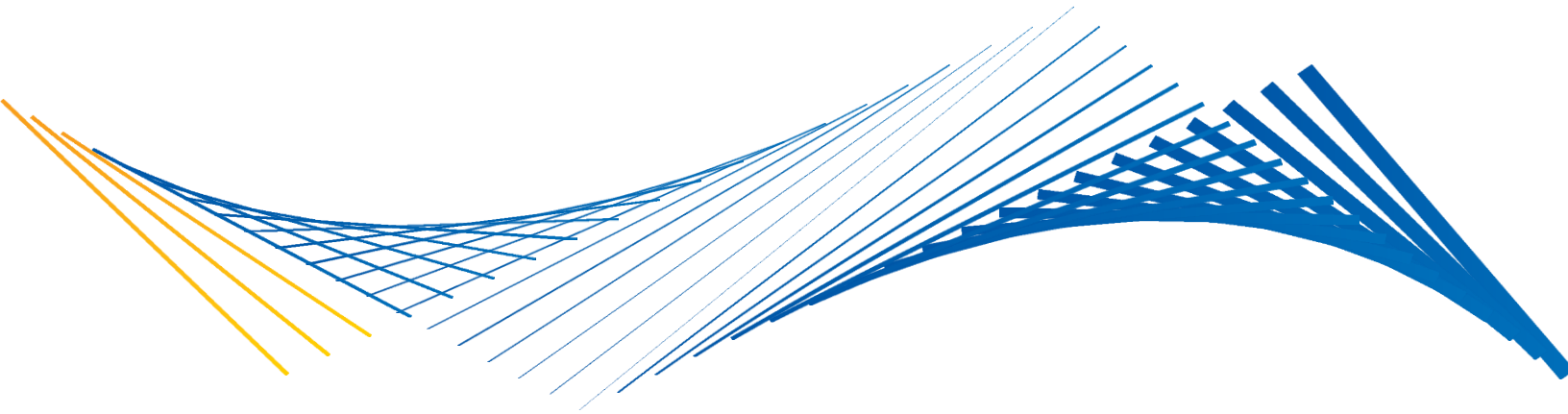
Frequently Asked Questions (FAQs)

Visa Chip Security Program

Security Evaluation Testing and Process

Version 1.3



Visa Approval Services
Visa Public
August 2024

Important Information on Confidentiality and Copyright

Note: This document is not part of the Visa Core Rules and Visa Product and Service 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 Core Rules and Visa Product and Service Rules, the Visa Core Rules and Visa Product and Service Rules shall govern and control.

Table of Contents

Abbreviations and Notations

Table below shows this Abbreviations and Notations used in this FAQ.

Table 1 Abbreviations and Notations

Abbreviation	Description
dCVV2	Dynamic Card Verification Value
IAL	Initial Assessment Letter
ICCN	Integrated Circuit Certification Number
LOA	Letter of Approval
LOQ	Letter of Qualification
PCN	Platform Certification Number
SE	Secure Element
VCSP	Visa Chip Security Program
VSDC	Visa Smart Debit/Credit
VMPA	Visa Mobile Payment Application

References

The following are the references used in this FAQ.

1. *Visa Chip Security Program, Security Testing Process Version 2.4, August 2024*
2. *Visa Chip Security Program VSDC Applet Security Guidance, Version 2.7, April 2023*
3. *Visa Chip Security Program VMPA Applet Security Guidance, Version 2.0, June 2018*
4. *EMVCo Security Guidelines, Security Evaluation Guidance (from www.emvco.com)*
5. *Visa Chip Security Program Security Testing Requirements and Guidance, Version 1.2, August 2024*

Support and Contact Information

Table below shows Approval Services' Support and Contact information.

Table 2 Support and Contact Information

Communication Method	Contact Information
Email	ApprovalServices@visa.com
Visa Digital Partner Services (VDPS) Website	https://digitalpartnerservices.visaonline.com
Postal Address:	Visa Approval Services Mailstop M3-2NW 900 Metro Center Blvd Foster City, California 94404 U.S.A.

1 General Questions

1.1 Where can I find the Visa Approved Products Lists?

The Visa Approved Chip Products lists are located under the "Chip Product Testing / Approved Products" tab on the Visa Digital Partner Services (VDPS) website at https://digitalpartnerservices.visaonline.com

1.2 Where can I find a list of Visa's approved security laboratories?

The "Visa Recognized Testing Laboratories" list is located on the Visa Digital Partner Services (VDPS) website at https://digitalpartnerservices.visaonline.com/ProductTesting/AccreditedTestLabs

1.3 Where can I find the most recent Security Testing Process and security requirements?

- The most recent Security Testing Process document (VCSP) for chip based products is located on the Visa Digital Partner Services (VDPS) website at https://digitalpartnerservices.visaonline.com/ProductTesting/Testing#security

- Chip card application specifications, security requirements and guidelines can be obtained under license from https://digitalpartnerservices.visaonline.com/Document

1.4 I have a product submission. Where can I find the Chip Card and Mobile questionnaires?

The most recent Chip Card Questionnaire and Mobile Questionnaire is located under the section "CHIP TESTING & APPROVAL SERVICES" on the Visa Digital Partner Services (VDPS) website at https://digitalpartnerservices.visaonline.com/Document

1.5 I have a new product for submission. Does the product require security testing?

- All new chip card and mobile products require full security testing.
- Wearables using a previously approved chip or SE may not require security testing.

1.6 I have a product that is a derivative of a previously approved product. Does the product require security testing?

Testing depends on the type of changes made to the base approved product. Visa Approval Services and the Visa Security team will review the questionnaire and make a determination based on the type of change being made.

1. Minor changes: If the changes are minor and do not impact product security, per VCSP policy, no security testing is required. A Letter of Approval (LoA) (*paper approval*) will be issued.
   EXAMPLES OF MINOR CHANGES:

   Changes that do not impact product security, e.g. changing the module, antenna, etc.

2. Changes requiring additional review: If the changes are not minor and require additional information or analysis, Visa Approval Service will request an Initial Assessment Letter *(IAL)* from the security laboratory to determine the scope of security testing.
   The Visa Security team will review the IAL and approve the security testing scope or suggest appropriate modifications.
   EXAMPLES OF CHANGE REQUIRING ADDITIONAL REVIEW:

   Change to the OS, change to the payment application, new 3rd party application loaded, enablement of features not evaluated in the based product, etc.

   Note:

   Derivative product with change/s on the loaded software or operational configuration such as clock configuration, security counter limits, etc. needs to be assessed for its security impact considering current state of the art attacks. It must achieved a HIGH JIL rating (31 or above) for all the attack paths.

1.7 How long does Visa Approval Services take to review an IAL?

Up to five (5) business days.
Review time increases if further information or clarification from the laboratory or vendor is needed. Clarifications may include:

- Security evaluation scope
- Important dates (e.g. ICCN, PCN expiration and site audit date)
- Reuse of security test results, etc.

1.8 How long does Visa Approval Services take to review a security report?

Up to ten (10) business days.
Review time increases if, e.g.:

- One or more security issue(s) are found by the laboratory
- Any additional clarification is required regarding Security test results, reuse of evidences, JIL scores, etc.

1.9 My product has gone through security testing. Due to functional issues, some minor changes are made to the product before

getting the approval. Does the product require additional security testing?

Any change to the product before getting the approval must be officially specified and declared by the vendor. Depending on the changes that Visa Approval Services and the security laboratory will review, delta security testing may be required.

1.10 I have a product that has one or more security issue(s). What are the required next steps?

All Visa primary and secondary assets are required to be protected against high potential attacks with JIL ranking of 31 or above. Based on the security evaluation report, if the product suffers from several security issues on primary or secondary assets, the product cannot be approved.
The vendor is required to fix the issues for the next cycle of security evaluation.

- In case of issues with secondary assets, Visa chip security team will analyze the risk of the attack path. The product might be approved with technical comments on LOA.
- Please note that with technical comments on LOA:
  - The product cannot have derivatives.
  - If the security issue involves Visa's primary assets, the product cannot be approved.

For more information regarding primary and secondary assets, please refer to the VMPA and VSDC security guidance documents.

1.11 I have a product that requires security testing. None of the Visa or EMVCo accredited security laboratories have available time slots. Can I submit the product to a security laboratory that is not Visa or EMVCo accredited?

No. The security evaluation must be completed by one of Visa or EMVCo accredited security laboratories. Vendors are responsible for scheduling a time slot with the laboratory for security testing.

Approval Services cannot facilitate this process or provide any guidance regarding scheduling.
Please refer to the VCSP requirements in Reference [1].

1.12 I have Product A that was evaluated by Security Lab A, and I would like to build derivative Product B from Product A, can I use another Security Lab to write the IAL?

Although it is not advisable, another lab may do the security assessment of a derivative product where it did not perform the parent product's security evaluation.

However, as the new lab did not perform the original evaluation and doesn't have access to the detailed security assessment and testing results of the parent product, it might be necessary for them to re-do code review and/or perform more security testing to be able to provide assurance and conclude on the security impact of the changes in the new derivative product. This will result in an increase in evaluation effort, thus cost and time needed for the evaluation.

It is recommended to contact ApprovalServices@visa.com first to discuss testing expectation as it could vary depending on the changes in the derivative product.

2 PCN and ICCN

2.1 Is a valid ICCN required before submitting a product to Approval Services?

- New chip card, mobile, wearable and other chip based products on other form factors require a valid ICCN at the time of product submission.
- New products on an IC pending EMVCo IC approval are not accepted.
- New products based on the IC with extended EMVCo certificate (product that has undergone the Expired Product Extension Process) are not accepted.
- Derivative product may be submitted with an expired ICCN.

2.2 Will an approval be invalid if an ICCN is not renewed?

No. A current ICCN is only required on the date the product is submitted to Visa for testing.

2.3 Is a valid PCN required before submitting a product to Approval Services?

- A valid PCN is required for Secure Element products (mobile and wearable form factor).

- A valid PCN is NOT mandatory for chip card products. The security laboratory conducts a comprehensive security evaluation that consists of code review and audit of the entire OS, etc. for chip card products that do not have a valid PCN. Using a platform with valid PCN allows re-using of assurances obtained during the platform evaluation, thus reducing testing effort and time.

2.4 I have a product with a pending PCN number. Can I submit the product for security testing while waiting for the PCN to be approved?

- Conducting the security evaluation while the PCN is pending is risky. If the PCN is not subsequently approved, the product may require additional security evaluation. Mobile products cannot be approved without the PCN.

- Although such product may be submitted to start testing activities in parallel, Approval Services is not responsible for any risks, costs or delays associated with a pending PCN.

3 Visa Chip Card and SE Life Cycle Management

3.1 Where can I find the most recent version of the complete Visa Chip Card and SE Life Cycle Management Policy?

The following documents address the Visa Chip Card and SE Lifecycle Management policy and are located under the section "CHIP TESTING & APPROVAL SERVICES" on the Visa Digital Partner Services (VDPS) website at https://digitalpartnerservices.visaonline.com/Document:

- For chip card products:
  - Visa Chip Card Life Cycle Management, Dec-15
  - Visa Card Lifecycle Management FAQ, Feb-16
- For mobile and wearable products:
  - Visa Secure Element Renewal and Lifecycle Management, Mar-15
  - ASA20191113 - Secure Element Lifecycle Management Policy Update, Nov-19

3.2 What happens if a bug or security flaw is identified after approval?

- If the issue is significant, Visa continues to reserve the right to remove products from the approved list ahead of the scheduled removal or expiry date.
- Removal from the approved list will trigger the requirement for immediate replacement/cancellation of cards in the field based on the product concerned, as well the destruction of stock of the product. In this extremely rare situation, Visa would work closely with impacted issuers and vendors.

3.3 What are the card vendor's responsibilities to ensure Issuers comply with the approved product's lifecycle? What are Issuers' responsibilities?

Card vendors:

- Are required to be totally transparent about the approval timeline and usage period of their products.
- Avoid inadvertently misleading issuers about their product lifecycle under Visa rules
- Must comply with the terms of their Visa specification and applet licenses.
- May not sell and/or ship products that are not on the Visa approved list.

Issuers:

- Must comply with new policy and ensure that cards expire and are replaced before the product is removed from the Visa approved products list.

3.4 How does Visa product lifecycle policy affect Chip Bulletin 16, i.e. how are specification and applet sunset dates impacted?

- Visa chip specifications and applets continue to be introduced and sunset independently of the card product approval process.
- Visa only accepts card products for testing/approval if they are based on a specification and/or applet version for which testing is still supported on the date of submission.

3.5 Does the Lifecycle policy have a grace period (comparable to Chip Bulletin 17's 'grace period') for products that are no longer allowed on the approved products list?

No. When a product is removed from the Visa approved product list it may no longer be sold, shipped or issued. Existing products in the field must be cancelled or replaced.

3.6 Can card vendors continue to sell products after the ICCN has expired?

Yes, if the product is on the Visa Approved Products list.

3.7 Are issuers required to support decreasing 'card-in-field' or expiry timelines as their card products get older?

Not necessarily. Issuers have this option, however, Visa recommends using a consistent 'card-in-field' duration of three (3) to five (5) years and planning for issuing a new product by the time the current one is reaching its end of life. For example, Issuers that use a 3 year 'card-in-field' duration must stop using the product 3 years before it is schedule to be removed from the approved list.

3.8 Are Common Payment Application (CPA) based products covered by the current policy?

No. For all questions regarding Common Payment Application (CPA) based products Contact VECPATypeApproval@visa.com.

4 Reused of Testing Evidences

4.1 Does Visa recognizes testing evidence obtained from the testing performed on other non-Visa products (e.g. from other 3rd party application) using the same IC and platform?

6. Reusing of testing result or evidence from other product on the same family (e.g same IC and platform) is accepted as long as it is justified. Evidence of its validity and applicability on the Visa product under test shall be thoroughly examined and rationalized. Validity of the reuse must be in accordance to Visa's policy for the reused of evaluation evidences as detailed in Reference [5]*EMVCo Security Guidelines, Security Evaluation Guidance (from www.emvco.com)*
7. *Visa Chip Security Program Security Testing Requirements and Guidance, Version 1.2, August 2024*

.

5 3rd Party Applications

5.1 Is security assessment of 3rd party application/s required?

- Security assessment of 3rd party applications is not required for mobile and wearable products (Secure Element).
  Nevertheless, Visa highly recommends that issuers perform due diligence security checks on the applications to be loaded on their products, following the security requirements outlined in the section 5.2 below.

- Security assessment of all 3rd party applications loaded in a chip card product is required irrespective whether platform has PCN or not.

5.2 What are the security requirements for 3rd party applications loaded into a Visa chip card product?

Visa security requirements for 3rd party applications are detailed in Reference [5]. At minimum, the following shall be considered:

- If the 3rd party application does share security assets with Visa payment application, security level of the shared assets shall be maintained and the interaction shall not impact the security of any primary and secondary Visa assets.
- Latest Oracle bytecode verification is passed for the 3rd party application.
- Profile side channel attack must not be feasible using the 3rd party application.

- Source code review is required to be conducted to ensure that no malicious code exists.
- The 3rd party application must be verified to be compliance with the platform security guidance.

5.3 Is it allowed for 3rd party applications to be evaluated without providing source code to the lab?

This can be acceptable as describe in Reference [5]. However, additional or alternative testing shall be conducted to provide an equivalent assurance. As an example, if the non-maliciousness of a 3rd party application cannot be guaranteed due to unavailability of source code, additional testing on the platform's firewall and resistance against ill-formed application shall be performed in order to provide assurance that even if this 3rd party application is malicious, it would not be able to compromise the Visa application assets. The approach is to assume that the 3rd party application is vulnerable and that the platform should be able to mitigate any possible weakness introduced by the application.

6 dCCV2 Security Test Requirements

6.1 What are the security requirements for dCVV2 based products?

- Visa Approval Services does not certify or approve dCVV2 functionality or security but requires due diligence testing if the feature is implemented on a secondary hardware component that reside on the card besides the secure element implementing the Visa Payment application.
- The dCVV2 secondary chip and component, in particular the recovery of dCVV2 key, is required to be protected against side channel and non-invasive perturbation attacks with JIL rating of at least 16 (Basic).
- The results of the security evaluation are valid for 24 months.

7 Biometric Sensor on Chip Card

7.1 Where can I find the security testing requirements for Visa's Biometric Sensor on Chip products?

Security requirements of Biometric Sensor on Chip Card products can be obtained from https://digitalpartnerservices.visaonline.com/Document and also described in Reference [5].

8 Chip Cards with Additional Components (Hybrid Cards)

8.1 What are the security requirements for chip cards with features involving additional computing and communication components (e.g. MCU, Bluetooth components, display, battery, etc.)

8. General security requirements of hybrid chip cards (e.g. chip card products with additional computing (MPU), communication and/or battery components or modules) are described in Reference [5]*EMVCo Security Guidelines, Security Evaluation Guidance (from www.emvco.com)*
9. *Visa Chip Security Program Security Testing Requirements and Guidance, Version 1.2, August 2024*

- .
- However, given the non-standard nature of such card products, vendors are required to contact ApprovalServices@visa.com for initial review of the product design and to confirm the necessary security testing scope and requirements.

9 System on Chip (SoC)

9.1 What are the security requirements of Visa for evaluating secure modules on a SoC used for payment?

At IC and platform level evaluation, including for SoC products, Visa recognizes and is fully leveraging the requirements and methodology defined by EMVCo. Refer to www.emvco.com for details.