



Australian Government

Department of Finance and Deregulation

Australian Government Information Management Office

National Smartcard Framework



December 2008

Case Studies

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	Transit Industry Case Study - Transit smartcards for Automatic Fare Collection	5
2.1	Project overview and background	5
2.2	Operating environment	7
	2.2.1 Business Environment	7
	2.2.2 Legal Environment	8
2.3	Technical Environment	9
	2.3.1 Interoperability	10
	2.3.2 Application description	11
2.4	Implementation overview	12
2.5	Program management and support	13
2.6	Cost/benefit analysis	14
2.7	Lessons learned and recommendations	15
2.8	Sources and references	17
3	Health Industry Case study – Multifunction smart ID badge for Hospital Staff in Australia	18
3.1	Project overview and background	18
3.2	Operating environment	18
	3.2.1 End-user characteristics	18
	3.2.2 Legal characteristics	19
	3.2.3 Business	20
3.3	Technical environment	21
3.4	Application description	22
3.5	Implementation overview	21

3.6	Program management and support	21
3.7	Cost/benefits analysis	22
3.8	Lessons learned and recommendations	23
3.9	Sources and references	23
4	Government Case study – Common Access Card for US Bureau of Land Management	24
4.1	Project overview and background	24
4.2	Operating environment	24
4.2.1	End-user characteristics	24
4.2.2	Legal characteristics	24
4.2.3	Business	26
4.3	Technical environment	26
4.4	Application description	26
4.5	Implementation overview	27
4.6	Program management and support	28
4.7	Cost/benefits analysis	28
4.8	Lessons learned and recommendations	29
4.9	Sources and references	29
5	Telecommunications Industry Case Study – Telephone card developments	30
5.1	Project overview and background	30
5.1.1	Phone cards	30
5.1.2	Mobile phone smartcards	30
5.2	Operating environment	30
5.3	Application description	32
5.3.1	Phone cards	33
5.3.2	Mobile phone smartcards	33

5.3.3	Mobile payment solutions	33
5.3.4	Non-Payment solutions	34
5.4	Implementation overview	35
5.4.1	Phone cards	36
5.4.2	Mobile phone smartcards	36
5.5	Program management and support	38
5.5.1	Phone cards	38
5.5.2	Mobile phone smartcards	38
5.6	Cost/benefits analysis	38
5.7	Lessons learned and recommendations	39
5.8	Sources and references	39

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 Framework sets out the vision, principles and concepts appropriate to smartcard implementations by government agencies.

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

- Smartcard Handbook
- Implementation Models and Checklists
- Smartcard Project Design Guide
- Case Studies (this document); 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 online at <http://www.finance.gov.au/e-government/>

This document provides an overview of representative domestic and international smartcard deployments. While it does not cover all possible smartcard uses, it provides an author preparing a business case with an insight into previous deployments. It includes smartcard deployments from the following industry sectors:

- Finance
- Transit
- Health
- Government; and
- Telecommunications

2 Transit Industry Case Study - Transit smartcards for Automatic Fare Collection

2.1 Project overview and background

Transit smartcards for Automatic Fare Collection (AFC) were introduced in the 1990s with the advent of a viable proximity radio frequency contactless interface operating at 13.56MHz. The most notable early pioneer in the area was an Austrian Company called Mikron, later to be taken over by Philips, with cards released under the 'Mifare' brand name. Initial take-up was primarily by smaller regional operators in the UK and continental Europe, but many transport agencies quickly saw the opportunity to usher in a radical improvement to existing paper and magnetic stripe ticketing arrangements.

Transit smartcard schemes illustrate examples of smartcard deployments in terms of:

- large numbers of cards issued
- large card transaction volumes
- stakeholder diversity
- complexity of business rules
- complexity of technical infrastructure
- range of operating environments
- security and fraud mitigation challenges and strategies
- potential impacts of deficiencies in system performance and availability on customer satisfaction, service delivery and even safety
- post-issuance application extensions; and
- governance challenges.

Contemporary transit smartcard schemes are based on cards with a proximity radio interface, generally but not universally compliant with ISO-14443, and in some cases supplemented by the traditional ISO-7816 contact set.

There are numerous contactless transit smartcard schemes either in operation or in the planning stage around the globe. Major success stories include the Octopus Card in Hong Kong, Transitlink in Singapore, the Oyster card in London, the VRR/VRS 'Baren' cards in the German Rhineland, Translink in San Francisco and significant schemes in Rome and Seoul.

The transit smartcard most often cited as a leading example is Octopus Cards Ltd in Hong Kong. Originally built around a consortium of public sector and private transport operators (now all

privately owned), this scheme acquires over 30 million transport and retail transactions per day across a base of 13 million issued cards, over half of which are in regular use.

The case study information below is an amalgamation of information from a number of implementations, all of which have many common facets, but each of which also has unique characteristics.

Table 1 below provides some statistics on some current and planned transit smartcard schemes.

Location	Project	Card Interface Type	Sectors Targeted	Initial Contract Value	Cards Issued To Dec 2006	Txns. per day
Hong Kong	Octopus	C	Trains, buses, ferries, trams, retail, parking meters, parking stations	A\$250M+	13M	30M
Rome	Atac/Cotral Metrebus	Dual Type B + Contact	Trains, buses, trams, parking meters	A\$350M	500K	4M
Singapore	EZ-Link	C	Bus, rail, retail	A\$200M	9M	4M+
San Francisco	TransLink	B	Heavy rail, light rail, bus, ferry and trolley buses	A\$225M	> 1M	Not available
Sydney	Tcard	A	Trains, buses, ferries, light rail	A\$360M	250K+ (students)	Not available
Brisbane	Translink	A	Rail, bus, other	A\$175M	< 500	Not available
Melbourne	MyKi	A	Rail, bus, retail	A\$200M	0	Not available
Perth	SmartRider	A	Rail, bus	A\$30M	450K	>100K
Rhineland	VRR/VRS	Dual Type B + Contact	Rail, bus	Not available	6M	Not available
London	Oyster	A	Rail, bus, retail	A\$400M	5M	2M+
Washington	Wamata SmartTrip	Cubic proprietary	Rail, bus parking	A\$250M	2.2M	500K
Seoul	T-Money	C	Rail, bus parking, retail	Not available	5M	500K

Table 1: Comparative Transit Scheme Statistics

2.2 Operating environment

2.2.1 Business Environment

Globally, public transport is a complex and costly endeavour involving massive infrastructure investment in rolling stock, physical infrastructure (carriageways, stations, terminuses, ferry wharves, etc), front end ticket sales points and equipment, and customer services, and back-end logistics, administration and customer support. The ownership mix has changed over the years, but in most jurisdictions there is significant public and private sector investment, with governments funding and operating services that by their nature are unprofitable or too capital intensive for private industry. Whatever the ownership model, the incentive to reduce costs and improve efficiencies is universal and compelling.

The services offered by transport providers are delivered to the public in various forms including distance, time and zone-based products. Concessions are a significant factor in most schemes.

At a transaction level, public transport hinges on the efficient collection of large volumes of low value fares. In pre-smartcard systems, paper and magnetic stripe tickets and passes have been (and remain) the primary credential for the right to travel on a given service. The introduction of smartcards represents a logical step in the evolution and integration of ticketing practices, with the detailed rationale for smartcard introduction including the:

- replacement of failure-prone magnetic ticket technology with a more reliable smartcard technology
- reduction in system operating costs through automation of manual business processes
- integration of formerly disparate ticketing practices across modes, cities or regions, improving the commuter convenience and the attraction of using public transport as compared to private transport
- improvement in passenger throughput in high-demand locations, especially railway gates or tripods in closed systems
- potential simplification of fare structures using a common purse
- reduction of fraud in areas such as cash handling and fare evasion
- provision of better delivery of concessional travel arrangements, and provision of better concession usage feedback to the responsible government agency
- addition of new services, including cashless low value retail payments at convenience stores
- achievement of interoperability between private and public service providers
- improvement of on-line services (such as web-based account management) to travellers; and
- removal of the need to queue at ticket office windows or machines by providing secure automatic purse or product load services.

The major stakeholder participants in transit card schemes typically include:

- scheme owner and operator (the card issuer)
- transport service providers covering all modalities including rail, bus and ferry
- cardholders
- retail merchants providing card load-agent services and cash-replacement convenience purchases; and
- in some cases, various public sector and commercial service providers such as campus payment, parking meter and vending machine operations.

While not always adequately acknowledged, the cardholder is a significant stakeholder in transit schemes as the owner of the remaining stored value on their card (more accurately, in their account as represented by their card), as the customer of the transport operators, and sometimes as the owner of the physical card.

Most, if not all current transit smartcard schemes involve close engagement between public and private sector operators. Typically, scheme governance and the majority or all of the initial capital is provided by a public sector agency, with various models to recover either capital or operating costs from private sector operators.

The operational model varies between systems. In some projects, the principal retains responsibility for operational management, while in others, the system builder or a third party is contracted to operate the system either on a fixed fee basis, or a transaction volume or value basis.

2.2.2 Legal Environment

Factors in a transit smartcard scheme legal and regulatory environment include:

- financial regulations covering value flows within the card network, touching on such matters as funds pool management, t-purse value limits and disposal of unclaimed monies (from inactive cards)¹
- consumer law and codes of conduct relating to the use of smartcards as payment instruments, covering matters such as stored value guarantees on lost and stolen cards, refunds, transfers and cardholder dispute resolution
- privacy legislation covering the handling of cardholder personal data, and prevention of misuse of the system for unauthorised tracking of a cardholders' spending or travel behaviour; and
- technical compliance regulations for cards, readers and other equipment, and including the radio frequency aspects of contactless smartcard interfaces.

¹ In order to meet Hong Kong Monetary Authority regulations, Octopus Cards were in fact obliged to acquire a banking license

2.3 Technical Environment

The business and technical topology of transit smartcard schemes typically involves functional and physical environments such as:

- closed railway stations with gates or tripod barriers actuated by the smartcard
- open railway stations with card readers located at entry and exit points
- buses, and trams with readers located at doors
- ferries with either on-board or wharf-based readers
- attended ticket offices and service points where card load, inquiry and general administrative transactions may be performed
- unattended add-value machines, mostly located within railway station or other transportation hub precincts
- retail counters at merchant locations offering either card load services or convenience payments using an electronic purse
- depots and station computer localities providing data aggregation and local reader control functions
- a secure back-end system providing transaction acquiring, data storage and accounting functions
- operational centres of various kinds providing cardholder support, operator support and network configuration services
- card issuance facilities; and
- the card issuer corporate environment where administrative and governance functions are located.

Finally, transit smartcard systems operate in a threat environment that is not dissimilar to that applied to the bankcard industry, with the primary risk being that of financial fraud. Key elements of this threat environment include:

- the potential for theft of cash wherever it is exchanged for stored value within the system
- card substitution fraud where add-value or payment terminal operators swap cards to their own advantage and the detriment of the legitimate cardholder
- unauthorised or improper use of add-value equipment
- the fraudulent use of lost and stolen cards
- the manipulation of back-end processes for financial gain; and
- hacking attempts against web-based interfaces and services.

2.3.1 Interoperability

Various inter-issuer interoperability initiatives have emerged around the globe, with varying success. In the UK, the ITSO Organisation² has promulgated a set of industry-based standards which are being adopted by most operators, and bringing, at least in principle, both card and reader interoperability. In practice, the ITSO Organisation designs result in technical, performance and cost issues associated with the interoperability overheads, and these have impeded the adoption of ITSO practices by some operators and also in other countries.

In France, the Calypso scheme has been promoted as a potential interoperability candidate, however its lack of technical sophistication has prevented its uptake.

The European Committee for Standardisation (CEN) is developing a standard for interoperability of data elements to be stored in travel credentials, including limited security features. Dublin (Ireland) appears to be alone in trying to adopt the standard for use on contactless smartcards.

In Asia, home to most of the largest transit smartcard schemes to date, there is effectively no interoperability between different card issuers or equipment platforms.

In Australia, while Perth, Sydney, Brisbane and Melbourne have each selected the same card interface, there is no immediate prospect of achieving smartcard data, reader or back-end inter-issuer interoperability. Efforts by the National Ticketing and Tolling Working Group (NTTWG) and Standards Australia are effectively on hold while each city rolls out its own vendor-specific implementation.

2.3.2 Application description

Transit smartcards are based on contactless smartcards carrying one or more applications. Generally there is a primary transit application comprising transit purse and 'product' areas, and sometimes additional applications such as an operator application providing access control and other functions to service provider staff members.

Combination/dual contactless and contact cards are sometimes used, with the contact set used for add-value operations at dedicated machines. Most schemes have found no need, either practical or security, to provide single interface contact cards.

Products loaded to transit cards include time-limited travel passes, or special travel data sets specific to particular operators. These products tend to be less interoperable than that of the transit purse.

Cardholders are allowed to load value to a predefined limit (typically in the range A\$200-\$1000). Debit transactions are made according to business rules calculated at the reader or attached host. For convenience, many transit purses permit a negative balance that may arise when a passenger alights at a destination for which the fare exceeds any reserve value deducted when they entered the system. Negative balances are not permitted against retail transactions.

² ITSO Organisation used to be called Integrated Transport Smartcards Organisation. ITSO is now the name of the organisation and is no longer used as an abbreviation

Schemes operating on distance or zone-based journeys require the cardholder to tag-on at the start of their journey, and tag-off at the end. Failure to tag-off normally results in the forfeit of an amount equivalent to the maximum fare, although exception processing rules and dispensations vary from system to system.

Inspectors in transit smartcard schemes use portable reader devices to check the legitimacy of the card and journey.

With the exception of special purse increment and decrement functions, transit applications are implemented as a set of on-card files manipulated by the reader after mutual authentication. Transit cards operate on relatively small data sets, but the business rules operating on those at the reader or terminal may be very complicated, including distance, time and loyalty calculations as well as measures to prevent fare evasion. The look-up time or calculation time for transactions at high-throughput locations (e.g. rail gates) is a significant problem for the industry.

Transit fare payment schemes can be implemented on cards having as little as 1KB of available file memory, but most schemes use cards with a memory in the range 2KB to 8KB.

Cards may be issued in a number of types as designated by their colour scheme and the electronic data encoded in the chip. Card types include child and adult anonymous cards, as well as personalised forms of both. Special concession cards may also be issued.

Most schemes offer a card registration service, after the completion of which a cardholder may have the card placed in the system hotlist if it is lost or stolen. Most schemes will refund or transfer the remaining value on cards after sufficient time has been allowed for the hotlists to reach all critical system nodes.

If a hotlisted card is presented to a reader, the card is normally blocked by setting a special flag in memory, after which the hotlist entry is removed. Blocked cards will be rejected by all readers in the system.

A key feature of most transit card systems is that readers are fully or partly offline to the central system during revenue usage, with transactions being posted in batch mode to back-end accounts. Special key management and anti-fraud measures are used to mitigate the risks arising from not having on-line authentication.

Transit readers typically, but not always, are fitted with security modules to protect the card access keys, and for performance reasons run-time authentication is almost universally based on symmetric key methods, often using retail banking algorithms.

Transaction acquiring normally uses intermediate data aggregation nodes at stations, bus depots or other locations, these in turn connecting to lower-tier cluster of readers, and to the central system.

At the centre of transit smartcard schemes is a back-end clearing house or bureau which provides issuer and stakeholder services including:

- transaction acquiring
- transaction sorting, switching and clearing

- accounting and reconciliation functions
- bulk settlement between participants and purse funds management over bank interfaces
- reporting and monitoring services
- reader management; and
- key management.

The clearing house is usually supplemented by a disaster recovery centre.

Both back and front-office cardholder support services are normally provided. Back-office support will include a cardholder call centre, dispute management, ad-hoc card issuance and other administrative functions. Walk-in centres may offer a comparable set of services, and include on-the-spot card replacement and sales.

Depending on the scheme, bulk card issuance is either outsourced or performed in-house.

2.4 Implementation overview

Transit smartcard systems typically spend a great deal of time in gestation and deployment. It is rare for a scheme to proceed from commencement to full production in less than three years, and five years is quite typical. This timescale is accounted for by many factors including the:

- sheer scope and complexity of the technical infrastructure and business rules found in public transport
- frequent need for customised hardware and software development to implement specific stakeholder requirements
- software and communications protocol complexities of integrating legacy equipment; and
- site planning and works needed to effect the schemes.

Few, if any transit schemes have met their original timescales, and similarly, few roll out within the original budget. To date, scheme owners have tended to significantly under-estimate the work involved, or are driven by unrealistic timescales imposed on them from other quarters.

A very clear message from transit to smartcard adopters is that the smartcard itself is actually a very small component in a very large undertaking. While the card is the most conspicuous aspect of the scheme in the public perception, the benefits of smartcards over the media which they replace can only be fully realised with:

- the deployment of well engineered readers
- close attention to business process and customer usage changes

- an improved customer service infrastructure to handle the new complexities arising from the card; and
- an enhanced security architecture to take advantage of the smartcard security features and changes to governance practices in line with potentially higher risks associated with significant stored value circulations and the introduction of computer interfaces that may be subject to a whole new range of threats.

2.5 Program management and support

There are many roles within a transit smartcard deployment, including:

- government and private sector principals as scheme owners, governors and card issuers
- transport service providers as stakeholders and having responsibility for readers and depot or station computer infrastructure
- cardholders
- network, computer and card reader technology suppliers
- card chip vendors
- card assemblers who embed the card chip modules into plastic carriers, and in some cases perform base colour stock printing
- card bulk initialisation and distribution facility operators
- card system operators, responsible for managing the back-end systems including such areas as system configuration, transaction acquiring, reader management, and key management
- systems integrators and site surveyors
- card load agents and service point operators
- third party service suppliers (for example call centres)
- banks which provide account, settlement and EFT facilities
- third party participants including retail merchants; and
- systems and reader maintenance agencies and facilities.

There is no one approach to ownership or execution of these various roles and responsibilities. Each scheme is established according to its own cost-benefit, risk and funding model. However common themes are:

- scheme governance, issuance and security management responsibility normally resides with the system principal

- technical and other services can successfully be subcontracted out to specialist organisations, but there are schemes which adequately address these requirements without doing so
- no one principal or contractor can embody all the knowledge or expertise needed to design, build and operate projects of this scale: strategic use of outside expertise is an important contributor to a scheme's success; and
- clear delineation must be kept between issuance functions and the functions of the major stakeholders or other parties within the program. Questions such as data ownership, back-end access and appropriate functionality must be decided early in the system design.

2.6 Cost/benefit analysis

Transit smartcard operators do not normally publish cost-benefit analyses, but some information is available from outside observation.

Few schemes are designed to return a direct profit to the scheme owner. The key drivers tend to be a reduction in costs in existing systems, and the delivery of improved services including better public transport system integration, or improvements to concessional travel provision.

A reduction in fraudulent travel may also be the target of a card deployment, both because of the anti-counterfeiting measures available from the card and through closure³ of existing open systems.

Over time, additional commercial opportunities may be sought, allowing the card issuer to leverage its large cardholder base to obtain a further return on investment. Typically this means extending the transit purse into the retail payments sector, allowing advertising, or entering into co-branding arrangements. Once transit usage reaches saturation as it has in places like Hong Kong, the only way for the business to grow is for non-transit applications to be found.

Most transit card schemes operate with high costs but a low fee structure. This tends to act as a brake on new technology deployment in the core business, and as a catalyst for new and more profitable conjoint applications in the retail sector.

To date, few transit smartcard systems contractors have achieved good returns from their involvement. Under-bidding at tender time, gaps in specifications for which no contingency provisions have been made, technology glitches and operator deployment delays have all contributed to poor revenues.

However for issuers, transit smartcard schemes have generally been an outstanding success, delivering significant benefits to the travelling public in convenience and functionality and to the transport operators in fare payment system operating cost reduction, and an increase in patronage.

³ In closed systems, commuters are forced to present tickets or cards on entering and leaving the system

2.7 Lessons learned and recommendations

Transit smartcard scheme operators have been world pioneers in large scale smartcard technology deployments. While their systems do not always reflect the latest advances (one good example is the absence of PKI usage), they probably reflect the greatest diversity of operating environments and challenges yet found in the smartcard domain.

The primary lesson from the transit domain is that smartcards can deliver convenience, flexibility, security and a reduction in operating costs, although early adopters have faced many challenges in pioneering the transition to the new technology.

Of all the issues facing transit card system developers, the integration of legacy systems has proven to be most problematic. In numerous cases, partly due to intellectual property issues, older technology communications and business logic interfaces have had to be 'reverse engineered', and old processes redesigned. The additional transaction and business data that accompanies the new smartcard technology also presents assimilation challenges to existing back-end systems.

Some other lessons that emerge from the ten or so years since smartcards entered the 'automatic fare collection' industry in a substantial way include the following.

- Contactless cards can deliver a highly secure and reliable service to a large and varied cardholder constituency
- Simple is better: complicated schemes, or schemes suffering function creep suffer the consequences in budget and timeline blow-outs
- Principals and contractors alike tend to underestimate the time and budget needed to get large schemes off the ground
- Imposing some level of cardholder investment in the card (ownership or a deposit) has proved important in containing recurring costs. Where there is no financial incentive to look after the card, card damage and loss statistics escalate
- Industry, national and international standards are important to system design, but it may be infeasible to bring every aspect of the system under such an umbrella. Having all elements of the system standardised is also not the only recipe for success. For example, the Octopus Card is based on a non-standardised contactless technology which at the time of its adoption, offered superior performance to any other card chip and reader technology. As a general rule, card system developers should endeavour to use standards wherever they make practical sense, but recognise that they may not fill all gaps in system design
- Stakeholder engagement and management is critical to scheme success and must start well before tenders are released; and
- Most fraud against transit smartcard systems is opportunistic, involving deceit and outright theft – there have been no published reports of sophisticated technical attacks against these systems despite the relatively low security of early cards.

- Security design for card systems should not be treated as an add-on or afterthought: it is an integral part of all aspects of a robust card system and must be considered at all levels of policy, business, technical and operational design
- Integration of COTS products into card schemes, especially but not only where internet connections are used, may introduce security vulnerabilities which may be difficult to address in an integrated manner. Most transit card schemes currently consist of a core security system protecting add-value, payment transaction and reader configuration traffic, and an overlay of commercial VPN and ad-hoc methods to protect TCP/IP and general communications traffic.
- ‘Card not present’ transactions such as those over the internet to the central system present the same types of risks that confront internet banking, and considerable care is needed in the design of the authentication processes
- Integration of legacy equipment can be a major stumbling block and must be given adequate attention from the moment a new card project is conceived
- Adequate cardholder support must be supplied from the first day cards are deployed
- Contactless card adopters must be aware of the likelihood of slow transactions or business logic problems when more than one card enters the RF field (for example, if a cardholder has two in a wallet), or where the reader must deal with more than one modulation scheme. Cardholder education is needed to deal with the first problem, and in the second case, it is highly preferable to choose a single modulation scheme
- The actual cost of the card may be a small part of overall issuance and management costs, and card managers should not therefore focus on card price to the exclusion of other potentially much larger cost factors
- Interoperability with other card issuers’ systems requires the resolution of many detailed technical design issues and should not be treated as a simple undertaking
- Card issuers must properly address the question of the fallback procedures to be used when cards fail upon presentation to readers; and
- Additional applications added to cards often have low utility and a marginal business case. Cardholder interest in optional uses may also be lacklustre. Card scheme developers must not forget that the potential cardholding population is now accustomed to technologies with a functionality and storage capacity that far exceeds that available on a smartcard. Hence the interest in technologies like Near Field Communications that integrate the smartcard chip into mobile devices, especially phones, thus combining the benefits of each technology in a single package.

2.8 Sources and references

Web sites carrying information on some of the transit schemes mentioned in this case study are given below. For further information on the:

- Hong Kong Octopus transit smartcard scheme, refer to: <http://www.octopuscards.com>
- Singapore transit smartcard scheme, refer to: <http://www.ezlink.com.sg/index.html>
- Sydney Tcard transit smartcard scheme, refer to: <http://www.tcard.com.au/tcardweb/>

THREE HEALTH INDUSTRY CASE STUDY

3 Health Industry Case study – Multifunction smart ID badge for Hospital Staff in Australia

The name of the institution is suppressed for confidentiality reasons.

3.1 Project overview and background

Staff identification has been a major issue at hospitals and healthcare institutions. Healthcare workers occupy special positions of trust and are subject to strict codes of professional conduct according to their roles, as well as conditions of employment. Photographic ID badges are therefore an accepted aspect of working in healthcare. Yet hospitals are extraordinarily dynamic working environments. Staff turnover is high and itinerant staff – especially agency nurses and locums – are commonplace. In-person visual verification of a photo ID is rarely practicable, and moreover, as healthcare comes to use more and more information technology, electronic verification of identity and credentials is becoming more complex and important to ensure that credentials are managed effectively.

This case study provides illustrations of smartcard deployments in terms of:

- smartcards supporting multiple functions (ID badge and online access to medical files)
- smartcards issued to professional staff in a dynamic environment
- high staff turnover
- multiplicity of business drivers
- complexity of technical infrastructure; and
- large potential impacts of deficiencies in system performance and availability on customer safety and health.

In at least one major hospital, staff ID badges are being migrated to in-house personalised smartcards, providing a powerful and extensible basket of identity management functions in one convenient package. The business case for the hospital in question was incorporated into an already-funded technology refresh program in one specialist ward, where new workstations and software applications were introduced to improve bedside patient management. However, the chosen card platform enables a set of upgrade paths, including integration with building access control, and compatibility with emerging state and national e-health programs.

3.2 Operating environment

3.2.1 End-user characteristics

The hospital smartcard project began with nurses working in one specialist ward. Funding had previously been secured for the implementation of bedside workstations and clinical record management software applications. Nurses in this environment are reasonably accustomed to

new technology and are well supported by training courses – which they regularly attend as part of their continuing education professional obligations.

Perhaps paradoxically given the safety criticality of hospital wards, nurses in these environments are relatively insensitive to computer usability. In a typical day they will use dozens of quite different pieces of medical equipment, and therefore have to cope with idiosyncratic user interfaces. This fact does not diminish the importance of good software design, but it does mean that end-users are more amenable to understanding new ways of working.

A particular issue that was faced at this hospital was the usability of passwords and contact smartcard readers. Security policy dictated that nurses' smart ID badges would be PIN-protected. It was thought that having to insert a smartcard at a workstation and enter a password at a keyboard would be inconvenient, but user acceptance testing in fact has shown that the smartcard is well liked. Small adjustments have been made to improve usability; for example, cards are hooked onto the end of elastic lanyards hung around the neck. In the longer term, contactless smartcards may be an attractive upgrade option. But even with a less-than-ideal user interface, the tangible benefits of smartcards far outweigh their impact on the workplace (see Applications below).

3.2.2 Legal characteristics

The primary legal context for the use of any ID technology in a hospital is the employment contract between the hospital and its staff. Terms and conditions for use of a smartcard – when it enables new functionality such as access to IT systems, and so brings new responsibilities – are easily folded into amended workplace contracts. At a high level, these terms and conditions are not dissimilar to those of a banking card, and focus on the need to safeguard one's PIN and to report lost and stolen cards promptly.

In the medium term, the hospital plans to augment its staff cards with digital certificates (see Applications below). These may eventually be used for transactions outside the hospital. Recent reforms to the Australian Government's Gatekeeper PKI Framework facilitate a flexible approach to administering digital certificates in a "Special Purpose" context. It does not appear that the Gatekeeper regime in itself will impose any additional regulatory burden on the use of the hospital's smartcards for transactions, over and above the sorts of conventional threat and risk assessment that would be undertaken as a matter of course when deploying new IT security systems.

In respect of privacy protection and compliance with privacy regulations, this project posed no particular challenges. The use of smartcards for staff identification and the management of digital credentials for medical professionals does not negatively impact the way that sensitive patient information is handled. Arguably, patient confidentiality will be enhanced in the long term by this application of smartcard technology because access to electronic records will be better controlled. The privacy of healthcare professionals within the local system is not a *prima facie* concern as full transparency of their conduct in the workplace (at least on a need to know basis) is implicit in their roles and responsibilities. Therefore, a Privacy Impact Assessment (PIA) was adjudged to not be necessary in the deployment of smartcards to these particular healthcare professionals.

Australian legal requirements may vary from the case studies and should be considered when reading the information on legal characteristics.

3.2.3 Business

The business environment of most large public hospitals has for many years embraced new technology. In and of itself, the role of high technology in healthcare remains controversial, and investment decisions are not made lightly. Nevertheless, significant budget allocations are routinely made for health information systems. There is a rich market for clinical software systems and in some hospitals, major systems are developed in-house in response to leading edge clinical demand drivers that have yet to be manifest by commercial vendors.

In this context, the hospital in question had over time established a well funded and well planned technology refresh programme. Smartcards for controlling nurses' access to in-ward patient information systems were factored in as part of a business case for new software and workstation hardware specially selected for the needs of the speciality area concerned.

3.3 Technical environment

The technology refresh gave the hospital the opportunity to standardise on a client-server workstation platform specially suited to the ward environment. Smartcard readers came as standard, built into the terminal equipment. The software platform was UNIX, with a mixture of specialist vendor and in-house developed applications. IT support was delivered by an array of expertise sourced from inside the clinical department, the hospital's IT department, and from local contractors with special knowledge of certain sub-systems.

3.4 Application description

The "headline" application around which the ward rollout was based was patient electronic medical records (EMR). When admitted for the first time to this ward, a new record is created for each patient, partly populated with data drawn from other systems such as the hospital-wide admissions system. Test results and progress notes are entered into each patient's record during their stay in the ward, with specific data components exported to other systems as need be. If a particular patient is re-admitted in future to the ward, their entire longitudinal record is recovered and updated.

The qualitative and quantitative benefits of these sorts of EMR and the closely related concept of more global shared electronic health records (SEHRs) are well documented. They include better clinical outcomes as a result of better availability and completeness of data to healthcare providers, greatly reduced costs associated with repeat tests which otherwise have to be ordered by providers when they don't have access to the complete record, time savings when healthcare team members interact with patients because they don't need to re-construct the person's history, and more efficient administration of the public health budget through accurate measurement of pharmaceutical benefits and so on.

This hospital's longer term objectives for transaction applications enabled by the smartcards (when cards are issued to the broader healthcare team) include electronic discharge notification to GPs, electronic prescribing, electronic pathology test order entry, and secure point-to-point communications between doctors both inside and outside the hospital. Physical access control (using dual interface cards) is also on the planning agenda.

Smartcards are deemed critical to these longer term applications by management (and lawyers), because of the need for reliable individual authentication of staff members when they act on behalf of the hospital. Smartcards enabled convergence of photo ID, building access and logical access.

3.5 Implementation overview

The clinical head of the ward concerned and the hospital CIO shared business ownership of the smartcard rollout. This arrangement also delivered some improved budget and resourcing flexibility as development proceeded and unanticipated costs were occasionally encountered.

Critically, there was close collaboration with end-users (notably the ward nurses) at all times during design. Redundant (paper-based) systems were always on hand during testing and rollout⁴.

Project planning was generally tied to visible milestones relating to clinical information system rollout and the technology refresh. Smartcards were viewed as a means to an end; project success at each stage was always judged on the basis of demonstrably enhanced patient care and ward workflow.

One special exception process that had to be developed was for the issuance of temporary cards to agency nurses and to staff who have left their smartcard at home. While some additional overhead was experienced in creating and maintaining this extra function, immediate business benefits were seen by way of vastly better management of outgoing agency nurses, through electronic revocation of rights and privileges, and automatic revocation by setting time limits in the card management system.

3.6 Program management and support

Much of the required technical support was sourced from specialist local companies as well as the new workstation vendor, and was funded by the technology refresh program. This avoided the need to draw too heavily on hospital IT resources, which are already allocated to other tasks and not particularly skilled in smartcards. Nevertheless, important knowledge sharing and skills acquisition was fostered from the bottom-up, by involving the IT department on a steadily increasing basis, while new systems are bedded down.

It was especially important to engage the Human Resources department in new card issuance technology. A desk-top smartcard printing and personalisation workstation was implemented, with partial integration at first to the staff database. Superficially this set-up is similar to any conventional instant (Polaroid or digital) photography badge production system. In the longer term, the system was selected to be compatible with out-sourced digital certificate integration as well.

⁴ The fact is that in hospitals, information systems are always redundant in order to safeguard patients. A paper based fallback is likely to remain for the foreseeable future. The way that hospital work practices inherently have to cope with system failings means that, ironically, they are relatively safe places in which to test new technologies like smartcards

3.7 Cost/benefits analysis

Quantified cost-benefit data is not publicly available. Qualitative benefits and costs include the following.

Benefits (not including the generalised benefits of e-health enabled by the technology).

- Smoother, more accurate handover of patient notes between nurses at end of shift (nurses can use their smartcards to access notes for a given patient at the nurses' station at handover time, rather than at the bedside, with major time-and-motion efficiency gains, this is viewed as highly important in the healthcare shift work situation)
- Better security of access to patient files by nurses; in the longer term, ability to fine-tune access privileges on a need-to-know basis
- Much more secure management of departing staff, and agency nurses in particular, with reliable instant revocation of their access privileges; ability to time-limit privileges for agency staff and locums at the time their temporary card is personalised
- Better auditability of who did/accessed what and when.
- Smartcards selected to enable addition of externally issued digital credentials such as that envisaged by the National Provider Directory project
- Ready compatibility with e-health transaction programmes
- Upgrade path to a single access mechanism for physical facilities; and
- Longer term upgrade path to control access to special physical assets like restricted drug cupboards.

Costs (Not including the baseline hardware and software costs entailed by the technology refresh).

- Smartcard readers (however, incremental cost of readers is reduced and shifted to capital acquisition budget by procuring workstations with integrated readers)
- Application enablement was probably the major cost, including the need for specialist software contractors to modify in-house code, and the research and acquisition of smartcard middleware and toolkits
- Smartcard personalisation workstation for HR is several thousand dollars more expensive than a conventional passive photo badge printer
- Smartcard technical skills acquisition for in-house software developers (with an associated opportunity cost relating to the fact that these individuals were necessarily diverted from other in-house projects while they up-skilled on smartcards and PKI)
- A degree of process design plus legal review was entailed, especially around modifications to employment contracts to include responsibilities for safeguarding one's smartcard; and

- End-user training (though not a large incremental cost given the frequency of regular clinical staff training).

3.8 Lessons learned and recommendations

- By implementing smartcards for the first time in a high tech environment, where end-users are more accustomed to change, a high profile beachhead is created, from where the penetration of smartcards across the organisation is made much smoother
- The high tech first stage environment also more readily supports piloting and “sand boxing” of new tools, sub-systems and applications
- There were indications that end-users adapt to the smartcard-plus-PIN logon method rather faster than some had feared, especially when the benefits are tangible, with respect to speed of access and richness of online functionality enabled by cards; and
- The incidence of leaving one’s smartcard at home was remarkably low. Only one instance was reported over six months involving at least 20 users daily. This is simply due to the ingrained habits of this particular workforce in respect of carrying photo ID badges.

3.9 Sources and references

National Health (Pharmaceutical Benefits) Amendment Regulations 2006 (No. 2) (SLI No. 200 of 2006) Explanatory Statement; Select Legislative Instrument 2006 No. 200; available at <http://www.austlii.edu.au>

4 Government Case study – Common Access Card for US Bureau of Land Management

4.1 Project overview and background

The United States Bureau of Land Management (BLM), within the Department of the Interior, was a pioneer of smartcards and associated PKI services in the federal administration's emerging Shared Services Provision (SSP) framework. Beginning in 2000 with a simple smartcard identity pilot, the BLM undertook a staged rollout of logical access, integrated credentialing and finally electronic forms functions, all the while focussing on reducing cost and improving business process efficiency. The BLM's primary measurable objectives were to improve logical security and reduce cost of managing user names and passwords. The outcome has been a fully integrated, enterprise-level staff smartcard provisioning service, logical access control and document authentication service, integrated with a commercial PKI service provider, and deployed across the bureau's offices nationwide.

This case study provides illustrations of smartcard deployments in terms of:

- smartcards issued to a large number of staff and contractors across a large geographically dispersed area
- complexity of technical infrastructure; and
- integration with a commercial PKI service provider.

4.2 Operating environment

4.2.1 End-user characteristics

The BLM has 13,000 staff and regular contractors spread across the country. Engaged in a broad range of land resource related services, BLM staff are broadly typical of any modern public service entity. Computerisation is taken for granted; most staff could be regarded as "knowledge workers". A wide range of office automation software is in use, as well as sophisticated technical applications to support the BLM's business.

4.2.2 Legal characteristics

The BLM was guided by the high profile E-Gov Strategy of the US Government Office of Management and Budget (OMB) as well as the OMB Circular A-130 Management of Federal Information Resources. The bureau's legal environment would not be described as particularly different from any other mid size public service enterprise.

Note that in respect of privacy protection and compliance with privacy regulations, this project was considered by the BLM to pose no particular challenges. The use of smartcards for staff identification does not, in and of itself, materially change the nature of workplace privacy issues. As logon authenticators, smartcards can improve the integrity of audit trails that record usage of the

system, and make it harder for unscrupulous staff to take over others' identities or otherwise abuse enterprise resources. Yet for routine network logon by legitimate staff members, including remote logon, smartcards do not create any additional audit information or other records of staff activity compared to regular authentication technology. When used for digitally signing work related electronic transactions, smartcards create a more robust picture of "who did what to whom" but again in respect of regular employee usage, no new tracking of activity results and no new exposure of employee privacy can result.

There is one change to potential workplace surveillance issues that results from an integrated smartcard based physical access control system, and that is the finer grained monitoring of workers' as they move about the workplace. When electronic door controls are introduced, it becomes possible for employers to acquire more information about workers' actual activity, such as lunch breaks, tea breaks, bathroom visits and so on, as opposed to the rather more crude picture provided by simple time and attendance record keeping which tracks just the start and end of the working day. Employers implementing smartcard based physical access control have to bear in mind certain rights and responsibilities in respect of workplace surveillance, depending on their jurisdiction (and depending on what they may or may intend to do with information acquired by their systems).

These are no novel legal challenges, as electronic facilities access control systems, whether based on smartcards or other contactless card technologies, are not new. Nevertheless, it would be prudent for the possibility of automatic surveillance to be spelled out in staff employment terms and conditions and any workplace privacy policy that applies. The necessity for a Privacy Impact Assessment (PIA) needs to be considered on a case by case basis, taking into account whether or not a new smartcard based access control system introduces changes to the way staff activity is recorded. The US eGovernment Act requires agencies to conduct PIAs for relevant projects, however it is not known if PIAs were undertaken for this case.

It should be noted that novel privacy issues would arise from the type of highly integrated multi-function campus-style smartcards where the one device is used for physical and logical access control as well as stored value redeemable at staff canteens and so on. These systems will generate much more detailed audit trails of staff activity and will expose staff to potential surveillance of a new nature. Enterprises considering multi-function staff cards are strongly advised to undertake a detailed PIA in this regard.

With respect to this case study, it is important to understand that the approach taken by BLM with respect to privacy may not be appropriate in Australia. For example, the Office of the Privacy Commissioner's PIA Guidelines states that a PIA should be conducted where personal information is involved. The approach taken may also be in breach of the Office of the Privacy Commissioner's Guidelines on Workplace E-mail Web Browsing and Privacy and privacy and other workplace legislation.

There is some potential similarity between the BLM initiative and the Australian Government's whole of government employee and contractor identity management project, IMAGE, which envisages that a smartcard may be used for identity, physical and logical access. A PIA was conducted on IMAGE in 2006 and a related Privacy Management Strategy is available on Finance's website, at www.finance.gov.au

4.2.3 Business

The end stages of the BLM smartcard project tackled the major issue of forms management. The bureau estimates that it provides around 600 different types of forms to the public, to land resource-related professional users, and to internal staff.

The BLM was able to manage and resource its smartcard development for the most part internally. Some of the smartcard solution was outsourced (in particular, certificate provisioning) but all management responsibility and decision making stayed in-house.

The most noteworthy business feature of the BLM's approach was that they sought no special budget allocation from Federal Treasury. All funding was from internal prior allocations. This meant that their return on investment had to be especially quick, and their business case had to be particularly robust so as not to in effect penalise other projects competing for resources. No remarkably novel technologies were involved; the project has in fact been described internally as 'technologically simple'.

4.3 Technical environment

The BLM workstation environment uniformly runs on Windows XP. This enabled them to leverage Windows GINA⁵ which seamlessly supports smartcard logon.

The BLM has a centralised Active Directory installation for all staff listings; this was readily extended to include a public key certificate repository as the project unfolded. It also facilitated certificate registration by providing a pre-existing user naming schema to guarantee name uniqueness.

The selected common access card solution required vendor middleware to be loaded at client workstations to interact with the smartcard, and to invoke digital signing functions.

A range of external smartcard reader types were deployed, including PCMCIA card readers for laptops predominantly and USB cabled-connected readers for desk tops. However, a high proportion of workstations used keyboards with integrated smartcard readers, thanks to a strategic procurement decision to include such keyboards in all PC purchases. See also Cost-Benefit Analysis below.

4.4 Application description

The initial application for smartcards was end-user authentication at logon. In later stages, digital signature enablement especially of e-forms became the major focus.

⁵ GINA stands for Graphical Identification and Authentication

4.5 Implementation overview

The overall smartcard implementation proceeded gradually over the course of some three years. As experience was gained, the project timelines indicate a clear acceleration in the deployment of steadily more complex functionality in the last 12 months. The timeline was as follows:

2000/01	Pilot investigations of smartcard technology Focus on Identification Issuance
Jan 2002	Approve Business Requirements Analysis
Mar 2002	Approve business case, investment proposal incl. technical requirements
	Start first single office pilot program (Reno, 200 cards)
	Roll lessons learned into systems design alterations
Jul 2002	Conduct user acceptance testing Parallel design of state-wide rollout program Obtain budget approval state-wide rollout
Through 2003	State-wide rollout (Nevada, 1000 cards)
May 2004	Complete security evaluation and other external reviews
Dec 2004	Complete national rollout (13,000 cards)

Little or no bespoke software development was required. Digital signature enablement was handled by COTS additions to the Adobe product suite. The only major technical challenge was to develop a connector for the chosen smartcard management system to interface to a commercial Certification Authority (and the vendors, who in the process appear to have productised this feature so it may be accessed commercially in the future).

Issuance procedures were developed according to bureau security policy (and informed by Federal Bridge CA CP/CPS).

4.6 Program management and support

The bureau assigned a dedicated e-Authentication Project Manager to run the smartcard deployment. The smartcard deployment was based on a centralised Card Management System (CMS) acquired and administered for the entire enterprise. Reasonably high levels of support appear to have been forthcoming from CMS, card and PKI vendors as the BLM was the first agency to come under the purview of the federal Shared Services Provision (SSP) framework.

Note that this visibility enhanced the strategic visibility of the project and would have facilitated external cooperation, but it was not a critical determining factor for BLM. The business case and investment case were made entirely on the merits of the project, based on anticipated cost savings.

4.7 Cost/benefits analysis

The quantitative and qualitative benefits to the bureau can be summarised as:

- simplify the administration of end-user accounts
- reduce help desk burden associated with password resets
- improve mobility of staff and contractors by using one mechanism to access diverse systems (leveraging the way a smartcard can carry multiple user IDs); and
- facilitate high reliability electronic forms via digital signatures.

Total implementation cost was reported to be US\$7M over five years. This investment was to furnish all 13,000 staff and contractors with cards & readers, but more significantly to also re-engineer the BLM's forms management systems. Note that smartcards were budgeted as US\$12/card in early 2004⁶. Major software licenses were concerned with end-user workstation middleware, card management, and digital signature enabled forms management.

The baseline cost for cost-benefit analysis is therefore approximately \$100 per head of staff per annum through the five-year implementation period.

Note that the BLM's procurement policy – to specify keyboards with built-in smartcard readers as part of the bureau's standard PC configuration – helped improve the cost-benefit results for the smartcard project. By accommodating the small marginal cost of special keyboards in the routine procurement spec – and budgeting accordingly in advance – the BLM was able to defray some of the start-up infrastructure cost that would otherwise have been carried by the project.

⁶ Smartcard price at the time was seen to be falling around 50% p.a. driven not only by Moore's Law generally but also by the rapid acceleration in US government-wide smartcard procurement leading to additional economies of scale to be enjoyed by all agencies

Quantified benefit data is not publicly available from the Department of the Interior. However, public statements indicate that the project delivered net benefit to the bureau on the basis of reduced password resets alone.

Furthermore, deeper and more specific payback was enjoyed from transforming the bureau's business processes from paper to electronic forms. A quote in the press from a senior business manager at the BLM suggested they had been able to shut down a warehouse devoted to paper archives and save all the associated "expense and headache".

4.8 Lessons learned and recommendations

- Use procurement policy to help drive the penetration of smartcard readers across the environment; require new workstations to be routinely specified to include built-in readers.
- The more modern operating systems and computing platforms (such as Windows XP) provide useful native support for smartcards, such as logon via Windows GINA. Extrapolating this lesson indicates that Windows Vista will be an important enabler for smartcard integration in the medium term.
- Similarly, in this case the project benefited from the native support for digital certificates featured in its existing Active Directory implementation; and
- Driven by the business side, as a focused cost savings exercise, not as a new technology expenditure.

4.9 Sources and references

- E-Authentication Smartcard – Logical Access Project Plan
http://www.doi.gov/ocio/documentation/logical_project_plan.pdf
- PKI Credentialing System AIMS-Enterprise Card Issuance and Troubleshooting Manual
http://www.doi.gov/ocio/documentation/blm_aims-e_issuance.doc
- "Self funded PKI" in Government Computer News 5 April 2004,
www.gcn.com/print/23_7/25438-1.html

5 Telecommunications Industry Case Study – Telephone card developments

5.1 Project overview and background

The telecommunications (Telco) industry was the first major industry to introduce smartcard technology on a large scale. The first deployments were related to stored value cards (phone cards) and later for mobile (GSM and UMTS) phones.

Telco smartcard schemes illustrate examples of smartcard deployments in terms of:

- being the first industry to implement smartcards on large scale
- large smartcard user base
- large card transaction volumes
- large number of different card readers (phones)
- large number of smartcard manufacturers
- interoperability and standards; and
- pioneering new technologies (e.g. Near Field Communications) and applications (e.g. for micro payments).

5.1.1 Phone cards

The first smartcard⁷ breakthrough was achieved in 1984, when the French PTT (Postal and Telecommunications Services agency) trialled the card as a payment mechanism for public payphones instead of coins. In this field trial, smartcards immediately proved to meet all expectations with regard to high reliability and protection against manipulation.

The integrated circuits typically used in phone cards are relatively small, simple and inexpensive memory chips with specific security logic that allows the card balance to be reduced while providing a high level of security from fraud.

5.1.2 Mobile phone smartcards

Smartcards, which are significantly larger and more complex than memory cards, were first used in large numbers in telecommunications applications, specifically for mobile telecommunications networks.

⁷ Technically, this card was not a smartcard but, as most phone cards are, a memory card

The technology of mobile telecommunications networks is classified by using a generation number. The 'first generation' (abbreviated as '1G') is applied to mobile telecommunication networks with analogue air interfaces. Some typical examples of 1G networks are AMPS and the German C-Netz. Second-generation (2G) systems are mobile telecommunication network with digital data transmission on the air interface.

The two most widely used 2G systems in the world are GSM and CDMA. Functional extensions of GSM, such as the General Packet Radio System (GPRS) and Enhanced Data Rates for GSM and TDMA Evolution (EDGE), which head in the direction of the third generation, are typically referred to as 2.5G systems.

The third generation (3G) also encompasses cellular mobile telecommunication networks with digital air interfaces, but with major extensions to mobile data communications and Internet-compatible services compared with 2G systems. Some typical 3G systems are UMTS and CDMA 2000. Both of these systems are in turn members of the IMT-2000 family.

Because GSM and UMTS are the most visible mobile networks in Australia, only these technologies relevant to smartcards will be described in this case study.

GSM

One GSM characteristic is the usage of the Subscriber Identity Module (SIM). This is a smartcard/ chip that is provided by the mobile network provider and contains a unique key that is used to identify and authenticate each mobile device. The SIM also performs a number of other functions. It allows program execution to be protected against manipulation and it makes it possible to store data such as dialling numbers, short messages and personal configuration settings for the mobile telephone. At the beginning of 1994, there were 1.3 million GSM subscribers worldwide, which has grown to more than 80% of the mobile market world wide in 2006, equalling to more than 2 billion users.

In 2001, WAP (Wireless Application Protocol) was regarded as the long-awaited new Internet technology for mobile telephones. WAP, however, was unable to live up to the expectations for a variety of reasons, including a lack of content and low data transmission rates. The specifications for WAP also included a security module in the mobile phone, called the 'wireless identification module' (WIM)⁸.

UMTS⁹

This mobile telecommunications system is generally known throughout the world as a 3G (third-generation) system, but in Europe it has predominantly come to be known as the Universal Mobile Telecommunication System (UMTS).

⁸ The WIM establishes a reasonably secure communication with applications. Two possible versions of the WIM have been specified: an application in a dedicated smartcard and a supplementary application in a SIM

⁹ This section is based on the Smartcard Handbook, third edition, by Wolfgang Rankl and Wolfgang Effing, John Wiley and Sons, Ltd, 2003

From the smartcard perspective, the greatest difference between GSM and UMTS is that UMTS uses a completely redefined security module called the 'universal subscriber identity module' (USIM). This security module is based on the ISO/IEC 7816 family of standards. It is thus the first such module in the world of smartcards for mobile telecommunications to guarantee compatibility with other smartcards specified in accordance with these standards, such as EMV-2000 compliant smartcards used in electronic payment systems.

The term USIM is also used to refer to the UMTS smartcard as well as the application, although this is not entirely correct. The USIM holds the identity of the subscriber and its primary function is to secure the authenticity of the mobile station with respect to the network and vice versa. Additional functions include executing programs with protection against manipulation (authentication), user identification (using a PIN) and storing data, such as the telephone numbers.

5.2 Operating environment

Increased competition between Telco's continues to place downward pressure on average revenue per unit and creates the imminent need for differentiation and the search for value added services. Additionally, mobile number portability is permitted in more and more markets, leaving the customers with the choice of service providers. This places additional pressure onto the Telcos as their services and prices are carefully monitored by consumers and with little or no loyalty to a particular provider – with the option to keep the current number – usually only a few clicks on a webpage away.

Telcos were, and still are, looking for additional revenue streams and several business ideas are being tested or are already in production. Most of these business models are capitalising on existing investments in smartcards (SIM and USIM) due to the value added services that a SIM/USIM chip can offer besides its main function of holding the identity of the subscriber. A chip allows program execution protected against manipulation and it is possible to store data including phone numbers, short messages, personal configuration or cryptographic keys in the cards memory. This functionality in combination with the high penetration of mobile phones across the prospective end-user base results in an opportunity for the Telcos to leverage already deployed smart chips and provide value added services to end-users.

There are generally two possible solutions to include value added services to SIM/USIMS:

- an application in a dedicated smart chip; and
- a supplementary application in a SIM or USIM

However, since dual-slot mobile telephones have yet failed to achieve widespread use, the second solution is likely to prevail on short term. The main reason for this is probably more the lack of viable business strategies of network operators and alignment with mobile phone manufacturers other than for technical reasons.

Some corporations (like TeliaSonera¹⁰ and Elisa¹¹, see below) have successfully formed business relationships with local companies and the Finish and Swedish Government, opening their SIM cards (in non dual-slot mobile phones) to store additional information and applications¹².

A specific concern with telecommunications smartcards relates to the protection of an individual's privacy. SIMs contain a unique identifier of the cardholder. This allows Telco's and potential business partners of Telco's (e.g. government and merchants) to store and process information about the transaction behaviour of individuals including the locations where calls and transactions have been made.

5.3 Application description

5.3.1 Phone cards

Phone cards generally come in two variations¹³. The first type is the phone card, which is produced and used in very large numbers. In financial terms, this is an electronic purse that the customer purchases before using it. In technical terms, the phone card is a memory card with an irreversible counter, a security feature and synchronous data transmission. In some countries, such as The Netherlands, Telcos and banks have aligned the usage of phone cards and e-wallets. This allows e-wallet smartcards issued by banks to be used in telephone booths and the phone card to be used for making micro payments such as vending machines.

The other type of card is the telephone charge card, which resembles a credit card. The end-user pays for the services (telephone calls) by means of a monthly settlement against his or her bank account. Since this type of card is not widely used in Australia, it will not be further discussed.

5.3.2 Mobile phone smartcards

In the original specifications for the GSM system, the GSM chip was simply seen as a means to identify the end-user using a combination of a PIN and an authentication token, in the interest of billing security that was independent of the mobile telephone. However, in the course of time the desire to utilise the GSM card for additional functions, particularly supplementary services, became increasingly pronounced. For instance, a mobile telephone is also a competent medium for checking the balance of a bank account or receiving news, such as football scores and daily horoscopes, sending and receiving photographs, downloading new ring tones and making payments. Often, these services are provided by separate business partners that rely on the Telco Sim/UMTS chip infrastructure.

¹⁰ <http://www.teliasonera.com>

¹¹ <http://www.elisa.com>

¹² <http://www.vaestorekisterikeskus.fi/vrk/bulletin.nsf/vwSearchView/2D4DB25BA2DF16E9C22572190047A7FB>

¹³ based on the Smartcard Handbook, third edition, by Wolfgang Rankl and Wolfgang Effing, John Wiley and Sons, Ltd, 2003

5.3.3 Mobile payment solutions

SMS Based Payments

Several different systems are currently tested / in use that involve the usage of SMS to transfer money from one account to another. In all of these scenarios, the mobile provider offers the infrastructure to send SMS messages to the end-user. As most Telcos and phone manufacturers support SMS, this solution typically does not require an application to be installed on the chip.

The simplest scenario consists of a customer and a merchant who both have an account at the same service provider, for example PayPal.com¹⁴. The customer sends an SMS to PayPal which deducts the specified amount from the customer's account and transfers it to the merchant, who receives either an SMS or an automated voice call to confirm the payment. This system currently works with mobile phones in the US, Canada, and the UK.

Reverse SMS Billing

A system which is very similar to the above mentioned payment method is 'reverse SMS billing'. Reversed SMS billing is based on the principle that the owner of the recipient phone is charged for the cost of the SMS message, rather than the message sender. Reverse billed SMS messages are only sent if specifically requested by the phone user. Currently available solutions cater for train timetables being communicated via SMS or to purchase items including mobile ring tones, wallpapers and logos. Reverse SMS Billing typically does not require an application to be installed on the chip.

Recently disclosed information shows that the security of mobile phones and SMS is questioned as supposed hacks show how to eavesdrop on calls¹⁵. This may cause Telcos to include additional security measures in their chips and/or move to payment solutions where a separate payment application is stored on the chip.

WAP/GPRS/UMTS based applications

Using secure applications and browsers stored on a SIM/WIM/USIM to pay for bills is another method considered by telecommunication providers. To enable a payment, the end-user has to connect to a bank's gateway using the GSM, GPRS or UMTS connection. The connection costs however, are still quite high to achieve widespread use and a viable business solution for mobile service providers. When connection costs drop and browsing the internet with a mobile device becomes easier and more accepted this option may become a viable solution.

¹⁴ PayPal.com launched its new SMS Based Payment Service in March 2006. For more information see <https://www.paypal.com/cgi-bin/webscr?cmd=xpt/cps/mobile/MobileOverview-outside>

¹⁵ <http://www.itwire.com.au/content/view/7216/990/>

Proximity Payments

Another example of mobile payments solution are Proximity – or Point of Sale (POS) – payments. These are payments in which the transaction initiation devices are all in the same vicinity. Proximity payment systems typically utilise 'Near Field Communication (NFC)' technologies. NFC is a short-range wireless connection technology. Communication occurs when two NFC compatible devices are brought within a couple of centimetres of one another. NFC operates at 13.56 MHz and transfers data at up to 424 Kbits/second.

Mobile service companies like NTT DoCoMo (Japan) are offering NFC payment services, where mobile phones act as the payment device. These mobile phones carry two smart chips¹⁶, the normal SIM and a separate NFC payment chip. The end-user is able to initiate a transaction by holding the handset in front of a NFC reader and entering a security PIN into the handset to authorise the transaction.

5.3.4 Non-Payment solutions

Besides the above mentioned payment methods, Telcos are also looking into other areas of value adding services. The remainder of this section provides an overview of a number of selected initiatives from around the world.

Finland and Sweden

Telcos in Finland and Sweden store Citizen Certificates issued by the government on the end-user's SIM card. This provides end-users with the ability to authenticate themselves to online government and banking services. End-user are required to enter a PIN and a digital signature is generated in the PKI-enabled SIM card, and the mobile phone serves as the card reader. TeliaSonera, the largest mobile operator in Finland and Sweden offers this service together with Elisa¹⁷.

South Korea

KT Corporation and SK Telecom launched in 2006 a wireless broadband and Internet service called WiBro (WirelessBroadband). To authenticate their customers, they use special SIM cards, which can be used in smart phones, PCs, notebooks and PDAs. These SIM cards hold encryption keys and algorithms for authentication of customers who want to access this wireless service¹⁸.

KT Corporation focuses mainly on delivering information search, e-mail, news, video-on-demand, multimedia blogging, video chat, multimedia messaging, online gaming and file management services via WiBro. They initially charge subscribers the basic service fees at 16,000 won (AUS 22.00) and 30,000 won per month, respectively. Soon to be introduced is a pricing structure based on the volume or type of data transactions conducted by the end-user.

¹⁶ It's possible to have credit cards with dual-interface (contact and contactless), but currently there's no SIM card available that offers phone and wireless credit card options. But it's foreseeable that such an integrated SIM will become viable in the future. An example for dual-interface credit cards can be found at http://www.jcbcorporate.com/english/news/200404_1.html

¹⁷ <http://ec.europa.eu/idabc/en/document/4500/334>

¹⁸ <http://www.wibro.or.kr/>

5.4 Implementation overview

This section provides some implementation characteristics of the smartcard / SIM projects around the world.

5.4.1 Phone cards

In 1986 France Telecom launched the first value phone cards on a large scale that were chip based. These smartcards stored the value on the card and were read by special public pay phones when docked in the phone's card reader. This usage of smartcards was the first mass smartcard implementation worldwide. The total usage rose to nearly 60 million in 1990, and to several hundred million worldwide in 1997. Germany experienced similar progress, with a time lag of about three years. These systems were marketed throughout the world after the successful introduction of the smartcard public telephone in France and Germany. Telephone cards incorporating chips are currently used in more than 50 countries worldwide¹⁹. After the initial success of telephone cards, they continue to lose market shares to e-wallets and the increasing use of mobile phones.

5.4.2 Mobile phone smartcards

In 1988, the German Post Office acted as a pioneer in the area of mobile phone smartcards by introducing a smartcard as an authorisation card for the analogue mobile telephone network (C-Netz). The main reason for the introduction of the smartcard was the increase of fraud with the magnetic-stripe cards that were then used. The positive experience gained from using smartcards in the analogue mobile telephone system was decisive and led to the introduction of smartcards into the digital GSM and UMTS networks.

5.4.2.1 Payment solutions

SMS Based Payments & Reverse SMS Billing

SMS based payment systems were introduced to the market in the late 1990s. Most schemes weren't very successful as the mobile phone penetration wasn't pervasive. This has changed in the last few years, leading to the introduction of several SMS based payment systems in different sectors, ranging from buying mobile content (ring tones or music downloads), congestion charge payment services in London²⁰ and closed user group solutions like PayPal.com.

Proximity Payments

NTT DoCoMo (Japan) launched its mobile wallet program mid 2004 and has currently issued more than 12 million handsets that support the company's mobile NFC payment system. To be able to accept proximity payments, merchants are required to buy NFC compatible point-of-sale terminals. There are currently about 78,000 stores with terminals that support NTT DoCoMo's value card and about 25,000 that support the credit card service²¹.

¹⁹ Based on the Smartcard Handbook, third edition, by Wolfgang Rankl and Wolfgang Effing, John Wiley and Sons, Ltd, 2003

²⁰ London Congestion Charging is currently the largest SMS based payment scheme in Europe. More information can be found at: <http://www.cclondon.com/howtopay-sms.shtml>

²¹ <http://www.techweb.com/showArticle.jhtml?articleID=160800003>

Proximity payment applications are currently being trialled in various European countries. A proximity payment pilot was carried out in Finland in cooperation with Nordea bank, Nokia, Visa, the Finnish retailer and bank-owned credit card service company Luottokunta and the firm of Finnish Manison Maksujärjestelmät Oy as the payment terminal supplier. The pilot group included 150 users and it took place in a Southern Finland town called Lahti between 15 September 2003 and 16 February 2004²².

JCB, in cooperation with CCV Holland B.V., Gemalto, KPN, Nokia, NXP Semiconductors, PaySquare, and ViVOtech, has recently announced the launch of Mobile J/Speedy, a NFC mobile payment pilot project in Amsterdam. Following initial trials in September 2006, the pilot service is being rolled out to a broader group of JCB's customers. The project marks Europe's first contactless international credit payment scheme using a mobile phone with an NFC chip²³.

In the United States, Citigroup, MasterCard Worldwide, Cingular Wireless and Nokia announced in December 2006 a trial in New York City of NFC enabled mobile phones with MasterCard PayPass(TM) contactless payment capability. The goal of this trial was to evaluate the speed and convenience that "tap and go" payments made through mobile phones can provide to Citi credit cards and Cingular customers in the New York City area. The trial is expected to run three to six months²⁴.

5.4.2.2 Non-Payment solutions

Finland and Sweden

TeliaSonera and Elisa started to offer SIM cards that are capable of storing the Government Citizen Certificate at the end of 2005²⁵. A number of applications are currently available that use the mobile Citizen Certificate, including services offered by the Social Insurance Institution, the tax administration, and the Ministry of Labour. OKO Bank group is currently offering an m-banking service based on the mobile Citizen Certificate.

Korea

KT Corporation and SK Telecom launched WiBro around Seoul on June 30, 2006. Subscribers can access the WiBro service only by using a PCMCIA card where the end-user inserts the WiBro enabled SIM. According to KT Corporation WiBro-enabled portable devices, including notebooks, PDAs and dual-mode terminals combining WiBro and other wireless communication services will be commercially available in February 2007.

²² Refer to <http://www.mobeyforum.org/?page=trials>

²³ Refer to http://www.paymentsnews.com/2006/10/jcbs_amsterdam_.html

²⁴ Refer to: <http://www.citigroup.com/citigroup/press/2006/061214b.htm>

²⁵ Refer to: <http://www.teliasonera.com/externalarticlenm/?hier=12815&mainUrl=http%3A%2F%2Fwww.sonera.fi%2FpressProviderWeb%2Fresources%2Fjsp%2FProvider%2FgetArticle.do%3Flocale%3DEN%26articleId%3D170512>

5.5 Program management and support

This section provides a description of the main roles in the discussed smartcard projects.

5.5.1 Phone cards

Phone cards are typically distributed by individual Telcos. As a result, most phone cards are not interoperable with other providers and can only be used within the country of issue. As an example, French phone cards are based on EPROM technology, whereas German phone cards are based on EEPROM technology. The latter type of chip does not need an external programming voltage, whereas the French type does. An unfortunate consequence is that the French and German telephone cards are mutually incompatible.

5.5.2 Mobile phone smartcards

GSM chips

During the early 1980s, analogue cellular telephone systems were experiencing rapid growth in Europe, particularly in Scandinavia and the United Kingdom, but also in France and Germany. Telcos in each country developed their own proprietary systems, which caused the systems only to be used within national boundaries. European Telcos realised the drawbacks of this at an early stage, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications were published in 1990.

UMTS chips

In 1998, a group of five standards organisations consisting of ANSI T1 (USA), ARIB (Japan), ETSI (Europe), TTA (Korea) and TTC (Japan) initiated the Third Generation Partnership Project (3GPP), whose purpose was to specify a successor to the GSM in the form of an international IMT-2000-compliant mobile telecommunications system based on the GSM specifications.

Chip based applications

The introduction of successful value added services based on mobile phone smartcards typically requires cooperation between various stakeholders. Stakeholders typically include the Telco's, mobile phone manufacturers, chip manufacturers, POS reader manufacturers, transaction processor and application developers.

5.6 Cost/benefits analysis

Detailed cost/benefit information relating to smartcard deployments by Telcos is typically not available in the public domain. It is also too early to comment on the cost/benefit analysis for Telcos with regard to smartcard implementation and usage apart from the infrastructure they are offering.

Telcos involved in solutions that leverage already deployed smartcards, such as SMS based payment systems, do not face additional costs to participate in and benefit from these schemes. On the

other hand, new technology such as NFC provides opportunities for Telcos, banks and service providers to offer more value added services. Most of these solutions are still in trial or testing phases and are not mature enough as they commenced in mid / end 2006. It is estimated that the additional costs of enabling SIMs with NFC is approximately A\$8 per handset.

5.7 Lessons learned and recommendations

- The breakthrough for phone cards did not come in an area where traditional cards were already used, but in a new application – the phone booth. Introducing a new technology in a new application has the advantage that compatibility with existing systems does not have to be taken into account, so the capabilities of the new technology can be fully exploited.
- End-user adoption of tedious applications is low and results in the slow uptake and the usage of the service, as shown in the WAP/GPRS solution. Further, the addition of mobile services requires service providers to adjust their screen sizes, resulting in reduced usability.
- Ensure the critical mass of smartcard users and smartcard readers are available. One of the success factors in Japan was the early availability of contactless smartcard readers in stores all over the country.
- Ensure transparency between involved entities when using multi-application smartcards. One reason banks and telecommunication companies failed in the past to work together with multi-applications on SIM cards was the constant distrust about who owned the customer, what kind of functionality the other entity was offering and the fear of losing business and customers.
- To ensure significant uptake, implement customer acceptance techniques, including customer usage incentives such as free service usage or discounts and frequent customer satisfaction surveys and interviews.
- End-user awareness and education have to ensure that the clients know about the new services the smartcard technology offers and how they can benefit from it.

The implementation of new technology requires a comprehensive and effective marketing strategy using different media to ensure market and customer acceptance.

5.8 Sources and references

The following references contain other useful background information on Telco smartcards around the world:

- For further information on facts and figures on the GSM association, refer to: <http://www.gsmworld.com/>
- For further facts and figures on contactless smartcard payments, refer to: www.smartcardalliance.org and <http://www.contactlessnews.com/>
- The Mobey Forum (pronounced Mo-Bay) is a financial industry-driven forum, whose mission is to encourage the use of mobile technology in financial services - <http://www.mobeyforum.org/>

- The Mobile Electronic Signature Consortium is an association of companies and organisations from the mobile phone and Internet sectors - <http://www.mobileoffice.co.za/mest.htm>
- The Near Field Communication (NFC) Forum is a non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs - <http://www.nfc-forum.org/home>