EMV Terminal Public Key Management Requirements

EMVCo, LLC

Version 1.0
March 31, 1999

TABLE OF CONTENTS

1. Scope

Static data authentication and dynamic data authentication as specified in Part IV of the *EMV '96 IC Card Specification for Payment Systems, Version 3.1.1* requires the presence in terminals of Payment System specific Certification Authority Public Keys necessary to verify the Signed Static Application Data and Signed Dynamic Application Data.

This document specifies the requirements for the management by the Acquirers of the Certification Authority Public Keys in the terminals. The requirements cover the following phases:

- Introduction of a Certification Authority Public Key in a terminal
- Storage of a Certification Authority Public Key in a terminal
- Usage of a Certification Authority Public Key in a terminal
- Withdrawal of a Certification Authority Public Key from a terminal.

For more details on the management of the Certification Authority Public Keys in general, see *EMV Public Key Revocation – Principles and Policies, Version 1.0.*

2. References

EMVCo, LLC	Integrated Circuit Card Specification for Payment Systems, version 3.1.1, 31 May 1998
EMVCo, LLC	Integrated Circuit Card Terminal Specification for Payment Systems, version 3.1.1, 31 May 1998
EMVCo, LLC	Integrated Circuit Card Application Specification for Payment Systems, version 3.1.1, 31 May 1998
EMVCo, LLC	EMV Public Key Revocation – Principles and Policies, version 1.0, March 31, 1999

3. Certification Authority Public Key Introduction

When a Payment System has decided that a new Certification Authority Public Key is to be introduced, a process is executed that ensures the distribution of the new key from the Payment System to each Acquirer. It is then the Acquirer's responsibility to ensure that the new Certification Authority Public Key and its related data (see Section 4) is conveyed to its terminals.

The following principles apply to the introduction of a Certification Authority Public Key from an Acquirer to its terminals:

- The terminal must be able to verify that it received the Certification Authority Public Key and its related data error-free from the Acquirer.
- The terminal must be able to verify that the received Certification Authority Public Key and related data originated from its legitimate Acquirer.
- The Acquirer must be able to confirm that the new Certification Authority Public Key was indeed introduced correctly in its terminals.

4. Certification Authority Public Key Storage

Terminals that support Static Data Authentication and/or Dynamic Data Authentication shall provide support for six Certification Authority Public Keys per Registered Application Provider Identifier (RID) for Europay, MasterCard and Visa debit/credit applications based on *EMV '96 IC Card Specification for Payment Systems, Version 3.1.1*.

Each Certification Authority Public Key is uniquely identified by the 5-byte RID that identifies the Payment System in question, and the 1-byte Certification Authority Public Key Index, unique per RID and assigned by that Payment System to a particular Certification Authority Public Key.

For each Certification Authority Public Key, the minimum set of data elements that has to be available in the terminal is specified in Table 1.

The RID and the Certification Public Key Index together uniquely identify the Certification Authority Public Key and associate it with the proper Payment System.

The Certification Authority Public Key Algorithm Indicator identifies the digital signature algorithm to be used with the corresponding Certification Authority Public Key. The only currently acceptable value is hexadecimal '01', indicating the usage of the RSA algorithm in the digital signature scheme as specified in the annexes E2.1 and F2.1 of the *EMV '96, Integrated Circuit Card Specification for Payment Systems, Version 3.1.1*. The Hash Algorithm Indicator specifies the hashing algorithm to produce the Hash-Result in the digital signature scheme. The only currently acceptable value is hexadecimal '01', indicating the usage of the SHA-1 algorithm.

The Certification Authority Public Key Check Sum is the technique specified in the *EMV '96, Integrated Circuit Card Terminal Specification for Payment Systems, Version 3.1.1*, to ensure that a Certification Authority Public Key and its related data is received error-free. The terminal may use this data element to subsequently re-verify the integrity of a Certification Authority Public Key and its related data. Alternately, the terminal may use another technique to ensure the integrity of this data.

The terminal implementation shall ensure that the environment in which the Certification Authority Public Keys are stored satisfies the security requirements specified the *EMV '96 Integrated Circuit Card Terminal Specification for Payment Systems, Version 3.1.1*, when applicable.

The integrity of the stored certification Authority Public Keys should be verified

periodically.

Name	Length	Description	Format
Registered Application Provider Identifier (RID)	5	Identifies the Payment System to which the Certification Authority Public Key is associated	b
Certification Authority Public Key Index	1	Identifies the Certification Authority Public Key in conjunction with the RID	b
Certification Authority Hash algorithm Indicator[1]	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b
Certification Authority Public Key Algorithm Indicator[1]	1	Identifies the digital signature algorithm to be used with the Certification Authority Public Key	b
Certification Authority Public Key Modulus	Var. (max 248)	Value of the modulus part of the Certification Authority Public Key	b
Certification Authority Public Key Exponent	1 or 3	Value of the exponent part of the Certification Authority Public Key, equal to 2, 3 or $2^{16}+1$	b
Certification Authority Public Key Check Sum	20	A check value calculated on the concatenation of all parts of the certification Authority Public Key (RID, Certification Authority Public Key Index, Certification Authority Public Key Modulus, Certification Authority Public Key Exponent) using SHA-1	b

Table 1 – Minimum Set of Certification Authority Public Key Related Data

[1] The Certification Authority Hash Algorithm and Public Key Algorithm Indicators are new data elements. Use of these data elements is not specified in the *EMV 96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1*, but will be addressed in the next release of the specifications.

Elements to be Stored in the Terminal

5. Certification Authority Public Key Usage

The usage of a Certification Authority Public Key during a transaction shall be as specified in the *EMV '96 Integrated Circuit Card Specification for Payment Systems,Version 3.1.1*, and the *EMV'96 Integrated Circuit Card Application Specification for Payment Systems, Version 3.1.1*.

6. Certification Authority Public Key Withdrawal

When a Payment System has decided to revoke one of its Certification Authority Public Keys, an Acquirer must ensure that this Certification Authority Public Key can no longer be used in its terminals for Static and Dynamic Data Authentication during transactions as of a certain date.

The following principles apply for the withdrawal by an Acquirer of Certification Authority Public Keys from its terminals:

- The terminal must be able to verify that it received the withdrawal notification error-free from the Acquirer.
- The terminal must be able to verify that the received withdrawal notification originated from its legitimate Acquirer.
- The Acquirer must be able to confirm that a specific Certification Authority Public Key was indeed withdrawn correctly from its terminals.

For more details on Certification Authority Public Key revocation and the corresponding timescales involved, see *EMV Public Key Revocation – Principles and Policies, Version 1.0.*