication** – Card usage design may employ authentication methods ranging from static to dynamic. An example of this is the distinction in new contactless micro-payment systems between transactions based on the verification of static issuer signatures over data stored on the card, and transactions based on a dynamic challenge-response process in which the card is required to produce a dynamic public signature over elements of the transaction.

- Anonymous or Registered Cardholder Base – In most government access control programs, assertion of cardholder identity is an implicit requirement for card usage. However in applications such as transit, the scheme's viability may depend in part on the availability of cardholder anonymity. Card system planners must firstly determine clear policy regarding card usage, and then embark on an analysis of the business process, technical and security implications of the chosen model.
- Authentication Depth – the question of the depth of authentication to be provided by the smartcard is also crucial. Certain applications (for example low-security building access) may be satisfactorily effected with single-factor authentication (e.g. where the card mutually authenticated against a door reader), whereas higher security applications may require multi-factor authentication including the use of PINs, passwords or biometric parameters.
- Back-end Availability – the detailed design of a smartcard system may depend heavily on the question of whether the front end, with respect to the back-end, is
 - fully on-line
 - partly or periodically on-line; or
 - fully off-line.

This decision impacts technical areas such as:

- choice of card authentication methods
- reader selection
- design of business rules
- the design of configuration, business and event-data delivery mechanisms between front and back end.

3 Deployment Framework

3.1 General

Independent of the smartcard system model adopted in a specific project, a similar card deployment model will have to be used to those sketched in Figure 1-3. The phases of card deployment are in large measure the same as those of any IT deployment:

- project conception and high level adoption including sign-off by high level policy makers and business owners
- planning and design including feasibility studies
- procurement
- building of the system from its constituent components, including unit and integration testing
- in some projects, transition from existing to new technologies and practices
- operation of the smartcard system (technical and business processes); and
- maintaining and refreshing (refurbishing) the system over time, including upgrades and replacement of obsolete components.

Each project commences with a range of policy decisions, leading on to the establishment of a set of high level business requirements. Design, policy and business requirements will be subjected to a set of 'filters' covering such aspects as:

- internal and external stakeholder requirements, gathered through consultation
- the specific project business context
- compliance and regulatory requirements; and
- commercial and technical feasibility and due diligence studies.

These lead to many detailed design, implementation and operational decisions within a structured framework. For a smartcard system, these activities loosely but not exclusively fall into the categories of:

- the physical and logical smart card design
- system infrastructure design and implementation (including reader infrastructure)
- cardholder business processes; and
- participant processes including those of the system owner, card issuer and system operator, and including any external stakeholders.

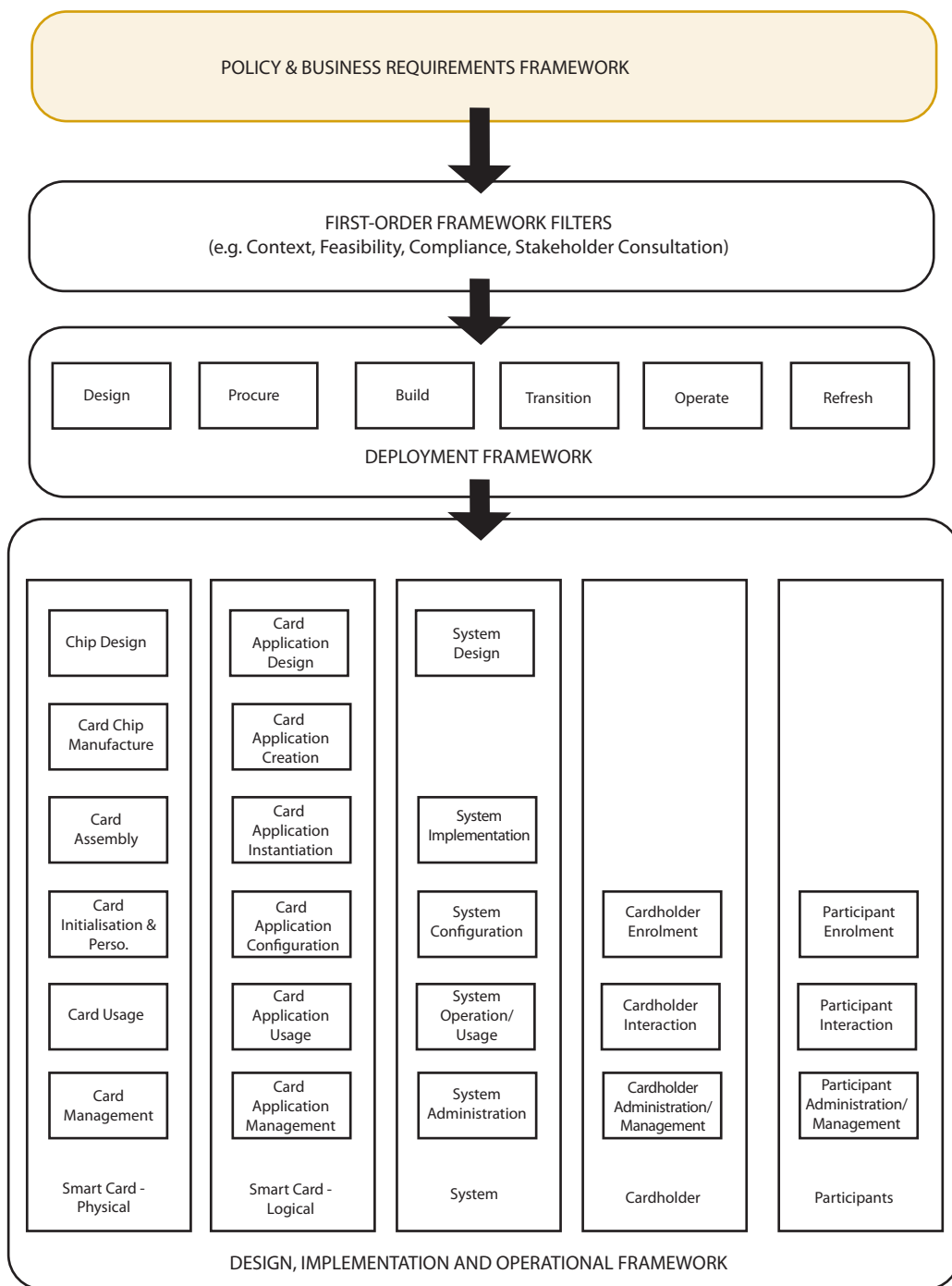


Figure 3: Deployment Model

3.2 Design & Operational Verification

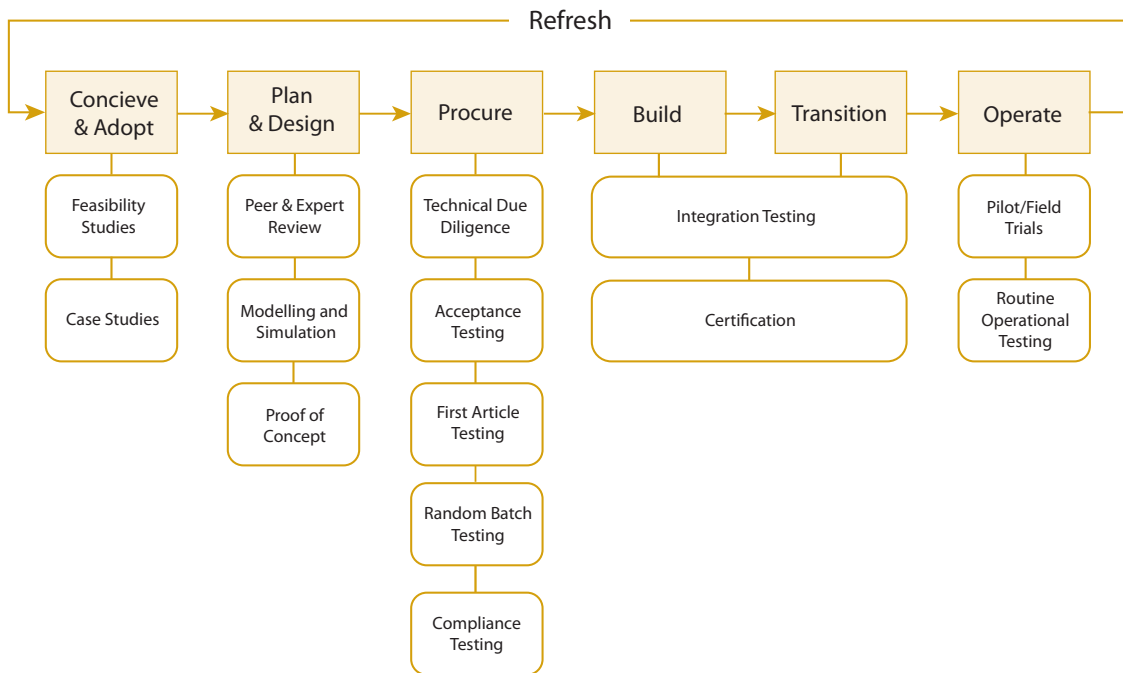


Figure 4: Design Verification Model

Smartcard system planners must not overlook the numerous components of design and operational verification that underlie a successful deployment. The key ingredients of this as depicted in Figure 1-3 apply to all IT projects, but there are some special qualities for smart card systems as noted below.

- Conception & Adoption Phase – feasibility and case studies can be performed to verify the feasibility of the design and identify potential pitfalls. Other Australian Government agencies might be consulted about their card programs, and international case studies also undertaken.
- Planning and Design Phase – design verification can be achieved both by ‘paper’ review, and where appropriate by modelling, simulation, or the development of a proof of concept implementation.
- Procurement Phase – during the procurement phase, card system planners are tasked with ensuring the deliverables meet the system specification. This potentially starts with a formal technical due diligence investigation of suppliers, and then moves through various layers of testing including:
 - performing acceptance tests of specific hardware and software components
 - completing compliance testing or reviewing reports by independent laboratories (for example, for common criteria security evaluations of smartcard implementations)

- requiring first article testing of smartcards, readers or other deliverables as the manufacturing process begins
- requiring random tests of card batches as they are manufactured.
- Building and Transition Phases – integration testing and agency internal certification for compatibility with existing software and hardware infrastructure should be carried out during system build and transition phases.
- Operational Phase – for large card systems, operational readiness can be assessed using pilots or limited field trials. Most smartcard systems will require some level of ongoing testing during the operational phase whether for equipment, software or bug fixes, or to rehearse for exceptional events such as disaster recovery. Periodic security penetration tests may also be required.

4 Community of Practice Checklists

4.1 Environmental Scan

This checklist can be used to identify issues to be considered in an environmental scan.

ISSUE	YES / NO (provide comments)
Can the Community of Practice (CoP) be clearly defined?	
Are there any implicit or explicit relationships with other CoPs?	
Can all members of each CoP be clearly defined or characterised?	
How closely knit will the agencies that comprise the CoP need to be?	
Are all stakeholders in the CoP counted as members of the Community?	
How will trust be achieved between members of the community?	
Are there any legislative, policy or socio-cultural issues that need to be considered?	
Is there a clearly recognised authoritative body or administrative function for the Community that can take on the role of a Policy Management Authority (PMA)?	
If a natural body does not exist, is it possible to allocate the role to a member of the Community?	
What formal membership/relationship processes are required or already exist?	
Are the processes well documented?	
Is a change management process required?	
Is there a formal process for participation in the CoP?	
Are members bound by clear Terms and Conditions for participation in the Community?	

4.2 Developing Terms and Conditions for a CoP

This checklist can be used when developing the CoP terms and conditions.

ISSUE	YES / NO (provide comments)
<p>If a level of interoperability is a business requirement for the successful operation of the CoP, has the CoP clearly defined which of the Framework Implementation Specifications (FIS) will be part of the compliance process?</p>	
<p>Has the CoP clearly defined the process for compliance monitoring and oversight?</p> <ul style="list-style-type: none"> • A peer review is recommended, as opposed to a formal audit process – this would rely on community practices being published in a central space available to all members. 	
<p>Has the CoP clearly defined the certification process?</p> <ul style="list-style-type: none"> • Mandating certification to ISO/IEC 27001 2005 Information technology -- Security techniques -- Information security management systems -- Requirements is recommended to CoPs. This would mean that supplier contracts should be contingent on having/maintaining certification of their Information Security Management Systems to ISO/IEC 27001. The required security features should be mandated in individual agency contracts 	
<p>Has the CoP clearly defined the CoP governance framework?</p> <ul style="list-style-type: none"> • The requirements of AS 8015 Corporate Governance of Information & Communication Technology are recommended to be met by the Framework. AS 8015 defines governance as “the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation”. • Six principles are set out for good corporate governance of ICT. <ul style="list-style-type: none"> - Principle 1: establish clearly understood responsibilities for ICT - Principle 2: plan ICT to best support the organisation - Principle 3: acquire ICT validly - Principle 4: ensure that ICT performs well, whenever required - Principle 5: ensure ICT conforms with formal rules - Principle 6: ensure ICT use respects human factors 	

In developing its terms and conditions, the CoP should also consider the following potential risks:

- Potential loss, or lack of interoperability in critical areas which leads to the possibility of having to integrate interoperability components at a later stage at a further cost to government.
- Reduced awareness of nationally-agreed or whole of government policy objectives, directions and programs.
- Not being aware of (and subsequently failing to engage with) all relevant stakeholder agencies within the CoP – including third parties.
- Implementing inconsistent approaches, particularly in areas such as privacy protection and public education.
- Decisions being made for short-term expediency at the expense of the national interest.

4.3 New CoP entrant to an established CoP

This checklist can be used when assessing the inclusion of a new smartcard deployment (entrant) within an established CoP.

ISSUE	YES / NO (please provide comments)
Is there a reduction in interoperability in critical areas, leading to the possibility of either forsaking interoperability, or having to integrate interoperability components at a later stage at a further cost?	
Has appropriate consideration been given to nationally-agreed policy objectives, directions and programs?	
Have all relevant stakeholder agencies been identified and engaged appropriately?	
Has a consistent approach been taken particularly in areas such as privacy protection and public education?	
Have decisions been made for short-term expediency at the expense of broader strategic interests?	
Has care been taken to identify and consider any reduction in the potential functionality (and return on investment) of the effected smartcard schemes?	