Visa Secure Element Renewal and Lifecycle Management

White Paper

Version 1.0

March 2015

Visa Public

Important Information on Confidentiality and Copyright

Note: This document is not part of the Visa Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Rules, the Visa Rules shall govern and control.

Contents

1 Summary

Visa has evolved its mobile secure element [1] compliance and renewal policy to meet today's mobile industry requirements. The new Visa policy:

- simplifies the secure element compliance and management process and provides transparency to all stakeholders who need to manage, develop, deploy, and replace Visa applications on secure element products.
- leverages the EMVCo platform certification process for product security evaluations, the GlobalPlatform composition model to manage additional applications, software update mechanisms to update products in the field, as well as additional controls that secure elements provide to manage risk.
- applies to all secure element form factors including removable products (such as UICC and microSD [2]) and embedded secure elements in handsets.

2 Background

The legacy Visa secure element compliance policy was based on a card product model that was used successfully for over 15 years. In this model the issuer has a direct cardholder relationship and has control over the card issuance lifecycle.

In a mobile environment, the Mobile Network Operator (MNO) is typically the owner and distributor of the secure element (e.g., Subscriber Identification Module (SIM)). This creates challenges in that an MNO does not know how long the distributed SIM is valid for payment applications and does not track this. There is a possibility that an issuer may have to request the MNO to replace an expired SIM if they want to continue offering the same payment functionality on the cardholder's mobile device.

In the mobile model the relationship between MNO, handset issuer, issuing bank ("issuer"), and end user ("cardholder") is more complex than the single relationship for cards. Additionally, secure elements operate in a different risk model, are virtually always online, and allow for software updates in real time in the field.

When operating under the re-certification requirements in the card-based mobile policy, the lifespan of a secure element is not known in advance and in the worst case would require a SIM card to be replaced within less than three years of usage. This is undesirable from an MNO's perspective and,

[1] A secure element is an EMVCo platform product with a payment application developed using the Visa mobile specifications, for example the Visa Mobile Payment Application (VMPA).

[2] The policy does not apply to microSDs with an internal antenna. Refer to the *Visa Mobile Testing & Compliance Requirements for MicroSDs and Mobile Accessories* document at https://technologypartner.visa.com for details.

because today's secure element compliance model unfortunately does not include full lifecycle management, is also undesirable from a risk management and issuer perspective.

The new Visa secure element policy addresses these concerns and emphasizes industry best practices.

3 New secure element policy

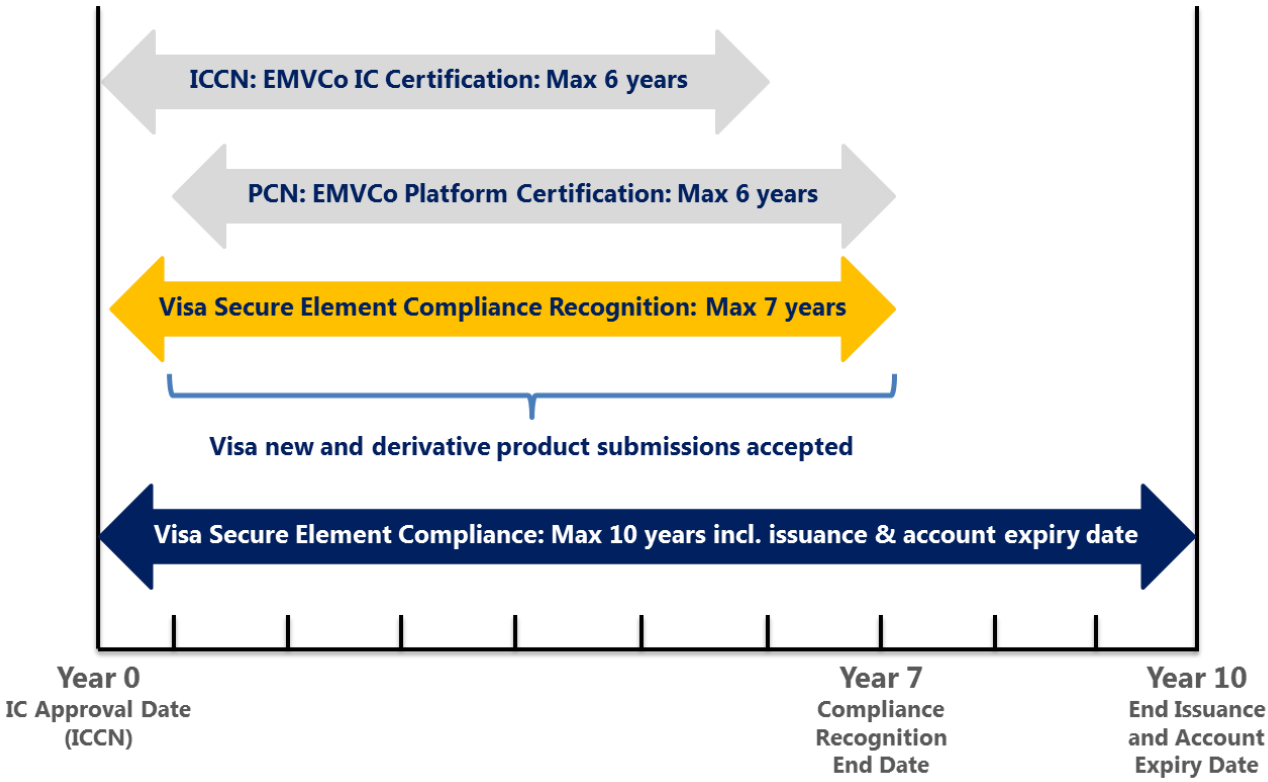
The new Visa secure element renewal and lifecycle management policy has two significant changes:

- The functional and security renewal testing requirement is removed for the vendor of the secure element product.
- The issuer must set the account expiry date for the Visa mobile payment account to at most ten years from the EMVCo assigned IC Certificate Number (ICCN) issue date.

The new policy is illustrated in Figure 1.

As before, a Visa application on a new secure element product can only be found compliant if it has a valid EMVCo Platform Certificate Number (PCN). With the new policy, the maximum compliance period (time that a vendor can sell their secure element product) is the EMVCo ICCN issue date + 7 years. Secure element product derivatives and updates follow the normal Visa compliance process. If issues are identified with the secure element product, the established Visa process will be followed.

Figure 1: New Visa secure element policy illustrated



The Visa application can be provisioned on the secure element (e.g., UICC) and instantiated any time until reaching the original ICCN issue date plus the 10 years milestone. Issuers will be required to limit the expiry date on a Visa mobile payment account. Following industry best practices, it is recommended that they set the expiry date to not exceed three years. The exception is when it is known at time of personalization, the issuer can set the account expiry date to any period up to the EMVCo ICCN issue date + 10 years.

The Visa compliance policy pertains only to the Visa payment application on a secure element product. Any application loaded on a Visa approved product must not impact the security of the Visa payment application assets. Visa does not provide security approval for additional applications. Applications that do impact the Visa payment application must be evaluated by a Visa-recognized security laboratory and the evaluation report must be submitted to Visa Approval Services for review.

4 Rationale for new policy

The following are the underlying principles of the new Visa secure element policy.

- Comprehensive testing - Focus on thorough functional and security testing during product submission, not on renewal testing.
    - The Industry has matured and vendors develop their products according to industry best practices. Visa has defined minimum platform requirements and Visa applets meet baseline security requirements.
    - Even though security degrades over time, risks related to evolving new attacks in the field can be managed without the need of a renewal testing requirement.
    - Eliminating the functional and security renewal testing requirement will facilitate simplified product management by avoiding unnecessary and redundant testing and paperwork.
- Transparency - Implement full lifecycle management with secure element end-of-life date.
    - Provide a uniform message to industry by managing the secure element product life-cycle including the account expiry date.
    - Allow issuers the flexibility to define stricter expiry dates based on their own risk assessment and risk tolerance.
    - Know the end-of-life date upfront when a compliant secure element is sold.
- Industry Best Practices - Build new products on recently approved chip products.
    - Encourage secure element development based on newer chip products in order to maximize product lifetime in market.
    - Manage secure elements via operating system update, application update, and patch mechanisms. In worst case, deactivate an insecure application. However, if the underlying hardware is insecure, it cannot be updated in the field. As the chip hardware ("IC") is the lowest common dominator, the product lifecycle is not managed by end-product, but by underlying IC.

- Tie the end-of-life date to the approval date of the underlying IC product + 10 years. This is the current maximum lifetime of an EMVCo approved platform with the industry recommended three year expiry date (see also Figure 1).

5 Role of EMVCo

EMVCo acts as the security certification entity for chip hardware and platform products. Visa leverages the EMVCo process for its secure element products to minimize cost and time spent in performing evaluation work and to avoid duplication of effort. Details about the EMVCo security evaluation and certification process can be found at www.emvco.com. EMVCo security evaluations are based on a modular certification process where the chip hardware is the lowest common denominator and a platform product (secure element without Visa payment application) is approved on top of it.

- Chip hardware is defined as the basic 'chip' or 'IC' product without a card operating system or application. EMVCo issues an IC certificate with an IC Certificate Number (ICCN) when a product provider has successfully completed the EMVCo IC security evaluation process.
- A platform product is defined as the integrated circuit (IC) hardware with its dedicated software, operating system, run time environment, and platform environment on which one or more applications (e.g., VMPA) can be executed. EMVCo issues a platform certificate with a Platform Certificate Number (PCN) for platform products that have successfully completed the EMVCo security evaluation process.

Visa will accept new secure element products for testing only if the platform product has successfully completed the EMVCo platform security evaluation process and is listed on the EMVCo approved platform list (see Figure 1).

6 Benefits for the mobile payment industry

The new policy enables all stakeholders to better understand the exact validity length of any secure element product being deployed. A defined end-of-life date that all parties are aware of, based on industry feedback and best practices, is considered a significant benefit.

Secure element vendors can realize cost, time, and management savings as no renewal testing and re-certification is required. The policy encourages secure element development based on newer chip products in order to maximize product lifetime in market.

For secure element owners and issuers, the policy facilitates better purchasing decisions, inventory management, and product replacement planning as the product-specific expiry date is known in advance. The policy provides clarity for the product business case, lifetime, and replacement.

The end user can proactively manage the replacement of a removable secure element.