Visa Card Lifecycle Management Policy

Version 2.0

Visa Confidential
June 2026

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

Contents 1

Tables 2

Figures 2

Document History 3

References 3

Supporting and Contact Information 4

1 Introduction 5

2 New Card Lifecycle Management Policy 5

2.1 “New” Product Submission 5

2.2 “Extension” Production Submission 6

2.3 Change and Derivative Product Submissions 8

3 Rationale for the update 9

4 Notes to Issuers 10

5 Role of EMVCo 10

Tables

Table 1 Document History 3

Table 2 References 3

Figures

Figure 1. New Product submission illustration 6

Figure 2. Extension submission illustration 7

Figure 3. Extension submission impact on Derivatives and Change products 8

Figure 4. Derivatives and Change product submissions 9

Document History

Version	Date	Changes description
1.0	November 2015	Initial release
2.0	June 2026	Introduced options to extend card “Usage Period” from EMVCo ICCN+12 years to ICCN+15 years

Table 1 Document History

References

Reference	Document Title/Name, Version, Date	Description
[VCSP_TestReq]	Visa Chip Security Program – Testing Requirements and Guidance, Version 1.2, August 2024	Details the Visa’s requirements and provides guidance when conducting security testing of chip based payment products
[EMVCo_Cert]	EMVCo-SEWG-15-W01 – EMVCo Certificate Issuance, Renewal, and Extension Process, v2.2, January 2026	Describes the EMVCo security certificate issuance and renewal process on IC, Platform and Card products
[JIL_AP]	JIL - Application of Attack Potential to Smartcards and Similar Devices, Version 3.2.1, February 2024	This document interprets the current version of Common Criteria Methodology [CEM], where it provides guidance metrics to calculate attack potential required by an attacker to effect an attack. *This work has been based on smartcard CC evaluation experience and input from smartcard industry through the International Security Certification Initiative (ISCI) and the JIL Hardware Attacks Subgroup (JHAS).*

Table 2 References

Supporting and Contact Information

Approval Services oversees testing of chip based payment products that will carry the Visa brand to evaluate whether they are developed in compliance with the mandatory provisions of Visa specifications and requirements. Security testing is one aspect of the chip based payment product approval process. Approval Services provides a single point of contact, both for vendors and for Laboratories, on the testing and approval process. For help and support, contact Approval Services.

Email address:	ApprovalServices@visa.com
Web site:	https://digitalpartnerservices.visaonline.com

For detailed information on the IC and Platform security evaluations, please see EMVCo security evaluation process available at www.emvco.com, or contact the EMVCo security evaluation secretariat at securityevaluation@emvco.com with any questions on the process.

1 Introduction

Visa has updated its card lifecycle management policy to better support current market requirements for chip card issuance while maintaining lifecycle control consistent with current chip technology and industry practice. These updates are designed to provide additional flexibility within the card lifecycle framework while continuing to maintain appropriate security assurance throughout the card lifecycle.

Visa previously replaced the former approval-period model with a **Usage Period** framework covering the entire life of the product in the field. Under this framework, each approved card product is issued a Visa Letter of Approval (LOA) with an assigned Usage Period beginning on the date the underlying chip receives EMVCo approval, that is, the ICCN issuance date. By the end of that Usage Period, all cards issued under the relevant LOA must be expired, cancelled, or replaced by the issuer. This requirement applies to all card product submission types, including New, Change, and Derivative submissions, unless a shorter or otherwise restricted Usage Period is imposed as a result of testing during the approval process.

While retaining the Usage Period framework, Visa is now updating the policy to support products that may require longer card expiry periods in the field than the typical industry norm of three to five years. The revised lifecycle policy therefore introduces a more flexible framework for eligible products while preserving Visa review and approval controls. This update also reflects the current maturity of chip technology and security mechanisms, together with EMVCo's revised certification lifecycle process described in *[EMVCo_Cert]* permitting extensions of chip product certifications for up to 10 years, including for IC (ICCN) and Platform (PCN) certifications.

2 New Card Lifecycle Management Policy

The following subsections set out the details of the Visa Card Lifecycle Management Policy. Collectively, they define Visa's card lifecycle management framework, under which a shorter or otherwise restricted Usage Period may be imposed, as necessary, based on testing results, approval conditions, or other product-specific considerations.

2.1 "New" Product Submission

The following policy and requirements apply to **New** card product submissions:

- Submissions are accepted only if the underlying **EMVCo ICCN is valid**, up to a maximum of 10 years from its initial issuance.

- Upon successful completion of applicable testing requirements and final approval by Visa,
    - new products **submitted before EMVCo ICCN + 4 years** will be assigned a Usage Period of **ICCN + 12 years**.
    - new products **submitted on or after EMVCo ICCN + 4 years** will be assigned Usage Period of **ICCN + 15 years**.

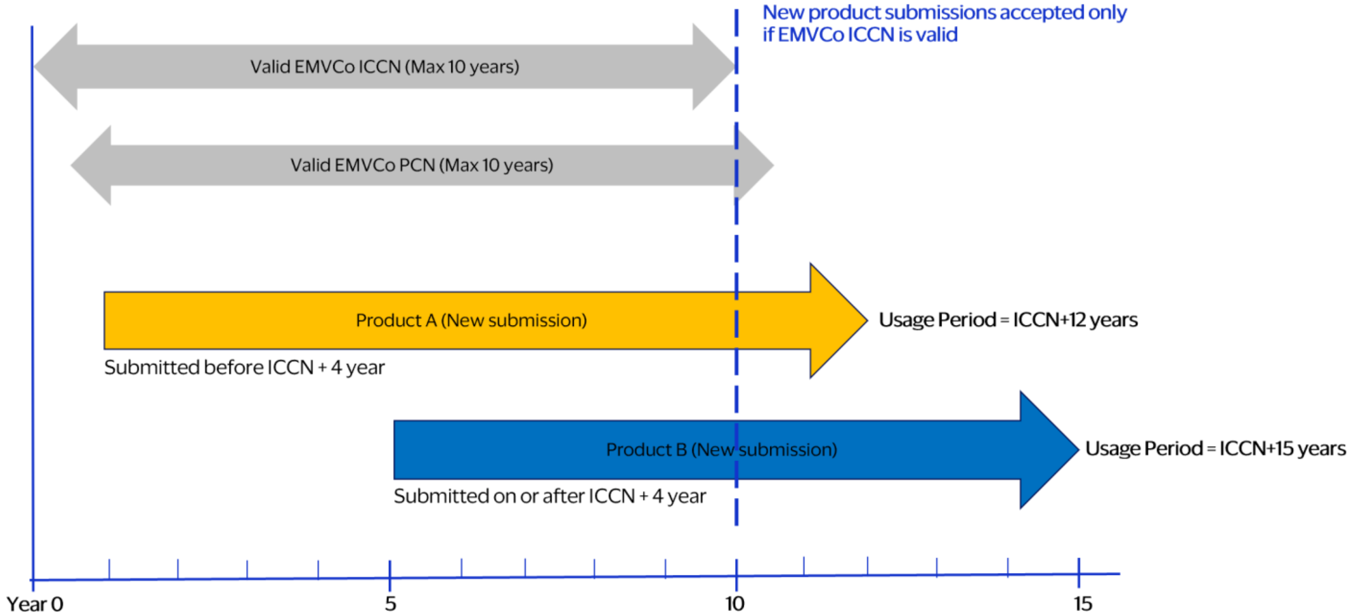

Figure 1. New Product submission illustration

2.2 "Extension" Production Submission

This policy introduces a new submission type, referred to as **Extension**. It allows the extension of the Usage Period of an approved card product to a maximum of **ICCN + 15 years**.

An **Extension** submission is subject to the following conditions:

- Accepted only for an **existing approved** card product, provided that it is **not subject to any restriction** and **has not been modified**.

- The product is **submitted on or after EMVCo ICCN + 4 years** of the underlying chip.

- Only **Full security testing is required** (Cross-testing, Level 1, and Level 2 functional testing are not required).
    - The card product must demonstrate resistance to attackers with **"High"** attack potential, as described in the Application of Attack Potential to Smartcards *[JIL_AP]*.
    - Security testing must consider state-of-the-art attack methods. This requires underlying components to have valid EMVCo ICCN (and PCN, if applicable) or at least have undergone EMVCo Extension Process to obtain valid and up-to-date testing evidence for these components.
    - Re-use of testing evidence from within the same product family (i.e. products based on the same parent product) is permitted, provided the test is considered valid and applicable to the target product, in accordance with the VCSP Testing Requirement and Guidance document *[VCSP_TestReq]*. The approach enables multiple card products within the same

family, when submitted for extension, to leverage common testing results thereby reducing testing effort, time and associated costs.

- Upon approval, the Usage Period extension applies only to the specific product submitted and tested. The extension does not apply retroactively to other previously approved products within the same card family, unless those products are separately submitted and approved under an Extension submission.

  For a previously approved Parent, Change or Derivative product submitted for extension, security testing may not be required if the differences from a successfully extended product in the same family are determined to have no security impact, such as differences related to the card body or antenna design. Any such determination remains subject to Visa review and approval.

- The maximum Usage Period is ICCN + 15 years. Extension submissions are not permitted for products that already have an assigned Usage Period of ICCN + 15 years.

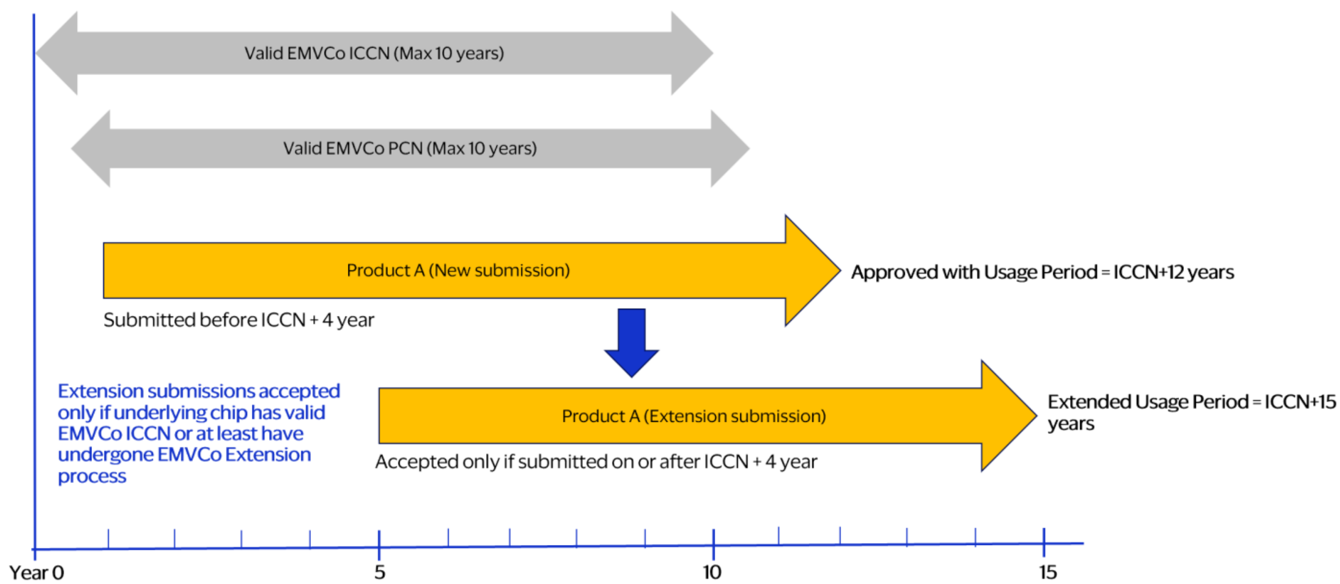

Figure 2. Extension submission illustration

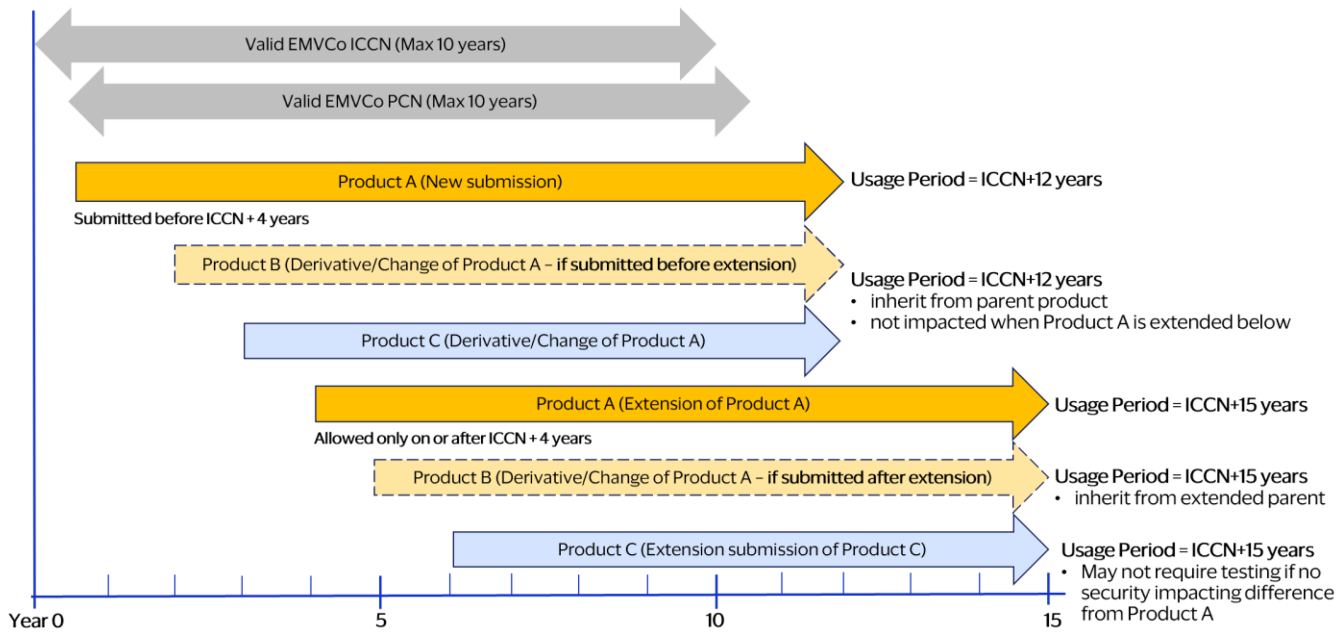

Figure 3. Extension submission impact on Derivatives and Change products

Note:

*While the **Extension** submission enables an increase to a product's Usage Period, Visa recommends that its use be limited to card products with real business need for extended card issuance expiry periods in the field. Partners are further encouraged to continue refreshing and migrating card products as frequently as practicable in order to maintain alignment with the latest specifications and technology.*

2.3 Change and Derivative Product Submissions

Newly submitted Change and Derivative products will continue to inherit the Usage Period of the parent product, whether it is ICCN + 12 years or ICCN + 15 years, in accordance with the updated policy.

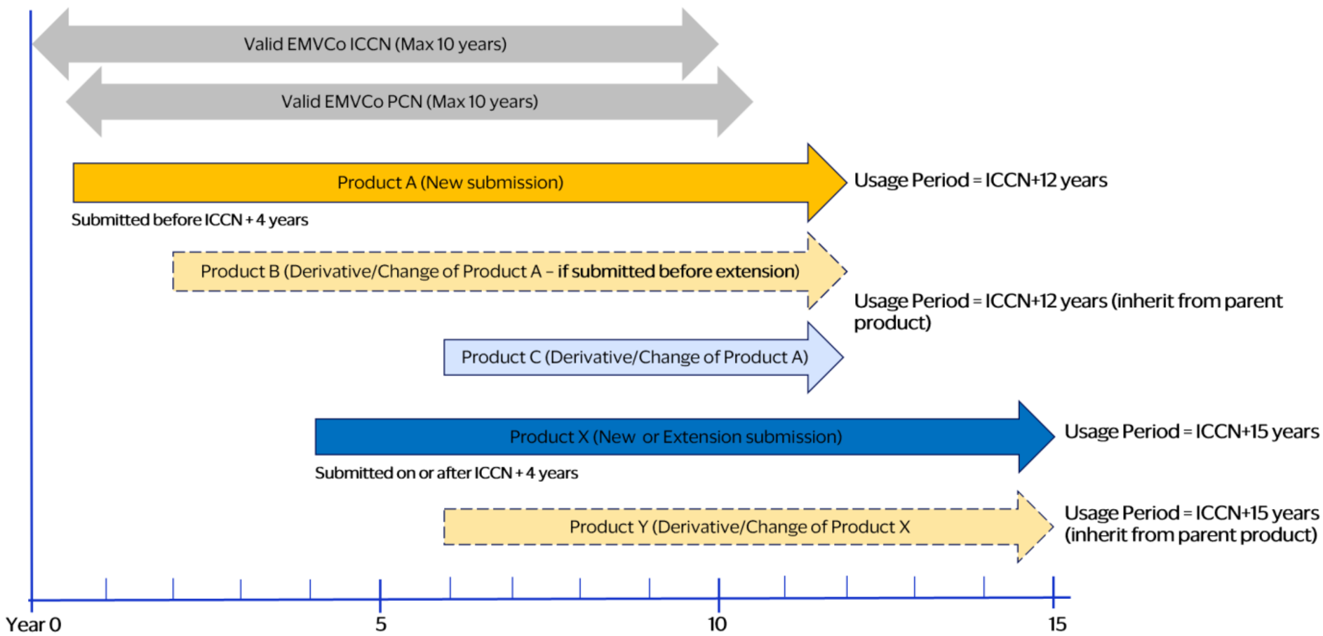

Figure 4. Derivatives and Change product submissions

3 Rationale for the update

The updated policy is intended to:

- Accommodate needs in certain markets for cards issuance with longer expiration period than standard industry practice, while not increasing the need for Vendors and Issuers to cycle their product more often, thereby not increasing testing effort, cost, migration complexity and inventory-management burden.

- Visa has received feedback from chip manufacturers indicating that current chip technology and security mechanisms have reached a higher level of maturity. Further design enhancements are becoming increasingly complex and resource-intensive, while delivering only marginal improvements in cost efficiency and security.

  In acknowldgement of this technology landscape and in conjunction with EMVCo's updated certification model, specifically the extension of chip product certifications for up to 10 years *[EMVCo_Cert]*, this policy updates allow longer lifespan of the underlying IC and card products in the field while still providing equivalent security assurance.

4 Notes to Issuers

In connection with these Card Lifecycle Management Policy updates, the following requirements and guidance apply to issuers:

- Issuers are required to verify the Usage Period assigned to card products they intend to issue to cardholders in order to ensure compliance with applicable Visa rules and this policy. The assigned Usage Period may be confirmed through the approved chip card products list published in https://digitalpartnerservices.visaonline.com or through the corresponding card product's LOA available from respective card vendor.
- Although card products may be assigned an extended Usage Period, issuers are advised, where practicable, to continue issuing cards with expiry dates consistent with prevailing industry practice (i.e. up to five years), unless longer expiry periods are required due to market-specific considerations.
- More so for cards issued with longer expiry dates, issuers should ensure that the corresponding certificates loaded onto the card remain valid through the card's expiry date. This is necessary to prevent field issues arising from expired certificates used during data authentication process in payment transactions.

5 Role of EMVCo

EMVCo acts as the security certification entity for chip hardware and platform products. Visa incorporates the EMVCo process for its card 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 card product (e.g. VSDC) 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.

Recognizing the importance of the underlyng IC to the overall security posture of card products, Visa bases the assigned Usage Period of an approved card product on the EMVCo ICCN issuance date of the underlying chip.

End of Document