Developments in Electronic Payment Systems Security
EMV and CEPS

Mike Ward
Europay International, Brussels, Belgium

Abstract: This paper provides an outline of the security features for Europay's chip card applications for Credit, Debit and Electronic Purse payments. It gives an overview of the EMV chipcard specifications and the Common Electronic Purse Specifications (CEPS).

Key words: electronic payment systems, EMV, CEPS, electronic purse, Clip

1. INTRODUCTION

1.1 Background

In June 1994, Europay became the first international payment organisation to commit to chip as the replacement technology for the magnetic stripe. At that time Europay's Chip Business Case focused on four key areas: Fraud Reduction, Telecommunications Cost Reduction, Credit Risk Management, and Value-added Services such as Electronic Purse.

To develop the global standards necessary to usher in the new technology, chip, Europay initiated a joint working group with MasterCard International and Visa International, known within the industry as EMV.

EMV'96, released in July 1996, marked the completion of the final phase of the global chip card specifications which served as the framework for chip card and terminal manufacturers world-wide. The EMV specifications have now been revised as EMV2000 version 4.0.

M. Gertz et al. (eds.), *Integrity, Internal Control and Security in Information Systems*

In addition to this activity, Europay have participated in the development of the Common Electronic Purse Specifications (CEPS).

This article provides an overview of the EMV'96 specifications and of Europay's supporting public key services. It also provides a brief overview of Europay's Electronic Purse, Clip.

2. EMV

2.1 Card Payments

Debit and credit card transactions normally take place between two parties that do not know one another. This is made possible by the contractual relationship that exists between the bank that issued the card to the cardholder and the acquiring bank of the merchant. The relationship between the two banks operating from two different countries is established by membership of a payment system, which also provides the network for authorising and clearing of cross-border payment transactions, and sets the rules of membership and operation along with an often complex set of guarantees.

Payment cards carry a magnetic stripe, a hologram, one or more payment brands, and a specimen signature of the cardholder. The card is also embossed with the cardholder's name and account number as well as the expiry date of the card.

The ultimate purpose of the EMV standard is to replace the magnetic stripe on the card by an Integrated Circuit or chip, thereby making it a 'smart card' with memory and processing capabilities. This added intelligence enables better issuer risk management, including improved offline and online authentication and authorisation. The characteristics of these cards are based on the ISO/IEC 7816 series, which is a generic cross-industry standard for IC cards.

2.2 Overview of EMV Application

The EMV application specification defines the terminal and integrated circuit card (ICC) procedures necessary to effect a payment system transaction in an international interchange environment.

It describes the following processes:

- Offline Data Authentication
- Cardholder Verification
- Terminal Risk Management
- Terminal Action Analysis
- Card Action Analysis
- Online Processing and Issuer to Card Script Processing

2.2.1 Offline Data Authentication

Offline Data Authentication is the process whereby the terminal verifies by means of a digital signature the authenticity of critical card data. This process is known as an "offline CAM" (Card Authentication Method) and can either be static SDA or dynamic DDA (see later).

2.2.2 Cardholder Verification

Cardholder verification is performed to ensure that the person presenting the ICC is the person to whom the application in the card was issued. The terminal uses the data in the ICC to determine whether one of the issuer-specified cardholder verification methods (CVMs) is to be executed:

- Offline PIN processing enables the ICC to verify a plaintext or enciphered PIN presented to it by the terminal
- Online PIN processing enables issuer verification of the PIN sent by the terminal
- A (paper) signature may be required, in which case this corresponds to the 'conventional' signature verification by the terminal attendant.

2.2.3 Terminal Risk Management

Terminal risk management is performed by the terminal to protect the acquirer, issuer, and system from fraud. It provides positive issuer authorisation for high-value transactions and ensures that transactions initiated from ICCs go online periodically to protect against threats that might be undetectable in an offline environment.

Terminal risk management consists of:

- Floor limit checking
- Random transaction selection
- Velocity Checking

With Velocity Checking, the terminal can compare the difference between the ATC (Application Transaction Counter) and the Last Online ATC Register with the Lower Consecutive Offline Limit to see if this limit has been exceeded.

2.2.4 Terminal Action Analysis

Once terminal risk management and application functions related to a normal offline transaction have been completed, the terminal makes the first decision as to whether the transaction should be approved offline, declined offline, or transmitted online. If the outcome of this decision process is to proceed offline, the terminal obtains a MAC (Message Authentication Code) from the card that can be used as a transaction certificate. If the outcome of the decision is to go online, the terminal initiates a challenge and response between the card and its issuer that enables online authorisation or decline (see below).

2.2.5 Card Action Analysis

An ICC may perform its own risk management to protect the issuer from fraud or excessive credit risk. Details of card risk management algorithms within the ICC are specific to the issuer and are outside the scope of the specification, but as a result of the risk management process, an ICC may decide to complete a transaction online or offline or request a referral or reject the transaction.

2.2.6 Online Processing

Online processing is performed to ensure that the issuer can review and authorise transactions - or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer.

In general, online processing is the same as today's online processing of magnetic stripe transactions. The primary exception being that with EMV the terminal obtains an Application Cryptogram (AC) from the ICC. The terminal may then choose to send this AC in an authorisation request message to the Issuer.

Although actions performed by the acquirer or issuer systems are outside the scope of EMV, for online authorisations it is generally assumed that the AC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system.

The issuer uses this key to authenticate the AC and thereby authenticate the card. Subsequent to card authentication, the issuer may generate a cryptogram on selected data included in the authorisation response or already known to the card. This cryptogram is sent to the terminal in the authorisation response and the ICC may use it to authenticate that the response message originated from the issuer.

2.2.7 Issuer-to-Card Script Processing

An issuer may provide command scripts to be delivered to the ICC by the terminal to perform functions that are not necessarily relevant to the current transaction but are important for the continued functioning of the application in the ICC. An example might be unblocking of an offline PIN, which might be done differently by various issuers or payment systems. Europay requires that such script processing be cryptographically secured using Secure Messaging.

2.3 EMV Offline Authentication

2.3.1 Static Data Authentication

Static data authentication is performed by the terminal using a digital signature based on public key techniques to confirm the legitimacy of critical ICC-resident static data and to detect unauthorised alteration of data after personalisation.

Static data authentication requires the existence of a certification authority, which is a highly secure cryptographic facility that 'signs' the issuer's public keys. Every terminal conforming to the specification contains the appropriate certification authority's public key(s). The relationship between the data and the cryptographic keys is shown below.

2.3.2 Dynamic Data Authentication

In the case of Dynamic Data Authentication, a three-layer public key certification scheme is used where the ICC owns a public key pair. The private key is used for signing the dynamic data, and the ICC's public key is stored on the ICC in the form of a ICC Public Key Certificate, signed by the issuer.

The corresponding issuer public key is also stored on the ICC in the form of a Issuer Public Key Certificate, signed by the Card Scheme.

2.3.3 The Europay-MasterCard Certification Authority

Europay and MasterCard have developed a Public Key Certification Service for their members for the management of the joint Europay-MasterCard public key pairs and the certification of the issuer's public keys. The Europay-MasterCard Certification Authority provides the 'top layer' of the Static and Dynamic Data Authentication schemes described above.

3. ELECTRONIC PURSE

3.1 Clip

This section provides a very brief overview of Clip, a pre-paid product from Europay based on CEPS (Common Electronic Purse Specification).

Unlike debit and credit payment applications, Clip is specifically designed to enable low value offline transactions.

Although there is a wide range of domestic pre-paid schemes in operation all over Europe, generally these schemes are incapable of inter-operating with each other and thereby lack an international dimension to transactions using pre-paid products. One of the purposes of Clip is to provide this international dimension.

Clip includes a minimum set of functionality that will be available internationally, wherever the product is used:

- Loading of electronic value in the local currency of the Load Device, a service typically provided by ATMs or by dedicated devices.
- Purchases of goods, provided by dedicated purchase devices or as a new feature to POS terminals.

Electronic value is stored as a number in a 'slot' of the ICC Electronic Purse application, one slot per currency.

3.2 CEPS Online Transactions

CEPS defines two types of online transactions:

- Load;
- Currency Exchange.

A successful load transaction results in an increase to the balance of electronic value in one of the Electronic Purse's slots. A successful Currency Exchange transaction results in an increase to the balance of electronic value in one currency slot and the appropriate decrease in another slot.

Both types of transaction involve mutual authentication between the Electronic Purse card and its issuer by means of the exchange of cryptograms computed with a double length DES key shared between the two entities.

3.3 CEPS offline Transactions

CEPS defines two types of offline transactions

- Purchase;
- Cancel Last Purchase.

The Purchase transaction enables the Electronic Purse card to make payments to a merchant PSAM (Purchase Secure Application Module) in one step or a series of incremental steps. The Cancel Last Purchase transaction enables a merchant to cancel the previous purchase transaction or, in the case of an incremental purchase, the final step thereof.

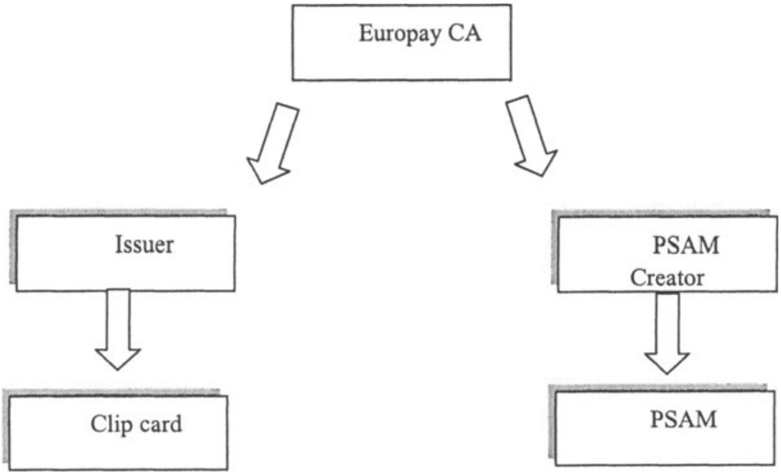
The purchase transaction requires that the Electronic Purse appropriately decrement the value in one of its slots and provide to the PSAM a cryptogram. For Europay this cryptogram is a MAC computed using a 112-bit key shared with the card issuer. The merchant can submit this 'transaction certificate' to the issuer (via the merchant acquirer) as evidence that the Electronic Purse was correctly debited.

In order that the merchant can obtain confidence that the transaction certificate is legitimate, the PSAM and the Electronic Purse perform a mutual authentication using RSA public key cryptography. A by-product of this mutual authentication is the establishing of a shared symmetric session key that can then be used for authenticating subsequent incremental purchase steps and purchase cancellations.

3.3.1 The Clip Certification Authority

In order that the Clip card be able to authenticate itself to the PSAM it is personalised with a private RSA key and public key certificates. The top-layer public key is provided by the Europay Clip Certification Authority and this public key must be installed in all PSAMs that accept Clip transactions. This situation is very similar to that of an EMV DDA card.

In order that the PSAM be able to authenticate itself to the Clip card it too is personalised with a private RSA key and public key certificates. The top-layer public key is again provided by the Europay Clip Certification Authority and this public key must be installed in all Clip cards.



4. CONCLUSIONS

This article has provided an outline of the security features for Europay's chip card applications for Credit, Debit and Electronic Purse payments. Further information can be found at Europay's web site:

http:\\www.europay.com

including the downloadable EMV specifications themselves:

EMV2000 Version 4.0: December 2000
Integrated Circuit Card Specifications for Payment Systems:

- Book 1 - Application Independent ICC to Terminal Interface Requirements
- Book 2 - Security and Key Management
- Book 3 - Application Specification
- Book 4 - Cardholder, Attendant and Acquirer Interface Requirements