Disclaimer

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

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

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

Department of Finance and Deregulation

Australian Government Information Management Office

© Commonwealth of Australia 2008

ISBN (online): 0 9758173 6 1

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

Commonwealth Copyright Administration,
Attorney General's Department,
Robert Garran Offices,
National Circuit,
Barton ACT 2600

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

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Copyright: Department of Finance and Deregulation
Contents

1 Introduction 2
1.1 Audience 2
1.2 Document structure 2
1.3 Acronyms 3
1.4 Contact details 3
2 What are smartcards? 4
3 What are the advantages of smartcards? 7
3.1 Fundamental properties 7
3.2 Applied benefits 8
4 Smartcard systems and deployments 9
5 Types of smartcard 12
5.1 Memory chips (including serial protected memory chips) 12
5.2 ROM-mask cards 12
5.3 Micro-controller cards 12
6 Smartcard interfaces: contact and contactless 14
7 Smartcard readers 16
8 Smartcard security 18
8.1 Special security features of smartcards 18
8.2 Potential security vulnerabilities 19
9 Operating systems 21
10 Typical smartcard applications 22
10.1 Where are smartcards used? 22
10.2 Financial applications 23
10.3 Communications applications 23
10.4 Government programs 23
10.5 Information security 24
10.6 Physical access 24
10.7 Transportation 24
10.8 Retail and loyalty 24
10.9 Health card 24
10.10 Campus cards 25
11 Developing the business case for smartcard deployments 26
11.1 What is a business case? 26
12 When should agencies consider implementing smartcards? 28
12.1 Specific capability required 28
12.2 Portability 28
12.3 Identity authentication/information security 28
12.4 Automatic forms population 29
12.5 Multi-application enabler 29
12.6 Updatable applications 29
12.7 Hybridising card technologies 29
12.8 Cost sharing 30
1 Introduction

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

The National Smartcard Framework (the Framework) is one of a number of frameworks and strategies developed to support interoperable whole-of-government business applications. The Framework should be read in conjunction with other Australian Government frameworks, including the Attorney-General’s Department’s National Identity Security Strategy, AGIMO’s Australian Government Technical 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 includes:

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

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

1.1 Audience

The Framework is aimed at government agencies deploying smartcards, and third-party service providers delivering smartcard solutions on behalf of a government agency. This Smartcard Handbook should be read by technically adept newcomers seeking a comprehensive introduction to the field as well as reference material on certain government issues, such as security and privacy.

1.2 Document structure

This Smartcard Handbook comprises an overview of smartcard technology (including its fundamental properties and benefits), smartcard systems and schemes, types of smartcard, security and privacy and typical smartcard applications. It includes an overview of how to make the business case for smartcard deployments and outlines a preferred model for smartcard content.
1.3 Acronyms

AGIMO Australian Government Information Management Office
AS Australian Standard
ATM automated teller machine
CPU central processing unit
EEPROM electrically erasable programmable read only memory
EFT electronic funds transfer
EFTPOS electronic funds transfer at point of sale
EMV Europay-MasterCard-Visa
FIPS Federal Information Processing Standards [United States]
GSM global system for mobile communications
ICC integrated circuit card
ICT information and communications technology
ID identity
IEC International Electrotechnical Commission
IMAGE Identity Management for Australian Government Employees Framework
ISO International Standards Organization
MultOS A programming language developed by Mondex for systems using MAOS (multi-application operating systems) for smartcards
NeAF National e-Authentication Framework
NIST National Institute of Standards and Technology [United States]
PC personal computer
PC/SC personal computer/smartcard (interface standards) [international]
PIN personal identification number
PIV personal identity verification [scheme of the United States]
PKI public key infrastructure
RAM random access memory
ROM read only memory
RSA Rivest Shamir & Adelman [a cryptographic algorithm]
SAM security access module
SIM subscriber identification module

1.4 Contact details

Inquiries and comments should be forwarded to <smartcard@finance.gov.au>.
What are smartcards?

The term ‘smartcard’ means an entire class of credit-card-sized devices fitted with a micro-chip to deliver one or more ‘intelligent’ capabilities. The classic examples of smartcards include stored-value cards or ‘electronic purses’ used to convey electronic cash, personal electronic health cards which might carry compact summary records of personal medical data, and smart credit/debit cards which replace insecure magnetic stripe storage of cardholder details with access-controlled chip-based storage that is resistant to copying.

Importantly, examples of smartcard technology encompass a far broader range of applications. A more complete but not exhaustive list of applications for smartcard technologies includes:

- health and services cards
- ATM and EFTPOS cards
- telephone (calling) cards
- identification (including government identity (ID) cards, employee ID badges and membership cards)
- mobile phone subscriber identification and administration (SIM)
- transport ticketing and tolling
- electronic passports; and
- healthcare (which can include portable record keeping as well as ‘identification’).

The physical form of smartcards extends beyond the plastic card. Smart ‘chip’ technology is available in various packaging and communication interfaces, including:

- mobile phone SIMs (typically punched out from a larger plastic card)
- ‘fobs’ that are usually carried on a conventional key ring or a lanyard
- USB keys
- radio frequency road toll tags
- electronic passports; and
- credit card-sized plastic cards.

A great deal turns on the sophistication of the chip. Some simple smartcard applications require no more than a memory chip in which off-card applications can store user-specific data (such as the number of remaining public transport rides or the value of remaining telephone calls). Other applications require the equivalent of an entire micro-computer to be embedded within the smartcard: a micro-controller, various types of memory and an operating system. Multi-application smartcards today have approximately the same capabilities and logical powers as the first
commercial micro-computers in the mid 1970s. The typical major elements of a multi-application smartcard are:

• Central processing unit (CPU) or simply the ‘processor’, which is the core of the micro-controller.

• Read only memory (ROM) for carrying operating system and built-in programs loaded at the time the card chip is manufactured.

• Electrically Erasable Programming Read Only Memory (EEPROM) non volatile memory normally used for storing data and card applications.

• Writable memory (RAM) is volatile and hence is only used for temporary storage (not used for permanent storage). Data and applications are generally stored in EEPROM, however, to save personalisation time card applications are sometimes stored in the ROM.

• Card Operating System for controlling execution of application software, loading of new application program files, reading and writing of data to memory, and general low-level functions, such as power on and power off. It is especially crucial when a card carries more than one program. In other words, the card operating system is used for accessing the CPU, EEPROM, RAM and ROM (typically referred to as the ROM-mask).

• File system (which may be part of the card operating system) manages how data is stored and how programs on the card (as well as external devices like card readers) can read and write to the EEPROM. Sophisticated smartcard file systems feature memory protection to safeguard against application bugs and deliberate hacking, and access controls, which can discriminate between different users and programs in terms of their rights to read from or write to certain areas of memory. A file system can be implemented as an application on a multi-programmable smartcard.

• Communications interfaces are the means by which a smartcard can interact with the outside world by exchanging electrical signals with a card reader. Broadly, there are two types of interface:

  - contact, in which signals are conveyed directly via the flat metal electrodes seen on the surface of many cards; or

  - contactless, in which signals are carried by a radio frequency link involving an ‘antenna’ (more commonly called a coil in which electrical current is induced) built into the plastic of the card. Critical to the performance of a contactless card is the integrity of the card reader.

• Application software (implement business rules) runs on the smartcard’s CPU, and is what produces the major functional differences between different smartcard deployments. Smartcard applications run in much the same way as regular personal computer (PC) software, except that, by PC standards, smartcards have tiny memory capacity and limited input/output capabilities.

• Special-purpose hardware is built into many sophisticated smartcards to deliver certain functions more securely and/or more efficiently. In particular, cryptographic co-processors are increasingly commonplace, providing asymmetric encryption, authentication and key generation services to the software running on the card.
Smartcards thus embody an ordered technology ‘stack’, comprising relatively discrete layers, each of which mainly interacts only with immediately neighbouring layers via formal and standardised interfaces (see Figure 1).

![Figure 1: Indicative Smartcard technology ‘stack’ (file system architecture)](image)

Figure 1: Indicative Smartcard technology ‘stack’ (file system architecture)
3 What are the advantages of smartcards?

3.1 Fundamental properties

While smartcards are plastic cards with an embedded chip, they have several truly unique fundamental properties that underpin their business benefits. The fundamental properties are as follows:

• For all practical purposes, it is not possible to copy or counterfeit a smartcard. Smartcards can be configured to divulge their data only to specially qualified and authenticated terminal equipment. Magnetic stripe cards, on the other hand, store everything in a passive magnetic stripe, and anyone with a reader can skim off the data and replicate it at will onto counterfeit cards. Furthermore, smartcards carry buried cryptographic codes, written onto the silicon chip or into firmware at the time of manufacture. Even if an attacker obtains a smartcard and the related personal identification number (PIN), they will not be able to clone the card or use it to spawn counterfeits.

For detailed qualifications to the claim that smartcards, for all practical purposes, cannot be copied see Section 8 ‘Smartcard security’ below.

• Smart ‘chips’ are ‘smart’. This allows a smartcard to exhibit a far more intelligent and therefore richer set of functions than a magnetic stripe card (or most other authentication tokens excluding ‘fobs’ which can have as many features as a contactless card). In addition, smartcards can act independently from a back-end system or offline, allowing security rules to be enforced offline.

• The chip allows intelligent access control around the contents and functions of the smartcard. Multi-application smartcards provide global PIN functionality. Smartcards allow a rich suite of access control rules that can be associated with different data containers. Smartcard data can therefore be protected so an attacker cannot freely read it, as is the case with magnetic stripe cards.

• Smartcards are capable of mutual authentication in online transactions. The chip and/or tamper-resistant memory allow the client side of a transaction to actively verify the identity of the server before the server identifies the client. This property assists in countering man-in-the-middle attack.

1 Recall that the scope of this Framework is multi-programmable smartcards. Other types of cards, such as memory-only devices, are not so smart in the sense meant here.

2 The head of cryptography at NIST has stated that, for Level 4 authentication in the PIV (that is, the highest level, where resistance to man-in-the-middle attack is required), the ‘only practical solution today uses PKI [and hard tokens]’, viz smartcards. Ref: Electronic Authentication in the US Federal Government, Bill Burr, Asia PKI Forum Tokyo, February 2005.
3.2 Applied benefits

As a consequence of the above fundamental properties, today’s sophisticated smartcards offer certain advantages in certain settings, including:

• Multi-applications. A single smartcard can perform multiple independent tasks. For example, a bank-issued smart credit card might also furnish an electronic purse, public transport ticket, telephone calling card, loyalty functions, personalised access to government services and multiple individual digital certificates.

• Sophisticated fraud detection and response is possible, for example, in environments where connection to backend systems cannot be relied upon. For instance, the card alone can enforce security rules relating to daily transaction caps, maximum PIN retries or purchasing patterns.

• Containers for multiple digital credentials. The writable memory, access control and encryption capabilities of modern smartcards allow them to carry multiple independent identifiers, or digital certificates. A card scheme operator may choose to use a third party’s digital certificate rather than their own which requires the certification authority to collaborate with the card issuer in the printing of the cards.

• Online security can be greatly enhanced using smartcards thanks to their mutual authentication capabilities. In particular, smartcards can help protect against website fraud, phishing and ‘pharming’ (where large numbers of unwitting users are directed to a fake or spoofed website, and subsequently led to divulge sensitive information or to initiate inappropriate transactions).

• Two-factor authentication requires two out of ‘something you know’, ‘something you have’ or ‘something you are’. A common example of two-factor authentication is a bank card (credit card, debit card); the card itself is the physical item, and the PIN is the data that goes with it. Smartcards also constitute two-factor authentication being physical tokens like the common bank card.

• Field upgrades are possible for functional enhancements, bug fixes or to load entirely new applications. The built-in security capabilities make it possible in many cases to upgrade smartcards remotely, avoiding the need to recall and re-distribute fresh cards.

In Section 10 ‘Typical smartcard applications’ the various sectors and business applications where smartcards are being canvassed in detail, and a number of case studies are presented.
Smartcard systems and deployments

Smartcards require readers in order to communicate with computer applications (these are discussed further in Section 7 ‘Smartcard readers’). Before going into detail, it is important to characterise the minimum combination of smartcard plus reader plus computer because it is the ‘edges’ of these sub-systems (that is, the interfaces between them) that most fundamentally determine interoperability. Standardisation of the edges is a necessary, but unfortunately not sufficient, condition for application-level interoperability. Figure 2 illustrates the interactions between the three main parts of a smartcard system.

Figure 2: Smartcard system schematic

If a number of parties – including agencies across jurisdictions – can agree to share a card and/or the associated infrastructure, then the system cost to each party may be reduced and the number of locations where the card can be used increased. The use of credit and EFTPOS cards is an example of this. Such deployments require careful and detailed consideration of the legal, management, technical, cultural, security and other issues involved from the outset. Agencies need to be aware that it takes time to satisfactorily resolve these issues.
To fully describe and manage smartcard implementations, a further layer of abstraction is needed on top of cards and systems – the deployment. For the purposes of this Framework, a smartcard deployment is referred to as an ensemble of:

- smartcard systems (that is, cards plus readers plus computers)
- business rules (including the business objectives, agreed technical standards, usage agreements, terms and conditions applying to all parties, liability arrangements, dispute resolution and so on)
- applications that use the card systems
- processes for getting cards to users and for supporting the infrastructure
- for a ‘full blown’ deployment, accreditation processes for determining the compliance of all parts of the implementation to the agreed standards; and
- Inter-deployment or Inter-agency arrangements; system-to-system issues

Deployment Rules; Liability arrangements; Compliance, Audit & Certification;

Interoperability Agreements with other Implementations/Deployments

Terms & Conditions; Enrolment procedures

Card fulfilment, distribution & support; Card lifecycle management; User Help Desk; Reader support

Sub-system procurement; Application Software Development and Support; Card & Reader upgrades

Figure 3: Smartcard deployment schematic
Some examples of smartcard implementations include:

- the United States Government’s new Personal Identity Verification (PIV) of Federal Employees and Contractors scheme
- the Australian Government’s Identity Management for Australian Government Employees Framework (IMAGE)
- the financial sector’s Europay-MasterCard-Visa (EMV) model for smartcard credit and debit products
- independent credit card programs of, for example, Visa and MasterCard, under EMV specifications
- consumer health card schemes in, for example, Austria and Taiwan; and
- any one of a number of commercial public transport ticketing projects.

When considering interoperability, it is important to examine interoperability at each of the following levels:

- technical - across the edges between cards, readers and computers
- information - where, for instance, one bank’s ATM network might be able to use data from another bank’s card
- business - where, for instance, much work has been done to join road tolling schemes, and how smartcard driver licences might be usefully and safely joined to commercial business offerings, or used to control access to government services.
5 Types of smartcard

Smartcards are distinguished by the design type of the chip they contain, and by the type of interface used to communicate with the reader. There are three different types of chip.

5.1 Memory chips (including serial protected memory chips)

Memory-only smartcards are functionally similar to magnetic stripe cards and store only data. They depend on the card reader (also known as the card-accepting device) for their processing and are suitable for uses where the card system performs a fixed operation.

Compared with magnetic stripe cards:

- memory cards have a far higher data capacity (typically up to 16 thousand bits (Kbits) compared with 80 bytes per track across usually no more than three tracks on a conventional card); and

- serial-protected memory chip cards have an additional security feature – they can contain a hardwired memory that cannot be overwritten.

An example of a memory card is a photocopier card.

5.2 ROM-mask cards

ROM-mask cards have a fixed set of rudimentary computing functions built into a special-purpose chip: they are not programmable after manufacture. These cards provide a static file system supporting multiple applications implemented external to the smartcard; memory contents may be encrypted depending on the design of the chip. Their file systems and command set can be changed only by redesigning the logic of the chip and manufacturing a new batch of cards. ROM-mask cards are cheaper than multi-programmable smartcards when produced in large numbers, and are simpler to support.

Examples of ROM-mask cards include pre-paid telephone cards and special-purpose ticketing and tolling cards (such as the MIFARE standard).

5.3 Micro-controller cards

Micro-controller cards contain a computer-on-a-chip, with operating system, and read/write memory that can be updated many times. Micro-controller cards contain and execute logic and calculations, and store data in accordance with their operating system. They are like a miniature PC one can carry in a wallet. All they need to operate is power and a communication terminal.

Contact, contactless and dual-interface micro-controller integrated circuits are available. Unlike memory-only products, these micro-controller integrated circuits have been designed (and can be verified) to meet security targets, such as Common Criteria.

A multi-programmable card may serve as an identity authentication token and may also provide the cardholder with additional capabilities, such as digital signing for email, message encryption, payment using an electronic purse, physical access to controlled buildings, logical access to computer systems, and (limited) data storage of, for example, medical information for use by authorised personnel. Both contact and contactless smartcards can be multi-programmable.
When using a multi-programmable card, each application may be managed by a different group within an agency or even by an external application provider (for example, a third-party electronic purse for cafeteria use). While requiring more complex organisational coordination, implementation of multiple applications can enhance the business case supporting the adoption of smartcards.
Smartcard interfaces: contact and contactless

There are two primary types of chip card interfaces – contact and contactless. The terms contact and contactless describe the means by which electrical power is supplied to the integrated circuit card and data is transferred from the card to an interface (or card-accepting) device (reader).

- **Contact smartcards** require insertion into a smartcard reader so the reader can establish a direct electrical contact with the chip. Contact cards are generally used for a wide variety of applications, including financial transactions and logical access control.

- **Contactless smartcards** contain a chip and an antenna sandwiched between two layers of plastic. Contactless smartcards only have to be close to the reader (generally within 10 cm) for data exchange to take place. The contactless data exchange takes place over radio frequency waves. The device that facilitates communication between the card and the reader is a radio frequency antenna internal to both the card and the reader.

Contactless chips are typically used for functions that require rapid user throughput, such as high-volume transit automated fare collection systems or office building access. Wear and tear on card readers is reduced, which is a significant practical consideration in facilities security and management. Contactless chips have become increasingly accepted as the token of choice for controlling physical access. The contact interface tends to be preferred when smartcards are implemented for logical access control (computer logon) because positive and tangible contact must be reliably maintained for long periods, especially when digital signatures are in use. A drawback of contactless cards in logical access control is that other cards may be in the field without the user being aware of it. Furthermore, contactless cards are, in principle, more vulnerable to eavesdropping and to denial-of-service attacks.

Cards may offer both contact and contactless interfaces in the same package, via two differing design strategies:

- **Hybrid smartcards** contain two chips, one supporting a contact interface and one supporting a contactless interface. The chips on hybrid smartcards are generally not connected to each other. These products allow organisations to use a single credential to satisfy both contactless physical access control applications and applications requiring a contact interface, such as logical access to computers and networks.

- **Dual-interface smartcards** contain a single chip that supports both contact and contactless interfaces. These dual-interface cards provide the functionality of both contact and contactless cards in a single physical package, with designs able to allow the same information to be accessed via contact or contactless readers.

---

3 One particular scenario of concern for denial of service is where an attacker with a relatively high-powered transmitter might be able to send repeated bogus PIN entry attempts to all contactless chips within range, causing the chips to block themselves and, in effect, shut down.
Contact, contactless and dual interface smartcards can support multiple applications, offering advantages to both the organisation issuing the card and the cardholder.

A card containing several types of read/write media is generally called a multi-technology card. For example, the user may want a newly issued smartcard to interface directly with an existing physical access control system that uses legacy technology. To accommodate this, the new card can be produced with contact or contactless smart chip technology, magnetic stripe, barcode, optical stripe and/or a 125 kHz proximity antenna.

While multi-technology cards may provide solutions for accommodating legacy access control systems, organisations should carefully consider the added complexity of implementing and maintaining multiple technologies.
7 Smartcard readers

Smartcard readers interface cards to computers, allowing them to communicate with one another and hence, at the card edge level, to ‘interoperate’. Very broadly, there are two families of smartcard readers, following the two types of communications interface discussed above. However, additional characteristics become important at the reader level and in respect of the reader-to-computer interface.

In particular, smartcard readers feature a range of security mechanisms at different price points. The simplest smartcard reader does little more than bring out the raw signals from the card and present them to a computer’s input/output port. In these cases, not only are there vulnerabilities to interception by attackers at the edge but more subtly, critical security information, especially PINs and passwords, can be intercepted by keystroke loggers within the computer application when the regular keyboard is invoked.

It is possible to classify smartcard readers in several ways:

- Contact versus contactless. Obviously the different communications methods necessitate different physical arrangements for readers to interface to smartcards through contact or through wireless. Note too that within the contactless group, different readers may be needed to handle different range protocols (although superficially all contactless readers may appear as fundamentally similarly plain plastic boxes near which a smartcard is passed).

- Slide contact versus landed contact. For contact cards, the reader may make physical contact with the card terminal pads either by sliding the card into position against what are typically leaf springs, or by a motorised arrangement which brings the reader connections into more active contact with the pads. In the latter case, the reader will often capture the card inside the mechanism, by a tractor arrangement, as is typically the case in Automatic Teller Machines. Readers that capture the card are more expensive, but they prevent ‘tearing’ where a card is removed for whatever reason in the midst of a transaction. Furthermore, they are far more resistant to attempts by criminals to insert mocked-up cards, because the capture mechanism can make sure the card conforms to ISO 7816 physical specification (and that it is in fact a card and not a long flat probe); such readers can, for example, include knives to cut off any wires that should not be inserted into the reader.

- Dumb readers versus intelligent readers. A so-called dumb reader basically passes signals straight through between the smartcard and the host computer. In contrast, intelligent readers take on a greater share of the host–card interactions and the human–card interactions. For instance, because PIN entry from a regular host PC may be vulnerable to keyboard sniffing, a more secure solution is for the PIN to be entered into a special purpose keypad built into the reader and controlled by dedicated firmware rather than the PC operating system. Naturally there is a cost–benefit trade–off in these more sophisticated types of readers.

- Readers with security access modules. These readers are required to accommodate external authentication functionality, that is, they securely store keys to access containers on the card.

- Hand-held readers. These will be a major infrastructure component for deployments such as smartcard driver licences, particularly for police roadside use.
Many environments mandate physically secure PIN pads integrated with the smartcard reader. Additional electronic security enforcing functions can be engineered into readers to make them resistant to tampering. Notably in the banking sector, peripheral equipment standards such as AS 2805 Electronic funds transfer – Requirements for interfaces (and industry association or even legislative mandates) have long governed the quality and tamper resistance of card readers; Security Access Modules (SAMS) tend to be standard in EFTPOS terminal equipment under banking standards of this type. Of course, wrapped around the issue of standards compliance is independent conformance testing and accreditation.

Another layer of security that may apply at the card reader edge is mutual authentication, in particular, authentication by the card of the reader and authentication of the card by the reader before establishing a session. This mechanism allows smartcards to detect rogue terminal equipment and shut down operations to avoid hacking. In particular, banking smartcards can detect the presence of non-accredited or unapproved terminal equipment.

Some smartcard deployments use special-purpose readers, put in the hands of specially authorised parties. For example, the Taiwan National Health Insurance smartcard has been configured to fully interoperate only with special medical sector devices, as a (rather strict) way of controlling function creep and eventual privacy compromises. Elsewhere, some policy makers have foreshadowed special terminals being used in hospital emergency rooms which might – provided the smartcards themselves are so designed – allow operators to override the usual user PIN protections in order to access information when the user is not competent, for example, in emergency situations.

Finally, customised cut-down readers have also been deployed to make use of smartcard functions for special applications. For example, EMV smartcards have basic cryptographic commands built into them so they can encrypt input data and return a result. These basic commands can be put to use in a simple challenge–response calculator into which an EMV card is slipped to provide the necessary computing and cryptographic keys; in effect the smartcard is transformed into a regular two-factor authentication token. Such customised readers make EMV cards valuable for online authentication, without the need for a traditional smartcard reader to be connected to a PC.
8 Smartcard security

This section explores the logical security features of smartcards, especially those safeguards that are afforded by the processing capabilities of the embedded chip, operating on its own and/or in concert with other sub-systems.

The field of plastic card technology overlaps with smartcards, and includes a whole spectrum of other security measures such as holograms, security overlays, guilloche printing, micro-printing, optically variable printing, etc. This is a rich and complex area, not peculiar to smartcards. It is, however, very relevant to smartcards, particularly when human-readable security features are required.

8.1 Special security features of smartcards

In contrast to magnetic stripe cards, as well as many other authentication technologies, today’s more sophisticated multi-application smartcards feature a wide menu of possible security functions. These security functions can each have its own access control rules which can be a secret of varying type, for example, PIN, symmetric key, biometrics, etc. Some of these have been canvassed already in this document:

- PIN-protected card access, with fine-grained access controls to data objects so that different areas of memory can be subject to different security rules. Likewise, functions in the card, including those realised using card applications downloaded into multi-programmable smartcards, can also be PIN-enabled, to help safeguard lost and stolen smartcards against potential abuse.

- Cardholder verification – the card may use a built-in PIN or biometric template to prevent misuse if lost or stolen.

- Card and terminal verification – the card and the card reader mutually authenticate to ensure each is genuine.

- Cryptography - including private key storage, on-chip key generation, symmetric encryption, public key security functionality, certificate storage and management. A smartcard may have sufficient processing power, especially if manufactured with a cryptographic co-processor, to carry out a range of cryptographic functions independently from external equipment to enforce a number of security functions. These include both symmetric and asymmetric (public key) functions. In particular, digital signatures may be generated on the card, without ever releasing the private signing key to the outside world.

Device security and prevention of counterfeiting, cloning or skimming are provided by a number of high-integrity features resistant to unauthorised access. For example, low-level codes or serial numbers can be hard-wired or ‘burnt’ into the smartcard hardware or firmware at manufacture. Thus smartcards cannot be duplicated without a comprehensive attack on the smartcard foundry itself, or by gaining access to design details of the semiconductor chip mask, information which is held extremely closely by the manufacturers and which is not useful to attackers unless

---

4 Any government smartcard deployment that incorporates digital certificates must ensure it uses digital certificates issued by a Gatekeeper accredited or recognised service provider
they themselves can fabricate chips. Even if an attacker obtains the cardholder’s PIN, while they may be able to abuse the card until such time as it is revoked, they will, for all practical purposes, be unable to duplicate the card.

- Tamper-resistance – attempts to access a chip directly, bypassing the contacts, can be detected, made evident by security plastics design, and/or responded to actively by shutting down chip functions or ‘zero-ising’ data.

- Biometrics – templates for secure one-to-one verification may be stored on the smartcard. Added security may come from implementing ‘match-on-card’, which obviates the need for biometric templates to be stored centrally. Match-on-card has several benefits including better resistance to replay attack, less reliance on network performance or availability, and a reduction in sensitive information being stored centrally where it might be attacked.

On the other hand, because biometric templates and algorithms are usually proprietary, interoperability between sensors, software and cards from different vendors is difficult to achieve, leading to difficult choices needing to be made around single vendor biometric solutions. A common compromise approach today is to only store raw biometric data – such as JPEG images of fingerprints or faces – on the smartcard, on the basis that a wider range of algorithms will be usable for match processing. Match-on-card is basically ruled out when raw data is stored on the chip as smartcard memory requirements are significantly increased.

- Identity management – smartcards can be configured as ‘containers’ for identifiers and digital credentials, as raw data, or for added security in the form of public key certificates. Such IDs might be held in free-read memory, or kept in access-controlled memory where PIN protection adds security and privacy (consent) mechanisms.

### 8.2 Potential security vulnerabilities

There is, of course, no such thing as perfect security. Like any other security component, smartcards have their own vulnerabilities. Moreover, smartcards are only one component of an overarching information system, the end-to-end security of which will depend on many other factors. In all cases, smartcard deployments should undertake threat and risk assessments specific to their local requirements, and/or other security reviews as appropriate. The major security vulnerabilities are:

- Direct probing by, for example, scanning electron microscope, bypassing the contacts can in principle be used to reveal memory contents. Codes might then be discovered or other secret firmware security functions reverse-engineered. A range of protective mechanisms are available, and are measured and certified under standards such as the United States Federal Information Processing Standards (FIPS) 140-2. These mechanisms should not be regarded as a definitive list.

- ‘Side channel’ attacks make use of inadvertent signals emitted by a system through the course of its operation to reveal critical information to an attacker. The term refers to the use of a communication medium other than the intended ones. Side channel attacks are the subject of intense academic and private sector research and development. Some of the better known side channel attacks on smartcard hardware, all of which have specific countermeasures known to the smartcard manufacturers, are:
- differential power analysis – the cryptographic operations of a chip can cause tiny real-time variations in power consumption which, if analysed carefully, can reveal information about the security codes contained inside; to effect a differential power analysis attack, surreptitious modifications might be made to a smartcard reader to retrieve the necessary power signal

- timing attacks – similar to differential power analysis, these involve looking at miniscule variations in the time taken to execute cryptographic operations, and analysing the data to shed light on the values of internal codes

- the ‘Belcore attack’ is a type of fault injection technique where irradiating a smartcard non-destructively can invoke exceptional behaviours and thereby reveal card contents to a skilled analyst.

• Cryptanalysis is the practice of seeking fundamental weaknesses in publicly disclosed algorithms.

• Quantum computing is recognised as an in-principle threat to today’s number theoretical approaches to cryptography. Today’s factorisation-based encryption algorithms like RSA are based on the computational difficulty of working out the factors of large numbers; the only known approaches rest largely on ‘brute force’ or trial and error, which takes unfeasibly long periods of time with conventional computing technologies. Quantum computers represent a radically different architecture, which in theory can perform certain types of parallel operations (like factoring) almost instantaneously, which would render today’s cryptography obsolete. There is a possibility that quantum computing will progress to commercial availability at some point in the future, but this prospect affects all security systems, not just smartcards.
9 Operating systems

Almost all computers feature a built-in ‘executive’ program called the ‘operating system’, which controls resources like memory, input/output, instruction processing and security, and allows application software to access and use those resources. Specialised computer systems like smartcards require special operating systems to address issues such as small memory size, relatively low-speed interfaces, unusual hardware features, and security in the multi-application environment.

Two of the most widely used card operating systems in the smartcard industry are Javacard and MultOS\(^5\) (although there are many others with smaller market share or special niche market positions, including some open source ones). These are both proprietary but over time have gradually become more transparent. MultOS defines a platform for card and application life cycle management, including application loading, deleting and data updating. Javacard, the Global Platform specifications, also provides standards for an open smartcard infrastructure that enables service providers from many industries to deploy and manage multiple applications for their customers through a variety of devices\(^6\).

Selection of an appropriate operating system can be critical to card success. Choosing the correct operating system increases the functionality of the card by supporting reconfiguration of applications after the card is issued. In many instances, an issuing organisation initially deploys a card with a single application; then, as card acceptance grows and market opportunities arise, the issuer can increase the functionality of the card by adding new applications. Applications can be added efficiently when an operating system supports secure dynamic loading and unloading of applications.

An open operating system allows any card deployment to migrate to more functionality as market and consumer acceptance increase.

---

\(^5\) For more information see Java Card Forum at [www.javacardforum.org](http://www.javacardforum.org) and MAOSCO at [www.multos.com](http://www.multos.com)

\(^6\) For more information see [www.globalplatform.org](http://www.globalplatform.org)
10 Typical smartcard applications

10.1 Where are smartcards used?

The properties and benefits of smartcard technology lend themselves to applications with the following features:

• ‘Offline’ electronic transaction environments where business rules can be enforced by the card without connection to back-end systems, for example, daily transaction limits with credit cards, entitlements with social security cards. This eases the burden on the back-end and on the network, and improves flexibility, for example, in retail environments. Note too that PIN match-on-card improves systemic security by reducing the extraneous personal information sent over the network.

• Where identity theft is a significant risk. Well-designed and manufactured smartcards for all intents and purposes cannot be skimmed, cloned from intercepted transaction data or counterfeited (hence the EMV scheme).

• Online transactions with relatively high-risk profiles where active mutual authentication is important to prevent website fraud through man-in-the-middle attack (refer, for example, to authentication Levels 3 and 4 in the National e-Authentication Framework published by AGIMO and Levels 3 and 4 in the United States National Institute of Standards and Technology (NIST) SP800-63: Electronic Authentication Guideline).

• Public key infrastructure (PKI). Smartcards with on-chip key generation and digital signature functions are the ideal key storage medium in a wide range of emerging PKI applications, especially e-health and the professions, e.g. legal, medical, engineering.

• Biometric systems, especially with one-to-one verification and match-on-card.

• Multi-application settings, where it is useful to offer multiple functions through the one card or to upgrade cards over time. The financial sector has, to date, offered most examples in this category, where sophisticated banking products have been launched which can roll together electronic purse and public transport ticketing with debit/credit offerings.

• Smartcards can serve as credit, debit or stored-value payment and/or payment token instruments, and can provide improved online authentication to underpin access to financial accounts, funds transfers, payment instructions and so on.

• Information storage and management tools. Depending on the memory size of the integrated circuit card, smartcards can store and manage data to assist with various applications; for example, summarised medical information stored on a smartcard could, in principle, be made accessible by an authorised medical official in the event of an emergency or on a routine medical visit, subject, of course, to careful privacy design and appropriate consent mechanisms being in place.

The remainder of this section lists major applications seen to date.
10.2 Financial applications

- Credit and/or debit accounts, replicating what is currently on the magnetic stripe bank card, but with greater protection against counterfeiting and skimming; and
- Securing payment across the Internet as part of electronic commerce to potentially reduce fraud in remote transactions.
- Electronic purse/stored-value cards to replace coins for small purchases in vending machines and over-the-counter transactions or even prepaid telephone cards (electronic purses have proven most practicable so far in tightly closed and temporary populations, such as holiday resorts and cruise ships).

10.3 Communications applications

- Mobile telephony – global system for mobile (GSM) communications SIMs are smartcards that identify the subscriber to the telephone system, for billing purposes, to control global roaming, and to manage keys for voice and data encryption. They can also store personal information such as frequently called numbers. SIM cards may be moved from telephone to telephone.
- Subscriber activation of programming on pay television; and
- Cards that allow set-top boxes on televisions to remain secure from piracy.

10.4 Government programs

- Electronic benefits transfer using smartcards.
- Cards may be used for a range of specific public sector applications, such as library cards or learning cards.
- Official documents may be issued in the form of smartcards, as a secure alternative to paper documents, for example, drivers licences, electronic passports.
- Digital credentials or business licences can be carried by smartcard.
- Identification cards may be used to identify either government employees or members of the public and provide access to buildings or computer systems.

For example, the city of Pusan, Republic of Korea has implemented a multi-application e-currency biometrics smartcard that is used as an e-government ID card, a payment card for mass transportation, as well as for banking transactions, point-of-sale transactions, Internet activity and other financial dealings. Other examples include the Smartcities initiative in the United Kingdom, ConneXions and electronic IDs (eIDs) as implemented on the Belgian eID card.
10.5 **Information security**

- Employee access card with secured passwords and the potential to employ biometrics to protect access to computer systems.

- An individual or an organisation may use cards to digitally sign electronic messages, thereby providing proof of authenticity and integrity (digital certificate included on chip).

10.6 **Physical access**

- Employee access card with secured ID and the potential to employ biometrics to protect physical access to facilities

10.7 **Transportation**

- Drivers licences

- Mass transit fare collection systems

- Electronic toll collection systems

10.8 **Retail and loyalty**

- Consumer reward/redemption tracking on a smart loyalty card that is marketed to specific consumer profiles and linked to one or more specific retailers serving that profile set.

10.9 **Health card**

The limited memory capacity of even the most sophisticated smartcards means they are not able to store a great deal of healthcare related information. In any case, the dynamic and decentralised nature of longitudinal personal health information means most shared electronic health record architectures today do not envisage using smartcards as more than security keys to access data.

- Consumer health card containing insurance eligibility and other entitlements.

- A patient’s smartcard can act as a key which healthcare professionals can use to access electronic health records, with the patient’s consent.

- Emergency medical data (medic alerts, allergies, drug reactions).

- Electronic prescriptions may be issued by doctors to a patient’s smartcard (though probably in summary form rather than in their entirety) and thus conveyed to dispensaries.

---

7 It is noteworthy that smartcards can support several different e-prescription architectures. One option is for a script to be written to the smartcard more or less in its entirety, and carried in that form to the dispensary. In this case, the smartcard acts as a direct replacement for the paper script. For disaster recovery and usability reasons, a copy of the script would typically be saved in the back-end somewhere. Given that reality, alternative e-prescription architectures save relatively little data on the smartcard and instead use the card as a key to access the script from a repository, and to prove the cardholder’s legitimacy and entitlements. Various e-prescription implementations are now using smartcards in Austria, Germany and Taiwan.
10.10 Campus cards

- All-purpose multi-function student ID card, containing a variety of applications such as electronic purse (for vending and laundry machines), library card, record attendance at classes, concession card and logical access control for network logon

- Similar multi-function cards have been deployed for employees at large commercial businesses, for access control and cafeteria use
11  Developing the business case for smartcard deployments

This section summarises issues an agency should address and/or consider when developing a business case for a smartcard deployment. The Project Design Guide will assist agencies with many of the issues that will arise when designing and implementing a smartcard deployment.

Agencies should bear in mind that before starting to develop a smartcard business case, a detailed risk analysis, based on the NeAF, should be undertaken to determine whether a smartcard is the appropriate technology for the proposed applications.

Each Australian jurisdiction should develop its own business case methodology to use when developing smartcard deployments.

11.1  What is a business case?

A business case provides the basis for taking an informed decision on whether to proceed with a new initiative or proposal. It defines the scope of the project, outlines the costs, benefits, budget and timeframes for delivery.

A business case should provide:

• an outline of the business requirements

• a concise statement of the benefits of implementing a smartcard program for service delivery for government, business, the community and individuals

• an outline of important background issues that contextualise the investment

• an outline of how the investment aligns with whole-of-government and/or agency policy

• an evaluation of viable alternative options for delivering the desired outcome

• details of the expected impacts on all stakeholders

• a robust estimate of whole-of-life costs of the investment

• a robust estimate of financial benefits of the investment

• an estimate of non-financial benefits of the investment

• a rigorous assessment of inherent risks, including how they are likely to impact on the investment and strategies for mitigating them

• an evaluation of the likely extent and cost of business process changes needed to realise the full benefits of introducing smartcards (and indeed to avoid project disappointments) including:
- designing, planning and introducing new positions, policies and processes required for issuing and managing smartcard and any associated applications; and

- eliminating old positions, policies and processes rendered unnecessary by smartcard migration processes required from legacy applications; and

• an indicative implementation schedule, timeframe and resourcing plan.
12 When should agencies consider implementing smartcards?

The salient characteristics of a smartcard deployment that can help evaluate the practicality and potential business benefits of this new technology for agencies are discussed below.

12.1 Specific capability required

Smartcards have specific unique capabilities that other technologies do not provide, including security features that help to thwart identity theft and card fraud.

12.2 Portability

One of the most fundamental smartcard characteristics is its data portability. By adopting smartcards, an agency can maintain data in a form that can be transported to any physical location. The smartcard portability allows data to move with the client between providers. Data on the card can be accessed wherever and whenever it is needed. Privacy can be an important consideration; privacy can be enhanced in some cases when smartcards are used to convey sensitive data, removing it from exposure from back-end systems.

Having said that, a major constraint is imposed by the limited EEPROM capacity of smartcards today. While the EEPROM capacity is continually improving, it comes at a significant price premium. This memory needs to be shared amongst card applications and application data. Furthermore, some important card applications which might not be apparent to the end user (or even the card issuer) can be required to meet underlying technical requirements of standards such as ISO/IEC 24727-3 and FIPS 201, or FIPS 140 Level 3 where applicable. Digital certificates, too, typically require 2 KB or more each. The net result is that the memory remaining available for use by user applications can turn out to be only a very few kilobytes.

Smartcards can provide various levels of security to ensure data integrity. When considering the portability of data, also consider how the data is going to be protected from illicit interception, modification or substitution. Smartcards are designed to address all these concerns.

12.3 Identity authentication/information security

It is becoming increasingly important to verify the identity of the transaction originator and receiver in today’s environment of increased agency use of electronic commerce and/or electronic service delivery, growing use of web-based applications, and the ongoing problem of identify theft.

By providing a mechanism for secure identity authentication (through a variety of means, including symmetric cryptography, digital certificate and/or biometric), the smartcard provides a means for cardholders to identify themselves in cyberspace.

---

8 There are different identification and access control design requirements that can be supported with assistance from smartcards, such as one-to-one, one-to-few and one-to-many. Business rules that pre-determine the appropriate access control checks must be developed at the time the smartcard system is designed, and care taken to analyse the infrastructure that supports access control, including key management rules and the most appropriate form of cryptography to deploy.
In addition, the smartcard’s on-board computing power plus commonplace cryptographic processing allows users to perform active verification of websites to be sure of the identity of the receiver of sensitive transaction data before it is sent.

12.4 Automatic forms population

Most government agencies spend substantial amounts of time processing an abundance of paper forms. Moving to electronic form submission could save significant staff time. The smartcard provides the capability to populate forms with agreed data carried on the card, with privacy parameters reducing the redundant capture of data for government and individuals.

12.5 Multi-application enabler

Because of their basic technical limitations, plastic card platforms have traditionally supported single applications. By leveraging the intelligence associated with smartcards, more than one application can reside on the card platform.

12.6 Updatable applications

Other card technologies entail static applications. Once a card is issued, any changes require traditional plastic cards to be re-issued. Smartcards on the other hand, built on an openly programmable platform, are dynamic and can accept new applications and data structures even after the card has been issued.

12.7 Hybridising card technologies

Smartcard technology need not be implemented in a chip-only device, especially over transitional periods where interim support for legacy card systems might be important; multiple technologies can be hybridised on the one piece of plastic. Hybrid cards are inevitably more expensive on an item-cost basis, but total cost of ownership and deployment may be lower with a hybrid card if back-end and card reader sub-systems can be phased in more gradually, or if a more highly functional single device can take the place of two or more cards. Without trying to be exhaustive, there are two major scenarios that can be worth considering when developing a smartcard concept and business case:

- Chip plus magnetic stripe - deploying a card with both conventional (or legacy) magnetic stripe and a new chip is attractive in such settings as banking and health cards, where not all retail terminal equipment can be swapped over at once (or at a reasonable cost).

- Contact plus contactless interfaces - especially where both physical and logical accesses are desired to be controlled with maximum convenience, a smartcard with two interfaces can deliver net benefits. Elsewhere in the Framework, alternative implementation strategies are discussed, including the hybrid card where two independent chip sub-systems are packaged in the one card, and the more sophisticated ‘dual interface’ card where the same core processor supports both contact and contactless channels.
12.8 Cost sharing

Agencies have the potential to experience substantial economies of scale when implementing multi-programmable cards. Rather than have each program pay for card issuance, management and customer service, multiple programs can share these fixed costs. The cost of the applications residing on the chip card platform can also be shared among the programs using the application. Although smartcards themselves are more expensive than other types of cards, the total implementation cost can potentially be reducing through multiple applications or shared services.