Visa payWave for Mobile

Testing and Compliance Guidelines for Mobile Device Manufacturers and Mobile Network Operators

Version 1.1
Effective: October 2012
Classification: Public

Contents

Figures

Tables

1 About This Guide

This document includes an overview of the Visa testing process and requirements for mobile devices enabled for Visa payWave for mobile payments.

The information in this document does not replace or supersede the testing requirements, compliance requirements, or processes outlined in Visa documents referenced in Chapter 2.

1.1 Audience

This document is intended for use by mobile device manufacturers (OEMs) and mobile network operators (MNOs) that are involved in the testing, production, and distribution of mobile devices enabled for Visa payWave for mobile payments.

1.2 Document Organization

This section describes the organization of this guide.

Chapter 1**, About This Guide**—This chapter provides an overview of this guide.

Chapter 2**, Related Documentation**—This chapter identifies documentation that specifies testing and compliance requirements, physical and logical security requirements, and Visa brand standards that apply to mobile hardware components that are enabled for Visa payWave for mobile payments.

Chapter 3**, Visa Compliance Requirements and Commercialization Process**—This chapter provides an overview of Visa compliance requirements and the commercialization process for mobile contactless products enabled for Visa payWave for mobile payments.

Chapter 4, Summary of Visa Security and Functional Testing—This chapter provides a summary of the major testing processes that Visa conducts (or accepts) for the purpose of approving a mobile product that will be used for Visa payWave for mobile payments.

Appendix A**, Visa payWave for Mobile Testing Requirements Checklists**—This appendix provides high-level checklists of Visa payWave for mobile testing requirements.

2 Related Documentation

This chapter identifies documentation that specifies testing and compliance requirements, physical and logical security requirements, and Visa brand standards that apply to mobile hardware components that are enabled for Visa payWave for mobile payments.

Visa Mobile Proximity Payment Testing & Compliance Requirements for Handsets and Secure Elements

This document describes the Visa submission process and testing requirements for the following mobile contactless payment devices:

- Handset (with an embedded or removable Secure Element)
- Universal integrated circuit card (UICC)
- Universal subscriber identification module (U/SIM)
- Embedded Secure Element
- Product that combines any of those components

This document is located at:

https://technologypartner.visa.com/Testing/TestMaterials.aspx

The document provides:

- A detailed overview of Visa's security and functional testing requirements
- Requirements for submitting products, including appropriate licenses, specifications, and agreements
- Quantity and configuration of products required for official testing
- A list of Visa-recognized testing laboratories; the vendor can engage these laboratories in quality assurance (QA) and debug testing in its development process

Visa Mobile Proximity Payment Testing & Compliance Requirements for MicroSDs and Mobile Accessories

This document describes the Visa submission process and the testing requirements for mobile contactless payment devices. The document focuses on micro secure digital (microSD) components and other mobile accessories.

This document is located at:

https://technologypartner.visa.com/Testing/TestMaterials.aspx

The document provides:

- A detailed overview of Visa's security and functional testing requirements
- Requirements for submitting products, including appropriate licenses, specifications, and agreements
- Quantity and configuration of products required for official testing
- A list of Visa recognized testing laboratories; the vendor can engage these laboratories in QA and debug testing in its development process

Mobile Requirements — Visa Mobile Contactless Payment Specification

This document covers:

- Read range functional requirements for all mobile contactless payment products
- Specific requirements for microSD and mobile accessory products

NOTE: Visa will issue a Letter of Compliance if a product satisfies all requirements, including the two centimeter read range as measured from the mobile device to the reader (the requirement is four centimeters for card products). Visa will continue to leverage the EMVCo test plans, but will issue a Letter of Compliance if the two centimeter read range requirement is met.

Visa Product Brand Standards for Mobile Applications

This document is currently under development. Upon publication, the document will contain:

- Baseline specifications on how to use the Visa brand standards in a mobile application, whether it is Visa-branded or integrated in a mobile application belonging to the issuer or another third party
- Guidelines for Visa brand standards on physical hardware and/or product packaging

Visa Mobile Product Questionnaire

The mobile product questionnaire is required for all submissions.

This document is located at:

https://technologypartner.visa.com/Testing/TestMaterials.aspx

Physical, Logical, and OTA Security Requirements for Secure Element (SE) and Mobile Contactless Payment Service Providers

This is a set of related documents that are currently under development. Upon publication, these documents will contain logical, physical, and over-the-air (OTA) security requirements. This information will be used by vendors engaged in providing services to personalize and provision Visa payWave for mobile payment accounts, manage Secure Elements enabled for Visa payWave for mobile payments, or manage the lifecycle of the Visa payWave for mobile payment application OTA.

OEMs and MNOs should review these documents to determine which requirements may apply to them based on the type of services being offered to Visa issuers.

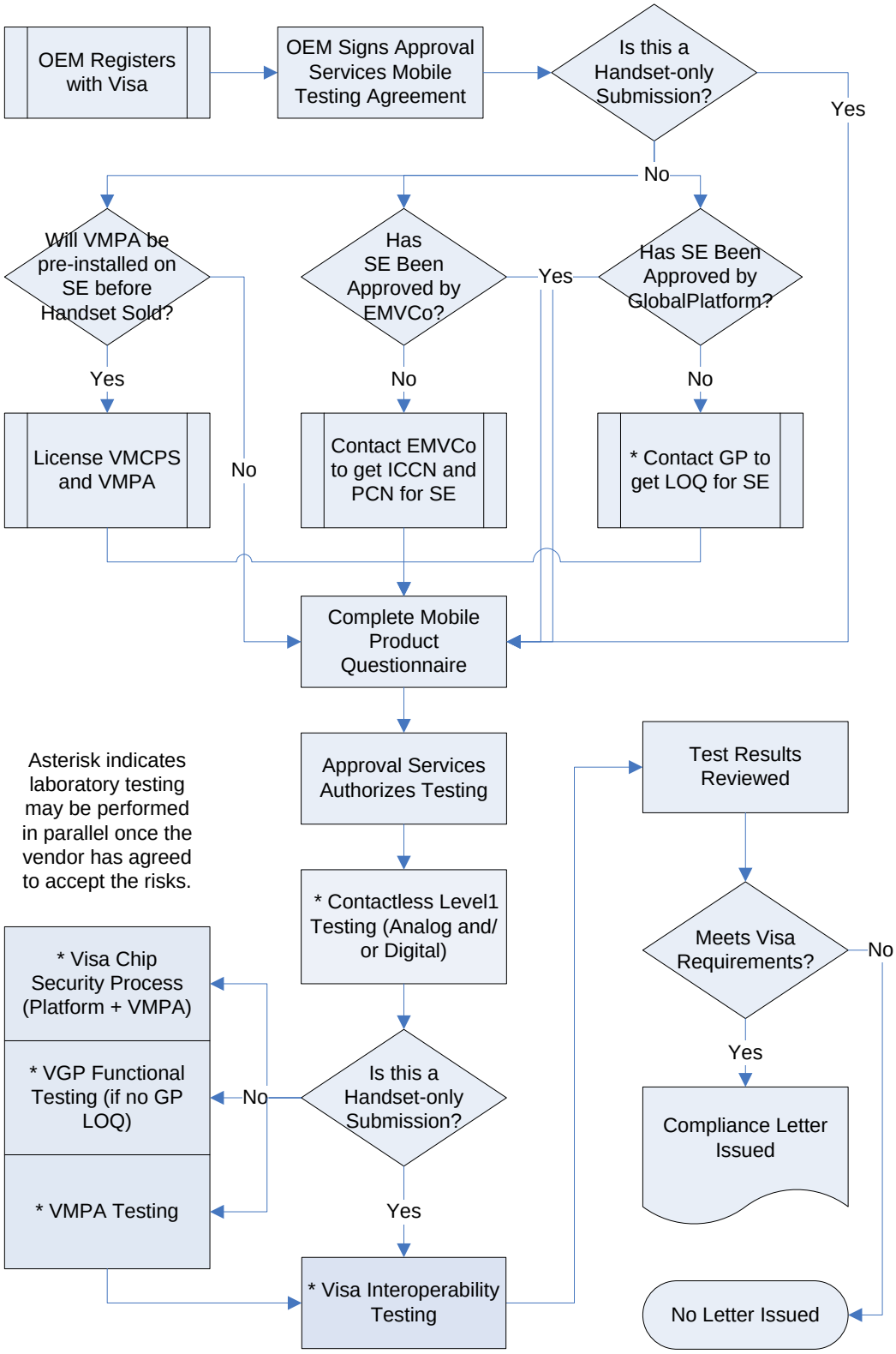
3 Visa Compliance Requirements and Commercialization Process

The Visa payWave for mobile compliance process is governed by the documents listed in Chapter 2.

The path to commercialization of a mobile contactless product enabled for Visa payWave for mobile payments is illustrated in Figure 3-1. As shown, the process varies depending on whether the product submitted is:

- A product that includes a Secure Element with a Visa mobile payment application
- A handset only (a handset that does not contain a built-in Secure Element and is not submitted with a removable Secure Element as a combination product)
- A combination of a handset and a Secure Element with a Visa mobile payment applications

Figure 3-1: Path to Commercialization



3.1 Eligibility and Licensing

Visa Mobile Licenses

This section describes the licenses that may be required for vendors submitting a mobile device with a Secure Element that will host the Visa Mobile Payment Application (VMPA).

Each vendor's license requirements may differ depending on the product that is being submitted. Vendors must verify that all required Visa licenses have been executed before official testing can begin by contacting technologypartner@visa.com or going to their web site https://technologypartner.visa.com.

Visa's licenses for mobile payment include:

- **Mobile Payment Specification License**— License for the Visa Mobile Contactless Payment Specification (VMCPS), required for those vendors submitting Secure Element components for Visa certification.
- **Mobile Payment Software License**— License for the use and distribution of the Visa Mobile Payment Application ("VMPA"). This license is required for vendors submitting Secure Element components for Visa certification or vendors directly involved in the distribution, loading, provisioning, and lifecycle management of the VMPA; typically these are Trusted Service Managers or OTA personalization vendors.

A vendor that submits a handset-only device for testing is not required to license Visa's mobile payment specifications or software. A handset-only device is a handset that does not contain a built-in Secure Element and is not submitted with a removable Secure Element as a combination product. The handset-only vendor is required to sign an Approval Services Mobile Testing Agreement (ASTA) before testing can start.

Visa Mobile Agreements

All vendors that submit mobile products to Visa for compliance testing and certification are required to execute an Approval Services Mobile Testing Agreement (ASTA). This agreement can be downloaded from the Visa secure web site at https://technologypartner.visa.com.

There are two versions of the ASTA:

- One that covers mobile handsets, regardless of whether the Secure Element is embedded or removable
- One that covers handsets with Secure Elements, Secure Element components, and mobile accessories

3.2 Visa Approval Services

The Visa Approval Services group oversees testing of mobile products that will be used to conduct Visa mobile payWave payment transactions to ensure that mobile products are developed to Visa specifications and requirements. Visa's requirements may incorporate applicable specifications and certifications defined by such organizations as EMVCo or GlobalPlatform.

The vendor must execute all applicable licenses and agreements before the compliance testing process can begin. Approved vendors are referred to Visa Approval Services and the vendor is then required to execute the applicable Approval Services Mobile Testing Agreement (ASTA) that governs the testing and compliance process between the vendor, the labs, and Visa.

Depending on the product being submitted Visa Approval Services requires testing on some or all the following components:

- Secure Element
  - Platform (Operating System, Java Card, and GlobalPlatform) + Payment Application + Secure Element (SE)
- Near Field Communication (Card Emulation)
  - Visa Contactless Interface—Analog and Digital
  - Visa Interoperability Testing

After Approval Services verifies that the vendor's submission meets all testing requirements, a Letter of Compliance is issued to the vendor for the compliant product. The compliant product will be added to either the public or the internal Visa Compliant Mobile Products List, as requested by the vendor or Visa regional business owners.

Approval Services can be contacted at approvalservices@visa.com.

3.3 Visa Brand Standards Review

Prior to approving a Visa payWave for mobile payment program for commercialization:

- The Visa Product Brand team must review and approve the use of the Visa brand elements in the mobile application, whether it is Visa-branded or integrated in a mobile application belonging to the issuer or another third party.
- The Visa Global Brand Design & Standards team must review and approve any product packaging that mentions the Visa brand.

As a general rule, Visa prohibits the use of the Visa brand mark on any mobile physical hardware. Please refer to the "Visa Product Brand Standards" for all applicable uses of the Visa brand mark.

The Visa Product Brand team can be contacted through their web site at https://www.productbrandstandards.com.

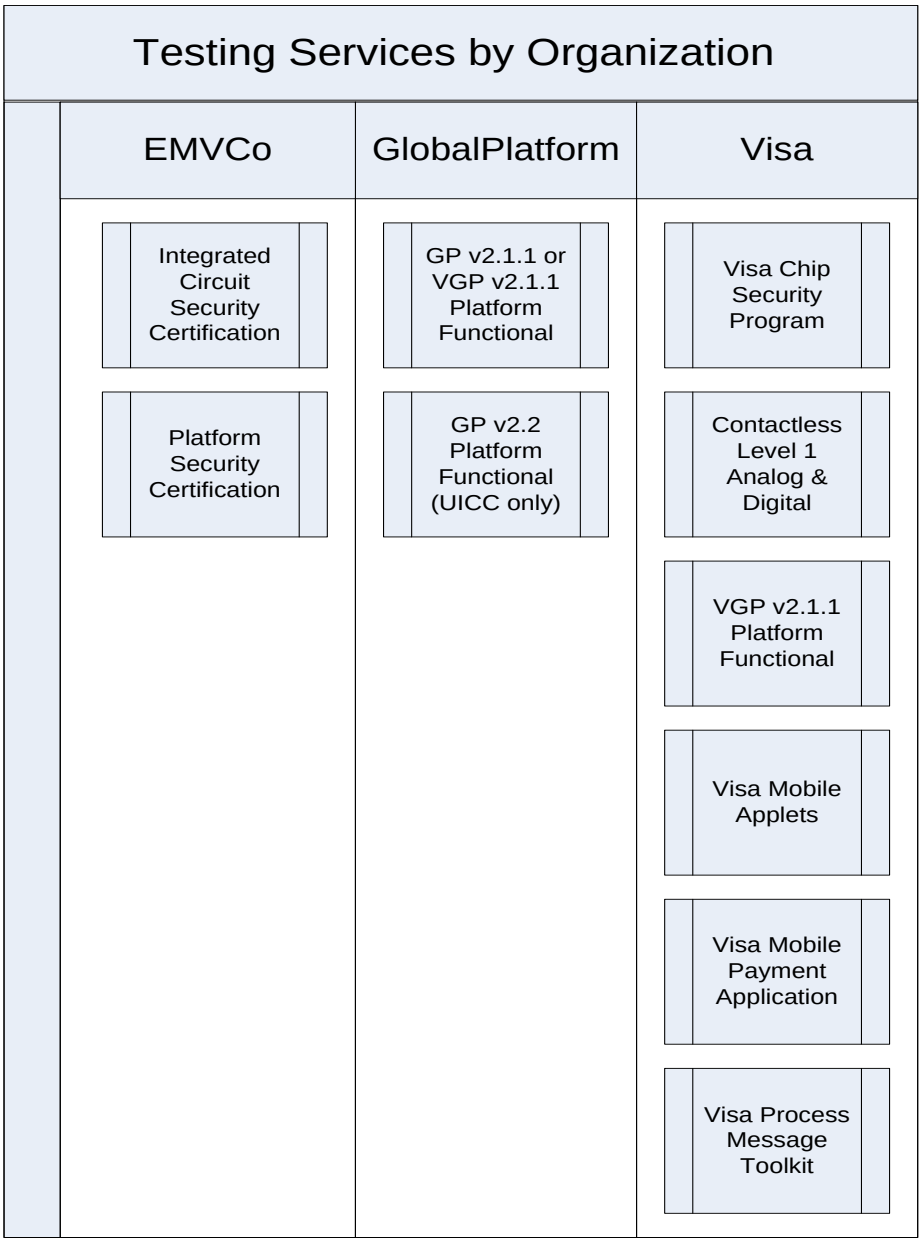
4 Summary of Visa Security and Functional Testing

This chapter provides a summary of the major testing processes that Visa conducts (or recognizes) for the purpose of evaluating a mobile product that will be used for Visa payWave for mobile payments.

The information in this chapter does not replace or supersede the testing and compliance requirements and processes outlined in the applicable Visa documents referenced in Chapter 2. Additionally, this document is not meant to limit the testing requirements as summarized below.

Based on each vendor's documentation of the product being submitted for compliance review, Visa Approval Services will have full discretion to determine any and all tests required to verify that the product meets all Visa requirements for commercialization.

Figure 4-1: Testing Services by Organization



4.1 Secure Element Testing

The following approvals must be obtained before submitting a Secure Element to Visa for testing:

- EMVCo IC Chip Hardware Review—Visa will accept a Secure Element for testing only if the chip has been approved by EMVCo and is currently listed on EMVCo's Approved Chips List (http://www.emvco.com/approvals.aspx?id=31).
- EMVCo Platform Security Review—Visa will accept a Secure Element for testing only if the platform has been approved by EMVCo and is currently listed on EMVCo's Approved Platforms List (http://www.emvco.com/approvals.aspx?id=31).
- GlobalPlatform Platform Functional Testing—Visa will accept a Secure Element only if the platform has been approved by GlobalPlatform and is currently listed on GlobalPlatform's Qualified Products List (http://www.globalplatform.org/complianceproducts.asp).

The following assessments will be performed on a Secure Element that is submitted for testing:

- Visa Chip Security Program (VCSP)—The final product (consisting of an EMVCo-approved chip, an EMVCo-approved platform, and the Visa Mobile Payment Application) must complete a composite security assessment:
  - Security testing is performed to help ensure that the chip and application are resistant to common attacks such as probing or differential power analysis.
  - Security testing involves *white box* testing with the combination of a Secure Element and software on the Secure Element.

NOTE: *OEMs are encouraged to submit products containing Secure Elements that have already passed VCSP requirements in connection with submission by the Secure Element chip component supplier. To avoid duplication of testing, Visa applies the previous testing of the Secure Element to the identical Secure Element in the OEM's corresponding product.*

- Visa Functional Testing—This assessment will ensure the ability of the platform and the product to perform a Visa payWave transaction. This may include Visa GlobalPlatform, Visa Mobile Payment Application, contactless digital testing, and interoperability testing.

4.2 Near Field Communication (Card Emulation)

The following testing will be performed on a mobile product that is submitted for testing:

- Visa Contactless Interface—Analog and Digital
  - Analog testing is related to radio frequency (RF) field power and modulation characteristics.
  - Digital testing focuses on the contactless protocol rules, including data frame structure and timing during the command-response exchange.
- Visa Interoperability Testing
  - Interoperability testing of the mobile product against Visa-approved contactless readers to ensure the correct functioning of the application with the terminal and host during a Visa payment transaction

A Visa payWave for Mobile Testing Requirements Checklists

This appendix includes high-level checklists of Visa's requirements for mobile product submission.

- The checklist in Table A-1 applies when the product includes a Secure Element with a Visa payment application.
- The checklist in Table A-2 applies when the product is a handset only (a handset that does not contain a built-in Secure Element and is not submitted with a removable Secure Element as a combination product).

Table A-1: Checklist for Submission of Product with Secure Element and Visa Payment Application

Task #	Task	Description	Form Required	Completed √
1	Complete the online registration form using the following link: https://technologypartner.visa.com	Required for all submissions.	√	
2	Obtain and execute applicable License Agreements. ***NOTE:*** *Obtain the agreement from the Visa Technology Partner web site.* *Sign the agreement and email it to* TechnologyPartner@visa.com.	Required if loading, installing or personalizing the VMPA applet.	√	
3	Obtain and sign the Approval Services Mobile Testing Agreement (ASTA). ***NOTE:*** *Obtain the agreement from the Visa Technology Partner web site.*	Required for all submissions.	√	
4	Obtain and complete the Product Questionnaire. ***NOTE:*** *Obtain the questionnaire from the Visa Technology Partner web site.* *Complete the questionnaire and email it to* ApprovalServices@visa.com.	Required for all submissions.	√	

Table A-2: Checklist for Submission of Handset-Only Product

Task #	Task	Description	Form Required	Completed √
1	Complete the online registration form using the following link: https://technologypartner.visa.com	Required for all submissions.	√	
2	Obtain and sign the Approval Services Mobile Testing Agreement (ASTA). ***NOTE:*** *Obtain the agreement from the Visa Technology Partner web site.*	Required for all submissions.	√	
3	Obtain and complete the Product Questionnaire. ***NOTE:*** *Obtain the agreement from the Visa Technology Partner web site.* *Complete the questionnaire and email it to ApprovalServices@visa.com.*	Required for all submissions.	√	