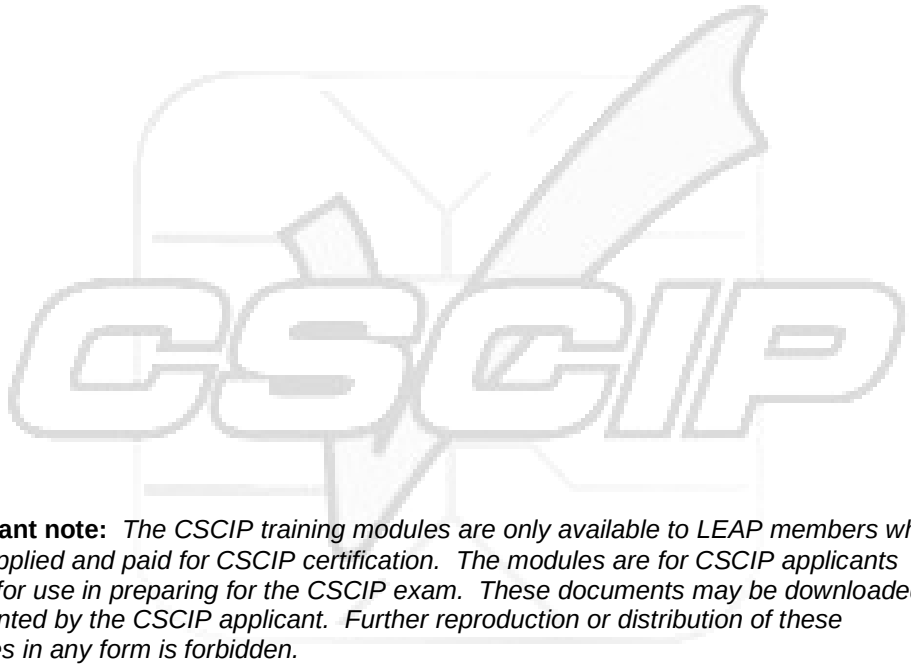
Module 3: Smart Card Application and Data Management

Smart Card Alliance
Certified Smart Card Industry Professional
Accreditation Program

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.



Important note: *The CSCIP training modules are only available to LEAP members who have applied and paid for CSCIP certification. The modules are for CSCIP applicants ONLY for use in preparing for the CSCIP exam. These documents may be downloaded and printed by the CSCIP applicant. Further reproduction or distribution of these modules in any form is forbidden.*

Table of Contents

1 Introduction

This module describes how smart card data and applications are managed and how organizations manage cards through their life cycle. After reviewing this module, CSCIP applicants should be able to answer the following questions:

- What are single and multiple application smart cards and how do they differ in the way data and applications are stored on the card?
- What is chip initialization and when is initialization done in the smart card manufacturing and personalization process?
- How are symmetric and asymmetric keys used with smart cards and how are they managed?
- What are the steps required for issuing a smart card?
- How do issuers manage the card and card applications through the card's service life?
- What are key standards and specifications that apply to data and application management?

2 Single and Multiple Application Smart Cards

2.1 Single Application Smart Cards[1]

One class of smart card is known as the single application smart card. This class of smart card is popular in vertical markets that require a fixed (and stable) set of functionality from the smart card, coupled with a large volume of cardholders. Examples of single application smart cards can be found in the financial services industry with smart card-based credit/debit applications as well as branded stored-value applications.

Single application smart cards require a large volume of cards to be produced to realize any economy of scale. A further disadvantage is that a single application may be made obsolete if there is a change in the application's functional requirements that require a change to be made to the smart card.

2.1.1 Dedicated Hardware in the Form of an ASIC

A single application smart card can be as fundamental as a card with dedicated hardware logic that supports fixed functionality addressed through a command/response protocol at the card edge interface. The allocation of storage for data, keys, access control status bits, and other information might be hardwired so that no change is possible without the direct intervention of the chip manufacturer. Application-specific integrated circuit (ASIC) technology continues to be used in the smart card industry to achieve single application functionality. An ASIC can be very low cost. However, the risk is that an ASIC solution generally takes a great deal of time to realize and a change to an ASIC may not be responsive to changes in application requirements.

2.1.2 Single Application Cards from a Vertical Industry Perspective

A single application smart card can also be implemented with a computer chip that has a fixed operating system controlling a limited set of computer resources that meets the needs of the single application. As with an ASIC design, the functionality that is supported from the card interface for a single application implementation is not extensible without the direct involvement of the chip manufacturer and/or the card provider.

2.1.3 Broad ISO Definition of a Single Application

A single application can also be provided on general purpose smart card computer hardware. What separates out a single application from the more general multiple application smart card is the manner in which functionality accessible from the interface is organized inside the smart card.

For smart cards conforming to ISO/IEC 7816 Part 4, the functionality is placed in a "common" area. The partitioning of data defines whether one application or many can be used by an implementation.

ISO/IEC 7816 Part 4 defines a single application as a common area of functionality that in turn works on a defined set of Elementary (data) Files (EF) that reside either directly below the Master File (MF) or are encapsulated within a "folder" known as a Dedicated File (DF). Figure 1 illustrates data file structure for a single application smart card. At most one DF defines a single application implementation.

[1] Source: ISO/IEC 7816

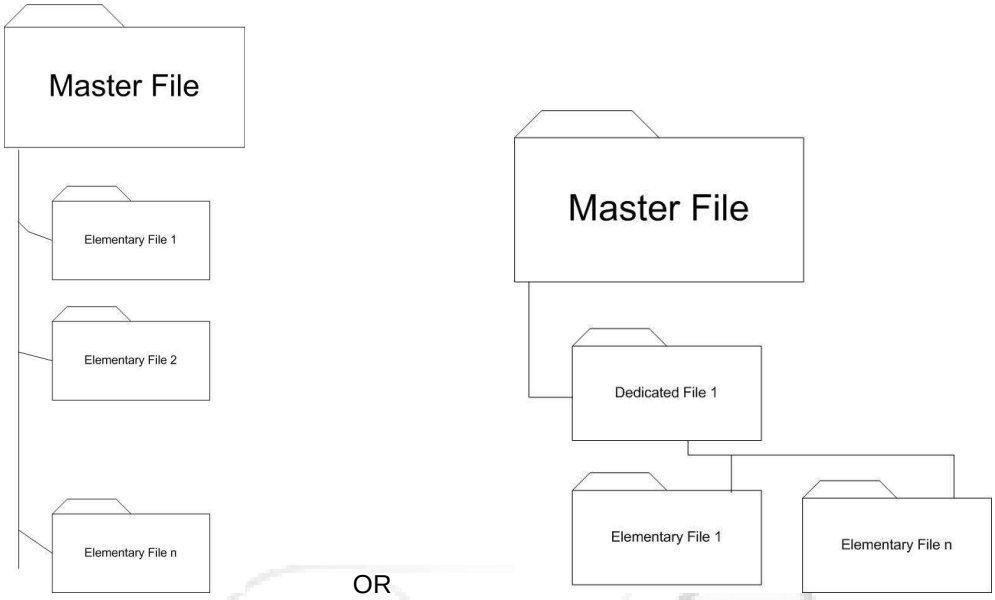


Figure 1. Data File Structure for a Single Application Smart Card

2.1.4 Single Application Instantiated on a General Purpose Operating System

Finally, a smart card using a general purpose operating system such as Java Card, MULTOS, or .NET can be classified as single application if only one application is loaded and instantiated.

2.2 Multiple Application Smart Cards[2]

Another class of smart card is known as the multiple application smart card, which is popular in many smart card-enabled industries today. One compelling reason for this popularity is that the application provider is no longer dependent on the chip manufacturer or the card manufacturer for creating and maintaining each smart card application based solely on the interpretation of requirements provided by the application provider. Developers of multiple application smart cards have access to software development kits (SDK) specific to a smart card platform that permit programming of the smart card in a widely available language (e.g., Java, C#, BASIC). An SDK is a valuable tool for creating, debugging and developing enhancements to a smart card application.

A multiple application smart card can be viewed much like a PC where applications are loaded by the owner of the PC. For a smart card, applications are usually loaded by an entity known as the card issuer. Several vertical markets can be accommodated using a multiple application smart card platform. For example, the telecommunications industry can add financial applications to an existing subscriber identification module (SIM) card to facilitate mobile banking.

[2] Sources: ISO/IEC 7816; Java Card specifications, http://java.sun.com/javacard/specs.html; MULTOS specifications, http://www.multos.com; .NET smart card specifications, www.gemalto.com/dwnld/5763_Gemalto.NET_User_Guide.pdf; Smart Cards, Tokens, Security and Applications, by Keith Mayes (editor) and Konstantinos Markantonakis (editor), Springer, 2008

2.2.1 Broad ISO Definition of Multiple Applications

Multiple applications can be provided on general purpose smart card computer hardware. What distinguishes multiple application smart cards is the manner in which functionality accessible from the interface is organized inside the smart card.

For smart cards conforming to ISO/IEC 7816 Part 4, the partitioning of data defines whether one application or many can be used by an implementation. This is known as a data-model approach to achieving multiple applications. In other words, an application is defined by its data and the access privileges to the data; the functionality is common across all applications residing in the multiple application smart card.

ISO/IEC 7816 Part 4 defines multiple applications as a common area of functionality that in turn works on a defined set of Elementary (data) Files (EF) that reside in multiple "application folders;" each folder is called a Dedicated File (DF) and is accessible from the outside world by a variety of methods including an application name.

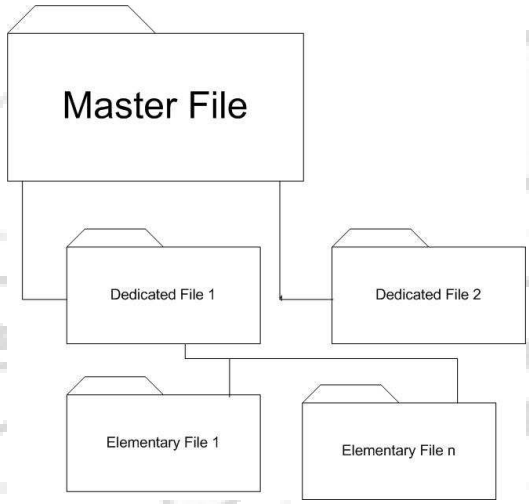


Figure 2. Data File Structure for a Multiple Application Smart Card

2.2.2 Multiple Applications Instantiated on a General Purpose Operating System

General purpose operating systems such as Java Card, MULTOS, and .NET were developed specifically to provide a new approach to enabling multiple applications. The key differences from the ISO/IEC 7816 Part 4 standard are the following:

1. The functionality is encapsulated in the same domain as the data for an application (or set of cooperating applications) and is not separate as in an ISO implementation.
2. Applications are isolated from each other unless one or more applications explicitly allow sharing of data and methods.
3. The security mechanisms for an application or suite of applications are under the control of the application provider and are not predetermined by ISO standard.

Each application residing on top of any multiple application architecture is free to define an application-unique command set, data organization and security attributes. Such freedom, however, often leads to

interoperability concerns if the application needs to be used by an infrastructure that was not considered when the application was first developed.

Multiple application platforms allow disjoint and diverse functionality to co-exist on a single smart card. This permits the multiple application smart card to be more valuable to the cardholder. In addition, multiple application architectures may allow for innovative new ways to offer goods and services that are both convenient to the cardholder and affordable to the card issuer and/or service provider.

3 Chip Initialization

During the card production phase of card issuance, the personalization of the card occurs in multiple steps, especially for multiple application cards. Phases of personalization over the life cycle of a smart card are known in the industry as:

1. Initialization/pre-personalization
2. Interim personalization
3. Final personalization/activation
4. Post-issuance personalization

3.1 Initialization

Chip initialization itself is a multiple step process in most card personalization systems (CPS) implementations.

The chip manufacturer ships modules with the chip in a "locked" state, so that the smart card chip is only accessible by the card production system using some form of challenge/response authentication protocol.

The steps involved in initialization often include:

1. Unlocking the chip.
2. Instantiating pre-loaded applications to at least an "initialized" life cycle state.
3. Loading additional applications and instantiating those that can be "initialized" for later stage personalization. (Some applications may only be instantiated during the post-issuance phase of personalization.)
4. Loading common static data into all "initialized" applications. (This may be skipped if there is no common data to load.)

3.2 Initialization versus other Phases of Personalization

Initialization usually refers to all steps in the loading of applications, instantiating applications (to make them selectable from the outside world), and loading data that is common to all cards for a given smart card issuance scheme.

All other types of personalization usually involve card-specific information (and possibly functionality) that requires a unique card profile per card to exist.

4 Key Management

Wikipedia defines key management as follows[3]:

> *Key management is the provision made in a cryptography system design that is related to **generation, exchange, storage, safeguarding, use, vetting, and replacement of keys**. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.*
>
> *Successful key management is critical to the security of a cryptosystem. In practice it is arguably the most difficult aspect of cryptography because it **involves system policy, user training, organizational and departmental interactions**, and coordination between all of these elements.*
>
> *These concerns are not limited to cryptographic engineering. K**ey management requires both technical and organizational decisions**, and as a result, some aspects of key management risk being neglected by managers and engineers, out of concern that the problem is technical or managerial, respectively.*

Key management in smart card systems is as critical as in any other system. Just because the smart card is a secure token does not solve the issue of key management. Key management is not simple and requires experience to implement. This training does not provide a complete course on key management, but only highlights what is specific to smart cards.

4.1 Symmetric Keys Used in Smart Card Systems

Symmetric keys are shared between parties and are generally not used when non-repudiation is required in a system. Symmetric keys are parameters provided to symmetric algorithms (such as 3DES or AES), which are used to provide the authentication, integrity and confidentiality security services. Since symmetric keys are shared, when one key is compromised, all of the users of that key must have their key replaced. It is extremely important that a symmetric key is shared by a very limited number of participants in a system (maximum of two, if possible).

The use of a symmetric key in an authentication process allows the establishment of mutual trust between two entities, since each side has the assurance that the other side is using the same key and, as such, is "in on the secret."

Session keys are very often symmetric keys that established between two parties as part of an authentication process (which may involve symmetric as well as asymmetric keys). Session keys only provide confidentiality in the process described by ISO/IEC 7816 as "secure messaging."

4.1.1 Diversification of Symmetric Keys in Smart Cards

Smart card systems are typically very hierarchical (many different cards interfacing with a given service provider), and implement key diversification for symmetric keys. If a random, unique key were assigned to every card, the provider would need to maintain a large database of all of the keys used for all the cards. This approach is technically secure, but creates a burden for the entire system which would have to protect this large central database of all card keys and would not be able to share the database with any terminal in the field. Key diversification uses a "master key" that is known by the service provider and used to create "other keys" using a unique number associated with the card. The card unique key is calculated by the issuing system by combining the master key and a unique number attached to the card (e.g., account number, credential number). The resulting key is loaded and stored securely in the card. Each time this key is used, the service provider will ask the card about its "unique number" and will be able to re-calculate the specific card key using its master key. The master key must still be very well protected, since all cards would have to be re-keyed if the master key were compromised.

[3] http://en.wikipedia.org/wiki/Key_management

4.1.2 Loading Symmetric Keys in Smart Cards

A symmetric key must be kept secret and must never be exposed in clear text at any time. The key should be shared only with trusted entities and transmitted between these entities ciphered by a "key encryption key." The key used to cipher a symmetric key for transport, as well as the key used to authenticate the devices (card and terminal), should both provide a level of security equal or higher than the key being transferred. (See Table 1 for NIST recommendations of key size guidelines.) Keys are identified as "secret material" that must be protected when they are loaded in smart cards.

Security (bits)	Symmetric Algorithm	Hash Algorithm	Minimum Size of Public Keys (in bits)		
			DSA	RSA	ECC
80	-	SHA-1	1024	1024	160
112	3DES	-	2048	2048	224
128	AES-128	SHA-256	3072	3072	256
192	AES-192	SHA-384	7860	7860	384
256	AES-256	SHA-512	15360	15360	512

Table 1. NIST Security Level and Key Size Guidelines

4.1.3 Key Usage Policy in Smart Cards

Symmetric keys do not have certificates indicating their usage policy, but a similar type of protection is enforced by the smart card operating system. When a symmetric key is loaded, it may have a policy attached to the loading message or the operating system may already know the key identifier. The loaded key will then be used either for authentication, integrity checks (through a message authentication code (MAC)) or confidentiality. Even though symmetric keys do not provide non-repudiation in principle, the use of diversified keys can enable trust in authenticity (integrity and certification of origin) of a message "signed" (MAC'ed) by a given card.

4.1.4 Secure Application Modules in Smart Card Applications

When a symmetric key is to be used by more than one point of interaction (e.g., in point-of-sale payment terminals at merchant locations), some applications are using security application module (SAMs) to protect key material in the terminal. The SAM is a smart card provided to the merchant by the service provider; the SAM contains some "master keys" that allows the terminal to interact with cards even in an offline mode. The use of SAMs requires service providers to manage the physical inventory of SAMs in an application (who has what and where) and may be quite expensive. However, SAMs increase application security by early detection of false cards. In systems using SAMs, the smart card generally generates two signatures with two different diversified keys. One signature can be verified by the terminal, the other by the service provider in its back-end system. This mechanism allows the service provider to detect if the "terminal master key" has been compromised.

4.2 Asymmetric Keys Used in Smart Card Systems

Most current smart cards are able to implement the complexity of asymmetric algorithms. Asymmetric algorithms are still executed slower than symmetric algorithms for the same level of security (measured in bit key length), but performance is improving.

4.2.1 Public Key Certificates and Path Validation

Asymmetric keys have two main parts, one public and one private. Both parts have elements in common which are either public or private depending on the details of the implementation of the cryptographic functions. The public part of an asymmetric key needs to be "certified" by the authority which issued the credential. This certificate uses the X.509 standard form and is a digital signature of the public part of the

key including all of its usage policy. The digital signature is executed using a private key of the authority which also has its public key part. This could be signed again by another higher authority, creating a "validation path" up to a signed root authority that everyone has confidence in. The provision and certification of public/private keys are part of a public key infrastructure (PKI). The public key component, along with all of the signatures attached to it, is stored on the smart card and provided to those with authorization.

As with any other secret key, the private part of the key must be protected and kept secret. When non-repudiation is required (for example, for keys used by the smart card to digitally sign data), the public-private key pair can be generated on the card[4] itself, guaranteeing that the private part of the key is never exposed to any other party. Once the key has been generated, the public part of the key is sent to the authority that will create the digital certificate for the key.

4.2.2 Loading Asymmetric Keys in Smart Cards

The private part of a public key must be kept secret and must never be exposed in clear text at any time. If the private key is not generated on the smart card itself (because of the time required for the process), it must be transmitted to the card ciphered by a "key encryption key." As with symmetric keys, the key used to cipher a key for transport, as well as the key used to authenticate the device, should both provide a level of security equal or higher than the key being transferred. (See Table 1 for NIST recommendations of key size guidelines.) Keys are identified as "secret material" that must be protected when they are loaded in smart cards.

4.2.3 Key Usage Policy in Smart Cards

The key usage policy of a public-private key pair is indicated in the certificate, but may also be provided to the smart card by more direct means at the time the key is created and loaded. The smart card operating system will enforce the key usage policy attached to a given key (e.g., used for authentication or signature).

4.2.4 Revocation of Asymmetric Keys

An important property of public key-signed objects is the potential for revocation. This property is the same for smart card keys and public key-signed data objects in cards. Part of the verification process must ensure that the object, the signature, the key or its certifier is not revoked. The methods involved (e.g., certificate revocation lists (CRLs), online certificate status protocol (OCSP) responders) are beyond the scope of this section.

[4] The process of generating public-private key pairs on a card may take minutes. This time typically is not a practical issue for an application since the process is used infrequently.

5 Issuance

It is important to understand what is meant by card issuance. According to the Free Dictionary by Farlex[5], issuance is defined as:

> "The act of providing an item for general use or for official purposes (usually in quantity); "a new issue of stamps;" "the last issue of penicillin was over a month ago."

Synonyms for issuance include: *issuing, issue, supplying, provision.*

A smart card issuer is usually involved in most, if not all, applications that are loaded, instantiated and personalized on behalf of the cardholder.

The foundation of a secure smart card is the issuance system. The three critical elements in issuing and managing a smart card are:

1. Information capture
2. Card production
3. Life cycle management

This section discusses these elements from the perspective of a card issuer that is providing a secure identity credential. While the details differ, similar functions are required for other smart card applications.

5.1 Information Capture

For a secure identity credential, cardholder information must be accurately captured at time of enrollment to ensure the data is:

- Usable for determining eligibility of the enrollee to be issued such a credential
- Accurate for purposes of vetting the identity of the enrollee
- Unique to ensure there are not duplicate entries in the resulting ID system

The type of information that might be captured includes:

- Demographic Information
- Facial image
- Fingerprint image data (used for multiple purposes)
- Other biometric attributes (e.g., iris, hand geometry)
- Immigration and proof of citizenship documentation

5.2 Card Production

The information captured is used to perform eligibility, identity proofing and internal system integrity checks to check for duplicate enrollments.

Assuming that all of these checks result in a "make card" request, the information captured is formatted to reside within the application domain of the smart card. For many systems, this formatting is a data exchange between an identity management system (IDMS) and a smart card management system (SCMS).

Many systems collect a number of "make card" requests based on time or volume (or a combination of both) which results in a "batch" of make card requests. This batch (or several batches depending on the card production architecture) is sent to a card personalization system (CPS) for creating and (in most cases) personalizing the smart card.

[5] http://www.thefreedictionary.com

The CPS is responsible for:

- Personalizing the card with captured information and card applications. This step may involve the creation of key material, X.509 certificates, or other security-related steps required of the application once the card is issued to the cardholder.
- Providing physical level card security, using protective overlays and tamper-evident materials as part of the issued card body.

Card production falls into two broad categories:

- Centralized production environment
- Decentralized (distributed) production environment

There are advantages and disadvantages with either environment. There is no "one best" issuance scenario that will satisfy all requirements of any large scale card issuer. Card issuers often use a hybrid environment where the decision to use centralized or decentralized production is based more on business rules than on available technology.

5.3 Life Cycle Management

Once a card is issued to a cardholder, the card issuer takes on the responsibility of managing the smart card for the duration of that card's service life. Depending on the application(s) on the smart card, the card issuer, through one or more card reader infrastructures, may need to "touch" the card from time to time. Reasons for needing to manage a smart card after issuance include:

- A need to change or reset a personal identification number (PIN)
- A need to block or unblock an application (e.g., a payment application) based on business rules and cardholder behavior
- A need to refresh key material or certificates associated with private keys
- A need to update demographic or service data held in an application on the smart card
- A need to update or replace an application
- A need to cancel a card by either deleting applications or setting configuration data that allows detection that a card has been cancelled.

Interacting with the smart card after it has been issued is known as post-issuance personalization. The primary component that facilitates post-issuance personalization is the SCMS (and connectivity to one or more infrastructures that allow a card-to-SCMS connection).

6 Card Life Cycle Management[6]

In any card system, roles and responsibilities must be assigned and policies and procedures developed for all facets of card and application management. The general card life cycle stages are very similar regardless of the industry segment, and include card procurement, inventory control, personalization, card issuance, card replacement, and application management. The security and the application management stages will vary by industry. These stages vary by: when and how industry-specific security approaches are applied to the application; when the application is loaded to the chip and when it is activated or instantiated and thus ready for personalization. These steps will be covered further in this section.

The three phases in the life cycle management of a smart card program that must be considered in the card management process are pre-issuance, issuance and post-issuance. Recommended card management functions for issuers implementing a smart identification card platform are described in this section.

This section describes each of the common life cycle stages for a *secure* card system, as opposed to a card system where card stock security is not a primary concern. In addition, areas that commonly vary by industry segment are indicated and the type of variation briefly described.

6.1 Card Procurement

The card issuer may procure cards from one or more card manufacturers and the chip that is embedded in the card body may also be from one or more chip suppliers. It is to the issuer's advantage to remain vendor-neutral with respect to the card and chip supplier to obtain competitive pricing. Vendor neutrality is possible due to the evolution of standards in the smart card industry and the adoption of open platform operating systems or implementing proprietary operating systems that follow a standard personalization process for the specific industry application.

The selection of the chip operating system has an impact on the operation specifics of other life cycle stages. If undecided, the issuer could work with consultants, the card manufacturer or a system integrator to identify the card operating system that best fits the issuer's needs. Certain industry segments pre-certify card operating systems and chip applications before they are made available for purchase. Card procurement will occur during all phases of smart card program life cycle.

6.2 Card Initialization

Initialization can have multiple meanings and it is always best to confirm each party's definition when discussing it. In this section, initialization is presented from the perspective of both the chip manufacturer and a card manufacturer. From the perspective of a chip manufacturer, initialization is the process of programming chips in a batch of cards with identical data for each card (e.g., writing a file structure or loading a payment application on the chip). During the card initialization process, the card manufacturer can perform functions such as:

- Loading the operating system into ROM;
- Loading chip applications into ROM;
- Allocating memory zones on the chip when using proprietary (native) operating systems (e.g., for photo, for digital signature);
- Loading the unique card serial number into ROM;
- Loading or initiating security keys; and
- Performing other card initialization tasks as requested by the issuer.

Most security-minded smart card systems have a transport key loaded into the chip to secure the transport of cards from the card manufacturer to the final customer. This is one of the leading advantages to smart card adoption. Card inventories can be secured for transport and storage until they

[6] Source: Government Smart Card Handbook, with additional contributions from Guy Berg.

are issued to the final cardholder. In a best practices implementation, a secure key is shared between the sender and the receiver of the cards in each stage.

Initialization from the card manufacturer's perspective may also include printing identical information, such as a logo or secure hologram on a batch of cards. This step is usually performed by the card manufacturer prior to card shipment, but can also be performed at the same time as personalization during card issuance for some industry segments like identification cards or mass transit cards. The adoption of higher quality and more secure instant printing technology now enables edge-to-edge printing of secure cards at the time of issuance. This approach is becoming more popular even for bank debit cards.

Historically card graphics have been preprinted by the card manufacturer and this procedure continues to be the most prevalent where large volumes of cards are involved and when secure holograms or other security print features are required. In recent years, printing approaches have evolved so that the secure elements are mass printed and the remaining graphics are printed at the time of personalization.

6.3 Card Personalization

Personalization occurs at the end of the manufacturing process and is the process of printing data on the surface of the card, encoding the magnetic stripe on the card (if applicable), and programming data into the chip that will uniquely associate the cardholder to the smart card. Issuers may employ different approaches to obtain data for the card personalization process, depending upon the requirements of each industry segment and individual issuer requirements. Downloads from existing legacy systems, web-based applications to collect data, or employee interviews are examples of techniques that may be used to obtain necessary card personalization data.

The data preparation for personalization and the manner of synchronizing the personalization data with the master cardholder system varies substantially by industry segment because of business workflow requirements for enrolling new cardholders. In the credit card industry, enrollment and credit assessment are performed prior to card personalization and data is passed to either instant or batch personalization processes after the master cardholder system is updated. In the identity industry and others, the sequence can be very different.

Once the information is collected, interfaces may be built to efficiently enter the data into a master or legacy database. An automated interface to the master system reduces the potential for manual errors. Security is also a factor to be considered, as the secure transmission of data is critical, particularly if automated interfaces will be used to transport card personalization data from master or legacy databases. Encryption may be used to protect sensitive data transmitted across open networks. For example, in the credit and debit card industry, PCI compliance requires sensitive cardholder data to be encrypted when stored for any length of time and when transported from one entity to another.

Depending on the applications to be supported by the card, the personalization processes may include some combination of the following:

- Encoding the magnetic stripe;
- Encoding the bar code;
- Loading application software, basic demographic information and/or keys on the chip;
- Printing card graphics;
- Printing a photo and signature image on the card;
- Printing demographic data on the card; and
- Printing other issuer-specific information on the card.

As part of the enrollment and card personalization process, the card issuer will perform some combination of the following functions depending on the specific industry segment, capabilities and implementation strategies required by individual issuers:

- Capture the digital photograph of the cardholder using a photo imaging system;
- Capture the digitized signature of the cardholder using a signature capture device;

- Capture the biometric of the cardholder using a biometric capture device;
- Capture demographic data to be maintained in the cardholder database and write this demographic data to the chip; and
- Populate the card with digital and attribute (i.e., biometric) certificates.

The personalization process can be performed at central personalization service bureaus or upon demand at distributed locations for instant issuance. The business needs and enrollment requirements of each industry segment determines when and where the personalization process is performed.

6.4 Card Issuance

The process of distributing personalized cards to cardholders is called card issuance. The specific timing and method of card distribution varies widely across industry segments. In most cases, both card personalization and issuance are performed at the same time. In other cases, there can be a final personalization or activation even after card distribution. The issuer's organizational structure and the business requirements of the smart card program determine if the cards are personalized at a central location to support mass card distribution, issued at distributed locations, or instantly issued.

Prior to authorizing the issuance of a card, the potential cardholder may be required to fulfill industry-specific identify verification and enrollment assessment procedures. These requirements may include presenting documentation that verifies identity and employment status, that can be compared to an issuer's personnel database, or that can used to execute a credit assessment. In some industries, an additional security measure is taken where the issuer compares the presented enrollment application with a picture and/or biometric that has previously been collected and stored in a personnel database.

The applications that will be loaded onto the smart card will vary depending on the industry segment and by cardholder role and responsibilities. For example, when a smart card is used as an employee ID card, all cardholders may have an application that allows secure physical access to the employers facilities. Not all employees, however, will require an application that supports digital signatures. In this case, the card personalization, issuance, and management solutions should provide the capability to capture and maintain records on the privileges associated with each employee's card.

6.5 Card Replacement

The card replacement process is used to provide replacement cards to individuals reporting a lost, stolen or a malfunctioning card. When a card is reported to be lost, stolen, or malfunctioning, the issuer will deactivate the card by revoking the certificates or blocking applications on the card and by placing it on a list of invalid cards (also known as a "hot list"). Typically, card deactivation is logged at a central host system to prevent future unauthorized use of the card. In some cases, an application block command can be sent out to the readers where the cards are used. For example, in the payments industry, an EMV application that is on a payment card can be locked the next time a card authorization is attempted by a POS terminal or an ATM.

When a replacement card is issued, it must be an exact duplicate of the card that was lost, and thus carry all of the privileges, data, applications and system access keys that resided on the original card that is being replaced. It should also indicate that it is a replacement card. Typically, the card issuer takes responsibility for the replacement process. The card replacement process includes:

- Procedures for re-issuance;
- Procedures for identifying the state of the application(s) on the card at the time it was lost;
- Procedures for checking hot-listed cards;
- Procedures for revoking certificates or blocking applications on the lost card;
- Time frame for hot-listed cards being deactivated in the card database;
- Personnel responsible for locking and unlocking cards;

- Procedures for removing hot-listed cards from the list;
- Procedures for generating new keys or biometric templates if the card has digital or attribute certificates;
- Time frame for reissuance and reactivation of cards; and
- Procedures for restoring value if the card has an electronic purse.

6.6 Card Block/Unblock

When a card is reported as lost or stolen, it must be deactivated to ensure that an unauthorized individual cannot use the card. The card issuer should have the capability to hot list any card that has been reported as lost, stolen or malfunctioning and to revoke certificates, block the application, or even lock the card. Additionally, other organizations who have an application on the card or other issuers that could grant access privileges to cardholders on the hot list should receive immediate notification of the deactivated card(s).

The ability to unblock cards or applications is required as a customer service function. At times, cards or applications on the cards will be locked as a result of someone forgetting their PIN, entering an invalid PIN, or possibly having other exception situations that may be caused from an unusual sequence of events. It is difficult to anticipate all of the possible reasons that a card, application or PIN could get locked, so issuers must take into consideration the ability to perform each of the relevant functions post-issuance.

6.7 PIN Reset

The cardholder must have the ability to securely reset the card PIN without requiring the cardholder to return to a smart card issuance facility. Depending on the deployment strategy, the mechanism to deploy a PIN reset solution may vary. One option may be a graphical user interface (GUI) to the system that allows a user to change the PIN by providing the old PIN for authentication and then the system allows a new PIN to be established. Another approach may be a web-based portal in the card management system; using this approach, the user can authenticate to the web site and then navigate to a PIN reset screen where the old PIN is required and validated using the rules set on the smart card during the chip personalization process. Ultimately, issuers must determine the best method to service cardholders to ensure customer convenience and satisfaction.

6.8 Certificate Management

One or more certificates can be carried on a smart card and used as a specific security application, or certificates can be used as part of overall application security. If certificates are placed on a smart card, they must be managed. Certificate management is both an issuance and post-issuance function in most, if not all, smart card systems that use them.

Certificates use public key infrastructure (PKI) technology to encrypt and sign data to create certificates in such a manner that another device reading the card can verify the authenticity of the certificate. PKI technology can be used by organizations to build ways to develop trust in electronic transactions and rely on digital signatures. The certificate authority or certification authority (typically called a CA) brings together two parties who may have never met and uses public key technology to facilitate digital business transactions. The CA helps to build confidence in transactions by acting as a well-known, trusted third party that vouches for the authenticity of a public key.

In the payment card industry, Visa, MasterCard, American Express and Discover all have a CA and use it to support EMV card issuance. For secure identity cards, there can be an issuer-specific or industry-wide certificate authority. In either case, the CA maintains the PKI certificates and keys that are injected into the smart card from the issuance system. The CA constructs, signs, and publishes a digital certificate using the CA's private key. The digital certificate is an electronic credential that can be used to verify another issuer, verify a person's signature, encrypt documents, and protect the integrity of the

transaction. In order to construct the digital certificate, the CA must identify the card issuer or person, verify that the card issuer or person possesses the associated private key, and know other information about the card issuer or person that is required to construct the certificate.

Once cards are issued with certificates on them, the certificates need to be managed to maintain integrity. This is frequently referred to as post-issuance card or certificate management. In certain industry segments like the secure identity industry, cardholders must have the ability to request new or updated certificates after the initial issuance in the event that: the CAs were unavailable at initial issuance; the card recipient did not have an email address at initial issuance; or the card recipient's email address has changed after initial issuance. Certificates also have projected viability dates based on the length of the key used to create the certificate (which affects the strength of security). As a result, the credit card payments brands have identified specific dates when issued cards will need a new certificate based on a longer key.

In summary, certificates are widely used in conjunction with smart card technology across industry segments. For certificates to be used effectively, they must have their own life cycle that is closely managed by a root certificate authority.

6.9 Key Management

Key management is an integral and significant part of smart card and application security. Key management is the procedure to control key generation, key storage, key distribution, key usage, and key destruction. Anyone planning to implement a smart card program should have the resources available to ensure a complete and thorough understanding of card and application keys. It is important to understand how keys will be used, especially if the card system plans to work with more than one organization or entity. Keys hold the secret to the system. If not managed properly, the integrity of the entire system can become compromised.

Smart card systems typically have either a tightly or loosely integrated key management system (KMS). A KMS is an application that is used for generating and maintaining cryptographic keys. The keys managed by a KMS can be used for encrypting other keys and data to protect them during the personalization process or used for accessing the card's memory and applications. The manner in which the KMS interacts with the rest of the card eco-system varies substantially by industry. In the payments industry, the KMS imports or exports keys with the card manufacturer, the payment brand CA, the data preparation system, the final personalization bureau, and the issuer's authorization system.

During the chip manufacturing initialization phase of card life cycle management, the chip manufacturer assigns a key or keys to the chip. These keys are used as access keys to the chip memory to secure them during transport and are frequently referred to as the transport keys. These keys are generally changed each time that another entity takes possession. In addition, at other life cycle stages such as the card manufacturing or personalization stages, application keys are loaded to the chip. In summary, from the time that a chip is prepared for shipping to a card manufacturer until the time that it is issued/distributed to the cardholder, each stage has a key management requirement and each entity should have a secure and robust key management system.

The types of keys incorporated in a smart card-based system vary according to the operating system selected and the application or applications to be loaded on the card. Each card application typically has very different requirements for keys and certificates. As mentioned in Section 6.8, Certificate Management, certificates can be an integrated component of an application or a certificate can be a form of identity used by identity systems. The different types of certificates are typically managed by different CA systems, but they can be managed at the cardholder level by the same cardholder system if both types are implemented on a single card.

Key management is one of the functions that must be continued after the card has been issued to provide a method for updating the application keys, replacing PKI certificates , regenerating the PKI signature and encryption key pairs, and allowing PIN resets.

6.10 Cardholder Database Management

The issuer should maintain an archive of all cards issued. This record should link the card serial number or unique identifier to the cardholder and maintain a record of the state of the card. The state of the card includes: the operating system and its version; the applications and their versions; certificates; photos and all other data required to meet the need for issuing an identical replacement card. This will allow a replacement card to be issued containing all initially authorized privileges and data in the event that the cardholder's card is lost or stolen or malfunctions.

6.11 Card Inventory Control

Smart card stock should be maintained in a secure environment. The card issuer records the serial numbers of cards received in inventory, as defined by the issuer's pre-issuance specification. Cards must be stored in a secure location with access limited to authorized individuals.

The card manufacturer is generally responsible for all cards until they are delivered to or accepted by the issuer at designated card issuance locations. Issuers must have the ability to track card inventory levels and control their availability. This is true for central issuance bureaus and distributed instant issuance system locations. Each day cards should be checked in and out of inventory under dual access and review requirements. In addition, the card issuer should be responsible for the following:

- Recording serial numbers and/or card counts received into inventory and issued from inventory;
- Monitoring inventory levels and requesting additional card stock from the card manufacturer or the central inventory of cards;
- Processing returned or damaged cards for inventory log update and chip failure testing;
- Maintaining a card database that details the number of cards issued weekly, monthly and annually by the issuer or the instant issuance location and printer; and
- Monitoring and logging card surface personalization and electrical personalization failures and exception processes.

During the card life cycle, inventory information can be transmitted from the manufacture's system to the issuer's system. The card inventory system can be incorporated into the card management system. This will allow the creation of business reports for additional card requirements and for card manufacturers to ship directly to the site where the cards are required. Other card inventory approaches can also be negotiated between the manufacturer and the issuer.

6.12 Cardholder Services

The card issuer must provide customer service support for the smart card platform. Typically, a help desk is established that provides a toll-free number for cardholder's inquiries. To serve cardholders, the card issuer should provide an automated response unit (ARU), in addition to customer service representatives. Anticipated client customer services via either the ARU or a customer service representative include:

- Reporting a lost, stolen, damaged, or inoperative card;
- Reporting a malfunctioning card;
- Reporting unauthorized card use or other breach of security;
- Reporting an update in demographic data (e.g., name change, change of address);
- Providing information support for card applications and services; and
- Ordering card replacements.

Additionally, the issuer will need cardholder training materials for the following topics:

- Basic card usage;

- Card application usage;
- Card security and key protection procedures; and
- Privacy safeguards.

7 Relevant Standards and Specifications

Numerous standards are relevant to smart card applications and more are created every year. They have various impacts at different levels of a smart card based-system and may deal with physical characteristics, security certifications, transmission protocols, and application loading or design. There are also industry "specifications," which are not "standards," but which play a very important role in smart card applications. Application specifications are not listed in this section; only those which are available for all applications (e.g., Java Card or GlobalPlatform) are listed.

The following should be noted:

1. Some standards listed below are available free of charge, but many must be purchased.
2. Some standards may not be listed in this section, but could be relevant to a specific application or a specific technique required by an implementation (e.g., standardized format of a biometric information).

This section contains a list of standards and specifications relating to this module. A more complete listing of standards and specifications, with descriptions of each, can be found in Module 1.

7.1 Standards Relevant to Smart Card Physical Characteristics

- ISO/IEC 7810 – Identification Cards – Physical Characteristics
- ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards[7]
- ISO/IEC 10373 – Identification Cards – Test Methods
- ISO/IEC 24789 – Identification Cards – Card Service Life

7.2 Standards Relevant to Technologies Which Could Be Found on a Smart Card

Smart cards often include other technologies in the card body. The following standards apply to common technologies:

- Magnetic stripes: ISO/IEC 7811 series, Identification cards – Recording technique
- Linear bar codes: ISO/IEC 15416 Information technology – Automatic identification and data capture techniques – Bar code print quality test specification – Linear symbols
- PDF417 bar code: ISO/IEC 15438 Information technology – Automatic identification and data capture techniques – PDF417 bar code symbology specification
- Optical memory cards: ISO/IEC 11693 Identification cards – Optical memory cards; ISO/IEC 11694 Identification cards – Optical memory cards - linear recording method

7.3 Standards and Specifications Relevant to Technologies the Card Interface

- ISO/IEC 7816 Series – Identification Cards – Integrated Circuit(s) Cards with Contacts
- ISO/IEC 14443 Series – Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards
- ISO/IEC 15693 – Contactless Integrated Circuit Cards – Vicinity Cards
- ISO/IEC 18092 – Information Technology – Telecommunications and Information Exchange between Systems – Near Field Communication – Interface and Protocol

[7] Source: http://www.iso.org

7.4 Standards and Specifications Relevant to the Card Commands and Application Data Structures

- ISO/IEC 7816 Series – Identification Cards – Integrated Circuit(s) Cards with Contacts
- GlobalPlatform[8]
- Java Card[9]

7.5 Standards and Specifications Relevant to Security or Cryptography

- ISO/IEC 9798 - Information Technology – Security Techniques – Entity Authentication
- ISO/IEC 11770 - Information Technology – Security Techniques – Key Management
- ISO/IEC 18033 - Information Technology – Security Techniques – Encryption Algorithms
- ISO/IEC 24787 - Information Technology – Identification Cards – On-Card Biometric Comparison

7.6 Standards and Specifications Relevant to Issuers or Specific Industry Sectors

- ISO/IEC 7501 Series, Identification Cards – Machine Readable Travel Documents
- ISO/IEC 7812 Series, Identification Cards – Identification of Issuers
- ISO/IEC 7813, Identification Cards – Financial Transaction Cards
- ISO/IEC 7816 Series, Identification Cards – Integrated Circuit(s) Cards with Contacts
- ISO 9992 – Financial Transaction Cards – Messages between the Integrated Circuit Card and the Card Accepting Device
- ISO/IEC 18013 – Personal Identification — ISO Compliant Driving License
- ISO/IEC 21549 - Health Informatics — Patient Health Card Data
- Doc 9303, ICAO Machine Readable Travel Documents
- ETSI TS 100 977: "Digital Cellular Telecommunications System (Phase 2+) (GSM)
- Comité Européen de Normalisation Technical Committee TC 224: CEM 15480 Identification Card Systems - European Citizen Card
- EMV - Integrated Circuit Card Specifications for Payment Systems
- Contactless Fare Media Standard

7.7 Other Standards Related to Smart Cards or their Software Clients

- ISO/IEC 24727 Identification Cards – Integrated Circuit Card Programming Interfaces

7.8 Primary U.S. Standards and Specifications Related to Smart Cards – Federal Information Processing Standards (FIPS)

- FIPS Standards for Digital Signatures

[8] GlobalPlatform specifications are available at http://www.globalplatform.org/specifications.asp
[9] Java Card specifications are available at http://java.sun.com/javacard/3.0.1/specs.jsp

- FIPS 186-2 Digital Security Standard specifies a set of algorithms used to generate and verify digital signatures. This specification relates to three algorithms specifically, the Digital Signature Algorithm (DSA), the RSA digital signature algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA).
- ANSI X9.31-1998 contains specifications for the RSA signature algorithm. The standard specifically covers both the manual and automated management of keying material using both asymmetric and symmetric key cryptography for the wholesale financial services industry[5].
- ANSI X9.62-1998 contains specifications for the ECDSA signature algorithm.

- FIPS Standards for Digital Encryption
  - FIPS 197 Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.
- FIPS 140 (1-3) Security Requirements for Cryptographic Modules Standard
- FIPS 201 Personal Identity Verification of Federal Employees and Contractors

8 References

Government Smart Card Handbook, General Services Administration, February 2003

ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards

Java Card specifications, available at http://java.sun.com/javacard/specs.html

MULTOS specifications, available at http://www.multos.com

.NET smart card specifications, http://www.gemalto.com/dwnld/5763_Gemalto.NET_User_Guide.pdf

Smart Cards, Tokens, Security and Applications, by Keith Mayes (editor) and Konstantinos Markantonakis (editor), Springer, 2008

9 Acknowledgements

This document was developed by the Smart Card Alliance for the Certified Smart Card Industry Professional (CSCIP) program. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance thanks **Bryan Ichikawa, Unisys**, for review of this CSCIP module.

The Smart Card Alliance thanks **Gilles Lisimaque, Identification Technology Partners** for developing content for Section 4, *Key Management*, and Section 7, *Relevant Standards*, **Gerald Smith, Identification Technology Partners** for developing content for Section 2, *Single and Multiple Application Cards*, Section 3, *Chip Initialization*, and Section 5, *Issuance*, and **Guy Berg** for providing content for Section 6, *Card Life Cycle Management*.

The Smart Card Alliance wishes to acknowledge the **GSA** for the content from the *Government Smart Card Handbook* used in Section 6 of this module.

About LEAP and the CSCIP Program

The Smart Card Alliance Leadership, Education and Advancement Program (LEAP) was formed to: offer a new individual members-only organization for smart card professional; advance education and professional development for individuals working in the smart card industry; manage and confer, based on a standardized body-of-knowledge examination, the Certified Smart Card Industry Professional (CSCIP) designation.

LEAP members who wish to achieve certification as experts in smart card technology may do so at any time. Certification requires that LEAP members meet specific educational and professional criteria prior to acceptance into the certification program.

A series of educational modules forming the CSCIP certification body of knowledge has been developed by leading smart card industry professionals and is updated regularly. These educational modules prepare applicants for the multi-part CSCIP exam administered by the Smart Card Alliance. The exam requires demonstrated proficiency in a broad body of industry knowledge, as opposed to expertise in specialized smart card disciplines. Applicants must receive a passing grade on all parts of the exam to receive the CSCIP certification.

LEAP membership in good standing is required to sustain the certification, and documentation of a required level of continuing education activities must be submitted every three years for CSCIP re-certification.

Additional information on LEAP and the CSCIP accreditation program can be found at http://www.smartcardalliance.org.

Trademark Notice