



Australian Government

Department of Finance and Deregulation

Australian Government Information Management Office

National Smartcard Framework



December 2008

SmartcardProjectDesignGuide

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	4
2	Project-specific Smartcard Issues	5
3	Technical issues	6
3.1	Introduction	6
3.2	Card interface (contact / contactless) issues	6
3.2.1	Issues related to contact cards	6
3.2.2	Issues related to contactless cards	8
3.3	Cardholder to Card Authentication	8
3.4	Security features	11
3.5	On-card cardholder credential	12
3.6	On –chip verification	12
3.7	Logically structured, on-card data model	13
3.8	Card access conditions	15
3.9	On-card logging	16
3.10	Identifiers	17
4	Legal issues	19
4.1	Introduction	19
4.2	Jurisdictional issues – up front identification of privacy laws	19
4.2.1	What privacy laws apply in different Australian jurisdictions?	20
4.2.2	Sector specific privacy obligations	21
4.3	“Ownership” and custody of data and records	21
4.4	Contractual arrangements	22
4.4.1	Vendor issues	22
4.4.2	Inter-agency issues	23
4.4.3	End-User issues	23
4.5	Branding of smartcards	24
4.5.1	Commonwealth, State and Territory Coat of Arms and Symbols	24
4.5.2	Other brands and symbols	24
4.5.3	Security considerations	24
4.6	Multi-application smartcards – privacy implications	25
4.7	Liability issues	25

4.7.1	Statutory liability	25
4.7.2	Contractual liability	26
5	Security issues	27
5.1	Overall security design of the smartcard	27
5.1.1	Smartcard components	28
5.1.2	Types of attack	28
5.1.3	Examples of counter measures	29
5.1.4	Security evaluations/certification	30
	Alternatives	31
5.2	Key Management issues	32
5.3	Card production	34
5.4	Card personalisation	34
5.5	Card distribution and issuance	35
6	Governance, Compliance and Policy issues	37
6.1	Governance and compliance in general	37
6.2	Jurisdictional compliance issues	39
6.3	Gateway Review Process	39
6.4	Gatekeeper	40
6.5	National e-Authentication Framework (NeAF)	40
6.6	Identity Management for Australian Government Employees (IMAGE)	42
6.7	The Australian Government Information and Communications Technology Security Manual (ISM)	42
6.8	National Identity Security Strategy (NISS)	42
7	Risk management and risk mitigation issues specific to smartcard implementations	43
7.1	Risk management methodology	43
7.2	Smartcard risk categories and mitigation strategies	44
7.3	Consideration	48
8	Data management issues	49
8.1	Registration data	49
8.2	Data synchronisation	50
8.3	Data management plan	50
9	User registration issues	52
9.1	Initial registration and verification	52

9.1.1	Supporting Evidence of Identity documentation	52
9.1.2	Authorisation verification	53
9.2	Card personalisation	54
9.3	Card lifecycle management	56
9.3.1	Card issuance and activation	56
9.3.2	Card suspension / revocation / destruction	57
9.3.3	Card replacement / renewal	58
10	Card Printing issues	59
10.1	General issues	59
10.2	Single-sided versus Double-sided	60
10.3	Front of the card	60
10.4	Reverse of the card	61
10.5	Other information	62
11	Infrastructure issues	63
11.1	Smartcard type	64
11.2	Smartcard IC chip	65
11.3	Smartcard applications	65
11.4	File system	66
11.5	Card operating system	67
11.6	Smartcard readers	68
11.7	Reader middleware	70
11.8	Smartcard network	70
11.9	Back office system	72
11.10	Card processes	79
11.11	Third parties	81
11.12	Card systems governance	82
12	Standards-related issues in enabling a smartcard deployment	83
13	Interoperability issues	84
14	Multi-application smartcard issues	86
14.1	Access to other agency's data	87

1 Introduction

The National Smartcard Framework (the Framework) aims to facilitate the adoption of a consistent approach to the implementation of smartcard technology by agencies in all levels of government in Australia. It will assist agencies that intend to implement smartcards and allow for the adoption of common policies and technologies that facilitate technical interoperability between smartcard deployments.

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, the National e-Authentication Framework, the Better Practice Guide to Authorisation and Access Management, and the Gatekeeper Framework (for use where public key technologies are implemented with smartcards).

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

- 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 (this document) – 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; and
- Framework Implementation Specifications (FISs) – allow for the sharing of functional specifications and reference models relating to smartcards implemented by a specific Community of Interest (COI). This will enhance interoperability and re-usability between agencies and third party providers while protecting intellectual property.

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

This Project Design Guide is intended to provide better practice guidance for Australian governments to consider when planning for, and deploying, a smartcard based business solution.

2 Project-specific Smartcard Issues

Smartcard technology has been in existence for more than 20 years. The rapid development of the smartcard, combined with the expansion of ICT has created a large number of possible uses, including authentication of identity and financial transactions, transit and telecommunications. For example, a smartcard could store a cardholder's biometric information in order to allow the cardholder physical access to a building or alternatively it could contain no biometric information for identity authentication, but simply be a smartcard with a stored financial value. An 'electronic purse' as it is known can be used as a substitute for cash in low risk and low value transactions, such as public transport.

Given the number of different possible implementations and the continuous development of smartcard technology and features, there are a number of associated issues that arise and may have to be considered during the development, implementation and deployment of smartcard solutions.

This section of the Guide provides an overview of the most common issues that may need to be considered at a project management level before and during the implementation of a smartcard project. It is by no means an exhaustive list of potential issues. Where possible, specific guidance and potential alternatives are provided for consideration by agencies.

Issues have been structured against the following 16 categories.

- Technical issues
- Legal issues
- Security issues
- Governance and Compliance issues
- Risk management and risk mitigation issues
- Data management issues
- User enrolment issues
- Card printing issues
- Infrastructure issues
- Standards-related issues
- Interoperability issues
- Multi-application smartcard issues
- Issues associated with creating economies of scale
- Issues of blended functionality for smartcards
- Installation and system integration issues; and
- User acceptance issues

These categories are discussed in the subsequent sections.

3 Technical issues

3.1 Introduction

Smartcard technology currently allows for a number of different smartcard system implementation options. Based on business requirements, agencies may choose memory or microprocessor cards, contact or contactless interfaces and single or multiple applications. This section identifies some of the technical issues that may need to be considered before and during the implementation of a smartcard project.

Some of the common issues considered are:

- Card interface (contact/contactless)
- Cardholder Card Authentication
- Physical smartcard security features
- On-card cardholder credential
- Logically structured on-card data model
- Card access conditions
- On-card logging - privacy issues with abuse of authority; and
- Identifiers.

3.2 Card interface (contact / contactless) issues

Contact smartcards require the docking of the smartcard into a smartcard reader to establish direct electrical contact with the chip. Contactless cards simply need to be within range of a contactless smartcard reader.

Card interface selection is normally determined by how the end-user will interact with the reader and in what business scenario the smartcard is to be used. In general, contactless interfaces are more efficient as the transmission is wireless and the end-user is not required to dock the card in the reader. In situations where end-user convenience is very important and high throughput rates of cardholders are required, such as in case of stadium access, physical security or public transport, a contactless interface may be more appropriate than a contact interface.

3.2.1 Issues related to contact cards

Where the proposed smartcard system is to utilise contact-based smartcards, the following issues should be considered:

- Availability of the required card reader infrastructure – for logical access and PC security applications, the simplest external contact smartcard readers tend to be less expensive than contactless readers. Furthermore, new PCs and laptops may increasingly come standard with an embedded contact card reader

- Security Application Module (SAM) – a SAM is essentially a specialised hardware security module integrated into the smartcard reader and configured with the terminal's encryption keys. Typically SAMs themselves have a GSM SIM form factor to facilitate distribution and maintenance. SAMs are important where multiple agencies or service providers will potentially need to access the one smartcard.

Multiple SAMs enable the card reader to support different service providers' and card issuers' cryptographic keys without requiring online key distribution which can expose keys between agencies and introduce other security vulnerabilities. There is limited support for SAMs in low-end Commercial Off The Shelf (COTS) contact card readers. However, they are standard in Electronic Funds Transfer (EFT) terminals, where typically up to eight SAM sockets are available

- Secure PIN entry – secure PIN entry, independent from a host computer which may not be hardened against compromise, tends to be easier to implement with contact readers than contactless because of the positive one-to-one engagement between the card and the terminal. PIN pad security and card reader tamper resistance is readily certified under various international and Australian standards
- Card reader integration with back office – while most card readers provide a transparent data path to the local host (e.g. a PC), integration issues can occur where local card reader controls require the operation of specific technologies (e.g. ActiveX) developed for sharing information among different applications. Other alternatives available to achieve back office integration include the use of intelligent and secure card readers (e.g. FINREAD), middleware and specific applications. FINREAD, for example, is a set of technical requirements specified by a consortium of international payment systems as well as a manufacturer for the secure independent smartcard reader connected to a PC. FINREAD enables the processing of secure and sensitive transactions, such as e-commerce, e-administration, e-banking, e-social welfare (health care, age care, etc) over the Internet and other open networks. The technical specifications (CWA 14174) have been endorsed by the CEN (European Committee for Standardization) under the form of a CEN/ISSS CWA (CEN Workshop Agreement)¹
- Card reader integration with business process – as already mentioned, contact cards are not ideal or feasible in business scenarios where a high throughput is required, e.g. stadium access, transport and ticketing. Transit operators tend to target 300ms or less for a complete transaction. Apart from being mechanically inconvenient, it is often infeasible to get adequate transaction times for these scenarios with contact interfaces
- Increased wear and tear of card and chip – issues and concerns with chip wear and tear and damage to cards through sustained exposure to electrostatic discharge (ESD) may need to be considered, e.g. chip contact wear/corrosion and card flexing from constant docking and removal from card reader slot and in wallets; and

¹ Note that FINREAD operates with minimum security functionality. In essence, the reader can authenticate itself to the system, but not to the smartcard. Security assumptions for FINREAD are:

The security level of the smartcard is out of the scope of the technical specifications. It is assumed that the payment scheme or the financial institution have chosen the appropriate security requirements for the ICC card

The security level of the payment scheme or any other financial scheme is assumed to be secure in itself.

The reader does not add security to the application itself but provides a secure interface for cardholder interaction.

The only secret that shall be securely stored in the reader is the private key used for reader authentication

There are no additional requirements for other secrets

The reader is intended to be linked to a distributed environment. There is no assumption or requirement for the security level of the remainder of the user environment.

- Extreme temperatures - exposure to extreme temperatures (below -20 and above 80 degrees Celsius) may cause the plastic to warp, changing the shape of the card.

3.2.2 Issues related to contactless cards

Where the proposed smartcard solution is to utilise contactless based smartcards the following issues should be considered:

- Use of a secure cryptographic session – eavesdropping on wireless connections is possible using commercially available equipment. Therefore, it is important to consider a cryptographic session between the reader and the contactless card to allow for the encryption of data being exchanged and mutual authentication
- Interruption of operation – interruption of communications may occur between the card and reader, for instance when the user does not hold the card steady in range of the reader. Backup and restore mechanisms may be considered to allow incomplete transactions to be successfully completed and also ensure duplicate transactions do not occur
- Denial of Service (DOS) – attackers may be able to disrupt (i.e. jam) the card communications from a distance by using electromagnetic waves. This could potentially deny a user access to a service
- Multiple cards detected – in some instances when more than one card is presented to the reader (e.g. the cardholder carries more than one card), the reader may be slow or unable to resolve the modulation scheme or choose the correct card to use for the specific operation
- Unauthorised transactions – even when sessions are cryptographically protected, there is a risk that an attacker may be armed with a legitimate reader and try to use it for unauthorised purposes. This risk is exacerbated because the user may be completely unaware that a rogue reader is in range. Far-reaching and effective countermeasures may include strong authentication between the card, the card reader and the user. In addition, protective card pockets with electromagnetic shielding are now commercially available for contactless chips to prevent the chip from being read by unauthorised readers
- Wear and tear of card and chip – contactless cards are inherently more resistant to wear and tear than contact cards. However, contactless chips may be exposed to excessive magnitude radio frequency fields from readers. This may affect the lifetime of the chip; and
- Extreme temperatures - exposure to extreme temperatures (below -20 and above 80 degrees Celsius) may cause the plastic to warp, changing the shape of the card.

3.3 Cardholder to Card Authentication

Cardholder to card authentication mechanisms exist for the purpose of linking the identity of the cardholder to the card. Once a user has established their identity to the card, the user is able to perform privileged operations or access personal data on the chip.

There is a wide variety of cardholder authentication mechanisms to consider. The most common mechanisms and potential issues:

- Personal Identification Number (PIN) – the most traditional method for linking the cardholder to the card is the PIN code, a numeric code² that must be remembered by the cardholder. The PIN may be enforced and validated by the chip so that it is never exchanged with the outside world.

It is imperative that smartcard application design provides appropriate protection for PIN entry. When PINs are entered into regular host computers that may be vulnerable to keystroke loggers, there are risks of PIN compromise. To reduce this risk, agencies may consider the use of smartcard readers with security mechanisms, e.g. secure PIN pads and hardware security modules (HSM) with cryptographic capability. However, with the number of potential smartcard applications ever increasing, this could result in users having to remember multiple PIN codes. Apart from inconvenience, this could lead to users to select PINs that are easily guessed or users writing PINs down, increasing the likelihood of compromise and the number of call to service desks for PIN resets³.

When users are able to select the PIN themselves, they are enabled to choose one single, strong PIN. This may not necessarily be a problem, provided that the user is aware of the risks associated with one PIN, the PIN is not easily guessable, not written down and periodically changed⁴ by the user.

As an alternative to PINs, biometrics may be used for cardholder authentication. However, biometrics give rise to various issues and the potential downside of a biometric being compromised may be far worse than having a single PIN compromised. Some implementations use biometrics to complement, rather than replace, PINs

- Biometrics – a biometric identification method is a method that can identify a person by means of unique, individual biological features. The main drivers for the usage of biometrics are increased security against identity theft (by guessing or eavesdropping on shared secrets like PINs and passwords), and increased convenience. Some of the most widely used types of biometric technologies in combination with smartcards use the following human biological features:

- Fingerprints
- Iris (eye)
- Face
- Hand geometry.

The primary issues of the use of biometrics to consider are:

- Protection of the biometric features – biometric features are personal data and therefore should be appropriately protected. Biometric features can either be stored on the smartcard itself or in a database of the biometric system. From a security and privacy point of view, on-card storage may be more secure, as biometric matching can be performed in a secure chip. A large central database with biometric data is not

² ISO and AS2805 allow 4 to 10 digits and banks are currently encouraging to use longer PINs to reduce the risk of brute force attacks

³ This is particularly true in cases when the PIN code is used only rarely

⁴ and definitely changed when compromise is suspected

required and the stored biometric templates will never have to leave the chip. When reference data is stored in a less secure environment, they may be manipulated and read

- Accuracy – the two basic parameters for judging the accuracy of a biometric method are its false acceptance rate (FAR) and its false rejection rate (FRR). Depending on the biometric method and technology used, different FARs and FRRs may apply, making the technology less or more appropriate for certain situations
- Failure to enrol rate – biometrics exhibit a finite failure to enrol rate, leaving a sub population of users which must be catered for by alternative authentication mechanisms. Examples include: hand geometry won't work for people with missing digits; facial recognition templates with sufficient differentiating features can be difficult to obtain from individuals with facial hair, or who wear face coverings for religious reasons; and useable fingerprints may be difficult to obtain from manual workers and the elderly
- User acceptance – all biometrics can be perceived as privacy intrusive. This may be less of a problem in the case of handwritten signatures or facial recognition, but may become more of an issue in the case of fingerprints and iris scans
- Costs – biometric technologies, especially more advanced technologies such as iris and retina scans are significantly more expensive than more conventional authentication methods such as PIN codes
- Interoperability – biometric systems are often proprietary and vendor specific. This may cause interoperability issues when multiple systems from different vendors are used
- Consent – by entering a PIN code at the smartcard terminal, the user is giving the smartcard application operator consent to perform privileged operations or access personal data in accordance with the agreed terms and conditions of the transaction. From a legal perspective, the “ceremony” of PIN entry is well understood to be associated with granting consent. Biometrics are a much newer technology, and may involve novel and varying experiences for the user. There is no unambiguous ceremony with most biometrics and it is not clear as yet that informed consent can be as clearly conveyed as it can by PIN entry
- Identity theft – one of the principle issues to consider in the case of biometrics is the impossibility of revoking and re-issuing of compromised biometric features. When a cardholder's biometric features are compromised, this may have severe consequences for the individual. While it is possible to replace a smartcard or change a PIN code, it is impossible to replace a biometric feature such as a finger print or iris; and
- Hygiene – users may have concerns regarding medical and hygienic aspects. For instance, users may be afraid of acquiring a disease from optical scanning of their retinas, or that the laser light will damage their eyes. Even though such fears may be subjective and lack any scientific basis, they can still strongly affect user behaviour and user acceptance of the method.

3.4 Security features

Security features refer to the features used to protect the physical card and are used during a manual (visual) card verification to provide evidence that the card being presented by the user is authentic.

Several card security mechanisms may be considered for on-card credential tamper resistance and forged/duplicate cards identification. It is important to note the discussed card security mechanisms do not protect the data in the chip. They aim to prevent the falsification and misuse of the smartcard and to enable visual verification of the card.

Some of the card security mechanisms include:

- Embossing – a relief impression, also referred to as a “dry seal”, which can be felt as well as seen. It is produced when the substrate (usually paper, but may also include a plastic material such as laminate) is formed in the pattern of a seal, crest or geometric design by a mechanical die under pressure. It is also referred to as “dry embossing” as the image is produced without ink
- Security inks – security inks have special optical, physical or chemical features added to the printing ink. Security inks include the following: metameric, photochromic, luminescent, thermochromic and magnetic. There are also taggant inks that have forensic characteristics which can contain secret compounds known only to the document issuer
- Microprinting – microprinting involves printing very small text, usually too small to read with the naked eye, and which may appear as a line of dots. Microprint is frequently hidden in an inconspicuous area on the document. Text of this form is very difficult to copy with current computer scanning or photocopying equipment. Attempts to counterfeit using a printing press do not accurately reproduce the microprint, because the text is too small to engrave into printing plates using methods available to the general public and counterfeiters
- Guilloché patterns – a guilloché or engine turning pattern is an ornamental pattern formed of two or more curved bands which interlace to repeat a circular design. They are most commonly seen on banknotes. These patterns were traditionally used for security printing purposes as a protection against counterfeit and forgery
- Optical variable device (OVD) – an OVD is a design, pattern or image which changes its colour or appearance depending on the angle at which the object is held to the light or viewed. For example, this variability may take the form of a switch between one artwork pattern to a totally different piece of artwork; or from the image of a face to the image of a logo. Image variability is the key security feature underpinning OVDs. OVDs are of many different generic types, determined by the method of manufacturing the microstructure, the range of optical features displayed by the device or the trademark associated with the device. Examples include Holograms, Kinegrams™, and Alphagrams; and
- Hidden Image – hidden imaging involves printing an image at high resolution in such a way that it remains hidden in the background and can only be made visible via the use of a specially coded transparent overlay screen.

3.5 On-card cardholder credential

On-card cardholder credentials refer to the visual aspects of the physical card and the card layout (face and reverse of the card) that are used for identifying the cardholder. As an example, the face of the card (FOC) could identify the card and user, providing information for visual authentication of the user so that the card can be authenticated in an offline environment where no smartcard reader is present.

There are several on-card primary cardholder credentials available to support visual identification and authentication of a user. Options may include:

- photograph of individual
- name
- signature
- cardholder number
- issuer identifier

The primary issue to consider is the privacy aspects of including specific cardholder details on the face or reverse of the card. Personal cardholder details on the face and reverse of the card can be easily read and copied. This issue becomes more significant when the card is perceived as highly trustworthy and is used in many different circumstances by many relying parties.

3.6 On-chip verification

Information stored on the ICC can also be used for verification. The primary issue to consider with on-chip verification is the privacy aspects of including specific cardholder details in the chip. Personal cardholder details in the chip can be easily read and copied when not protected by access controls and PINs. This is especially true for contactless chips that may be skimmed.

3.7 Logically structured, on-card data model

Logically structured on-card data models apply to the means by which data is stored and protected within the chip.

Smart chips can be designed to contain multiple types of applications and data, ranging from highly sensitive information (e.g. cryptographic applications and keys) to public data (e.g. issuing agency and card number). By using access controls and encryption based on the sensitivity of the data, the logical data structure on the chip may be divided into a number of logically separated zones and security domains. In general, the following logically separated zones can be distinguished:

- Locked zones – a locked zone could be implemented on the chip to prevent data from being read, changed or deleted from the chip. This zone contains the smartcard firmware and the operating system and cannot be changed or deleted after initial personalisation of the chip at the time of manufacture

- PIN protected zones – these virtual zones can contain information that can only be read, changed or deleted after successfully entering the chip PIN code or providing a valid authentication key⁵. In addition, this also prevents unauthorised persons or applications from retrieving information from the chip or installing applications without the approval of the user or the application provider. The main issue to consider is which information should be protected by a PIN and which information can be read without a PIN. Typically, this will largely be determined by the security, privacy and usability requirements relating to the information
- Access controlled zones – access controlled zones prevent unauthorised parties from reading or changing information on the chip. Access controlled zones are particularly effective when multiple parties are using applications on the chip. By using unique cryptographic keys for each relying party, applications and data on the chip can be logically segregated by storing the application provider's unique set of keys which limit the area of control within the smartcard. The main issues to consider are the way specific relying party cryptographic keys will be managed and what information should be access controlled. As with PIN protected zones, this will largely be determined by the security, privacy and usability requirements relating to the information; and
- Public zone – this zone could contain information that can theoretically be read from the chip by anyone who has physical access to the chip and a reader. The public zone is typically suitable for non-sensitive information that is allowed to be read by anyone. The main issues to consider are security and privacy impacts of storing information in the public zone.

Protection of information stored within the chip often includes a trade-off between retaining the usability of the smartcard and sensitivity/privacy of that information. A common example used to illustrate this predicament is when emergency medical data resides on a smartcard (e.g. allergies and emergency contact information). Some might argue that this type of information should not be placed in a public zone and should be protected by an access mechanism such as a PIN code. However, in the event of an emergency, this information should be able to be read by authorities where the cardholder is unable to facilitate this process. In the latter case, PIN protection would not be an option.

Options to be considered in this case are:

- information could be protected by other means of access controls using unique cryptographic keys for authorised parties and/or specific readers. This would enable only authorised parties to access the information, without the need for a PIN code
- information could be stored in the public zone on a voluntary basis. In this case the cardholder may need to be made aware of the associated risks and the reduced degree of control that the cardholder has over information being read; and
- information is not stored in the chip itself, but in back office systems that can be accessed online (e.g. through web services). In such instances, the card will have a reference (a card or cardholder credential) that refers to the applicable record of the cardholder in the back office system.

⁵ Alternatively, biometrics may also be used to protect these zones

The table below provides an overview of different data areas on smartcards, examples of data that can be stored in these areas and access conditions that apply to each of these areas.

Area on card	Data stored (examples)	Ability to access/change data after personalisation
Magnetic stripe	Cardholder identifier, issuance date, expiry date, pin verification value	Magnetic card reader (read only)
Face/reverse of the card	Cardholder identifier, photo, signature, barcode, machine readable zone (MRZ)	Visual (read only) MRZ / Barcode reader (read only)
Chip – Locked zone	Firmware / operating system	None
Chip – Access controlled zones	Agency identifiers, concession status, emergency contact information, health information	Authorised card reader/ application
Chip – Pin protected zone	Address, date of birth, photograph financial details and/or health details, biometric templates and cryptographic keys	PIN code or authentication key required
Chip – Public zone	Card number, user's name, unique ID, expiry date and digital certificates	Unrestricted read access to data. Potential ability to change data
Back office system	Additional cardholder details, biometric templates, PIN/PUK ¹ , card, transaction information, card status (active, expired, revoked)	Logical access controls (identification, authentication and authorisation) implemented in back office system for read and modify data

¹ Pin Unblocking Key (PUK)

3.8 Card access conditions

Card access conditions refer to the process in which the smartcard and/or the smartcard reader determines whether its communication partner is a genuine reader or a genuine smartcard respectively.

Several commonly adopted card access mechanisms exist for the secure access of data, however the level of assurance required by the business process will determine the type of card access implemented. Access mechanisms may include passwords, PINs, biometrics and cryptographic access controls at session establishment (such as unilateral and mutual authentication) and during the session using session keys. The base security mechanisms defined by ISO 7816-4 are as follows:

- Authentication via a PIN or password – the user is required to successfully enter a password or PIN prior to being provided with access. Issues with regard to PINs and biometrics have been discussed in Section 3.3.
- Authentication via a cryptographic key – this authentication is normally automatically performed between the reader and the smartcard and does not require any direct input from the cardholder. This technique typically uses cryptography in a challenge-response arrangement. Specific issues to consider are the following
- Unilateral and mutual authentication - unilateral authentication only establishes the authenticity of one of the communication partners. Mutual authentication aims to establish the authenticity of both communication partners. Mutual authentication typically takes more time to perform and may therefore be less appropriate in scenarios where a high throughput rate of users is required. In general, when the card stores sensitive information or provides access to sensitive information, mutual authentication may be the preferred option, rather than just verifying the authenticity of the smartcard
- Symmetric and asymmetric cryptography - symmetric encryption is typically faster than asymmetric encryption. In the case of symmetric encryption, the value of the card-specific secret key may be a function of the card number and the master key, which is known to the reader. If the master key is compromised, the entire system may be compromised, since all card-specific authentication keys can be computed using the master key. The master key must therefore be securely stored in the card reader (for example, in a Secure Application Module). Appropriate key management procedures apply to life cycle management of card reader keys and should address generation, expiry, revocation and renewal of cryptographic keys⁶. Asymmetric cryptography may provide a higher level of security and less key management issues, but is typically slower in execution speed and may be problematic in a contactless card implementation. However, private keys in readers and system private keys are still required to be adequately protected and managed during their lifecycle; and
- Static or dynamic - asymmetric authentication can be static or dynamic. With a static procedure, there is no protection against replaying previous data. This is why it is mainly used as a supplementary verification of the authenticity of the card, after it has already been verified using a dynamic symmetric procedure. Alternatively, to provide protection against the re-entry

⁶ Adequate protection and lifecycle management of card readers private keys and system master keys applies when asymmetric cryptography is used

of data intercepted from earlier sessions, a dynamic asymmetric procedure can be used, where a random number is used as the input value for the cryptographic algorithm. Dynamic asymmetric requires an arithmetic processing unit in the chip that can execute the asymmetric cryptographic algorithms, which adds to the cost of the chip.

3.9 On-card logging

On-card logging refers to the process where (application specific) logs are stored in the chip of the card. On-card logs are typically maintained by the card operating system. Logs are usually updated during each session to reflect the current state of applications and any signatures or other data that may have been received from the card reader. Logs are typically located in a cyclic file where the oldest logs are overwritten by the latest logs.

On-card logs may be used for the following purposes:

- automatic error recovery, such as an automatic roll back to the previous state of the card when a session is terminated unexpectedly
- to assist in providing proof that a disputed transaction was actually carried out. Conclusive transaction 'forensics' may entail inspection of card reader logs or back-end transaction accounts as well as the card log itself
- to provide the cardholder with a source of reporting on card usage that does not necessitate a direct interaction with the central system; and
- to provide security managers with an audit trail of card administrative access, or of possible unauthorised card access by certain readers.

From a privacy perspective, the primary issues associated with on-card logging is that information in the on-card log may be used for unauthorised purposes, and in particular to make associations between cardholders and business processes which an agency or third party is not entitled to.

The key consideration during a smartcard deployment is to establish clear policy and risk analysis regarding on-card logs, reader logs and backend system logs. In the case where the smartcard is used by various agencies and service providers, it is important that policy and risk analysis addresses address capturing and sharing of logs.

Depending on policy specifics, safeguards to be considered with on-card logging include:

- each application should have its own on-card log, in which only information relating to that application is held
- access to the on-card logs is only allowed using cryptographic keys belonging to authorised readers and applications
- card reader equipment to retain only the cryptographic keys is needed for the given agency or service provider application, thus precluding unauthorised access to other applications or parts of the card

- log information written to and read from the card should be encrypted during the session to prevent eavesdropping attacks
- log design to incorporate only the absolute minimum information needed to carry out associated business processes
- a PIN verification feature to allow the cardholder to determine when access to the card log is allowed; and
- determine the events and amount of information per event that will be stored. Smartcards are typically small in size and may run out of memory when many transaction logs are stored. Alternatively, logs can also be stored in readers and back office systems and applications and not just on the card.

3.10 Identifiers

One of the primary functions that smartcards can support is the secure identification of cardholders and other entities. Identifiers can be used to represent a cardholder's identity and associated attributes. A name or a card number are examples of identifiers. To be able to deliver more effectively deliver services to cardholders, the cardholder identifiers are typically linked with information residing in back-office systems.

Issues relating to identifiers to be addressed when designing card systems include:

- Subject identification – identifiers may not only be used for identification of cardholders, but may also relate to other subjects, such as the smartcard itself (card number), the chip, the smartcard issuer, relying parties or specific services. Different types of identifiers may be required to allow for identification of these subjects
- Uniqueness - one of the main characteristics of identifiers is that they should be uniquely related to the cardholder (or other type of subject) in the domain in which the smartcard is used. To prevent data clashes, it is important that issuers within a domain do not issue identical identifiers. In case of multiple issuers in one domain (e.g. a certain government sector), issuers may adopt mechanisms and protocols that ensure that identifiers are unique within the domain and are interoperable. Further, to achieve interoperability of identifiers between multiple domains, issuers may agree on name spaces that may only be used by certain issuers. An example is the adoption of Object Identifiers (OIDs). OIDs are hierarchically managed by the International Organization for Standardization (ISO) and where relevant, the International Telecommunication Union (ITU), and are intended to be globally unique (similar to a VIN/Chassis number on a vehicle or a primary account number on a credit card). The ISO and ITU delegates OID management to organisations by assigning them OID numbers. These organisations can then assign OIDs to subjects or further delegate to other organisations
- Persistence – identifiers may change every time a new smartcard is issued to the cardholder, or may be persistent. Typically, card numbers will change upon every issuance, whereas cardholder identifiers may not change. From a privacy point of view, cardholder privacy may be better protected when identifiers periodically change. The disadvantage of frequently changing identifiers is that it may require the cardholder, issuer or relying party to update the links to the various back office systems. In some circumstances, particularly where the smartcard is intended

to be widely used, even a changed identifier with each new smartcard may not adequately mitigate the risks associated with a unique identifier. In such cases, other mitigation methods should be considered to reduce the risk of creating a universal ID number

- Privacy – an important issue to consider in relation to the use of identifiers relates to the protection of the privacy of the cardholder. This is especially true when unique identifiers are issued to large groups of cardholders and the identifier is used by many relying parties in a multiple domains. Conducting a Privacy Impact Assessment (PIA) in accordance with guidelines published by the Office of the Privacy Commissioner on the use of identifiers and designing privacy enhancing controls is strongly recommended for all types of smartcard implementations. This guide is available at <http://www.privacy.gov.au/publications/pia06/index.html>; and
- Standards – various standard approaches are being or have been developed with regard to the allocation of unique identifiers. One example are the OIDs managed by ISO, another example is the development of the Cardholder Unique Identifiers (CHUID) as defined by the United States Federal Government Physical Access Control Systems Implementation Guidance. ISO/IEC 7812 'Identification Cards – Identification of Issuers' defines a standard for identification cards and identification of issuers. Part 1 of the standard specifies a numbering system for the identification of issuers of cards that require an issuer identification number to operate in international, inter-industry and/or intra-industry interchange. Part 2 of the standard specifies application and registration procedures.

4 Legal issues

4.1 Introduction

This section identifies some of the legal issues that may need to be considered before and during the implementation of a smartcard project.

Legal issues that are relevant to a specific smartcard project need to be considered on a case by case basis (and by reference to the specific circumstances). For that reason, this section of the Project Design Guide is not legal advice. It is simply intended as a guide to highlight some potential legal issues for government agencies to consider. Agencies seeking to implement smartcards should obtain their own independent legal advice.

This section is structured around the following sections:

- Jurisdictional issues
- Ownership of data and records
- Contractual arrangements
- Branding of smartcards
- Multi-application smartcards – privacy implications; and
- Liability issues.

4.2 Jurisdictional issues – up front identification of privacy laws

A Community of Practice (CoP) that issues smartcards must ensure that the design, implementation and operation of its smartcard system complies with all applicable privacy laws. This is because smartcards and smartcard systems may contain personal information (it is noted that there may be some exceptions to this – e.g. smartcards that are simply stored-value cards). In this context, personal information can be defined as information or an opinion from which a person's identity is apparent, or can reasonably be ascertained.

Identifying what privacy laws are relevant to a smartcard project is an important early step in any smartcard implementation project. This will involve a consideration of the types of entities that will use the smartcard, which sectors and jurisdictions they operate in, what type of personal information will be involved, and whether personal information might be further regarded as “sensitive” under privacy law, that is, if it relates to an individual's race, ethnicity, religion and so on, or to their health.

There are different privacy laws that apply to federal, state and territory agencies, and to private sector organisations. Among other things, these laws apply to the way that personal information is collected, used, disclosed, stored and handled, as well as regulating how individuals can seek access to personal information that is held about them. There are also sector specific privacy laws that apply in areas such as telecommunications and health.

4.2.1 What privacy laws apply in different Australian jurisdictions?

Information on privacy laws can be obtained from the Office of the Federal Privacy Commissioner (OFPC). The OFPC provides privacy information at www.privacy.gov.au.

A comprehensive overview of the current privacy laws across different Australian jurisdictions is contained in the Australian Law Reform Commission's Issues Paper 31: Review of Privacy (October 2006)⁷.

The following (non-exhaustive) list highlights some privacy laws to be aware of when a smartcard solution is being designed, implemented and operated:

- Australian Government agencies must comply with the Information Privacy Principles (IPPs) in the Privacy Act 1988 (Cth). Agencies are also required to include appropriate privacy clauses in contracts to ensure that contracted service providers do not act in a way that would be a breach of the IPPs if the act or practice was done by the agency itself
- private sector organisations (which are not “small businesses” as defined in the Act) must comply with the National Privacy Principles in the Privacy Act 1988 (Cth)
- the Federal Privacy Act does not regulate state or territory agencies, except for the ACT. States and territories have their own privacy laws that apply to their public sector agencies. The OFPC website provides links to state and territory privacy laws at http://www.privacy.gov.au/privacy_rights/laws/index.html. Some of the laws are summarised below
- New South Wales (NSW) public sector agencies are required to comply with the Information Privacy Principles under the Privacy and Personal Information Act 1998 (NSW)
- Victorian public sector agencies are required to comply with the Information Privacy Principles under the Information Privacy Act 2000 (Vic)
- Tasmanian public sector agencies are required to comply with the Information Privacy Principles under the Personal Information Protection Act 2004 (Tas); and
- Northern Territory public sector agencies are required to comply with the Information Privacy Principles in the Information Act 2002(NT)
- Australian Capital Territory (ACT) government agencies are required to comply with the Commonwealth Information Privacy Principles by virtue of the Australian Capital Territory Government Service (Consequential Provisions) Act 1994 (Cth).

In states that have not enacted privacy legislation, there may nevertheless also be government guidelines that need to be addressed. For example, Queensland public sector agencies are required to follow the Information Privacy Principles under the Information Standard No. 42 (Queensland) published by the Queensland Department of Innovation and Information Economy.

There are also specific privacy laws relating to the use of credit information and tax file numbers that may need to be considered.

⁷ Available at: <http://www.austlii.edu.au/au/other/alrc/publications/issues/31/IP31.pdf>

4.2.2 Sector specific privacy obligations

Specific privacy obligations may apply to some industry sectors. It is important to consider whether any such laws are relevant to a smartcard project. There are some sector specific laws that are relevant to various case-studies including:

- telecommunications operators (including carriers and carriage service providers) are regulated under Part 13 of the Telecommunications Act 1997 (“Protection of Communications”)
- the handling of health records is regulated under some State privacy legislation, including under the Health Records Act 2001 (Vic), the Health Records and Information Privacy Act 2002 (NSW) and the Health Records (Privacy and Access) Act 1997 (ACT); and
- special rules apply to the collection, use and disclosure of personal information in the workplace in some jurisdictions – such as under the Workplace Surveillance Act 2005 (NSW).

At this time, there are no sector-specific privacy laws that apply to areas such as transport and ticketing, but the handling of personal information by participants in those sectors will be regulated under the general privacy laws described above.

4.3 “Ownership” and custody of data and records

In Australia, privacy laws generally are not based on any concept of “ownership” of personal information. As noted, obligations under privacy laws are based on how agencies and organisations collect, use, disclose, store and handle personal information. These obligations however are not based upon whether or not those agencies or organisations “own” the relevant records or databases that contain that personal information.

Nevertheless agencies will need to manage issues relating to the custody of data and records at a contractual level, together with operational arrangements relating to the storage and processing of data and associated access rights. Ongoing rights of access that might be required for operational purposes when data is stored or processed by a third party vendor (including ongoing rights of access in the event of insolvency of the relevant third party vendor) need to be very carefully weighed.

Offshore transfer of personal data that might be associated with smartcard management is not necessarily forbidden by Australian law but is expressly covered by the National Privacy Principle 9 (Transborder Data Flows). Considerable time and expense can be incurred under NPP 9 by organisations seeking to determine the nature of foreign privacy provisions and the degree of compliance of third parties with those provisions. Given these complexities, plus the widespread community concern over these issues, some agencies might consider taking policy positions with respect to outsourcing, off-shoring and privacy related matters in general that are stricter than the NPPs, in the interests of engendering better support from smartcard users. Privacy legislation and schemes in different jurisdictions reflect the public policy in minimum privacy standards. Where higher standards are required to address particular privacy risks, agencies should consider the need to extend these minimum standards, for example by including specific provisions in the Smartcard enabling legislation.

Furthermore, vendors contracted by government agencies must be aware of their duties to comply with the Information Privacy Principles (which apply to agencies) rather than (or in addition to) the National Privacy Principles which ordinarily apply to private sector organisations.

Privacy issues associated with trans-border data flows need to be managed at the contractual level where the recipient of the information transferred overseas is not subject to privacy laws similar to those in Australia.

Finally, it is wise to acknowledge the strong feelings of “ownership” that many individuals (including agency employees) feel towards their personal information pertaining to them. While ownership of personal information is not a concept sanctioned by law, closely associated attributes such as rights of access, rights to correction, and consent to sharing with third parties are clearly described and governed by privacy law as well as by specific statutes relating to workplace surveillance. When a smartcard deployment has an impact on the volume and nature of personal information that is managed by an agency and exchanged with others, great care should be taken to explain to end users terms and conditions of data custody, in language that is sensitive to the lay person’s common sense of ownership of their data.

As it is important for individuals to be able to choose to retain their anonymity, agencies and organisations should consider whether this is legal and practicable when designing a smartcard application.

4.4 Contractual arrangements

When implementing a smartcard project, it will be important to understand how the various relationships operate from a contractual perspective. This includes the relationships between:

- the smartcard issuing agency and the cardholder
- the smartcard vendor and the issuing agency
- the issuing agency and its subcontractors; and
- the issuing agency, its subcontractors, and cardholders.

Some key contractual issues are identified below.

4.4.1 Vendor issues

An agency proposing to develop and issue smartcards will need to ensure that its contractual arrangements with vendors incorporate enforceable undertakings and warranties from the vendor in relation to:

- the ability of the proposed solution (including the smartcard, associated applications and infrastructure) to comply with all applicable laws and regulations
- the capability of the proposed solution to meet the agency’s projected capacity, functionality and performance requirements, and to interoperate with other specified systems (including on an intra-agency or inter-agency basis) as required
- commitments to achieving the agency’s key milestone dates for delivery and installation

- managing complexities in the supply chain, involving chip manufacture, card fabrication, printing, initialisation, personalisation, third party Card Management Services, and third party application provisioning
- commitments to maintaining “best practice” standards, including security requirements, protection of the integrity of data and functions, virus protection, etc
- indemnifying the agency against any potential risks associated with the intellectual property rights incorporated in the solution
- long-term commitments in relation to the ongoing availability of the smartcard and other key components of the solution, and the long-term maintenance of supporting applications and infrastructure; and
- managing the agency’s risks associated with the potential insolvency of those key vendors involved in the support of the solution on an ongoing basis.

This involves obtaining contractual undertakings from vendors in relation to specific details of the hardware, software and application features throughout the implementation and on-going system support and maintenance of the smartcard infrastructure and applications.

4.4.2 Inter-agency issues

Arrangements may need to be established with other agencies and relevant parties in relation to matters such as:

- establishing a Community of Practice (CoP). (CoPs are described in Section 13)
- the ongoing operation and maintenance of shared infrastructure (and possibly, shared applications), where the relevant smartcard will support the activities of more than one agency
- security and interoperability standards to be adopted across agencies, where applicable
- rules governing restrictions on the sharing of databases (and the associated use of applications and access to data) between agencies for various applications, where applicable; and
- restrictions on the matching of security data, such as restrictions on the use of security data to search smartcards and the entire database for a match in circumstances where such access is not permitted.

Inter-agency arrangements may not necessarily extend to formal contractual arrangements, and could be managed through the establishment of a CoP governance framework.

4.4.3 End-User issues

Agencies may also wish to consider the development of standard terms and conditions applicable to users, setting out:

- terms and conditions of use (including associated restrictions on use); and
- limitations on the liability of the issuing agency.

4.5 Branding of smartcards

Agencies should consider whether there are any legislative or other restrictions on the use of logos, brands, symbols or other marks on smartcards.

Agencies may have their own branding rules and style guide to using branding and should check with their corporate communications division for advice. The Awards and Culture Branch within the Department of Prime Minister and Cabinet provides design files and guidelines to Australian Government agencies. The Australian Government Branding Design Guidelines are available from http://www.dpmc.gov.au/guidelines/docs/design_guidelines_PMC.rtf

It is important to consider all relevant intellectual property rights, in addition to legislation that regulates the use of particular marks. As with all trademark issues, and as per consumer protection law in general, it is important to ensure that all marks, brands and marketing representations give a fair and accurate impression of what the smartcard is intended to do.

4.5.1 Commonwealth, State and Territory Coat of Arms and Symbols

Agencies need to be aware that the use of government symbols or Coat of Arms generally requires special permission. For example, the Commonwealth Government Coat of Arms may only be used with the permission of the Department of Prime Minister and Cabinet, and use without such permission may breach laws including Section 53 of the Trade Practices Act 1974 (relating to false or misleading representations) and Section 145.1 of the Criminal Code Act 1995 (relating to forgeries)⁸. Similar consent obligations generally apply in relation to the use of State and Territory government symbols or Coats of Arms.

4.5.2 Other brands and symbols

As a general rule, if a mark is proposed to be used on a smartcard, consideration needs to be given to whether permission or licenses are required (e.g. from the owner or licensor of the mark).

Agencies should be aware that there is also specific legislation that restricts the use of particular types of marks (e.g. under the Advance Australia Logo Protection Act 1984, the Olympic Insignia Protection Act 1987).

4.5.3 Security considerations

Note that printing information relating to employer and place of work on the surface of an employee ID badge can raise the risk of theft of the card for unauthorised access. For this reason, some organisations print a bare minimum of data on their employee cards that provides some contact information to allow lost cards to be returned. The use of smartcard technology and storage of cardholder data on the chip enables more flexibility and security in the way organisational details are managed.

⁸ More information is available at <http://www.itsanhonour.gov.au>

4.6 Multi-application smartcards – privacy implications

If a smartcard is proposed to be used for multiple applications, this can be expected to raise specific privacy law compliance issues. An example of a multi-application card is where a card issued for a specific function (e.g. as a public transport ticket), may also operate as an electronic purse, a loyalty card and a mechanism for accessing particular types of local government services.

This is because it can be expected that multi-application smartcards will store a range of personal information and other information in various locations such as:

- the face of the card
- in a chip in the card; and
- in a “security protected” section of a chip in the card.

This means that it will be important that the technology used to support the smartcard is capable of distinguishing between different types of users and different types of uses so that:

- those relying on the card are only able to access that personal information stored on the card which is necessary for the relevant transaction; and
- other personal information stored on the card is reasonably secure against unauthorised access.

Otherwise, there will be challenges in complying with obligations under privacy laws.

4.7 Liability issues

4.7.1 Statutory liability

It is assumed that all agencies implementing smartcards will prioritise compliance with their statutory obligations.

To ensure that staff are aware of the importance of compliance, agencies may wish to consider informing staff of the potential consequences of breaches, including:

- adverse determinations by privacy regulators. Such determinations may require the payment of compensation⁹, or the taking of other steps to rectify privacy breaches
- publicity about breaches of statutory obligations damages public trust and the agency’s reputation; and
- prosecutions in Court (e.g. by fair trading regulators or owners of intellectual property), which can be potentially time consuming, costly and embarrassing (if breaches of laws are found).

⁹ It is important to note that in some jurisdictions, “representative complaints” (or complaints on behalf of a class of individuals) may be brought before privacy regulators, and if breaches of privacy laws resulting from the use of a smartcard are demonstrated, this could lead to significant liability

4.7.2 Contractual liability

The allocation of risk between the agency, its vendors and smartcard users will need to be managed through the development of appropriate contractual terms.

Liability arrangements with the agency's vendors will be a commercial matter for negotiation between the parties – subject to the overriding procurement guidelines applicable to the agency. The agency's position will need to be determined in accordance with a thorough risk assessment – focusing on key areas of risk to the agency such as loss of data, breaches of applicable privacy laws, and breaches of security obligations that have the potential to expose the agency to the risk of fraudulent or unauthorised access.

5 Security issues

One of the essential characteristics of smartcards is that they can provide a secure environment to store data and applications. Although no system or smartcard can be configured to be resistant to all physical tampering attempts (when time and money are no object), breaking into a smartcard is generally considered to be a process that requires substantial time and energy.

This section identifies some of the security issues that may need to be considered before and during the implementation of a smartcard project.

This section is structured as follows:

- Overall security design of the smartcard
- Key management issues
- Card production issues
- Card initialisation issues; and
- Card personalisation issues.

5.1 Overall security design of the smartcard

When designing the card and card system, agencies must take into account any security policies, practices and procedures that provide a protective security environment. For example, Australian Government agencies must be compliant with the Australian Government Protective Security Manual (PSM)¹⁰ and the Australian Government Information and Communications Technology Security Manual¹¹ (ISM). State and territory governments may have their own implementation guidelines or other specific localised standards for information security design. Where applicable, these sorts of standards should be consulted. Section 6.2 provides more information on jurisdictional security compliance.

The ISM states that Australian Government agencies must have security risk assessments, policies and plans that cover ICT systems. These documents should be consistent with the agency's high-level security documents:

- Agency Security Policy
- Agency Security Risk Assessment; and
- Agency Security Plan

¹⁰ [http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual\(PSM2005\)](http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(PSM2005))

¹¹ <http://www.dsd.gov.au/library/infosec/ism.html>

5.1.1 Smartcard components

Smartcard security is typically addressed by four components¹²:

- card body – the face and reverse of the card, including the chip
- chip hardware
- operating system; and
- applications running or held on the chip

Smartcard security may only be assured when the defence mechanisms for each component are working properly and in concert. Further, the card is only one component in a smartcard system. Other components, such as back-end and network infrastructure, reader technology, card and reader issuance processes and the cardholder and card network services within the environment, must be equally secured to achieve high levels of trust. Each of these must be subject to continuous lifecycle security analysis and risk treatment.

5.1.2 Types of attack

Unlike many other high-security systems, which are typically developed for a special function and used by trained specialists in relatively small numbers, smartcards are intended for large-scale use in a broad range of applications. Whereas the system operator is in control of all the components of an IT system, once smartcards have been issued to end-users they are out of the physical control of the service provider. This exposes the smartcard to particular risks and attacks.

Attacks can typically be categorised into three distinct groups¹³.

- Physical attacks – attacks that are targeted at the smartcard chip. Successful physical attacks usually require sophisticated technical equipment, since it is necessary to obtain physical access to the smartcard's chip components in order to, for instance, use optical or voltage analysis to observe data exchanges between the central processing unit (CPU) and memory locations in the chip. Physical attacks can be either static, which means that no power is applied to the microcontroller during penetration attempts, or dynamic, with the microcontroller operating. Examples of attacks at the physical level are static and dynamic tapping of microcontroller internal signals and manipulation of microcontroller behaviour
- Logical attacks – attacks that are targeted on the operating system or applications residing on the card. This category includes cryptanalysis, message protocol manipulation of data or card handling processes, attacks that exploit known faults in smartcard operating systems, backdoors or Trojan horses in the executable code of smartcard applications; and
- Social attacks - attacks that are primarily directed against people that work with or use smartcards. These can be chip designers working for semiconductor manufacturers, software

¹² Based on the Smartcard Handbook, by Wolfgang Rankl and Wolfgang Effing [third edition]. Published by John Wiley and Sons

¹³ Based on the Smartcard Handbook, by Wolfgang Rankl and Wolfgang Effing [third edition]. Published by John Wiley and Sons

designers, card issuance staff or back-end systems operational staff and card users. Examples of social attacks include the use of coercion or financial inducements to gain unauthorised access to smartcard data or business processes and exploiting naïve cardholders. Typically, these types of attacks can only partially be countered by technical measures.

5.1.3 Examples of counter measures

An overview of some examples of common counter measures to be considered for each of the described types of attacks is provided below:

- Physical attacks
 - use of smartcards and readers with physical security certification
 - use of certified Hardware Security Modules (HSMs) to protect keys at the back-end
- Logical attacks
 - use of smartcard operating systems, applications and middleware security certifications
 - application security evaluations (e.g. application/code reviews and application evaluations by the Defence Signals Directorate)
 - developing software in small functional building blocks that can easily be understood and validated by smartcard application developers and code reviewers
 - using mathematical models to prove the soundness of functions
 - use of expert independent advice on cryptographic and other security methods
 - digital signing of applications and data by the relevant application provider
 - data and application are only disclosed after successfully entering the PIN code
 - configuring the chip so that it locks after a number of unsuccessful access attempts
 - applications and data can only be changed by the authorised application provider (e.g. usage of secure card readers)
 - applications and data are only to be loaded onto the chip, changed or removed with consent of the user (after entering the correct PIN code)
 - implementing safeguards during the application load process ensures the authenticity, integrity and confidentiality of the application code and data, i.e. creating access controls to be able to write data
 - unilateral or mutual authentication of the smartcard and card reader
- Social attacks
 - cardholder education and awareness

- agency anti-fraud training
- strong smartcard system security governance
- rigorous fraud detection and prosecution measures.

5.1.4 Security evaluations/certification

To obtain assurance about certain security features offered by smartcards, smartcard components can be assessed by third parties. There are various standards that apply to security evaluations for smartcard products. The most common certification processes used is Common Criteria.

Common Criteria (CC)¹⁴ is a means to define, assess, and validate the security aspects of IT products. Agencies using security products can define their technical security requirements for a type of product in a Protection Profile (PP). Smartcard developers may be required to undergo evaluation testing to show compliance of their product to a PP described in the developer's Security Target. The Common Criteria distinguishes between seven sets of tests, called Evaluation Assurance Levels (EAL). These levels range from EAL 1, which is a simple and brief examination of the product to EAL 7, which is an extremely detailed examination of the product, its documentation and design processes. Because CC certification is recognised internationally, the developer's investments can be used to fulfil the requirements of different customers worldwide.

Some important factors to consider regarding CC evaluation are:

- Protection Profile – the security requirements are defined in a Protection Profile (PP). The PP defines the agency security requirements regarding the smartcard product. PPs can be defined by anyone. One of the main challenges in developing PPs is to be specific and complete. Ideally, the PP is based on a comprehensive threat and risk analysis performed by the agency. Further, various PPs are available for smartcard products and can be (re)used¹⁵. An important element to consider is that the PP is fit for purpose and covers all security requirements of the smartcard
- Definition of the Security Target – the security functionality claim is defined in a Security Target (ST). The CC has strict requirements for the content of the ST. The ST is typically written by a developer and can be based on one or more PPs. Writing an ST is a fairly difficult task because formal CC dedicated requirements must be specified. During the development of a ST, one or more PPs can be used. Certain choices in the ST can influence costs and duration of the evaluation. Agency responsibilities are to verify whether the ST is fit for purpose and addresses all required functionality and security requirements
- Evaluation Assurance Level (EAL) – the agency and/or developer should determine what Evaluation Assurance Level is required. An ST may be used for all seven EALs. The EAL dramatically influences the time and costs of the evaluation. It is the responsibility of the agency to verify that the EAL provides a sufficient level of assurance that is fit for purpose.

¹⁴ <http://www.commoncriteriaportal.org/>

¹⁵ An overview of PPs can be found at <http://www.commoncriteriaportal.org/public/developer/index.php?menu=7>

- Costs and timing – costs and time of a CC evaluation can be substantial and typically depend on:
 - how much and what functionality is to be certified
 - how much testing is required to be done (the EAL); and
 - how 'good' the smartcard product is and how well the design has been documented.

Evaluation costs for EAL 4 and higher can easily exceed A\$250,000, excluding potential costs for adapting the product and updating design documentation. Because of their large market size, EAL 4+ certifications for the chip and operating systems are relatively common. Security certifications for smartcard applications, card readers, middleware and front/back office applications, however, are far less common due the significant investments required for the developer and the typically smaller market size. EAL4 certifications may take between 9 to 12 months to complete under ideal¹⁶ circumstances.

Alternatives

Alternative certifications that may be considered include:

- Product certifications – there are older standards (mainly the European ITSEC) but these are often dated and localised. For instance, while ITSEC is still recognised in Australia it is not recognised in the United States. This certification are being replaced by the Common Criteria.
- Process certifications – the smartcard development, production or security processes may be evaluated or certified. Examples are:
 - ISO/IEC 9000 series for generic process quality evaluation and certification
 - ISO/IEC 27001 for Information Security Management evaluation and certification
 - design processes such as ISO 15504 (Software Process Assessment) or the Capability Maturity Model for Software (CMM) and the Systems Security Engineering CMM (SSE-CMM).

These certifications, however, only provide assurance about the smartcard developers' processes and do not provide any assurance relating to the smartcard product.

- US Federal Information Processing Standards (FIPS) - The Federal Information Processing Standards Publication Series of the US National Institute of Standards and Technology (NIST) is a series of publications relating to standards and guidelines for IT security. NIST has defined various FIPS standards that may apply to smartcard products, including FIPS 140-2 and FIPS 201-1. An overview of FIPS standards that may apply to smartcards can be found on the NIST website¹⁷.

The main advantage of FIPS is that specific requirements have been defined for specific products. As a consequence, FIPS might not address all smartcard required functionality. Furthermore, as FIPS is a United States government standard it does not necessarily apply in the Australian government environment. Additionally, local products may not have been certified against the FIPS standards.

¹⁶ In cases where the product and design documentation is correct the first time

¹⁷ Refer to <http://csrc.nist.gov/publications/fips/index.html>

5.2 Key Management issues

Key management refers to the procedures and processes used to generate, distribute, protect, renew and destroy as required the various cryptographic keys that apply at all levels of the smartcard technology stack to minimise the risks of key compromise. Key management may apply to:

- card issuance and application keys (symmetric and/or asymmetric)
- card reader keys (symmetric and/or asymmetric)
- card to reader or reader to system communications session keys (typically symmetric)
- keys used in the general smartcard network, such as VPN keys.

Significant key management issues to consider include the following:

- public key methods can be used, where fit-for-purpose, without necessarily resorting to a full X.509 PKI implementation (refer to Gatekeeper¹⁸ for further details)
- typically, public key methods are considered slow for use in high performance card applications. For example transit card schemes use derived symmetric keys for card accesses at high throughput entries and exits, and as a natural corollary, this method is also used at other readers where performance metrics are less severe
- public key methods based on RSA or discrete logarithms may result in large key storage allocations and potentially unwanted network loading. This is specifically significant in small footprint systems such as smartcard authentication schemes over low data rate channels
- public key methods are well suited to use in creating signatures over configuration data and hotlist distribution. Accordingly if the public verification key is exposed, provided the private signing key is protected, it does not facilitate message counterfeiting
- simple symmetric key diversification algorithms are very efficient for use in one-to-many relationships such as those between reader and cards, or between system and readers. However, they cannot provide the same level of functional separation between signer and verifier, or between encryptor and decryptor
- a potentially significant number of keys may be required to provide cryptographic separation between system or card application functions.
- examples of keys in common use include various high level administrative keys for establishing supply and other arrangements:
 - card issuance transport keys
 - card issuance production keys including key encrypting keys

¹⁸ Gatekeeper is a requirement for all Australian government agencies. Further information about Gatekeeper can be found at www.gatekeeper.gov.au

- card identity and application discovery keys
 - application issuance keys, including key encrypting keys
 - application file access keys (separated by create, read, write, erase and other)
 - special purpose signature keys
 - issuer data set signature keys
 - reader/terminal configuration and key management keys
 - reader to host mutual authentication keys
 - card usage data protection keys
- a prudent card key management design provides successive versions of keys which allow successive generations of cards to be dissociated from each other. The security benefit is strongest where the card authentication process is on-line to a trusted back-end, and weakest where off-line readers are used and where the exposure of one key through reader penetration implies the exposure of all generations of master keys
 - the use of tamper resistant hardware security modules wherever card or mission-critical keys are needed in an unencrypted form is vital to most key management infrastructure. Such modules may include smartcard chip based SAMs in reader equipment and more complex host security modules at back-end systems. Security modules should be issued and managed in an analogous manner to smartcards
 - cryptographic testing and validation of key management processes should include assessing whether:
 - key generation and activation occurs within a secure cryptographic device that is fit for purpose¹⁹. Appropriate security enforcing functions may be implemented and based on a comprehensive threat and risk analysis, meeting the DSD EPL required Standard
 - keys are generated as defined using (n out of m) multi-person control
 - key usage is as defined (for example, a CA's signing key is typically only used to sign Certificates and CRLs)
 - key usage purposes are correctly entered (as per X.500 version 3 usage field)
 - key life span for keys issued is as defined
 - key generation uses a prescribed random number generator (RNG) or pseudo random number generator (PRNG) on the Defence Signals Directorate Evaluated Product List (DSD EPL) or otherwise deemed fit for purpose by DSD

¹⁹ Security enforcing functions should be based on a comprehensive Threat and Risk Analysis

- public key generation uses (if required) a prescribed prime number generator on the DSD Evaluated Product List (EPL) or otherwise deemed fit for purpose by DSD
- key generation uses a key generation algorithm that adheres to the standards defined by Gatekeeper. Refer to Section 6.4 for more information on Gatekeeper.

5.3 Card production

Card production is typically performed by specialised card manufacturers. Major smartcard security concerns related to card production include:

- Security certifications – this entails process and security certifications of the card producer and security evaluations of chip, operating system and applications
- Transport keys – transport keys are used to protect the file layout of the card between different sites by verifying the files before any initialisation or personalisation
- Master keys – in order to ensure a high level of security, master keys used should not be disclosed to any single person or ever kept in a readable form. The master keys are generated by the hardware at a secure computer terminal and the output is often split into two or three key parts
- Derived keys – while using keys provides security, when all cards share the same set of keys this can be an issue if the keys become compromised. A preferred option is to have unique keys for each cardholder. The technique used to achieve this involves deriving the keys by combining a master key and some feature unique to the cardholder, e.g. card serial number
- ROM or chip password – to prevent unauthorised changes to the chip structure during the card initialisation process, knowledge of the ROM password should be controlled. The ROM password is used to erase the EEPROM before writing data to it
- Environment – the security environment at the card production site, especially with regard to the secure storage of non-personalised cards
- Readers – the security of the storage of card reader(s) being used to erase the EEPROM and write data to it; and
- Secure storage - non-personalised cards should be securely stored. This is especially important when smartcards are pre-personalised with generic characteristics and physical security features such as Optical Variable Devices (OVDs).

5.4 Card personalisation

Card personalisation may occur in the same facilities where the non-personalised smartcards are manufactured, but may also be performed at different locations by a specialised personalisation facility.

The principal security concerns during card personalisation to be considered include:

- Personalisation keys - when the card is to be personalised with cardholder-specific data (including passwords, certificates, keys) it may be necessary for the data to be securely encrypted during transport to the card personalisation site. To prevent any unauthorised access, personalisation keys can be loaded onto the card during initialisation and are used by the chip to decrypt the cardholder data before storing it in the EEPROM. The advantage of this method is that the party conducting the personalisation activity does not know the secret data in the card and also has no possibility of intercepting it by tapping data lines
- Logistics – secure storage of non or pre-personalised cards received from the card manufacturer
- Secure generation of cryptographic keys – although some cards are capable of generating cryptographic keys, this is a very slow process. Often it is more efficient to generate cryptographic keys in a specific hardware security module and load the keys onto the smartcard. The generation and load process should be adequately protected, minimising the risk of unauthorised disclosure of keys
- PIN code generation – initial PIN codes are typically generated during the personalisation process. To prevent PIN codes from unauthorised disclosure, PIN codes should be random, generated in secure devices and printed in secure PIN mailer forms. The PIN mailer may be constructed in such a way that an unauthorised person cannot read the printed PIN code without visibly damaging the envelope. The PIN mailer should be stored in a different location to the smartcard, thereby reducing the risk of a compromise
- Accountability and destruction of defects – Smartcards that contain errors and/or defects should be accounted for and securely destroyed to prevent those cards from being used
- Card management system (CMS) – the CMS will play a very important role in the lifecycle management of smartcards. A CMS provides the management and processing engine to manage smartcards from registration and initial issuance through to expiry, revocation, replacement and update. As the CMS will hold cardholder registration details and will interface with smartcard personalisation systems, the CMS and its interfaces should be adequately secured. Further, the CMS may be subject to a security evaluation (e.g. Defence Signals Directorate ISM); and
- Secure location of equipment – pre-personalisation equipment should be adequately protected and subjected to appropriate environmental and logical controls.

5.5 Card distribution and issuance

Card distribution and issuance may be performed by a different party and at a different location to where card personalisation occurs. Below is listed the key security concerns during card distribution to be considered:

- Distribution of cards and PIN mailers – cards should be securely stored prior to issuance and stored separate from PIN mailers at all times. Typically, PIN mailers are sent a few days earlier or later than the card. Further, in some cases it may be appropriate that the cardholder personally collect the smartcard at an issuer or registration point; and

- Activation – cards may be lost during distribution between various parties involved in the manufacturing, personalisation and issuance. Therefore, agencies may consider having the smartcard activated by means of entering a separate activation code through a specific website²⁰ or have it activated during physical issuance (e.g. by changing the PIN code).

The production, personalisation and distribution steps described above typically represent a standard mass production scenario. Agencies or card issuers may have other requirements with regard to card production. For example, some smartcards may be pre-personalised by a specific manufacturer but be personalised 'on site' at the agency or at a registration point and then directly issued to the cardholder. This is dependent upon the agency business and security requirements.

5.6 Supply Chain Security

Card reading devices are usually tamper-proof. Nevertheless corruption and collusion are possible in the supply chain from factory to operating site, and in operation. Card reading devices may be physically compromised to affect their integrity, confidentiality or availability in operation.

A compromised device may affect the information being processed and transferred to and from cards or other connected systems. In particular sensitive information may be recorded and transferred to a third party by on- or off-line means. Data used by cards in financial transactions is particularly at risk if decrypted at any stage.

When acquiring card reading devices care should be taken to select suppliers with effective security throughout their supply chain and ensure that contractual remedies are available in the event of compromised devices. Operating procedures should be established to ensure that any compromised card reading devices are quickly detected in operation.

²⁰ Use of the internet for activation may introduce a distinct set of risks that need to be considered appropriately

6 Governance, Compliance and Policy issues

Various governance and compliance criteria and policy requirements apply to the business, technical and operational aspects of smartcard deployments. These criteria and policies play an important role in establishing accountability, security, transparency, interoperability and equitable business practices related to smartcard implementations. General governance principles apply but increasingly, smartcard specific frameworks are also being developed that agencies will need to be aware of.

The following sections describe specific governance, oversight and policy framework issues that may need to be considered by CoPs before and during the implementation of a smartcard project. Topics that will be discussed are:

- Governance and compliance in general
- Gateway Review Process
- Gatekeeper
- National e-Authentication Framework (NeAF)
- Identity Management for Australian Government Employees (IMAGE)
- National Name and Address XML Schema
- The Australian Government Protective Security Manual (PSM)
- The Australian Government Information and Communications Technology Security Manual (ISM); and
- National Identity Security Strategy (NISS)

Note that it is not the purpose of this Guide to canvass all applicable governance, compliance and policy issues that might apply to a smartcard project. Like all government projects, most smartcard deployments may be required to undertake processes like Gateway reviews, and to comply with various laws and regulations with their own jurisdictions.

All agencies should be aware of the governance and compliance issues that are applicable within their environments.

6.1 Governance and compliance in general

There are several types of governance and compliance frameworks that may be considered for smartcards. Each of these is aimed at assessing a level of monitoring and compliance in the respective areas of project management, areas of security, privacy, policy and process.

Depending on the specific framework, compliance may need to be periodically validated by means of self assessment, reviews or audits.

Typically, compliance with governance frameworks is driven from:

- federal, state, sector and agency specific jurisdictional and legal requirements
- industry and sector specific regulations and guidelines
- corporate governance requirements; and
- business and security requirements.

Achieving compliance and certification with governance frameworks can be expensive and time-consuming. However, IT project experience frequently demonstrates that Return on Investment (ROI) is improved when governance is approached as an embedded part of the proactive risk management process and a continuous business improvement program, and is incorporated into project business cases and detailed design. Benefits can include:

- improved interoperability as a result of better standards compliance, with long term improvements in re-use and sharing of infrastructure
- improved transparency, enhanced user control and trust in government systems, with better take-up of services as a result; and
- efficiencies through the reduction of errors, and earlier detection of issues, by judicious application of Threat & Risk Assessment, Privacy Impact Assessments at appropriate milestones and similar governance and risk management tools.

A standard that provides guidance on corporate governance of ICT is AS/NZS 8015-2005: Corporate governance of information and communication technology. The standard articulates its guidance using a simple framework – three tasks (evaluate, direct and monitor) and six principles. The tasks are described in the context of how ICT is used in support of business processes, through projects to establish new capability and operations of existing capability. In carrying out the three tasks, CoPs should evaluate, direct and monitor directly or through appropriate delegation:

- evaluate the use of ICT in the context of the environment in which the CoP operates and the aspirations the CoP has established for itself. The scope of evaluation should include existing assets – equipment, software, data and other resources, and proposed investments
- direct the use of ICT by:
 - setting top-level policies
 - determining the role of ICT as a fundamental aspect of the agency's overall business direction and strategy
 - assigning responsibility for detailed planning and control of how ICT is used by the agency
 - controlling the allocation of resources
- monitor performance and conformance of ICT – not in terms of technical statistics, but in respect of business operations, goals and direction. Performance and conformance monitoring should provide ongoing assurance that the members of the CoP can continue to conduct their business in the short to medium term, and can attain their objectives in the medium to longer term.

The following sections describe how a smartcard implementation can relate to certain security frameworks. It should be noted that the NeAF and IMAGE Frameworks are voluntary better practice policy frameworks.

6.2 Jurisdictional compliance issues

In general terms with regards to governance, compliance and policy, there is not a great deal of variation in legislation and regulations across Australian jurisdictions. This is in contrast to privacy where it is important to take note of fine differences in legislation between states and territories, and certain sector specific requirements, as discussed in Section 4.2.

Perhaps the greatest interest around compliance in smartcard deployments will pertain to information security and information risk management. Most, if not all, jurisdictions in Australia that have considered these matters in detail have taken a consistent approach based on the following two standards:

- AS/NZS ISO/IEC 27001: Information technology – Code of practice for information security management; and
- AS/NZS 4360: Risk Management

Certain states have developed their own more detailed implementation guides based on these general standards. The main examples are:

- The New South Wales Government Chief Information Office has published a set of Information Security guidelines, available at <http://www.gcio.nsw.gov.au> (under the link Publications > Guidelines); and
- The Queensland Government Chief Information Office has published a series of Information Standards and Guidelines, including Information Security IS18 available at http://www.qgcio.qld.gov.au/02_infostand/standards/is18.htm

As a rule, agencies planning to deploy smartcards in particular jurisdictions should explore whether governments there have developed their own information security and risk management guidelines and should acquaint themselves with those guidelines where applicable.

6.3 Gateway Review Process

Agencies subject to the Financial and Management Accountability Act 1977 (FMA Act) should be aware that some projects may be subject to the Gateway Review Process (Gateway) where such projects meet the financial and risk thresholds.

Gateway is a project assurance methodology. It involves a series of brief, independent reviews at critical stages in the development and implementation of a project. At key decision points (referred to as Gates), a Gateway review focuses on the issues that are important to the project at that stage of the project's life. The Gate 1 - Business Case review examines the robustness of the Business Case and the project's readiness to proceed to the next phase. FMA Act agencies are advised to acquaint

themselves with Gateway guidance material, particularly that referring to the Gate 1 - Business Case review in preparing a Business Case.

Detailed information on the Gateway Review Process is available from Finance online at www.finance.gov.au/gateway.

6.4 Gatekeeper

Gatekeeper 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. AGIMO is responsible for maintaining the framework.

The Gatekeeper PKI Framework governs the use of PKI in the Australian government for the authentication of organisations and individuals by means of digital certificates. The Framework provides a whole-of-government approach that delivers integrity, interoperability, authenticity and trust for agencies and their clients. The Framework is underpinned by a standards-based, technology-neutral accreditation program for issuers of digital certificates.

AGIMO has developed a suite of documentation to give operational support to the Framework. Where smartcards are implemented in conjunction with PKI services and components, project managers should refer to the Gatekeeper documents which are available at the Gatekeeper website²¹.

6.5 National e-Authentication Framework (NeAF)

The National e-Authentication Framework (NeAF) will assist agencies, jurisdictions and sectors in authenticating the identity of the other party to a desired level of assurance or confidence. The NeAF encompasses the electronic authentication (e-authentication) of the identity of individuals and businesses dealing with the government, on one side of the transaction, as well as the authentication of government websites on the other side. The NeAF positions e-authentication within the broader context of an agency's approach to identity and risk management and provides guidance on developing the processes and technology required to provide the desired level of confidence.

While the Framework supports an agency-specific model where each agency develops its own, separate technology solution, it recognises and accommodates broader sectoral and whole of government e-authentication initiatives.

²¹ Refer to www.gatekeeper.gov.au

The NeAF comprise a set of principles, a standardised set of assurance levels, and a standardised approach and process for determining assurance levels and related e-authentication solutions. It provides guidance on models for the implementation of e-authentication solutions and planning standards for website authentication.

e-Authentication represents the process that delivers (a level of) assurance of the assertion of identity made by a user. The level of assurance required will be dependent upon the level of risk associated with the transactions that the user will undertake, and the mitigating factors, other than e-authentication that will reduce this risk. A range of assurance levels are possible. In NeAF, five assurance levels are prescribed calibrated from minimal through high.

Achieving the required assurance level for the e-authentication solution is then a function of the strength of the registration and enrolment processes on the one hand, and the strength of the user's e-authentication credential (e.g. userid+password, biometric) and its on-going management on the other. This is illustrated below.

Strength of Registration	4	Minimal	Low	Moderate	High
	3	Minimal	Low	Moderate	Moderate
	2	Minimal	Low	Low	Low
	1	Minimal	Minimal	Minimal	Minimal
	0	Null (0)	Pseudonymous Minimal	Pseudonymous Low	Pseudonymous Moderate
	0	1	2	3	4
		Strength of Authentication Mechanism			

Mapping of Assurance Levels

The Framework identifies a seven-step process for assessing the strength of authentication demanded by the transaction, the technology components that will provide the desired authentication strength, and the business processes that are required to achieve this level of authentication.

This is an iterative process that takes into account existing controls, the possible consequences of incorrectly authenticating the parties to the transaction and the likelihood of these consequences eventuation.

6.6 Identity Management for Australian Government Employees (IMAGE)

The Identity Management for Australian Government Employees (IMAGE) Framework is a better practice approach for Identity Management of Australian Government employees and contractors. AGIMO is responsible for maintaining the framework²².

IMAGE is intended to facilitate the adoption of a consistent approach to identity management within Australian Government agencies. It aims to promote trust between government agencies in staff identification processes employed by each government agency.

IMAGE comprises a standard set of business processes and standards in relation to identity verification, card specifications and data storage that support the issue of smartcards which can be used as an identity credential for physical and logical access, where required. In this regard the IMAGE Framework should be read in conjunction with this Framework.

6.7 The Australian Government Information and Communications Technology Security Manual (ISM)

The Australian Government Information and Communications Technology Security Manual (also known as the ISM) has been developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government agencies on how to protect their ICT systems.

Australian Government agencies are required by the Protective Security Manual (PSM) to comply with the ISM. Agencies must consider the security implications of their IT systems and devise policy and plans to ensure the systems are appropriately protected. Although security needs will be greatest when national security classified or non-national security classified information is being processed, even unclassified systems with no special safety, mission critical, or financial implications should have some degree of protection if a reliable or accurate service is to be maintained.

6.8 National Identity Security Strategy (NISS)

The NISS is an Australian Government initiative to improve identity security, combat identity crime and protect the identities of Australians from being used for illegal purposes.

More information can be found on www.ag.gov.au.

²² Refer to <http://www.finance.gov.au/e-government/security-and-authentication/image-framework.html>

7 Risk management and risk mitigation issues specific to smartcard implementations

Smartcard implementations may bring significant challenges in how government agencies electronically transact, process and record information. Smartcards often form critical infrastructure to governments and may be used to secure transactions, provide access to sensitive data and identify end-users or employees. These challenges will carry risks, which need to be formally managed to avoid or minimise the consequences of their potential occurrence.

This section covers specific risk management and risk mitigation issues for smartcard implementations. The sections below address the following elements of risk management and mitigation:

- Risk management methodology
- Smartcard risk categories and mitigation strategies

7.1 Risk management methodology

Smartcard deployments can be characterised as complex projects. They usually involve a large number of stakeholders and often carry and protect sensitive and valuable information related to stakeholders. Furthermore, once a smartcard deployment has moved to a large rollout of smartcards, it is usually difficult and costly to make changes to the infrastructure and implementation model.

A structured and managed approach towards risk management for smartcard deployment is therefore crucial for successful smartcard implementations. Especially as smartcard deployments face risks additional to the usual project risks including:

- Legal and compliance risks – sensitive cardholder data may be stored in backend systems or on/in the smartcard. Stringent laws typically cover the custody of sensitive data, and significant legal and business consequences can arise if those laws are breached. A conservative approach to mitigating legal risks in this area is advisable, not only because the impact of legal proceedings can be difficult to predict and contain, but also because any appearance of compromising on legal safeguards is likely to undermine acceptance of new smartcard technologies
- Theft or loss of smartcards – one of the primary risks that end-users face is theft or loss of their smartcards. Established revocation and re-issuance processes are required to re-enable service access for cardholders, otherwise the degree of user access, user satisfaction and/or agency reputation may be compromised
- Identity theft – a severe risk in smartcard projects lies in the theft of smartcards together with the possible associated PIN / passwords where one person can impersonate a legitimate smartcard holder
- Card Management Issues – card management issues associated with multi-application smartcards that result from the interactions between the different entities that issue, update and rely on the card data; and

- Lack of standardisation – smartcard standardisation can be ambiguous and can be interpreted differently between the various entities. This leads to the significant risk of systems that are not interoperable or dependent on one vendor. CoPs will need to determine what chosen application interfaces (referred to as stacks) are to be the standard for their deployment.

The primary purpose of risk management is to identify and minimise the likelihood and/or impact of adverse events during the project and after implementation. Risk management involves establishing an appropriate infrastructure and culture; and applying a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organisations to minimise losses and maximise gains²³.

Recognised risk management practices clearly identify that not all risks can be avoided and seek to reduce both the likelihood and impact of a risk eventuating. Strategies may include implementing controls to mitigate the risk, transferring the risk to another party and accepting some or all of the potential consequences of a particular risk.

Agencies should implement risk management practices in accordance with appropriate Australian standards such as AS/NZS 4360: Risk Management.

7.2 Smartcard risk categories and mitigation strategies

For the purposes of rating identified risks, the potential impact of the risk occurring and the likelihood that it will occur should be assessed. Critical risks that can have an adverse impact on the smartcard project's success are then given maximum importance and strategies are formulated to deal with them. A framework can be used to classify both project and business related risks.

The following risk categories have been specified as examples:

- Strategic risks – risks that are generated by the broader environmental context of the smartcard project, including funding approval, public acceptance, policy changes, duplication, scope creep
- Project risks – risks that are generated inside the project operations, including the delivery of project objectives, planned methodology, quality, costs and timeliness of delivery.
- Implementation and integration risks – risks that are generated by the immediate context of the project, including relationships with involved stakeholders; and
- Information security risks – risks specific to confidentiality, integrity and availability of cardholder data.

While any major project will have many risks, the following table (non exhaustive) lists risks that can usually be found in most smartcard implementation projects and may be in the high risk category. For each risk, example mitigation strategies have been identified.

²³ This definition is based to AS/NZS 4360:2004 SET Risk Management

#	Description of risk	Category	Example Mitigation Strategies
1	Decision made not proceed with the smartcard project	Strategic	<p>Development of a comprehensive business case that clearly expresses the benefits and costs of the smartcard implementation (both in quantitative and qualitative terms)</p> <p>Establishing an Advisory Board representing stakeholder and community interests to advise the project sponsor</p>
2	Lack of community support / acceptance of project	Strategic	<p>The implementation program should incorporate a substantial education and communication campaign to educate the stakeholders and community around the nature and use of the smartcard</p> <p>Conducting a Privacy Impact Assessment</p>
3	Change in stakeholder attitudes or requirements	Strategic	<p>While maintaining a focus on delivering is critical to success, major review points may be incorporated into the project, where issues arising from the Advisory Board or from additional privacy impacts assessments might be considered</p>
4	Disinvestments of current infrastructure components	Strategic	<p>The implementation model may utilise existing infrastructure components as much as possible and prevent 'green field' operations</p> <p>A transition period may be used to allow stakeholders to phase out existing infrastructures</p> <p>The smartcard project may be viewed from a 'whole of government' perspective and a delivery and management structure may be established outside of existing agencies and private organisations</p> <p>Establishing a clear point of accountability for delivery of the project and realisation of benefits</p> <p>Benefits and benefit owners should be clearly defined</p>
5	Failure to execute the project	Project	<p>A Program Office, responsible for coordinating and overseeing the build and implementation of the solution should be established</p> <p>Substantive changes to scope and functionality may be the subject to a separate business case</p> <p>Avoiding complex integrations or large-scale changes to existing public or private sector systems</p> <p>Adopting mainstream standards for infrastructure, interface and registration processes</p> <p>Project monitoring and assurance by an independent body</p>

#	Description of risk	Category	Example Mitigation Strategies
			Strong project management
6	Unable to meet deadlines	Project	<p>Clear and unambiguous communications of expectations, tasks and deadlines</p> <p>Clear escalation processes</p> <p>Project monitoring and assurance by an independent body</p>
7	Self-interest of stakeholders influences outcome	Project	<p>Development and implementation of the smartcard solution may remain operationally independent of agencies, relying parties and technology vendors</p> <p>Clear and unambiguous agreements between stakeholders</p> <p>Project monitoring and assurance by an independent body</p>
8	Loss of focus on key objectives	Project	<p>After approval of the high level design, any additional functionality or application may be made subject to a separate business case</p> <p>Adoption of thorough change management procedures and protocols</p> <p>Clear definition of scope is to be provided in the business case and high-level solution design</p> <p>Clear use cases may be developed, which are consistent with the principal objectives of the smartcard project</p> <p>Project monitoring and assurance by an independent body</p>
9	Extensive customisation beyond approved smartcard business case	Project	<p>Development of thorough change management procedures and protocols</p> <p>Project monitoring and assurance by an independent body</p>
10	Liability issues between stakeholders	Project	<p>Clear and unambiguous tender process</p> <p>Clear and unambiguous Request for Tenders (RFT)</p> <p>Development of a comprehensive liability framework that stipulate the rights, obligations and liabilities of the stakeholders, including relying parties, vendors and end-users</p> <p>Conducting a legal assessment</p> <p>Project monitoring and assurance by an independent body</p>

#	Description of risk	Category	Example Mitigation Strategies
11	Legal implications of smartcard deployment (privacy)	Implementation	<p>Conducting a legal assessment</p> <p>Conducting Privacy Impact Assessments at appropriate milestones</p>
12	Errors in charging service costs/fees	Implementation	<p>Costs and benefits may be determined during a business case</p> <p>A comprehensive cost and charging model may be developed in the Design phase</p>
13	Use of unproven technology	Implementation	<p>The design of the smartcard solution may only consider tried and proven technologies</p> <p>An extended period of system and stress testing may be considered prior to deployment</p> <p>Continuous unit, module, application and infrastructure testing</p>
14	Poor response times/ inability to scale to handle production volumes	Implementation	<p>An extended period of system and stress testing is may be considered prior to deployment</p> <p>The architecture design may take scalability into account</p>
15	Failure to integrate smartcard with stakeholder systems and broader government and private sector initiatives	Implementation	<p>Design may make use of non-proprietary and industry accepted standards for technical infrastructures, smartcards, smartcard readers, interface, authentication and application integration technologies</p>
16	Vendor lock-in due to either ambiguous or lack of specific standards	Implementation	<p>Clear an unambiguous tender process</p> <p>Clear, detailed and unambiguous RFTs, based on industry accepted standards</p> <p>Intellectual property and licensing to be addressed prior to tender</p>
17	Poor or inconsistent integrity of registration data	Information security	<p>A key deliverable of the detailed design phase may be a data dictionary for end-user personal details and notifiable events amongst the stakeholders</p> <p>Generation of a new high-quality data set during pre registration and registration processes may be considered during the implementation planning</p>

#	Description of risk	Category	Example Mitigation Strategies
			The smartcard infrastructure may be classified as Critical National Infrastructure and subject to the protective measures prescribed by the federal Attorney General's Department
			The project organisation should operate a continuing security evaluation and testing program covering systems, infrastructure, and business processes and personnel awareness
18	Security or privacy breaches	Information security	<p>The design of the smartcard infrastructure should be highly physically and logically secured</p> <p>Continuous application and infrastructure testing</p> <p>Extensive risk analysis and auditing of processes and technology components</p> <p>Application security certifications</p>
			Define security requirements for the registration and issuance processes during the Design phase
19	Identity theft during pre-registration or issuance	Information security	<p>Define best-practice registration and issuance processes</p> <p>Reusing existing financial services and government registration processes</p>

7.3 Consideration

Risks – or anything that could impact on the ability to achieve the smartcard project objectives on-time and to-budget – are important factors to be considered during smartcard implementations. Based on the level of risk acceptable to the project owner or key stakeholders, the decision on how to mitigate each risk needs to be made. This requires the risks to be identified and processed continuously by addressing the following steps:

- establishing the context of the risks
- undertake a risk assessment, including:
- identification of risks
- analysis of risks
- evaluation of risks
- treating risks; and
- monitor and review

The output will be a risk matrix with quantified risks and action plans on how to mitigate the critical risks. Risk management is therefore not just a reactive, but a proactive process that needs to be managed throughout the entire smartcard implementation project. A robust risk management approach also includes thorough consultation and clear communication.

8 Data management issues

Data management is a collective term for 'what data is there to manage' and 'how to manage it'. Data management can be divided into several different tasks, such as data architecture and modelling, storage, transport or security and is usually formalised in a Data Management Plan (among other documents) that provides data management guidance, procedures and processes on how to handle what kind of data.

For smartcard implementations, data management issues typically apply to:

- the quality of cardholder registration data
- data synchronisation between agency back-office systems
- smartcard data design
- smartcard initialisation facility data delivery, synchronisation and security control
- intelligent reader configuration data design and distribution
- intelligent reader card usage data design transmittal and reporting
- intelligent reader exception and audit log design and transmission to back-end systems
- key management data design and distribution
- intelligent reader or reader host middleware distribution; and
- software and data set version control and release management.

This section expands on the first two issues relating to smartcard projects and discusses the development and usage of a data management plan to mitigate and prevent data management issues from occurring.

8.1 Registration data

A data management issue specific to smartcards arises prior to and during a roll-out phase of the smartcards. The smartcards will be personalised and shipped with data which is typically extracted from agencies' backend systems. This data can be inaccurate, incomplete or missing and may cause delays in smartcard issuance, smartcards being issued to the wrong end-users or smartcards being issued containing inaccurate or incomplete data.

Prior to personalising and issuing smartcards, the agency needs to assess the quality of end-user data and make a decision on how to proceed. Agencies typically have the following options:

- Option 1: the quality of pre-existing end-user data is high and a high level of confidence can be placed on relying on that data in issuing a smartcard

- Option 2: the quality of end-user data is not accurate enough to solely rely on it. This may result in a data cleansing/updating process to be initiated; and
- Option 3: where the registration data is not present or the quality of the data is unreliable, it needs to be re-collected. In this case, the agency may need to perform a complete re-registration of its users/customers prior to proceeding with the smartcard deployment.

The last two options are usually enforced if the data repository has been built for a legacy application and is not considered necessary that the data pool be updated regularly. Alternatively, the CoP may look for consistency of registration data across a range of agencies' registration databases to avoid a complete re-registration of end-users. The privacy implications of this approach must be fully considered.

Gatekeeper has established policies and procedures in relation to the use of known customer approaches to the deployment of digital certificates (see www.gatekeeper.gov.au). Standards Australia has developed a known customer standard, AS 4860 (2007) – Knowledge based identity authentication – Recognising known customers. The standard is available at www.saiglobal.com

8.2 Data synchronisation

Another area the CoP will need to consider with regard to data management for smartcard deployments is the processes around data synchronisation between different involved entities, as the smartcard issuing agency and the relying parties can be different organisational units. This specific issue arises if there is a duplication of data stored in various agency databases and additionally on the smartcard.

Data synchronisation processes need to ensure the cardholder backend data is consistent with the data stored in and on the card and within all systems and repositories that access or store this user data. For example, a cardholder's postal address will be stored at each agency individually as they are using their proprietary backend systems and not a common address repository. An address change which is communicated by the smartcard holder to an agency may need to be distributed to all involved agencies to circumvent data inconsistency resulting in mail which will be sent to an incorrect postal address.

Another element to consider is which unique identifier will be used to identify the end-user, especially when the smartcard can be used across different agencies. The privacy implications of this approach must be fully considered.

8.3 Data management plan

A smartcard project faces various data management issues, especially when several different entities are involved – or will be involved in the future. It is therefore important to have an understanding of the data that will be used in the project and how the entities are supposed to work and process it in order to circumvent data inconsistency or issues like those mentioned in the sections above.

A data management plan helps to prevent these issues as it describes project-specific data and elaborates on how to process and work with this data. This includes a detailed description of processes, procedures, rules and responsibilities. It is essential to note that documentation, source code and metadata also need to be considered as project-specific data and be included in the data management plan.

The following general topics give a non-conclusive overview of the topics that need to be considered in a data management plan:

- Data ownership
- Roles and responsibilities
- Data access / security
- Data accuracy / quality and authenticity
- Data maintenance processes, including data distribution / update across multiple entities
- Data standardisation / data format conversion
- Data storage; and
- Privacy.

An accurate data management plan which is followed and maintained to reflect project changes and updates is a necessary tool to prevent data inconsistency and will result in cost and time savings over the course of the smartcard project.

9 User registration issues

This section outlines the issues associated with the critical activities that encompass the overall user registration process. The registration process is the establishment of a user's credentials before smartcard issuance. Registration may involve the requirement for the presentation of Evidence of Identity (EOI) documentation and the issuing of one or more smartcards.

Agencies should also ensure that adequate notice is given to individuals about how their personal information may be handled.

Multiple enrolments may occur after a user has been registered. Enrolment is the act of setting up permissions that enable a known user to gain knowledge of or to alter information or material on systems (e.g. a known user will be enrolled into the email, HR and financial systems). Enrolments into multiple systems may occur after a user has been registered.

Although 'Registration' and 'Enrolment' are sometimes used as synonyms, a distinction is being drawn here between the two terms. The remainder of this section focuses on Registration only.

The registration processes may include:

- Initial registration and verification
- Card personalisation; and
- Card lifecycle management

The following sections describe some specific issues relating to these activities.

9.1 Initial registration and verification

The registration process consists of a number of steps which must be completed successfully before card personalisation and card lifecycle management activities can occur. The initial registration of a user is typically the first step. Initial registration issues to be considered as part of this initial step include:

- EOI documentation - issues regarding provision of the required EOI documentation; and
- Authorisation verification – issues regarding verification of whether the user is authorised to register for a smartcard.

9.1.1 Supporting Evidence of Identity documentation

The need for supporting EOI is determined by CoP policies relating to cardholder identification. Evidence (e.g. in the form of documents) is used to substantiate the identity of the user.²⁴

²⁴ This is defined by the Proof of Identity Framework which is part of the National identity Security Strategy (www.ag.gov.au) and the Gold Standard Enrolment Framework which also provides guidance on EOI registration requirements for issuance of high integrity credentials.

he following issues may need to be considered:

- various government agencies and commercial businesses have widely varying risk tolerance in regard to cardholder identity, generally related to the value of the asset at risk, but are sometimes governed by factors such as public perception. The EOI policy may consider the trade-off between inconvenience and problems associated with fraud
- end-users may not be able to provide the required EOI information. In case the agency may still be required to issue a smartcard to these users, the agency can keep a record that the user was not able to provide the required EOI information. This record may reside in the registration system, but may also be included in the chip. This would allow the end-user to access the services associated with the card, and the agency to implement compensating controls to this user group
- EOI may not be required at all, such as in transport and ticketing scenarios. In such scenarios, it is often sufficient to verify certain attributes of the applicant, such as whether the applicant has made a payment, has attained a certain age or is entitled to a concession
- another person might be authorised or nominated to register new users (e.g. in case of nominated professional carers)
- where users are geographically dispersed or reside in remote areas, physical presence during registration may not always be feasible
- depending on policies, physical presence during registration may not always be required and may be done via mail, email, telephone or website
- determination of whether the registration officer is authorised to ask for certain EOI documentation
- determination of whether the registration officer is authorised to validate the status of EOI documentation provided at the issuing agency entity
- whether the registration officer can store the EOI documentation provided
- whether it is permitted by policy or legislation to store initial registration information in the chip, on the card face or in registration systems; and
- duties conducted by registration officers may be segregated.

9.1.2 Authorisation verification

Different card schemes will have different criteria for associating underlying processes or services with particular individuals. Authorisation to obtain a smartcard can depend on a large number of qualifying factors such as whether the end-user:

- is an employee, contractor or holds a certain position
- is an Australian/state/local citizen
- is a concession holder
- is a member of a certain group or club

- meets the age, or other scheme requirements; and
- has made the required payment.

Some issues for consideration may be:

- what authorisation information is required
- whether it is allowed to require certain authorisation information.
- quality of data acquisition
- validation of the authorisation before registration takes place
- management of authorisation criteria and procedures
- EOI of the person who is authorised to approve registration requests
- whether evidence of authorisation information can be stored by the registration officer
- whether it is allowed to store authorisation information in the chip, on the card face or in registration systems; and
- segregation of duties regarding registration officers.

9.2 Card personalisation

As with all aspects of smartcard system development, the personalisation requirements should be clearly defined before the design of the registration process.

The card personalisation process may vary widely depending on:

- the amount of data to be printed or written to the card, i.e. visual (photo, logo) data, magnetic stripe data, EEPROM data; and
- the degree of decentralisation of personalisation activities.

The following issues may need to be considered:

- depending on the policy, personalisation may not be required at all or may occur at a centralised location or decentralised location. Centralised personalisation may be made more secure and may be more efficient as less personalisation equipment is required. However, decentralised personalisation is typically more flexible and convenient for end-users
- personalisation may effectively only be an initial registration process. In these cases, there may be no intention to associate the card with specific cardholder attributes such as name, birth date or photograph). For such schemes, it is feasible to design business processes that allow registration to occur in both card-present and card-not-present environments. For the latter, additional

safeguards may be required to prevent unauthorised persons registering cards belonging to other parties

- establishing and securing supply chains between chip suppliers, card assemblers and printers and electronic initialisation facilities
- how card stock, including wastage, is to be controlled
- establishing or contracting a secure initialisation environment and maintaining assurance controls
- establishing and managing issuer card serial number ranges, including making key decisions on whether to comply with a standard such as ISO 7812
- managing card manufacturer serial number ranges separately from the issuer serial number and establishing the binding of the two
- determining the role of the operating system in the issuance process and whether this involves key management dependencies on outside parties
- determining which applications are issued at the time of card issue, and the approach to adding new applications at a later time²⁵; and
- collection of personalisation data may be a major task. Factors that need to be considered include:
 - geographic convenience of location to the end-user
 - consideration of disabilities, social customs and religious beliefs
 - the need to provide a trusted environment in which the capture process occurs, including consideration of privacy
 - secure capturing, storage and distribution of personalisation data
 - what personalisation data will be printed on the face or reverse of the card, stored in the chip or in registration systems
 - whether an end-user can provide the photos themselves or whether they can be captured at the point of registration. It is typically more cost efficient to have end-users bring their own photos. However, these photos may be of lower quality than when a photo is captured at the point of registration, and might not be a photograph of the person presenting for registration. If photos are captured at the point of registration, a high stability lighting environment may be required, especially where the resulting data is to be rendered as a biometric template for matching purposes
 - the need to design the electronic capturing processes of personalisation data to ensure that accidental or deliberate transposition between cards cannot occur.

²⁵ Decisions will include whether to add initial keys for new application induction which will be, as part of application issuance, replaced by production keys. Issues will include whether cards must be returned or reissued with new applications, or whether the new applications can be initialised at all or some service or transaction points

9.3 Card lifecycle management

Card lifecycle management processes refer to the processes that manage cards after card production and personalisation. Lifecycle management processes include the following:

- Card issuance and activation
- Card suspension / revocation / destruction; and
- Card replacement / renewal

9.3.1 Card issuance and activation

Card issuance and activation is one of the most significant aspects of any card scheme. During issuance and activation, the smartcard is transferred to the end-user and activated. Factors to consider include:

- Application activation - in many cases, it is undesirable for security reasons to have the capability (keys and business logic) to activate new applications at 'remote' readers that are not located in well protected environments, but this must be judged case by case
- EOI verification of the user during issuance – this would only apply if the issuance does not occur at the same time as registration. Refer to 9.1.1 for specific issues
- Distribution of cards and PIN mailers – unused cards should be securely stored and kept separate from PIN mailers at all times. Typically, PIN mailers are sent a few days earlier or later than the card. In some cases it may be appropriate that the cardholder personally collect the smartcard at an issuer or registration point; and
- Card activation - cards may be lost during distribution between various parties involved in the manufacturing, personalisation and issuance. Different schemes will have different policies on whether the card as a whole, or an application on the card, are enabled at time of issuance, determined primarily by risk and convenience considerations. Activation procedures in use today include:
 - none – the card is issued in the armed state (generally in transit where, if the purse has zero value and is not initially linked to an automatic add value service). This method is used when there is no cardholder impact and negligible system impact of individual cards being lost or stolen during distribution
 - card presentation – requiring the cardholder to present the card at a staffed location where proof of identity check is performed before activation²⁶
 - activation code – having the smartcard activated by means of entering a separate activation code entered through a specific activation website.

²⁶ Suitable for both on-line and off-line systems

In online environments, such as enterprise local area networks, card activation processes can be further strengthened by arranging that only certain designated readers are capable of activating a presented card, perhaps during a specified time window (such as the first day of work for a new employee).

9.3.2 Card suspension / revocation / destruction

Card suspension, revocation and destruction are significant aspects within card schemes to prevent invalid cards from being used. The following factors should be considered:

- there will be situations where it is desirable to suspend or deactivate single applications on a card, but not other applications or the card as whole
- interfaces can be provided to allow for easy reporting of lost and stolen cards. Care is required to ensure this interface is not able to be abused. Schemes may require proof of knowledge of some private information furnished and registration time before acting on a suspension or revocation request
- in an on-line system, hotlists (i.e. revocation lists also known as “blacklists”) may be held and actioned centrally
- in an off-line system, hotlists may need to be specially distributed to smartcard readers, either by occasionally connecting to the network or by out-of-band methods, both of which leave the system vulnerable to time windows during which revoked smartcards might still be accepted at various readers
- hotlist distribution frequencies should endeavour to address the risk window, but there may be some cases where the issuer will adopt the risk associated with slower than optimal hotlist distribution
- considerable care is needed in forecasting and managing the size of hotlists. If hotlists are allowed to grow without limit, in offline settings they can exceed the capacity of terminal devices leading to unpredictable system behaviour and likely loss of ability to detect hotlisted cards
- control may be needed over business processes and environments in which previously blocked or suspended cards or applications are re-enabled. Furthermore, a suspension log may be kept to provide evidence that a certain card was actually suspended during a certain amount of time
- in cases where revocation or suspension information is stored only in the chip itself, it should be noted that certain types of technical failures (e.g. memory or functional malfunctions) may cause revocation or suspension status information in the chip not to be correctly updated. This could severely impair the security and reliability of the system, particularly in off-line systems
- returned cards in some transit schemes are recycled rather than destroyed, however the economics and security of such an arrangement must be considered²⁷

²⁷ Recycling is generally criticised by cards experts, but environmental waste is now an issue that all schemes must take into consideration

- card physical destruction may require the use of special shredders; and
- hotlist distribution may use message authentication codes to prevent network-originated abuses, and encryption where privacy issues may be of concern²⁸.

9.3.3 Card replacement / renewal

Card replacement and renewal are significant aspects within card schemes to ensure that smartcards are replaced in time for end-users to continue to use their card with minimum disruption. Some important issues to consider here are:

- card life may be set to meet both wear and tear considerations and cardholder administration or other non-technical considerations
- reliable figures on card scheme natural attrition and other mortality statistics are hard to obtain, but reasonable estimates are that a smartcard life of four years can be expected, and an annualised natural failure rate of as high as 2.5% may need to be planned for
- typically average card life can far exceed the expiry date decided by the issuer – in transit, contactless cards with a nominal four year life are still in operation after seven or eight years²⁹
- on the other side, usage patterns by certain users will subject cards to excessive stresses that shorten their operative lives (e.g. usage of cards by school children)
- schemes in which cards are issued free of charge in bulk to a given cardholder sector tend to have a relatively high return rate due to changes of address
- card replacement processes should match levels of control agreed for initial card issuance to ensure the accurate and secure transfer of the electronic and printed information
- particular attention may be paid to possible opportunities for card substitution fraud which has arisen in some e-purse-related schemes
- consideration should be given to only using back-end processes for card replacement (some schemes are able provide on-the spot replacements), but consideration must also be given to providing temporary access to the services until the primary card can be replaced
- in schemes using photographs or biometric identifiers, card replacement may be used as an opportunity to update biometric data; and
- in many schemes, the total cost of smartcard re-issue can be up to an order of magnitude greater than the cost of the basic card³⁰.

²⁸ It is highly desirable to adopt a policy of encrypting hotlists over communications networks

²⁹ Contactless cards typically suffer less from wear and tear, which causes their lifetime to be inherently longer than contact cards

³⁰ One message from this is that it is often far more beneficial for business managers to focus on savings in areas other than ship or assembled card price

10 Card Printing issues

In practice, there are few, if any, universally mandated printed items for a card. Mandatory items should only be those items which are deemed to deliver a specific administrative or security function for a given project. Such features vary greatly between projects. It can be argued that most if not all smartcard surface features may be optional. Perhaps the only feature which has almost universal applicability is a card serial number.

The sections below address the following card printing issues:

- Generic card printing
- Single-sided versus Double-sided
- Front of the card
- Reverse of the card
- Other agency information

10.1 General issues

In principle, printed material on the card (or the method of printing) should not interfere with the operation of the chip on the contact or contactless card (e.g. embossing is problematic for smartcards due to the potential for chip or antenna damage) and it should not prevent data from being accessed. Each element added to the front and/or back of the card should be able to be justified on the basis of the functionality or business process it is enabling.

Key considerations relating to generic card printing issues include:

- complying with international ISO standards when determining the physical card printing characteristics of the smartcard. Refer to the National Smartcard Framework for details of relevant standards for smartcards
- essential information, such as card serial number (CSN) to facilitate the identification of individual cards, is needed for card administration and management. Without such a unique reference number it is difficult to identify failed cards
- inclusion of information which may be required for use in manual processes, often referred to as human readable form, for example, confirmation of the cardholder's identity in situations where readers may not be online or unavailable
- inclusion of information which may be needed to supplement automated processes. For example, when the process requires strong authentication of the cardholder to the card in addition to the card to the system (e.g. comparison of a printed photograph)
- inclusion of information that may assist in fraud reduction in card-not-present situations (for example, a card verification value)

- inclusion of security printing features that allows the automatic or manual detection of counterfeiting attempts. There are many of these, targeted at differing levels of sophistication in attack. Consideration may be given to their relevance to the CoP before adopting them, as some card schemes achieve high levels of security without resorting to sophisticated security features on the card face. The National Identity Security Strategy include guidance on security features on cards
- exclusion of information which may constitute an unnecessary infringement of privacy or would facilitate identity theft
- exclusion of such features which detract from the sensible use of other visual or mechanical features (for example attempts to provide excessive information on the card surface)
- the possibility that business functions do not include any conventional printing approaches, for example, with the introduction of fob-based smartcard tokens and Near Field Communication (NFC) smartcard replacement technologies where there may be no practical opportunity to apply printed, engraved or other graphical information; and
- certain metallic inks may have an impact on the performance of the embedded antenna in contactless cards.

10.2 Single-sided versus Double-sided

The decision regarding whether and what to print on each side of the card should be driven by business and security requirements. Card graphics planners need to consider many factors including legibility, aesthetics, possible trademark clashes (extending to selection of colour combinations), and the ability of design features to stand up to the expected wear and tear.

10.3 Front of the card

Cards will mostly have a unique number printed on the front of the card in large enough format to be readable by most cardholders in reasonable lighting conditions. The serial number will be used by the cardholder for manual interactions with the system, including identifying the card to call centres, and in checking paperwork associated their 'account'. In banking systems this is called the 'Primary Account Number' or PAN, but it has various other names in other systems including simply the card number. In practice, this number may identify both the back-end master record relating to the card, and the physical card itself. The PAN or card number may be electronically encoded in the card, but there may be security advantages in using an unrelated numbering scheme for this purpose, for example, for practical design reasons, the electronic serial number may be reserved for establishing the cryptographic identity of the card separate from the card number.

Furthermore, there may be privacy risks associated with printing a unique number on the face of the cards. Especially in scenarios where the card is used many times by various agencies and other relying parties, the card number may become a de-facto identity number for the cardholder.

Where appropriate, the front of the card (FOC) may carry such features as:

- Photograph of individual – where photos are used a number of issues should be considered:
 - Actual need – a photo should only be placed on the card face where it is to be a primary means of cardholder identification independent of the chip, or where there is a serious cost or functionality impact of recording the photo on chip and accessing an image at the time of cardholder verification is required. Access control programs such as employee cards and drivers licences are the main environments in which the photographs serve a necessary supplementary purpose to the information stored on the chip
 - Printing durability – if the card will be primarily be used for visual authentication, high endurance printing methods may be considered. This may include the use of dye sublimation techniques, special laminations, or providing a transparent wallet to protect the card surface
 - Image placement – the graphics design of the cards should provide a suitable photo size and placement. To avoid on-costs, it is suggested that where card stock is manufactured with a base colour scheme, an unprinted white window is reserved for the photograph
- Cardholder name – like the photo, a name may only be considered for printing on a card if it serves a definitive purpose and meets privacy and security requirements of the given agency. Transit systems are very good examples of schemes which can operate securely and effectively without any personal identifiers on the card surface, or even without any electronic personalisation at all³¹.
- Expiry date – expiry dates on cards have come to serve two purposes: to provide an end of card life reminder to the cardholder and as a supplementary identifier in cardholder verification during card-not-present transactions. Other values including the Card Security Code (CSC), sometimes called Card Verification Value (CVV) or Card Verification Code (CDC) can serve equally well in the latter role; and
- Card number – where there is a printed card number, it is highly desirable that the number include a Luhn check digit³² or equivalent to allow easy detection of data entry errors prior to submitting the numbers to automated processes. The check digit should be included in any printed or displayed representation of the serial number.

The reason for including this information on the front of the card is for ease of handling (card handling agents only need to inspect one side of the card).

10.4 Reverse of the card

The reverse side of card normally carries supplementary features such as signature panels, magnetic stripes, card verification values and often, a help desk contact number. Note that each additional feature imposes an additional cost on card production and may incrementally reduce the card's useful life. The general rule is to print as little as is possible in order to meet specific functional and security objectives. The features on the reverse of the card may include:

³¹ Anonymous smartcards have proven an ideal and reliable replacement for anonymous magnetic and paper tickets

³² As used by bank and credit cards

- Magnetic stripe – card designers may wish to consider new security developments in conventional plastic card technology, such as un-duplicable magnetic stripe technology. Smartcard scheme designers may only consider incorporating a magnetic stripe if compatibility with an installed magnetic stripe terminal base is needed or when smartcard readers are not yet available or not operative. Such a situation might arise for instance if there is a need to provide an ATM or EFTPOS terminal-based function in connection with the card. It should be noted that reliance on magnetic stripe technology may significantly reduce the useable life of the card due to demagnetisation or wear. The economic impact of card replacement due to magnetic stripe failure in a smartcard scheme will be far greater than for straight plastic cards due to the chip and initialisation costs. Additionally, alternatives or backup strategies such as embossing or manual re-keying of information and validations against back office systems need to be considered when smartcard and magnetic stripe readers are not available
- Card Number – the card number may be printed on the front or back of the card of both
- Card Security Code – card scheme planners also need to factor-in the threat posed from attackers skimming information from the card faces. Safeguards may include placing two features which together are used for card or cardholder verification on opposite sides of the card, as well as ensuring that business processes minimise the ability to easily make copies of the critical elements (e.g. both card number and CSC on credit cards required for payment). The CSC, which is present only on the rear surface of the card and in back-end databases is highly desirable for assisting with card verification in card-not-present situations. Such digits, if present, should be printed in a small font to mitigate the risk of collection through visual surveillance.

10.5 Other information

Each CoP will have its own business, functional and security requirements that will need to be addressed when considering the information that will be included on the smartcard. In general, CoPs should avoid printing too much information on the surface of the card. This can potentially lead to problems with cards becoming prematurely out-of-date if non-critical facts about the cardholder change (such as phone number, or trivial aspects of their staff position). Further, the more personal data is contained on a card, the greater the potential vulnerability should the card fall into the wrong hands. Further information is included in Section 4.5.

Wherever possible, agencies should consider storing data to the chip rather than using the card surfaces. Not only can the chip be more readily updated than can the surface printing, but certain private information is more effectively managed in memory where access can be better protected by PIN, reader-to-card authentication and so on.

11 Infrastructure issues

Smartcards can play a vital role in securing confidential data. Therefore, the underlying infrastructure of a smartcard implementation should be subject to various requirements. The sections below provide an overview of the following relevant smartcard infrastructure related issues:

- Smartcard type
- Smartcard chip
- Smartcard applications
- File system
- Card operating system
- Smartcard readers
- Reader middleware
- Smartcard network
- Back office systems
- Cards processes
- Third parties
- Card systems governance

As part of the infrastructure implementation, agencies should ensure the appropriate system security policies and procedures are developed. For example, the ISM states that Australian Government agencies should ensure every system is covered by a Risk Management Plan (RMP), a System Security Plan (SSP) and Standard Operating Procedures (SOPs). DSD recommends that an over-arching document describing the agency's documentation framework be created and maintained. The RMPs, SSPs and SOPs should be logically connected and consistent for each system. The documents described here are only a subset of the recommended documentation suite. For comprehensive guidance on security documentation refer to the ISM.

Other jurisdictions should comply with their own security standards.

11.1 Smartcard type

Multiple fundamental smartcard 'type' choices face card scheme designers. Selection must be made between the following:

- Functionality:
 - true microprocessor cards and advanced memory cards³³
 - cards which can sustain varying degrees of memory wear (for example those using EEPROM and flash technology versus those (few cards) using Ferroelectric random-access memories (FERAM))
 - cards intended to be disposable or for limited use and those intended for long-term use
 - cards with a fixed behavioural or application repertoire versus cards with programmable behaviour
- Physical features and dimensions:
 - cards using different chip - carrier materials, for example, plastic versus paper
 - cards which match the ISO 7816 physical format and those that have non-standard physical formats
- Interface and readers
 - contact card interface types - standard contact versus USB (now adopted under ISO 7816 contactless)
 - contactless interface types (Type A versus Type B)
- Cryptography
 - cards which have varying levels of security evaluation and tamper resistance
 - cards supporting differing forms of symmetric and asymmetric cryptography

Even within specific industry segments, there is wide variation on the approach to card selection or configuration. Primary decision drivers tend to be price, security and being able to meet immediate project requirements for capacity and performance, with factors like the addition of future applications and interoperability taking secondary importance.

³³ Simple memory cards generally do not come under the rubric of 'smartcards'

11.2 Smartcard IC chip

The smartcard chip will, in most cases, comprise a monolithic silicon implementation combining the elements of microprocessor, memory, cryptographic co-processor and interface circuits (contactless and contact). In the case of contactless cards, a radio frequency interface is integrated with the chip, consisting of both digital and analogue circuits. The chip is mounted in a module which provides mechanical and (ultra violet) light protection to the chip and connections to the smartcard contacts or antenna.

Additional chip features will include power supply regulation, clock generation, a random number generator, and various probing and side-channel attack hardware countermeasures.

The chip memory tends to occupy the largest area on the chip, followed by the CPU and other circuits. As a rule of thumb, the cost of the raw chip will be linearly proportional to the amount of silicon used in its implementation.

Note also that from a mechanical reliability perspective, chips with larger memory will be more susceptible to mechanical stress than smaller memory chips.

There are many different chip implementations on the market, but the primary issues for smartcard implementers involve:

- Interface type
- Memory size
- Performance/speed
- Security features including cryptographic functionality
- Price

Price is also volume-sensitive. Small volumes used in small projects or trials (up to tens of thousands of parts) will normally be significantly more expensive than large scale procurement (hundreds of thousands or parts and above).

11.3 Smartcard applications

The term “smartcard application” has assumed several broadly related interpretations. These are:

- most narrowly, a set of related data files on the card; or
- more generally, a set of data files and application specific functions or computations on the card
- widest of all, the combination of on-card data and executables on the card and all associated front and back-end business processes.

From a smartcard system design perspective, the third definition is the most appropriate in conveying the extent of the technical infrastructure. For the purposes of a chip-level discussion, the first two are the most relevant.

Smartcard applications based on ISO 7816-4 file system or ISO 24727 are implemented with a hierarchical structure. The card issuer application is at the apex and serves as the gateway to all other applications on the card. Each application will typically be isolated from other applications and occupy a peer position in that hierarchy. In almost all cases, only one application may be selected or executed at any one time and special non-standard functions will be needed if applications are required to intercommunicate³⁴.

Card applications based on passive data sets as described above can satisfy many requirements, but do not address the issue of unique executable functions or functions loadable on the fly. In the first case, a 'standard' design is supplemented by inclusion of special algorithms to address specific business needs. These are typically included on the card for security reasons, for example, the calculation of a digital signature or the execution of a unique mutual authentication protocol.

In the second case, best demonstrated by the JavaCard, atomic applets³⁵ may be loaded on the fly and executed in the generic card architecture, typically using some stored data elements on the card. Such applications carry a signature which must be verified before the application is allowed to execute.

The benefit of this approach is that it provides the best model for application issuance after the card itself has been issued and does not require any special additional load procedures at the card issuance layer. The demerits of this approach include the need for larger static RAM on the chip (occupying larger real-estate than flash or EEPROM memory), the communication time taken to load the applet (one of the greatest impacts on performance is data serialisation delay at the interface) and in the case of JavaCards, the need for a code interpreter which adds to the silicon size if in hardware or reduces performance if in software.

Card application designers should take care to assess the virtues and impacts of each approach before deciding on their approach.

11.4 File system

Smartcard file systems generally but not always conform to the ISO 7816-4 hierarchy and types, for example, Master File (MF – the root file of a card), Dedicated Files (DF) – effectively root files for applications and Elementary Files (EF) where actual user data is stored.

Several fundamental types of EF are specified including linear and cyclic files. Note however that ISO 7816-4 does not include a file type called "counter", leaving it to the individual application implementer to determine how to implement such a feature. This is particularly evident in e-purse schemes based on increments and decrements of purse files.

³⁴ Note that most transit smartcard systems implemented to date use a fully or partly proprietary application design, either on a bespoke basis as defined by the card issuer, or based on a common design from a major chip vendor targeting this industry segment

³⁵ Atomic applets contain operations that are executed either entirely or not at all. In smartcards, atomic applets are frequently used in connection with EEPROM 'write' routines, in order to ensure that the data content is consistent at all times

Perhaps the most complicated issue facing card application designers is that of key management. Application keys are typically assigned to an elementary file from which they may be accessed according to the file access type being dictated. However there are no firm standards yet in place to describe a normalised key management approach. Implementers must either accept what vendors offer or embark on a bespoke development.

11.5 Card operating system

There are a plethora of operating systems available for smartcards including a small number of multi-application operating systems which have achieved significant market recognition (JavaCard and Multos). The Global Platform specification is compatible with both Multos and JavaCard, but there are more formal card issuances prescriptions in the latter.

The primary advantages of adopting a recognised card operating system are that:

- it should come with a formal security evaluation
- it will have been designed to address a range of applications and should contain a rich feature set; and
- implementations will have been well tested.

Disadvantages may include the need to pay per-card royalties and the possibility that there may be a permanent cryptographic linkage back to the operating system vendor for card or application issuance.

It is important for implementers to note that almost any card operating system can offer multi-application services, including on the contactless DESFire platform which has been widely adopted in transit and North American access control programs. What differentiates the different types tends to come down to:

- whether the operating system supports PKI
- whether a 'load on the fly' application architecture is required; and
- how wide a choice of suppliers is desired.

Again, it is crucial for system designers to fully evaluate their requirements before making a choice and it is also important to examine whether the certifications available with the card actually cover all proposed uses for the specific applications of the given implementer.

It is also crucial for developers to recognise that Common Criteria certification for the operating system does not imply that applications loaded by that operating system themselves by implication meet any security evaluation level. Each implementation should be assessed in the context of the operating system over which it resides.

11.6 Smartcard readers

Smartcard reader selection or designs present many issues to be resolved in a smartcard system implementation. Key points include:

- implementers should first establish a clear requirements specification for reader business and security functionality
- from a security and system functionality perspective, readers may be passed through (simply providing the electro-mechanical interface for a remote host to access the card) or more intimately involved in card authentication and the ensuing system or card accesses. Simple pass-through readers are available and reasonably low cost, both for contact and contactless cards, although they will require integrated client card support for conventional authentication regimes (e.g. Active Directory and e-Directory)
- readers which are off-line require greater security and data storage metrics than those directly connected; and
- in the smartcard standardisation arena, there are as yet no completed standards defining universal architectures in relation to card readers. There are however, some good specific examples from the payments industry in the form of the EMV terminal specification and from the Australian electronic funds transfer marketplace in which terminals must generally comply with both the AS-2805 standards and the security requirements of the Australian Payments Clearing Association. Requirements for payment card processing terminals are also issued under the Visa PIN Entry Device (PED) program (now coming under the joint MasterCard and Visa of the Payments Card Industry (PCI) requirements). For implementers seeking a good selection of guidelines on implementing readers with cryptographic and key management functions, these standards or quasi-standards may be a starting point as they cover such issues as:
 - initialisation requirements
 - tamper resistance and responsiveness and other hardware assurance requirements
 - logical safeguards, including those relating to different terminal subsystems
 - key management general requirements.

These standards, however, are in evolution and reflect commercial as well as technical compromises that may not be acceptable in deployments needing to be highly secure.

These models may be contrasted with those implementations in some industry segments where the securing cryptographic keys for card access has been well treated, but the securing of the surrounding business logic has not. Even where readers embody a SAM, it may be infeasible to implement all of the sensitive application logic in that component for performance, memory resource or other reasons.

CoPs need to look closely at the question of how the card authentication logic couples with subsequent security activities and the business being conducted at the front end. Matters to be considered include:

- whether, in addition to cryptographic authentication, the terminal requires PIN entry and a display, and if so, the level of security attaching to the terminal keyboard
- in the case where a central system authenticates a card shared by multiple agencies, how the agency processes can be bound to the electronic confirmation of authentication issued by the central system (this may mean the agency must share cryptographic keys with the central system) and that part of the authentication process will involve the exchange of application access keys subsequent to mutual authentication
- choices also need to be made on reader acquirer (network) side interfaces. Reader technology is rapidly moving towards IP connectivity and this may be over almost any combination of fixed and mobile network backbones. For additional security (or at least the perception of it), some smartcard system implementers may still adhere to the use of private networks, but as these often traverse the infrastructure of a telecommunications carrier, and as carriers move ever more to link aggregation, there is little guarantee that traffic in private networks is physically isolated from other traffic
- where the reader provides security access functions to the smartcard it should have equivalent Common Criteria certification to those required for the smartcards
- on the network management side, considerable attention must be given to the lifecycle management of readers. Where they carry out security functions, readers should be managed analogously to the cards, with a secure issuance and distribution process, and suitable measures when readers are being serviced or decommissioned
- it is highly likely that some readers will play a key role in enforcing business rules in a card application. Special security features may be needed in the reader, including automatic self-disabling on network detachment, mutual authentication to local workstations, enforcement of transaction quotas, handling agent log-ons, and managing card hotlists
- where it is desired to integrate the agency functions with EFT functions, then the agency application may need to be evaluated for compliance with EFT security specifications as described in AS2805 – Electronic funds transfer before network connection is allowed
- where contactless readers are to be used in a portable environment, good power management will be essential to achieving reasonable service duration for the scheduled hours of operation. This also applies to portable reader battery charging cycles. To achieve acceptable use and service from portable contactless readers, a power management strategy may need to be developed to ensure devices are at full operating capacity and availability; and
- careful selection or design will be needed for readers in harsh environments (outdoors, marine etc). It is easier to achieve good moisture and dust exclusion ratings for contactless readers than for contact readers, and this may be an important consideration for emergency services.

11.7 Reader middleware

In the context of this implementation guide, the term 'middleware' should be taken to refer to the underlying applications which support smartcard acquisition, mutual authentication (if any) and subsequent card accesses and related agency business logic.

As mentioned earlier, such reader applications should be subject to the same risk analysis and evaluation criteria as apply to the card applications with which it interfaces.

Additional factors to be considered will include:

- how each middleware application is to be issued on the reader
- how the middleware interacts with the reader security module (if any)
- how each middleware application is to be key managed
- the storage and communications metrics associated with such factors as:
 - applications and configuration data downloaded to the reader including hotlists
 - persistence length for data downloaded to the reader
 - the usage data acquired as part of the card access or transaction
- the need to retain logs until such time as they are transferred to some other repository or are otherwise no longer needed; and
- the likely impacts on security or system integrity of a reader failure including possible data loss thereon.

11.8 Smartcard network

Smartcard networks vary greatly between applications. Examples include:

- building access control where card readers may be on-line to some form of central access control manager, but fully off-line to the card issuer
- transit and general stored value purse systems where most transactions are conducted off line to the central system, with transaction data being delivered in batch mode to the back-end
- computer logical access controls where the card may interact with either a centralised or a distributed access control management system
- bank cards where transaction authorisations are furnished real time either by the issuer or by an acquirer standing in for the issuer; and
- entitlement cards where the card is mainly used to identify the cardholder before non-card-related transactions take place.

Communications network paths which must be addressed by a smartcard system network plan include:

- reader to acquirer, possibly via an intermediate tier, and using wired or wireless interconnects
- acquirer to issuer
- issuer to card issuance centre
- issuer to central system
- central system to cardholder (e.g. web access)
- central system to operations, and including cardholder support services
- issuer or central system (e.g. configuration and reporting)
- issuer to card supplier for the communication of card transport keys
- issuer to reader supplier for the communication of reader transport keys
- issuer to third parties (e.g. where there may be settlement or authorisation transfers with financial institution or suppliers of identity-establishing information)
- central system to service providers or agencies to facilitate, reconcile or report relevant transaction or event data
- central system to backup facilities
- central system to archive facilities
- in some cases, software maintenance staff to the central system; and
- the card issuer's own internal corporate communications network which should be fully isolated from the card-facing network.

Issues to be addressed when designing card systems networks include:

- the need for configuration data needing to be communicated to the readers, including hotlists if any
- the timeliness and sequencing of information transfers to avoid replay or versioning attacks
- the volume of configuration data that needs to be transferred to the reader and frequency of the transfers
- authentication and encryption processes associated with configuration data delivery
- real-time authentication traffic between the reader and the acquirer system, or possibly the next intermediate tier

- usage data transfers between reader and acquirer system, including whether this needs to be real-time or batch
- audit register or log data transfers between reader and acquirer system, including whether this needs to be real-time or batch
- authentication and encryption processes associated with usage data, audit registers and logs
- administrative data transfers between the system and the reader including for general terminal management (for example, taking units off-line and on-line), as well as exception reporting traffic
- network monitoring service to determine reader disconnection or relocation
- reader initialisation or installation traffic
- traffic related to the agency business including operator log-ons, end of business day functions, alerts, and, potentially, client application or driver updates
- key management traffic between the key management system and individual or groups of readers
- where and how interfaces can be built to suit existing agency communications infrastructure to carry card program data (alleviating the need to build a completely separate network)
- whether the data design is standards based or proprietary, and the impact each may have on system performance or network bandwidth requirements
- a full impact analysis on the resourcing requirements to meet peak or 'busy hour' loadings
- a full analysis of availability requirements including the need for load sharing and alternate routing of traffic
- consideration of data recovery paths in the event of network failure; and
- consideration of security elements that apply end-to-end and link-by-link.

11.9 Back office system

The precise approach to back office system design will depend on the type of application to be supported. Components of the back office may include some or all of the following infrastructure and functions:

- Card issuing – this function will include card stock procurement, initialisation, personalisation, and distribution. Parts of this function may be subcontracted to specialist suppliers and subject to acceptable risk levels
- Card and cardholder registration and personalisation – different schemes will have different registration and personalisation requirements, depending on the importance of identity

establishment. In some cases, on-line registration may suffice (as practiced in some transit schemes) while stronger procedures, including possible capture of biometric data will apply in other circumstances. Important considerations will include environmental requirements, process design and security for data capture, data entry, paper forms management, forms imaging and archiving and special measures to protect against identity theft. Privacy concerns will need to be addressed wherever personal data is handled or stored

- Central databases – most card schemes operate on the concept of a card master record in a central database. This record will contain baseline data about the card, along with usage data where relevant. While some schemes store personalisation data in the same record, others, in order to protect against data aggregation exposures or to provide operational advantages, maintain a separate ledger for personal data and only permit linkage to the card in controlled circumstances. In any case, it is highly desirable practice that card records be held in encrypted form on the storage media to mitigate the risk of unauthorised access or accidental exposure
- Reader issuing – if card readers have no security functions, then no special provisions need to be put in place for reader management, beyond normal hardware management. However for situations where the terminals are cryptographic participants in card access or in post-authentication business processes, the readers must be treated as a security domain with lifecycle security concerns starting with manufacture and progressing through initialisation, distribution and activation, use and finally decommissioning. A component of this may involve tracking the physical location or network addressed location of the device
- Reader configuration data management and distribution – where readers play a significant business rules enforcement role, then configuration data management must be properly provisioned and suitable security measures adopted to protect the configuration data flows. In systems where readers have an on-line connection to the back office, bilaterally authenticated sessions based ad-hoc configuration data management is mostly employed. However for systems in which the reader population is off-line, a store and forward methodology must be used. The latter requires special security measures to protect against replay or versioning attacks, as well as a feedback mechanism which provides the back office with a snapshot of the reader state at appropriate intervals. A useful precaution is the provision of a timeout mechanism where a secure reader disables itself after a preset period of time has elapsed without receipt of a valid next-in-sequence communication from the central system
- Card acquiring – the extent of back office interaction with the card and reader depends on system design. In some cases the central system may provide a direct mutual authentication function, or a similar service through a distributed authentication model with intermediate network points providing proxy authentication services. In other schemes, the card acquiring function may include establishment of a session with the reader and exchange of card or cardholder authentication and transaction authorisation requests and system authorisation responses (this equates to the bank card acquiring model). In other schemes, readers may accumulate records of prior authenticated off-line transactions before submitting them to the acquirer subsystem. The acquiring function may also include terminal management and merchant or agent functions
- Card transaction accounting subsystems – on the card or application issuer side of the acquiring network there will generally be some form of reader and card transaction clearing or processing function. This may connect to the card or cardholder database master record and/or to reporting

and, in the case go financial transaction, a settlement function or subsystem. Features of the clearing function (perhaps shared with an acquirer function) may include:

- separation and forwarding of transaction streams or messages between different application issuers or operational functions (for example reader management responses)
 - verification of message authentication codes and marking of data objects as fit for further processing
 - message sanity checks
 - verification of card reader or merchant terminal identities
 - removal of duplicate transactions
 - detection of missing transactions
 - confirmation of reader key management status
 - reporting on verification failures or other exceptions
 - creation of backup copies of transactions.
- Settlement functions – as implemented by transit or purse operators and for more traditional banking is a large and complex topic in its own right and hence is not elaborated here other than to indicate that there are many accounting, reconciliation, audit, authorisation and governance processes involved
 - Key and certificate management functions – almost without exception, significant smartcard deployments involve both centralised and distributed key management functions. Core elements in these may include:
 - a central key and/or certificate management application or facility which is the source or repository of system master keys. Key management hosts come in many forms but in government and banking systems will almost certainly be based on some form of Hardware Security Module (HSM) for the protection of keys and other secrets
 - a set of cryptographic relationships forming the basis of a series trusted communications paths between the key management function and suppliers or recipients of key material and other secrets
 - in some smartcard systems, intermediate key storage or handling nodes, these also being protected by an HSM
 - in smartcard systems with secure reader functionality, key storage and use at the reader within a security module environment

- in almost all smartcard systems, the card itself as a container and user of keys in the case of PKI, various interfaces for the creation and distribution of key certificates and revocation lists
- Key management system – the detailed design of the key management system will hinge on many factors including:
 - whether symmetric, asymmetric or hybrid keys are in use at various points in the smartcard network
 - whether the system is providing on-line authentication functions
 - whether each front-office endpoint (reader or terminal) can be uniquely addressed for key management purposes, or whether group addressing is required
 - the nature of any key management gateway functions being provided for third-party application issuers
 - the location and type of card issuance, personalisation and enablement functions
 - the volume of keys needing to be handled
 - whether a unique key per association or a derived key per association approach is required
 - the timing and methods for key-rollover within cards, and readers
 - whether there is a layered security architecture and whether security associations are end-point to end-point or link by link
 - whether there is a formal acquirer layer where another party or function acts as proxy for card and application issuers
 - the extent to which the core key management system must support a range of key management functions in COTS software and hardware elements in the system in addition to card or reader-specific functions. This may include:
 - VPN keys or SSL keys used to protect public web sites and intranet functions
 - public keys used for the exchange of sensitive data between system participants
 - LAN keys (where for example, wireless networks are used to acquire card data from portable or mobile readers)
 - data from portable or mobile readers.
- Issuer and agency reporting interfaces – in most smartcard schemes there is at least a basic reporting function established between the card issuer and application issuers or participating agencies. This may cover many factors, including card or application issuance volume, transaction volumes and types, exception volumes and type, reconciliation and settlement summaries,

and KPI statistics. Often this data is of a highly sensitive nature and security processes must be designed for its transmission.

- Access control management – fully featured smartcards systems will have a complex array of access controls, and adequate resourcing and tools must be provided for its administration. Areas to be covered include:
 - issuer facilities access
 - issuers systems computer and network log-ons
 - card issuance and personalisation platform log-ons
 - agency reader operator log-ons
 - key management system access control provisions
 - reporting systems access control
 - database and computer maintenance log-ons
 - various application layer log-ons including for authorisation of specific actions

Each domain of access will have an associated log which may require continuous automated analysis and periodic manual audit.

- System deployment and integration test management and execution – primary issues for smartcard deployers to consider during deployment and integration testing include:
 - interfacing to legacy equipment
 - keeping a separation between test and production systems, including, cards, readers and cryptographic keys
 - sequencing with agency and cardholder education
 - ensuring adequate agency liaison
 - constraining field trials to a practical and manageable scope
 - maintaining rigorous version control on software and hardware releases
 - avoidance of back-door work-arounds
 - ensuring adequate unit testing before field release
 - maintaining adequate asset management registers

- System maintenance management – large smartcard systems entail significant levels of ongoing support for infrastructure including readers. Issues to be addressed include:
 - contracting maintenance services to suitable parties
 - maintainer access to system elements
 - removing or disabling security functions before equipment is removed from its normal location
 - adding or enabling security functions when equipment is commissioned or returned to its normal location after repair
 - ensuring that test sites and test beds have no access to production data
- Cardholder management including help desk – smartcard back-end system design must make adequate provision for handling post-issuance card management issues:
 - cardholder general inquiries about aspects of card usages
 - changes of registration data, concession status or usage status
 - lost, stolen and failed card reports (see later)

Demands on such systems will be greatest immediately after cards are issued, and especially high when a system is first commissioned.

- Cardholder web sites – most large card systems where cardholders are members of the general public implement some form of web interface to support various cardholder services drawn from:
 - on-line card registration
 - change of registration details
 - transaction usage record inquiries
 - balance inquiries
 - issuance requests for additional applications
 - post-distribution card enablement
 - initiating ad-hoc operations on the card (for example, transit purse load)
 - new card ordering
 - requesting mailed printed card usage statements
 - submission of complaints or questions

- viewing the scheme policy on various issues including privacy
- learning about other points of service delivery
- finding links to various scheme participants

In some cases, web site maintenance will be subcontracted out to third party specialist web-hosting providers.

Many factors need to be considered in relation to the web site including:

- content development
- establishing secure paths between the issuer and the web hosting site for real and non-real time content update and collection of cardholder data input via web pages
- protection of the site against denial of services attacks
- user authentication
- protection against scripting attacks aimed at cardholder passwords and/or other sensitive personal information
- management of the web server public key as used to establish a secure sessions with client browsers

Particular attention must be paid to any web function which requires read or write access to the card or cardholder master records

- Agency management including help desk – smartcard back-end system design must also make adequate provision for handling inquiries from agencies or reader operators including:
 - agency general inquiries about aspects of reader and card usage
 - changes in reader location or configuration profiles
 - lost, stolen and failed reader reports

Similar to card issuance, demands on agent or agency support systems will be greatest when a system is first commissioned, or when substantive operational changes are introduced

- Backup and disaster recovery – smartcard system designers must ensure adequate provision for backup and disaster recovery. Many of these issues are no different to those applying to any mission-critical system. Some of the issues to consider include:
 - sequencing of backups to meet the system data retention requirements
 - protection of the back up data including the use of encryption and integrity measures to prevent tampering and meet privacy and security policy requirements
 - mirroring system data to a disaster recovery location

- determining whether cold, warm or hot standby is required and the time metrics and impacts for switch-over
- protecting links between primary and disaster recovery sites
- appropriate location of disaster recovery sites
- maintaining separated stocks of smartcards to ensure business continuity in the event that one bulk stock location is damaged or destroyed
- recovering data from failed or damaged reader devices
- ensuring smartcard network immunity to single points of failure.

11.10 Card processes

This section covers card processes not covered (or not fully covered) elsewhere:

- Card procurement – card procurement may be an issue of considerable complexity and requires careful technical, legal and commercial management. The technical selection will presumably be established in the issuer’s specification. However other issues to be considered include:
 - establishing manufacturer trust credentials
 - determining second source³⁶ requirements
 - distinguishing between differing manufacturing models including price-reliability trade-offs
 - verifying specification compliance
 - establishing transport keys
 - determining policy in relation to country of card manufacture
 - determining production test requirements
 - setting card reliability thresholds and determining warranties
 - managing warranties on failed cards and determining the risks associated with allowing manufacturers to perform forensic tests on failed cards
 - differentiating warranty failures from abnormal wear and tear (lack of cardholder diligence) or deliberate card damage
 - accommodating currency exchange rate risk (the card silicon market generally trades in either US dollars or Euros)

³⁶ An alternative supplier of an identical or compatible product. A second source manufacturer is one that holds a license to produce a copy of the original product from another manufacturer

- forward planning to allow for potentially long lead times in chip module or card supply
- planning for technology obsolescence or migration
- Stock management – card system designers must develop suitable procedures for bulk card stock management, whether at the issuer premises or at subcontractor premises to ensure secure management of inventory and prevent loss, theft or unauthorised access to that stock. Good stock management procedures include isolating failed cards from good card stock and routine stock takes. Other considerations include the management of temporary cards, if used in the system, and in the case of some schemes, recycling of cards whose technical life far exceeds the period for which it is assigned to a given cardholder³⁷.
- Expired card management – smartcard scheme designers and managers must make proper provision for expired card management. Issues here include:
 - whether expired cards are to be recovered
 - whether expiry is permanent or revocable
 - what warning needs to be provided to the cardholder and what budgeting and provisioning is in place for card replacement
- Lost and stolen card management – in any large card scheme, there will be significant effort needed to deal adequately with lost and stolen cards. Considerations will include:
 - reporting and hotlisting or revocation mechanisms
 - establishing the veracity of claims of lost or stolen cards
 - assignment of commercial liability in respect to card replacement
 - in the case of stored value cards, determining the value transfer policy including whether it is to take place at the front or back-ends (and considering convenience versus risk)
 - implementing safeguards to protect against abuse of the card replacement procedures
 - determining the role, if any, of temporary replacement cards
 - determining appropriate latencies in reader systems for the distribution of hot or revocation lists, and providing for list aging³⁸.

³⁷ Card recycling is deprecated for personalised cards on privacy grounds, but feasible in some schemes (e.g. transit) with high non-personalised card turnover. A full security risk and commercial impact analysis should be undertaken before committing to recycling program

³⁸ If the delay is too long, devices or cards that have been compromised may be permitted into the system. Alternatively if the delay is too short it can impact on operations and bandwidth

- Failed card management – smartcard issuers and scheme managers must plan for reasonable levels of card failures during normal operations. Card failure rate statistics are jealously guarded by chip makers and scheme operators, but issuers should allow for up to several percent of cards issued. Considerations will include
 - differentiating normal wear and tear from deliberate abuse
 - determining fallback policies for when the chip fails to work: In some cases this may entail reversion to use of the data printed on the face of the card, but this may usher in simple attacks for which the chip was to provide a security solution
 - being alert to card failure modes which may compromise card anti-abuse safeguards – for example, in an off-line card authentication environment, cards which cannot be blocked must be permanently hotlisted, or hotlisted until such time as the keys used to access that card are revoked and removed from readers or authentication engines.

11.11 Third parties

Smaller smartcard deployments may provide most functions or services internally. However most larger schemes rely to a certain extent on third party service providers, including:

- card assemblers, printers and electronic initialisers
- mail-houses for card distribution
- call centres for front-line handling of cardholder inquiries
- web hosting providers for the delivery of cardholder web interfaces
- service point agents, providing walk-in cardholder services such as card registration and faulty card replacement
- reader installers, for the installation and commissioning of readers and smartcard network equipment
- maintenance agencies for the repair of readers or other system equipment
- secure archive organisations providing safe storage of system electronic and paper records
- security disposal service providers for the secure destruction of paper records and electronic storage media³⁹
- disaster recovery centre providers offering standby computing and operational facilities; and
- independent test and evaluation laboratories and security auditors providing services to the card system assurance program.

³⁹ It is highly desirable that at least a first level of media destruction be carried out by the issuer even where a secure disposal outfit is contracted

11.12 Card systems governance

Smartcard systems governance principles must embody numerous regulatory and fit-for-purpose principles. Issues to be addressed may include:

- compliance with corporate, financial and taxation law
- compliance with privacy and consumer laws
- prevention of conflicts of interest
- establishing a clear set of business objectives and performance measurement metrics
- implementing appropriate and on-going risk management procedures
- establishing a standards-compliant Information Security Management System
- promulgating suitable security and privacy educational material throughout the organisation
- instituting and enforcing policies and procedures to mitigate fraud or other systems abuse
- establishing a coherent security and fraud incident management approach and ensuring adequate escalation procedures
- rehearsing business continuity and disaster recovery procedures
- establishing appropriate authorisation and reporting structures and ensuring isolation between authorisation and execution of security- critical tasks
- maintaining separation between development and production systems
- wherever possible, performing proactive trend analysis on card usage in an effort to detect emerging attacks
- carrying out pre-employment background checks against all employees and contactors
- instituting periodic independent audits and reviews
- providing suitable mechanisms for the communication and handling of cardholder, agency stakeholder or other complaints or concerns; and
- remaining abreast of technology developments, especially in the areas of smartcard and network security threats and vulnerabilities.

12 Standards-related issues in enabling a smartcard deployment

A smartcard is normally one component of a complex system. This means that the interfaces between the card and the rest of the system must be precisely specified and matched to each other. Of course, this could be done for each system case-by-case, without regard to other systems. However, this would mean that a different type of smartcard would be needed for each system. Users would thus have to carry a separate card for each application. To avoid this, attempts have been made to generate international application-independent standards that allow multifunctional cards to be developed.

To achieve interoperability, it is therefore important that smartcard properties are strongly based on international application-based standards⁴⁰. This is fundamentally important with regard to the usually compulsory need for interoperability. Unfortunately, these standards are often very difficult to understand, can be ambiguous and in some critical places require outright interpretation.

The detailed specifications of the smartcard therefore need to be confirmed with the various applicable agency stakeholders during the design phase.

⁴⁰ Where suitable standards exist

13 Interoperability issues

Smartcard interoperability can mean different things to different smartcard schemes. Variants include the ability to use a card designed for one system in another system (this might be called 'issuer layer interoperability'), and the ability to use a card designed for one purpose or sector for an unrelated purpose or sector (this might be called 'application layer interoperability').

Interoperability is discussed in the National Smartcard Framework at the policy, business and technical levels and introduces the concept of Communities of Practice (CoPs). A CoP can be defined as a particular population of smartcard issuers and third parties that have a common requirement to interoperate and agree to issue smartcards according to an agreed set of rules. More information on CoPs can be found in the National Smartcard Framework.

The following is a summary of some of issues associated with interoperability:

- Card interface technical interoperability – is handled either through the use of a common interface between cards, or the use of readers that support multiple interface standards
- Card and application discovery – in order to achieve card interoperability, readers or the associated host applications may be required to identify the card and/or application and other relevant unique identifiers. This requirement may in some cases be in conflict with the desire to prevent leakage of any information which might reveal cardholder attributes. Interoperable card system designers must consider the question of whether they need to use registered identifiers to achieve national or international compatibility and uniqueness; and
- Reader interoperability – there are various standards regarding interoperability of card readers. The ISO/EIC 14443 and 7816 standards for example provide physical and link layer interoperability at the card interface. Further, PC/SC provides basic interoperability at the host interface and ISO/IEC 24727 addresses programming interfaces between the chip and host applications. The PC/SC specifications are based on the ISO 7816 standards and are compatible with both the EMV and GSM industry-specific specifications. For readers that operate in pass-through mode only, interoperability is relatively easy to achieve.

If a smartcard implementation however requires readers that provide more functionality than simple pass-through, for example application management and complex run-time functionality, achieving reader interoperability can be a much more elusive target. It should be noted that EMV, the financial-industry specification, does address reader interoperability in the wider application area. However presently there are a lack of industry standards in terms of:

- multi-application handling
- key management; and
- configuration and transaction data management on the host side.

In most interoperable environments, the reader to back-end physical and electrical interfaces are out of scope. However, the question of data object management must be addressed in the trivial sense so that readers, at least in an off-line architecture, must be able to support data storage and forwarding capabilities that fit the interoperable business rules and acquiring model.

The development of ISO/IEC 24727 will allow for new plug and play capabilities in smartcard technology:

- Extent and nature of interoperability – decisions must be made as to whether interoperability is to be based on a shared application or separate compatible applications, and the extent to which and types of information flows needed to underpin interoperability. Seemingly simple questions such as concession interoperability between state governments in the transit environment may require considerable design time and negotiation. Likewise interoperable data designs presuppose that critical data objects used in one issuer system are recognisable in another issuer system
- Information transfers – assuming front-end interoperability is achieved; system designers must consider what level of back-end (issuer-to-issuer) information needs to be exchanged including configuration and usage data, hotlists, settlement data, key management data and various types of reports
- Service levels – card issuers seeking interoperability must decide which of the range of services available in the primary issuer's network must also be available in the second-party issuer's network. For example, it should be determined whether the second issuer is responsible for dealing with cardholder inquiries or malfunctioning card issues when they did not issue the card or application
- Security model – interoperability may not be feasible where different system operators subscribe to different security methodologies. For example, an issuer will normally not want its keys exposed in a potentially interoperable system that does not implement the same levels of anti-tamper protection or the same level of procedural controls over operations on their applications in the other party's system
- Liability assignment – issuers seeking interoperability must consider which party will be liable for card 'misadventures' or abuses in the other party's system, including fraudulent use
- Revocation or blocking policy – in an interoperable environment, card and application issuers must clearly understand the implications of revocation and blocking in one system for card or application use in another system. Blocking for administrative reasons in one domain may impose unforeseen penalties on a cardholder in another domain
- Contact Card Voltage – smartcards based on ISO-7816 may operate at 5, 3.3 or 1.8V. Cards are not required to operate at each of these voltages, but must not be damaged by the presentation of any of these voltages. Manufacturers generally offer parts that are capable of operating anywhere in the range 5.5 and 2.7V, but due to the additional power needing to be dissipated by on-card regulators, 1.8V chips may not operate at 5V. It should be noted that 5V logic levels are slowly disappearing from the semiconductor industry, with 3.3V currently being the most commonly used chip I/O voltage; and
- Card Communication Protocol (T=0, T=1, T=CL) – card communications methodologies depend on card interface type and application requirements. For contact cards, either ISO7816-3 T=0 or T=1 link-layer protocols are both in widespread use, although T=1 offers improved error detection and is more consistent with the ISO HDLC communications methodology. For ISO1443 – for contactless cards – T=CL is the generally preferred link-layer protocol due to its standardisation, but other proprietary protocols are in widespread use. Above the link layer, ISO 7816-4 message formats are by far the most commonly used.

14 Multi-application smartcard issues

This section deals with specific issues relating to multi-application issuance. Points for system implementers to consider include:

- multi-application environments in existing schemes range over a wide set of potential uses. The most common form of multi-application card is one which carries secondary applications which are indirectly related to the primary application. A good example is the inclusion of a separate 'operator application' in conjunction with a transit smartcard purse. Operator employees are able to use the one smartcard for travel as well as equipment log-on and operator-specific functions⁴¹
- in other multi-application environments, the card architecture supports second and subsequent generic data storage and retrieval applications. The ISO/IEC 24727 provides good examples of how to handle a generic multi-application card environment
- applications sharing a card will be dependent on security and administrative features provided by the card operating system and the 'issuer application' on the card. Access to spare application space on the card will normally require access to keys created for that space by the issuer and may also rely on cards being passed through a special reader-based issuance process to add the additional application. Some multi-application issuers pre-partition the memory space on their cards, and also pre-populate these applications areas with transport or 'placeholder keys' to ease downloading of new applications on the card
- close consideration must be given in multi-application environments to a number of practical issues including:
 - whether the application is to be resident at time of card issue or loaded subsequently
 - if the application is loaded post card issuance, whether the application is dynamically loaded and unloaded (as can be provided on a JavaCard platform), or whether it is statically loaded to be card resident
 - where the application is to be a passive file-based data read-write application or whether it requires specific algorithms or business logic on-card
 - whether revocation or blocking of an application necessitates or warrants card blocking
 - which information elements must be provided in support of card and application discovery
 - memory wear and tear issues – heavy use of one application may result in reduction of card useful life for all application providers on that card and unfairly impose card re-issuance costs on other parties
 - cardholder support for problems or queries not related to a given application issuer's business, and/or the possible sharing of a common help desk

⁴¹ The two applications are cryptographically isolated

- whether there is any need for applications to share a common data space (e.g. some transit multi-applications have a common purse); and
- card co-branding (see also Section 4.5).

14.1 Access to other agency's data

Concerns and benefits surround the question of sharing data between applications. Where an agency's data is to be restricted to that one agency, the separation must be strongly enforced by using agency-specific keys. Where, by policy, agency data may be shared then a decision must be made as to whether that data is to be located in a public part of the card memory (accessible to anyone) or accessible only through the use of an inter-agency key set.

Examples of beneficial sharing are, but are not limited to, sharing of one PIN between multiple applications, or sharing of an on-card service like biometric template verification. Dependent upon the implementation, and subject to a privacy impact assessment, the ability of sharing such information as common cardholder information, e.g. contact details, may be viable.

Some other questions needing to be addressed include:

- which agency or application issuer has prime responsibility and liability for the integrity of shared data?
- is minimising data held on the card a better option than retaining such information at the system back-end? Where the card is used to actuate sharing of data held elsewhere in the network rather than providing the data directly, there are clearly issues relating to the binding of access to that information to authentication of the cardholder; and
- what are the underlying key management and control processes needed to grant the relevant access privileges and revoke them at appropriate points?