

EMV

Issuer Security Guidelines

EMVCo, LLC

Draft Version 0.5
October 31, 2000

Copyright 2000 © EMVCo. LLC. All rights reserved

© 2000 EMVCo, LLC ("EMVCo"). All rights reserved. Any and all uses of the EMV 2000 Specifications ("Materials") shall be permitted only pursuant to the terms and conditions of the license agreement between the user and EMVCo found at <http://www.emvco.com/specifications.cfm>

The specifications, standards and methods set forth in these Materials have not been finalized or adopted by EMVCo and should be viewed as "work-in-process" subject to change at anytime without notice. EMVCo makes no assurances that any future version of these Materials or any version of the EMV Specifications will be compatible with these Materials. No party should detrimentally rely on this draft document or the contents thereof, nor shall EMVCo be liable for any such reliance.

These Materials are being provided for the sole purpose of evaluation and comment by the person or entity which downloads the Materials from the EMVCo web site ("User"). The Materials may not be copied or disseminated to any third parties, [except that permission is granted to internally disseminate copies within the organization of the User]. Any copy of any part of the Materials must bear this legend in full.

These Materials and all of the content contained herein are provided "AS IS" "WHERE IS" and "WITH ALL FAULTS" and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these materials. MATERIALS AND INFORMATION PROVIDED BY EMVCO ARE NOT FINAL AND MAY BE AMENDED AT EMVCO'S SOLE OPTION. EMVCO MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE MATERIALS AND INFORMATION CONTAINED HEREIN. EMVCO SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE.

EMVCo makes no representation or warranty with respect to intellectual property rights of any third parties in or in relation to the Materials. EMVCo undertakes no responsibility of any kind to determine whether any particular physical implementation of any part of these Materials may violate, infringe, or otherwise use the patents, copyrights, trademarks, trade secrets, know-how, and/or other intellectual property rights of third parties, and thus any person who implements any part of these Materials should consult an intellectual property attorney before any such implementation. WITHOUT LIMITATION, EMVCO SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO INTELLECTUAL PROPERTY SUBSISTING IN OR RELATING TO THESE MATERIALS OR ANY PART THEREOF, INCLUDING BUT NOT LIMITED TO ANY AND ALL IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT OR SUITABILITY FOR ANY PURPOSE (WHETHER OR NOT EMVCO HAS BEEN ADVISED, HAS REASON TO KNOW, OR IS OTHERWISE IN FACT AWARE OF ANY INFORMATION).

Without limitation to the foregoing, the Materials provide for the use of public key encryption technology, which is the subject matter of patents in several countries. Any party seeking to implement these Materials is solely responsible for determining whether their activities require a license to any technology including, but not limited to, patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights.

1 Scope

As in the magnetic stripe world, the IC card issuer is liable for both the accuracy and the protection of the data used in the personalization of its cards. Such data includes, in addition to the cardholder and account information, cryptographic keys and other cardholder secrets, that if revealed to unauthorized parties, could result in the creation of counterfeit cards and fraudulent transactions. To protect against the unauthorized disclosure of this information, Issuers must create and manage these types of data in a secure environment. Such an environment is one where the appropriate physical and logical security controls have been implemented and where sufficient audit trails have been established to assure procedural consistence relative to the security objectives.

The materials contained in this document define methods for the secure management of sensitive data used in the implementation of EMV compliant payment applications. The methods discussed include the management of cryptographic keys and guidelines for the protection of the cardholder data. The principles presented in the following pages are applicable to all phases for card personalization, authorization, and transactional clearing. Where Issuers use third party agents to perform these functions, the same principles are also applicable. Application of these principles may also be useful for other payment applications that require and use similar sensitive data.

2 Normative References

Europay, MasterCard, and Visa (EMV) May 31, 2000	Integrated Circuit Card Applications Specification for Payment Systems
Europay, MasterCard, and Visa (EMV) May 31, 2000	Integrated Circuit Card Terminal Specification for Payment Systems
ISO/IEC 10118-3	Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions
Federal Information Processing Standard (FIPS) 140-2: 1999	Requirements for Secure Cryptographic Modules
ISO/IEC 8731-1: 1987	Banking - Approved algorithms for message Authentication
ISO/IEC 10116	Information technology – Security techniques – Modes of operation for an n -bit block cipher
ISO/IEC 9564-1: 1997	Banking – Personal identification number management and security
ISO/IEC 11568-1:1994	Banking – Key management (retail) - Part 1:Introduction to key management
ISO/IEC 11568-2:1994	Banking – Key management (retail) - Part 2:Key management techniques for symmetric ciphers
ISO/IEC 11568-3:1994	Banking – Key management (retail) - Part 3 Banking - Key management (retail) - Key life cycle for symmetric ciphers
ISO/IEC 11568-4:1994	Banking – Key management (retail) - Part 4:Key management techniques for public key cryptosystems
ISO/IEC 11568-5:1994	Banking – Key management (retail) - Part 5:Key life cycle for public key cryptosystems
ISO/IEC 11568-6:1994	Banking – Key management (retail) - Part 6:Key management schemes
ISO/IEC 13491-1:1998	Banking – Secure Cryptographic Devices (retail)

3 Definitions

Term	Definition
Audit Trail	A record of system activities, which is sufficient to enable the reconstruction, review, and/or examination of the sequence of events/activities leading to an event.
Authentication	A cryptographic process that validates the identity and integrity of data.
Certificate (public key)	The public key and the identity of an entity together with some other information, made unforgeable by the signing of the certificate with the private key of the certification authority issuing the certificate.
Certification Authority	The entity that is trusted by one or more other entities to create and assign certificates.
Cryptographic Algorithm	A set of rules, setting forth procedures necessary to protect data, e.g. to perform encipherment and decipherment of data. The algorithm is specified in a manner that it is not possible to determine any of the secret control parameters; i.e., the secret or private key, except by exhaustive search.

Term	Definition
Cryptographic Hash Function	<p>A function, which maps values for a large domain into a smaller one. The function satisfies the following properties:</p> <ol style="list-style-type: none"><li data-bbox="695 415 1395 491">1. It is computationally infeasible to find for a given output, an input that maps to this output.<li data-bbox="695 527 1395 632">2. It is computationally infeasible to find for a given input, a second input that maps to the same output.
Cryptographic Key (Key)	<p>A parameter that defines the operation of a cryptographic algorithm.</p>
Cryptography	<p>The process which transforms data in order to guarantee its origin, conceal its information content, prevent its undetected modification, prevent its unauthorized use, prevent its repudiation, or any combination of the above.</p>
Cryptoperiod	<p>The period of time during which a specific key is authorized for use or in which the key(s) for a given system remain in effect.</p>
Digital Signature	<p>The cryptographic transformation of data which, when properly implemented, provides:</p> <ol style="list-style-type: none"><li data-bbox="695 1409 1013 1444">1. origin authentication,<li data-bbox="695 1444 971 1480">2. data integrity, and<li data-bbox="695 1480 1036 1516">3. signer non-repudiation.
Dual Control	<p>The process of utilizing two or more separate entities to protect sensitive information or functions, such that no single entity is able to access or utilize the information or functions.</p>
Exclusive-OR	<p>See Modulo-2 addition.</p>

Term	Definition
Hash Value	The result of applying a cryptographic hash function to a message.
IC Card	A card with an embedded chip that communicates information to a point of transaction terminal.
Key Component	One of at least two parameters having the characteristics of randomness and format of a cryptographic key that is combined with one or more like parameters, forming the cryptographic key.
Key Pair	When used in public key cryptography, a public key and its corresponding private key.
Key Space	A set of all possible keys used by a cryptographic algorithm.
Keying Material	The data (e.g. keys, certificates, initialization vectors) necessary to establish and maintain cryptographic keying data.
Modulo-2 Addition	<p>Exclusive -OR, XOR. Binary addition with no carry, defined as follows:</p> $0+0 = 0$ $0+1 = 1$ $1+0 = 1$ $1+1 = 0$
Payment System	A payment system includes a number of participants where the Issuer and the Acquirer distribute liabilities amongst the different parties according to scheme rules and according to the allocation of risks.

Term	Definition
Physically Secure Device	A module that has a negligible probability of entry without detection or erasure of its contents.
Private Key	In an asymmetric algorithm (public key) cryptosystem, the key of an entity's key pair that is known only to that entity.
Private Prime Factors	In the RSA algorithm, the two large prime numbers, namely p and q , whose product is the modulus, $pq = n$.
Pseudo-random	A process that is statistically random and essentially unpredictable although generated by an algorithmic process.
Public Key	In an asymmetric key system, the key of an entity that is publicly known.
Secret Key	A key that is used in a symmetric cryptographic algorithm and cannot be disclosed publicly without compromising the security of the system. This is not the same as the <i>private</i> key in a public/private key pair.
Secure Cryptographic Device	A device that provides secure storage for secret information such as keys and provides security services based on this secret information.
Split Knowledge	A condition whereby two or more parties; i.e., key custodians, separately and confidentially have custodial control of a constituent part of a cryptographic key that individually conveys no knowledge of the resultant cryptographic key.

4 Cryptography - Overview

4.1 Background

Cryptography is a technology that is widely used in smart card applications. Historically, cryptography has been used to provide data confidentiality. The increasing roles of computers, networking, and the digital economy have expanded the role of cryptography to include other cryptographic services such as data integrity, entity authentication, and non-repudiation. As the role of these various cryptographic services increased so did the need for increased standardization to assure both inter-operability of products and services between different vendors and various implementations. The materials contained in the following pages represent the best practices drawn from these different standards.

The key management principles set forth below are applicable to all situations where cryptographic keys are used for the personalization of cards, the management of authentication protocols, and the clearing of transactions. These principles are based on the international standards cited in the references section above.

4.2 Cryptographic Basics

Modern cryptography depends on two basic components, (1) the algorithm, and (2) the cryptographic key. The algorithm defines how ciphertext is obtained from the plaintext and vice versa (in the case of encryption algorithms) and defines how signatures are both derived from data and verified (in the case of digital signature algorithms). The cryptographic key, which is typically a sequence of bits, is used as input to the algorithm and ensures that knowledge of the algorithm does not enable unauthorized parties to decrypt sensitive data or forge other parties' digital signatures.

The security of modern cryptography depends on public access to the algorithm and the secrecy of the cryptographic key(s). Algorithms are typically published and have been extensively studied by cryptographers. The DES algorithm for example, has been published in various standards and other documents. The RSA algorithm is based on widely known mathematical principles. The operational security of these different cryptographic algorithms depends entirely on how well the secret and private keys have been managed over their active life.

There are two basic types of cryptographic algorithms, (1) symmetric or secret key algorithms, and (2) asymmetric or public/private key algorithms.

4.2.1 Symmetric Algorithms

'Symmetric' or 'secret key' algorithms require that the secret key used for the encryption process also be used in the decryption process. Therefore, the security of the algorithm depends entirely on protection of this secret key.

The EMV application requires the use of the Data Encryption Standard (DES), an example of a symmetric algorithm. This algorithm is widely used in the financial services industry today. DES belongs to the family of encryption algorithms called "block" ciphers because they process data in blocks. The DES algorithm takes an input block of 64-bits and maps it to a 64-bit output block, using a 56-bit key in an iterative process of sixteen rounds.

All references in the text of this document regarding the use of the DES algorithm are to be read as references to the use of 'triple DES', in which a single DES encryption is replaced with three DES operations. Similarly, references to DES keys are to be read as pairs of DES keys, as used in conjunction with triple DES.

4.2.2 Asymmetric Algorithms

Members of a second family of cryptographic algorithms are referred to as "asymmetric" or "public/private" key algorithms. This group of algorithms requires the communicating endpoints to use two keys each; a "public" key and a "private" key. For the purposes of confidentiality the "public" key of the sending entity is used to encipher data and the "private" key of the receiving entity is used to decipher the message.

Asymmetric algorithms are used by EMV to create digital signatures. In a digital signature scheme the private key is used to derive a signature from a message and the public key is used to verify the signature.

5 Functional overview

5.1 Introduction

The purpose of this functional overview is to provide a framework for the Issuer security guidelines. A payment system model is provided, and the roles of the entities within the model are outlined. The key management architecture underlying the EMV card authentication process is then described. This is followed by a specification of the main security processes that need to be performed by an EMV Card Issuer.

5.2 Payment System Model

The Payment System will consist of the following types of entity:

- Cardholders,
- Merchants,
- Issuers,
- Acquirers, and
- Schemes (i.e. Payment System brands, including Eurocard/MasterCard and Visa).

The main role of each of these entities is as follows.

5.2.1 The Cardholder

The role of the Cardholder includes the following:

- To obtain a chip card containing the payment product application by contracting with an Issuer.
- To choose, remember and possibly update his/her PIN.
- To present his/her chip card to devices accepting the payment product for payment (ATM, Merchant POS, vending machines, payphones, etc.).

5.2.2 The Merchant

The role of the Merchant includes the following:

- To obtain Terminals accepting payments with the payment product(s) on an IC Card by contracting with an Acquirer.

- To accept chip cards containing the payment product(s) for payment.
- To obtain reimbursement for the purchase transactions by collecting and transmitting them from his Terminal(s) to the Acquirer.

5.2.3 The Issuer

The role of the Issuer includes the following:

- To certify to the Scheme that every chip card issued bearing the application logo complies with the application system specified rules.
- To contract with, and to personalize and issue a chip card containing the application to the Cardholder. This includes the installation of the necessary cryptographic keys in the card to support the application.
- To securely transmit to any other parties the necessary cryptographic keys needed for the correct operation of the system.
- To manage and protect the integrity of the Public Key(s) supplied by the Scheme (as part of the provision of secure storage for keying material).
- To accept and process transactions whenever 'on-line to Issuer' is selected for risk management reasons, either by the card or by the Terminal.
- To dynamically generate a cryptogram allowing the card to verify the authenticity of the Issuer.
- To generate updates to the card application.

5.2.4 The Acquirer

The role of the acquirer includes the following:

- To certify to the Settlement institution (Scheme) that his transaction processing system complies with the system rules specified.
- To contract with and to release payment accepting terminals to the Merchants.
- To process Terminal transactions and to pay the Merchant for them.
- To transmit the collected/truncated transactions to the Issuer in order to obtain the settlement.

- To protect the integrity of the Public Key(s) supplied by the Scheme (as part of the provision of secure storage for keying material).
- To decide under which conditions he takes the risk of accepting a transaction without further cryptographic or non-cryptographic (e.g. to 'skip' asking for authorization) verification.

5.2.5 The Scheme

The role of this organization includes the following.

- To specify the system rules for the products and services and to verify the compliance with them.
- To certify certain cryptographic keys used within the system.
- To produce cryptographic keys if required.
- To run networks providing on-line communication between Acquirers and Issuers.
- To perform Clearing and Settlement for transactions on this network.

The inter-relationship between these entities is as shown in Figure 1.

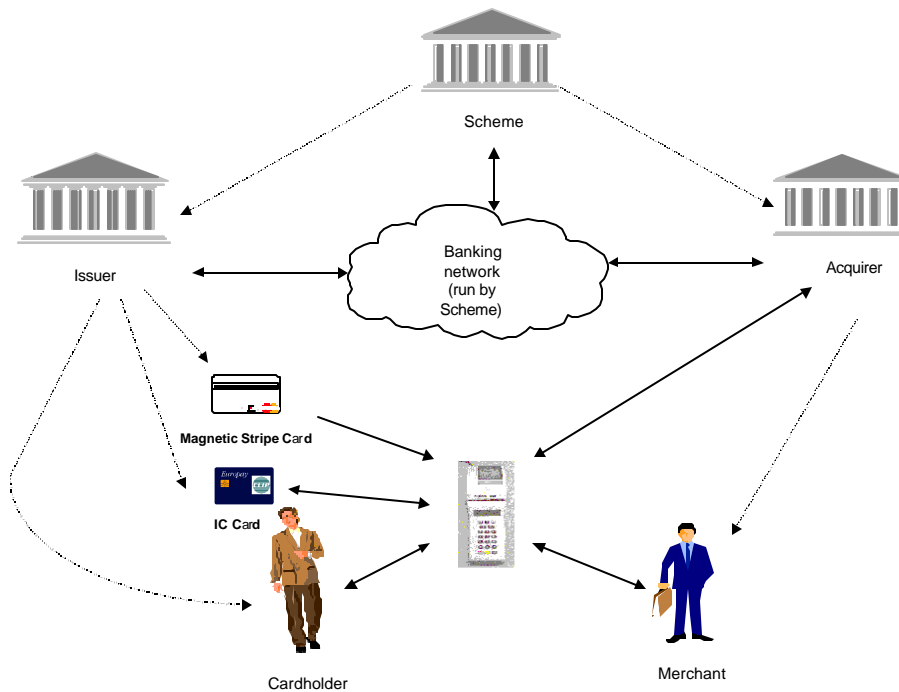


Figure 1 - System Model

5.3 Key Management Architecture

5.3.1 Certificates and Certification Authorities

In traditional cryptographic systems, key management has primarily been concerned with the establishment and maintenance of shared secret keys. With the growing use of Public Key or *Asymmetric* cryptography, the nature of the key management problem has changed. In a Public Key cryptosystem such as RSA, keys come in pairs, one half of which, the *Public Key*, can be widely disseminated, and the other half of which, the *Private Key*, needs to be kept secret by its owner. The key management problem is then to distribute Public Keys in a reliable way to those parties that need them.

More specifically, although these Public Keys do not need to be kept confidential, to be useful the recipient of a Public Key must have some assurance that the Public Key does indeed belong to who it claims to belong to. This problem is usually solved by the use of *certificates*.

To understand what a certificate is, we need to consider one specific type of Public Key cryptosystem, namely a *digital signature scheme*. With a digital signature scheme, an entity's Private Key can be used to *sign* a message, i.e. to generate a string of bits known as a *digital signature*, which is a function of the message being signed and the entity's

Private Key. The recipient of a message with a digital signature attached can verify the signature by using the signer's Public Key. Thus a digital signature can be used to check the origin and integrity of a message (and also provide protection against an originator repudiating a message).

A *certificate* consists of a user's Public Key concatenated with other related data (including the name of the user and a validity period) with a digital signature attached. This digital signature is generated by a widely trusted entity known as a *Certification Authority (CA)*. This CA distributes his/her Public Key to a group of entities by some physically trusted means; any user with a trusted copy of the CA's Public Key can then verify all certificates generated by that CA, and thereby obtain trusted copies of other users' Public Keys.

In the EMV environment, the Scheme will act as the Certification Authority. The Scheme Certification Authority will create certificates for each Issuer by signing each Issuer's Public Keys. The Scheme CA's Public Keys will then be distributed to the terminals through the Acquirers for verifying Issuer certificates; thereby yielding trusted copies of Issuers' Public Keys.

An Issuer's certified Public Key can be used in a two-layer scheme providing Static Data Authentication for Debit / Credit products as described in Section 5.3.2 below. An Issuer's certified Public Key can also be used in a three-layer scheme providing Dynamic Data Authentication for Debit/Credit and Purse products as described in Section 5.3.3 below.

The primary focuses of this document are the responsibilities of a card Issuer in relation to the lower layer of the Certification Scheme, i.e. that are concerned with:

- the generation, management and use of asymmetric keys, including the generation of an Issuer Key Pair,
- either signing of application data for use in Static Data Authentication (as described in Section 5.3.2), or the generation and certification of IC Card Asymmetric Key Pairs for use in Dynamic Data Authentication (see Section 5.3.3), and
- the generation of Issuer Secret Keys and their use to derive the IC card DES keys,

Note that this specifically excludes other card personalization functions of the lower layer, including the preparation and protection of IC Card personalization data.

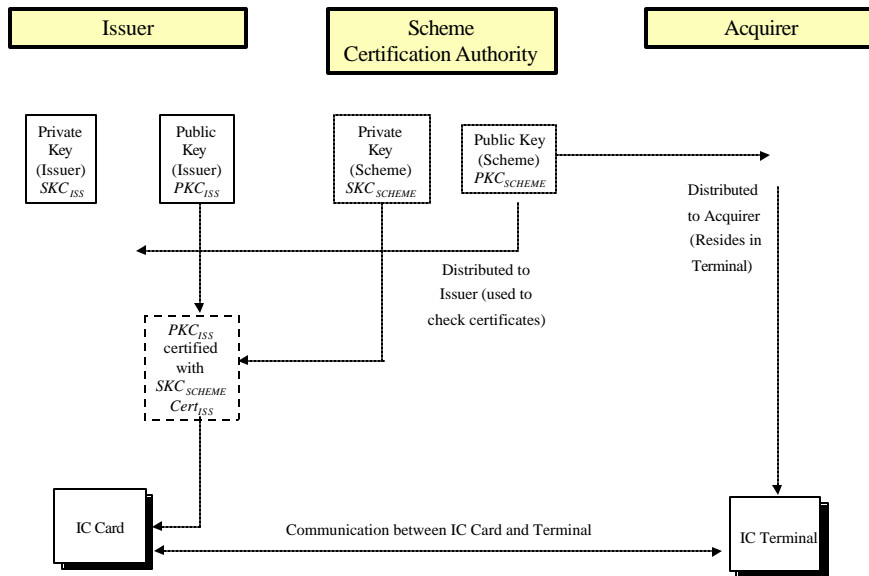
5.3.2 Static Data Authentication – A Two-layer Scheme

A two-layer scheme provides Static Data Authentication when the terminal uses a digital signature based on Public Key techniques to confirm the legitimacy of critical ICC-resident static data.

Static Data Authentication relies on the Scheme Certification Authority, which is a highly secure cryptographic facility that ‘signs’ the Issuer’s Public Keys. The relationship between the data and the cryptographic keys is shown in Figure 2. For further information, please refer to EMV ’96 Section IV-1.

Card provides to terminal :

Terminal



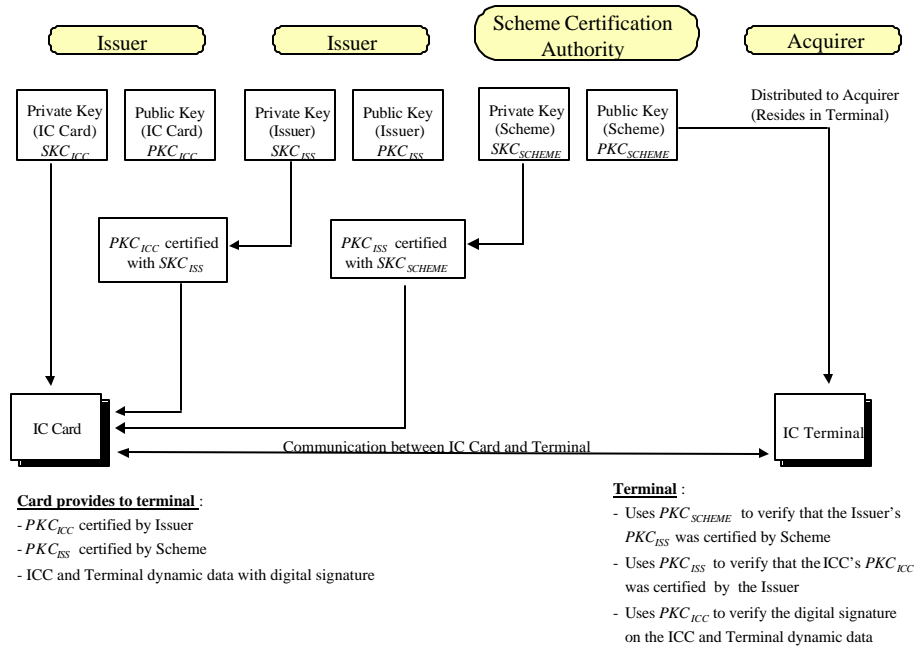
- PKC_{ISS} certified by Scheme Certification Authority
- Card data with digital signature
- Uses PKC_{SCHEME} to verify that the Issuer’s PKC_{ISS} was certified by the Scheme Certification Authority
- Uses PKC_{ISS} to verify the digital signature of the card data

Figure 2 - Diagram of Two-layer Scheme

5.3.3 Dynamic Data Authentication – A Three-layer Scheme

A three-layer scheme provides Dynamic Data Authentication when the terminal uses a digital signature based on Public Key techniques to authenticate the ICC, and confirms the legitimacy of critical ICC-resident data identified by the ICC dynamic data and data received from the terminal identified by the Dynamic Data Authentication Data Object List (DDOL). This precludes the counterfeiting of any such card.

Dynamic authentication will rely on the Scheme Certification Authority, a highly secure cryptographic facility that ‘signs’ the Issuer’s Public Keys. The relationship between the data and the cryptographic keys is shown in Figure 3. For further information, please refer to EMV ’96 Section IV-2.



Card Provides to Terminal :

- PKC_{CC} certified by Issuer
- PKC_{ISS} certified by Scheme Certification Authority
- Card and terminal dynamic data with digital signature

Terminal

- Uses PKC_{SCHEME} to verify that the Issuer’s PKC_{ISS} was certified by the Scheme Certification Authority
- Uses PKC_{ISS} to verify that the Card’s PKC_{CC} was certified by the Issuer
- Uses PKC_{CC} to verify the digital signature of the card data

Figure 3 - Diagram of Three-layer Scheme

5.3.4 Issuer Functionality

The Issuer will be responsible for providing the key management part of the lower layers of the two- and three-layer schemes described above. The functionality that must be provided by the Issuer includes the following, each of which are described in a little more detail in Section 5.4:

- the generation, maintenance and secure storage of the Issuer Key Pairs (asymmetric Key Pairs),

- the transfer of the Issuer Public Keys to the Scheme CA for certification,
- the storage of the Scheme Public Keys and certificates for Issuer Public Keys,
- the generation and secure transfer of the IC Card Keys (RSA Key Pairs),
- the use of an Issuer Private Key to certify IC Card Public Keys, or to sign application data,
- the generation and secure storage of Issuer Secret Keys (used to derive IC card DES keys),
- the import/export of Issuer Secret Keys (only necessary if other entities are to perform ‘on-behalf’ card verification services), and
- the derivation of IC card DES keys from Issuer Secret Keys.

These functions complement those provided by the Scheme CA, namely:

- the generation, maintenance and secure storage of the Scheme’s Payment System Key Pairs (asymmetric Key Pairs),
- the use of the private part of a Scheme Key to certify Issuer Public Keys, and
- the secure transfer (with respect to integrity) of the Scheme Public Keys to Acquirers for subsequent storage in Merchant Terminals.

5.4 Processes

We next describe the main security-relevant functions that need to be performed by an Issuer. We divide these processes into six classes:

- **Preparatory steps**, which need to be completed prior to any card issuance,
- **Card production (SDA)**, i.e. those steps which need to be followed to issue cards employing static data authentication,
- **Card production (DDA)**, i.e. those steps that need to be followed to issue cards employing dynamic data authentication,
- **Card issuance**, i.e. those steps that need to be followed to equip cardholders with newly produced IC cards,
- **Ongoing card management**, i.e. those procedures which need to be performed to support the ongoing use of IC cards, including on-line cryptogram exchanges with IC cards, and on-line cardholder verification, and

- **Transaction processing**, i.e. those processes which need to be performed by the card issuer to support the clearing and settlement of EMV card transactions.

5.4.1 Preparatory Steps

The following steps need to be performed by an Issuer prior to any card issuance. They will also need to be performed from time to time during the use of the Payment System.

- **Issuer Key Pair Generation.** The Issuer needs to securely generate and store one or more pairs of Public and Private Keys. The Private Keys will be used to sign either IC Card static data or IC Card Public Key Certificates (depending on whether the IC Card performs static or dynamic data authentication respectively).
- **Issuer Secret Key Generation.** The Issuer needs to securely generate and store one or more Secret Keys, as required to derive the IC Card Secret Keys.
- **Receive the Scheme Public Key(s).** The Issuer will need to receive and securely store one or more Scheme Public Keys. These Public Keys must be transferred in such a way that the issuer can verify their integrity and origin. These Public Keys will be used to verify Issuer Public Key Certificates.
- **Request and Receive Issuer Public Key Certificates.** The Issuer will need to obtain Public Key Certificates for each of the Issuer Public Keys. Transferring each Issuer Public Key to the Scheme CA, and subsequently receiving in return a signed Public Key Certificate achieve this. The Issuer Public Keys must be transferred to the Scheme CA in such a way that the Scheme CA can verify their integrity and origin. On receipt of a Public Key Certificate from the Scheme CA, the Issuer can verify it using the relevant Scheme Public Key.
- **Transfer of Issuer Secret Keys.** If the Issuer wishes to delegate responsibility for generation and verification of IC Card cryptograms to a third party, then it will be necessary for the Issuer to securely transfer the Secret Key(s) used to derive the IC Card Keys to the third party.

5.4.2 Card production (SDA)

The following steps need to be performed by an Issuer¹ for each SDA card issued. Note that only the security-relevant steps are considered here.

- **Static data preparation.** The set of static data stored on the IC Card, and used for card authentication, needs to be assembled by the Issuer.

¹ The IC Card Secret Key derivation could be performed by a third party, e.g. the card personalizer, on behalf of the Card Issuer.

- **Signing of static data.** The set of IC Card static data shall be signed using one of the Issuer Private Keys.
- **IC Card Secret key derivation.** The IC Card Secret Keys shall be derived from the appropriate Issuer Secret Key(s).
- **PIN generation.** A PIN shall be generated for the IC card if offline PIN supported.
- **DAC generation.** The Data Authentication Code (DAC), transferred from IC card to terminal as part of card authentication, needs to be generated by the Issuer.
- **Arrange for Issuer Public Key Certificate, signed static data, and derived secret keys to be provided to card personalization process.** All these values shall be securely transferred to the card personalizer so that they can be written onto the IC Card.

5.4.3 Card Production (DDA)

The following steps need to be performed by an Issuer¹ for each DDA card issued. Note that only the security-relevant steps are considered here.

- **IC Card Key Pair generation.** A unique Key Pair shall be securely generated for each IC Card.
- **Signing of IC Card Public Key to get IC Card Public Key Certificate.** The IC Card Public key (and associated data) shall be signed using one of the Issuer Private Keys to form the IC Card Public Key Certificate.
- **IC Card Secret Key derivation.** The IC Card Secret Keys shall be derived from the appropriate Issuer Secret Key(s).
- **Arrange for Issuer Public Key Certificate, IC Card Public Key Certificate, IC Card private Key, and derived secret keys to be provided to card personalization process.** All these values shall be securely transferred to the card personalizer so that they can be written onto the IC Card. Note that this shall be done in such a way that it can be verified that both the IC Card Issuer and the personalizer erase all records of the IC Card Private Key after personalization is complete.

5.4.4 Card issuance

The following steps need to be performed by an Issuer for each DDA card issued. Note that only the security-relevant steps are considered here.

- **Arrange for transfer of IC Card to Cardholder.** The personalized IC Card and PIN shall be securely transferred to the Cardholder.

5.4.5 Transaction processing

The following steps need to be performed by an Issuer for each DDA card issued. Note that only the security-relevant steps are considered here.

- **Cryptogram exchanges.** As part of the security procedures surrounding a card transaction at a merchant (with an on-line capability), the IC card or the merchant terminal may require on-line card verification. This will involve an exchange of a cryptogram (ARQC) between the IC card and the Issuer, where the cryptogram will be generated and verified using card-specific secret keys (derived from Issuer secret keys). The Issuer may generate a response cryptogram (ARPC) using the same secret key, proving that the response came from the valid Issuer
- **Secure messaging.** As part of the overall card management process, *secure messages* (cryptographically protected) may be exchanged between the IC card and the Issuer. These may be used for a variety of purposes including PIN change and application blocking/unblocking the cryptographic protection will be performed using card-specific secret keys, derived from Issuer secret keys.
- **On-line cardholder verification.** The cardholder PIN may be verified either off-line (by the card) or on-line (by the Issuer).

5.4.6 Transaction clearing

The following steps need to be performed by an Issuer for each DDA card issued. Note that only the security-relevant steps are considered here.

- **TC processing.** As a result of every IC card transaction, the IC card will provide the merchant terminal with a Transaction Cryptogram (TC), generated using an IC card secret key. This TC will be passed by the merchant to the Acquirer, and will then be passed from the Acquirer to the Issuer as part of the clearing process. The Issuer will be responsible for verifying the correctness of the TC as part of clearing and settlement.

6 Integrated Circuit Card (ICC) Cryptographic Key Types and Key Management Principles

The different types of cryptographic algorithms support different functions with the EMV specification. The intended role of the cryptographic algorithms, however, will be negatively impacted when not implemented correctly. A secure implementation will depend on how well the different keys required by the specification are managed by the Issuer. The following materials are intended to provide an overview of the cryptographic role played by the different algorithm types and to present the basic requirements necessary to securely manage the cryptographic keys.

6.1 Asymmetric (RSA) Key Management

The security of IC cards depends upon the protection of the private (signature) keys. Failure to secure the private keys used to sign static or dynamic data elements risks the creation of counterfeit IC cards. The primary risks to the private key include; (1) the successful factoring of the RSA modulus and, (2) the compromise of the private key itself. To limit the potential exposure represented by these separate risks the following Issuer best practices are encouraged.

The security of the private (signature) key depends on a number of factors including:

- the length in bits of the RSA key modulus; i.e. 768, 896, and 1024,
- the quality of the prime numbers making up the public/private key modulus, and
- the methods used to physically secure (protect) the private (signature) key from unauthorized access and exposure/compromise.

6.1.1 Key Lengths and Cryptoperiods

The primary risks to the private (signature) key include:

- A successful computational attack resulting in the exposure of the prime number components making up the RSA modulus.
- The physical compromise of the private (signature) key exponent.

To limit the risks associated with these potential risks the following best practices are recommended:

The strength of the RSA algorithm is exponentially related to the length of the key modulus. The size of the key is in bits. EMV has recommended the following scheme key sizes and cryptoperiods for the scheme RSA keys.

Modulus Size (N_{CA})	Public Key Exponent	Cryptoperiods
768-bits	3 or $2^{16} + 1$	12/31/2002
896-bits	3 or $2^{16} + 1$	12/31/2004
1024-bits	3 or $2^{16} + 1$	12/31/2008

Table 1. EMV Scheme Key Sizes and Cryptoperiods

Issuers are responsible for the creation of the following RSA key pairs:

- Issuer Public/Private Key Pair (SDA/DDA)
- Card Public/Private Key Pair (DDA)
- ICC PIN Encipherment Key Pair

To minimize the risks of computational attacks, i.e., factoring of the public key modulus, Issuers are encouraged to select moduli of sufficient size that are resistant to such attacks. Successful attacks on a modulus of length 512 bits have already been recorded. Because cards are issued for periods of three years and more, public key moduli have to be of sufficient size to resist computational attacks over the active life of the card.

The EMVco_Security Working Group performs an annual review of scheme key sizes and corresponding cryptoperiods in August. This review is based on independent analyses of the participating payment schemes. Published cryptoperiods for existing keys may be adjusted and larger key sizes and their cryptoperiods approved. The process leads to the schemes updating their published scheme key cryptoperiods and key sizes.

Issuers are strongly encouraged to perform a similar review of their RSA key pairs for adequacy. Where a scheme key of particular size has been determined to be no longer fit for service, Issuers should not continue to use that key, and should replace such key(s) with larger key(s) to ensure that card level key certificates cannot be counterfeited.

In the event an Issuer detects that their private (signature) key corresponding to their Issuer Public Key Certificate has been compromised, it is strongly recommended that the compromised key pair be replaced and re-issuance schedules for cards with public key

certificates created by the compromised key be established and implemented to mitigate the Issuers potential fraud risk.

6.1.2 RSA Key Generation

When generating the RSA public/private key pair, it is recommended that the process be completed in the protected memory of a physically secure device. Such a device must contain a random or pseudo-random number generator, perform primality-checking routines, and support tamper responsive mechanisms.

- The RSA private (signature) key may remain ephemeral to the physically secure device.
- Key generation shall utilize a random or pseudo-random process such that it is not possible to predict any key or determine that certain keys within the key space are more probable than any other.
- The physically secure device used to create the RSA key pairs and to secure the private (signature) key should satisfy the security requirements set forth in Section 7; *Cryptographic Security Modules*.
- A personal computer or other such insecure device, i.e., untrusted device, should never be used to generate RSA public/private key pairs.

6.1.3 Key Usage

Standards require that cryptographic keys be used only for the purpose for which they were intended.

- Issuer public/private key pairs must be unique to each scheme.
- EMV scheme keys may only be used to sign Public Key Certificates for scheme branded, EMV compliant products.

6.1.4 Key Transport and Storage

To protect the integrity of the public/private key pair(s), it is important the following steps be used by an Issuer to ensure the integrity of this keying data.

- Public keys should be secured and transported in a manner that guarantees their integrity. It is recommended that public keys always be transported within a data structure such as a certificate, or with a Message Authentication Code (MAC) for the public key and associated data using an algorithm defined by ISO 9807 and a key used only for this purpose. It is also recommended that dual control techniques be used to ensure that the recipient of a public key has the means to

verify its origin and integrity, e.g. by separate and independent transfer of a check value on the public key.

- Private keys must be secured and transported in such a manner that guarantees the their integrity and secrecy. Transportation mechanisms may include:
 - a secure cryptographic device,
 - encipherment using an symmetric algorithm of at least equal cryptographic strength to the private key of the key being protected, or
 - as fragments, secured on tokens and enciphered using a symmetric algorithm.
- Business resumption strategies will require that copies of public/private keys be made and secured. These keys are necessary in the event of a catastrophic system failure. Back-up copies of system keys are to be secured using the same principles as described in the previous bullet.

6.2 Symmetric (DES) Key Management

DES keys in the EMV specification are used for specific transaction functions. DES keys are derived from a Master Derivation Key at the time of personalization. The resultant card level keys are unique.

Issuer DES Master Keys include:

- *Issuer Master Derivation Key (IDK_{AC})* - used to derive the card keys that are employed to generate MACs known as Application Cryptograms (AC).
- *Issuer Secure Messaging Master Keys (IMK_{SMC} IMK_{SMT})* - used to derive the card keys used in the secure messaging of certain post issuance processes between the card and the authorization system; i.e., card blocking, application blocking/unblocking, updating card specific data, and PIN changes.

6.2.1 Key Lengths and Cryptoperiods

- All EMV DES Master Keys are 16 bytes or 128-bits in length.
- Standards require that a symmetric key be used no longer than the time necessary to find the key by exhaustive search of the key space.
- Keys must be replaced when their compromise is known or suspected.

6.2.2 Key Generation

The following principles are to be used by Issuers to minimize the opportunity for the compromise of keying data during its creation.

- When DES keys are created they must be generated either inside a physically secure device protected by tamper responsive mechanisms, or by authorized personnel in component form (see below). The device must contain a random or pseudo-random number generator.
- At no time is an unprotected key ever to exist outside the protected memory of a physically secure device. The plaintext key must never be output by the physically secure device other than as a cryptogram or in the form of two or more components.
- When secret keys are to be generated by authorized personnel through a process of combining components, each party must be required to generate a component that is as long as the key being generated. The key combination process must take place inside a physically secure device. Moreover, the method of combining the components shall be such that knowledge of any subset of the components shall yield no knowledge about the key value.
- Check digits shall be calculated for the full 16 byte component or for the actual key.
- A personal computer or similar insecure device must never be used to generate keying materials.
- If any cryptographic keys are found to exist outside of a physically secure device or the components of cryptographic key are known or suspected to have been under the control of a single individual, the key(s) is to be considered to have been compromised and must be replaced with a new key.

6.2.3 Key Usage

Key usage occurs when a key is employed for a cryptographic purpose. A key must only be used for the cryptographic purpose for which it was intended and not for any other purpose, i.e., a master derivation key must only be used to derive card specific keys and may not be used as a MAC key.

6.2.4 Key Transport and Storage

It may be necessary to transport and/or store DES keys. Examples include the transport of DES keys from the Issuer's site to that of a third party processor or card personalization vendor. When DES keys are being transported or stored, the following measures will limit the potential for the compromise of the data.

- Cleartext DES keys may be securely transferred to the protection of a secure token or smart card for both transport and storage.
- DES keys may only be transported or stored outside the protected memory of a secure token or smart card in one of the following ways:
 - In the form of two or more components using the principles of dual control and split knowledge, or
 - As a cryptogram, created by a transport or storage key that has securely been established by the parties.

6.2.5 Key Destruction

- Obsolete keying data must be destroyed using methods that are appropriate for the medium containing the keying material(s).
- An independent third party; i.e., an internal auditor, should witness the destruction of keying materials, documenting the process. The resultant documentation should be retained for a period consistent with the Issuers documentation retention policies.

6.2.6 Key Backup and Archiving

It may be necessary to recover keys used in the personalization of cards. Therefore, it will be necessary that certain cryptographic keys be securely backed-up or archived. When backing-up critical master keys used in the personalization of cards, the following steps are recommended:

- When a cryptographic key is not enciphered under another key of equal size, i.e., a Master File Key, it must be maintained as two or more components secured using the principles of dual control and split knowledge.
- When the cryptographic key is not secured as two or more components using the principles of dual control and split knowledge, it must be maintained as a cryptogram under a unique storage key of equal size that is maintained in a secure token or as components using the principles of dual control and split knowledge.
- Audit procedures should be implemented to assure that the above practices are implemented.

7 Key Custodians - Practices and Responsibilities

7.1 Appointment of Key Management Personnel

Personnel responsible for the management of encryption keys and key components, secure tokens and other keying data devices must be designated by the different parties; i.e., Issuers, third party processors, and/or card personalization vendors.

When designating individuals to be responsible for the custodial control of keying data or secure tokens, sufficient controls must be implemented to assure that no single individual or unauthorized individual can obtain access to the data comprising a cryptographic key or secure token.

Key custodians should be trusted employees and never temporary help or consultants.

To assure service continuity alternate personnel may also be identified as "back-ups" to the primary key custodians. The criteria used to select "back-up" custodians should be the same as used to select the primary custodians.

7.2 Functions of Key Management (Custodial) Personnel

Key custodial responsibilities are important and a fundamental part of an Issuer's security protocol. The keying data that will be managed by these persons represent the most important keys in the cryptographic applications for an Issuer's card program. Each Issuer is encouraged to review its internal key management procedures and the roles of those individuals relative to the following practices.

- The responsibilities of the key management personnel (key custodians) include the control of keying materials, verification of the materials, and their secure storage.
- Key custodians or their back-ups are responsible for the:
 - Receipt and secure storage of key components and/or secure tokens
 - Maintenance of records or logs tracking access to and usage of keying data; including times of access, date, purpose, and return to secure storage.
 - Verification of all transfers of keying data to other designated individuals outside the Issuer's control.
 - Witnessing the destruction of old/obsolete key components.

- Entering of keying data into secure cryptographic modules as required from time to time.
 - Directing and overseeing the destruction of obsolete keying materials, as instructed by the owner of the data.
- Custodians where keying data is first originated are responsible for securing and forwarding that data to their designated counterpart at the receiving entity. This responsibility includes verifying receipt of the data.

7.3 Procedures for Shipping Keying Materials to Third Party Agents

- A two-part form should accompany the forwarding of all keying data to a party other than the originator. This form will identify the sender and the materials being sent to the receiver. The originator will sign the form. Immediately upon receipt of the materials, the receiving custodian will verify the contents against the form and should sign and return one part of the form to the originator.
- When forwarding key components and other cryptographic data to third parties, different delivery services should be used for each of the various components; i.e., registered mail, express mail, standard mail or air courier service. Where the keying data is secured using a secure token or smart card, registered mail is sufficient.
- The receiver of the keying data should be pre-notified of the forwarding of keying materials.

7.4 Physical Procedures for Securing Keying Data at Third Party Agents

- Upon receipt the responsible key custodian must immediately examine the shipping package for tampering, and must verify the contents.
- If the receiving custodian has any uncertainty regarding the integrity of the keying data, the sender is to be immediately notified. The sender, in consultation with the receiving party, will decide the future status of the keying data. The basis for any decision regarding the continued use of the keying materials should be documented and retained by the two parties.
- If the hard copy keying data is to be retained for any period of time, the individual hard copy components, secure token, or smart card must be secured in a serialized tamper evident envelope.

-
- The serialized tamper evident envelope must be continually protected in a physically secured container, accessible only to the designated key custodian or alternate. Each access of the keying data is to be logged, including time, date, envelope serial number, purpose, and signature. These logs are to be made available to any appropriate requesting authority.
 - Keying materials are never to be maintained outside of tamper evident envelopes and their physically secure environments longer than necessary for the task requiring the access.

8 Cryptographic Security Devices

Relative to the EMV specifications, secure cryptographic devices (SCDs) include, but are not limited to, host secure cryptographic devices (SCD) and IC cards. Of these devices the more critical cryptographic device is the SCD. This criticality is the product of the EMV specification requiring master derivation keys to be used to derive unique card level keys, and Issuer private (signature) keys to be used to create signed data that is stored on cards. Consequently, it is important that Issuers understand the importance of using SCDs that are tamper resistant and properly operated to achieve the intended security for their system cryptographic keys.

8.1 Tamper Resistance Requirements - Physical Security

8.1.1 Penetration

SCDs must be protected against penetration, either by employing physical protection sufficient to ensure that penetration is not feasible, or by the inclusion of mechanisms that detect any penetration. When the SCD is operated in its intended environment and manner, any attack on the device must cause the automatic erasure of all keying and other sensitive data, including any cryptographic residues of such data.

8.1.2 Modification

The modification of a SCD for the purpose of determining keys and other sensitive data stored in the device, shall require that the SCD be taken to a specialist facility. Tampering with the device for the purposes of inserting tapping or bugging equipment should result in sufficient damage to the device to cause it to become inoperable.

The determination of sensitive data by modification of the SCD must require skills and specialized equipment that is not generally available in the general marketplace.

8.1.3 Monitoring

Passive physical barriers shall be included in the device to:

- shield against x-rays and other techniques used to monitor electrical emissions from the device,
- provide privacy shielding so that during the manual loading of cryptographic data, the information will not be easily observable to other persons in attendance during the process.

8.1.4 Removal

Removal of the device refers to cases where the device is taken from its operating environment. Where the security of the device depends on the operating environment, unauthorized movement of the SCD shall be infeasible or cause the activation of tamper responsive mechanisms.

8.2 Tamper Resistance Requirements - Logical Security

8.2.1 Assurance of Device Genuineness

If the device management does not assure its genuineness, then the SCD should be delivered with sensitive information, giving assurance to the user that the device is genuine and has not been compromised.

An example of such sensitive information is a symmetric key, without which the device will not properly operate.

8.2.2 Design of Functions

The function set of the SCD shall be designed such that no single function or combination of functions can result in the disclosure of sensitive information by the device. This protection must be sufficient to ensure such protection even when using legitimate functions.

8.2.3 Use of Cryptographic Keys

The SCD shall enforce key separation schemes, ensuring that no key can be used for any purpose other than its intended purpose. Key creation methods shall comply with ISO 11568, part 3.

8.2.4 Sensitive Device States

If the SCD can be placed in a sensitive state; i.e., a state that allows functions that are normally not permitted (manual key loading), then such a state must require dual or multiple control.

If passwords or some other cleartext data are required to use a sensitive function, the input of data shall be protected in the same manner as other sensitive data.

To minimize the risks of unauthorized use of sensitive functions, the sensitive state is to be established with limits on the number of function calls and time limit. After one of these limits has been reached the device will automatically return to a normal state.

8.2.5 Downloadable Software

If software is to be downloaded to the SCD, a specific technique for authentication of the software must be included with the device. This technique is to ensure that only software that has been authenticated and/or enciphered by the provider or owner has been approved.

9 The Authorization System

Authorization is a process whereby an issuer or the representative of the issuer, approves a transaction of its cardholder. The authorization is in response to an authorization request from a merchant or an Acquirer.

The authorization request includes a card generated authorization cryptogram (ARQC) for transactions requiring online authorization. The issuer validates the ARQC during the online card authentication process to ensure that the card is authentic and not created using skimmed data.

In response to the ARQC, the issuer optionally creates an authorization response cryptogram (ARPC). This cryptogram is the result of encrypting the ARQC and the authorization response using the unique derivation key for that card. The card validates the ARPC to assure that the authorization response came from the issuer. The integrity of the authorization process is based on the protection afforded to the unique master derivation key. Therefore, the issuer should take the same care in protecting the confidentiality of this cryptographic key when being used in the issuer's authorization system as when it is used for card personalization. Therefore, the symmetric key management principles described above are strongly recommended to secure the cryptographic integrity of the authorization process.