EMV Public Key Revocation Principles and Policies

EMVCo, LLC

Version 1.0
March 31, 1999

TABLE OF CONTENTS

1. Scope

The aim of this document is to define a framework for the principles and policies for a Payment System for the revocation of a Certification Authority Public Key used for Static and/or Dynamic Data Authentication as specified in the *EMV '96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1*.

Principles are concepts identified as the basis for implementing key revocation. These principles can give rise to policies that may be shared across the Payment Systems, or policies that are adopted by individual Payment Systems. Each Payment System will develop its own set of procedures to implement these policies.

This document is organised as follows.

- Sections 2 and 3 contain the references and terminology used in the key revocation process.
- Section 4 is an overview of public key management as it pertains to Certification Authority Public Keys in EMV.
- Section 5 contains key revocation principles and shared Payment System policies.
- Section 6 specifies key introduction and withdrawal timelines based on the principles and shared policies described in this document.

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 Terminal Public Key Management Requirements, version 1.0, March 31, 1999

3. Terminology

Accelerated Revocation: A key revocation performed on a date sooner than the published key expiry date.

Authentication: The provision of assurance of the claimed identity of an entity (ISO/IEC 10181-2: 1996).

Certificate: The public key and identity of an entity together with some other information, rendered unforgeable by signing with the secret key of the certification authority which issued that certificate.

Certificate Revocation: The process of revoking an otherwise valid certificate by the entity that issued that certificate.

Certification Authority: A centre trusted to create and assign public key certificates which provide evidence linking a public key and other relevant information to its owner (ISO/IEC 11770-3).

Key Expiry Date: The date after which a signature made with a particular key is no longer valid. Issuer certificates signed by the key must expire on or before this date. Keys may be removed from terminals after this date has passed.

Compromise: The breaching of secrecy or security. (ISO 8908)

Cryptoperiod: Defined period of time during which a specific cryptographic key is authorized for use, or during which time the cryptographic keys for a given system may remain in effect. (ISO 8908)

Data Key (KD): Cryptographic key used for the encipherment, decipherment or authentication of data. (ISO 8908)

Decipherment: Process of transforming cipher text into plain text. (ISO 8908)

Digital Signature: An asymmetric cryptographic function of data that allows the recipient of the data to prove the origin and integrity of the data, and protect the sender and the recipient of the data against forgery by third parties, and the sender against forgery by the recipient. *(EMV '96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1)*

Encipherment: the reversible transformation of data by a cryptographic algorithm to produce ciphertext. *(EMV '96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1)*

Expiry Date: Date after which a financial instrument or agreement ceases to be valid. (ISO 8908).

Key Activation: The process of beginning to use a key at the Certification Authority for the production of public key certificates.

Key Installation Deadline: The date by which all terminals must be able to verify issuer certificates based on this key, and the earliest date that cards may be issued that contain issuer certificates based on this key.

Key Introduction: The process of generating, distributing, and beginning use of a key pair.

Key Life Cycle: All phases of key management, from planning and generation, through revocation, destruction, and archiving.

Key Replacement: The simultaneous revocation of a key and introduction of a key to replaced the revoked one.
Key Revocation: The key management process of withdrawing a key from service and dealing with the legacy of its use. Key revocation can be as-scheduled or accelerated.
Key Revocation Date: The date after which no legitimate cards still in use should contain certificates signed by this key, and therefore the date after which this key can be deleted from terminals. For a planned revocation the Key Revocation Date is the same as the key expiry date.
Key Withdrawal: The process of removing a key from service as part of its revocation.
Logical Compromise: The compromise of a key through application of improved cryptanalytic techniques, increases in computing power, or combination of the two.
Migration Key: A key introduced into the system for future use.
Payment System: In the context of EMVCo, LLC Security Work Group and Key Revocation policies, Europay, MasterCard, or Visa.
Physical Compromise: The compromise of a key resulting from the fact that it has not been securely guarded, or a hardware security module has been stolen or accessed by unauthorised persons.
Planned Revocation: A key revocation performed as scheduled by the published key expiry date.
Potential Compromise: A condition where cryptanalytic techniques and/or computing power has advanced to the point that compromise of a key of a certain length is feasible or even likely.
Private Key: That key of an entity's asymmetric key pair that should only be used by that entity. In the case of a digital signature scheme, the private key defines the signature function. (*EMV '96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1)*
Public Key: That key of an entity's asymmetric key pair that can be made public. In the case of a digital signature scheme, the public key defines the verification functions. *(EMV '96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1)*
RSA Failure: An advance in mathematics, cryptanalysis or technology, that renders RSA key technology ineffective, regardless of key or key size.
Suspected Compromise: A condition where information from system monitoring indicates malfunction which could be caused by key compromise, but which has not been confirmed as such.

4. Certification Authority Public Key Management Overview

4.1 Background

The *EMV '96 Integrated Circuit Card Specifications for Payment Systems Version 3.1.1* defines two off-line Card Authentication Methods (CAM), namely:

- *Static Data Authentication*, where the Issuer pre-signs unique static card data to protect against alteration of the data after personalisation. During a transaction the terminal can retrieve this signed static data from the IC Card and verify its correctness.
- *Dynamic Data Authentication*, where during a transaction the IC Card produces a dynamic signature on a random challenge it has received from the terminal. By verifying this dynamic signature, the terminal can authenticate the IC Card, and confirm the legitimacy of critical IC Card data.

In order to ensure interoperability, both off-line CAMs are implemented using the RSA public key cryptosystem and public key certificates. In the case of Static Data Authentication, the Issuer Public Key is stored on the IC Card in the form of a public key certificate. A two-layer public key certification scheme is used where the Issuer has its own private key to sign the card data, and the corresponding Issuer public key is signed by the Payment System to create the Issuer Public Key Certificate.

In the case of Dynamic Data Authentication, a three-layer public key certification scheme is used where the IC Card owns a public key pair. The private key is used for signing the dynamic data, and the IC Card Public Key is stored on the IC Card in the form of a IC Card Public Key Certificate signed by the Issuer. The corresponding Issuer Public Key is also stored on the IC Card in the form of a Issuer Public Key Certificate signed by the Payment System.

These certification schemes ensure full interoperability for off-line CAM by just storing Payment System owned Certification Authority Public Keys in the terminals. For more details, see Part IV of *(EMV '96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1).*

The remainder of this chapter gives an overview of the key management of the Certification Authority Public Key pairs during their life cycle.

4.2 Certification Authority Public Key Life Cycle

4.2.1 Normal Certification Authority Public Key Life Cycle

The life cycle of a Certification Authority Public Key in normal circumstances can be divided into the following consecutive phases:

- Planning
- Generation
- Distribution
- Usage
- Revocation (Scheduled).

4.2.1.1 Planning

During the planning phase, the Payment System investigates the requirements for the introduction of new Certification Authority Public Key pairs in the near future. These requirements are related to the number of keys required and the parameters of these keys.

An important part of the planning phase is the review of the security of RSA to determine the life expectancy of existing and potential new keys. This review will lead to the setting of lengths and expiration dates for new keys and the potential modification of the expiration dates of existing keys, and a roll-out schedule of replacement keys.

4.2.1.2 Generation

If the results of the planning phase require the introduction of new Certification Authority Public Key pairs, these will have to be generated by the Payment System. More precisely, the Payment System Certification Authority (a physically and logically highly secured infrastructure operated by the Payment System) will generate in a secure way the necessary RSA Certification Authority Private/Public Key pairs for further use. Subsequent to generation the secrecy and integrity of the Certification Authority Private Keys must be maintained, and the integrity of both Certification Authority Public and Private Keys must also be maintained.

4.2.1.3 Distribution

In the key distribution phase, the Payment System Certification Authority will distribute newly generated Certification Authority Public Keys to its member Issuers and Acquirers for the following purposes (see Figure 1):

- To Issuers, to verify Issuer Public Key Certificates supplied by the Payment System Certification Authority during the key usage phase (see below).
- To Acquirers, for secure loading of the Certification Authority Public Keys in its merchant terminals.

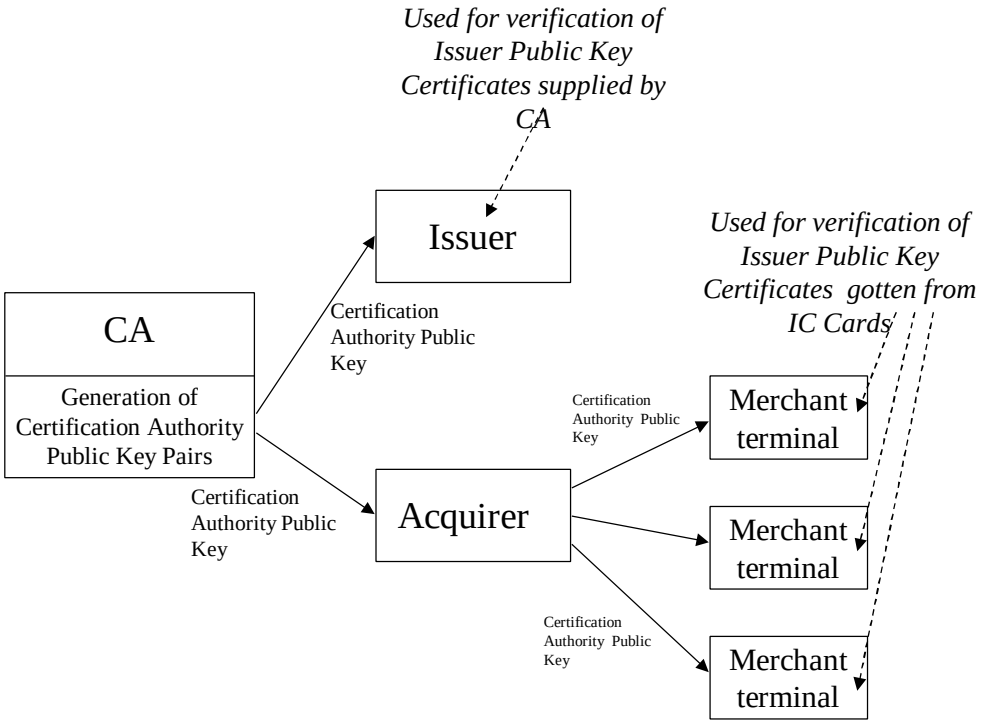


Figure 1 – Certification Authority Public Key Distribution

In order to prevent the introduction of fraudulent Certification Authority Public Keys, the interfaces between the Payment System Certification Authority and the Issuers and Acquirers need to ensure the integrity of the Certification Authority Public Keys distributed.

4.2.1.4 Usage

The Certification Authority Public Key is used in the merchant terminals to perform Static or Dynamic Data Authentication as specified in Part IV of *(EMV '96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1).*

The Certification Authority Private Key is used by the Payment System Certification Authority for the generation of the Issuer Public Key Certificates. More precisely, the following interactions take place (see Figure 2):

- The Issuer generates its Issuer Public Key and sends it to the Payment System Certification Authority.

- The Payment System Certification Authority signs the Issuer Public Key with the Certification Authority Private Key to obtain the Issuer Public Key Certificate that is returned to the Issuer.
- With the Certification Authority Public Key, the Issuer verifies the correctness of the received Issuer Public Key Certificate. If it is correct, the Issuer can then include it as part of the personalisation data for its IC Cards.

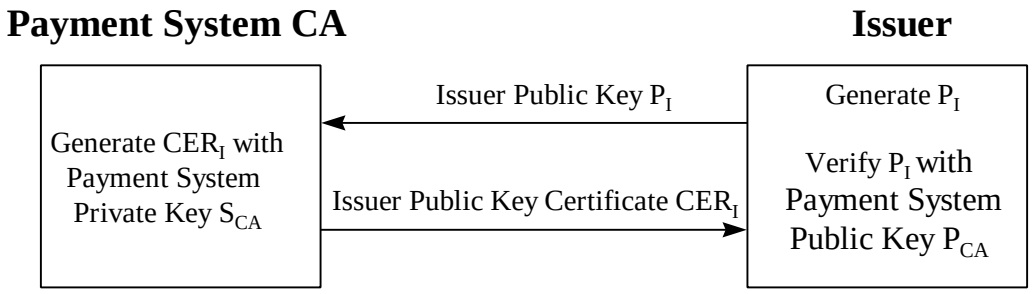


Figure 2 - Issuer Public Key Certification

In order to prevent the introduction of fraudulent Issuer Public Keys, the interfaces between the Issuer and the Payment System Certification Authority need to ensure the integrity of the Issuer Public Keys submitted for certification.

4.2.1.5 Revocation (Scheduled)

Once a Certification Authority Public Key pair has reached its planned expiration date set during the planning phase, it has to be removed from service. Practically speaking, this means the following.

- As of that expiration date, Issuer Public Key Certificates produced with the Certification Authority Private Key will no longer be valid. Issuers should

therefore ensure that IC Cards personalised with such Issuer Public Key Certificates expire no later than the expiration date of the Certification Authority Public Key pair.

- At an appropriate time prior to that expiration date, the Payment System Certification Authority will stop signing Issuer Public Keys with the corresponding Certification Authority Private Key.
- As of that expiration date, Acquirers need to remove the Certification Authority Public Keys from service in their terminals within a specific grace period after expiration.

.

4.2.2 Certification Authority Public Key Pair Compromise

In the event of a Certification Authority Public Key pair compromise, an emergency process needs to be put in place that in the end may lead to the accelerated revocation of the Certification Authority Public Key pair before its planned expiration. In this case, there are additional phases in the key life cycle:

- Detection
- Assessment
- Decision
- Revocation (Accelerated).

These phases are described below.

4.2.2.1 Detection

The compromise of a Certification Authority Public Key pair can be either an actual compromise, for example a confirmed security breach at the Payment System Certification Authority, or a confirmed breaking of the key by cryptanalysis. In addition, compromise may be:

- Suspected: system monitoring or member and cardholder complaint indicates that fraudulent transactions have occurred which could be due to key compromise, but this is not confirmed, or
- Potential: cryptanalytic techniques, for example factorisation, have developed such that with resources available any key of a given length could be compromised, but there is no evidence that this has occurred.

Detection of a key compromise may vary from awareness of an actual physical break-in of the Payment System Certification Authority, through the reporting of fraudulent off-line transactions by the fraud and risk management systems put in place by the Payment

System and its Members, to intelligence on factorisation advances gathered from the cryptographic community.

4.2.2.2 Assessment

The assessment of a (potential) Certification Authority Public Key pair compromise will include technical, risk and fraud, and, most importantly, business impacts for the Payment System and its Members. The results of the assessment will include the confirmation of the compromise, the determination of possible courses of action against costs and risk of the compromise, and presenting results of the assessment to support a decision.

4.2.2.3 Decision

Based on the results of the assessment phase, the Payment System will decide on a course of action that will be taken for a key compromise. In the worst case, this decision will consist of the actual unplanned revocation of a Certification Authority Public Key before its planned expiration date.

4.2.2.4 Revocation (Accelerated)

The decision to revoke a Certification Authority Public Key will lead to the communication to the Payment System Members of a new expiration date of that key. The process after that is the same as for the planned revocation described in Section 4.2.1.5.

5. Key Revocation Principles and Policies by Phase

This section outlines principles and policies for Certification Authority Public Key Revocation that will be followed by EMV participants. After presenting general revocation principles, the section is divided into the key life cycle phases defined in the previous section. Each phase presents key revocation principles and the policies that EMV participants have agreed to as shared policies for that phase of the Certification Authority key life cycle.

5.1 General Principles

- Support of Certification Authority Public Key revocation is a requirement for each Payment System's IC Card credit and debit products.
- Payment Systems will align policies, procedures, and schedules for Certification Authority Public Key revocation where practical.
- EMVCo, LLC will develop a common definition of the phases of the Certification Authority Public Key revocation process and agree on common terminology to be used in internal and Member communications.
- Each Payment System operates as a closed system with regard to any legal requirements relative to Certification Authority Public Key pairs.

5.2 Planning Phase

Phase Definition: The Planning phase involves review and planning of Certification Authority Public Key pairs. Existing keys are reviewed for resistance to attack, and new key planning is undertaken. Length and expiration dates of existing and new keys are reviewed by risk and cryptography staff to confirm that the key life expectancy is considered secure. Lengths of new keys are determined, and a rollout schedule of replacement keys is maintained.

5.2.1 EMV Principles

- Key sizes should reflect maximum feasible security consistent with terminal capability and POS operational timing.
- Payment Systems should synchronize the expiration date of keys of a particular length where practical. Final decision authority for key revocation rests with each Payment System.

- In the event of announcement of an accelerated revocation by a Payment System, the Payment System may request convening an EMVCo, LLC Security Working Group planning session to address the revocation, the key compromise, and its impacts.

.

5.2.2 Shared Payment System Policies

- EMVCo, LLC will conduct annual review sessions for Certification Authority Public Key pair strength evaluation, using state of the art information and analysis from the fields of computer science, cryptography, and data security. Any Payment System may request an emergency meeting for key review at any time.
- EMVCo, LLC will prepare "best information" estimates of relative key strength for existing key lengths based on current evaluation criteria, and will make recommendations for rollout of new key lengths.
- The recommendations of this review process will be circulated to the Payment Systems, who will use them to set their individual policies. Each Payment System will identify areas where Payment System differentiation is required.
- Payment Systems will use EMVCo, LLC recommendations as a factor in determining policy on number and length of live keys, exponent value, expiry date, and planned revocation schedule. Payment Systems will publish these details to members within 90 days of receipt of EMVCo, LLC recommendations.
- Key replacement will normally be on a planned, scheduled basis, but can be accelerated based on results of key life review.
- All Certification Authority Public Keys will have December 31st as planned expiration date.
- Acquirers have a six month grace period starting from the planned expiration date (until June 30th of the following calendar year) to withdraw an expired key from all terminals.
- All new Certification Authority Public Keys will be distributed prior to December 31st.
- Acquirers have a six month grace period (until June 30th of the following calendar year) to install any new keys in all terminals.
- New Certification Authority Public Key pairs will be valid starting July 1st of that same calendar year.

- The existing Certification Authority Public Keys will be revoked on December 31, 2002 (768 bit), December 31, 2004 (896 bit), and December 31, 2007 (1024 bit).[1]
- In the event of an accelerated revocation, a six-month grace period will similarly be maintained for key withdrawal in all terminals, but the fixed date of December 31st is not applicable.
- Notification to members and timing for any key revocation is the responsibility of each Payment System.

5.3 Generation Phase

Phase Definition: Key generation is the process of a Payment System generating a Certification Authority Public Key pair.

5.3.1 EMV Principles

- Certification Authority Public Key pairs shall be generated in a secure environment according to accepted industry practice.
- Within each Registered Application Provider Identifier (RID), the Certification Authority Public Key Index is a unique value pointing to a particular Certification Authority Public Key pair. The value of a Certification Authority Public Key Index for a specific key shall not be changed.

.

5.3.2 Shared Payment System Policies

- None Identified.

.

5.4 Distribution Phase

Phase Definition: Key distribution is the process of circulating the public component of a Certification Authority Public Key Pair to get it into the marketplace. Certification Authority Public Keys must ultimately appear in merchant terminals. Certification Authority Private Keys will be used to produce Issuer Public Key Certificates, and are to be kept in the secure environment of the Payment System certification Authority.

[1] The Europay/MasterCard 768 bit key was scheduled to be revoked on October 31, 2002. This date is now being changed to December 31, 2002.

5.4.1 EMV Principles

- Key distribution will ensure of key integrity and origin authenticity.

.

5.4.2 Shared Payment System Policies

- Payment Systems will support distribution of their public keys from the Certification Authority to Acquirers and Issuers via physical or electronic means.
- All new Certification Authority Public Keys will be distributed for receipt by recipients before December 31st.
- Payment Systems will include a method allowing a recipient to validate a received public key, regardless of method of transmittal.
- Certification Authority Public Keys will be distributed to Acquirers with adequate lead time to allow installation in terminals before the corresponding private key is used to sign Issuer Public Keys.
- Certification Authority Public Keys will be distributed to Issuers so that they may validate the Issuer Public Key Certificates produced by the Certification Authority.
- Each Payment System Certification Authority will ensure that it does not distribute more than the maximum number of keys that can be stored per RID in a terminal (see Section 5.5).

5.5 Key Usage Phase

Phase Definition: This phase is concerned with the normal day to day use of the Certification Authority Public Key pairs. Copies of the Certification Authority Public Keys will be used by terminals to perform Static or Dynamic Data Authentication (SDA or DDA) during transactions with the appropriate Payment System branded cards. The Certification Authority Private Keys will be held in the Payment System Certification Authority and used to sign Issuer Public Keys, creating Issuer Public Key Certificates which the issuer will personalize onto its cards.

5.5.1 EMV Principles

- Terminals that support SDA and/or DDA shall provide support for six Certification Authority Public Keys per RID for Europay, MasterCard and Visa debit/credit applications based on EMV'96 Version 3.1.1. Terminals shall support these keys up to 1984 bits (248 bytes) in length, as specified in EMV'96 Version 3.1.1.

- Terminals shall support the ability to install a Certification Authority Public Key, and the ability to withdraw a key from service as of a given date.
- Terminals shall have the ability to validate Certification Authority Public Key integrity.
- Payment Systems will be responsible for ensuring the security of their Certification Authority Public Key pairs.

.

5.5.2 Shared Payment System Policies

- Payment Systems will validate the integrity and origin of Issuer Public Keys prior to issuing a certificate.
- A Payment System Certification Authority will begin using the private component of a Certification Authority Public Key pair no sooner than six months after the distribution of that key to Acquirers.
- The expiry date of any issued IC Card shall be no later than the expiry date of the Issuer Public Key Certificate on that IC Card, and shall be no later than the published (at the time of card issuance) revocation date of the Certification Authority Public Key pair used to produce the Issuer Public Key Certificate.
- The expiry date of an Issuer Public Key Certificate shall be no later than the published (at the time of certificate issuance) revocation date of the Certification Authority Public Key pair used to produce the Issuer Public Key Certificate.
- The expiry date of an IC Card Public Key Certificate shall be no later than the expiry date of the Issuer Public Key used to produce the IC Card Public Key Certificate.

5.6 Detection Phase

Phase Definition: The process that enables an entity to recognize that a Certification Authority Public Key pair has been, or is suspected of being compromised. There are multiple types of compromise, including physical and logical, suspected, potential, and confirmed.

5.6.1 EMV Principles

- EMVCo, LLC will provide a forum for Payment Systems to share evaluation of cryptanalytic advances that might lead to potential compromise of the digital signature scheme specified in *(EMV '96 Integrated Circuit Card Specifications for Payment Systems, Version 3.1.1).*

- Monitoring of key integrity and detection of suspected or potential Certification Authority Public Key pair compromise is the responsibility of each Payment System.

.

5.6.2 Shared Payment System Policies

- Members shall notify a Payment System of conditions or transactions that indicate possible or suspected compromise of a specific Certification Authority Public Key pair from that Payment System.

5.7 Assessment Phase

NOTE: **This phase applies only to accelerated revocations.**
Phase Definition: If a Certification Authority Public Key compromise is detected or suspected, the owning Payment System must assess the impact to business operations. Assessment includes confirming the compromise, determining possible courses of action, evaluating the cost of action against costs and risk of the compromise, and presenting results of the assessment to support a decision.

5.7.1 EMV Principles

- Assessment of suspected or potential Certification Authority Public Key pair compromise is the responsibility of each Payment System.
- Payment Systems will develop assessment policies and procedures that follow generally accepted best practices in risk management.
- There are different levels of compromise requiring different sets of actions depending on the compromise and a business assessment.

.

5.7.2 Shared Payment System Policies

- Payment System assessment will include actual and reputational costs to the Payment System and to Members. Potential courses of action will include an assessment of Member and marketplace impact.

5.8 Decision Phase

NOTE: **This phase applies only to accelerated revocations.**
Phase Definition: As a result of the assessment phase, a Payment System decides on a course of action that will be taken for a Certification Authority Public Key pair compromise.

5.8.1 EMV Principles

- The decision to revoke a specific Certification Authority Public Key Pair is at the sole discretion of the Payment System that operates the Certification Authority for that key.
- Payment Systems will develop and publish to their Members a set of policies and procedures that detail the decision-making process for accelerated key revocation. These policies will include a method of notification to all effected Issuers and Acquirers.

.

5.8.2 Shared Payment System Policies

- None identified.

5.9 Revocation Phase

Phase Definition: The key management process of withdrawing a key from service and dealing with the legacy of its use. Key revocation can be on schedule or accelerated. In the case of Certification Authority Public Key pairs, revocation means that the private key is no longer used to produce Issuer Public Key Certificates and that copies of the public key are withdrawn from service in terminals. Issuer Public Key Certificates signed with the private key are (as of a specific date) no longer valid in circulation on IC Cards.

5.9.1 EMV Principles

- Certification Authority Public Key revocation will be according to a previously published schedule unless a Payment System has detected an imminent threat to product security. All scheduled revocations will conform to the "revocation window" dates developed by EMVCo, LLC.
- In case of an accelerated revocation, Payment Systems will take Member impact into account, including terminal access, card re-issuance, and increased network traffic. Lead times for Member activities shall be the same as during a scheduled revocation.

.

5.9.2 Shared Payment System Policies

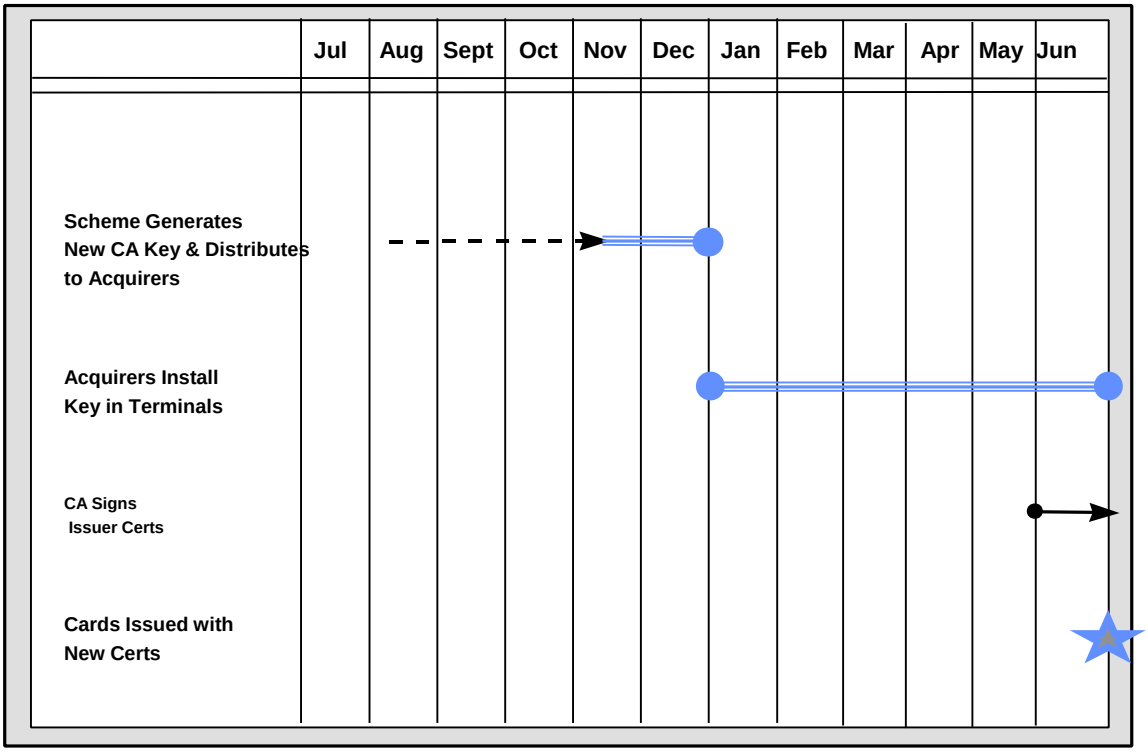
- Revocation policies and procedures will be the same as for scheduled and accelerated revocations, wherever practical.
- All Certification Authority Public Keys will have December 31st as their planned expiration date. Acquirers shall have a six month grace period (until June 30th of the following calendar year) to withdraw the revoked key.

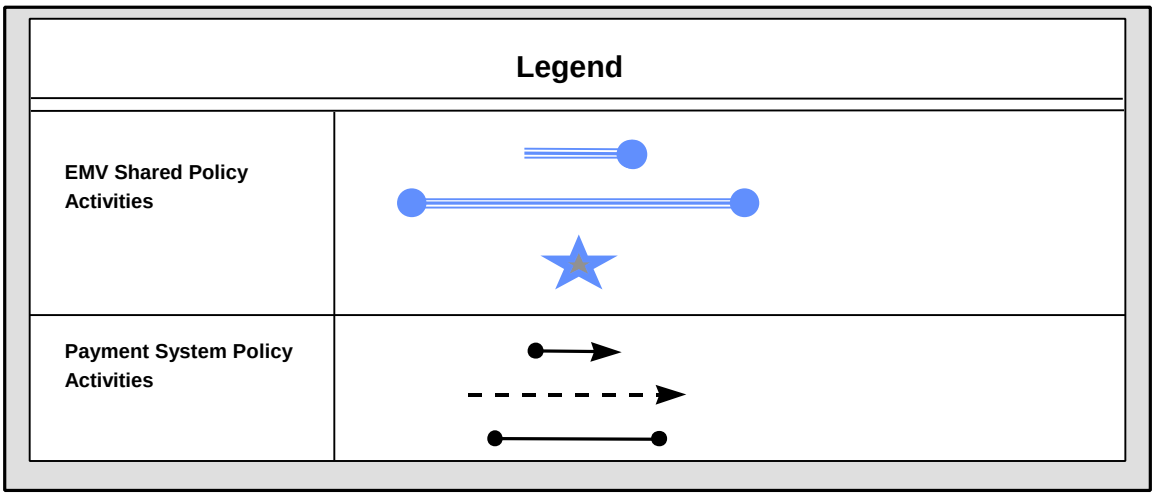
- Revocation of a Certification Authority Public Key pair requires that the public key component is withdrawn from service in all terminals within a six-month timeframe, consistent with Payment System rules.
- In the case of an accelerated revocation, the introduction and withdrawal lead times will be the same as for scheduled revocations, however, the revocation date will be determined at the discretion of the Payment System.

6. Sample Timelines

The following pages present sample timelines for the revocation and introduction of Certification Authority Public Keys based on the principles and policies detailed in this document. Each timeline represents a scheduled key introduction or withdrawal. In the case of an accelerated introduction or withdrawal, lead times for tasks would remain the same, but the month of the actual key introduction date and key revocation would be at the discretion of the Payment System.

6.1 Key Introduction





6.2 Key Withdrawal