

# Smart Card Management Systems

An overview by Mike Hendry

Mike Hendry <mike@mikehendry.com>  
V 2.4, 24 March 2008

## Table of Contents

Introduction.....	3
Scope.....	3
Card Management .....	3
Development of SCMS .....	3
Functions .....	4
Common Functions .....	4
Application-specific Requirements .....	5
Government.....	5
Banking.....	6
Telecoms.....	7
Transportation .....	7
Universities and schools.....	8
Corporate cards .....	9
JavaCard, Multos and GlobalPlatform .....	9
Buying an SCMS .....	10
Do I need an SCMS? .....	10
Criteria.....	10
ActivID .....	11
Appendix: Table of ActivID CMS features .....	12

## Smart Card Management Systems

---

### Introduction

---

#### *Scope*

---

This paper provides an introduction to Smart Card Management Systems. It is written primarily for organisations that issue cards to their customers, employees, members or citizens, and that are moving or have moved to using smart cards (chip cards). Smart cards offer more functionality and more security but are also more complex than other card types (such as magnetic stripe cards) and can therefore be more difficult to manage.

The paper describes the main functions of an SCMS, and in particular the special functions needed by each user sector; as one of the advantages of smart cards is their ability to carry multiple applications, it is important that any SCMS can handle the functions needed by all the different application types on the card. It then looks at some of the issues involved in procuring an SCMS and evaluates the functionality of ActivID CMS from ActivIdentity.

---

#### *Card Management*

---

The main purpose of a Card Management System is to track cards issued, from the point when it is decided to issue a card to a person, through to that person's removal from the system. A Card Management System should normally allow the issuing organisation to identify the card number or numbers, the standing data on the card, and the card status (in production, issued, lost, withdrawn etc).

Usually the actual data are held in a separate system (an accounts system, personnel database etc) and in this case the CMS can be very simple: a flat file that links a card number to a database entry. When the card is issued, the data are assembled from the different sources and sent to the card production machine.

This kind of structure makes it easy to give a help desk operator, for example, access to only those parameters he or she needs, and it is also feasible for the card management to be performed by a bureau or third-party service.

---

#### *Development of SCMS*

---

When a chip is substituted for the magnetic stripe or bar-code, the structure described above may still be perfectly adequate if the card has a single function that will not change during its life.

There are some complications:

- A chip card can store more data than most other card types;
- Those data are more easily changed during the life of the card; and

- They include some secret areas that must not be copied or held in clear on a host system

These imply that the CMS must link to a more complex database, but do not actually increase the complexity of the card management function itself.

Where, however, the applications (programs) on the card may be updated during its life, or new applications added, there must be a system to track these changes, and to ensure that the memory on the card is used correctly. These are the main functions associated with a Smart Card Management System (SCMS).

Use of an SCMS is probably essential if the card applications will be developed, loaded and managed by different organisations – this is still quite rare but many cards have that capability. As we will see in a later section, many SCMS also handle complex cryptographic hierarchies and certificates, or functions associated with particular applications or sector requirements. Although these could be handled by different subsystems, an SCMS can often provide all the functions needed for a given application, and thereby reduce complexity and integration requirements.

---

## Functions

---

### *Common Functions*

---

Almost every organisation specifying an SCMS will require some common functions:

- A link to an external database or legacy Card Management System. Although this is a generic requirement, we will see that some sectors have specific requirements as to platforms, database structures and secure access;
- Support for a Host Security Module (HSM) or similar system that protects master keys and performs secure cryptographic operations. Again, although this is a common requirement each sector has its own algorithms and preferred HSM types;
- Life-cycle support: the ability to manage all the possible phases of a card's life and of a card application's life, using a combination of workflow and automatic functions. Issuers must recognise that the workflow required to replace a lost or damaged company ID card may be quite different from that needed to issue a replacement bank card;
- Registration, issuing and fulfilment: a combination of automated and workflow functions to allow new cardholders to be added to the system, to generate the data to be passed to the personalisation machine and any additional requirements (envelopes, PIN mailers, biometric data capture) that allow the card to be sent or handed to the person who will use it;
- Integration with logical access control and single sign-on processes; because an SCMS is only one part of the issuer's system, it must support the user

rights and permissions structure used by other subsystems. The SCMS may be expected to play a proactive role in enforcing the organisation's security policies.

---

### *Application-specific Requirements*

---

In addition to these common requirements, each sector expects further specific functions and characteristics from its SCMS, largely determined by the different ways it uses the card. A company wanting to work with another sector must be aware of its partner's requirements. For example:

#### *Government*

Central Government applications are most likely to be based on mainframe platforms. Although in most cases one government department or agency is designated as the card issuer, many other departments may contribute data and require access to the data on the card, often in different logical areas or files on the card. Because of the widespread distribution of cards and need for 100% coverage of the population, it is common for registration, processing and sometimes even card issuing to be distributed across the country.

Some government cards have a long life – up to ten or even twenty years – which may outlive the governments and departments that created the data; the structures must be sufficiently flexible to survive such changes. Attitudes and policies may change as well: for example, doctors may be required to disclose data that were previously kept private in a health card.

Government data in most Western countries are subject to a complex mix of privacy and Freedom of Information standards; in some countries people may request secrecy at an individual field (data item) level. The SCMS must carry across and take into account any such flags and secrecy requirements.

The US Government mandates the use of a Federal Standard (FIPS 201) for personal identification in US government bodies; this is regarded as a benchmark for secure access control and many other governments now follow it, so this sets the standard for cryptography, credential management and smart card interoperability in this sector.

Outside the USA, some governments have standardised on Multos as their preferred card platform; its tight controls and rigid hierarchy are well-suited to this environment. For sale to government departments in these countries, an SCMS must therefore support the Multos loading processes. However many governments – including the US – have adopted an open platform policy, for which GlobalPlatform appears most suitable, although the flexibility it offers may call for more expertise in its deployment.

Governments are increasingly interested in supporting the International Civil Aviation Organization (ICAO) standards for e-passports; this is leading them to demand support for biometrics (particularly facial image, iris and fingerprint) and for contactless cards.

Local government requirements vary much more: some local government cards are simple loyalty and discount cards that require little security and no dynamic updating. Others include monetary value (where central government cards include this function, it is normally supported by a bank or other organisation). In the UK there is a framework (the National Smart Card Project: NSCP) that local authorities must follow in order to receive central government support. The NSCP SmartConnect software package is an SQL database with built-in registration and personalisation machine support; these are considered to be the main SCMS functions required.

### *Banking*

A bank card issuer (whether a bank or a bureau working for several banks) is subject to stringent standards imposed by the card scheme (typically Visa and/or MasterCard). Security policies are set and imposed across all systems, and can actually vary surprisingly from bank to bank. External service providers must be vetted directly by the card schemes and must meet the tight requirements of the Payment Card Industry Data Security Standard (PCI-DSS).

Most banks have a strong preference for non-stop, Unix or mainframe platforms and are resistant to mixing platforms, even often down to Unix flavours and database types. So a supplier must be able to support a wide range of platforms and databases.

Bank chip cards all comply with one specification (EMV) but there are variations for each card scheme (Visa, MasterCard, American Express, JCB, China Union Pay etc) when it comes to security and some data elements; the SCMS must be aware of these requirements when preparing data for card personalisation. A single EMV application can support multiple payment card functions: for example, a credit, debit and ATM card, however the electronic purse (pre-paid) applications used in some countries are separate and do not conform to EMV.

EMV specifies quite a simple key structure, using triple-DES and RSA; it also includes a mechanism for sending scripts to the card to update parameters or to enable/disable applications. These scripts are appended to authorisation responses, so there must be some integration with the authorisation system.

Each card scheme has its own requirements for the data structures used in card personalisation, so an SCMS must be able to support all the relevant structures. Although Visa is most closely associated with JavaCard and MasterCard with Multos, this is not a rigid boundary and in fact by far the majority of all bank cards today use native card platforms. This is true even for those cards that do support multiple applications (most often loyalty or e-purse).

However, banks in some parts of the world are keen to move on to multi-application cards and dynamic application management for their next generation of cards. Asian banks have issued many more multi-application cards than their colleagues on other continents.

The major area of interest for banks at present is contactless cards; it is very likely that the spread of multi-application cards in Europe will take place in

parallel with, and partly driven by, the move to contactless. Since contact functions are still required for compatibility, dual-interface cards (with both contact and contactless interfaces) will be used; personalisation may need to take place through both interfaces.

### *Telecoms*

The T2G and Eurochip cards used to replace coins in public telephones are quite simple and are unlikely ever to be updated in the field. Cards used for mobile telephony (SIM and USIM) and in cable and satellite television, on the other hand, are connected to the operator most of the time and are updated frequently.

The mechanisms in the GSM and 3G specifications permit the network to change any parameter in the SIM card at any time when the telephone is on its home network. Additional applications may be downloaded to the SIM using the SIM toolkit (GSM 11.14); most SIMs support this function. For cable and satellite television the corresponding standards are DVB-T and DVB-S.

Telephone users (customers) have access to significant storage capacity on the card; as well as phone numbers and text messages, modern phones and SIMs may be expected to save quite long video sequences which require many megabytes of storage. Since an important function of an SCMS is to manage memory, an SCMS designed for this application must be able to allocate memory dynamically to program downloads, video capture etc.

Most SIM cards are distributed not directly to the end user, but through a distribution and retail network; this requires a further level of batch and activation controls that are not needed in other sectors.

Telecoms businesses are very Unix- and Linux-oriented; these are mandatory platforms for systems in this sector, while most SIM cards are based on a JavaCard platform. One of the reasons for the global success of the GSM system, and now 3G, is the extent to which interfaces and systems are standardised, with a small number of key suppliers dominating the market.

### *Transportation*

Nearly all cards used in public transportation are now contactless. The majority are actually wired-logic cards using the Philips MiFare or Sony FeliCa standards, although the less proprietary ISO 14443B standard is now gaining momentum. We must distinguish between the contactless interface used (ISO 14443A, B or FeliCa) and the functions on the card: where MiFare or FeliCa functions must share a card with other chip card applications that require a microprocessor (ISO 7816-3) card, the MiFare or FeliCa functions must be emulated, and this often means that the cards cannot be personalised in a single machine.

Most systems have a requirement for a mix of personalised cards (typically for monthly and longer season tickets) and unpersonalised day and single-journey tickets. Many also incorporate pay-as-you-go value, using proprietary protocols.

Many schemes aim for inter-modal use (one card can be used on the metro, in buses, ferries and sometimes even in taxis). Although the revenue-sharing aspect is unlikely to impact the SCMS, it may mean that cards and terminals within the scheme are owned by different companies and brought together under a single umbrella, which may require a more complex key structure. In Europe many cities and governments are keen to promote interoperability between the transport cards of different cities or regions; the Calypso and ITSO standards are designed to handle this situation, although many large schemes (e.g. London's Oyster card) do not follow these standards.

Updates to cards (the equivalent of scripting for bank cards) are handled through Action Lists: messages scheduled to be sent to a card when it is next seen by the system. However, unlike bank cards, most transport cards work offline, and so the Action Lists must be sent to the individual terminals where the card is most likely to be used. A message structure is needed to record delivery.

Because of the legacy of wired-logic cards in the transportation industry, application management has traditionally lain in the terminal domain rather than being linked to cards; where card application management is now being added, it is more likely to be a subsystem linked to the main Card Management System. The CMS is likely to reside in a mainframe environment and its functions are extended to cover those performed by an SCMS in other sectors; the CMS itself provides the database, which may be proprietary or a conventional relational database management system such as Oracle or DB2.

This means that card and transaction management are merged into one system, although there is growing interest in extracting customer data on the one hand, and real-time monitoring and fraud control on the other. Many operators, particularly those specifying systems today, are looking to move to more modern platforms and open, international standards such as ISO 24014<sup>1</sup>, ITSO and Calypso.

### *Universities and schools*

Most smart card schemes in universities and schools operate primarily online: nearly all the data, including permissions etc, are held on the host system, although there may be some exceptions for vending or car park access etc. Contactless cards are preferred for access control functions, however many systems also use contact or dual-interface cards to allow use in computer networks.

The main requirement for an SCMS is therefore to interact with the student registration system (e.g. SIMS in the UK) and to allow enrolment (including a biometric) on-site, preferably with immediate card issue using a local card printer/encoder.

There is increasing demand for authentication systems in universities in particular to follow Shibboleth (WWW2) standards to allow users to access

---

<sup>1</sup> ISO 24014:Public transport -- Interoperable fare management system

resources on other systems. Although Shibboleth does not require the use of a smart card, any smart card system should include Shibboleth "Where are you from" functions.

### *Corporate cards*

Corporate cards are in many respects similar to campus cards in universities and schools, but without the unifying standards. There may be a greater need for a wide range of functions on the card itself, particularly if the company operates across many sites. Immediate issuance is a frequent requirement.

Products must be capable of integration with network software, common operating systems (Microsoft CAPI etc) and enterprise software. In particular they must support the security requirements and authentication structures of the relevant packages, which may be quite complex. The internal corporate environment is also often more complex with many different subsystems to interact with (including Single Sign-On, PKI, ID Management, authentication services etc). Software and network environments are often heterogeneous, mixing Wintel, Unix and more specialised platforms; there may be a range of overlapping security domains with varying security objectives.

Processes must be automated to minimise the cost of deploying, issuing and maintaining cards. In some applications it is important for users to be able to access their own profiles, making or requesting changes as appropriate.

Because Single Sign-On is a very common part of the functionality requested in this sector, cards are often left in PC card readers for longer periods and may be managed and updated by a corporate IT department.

---

### *JavaCard, Multos and GlobalPlatform*

---

The two main contenders for "open" multi-application cards allowing applications to be loaded independently are JavaCard and Multos.

Multos uses a strict security scheme, with every application certified by the card issuer and by the StepNexus<sup>2</sup> Global Key Management Authority. Applications are loaded in an encrypted form, and only decrypted after the card checks the application certificate. The SCMS must work with the card issuer, application developer and StepNexus KMA to produce and deliver the Application Load Units to the card.

JavaCard allows a wider range of load options, however GlobalPlatform offers a combination of run-time environments and back-end system specifications that define a secure application load and memory management process. It is even possible to implement GlobalPlatform card management using Multos cards and load processes.

---

<sup>2</sup> StepNexus is the organisation that promotes the Multos standards.

## Buying an SCMS

---

### *Do I need an SCMS?*

---

Many card-issuing organisations believe that because they have a Card Management System and are moving to smart cards, they will now need a Smart Card Management System. This is often not true, because as we saw above the primary focus of many SCMS is the management of card applications; so if there is an existing CMS handling the parameters, and the applications on the card are not likely to change during the life of the card, an SCMS may well not be needed.

However, if the applications are complex and will require frequent updates, particularly through scripts or action lists, then an SCMS may well offer a simpler implementation route than integrating many separate subsystems. It is better to implement an SCMS before the structures become too complex, as migration or back-filling data brings its own risks.

On the other hand, if the long-term requirements for the card are unclear, and in particular if the requirements for support of other card types, standards and procedures have not been specified, then it may be premature to consider installing an SCMS that may need substantial modification and new features in the future.

For corporate or Government ID management applications, the requirement often presents itself differently: the existing databases (personnel records etc) have no card management functions, and there is a need for a system to manage the whole personalisation process, usually in-house. In this case an SCMS may perform the dual role of CMS and card personalisation without the need for further systems.

---

### *Criteria*

---

Organisations contemplating buying a Smart Card Management System are advised to consider carefully their long-term objectives for partners, IT and card platforms, and for backwards and forwards compatibility.

They may use the descriptions in this paper to create a checklist of likely requirements, however it is always best to discuss with each potential partner its specific requirements in order to ensure a "best fit". It is good to remember that the purpose of the card is to represent a relationship between the issuing organisation and the person to whom the card is issued; any system must reflect the relationships, terminology and values appropriate to the cards it is supporting. Often the terminology used betrays the target sector: the person to whom the card is issued may be an employee, citizen, cardholder or account-holder, passenger, customer or student.

Important criteria (in addition to all the usual criteria for IT procurement) include:

- The platforms and environments on which the software runs: not only the operating system but also any databases and reporting tools, and the security environments supported or offered;
- The card platforms, personalisation systems and Host Security Modules supported (including data synchronisation for contactless or dual-interface cards where appropriate);
- Capacity (in terms of cards, applications, simultaneous users, numbers of cards issued per minute etc)
- Structure of the issuing process (immediate, batch, bulk, multi-phase);
- Any specific interfaces to external databases required, for example a Certification Authority, registration or authorisation system;
- Cryptographic algorithms and key management systems to be used;
- Workflow and processes for all relevant activities and lifecycle phases, including integration with legacy processes where required;
- The method to be used for updating cards (online 'push', 'pull' through scripting or action lists);
- Any certifications or approvals required by international or national authorities;
- Ease of use and future-proofing.

---

### *ActivID™ Card Management System (CMS)*

---

**ActivIdentity** (formerly known as ActivCard) is one of the world's leading suppliers of Smart Card Management Systems. It developed its *ActivID* CMS to meet the needs of large corporate users and government agencies for multifunctional identity management systems for employees. Its flagship customer is the US Department of Defense, and ActivID has benefited significantly from the introduction of FIPS 201, but the majority of its customers are in fact operating corporate employee ID systems.

## Appendix: Table of ActivID CMS features

Platforms	Databases	Personalisation machines	Algorithms	HSM types	CA's supported	Scale (typical card volumes)	Web site	Contact				
Windows, Solaris	Oracle, SQL Server	Fargo, Datacard desktop	All PKCS#11	AEP Keyper; nCipher; SafeNet	Cybertust; Entrust; Microsoft; VeriSign; Exostar; CryptoVision; OpenTrust	500 - millions	<a href="http://www.actividentity.com">www.actividentity.com</a>	info@actividentity.com +1 510 574 0100				
Card platforms						Application management functions						
Native ISO 7816-4	JavaCard / Open Platform	Multos	ISO 14443B	MiFare	FeliCa	Also support magstripe	Appn devt mgmt	Appn certn	Appn mgmt	Appn parameter mgmt	Dynamic memory allocation	Track life-cycle status
Y	Y	Planned Q2/08	Supports perso. of FIPS201 data through contactless interface	N	N		Separate products	Y	Y	Y	Y	Y
Issuing process									Card updates			
Directly control perso machine	Perso data prep	Immediate issue	Bulk issue	Both perso & anon cards	Distributed regn. & issuance	Retail / indirect distribution	Multi-issuer (bureau)	Biometrics	Self-service "pull"	On-line "push"	Post issuance scripting (delayed delivery)	Action lists
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Subject to configuration
Compatibility				Application-specific functions								
Global Platform	Shibboleth	FIPS201	Microsoft CAPI	VIS data prep	M/Chip data prep	EMV scripting	SIM & SIM toolkit	E-purse / stored-value	Loyalty	Calypso	ITSO	Physical access control
Y	N	Y	Y via ActivClient	N	N	N	N	N	N	N	N	N