Visa Chip Security Program – Security Testing Process

Visa Supplemental Requirements

Version 2.4

August 2024

Visa Public

Important Information on Confidentiality and Copyright

Note: This document is a supplement 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.

Contents

Tables

Figures

Introduction to the Visa Chip Security Program – Security Testing Process

This document describes the Visa chip security testing process to evaluate whether 'chip', 'platform' and 'chip card' products properly submitted for evaluation [AS1] provide adequate protection against industry-known threats and attacks. The Visa chip security program provides security testing for all Visa chip-based payment products globally, including those for Visa Europe (VE).

Note: This document is a supplement 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.

Audience for the Visa Chip Security Program – Security Testing Process

This document describes the Visa Chip Security Program (VCSP) and provides information for chip and platform suppliers, secure element and chip card vendors and manufacturers, issuers, test laboratories, test tool suppliers and Visa staff to support the security evaluation process.

Key Terms

Throughout this document the terms below are defined as follows:

Table 1: Key Terms

Term	Definition
Black-box testing	The term 'black-box testing' means that the test laboratory has limited knowledge of the test object. The test laboratory has no access to design information and source code and considers the test object as a black-box. The opposite of 'white-box testing'.
Chip (IC)	The term 'chip' or integrated circuit (IC) product is used to reference a very small electronic circuit on a single piece of material designed to perform processing and/or memory functions.
Chip card (ICC)	The term 'chip card' or integrated circuit card (ICC) product is used to reference a Visa chip-based payment product. For the purpose of this document a card comprises a chip, operating system, and one (or more) Visa application(s). In general these components are part of a payment card but they may also be in alternative forms such as tokens, stickers, mobile phones, etc.

Term	Definition
Platform product	The term 'Platform' product is the collective name for 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. VSDC, VMPA) can be executed.
Secure element	The term 'secure element' refers to an EMVCo Platform product with a payment application developed using the Visa mobile specifications (e.g., VMPA).
Visa reference number	A Visa reference number (or VTF#) is assigned by Approval Services and uniquely identifies a chip card for Visa testing.
Visa-recognized Security Laboratory	A Visa-recognized Security Laboratory (hereafter referred to in this document as Test Laboratory) is an approved EMVCo Security Evaluation Laboratory for ICC product testing that has signed the Visa test house relationship agreement.
White-box testing	The term 'white-box testing' means that the test laboratory has full knowledge of the test object, including source code and high & low level design information. The opposite of 'black-box testing'.

Acronyms

The following acronyms have been used in this document.

Table 2 Acronyms

Acronym	Definition
AS	Approval Services
CC	Common Criteria
CNN	Card Certificate Number
IAL	Initial Assessment Letter
IAR	Impact Analysis Report
IC	Integrated Circuit
ICC	Integrated Circuit Card
ICCN	Integrated Circuit Certificate Number
JHAS	JIL Hardware Attack Subgroup
JIL	Joint Interpretation Library

Acronym	Definition
PCN	Platform Certificate Number
SE	Secure Element
TOE	Target of Evaluation
VCSP	Visa Chip Security Program
VMPA	Visa Mobile Payment Application
VSDC	Visa Smart Debit Credit

Summary of Changes from version 2.3

This section provides an overview of the changes made since the last publication.

Table 3: Summary of Changes

Change	Description	Section
Formatting and Editorial	Formatting and minor editorial updates	Whole document
Removal of UICC and USIM reference	Remove UICC and USIM as example of Secure Element (to align with Approval Services testing availability for such form factor)	Acronyms Section 1
Clarification on Production site audit requirement	Production site audit requirement, including accepted evidence	Section 3.4 Site Audit
References updates	Added source of document references	Related Publications

Contact Information

Approval Services oversees testing of chip cards, secure elements, and other 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 card and secure element approval process. Approval Services provides a single point of contact, both for vendors

and for Test 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

Postal Address:	Visa Approval Services Mailstop M3-2NW 900 Metro Center Blvd Foster City, California 94404 U.S.A.

Vendor licensing information and registration requirements can be done via https://technologypartner.visa.com/Registration.

For detailed information on the EMVCo 'IC' and 'Platform' security evaluation process, please see EMVCo security evaluation process document [EMV1] available at www.emvco.com, or contact the EMVCo security evaluation secretariat at securityevaluation@emvco.com with any questions on the process.

1 Visa Chip Security Program Overview

Security testing focuses on aspects of the chip card and secure element product implementations that may have a security impact. Security testing goes beyond the functional testing to see if the product is vulnerable to well-known attacks, whether or not these are explicitly cited in the specification. Security testing is not exhaustive and focuses on the most likely vulnerabilities as revealed by previously testing, knowledge of the particular application(s), and past experience with similar products.

The testing seeks to evaluate that the security features provided by the chip product are appropriately implemented. The testing evaluates the protection that these features provide against various known and documented attacks. Testing further examines the interaction between the chip, operating system, platform environment, and application to evaluate (composite evaluation) whether sensitive and secret information is adequately protected by the chip product.

Note: Unless explicitly stated, the terms 'chip card' and 'secure element' are used interchangeable throughout this document and referred to as Target of Evaluation (TOE).

The Visa Chip Security Program (VCSP) seeks to minimize the cost and time spent in performing evaluation work and avoids duplication of effort. Visa has adopted the EMVCo Integrated Circuit (IC) and Platform security evaluation process [EMV1] for 'IC' and 'Platform' products respectively. The final composite security evaluation for its chip card and secure element testing leverages the GlobalPlatform Composite Evaluation Model [GP1]. The program supports any type of Secure Element (SE) regardless its form factor.

The Visa security evaluation methodology strives to achieve a balance between 'black-box' and 'white-box' testing. This balance is promoted by carrying out a security analysis that considers all viable attacks on a product [JIL1], and derives a set of penetration tests based on individual TOE characteristics. The objective of the evaluation is to evaluate the level of assurance that the TOE product may provide throughout its lifecycle as defined in [JIL2].

The level of testing is continuously increasing to reflect 'state-of-the-art' attack potential. Consequently, the introduction of new chip products should offer a higher level of protection against the latest threats. However, no testing can anticipate all potential future attacks. Security, by definition, is an ongoing process – as time progresses, attack and defense becomes a race.

1.1.1 Requirement: VCSP security testing

Visa Chip Security Program (VCSP) security testing is required for all Visa chip-based products.

1.2 Objective

The objective of the Visa chip security program is to evaluate whether the composite chip product (TOE) properly submitted for evaluation provide adequate protection against industry-known threats and attacks. The program provides security testing for all Visa chip-based payment products globally, including those for Visa Europe (VE).

The program is designed around industry best practices for open and transparent assessments. This allows Vendors to re-use existing test results and evaluation reports to avoid duplication of effort and cost. The program further reduces inter-payment system redundancies and inconsistencies in chip card security testing.

The Visa Chip Security Program:

- leverages industry-established best practices and the common criteria (CC) methodology for chip card evaluations, particularly the document 'Application of Attack Potential to Smartcards'. This work has been based on chip card evaluation experience and input from the chip card industry through the International Security Certification Initiative (ISCI) working group and working group JIL Hardware Attack Subgroup (JHAS).
- has adopted the EMVCo 'IC' and 'Platform' security evaluation process and is aligned with EMVCo ICC testing [EMV1].
- leverages the GlobalPlatform Composition Model [GP1] for the evaluation of composite products to support mobile applications and post issuance.
- is based on a set of Visa security guidelines that provide security guidance for the design of chip card and secure element products.

1.3 Legal notes

Compliance with the procedures set forth herein, successful completion of the Visa chip security program, or approval by Visa of cards or components subject to these requirements does not guarantee that such cards or components will be secure against all attacks, including attacks known at the time of approval. It is card and component manufacturers' responsibility to design and manufacture cards and components with security features sufficient to satisfy market, customer, or other applicable requirements in addition to the applicable requirements of the Visa chip security program. Completion of the Visa chip security program and/or approval by Visa shall not be deemed to be an endorsement or warranty by Visa that the card or component is secure against any attacks, including attacks known at the time of completion of the program and/or approval. Nor shall any card, chip or component manufacturer represent that such completion and/or approval constitutes an endorsement or warranty by Visa.

It is the sole responsibility of each card or component manufacturer to conduct the appropriate analysis of intellectual property issues related to each card or component submitted to the Visa chip security program and to ensure that each such card or component is within the scope of any necessary licenses, or is otherwise not in violation or infringement of any intellectual property rights or import-export requirements for the product.

It is the sole responsibility of each test laboratory to conduct the appropriate analysis of intellectual property issues related to each test, test plan, evaluation, or other technique used to evaluate any card or component submitted to the Visa chip security program to ensure that each such test, test plan, evaluation, or other technique is within the scope of any necessary licenses, or is otherwise not in violation or infringement of any intellectual property rights.

Visa reserves the right to conduct additional security testing on any products that have gone through the testing and approval process.

If residual vulnerabilities are discovered during the testing process but are addressed to the satisfaction of Visa and are considered a manageable risk, the product may receive an approval with comments from Approval Services.

Approval Services reserves the right to withdraw or to not issue a Visa approval/compliance when Visa finds that the product does not offer sufficient protection against the threats identified in the relevant Visa security guidelines or JIL documentation.

Whenever Visa considers withdrawal or non-issuance necessary (and where it is able to do so given confidentiality restrictions), Visa may inform vendors about newly discovered vulnerabilities of their approved products, thus enabling and supporting the vendor to minimize consequent risks, and to support Visa's client's/member's risk management. This may also include the withdrawal of a Visa approved product.

1.4 Organization of document

This document contains the following information:

Chapter 1 (Visa Chip Security Program Overview) offers a general outline of the document, describes its objective and intended audience, clarifies the used terminology and provides support and contact information.

Chapter 2 (IC and Platform Security Testing) describes the 'IC' and 'Platform' security testing process.

Chapter 3 (Composite Security Testing) describes the Visa security testing process for chip card and secure element products. This process consists of three phases: scoping, exploration and penetration, which are described in detail.

Chapter 4 (Further Information) provides additional information of the Visa chip security program for Test Laboratories and Vendors.

Appendix A (Related Publications) provides references that have been used in this document.

2 IC and Platform Security Testing

EMVCo evaluates the security features of IC, platform and common ICC products. The EMVCo security evaluation process [EMV1] considers the security of chip products and is aimed at providing a high level of assurance in the security functions that are designed to effectively deal with known attack methods [JIL1]. Visa leverages the EMVCo process to minimize cost and time spent in performing evaluation work and to avoid duplication of effort.

EMVCo approved 'IC' and 'Platform' products are listed on the EMVCo website at www.emvco.com.

2.1.1 Requirement: EMVCo product

Visa vendors that build upon EMVCo approved 'IC' or 'Platform' products must continue to monitor and adhere to the expiration date and latest security guidance that is assigned to each product.

2.2 Chip or IC products

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 successfully completed the EMVCo IC security evaluation process.

2.2.1 Requirement: New chip card (ICC) product

Visa will accept new chip card (ICC) products for security testing only if the chip has successfully completed the EMVCo IC security evaluation process and the chip is on the EMVCo approved chip list.

2.3 Platform products

A platform product is the collective name for 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 successfully completed the EMVCo security evaluation process.

2.3.1 Requirement: New secure element product

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

2.4 Additional Applications

The VCSP composite approval pertains only to the Visa payment application on the platform product.

2.4.1 Requirement: Additional applications

Any application loaded on a Visa approved product must not impact the security of the Visa payment application assets.

Note: Visa does not provide a security approval for additional applications

3 Composite Security Testing

This chapter describes the Visa composite security testing process for 'chip card' and 'secure element' products. It is closely aligned with the EMVCo ICC security evaluation process [EMV1] and leverages the GlobalPlatform Composition Model [GP1] for secure element products. The model is applicable to any type of chip product regardless its form factor.

3.1 Process overview

The composite security evaluation process is intended to evaluate the level of assurance for chip cards and secure elements at all stages of the development process. The testing process consists of following three phases:

Phase 1 (scoping): Initial Assessment

- Documentation review
- Site audit, when applicable
- Laboratory provides Approval Services with a test recommendation (Full, Delta, No test), and requests for security testing authorization, if required

Outcome: Initial Assessment Letter (IAL)

Phase 2 (exploration): Code review and vulnerability assessment

- Security guidance review
- Code review
- Vulnerability analysis
- Initial and/or verification testing, if required
- Estimate resistance against attacks [JIL1]

Outcome: penetration test plan or recommendation for product approval

Phase 3 (penetration): Penetration testing

- Penetration test
- JIL rating of chip product and description of potential residual vulnerabilities

Outcome: final test report

The following sections describe the three phases in more detail.

Note: Although the three phases are presented as one long sequence, each phase might have multiple internal iterations or 'loop backs' and might even loop back to the previous phase. In each phase there might also be 'iterations' between the Test Laboratory and vendor. Ultimately, the final outcome would be equivalent to that of the chip card that has successfully gone once through Phase 1, 2 and 3 of the Visa chip card security testing process.

3.1.1 Requirement: Assurance level

The evaluation process intends to provide assurance that the chip product protects the Visa assets against attackers with attack potential "High" as described in [JIL2] by evaluating the chip product at all stages of its development process. The "High" assurance level equates to the globally accepted Common Criteria evaluation assurance level EAL 4+.

Note: The '+' in EAL4+ indicates at a minimum Common Criteria assurance class AVA_VAN.5 specifying the highest level vulnerability analysis.

3.1.2 Requirement: Product change

Any change to a Visa approved product requires an impact assessment by a Test Laboratory. The assessment result must be submitted to Approval Services.

3.2 Scoping phase: Initial Assessment

The purpose of an Initial Assessment Letter (IAL) is for the Test Laboratory to provide Visa with its assessment of the type of security evaluation that needs to be performed for a given product. The outcome is a recommendation by the Test Laboratory of one of the following:

- Full security testing required – in case of a new product that has not been evaluated previously by the Test Laboratory under the VCSP program.
- Delta security testing required – in case of (i) product modification or patch; or (ii) product renewal.
- No security testing required – in case the product has been evaluated before and the changes have no negative security impact (e.g., Minor Change).

The completed IAL must be submitted to Visa Approval Services for review, approval and testing authorization.

Note: *Visa may decide that delta or full security testing is required for a product based on the information provided by the Test Laboratory, product history and other factors.*

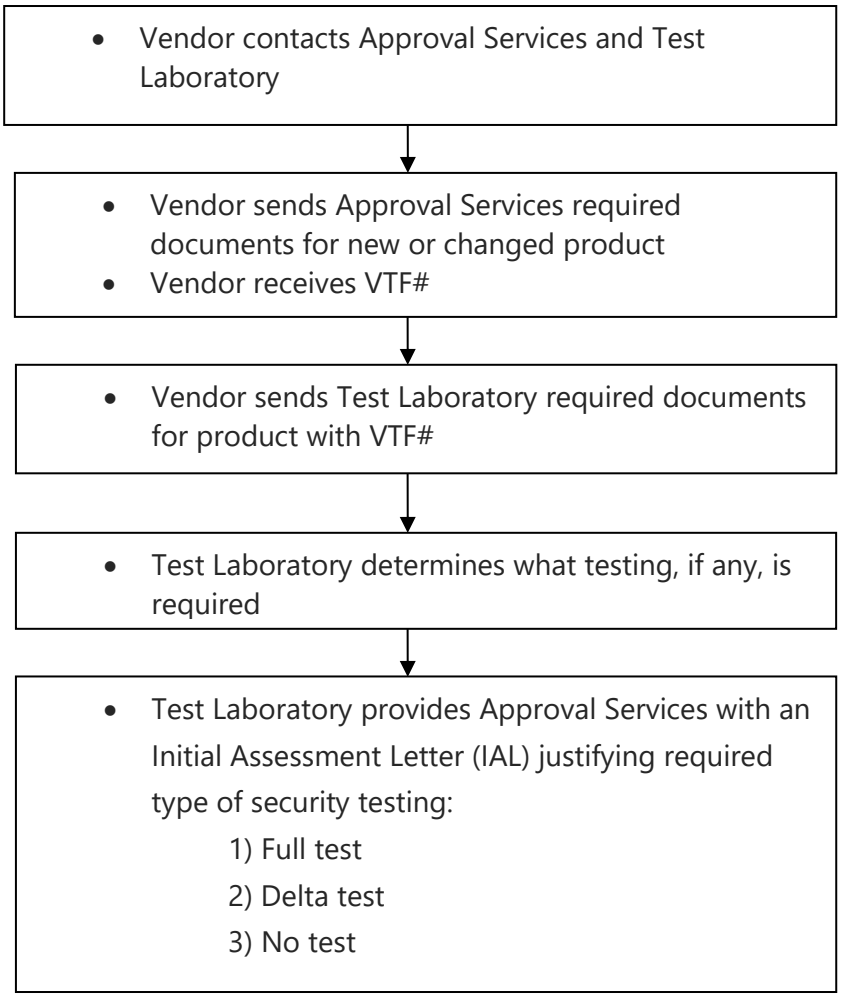
In case of memory size or IC specific config change that has been demonstrated in the chip evaluation as having no negative impact on the security of the chip no security testing may be required. Delta security testing may be appropriate when mask changes are made or patches have been applied.

Note: A vendor is allowed to submit more than one chip card for testing at a given time. In such a case, it may be possible for the Test Laboratory to schedule simultaneous testing of two or more products. The Test Laboratory will determine the appropriate type of testing if this scenario is requested by the vendor.

3.2.1 Requirement: Initial Assessment Letter (IAL)

In order to receive security testing authorization, the Test Laboratory must submit an Initial Assessment Letter (IAL) to Visa Approval Services for review and approval. The IAL requirements are described in [AS4].

Figure 3-1: Description of scoping phase



3.3 Exploration phase: Code review and vulnerability assessment

In the exploration phase, the Test Laboratory performs either a delta or full security evaluation on the TOE. In both cases it follows the same steps as illustrated in Figure 3-2. The Test Laboratory requests documentation from the vendor, such as high and low level design information, security guidance

documentation, source code, impact analysis report and test samples to perform the security evaluation.

Note: In case of a delta security evaluation, the Test Laboratory must clearly identify the differences between the current product (TOE) and the base product including security impact.

In the next step, the TOE, and where considered necessary, the related processes, are assessed to determine if the vendor has taken sufficient threats and attacks into account. The Test Laboratory must identify the assets, threats and perform a vulnerability analysis for the TOE and document the results. For this analysis, primary assets need to be identified such as cryptographic keys, and PIN data. There are also secondary assets (i.e., assets that that can be used to compromise a primary asset) such as security and risk management counters.

Next, the Test Laboratory performs a source code review that includes an analysis of the security functions. At this time, the Test Laboratory will evaluate whether the security guidance has been followed. It will also evaluate proper functioning and the effectiveness of the security functions, which might include code analysis and initial testing. The goal of initial testing is to observe the dynamic behavior of the TOE and to gain additional trust about the card's security. In this step simple measurements may be performed on the TOE for particular functions to identify obvious weaknesses and specific card behavior. This may provide information about relative strengths and weaknesses of the card for particular attack techniques.

Note: It is important that the final report clearly documents the Test Laboratory's understanding of the TOE's strengths and weaknesses.

The attacks, considered as the current state of the art and applicable to the payment applications implementation, can be split into three categories:

- software attacks: for example, using the application data unit (APDU) commands or malicious applications to break the payment application or platform security;
- side-channel attacks: for example, getting information through power consumption, electromagnetic emanations or execution timing;
- physical perturbation attacks: for example, changing the normal operation by injecting faults through laser, power glitches, and clock glitches.

The attacks aim at breaking the confidentiality and/or the integrity of sensitive:

- data (disclosure and/or modification);
- operations (forcing a non-expected result, disclosing the value of sensitive data during operation).

Once the assets/threat assessment and security function analysis has been completed, a penetration test plan is documented on most practical attacks for execution in the next testing phase by the Test Laboratory. For this, the Test Laboratory documents the estimated resistance against attacks as documented in [JIL1]. This TOE specific test plan may use all or some of the tests that are described in the latest JIL document [JIL1]. The goal of this step is to make a decision on which areas require further practical testing. Information about the TOE's vulnerabilities and information gained in the previous

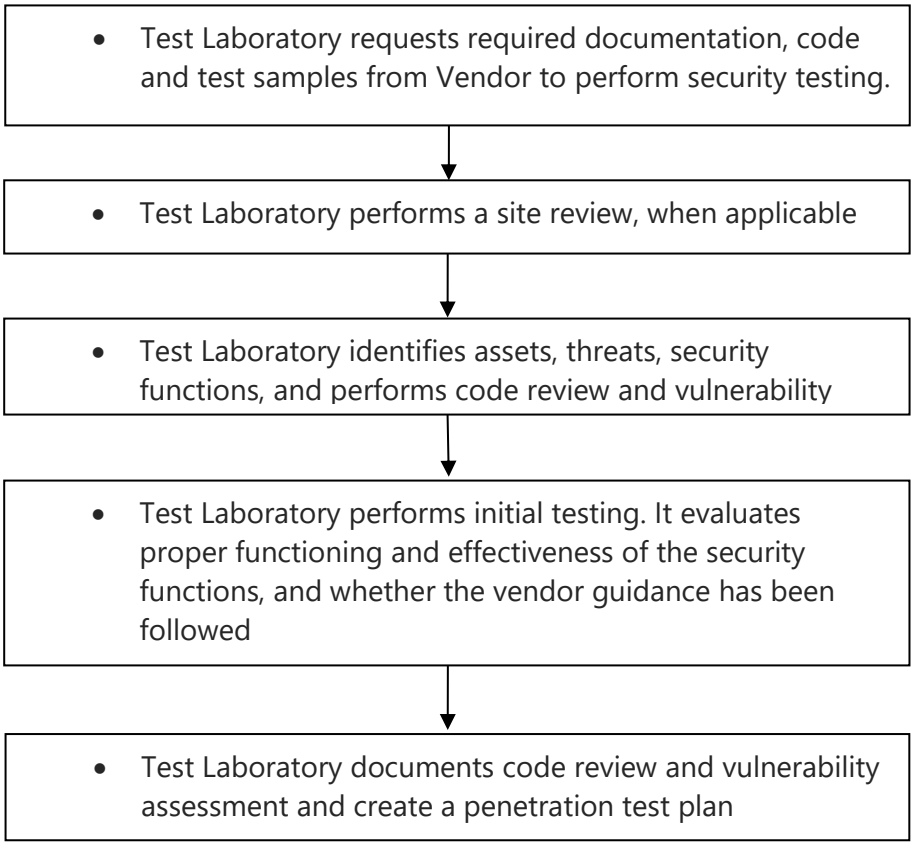
steps is combined in this step and is used to assess which suspicions remain and as a result need assurance from execution of further in depth practical tests. The Test Laboratory may combine two or more of these tests to produce a complete attack path.

When a Vendor patches its product during testing, the Test Laboratory must review and document the impact of the patch on the product and on testing that has been performed.

3.3.1 Requirement: Product change during testing

When a vendor modifies or patches its product during security testing, the Test Laboratory must notify Approval Services immediately.

Figure 3-2: Description of exploration phase.



Finally, the Test Laboratory documents the code review and vulnerability assessment results and creates a penetration test plan.

3.4 Site audit

The TOE testing activity includes an assessment of the vendor's infrastructure. Each stage of the TOE development and delivery process must be addressed. The EMVCo development and production site audit requirements document [EMV2] provide the Test Laboratory with guidance and requirements regarding how to perform a site audit on the Vendor's development site.

Production sites where the product with non-finalized security configuration or where binary code is processed or programmed (e.g. product where its security configuration is not yet at the evaluated state or with part of its binary code yet to be loaded) are also required to be in scope of the site audit requirements specified in [EMV2].

3.4.1 Requirement: Site audit

The Test Laboratory must verify that the vendor meets the development and production site(s) audit requirements as defined in [EMV2]. The Vendor must successfully pass the development and production site(s) audit.

Note: Acceptable documents that can be re-used by the Test Laboratory are Common Criteria, EMVCo, or VCSP site audit reports as long as they cover the scope. For production site(s), successful and up-to-date validation against the PCI Card Production Security Requirements [PCI1] of the vendor's production facility(s) may also be acceptable as evidence.

3.5 Penetration phase: Penetration testing

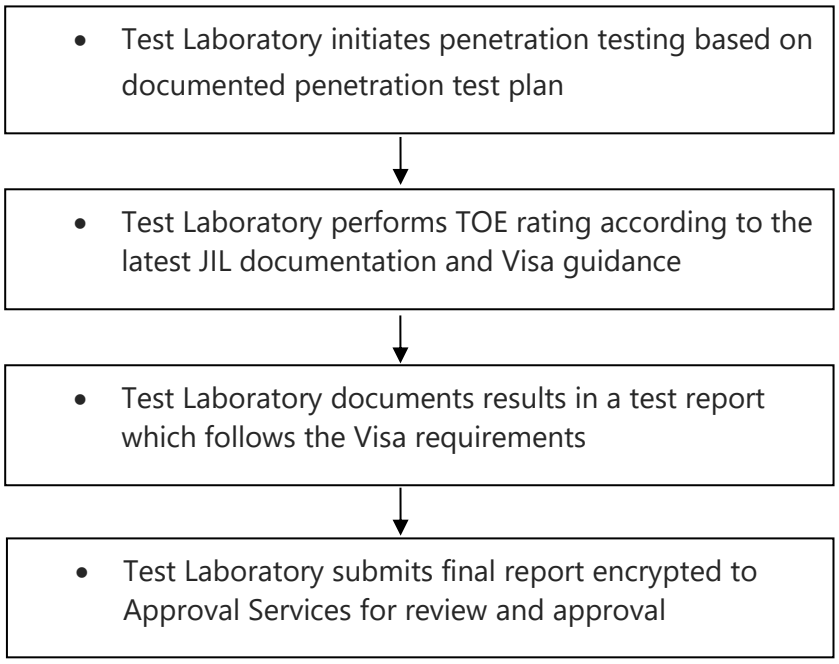
The Test Laboratory performs the penetration tests based on the documented test plan. After the test plan has been successfully completed, the Test Laboratory must rate the TOE according to the latest JIL documentation [JIL1] and Visa guidance.

Attack path identification and exploitation analysis and tests are mapped to relevant factors: elapsed time, expertise, knowledge of the TOE, access to the TOE, equipment needed to carry out an attack. The Test Laboratory must make a distinction between the cost of 'identification' (definition of the attack) and the cost of 'exploitation' (for example, once a script is published on the world wide web and can be downloaded by a script kiddy). Although this distinction is essential for the TOE evaluation to understand and document the attack path, the final sum of attack potential is calculated by adding the points of the two phases, as both phases build the complete attack.

The Test Laboratory documents the TOE penetration testing and rating results in the final test report that follows the Visa-specified format (see [AS4]). The Test Laboratory submits the final report to Approval Services for review and sign off.

Note: The final report should be encrypted using the Approval Services PGP key located under the CHIP TESTING & APPROVAL SERVICES section at https://digitalpartnerservices.visaonline.com/Document.

Figure 3-3: Description of the penetration phase.



3.6 Roles and responsibilities

The roles and responsibilities of the chip card security testing process are summarized in Table 3-1.

Table 3-1: Stakeholders and their responsibilities

Entity	Activity
Test Laboratory	• Check that forms are completed in full and submitted to the Test Laboratory prior to starting security testing • Estimate time to complete security testing • Provide Approval Services with a testing date and testing status updates • Perform security testing • Supply test results to vendor • Provide test results to Approval Services
Vendor	• Contacts Test Laboratory to schedule security testing. • Provide Test Laboratory with questionnaire, high and low-level design information, implementation information, source code, hardware guidance for software developers, hardware evaluation results, documentation, and test samples upon their request • Provide signed request for approval form to laboratory, authorizing laboratory to submit the security testing results to Approval Services.
Approval Services	• Single point of contact • Maintain testing infrastructure • Authorize security testing • Review the security testing results • If applicable, approve the chip card product as described in [AS1] • Maintain quality assurance • Alignment with industry

4 Further Information

This chapter provides additional information of the Visa chip security program for Test Laboratories and Vendors.

4.1 Test Laboratory

To become a Visa-recognized security laboratory for the Visa chip security program, the Test Laboratory must be an approved EMVCo security evaluation laboratory for ICC product testing and must have signed the Visa test house relationship agreement.

4.2 Vendor

Vendors who wish to have a chip product evaluated need to engage a Test Laboratory for testing. All arrangements for testing should be made by the vendor with the Test Laboratory [AS1].

Before testing can start, the vendor should complete all the required forms and documentation. These include forms which the Test Laboratory has prepared as its own normal business practice, and the Visa specified documents and forms [AS1].

Note: Normally the Test Laboratory (whether performing functional testing or security testing) will provide the vendor with all necessary forms to be completed, including those required by Visa.

The vendor should provide the Test Laboratory with the requested documentation. Examples of such documents are:

- Questionnaire
- High and low level design information
- Implementation information (for example, source code)
- Hardware evaluation security evaluation results
- Hardware guidance for software developers (for example, application guidelines)
- Impact analysis report

The vendor should consider the Visa security guidance [AS2, AS3], EMVCo guidance, and industry best practices [JIL1, JIL2] in the design of their products at a minimum.

A Related Publications

Throughout this document, the following references have been used. Card, secure element, mobile handset and component manufacturers and Test Laboratories shall be solely responsible for determining whether their particular use of any of the following references, or any of the recommendations or techniques described in the following references, requires a license or otherwise raises intellectual property concerns. Card, secure element, mobile handset and component manufacturers shall be solely responsible for evaluating the impact that adopting any of the provisions of the following references may have on the performance, stability, efficiency, or other aspects of manufacturer's product(s).

Table A–1: Related Publications

Reference	Document Title/Name (check respective source for latest version)	Description
AS1	Products, Testing and Approval Requirements	Provides an overview of the Visa products, testing and approval process and requirements Available at https://digitalpartnerservices.visaonline.com/
AS2	Visa Security Guidelines – VSDC Applications	Provides information that developers may choose to use in implementing (or improving) the security of the VSDC applications implementations. Available at https://digitalpartnerservices.visaonline.com/
AS3	Visa Security Guidelines – Multi-Application Platforms	Provides information that developers may choose to use in implementing (or improving) the security of smart cards that can provide a multi-application environment. Available at https://digitalpartnerservices.visaonline.com/
AS4	VCSP Security Testing Requirements and Guidance	Describes in detail the Visa security testing and reporting requirements. Available at https://digitalpartnerservices.visaonline.com/
EMV1	EMVCo Security Evaluation Process	Describes the requirements and procedures of the EMVCo Security Evaluation Process for IC, Platform and ICC products. Available at https://www.emvco.com/
EMV2	Development and Production Site Audit Guidelines	Provides Test Laboratories with guidance and requirements regarding how to perform a vendor site audit on the development site. Available at https://www.emvco.com/
GP1	GlobalPlatform Card Composition Model	Describes a model for composite security evaluations of GlobalPlatform products. Available at https://globalplatform.org/

JIL1	Attack Methods for Smartcards and Similar Devices	Refines the attack methods given in the JIL-paper about application of attack potential to smartcards [JIL-AP], providing guidance as to which attack methods have to be considered in a smart card evaluation and standardization of attack security rating. Distribution controlled by member schemes of the JIWG.
JIL2	Application of Attack Potential to Smartcards	This document interprets the current version of Common Criteria Methodology, where it provides guidance metrics to calculate attack potential required by an attacker to effect an attack. Available at https://www.sogis.eu/
PCI1	PCI Card Production and Provisioning Physical Security Requirements PCI Card Production and Provisioning Logical Security Requirements	PCI physical and logical security requirements for card manufacturing, chip embedded, etc. Available at https://www.pcisecuritystandards.org/