Visa Mobile Proximity Payment Testing & Compliance Requirements

Visa Approval Services

Version 6.0

June 2024

Visa Public

DISCLAIMER

Visa's testing services and policies are subject to change at any time in Visa's sole discretion, with or without notice. This document does not create any binding obligations on Visa regarding Visa testing services or product approval. Any such obligations, to the extent they exist at all, are pursuant to separate written agreements between Visa and the party submitting products for testing and approval. In the absence of a fully-executed written agreement under which Visa has agreed to perform testing services for you or your company you should not rely on this document, nor shall Visa be liable for any such reliance (detrimental or otherwise).

This document is provided on an "as is", 'where is", basis, "with all faults" known and unknown. To the maximum extent permitted by applicable law, Visa explicitly disclaims all warranties, express or implied, regarding this document, including any implied warranty of merchantability, fitness for a particular purpose and non-infringement.

In no event shall Visa, its principals, members, officers, employees, affiliates, contractors, subsidiaries, or parent organization, be liable to you for any special, consequential, incidental, or punitive damages, including, without limitation, any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, whether or not Visa has been advised of the possibility of such damages.

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.

Important Information on Copyright

The trademarks, logos, trade names and service marks, whether registered or unregistered (collectively the "Trademarks") are Trademarks owned by Visa. All other trademarks not attributed to Visa are the property of their respective owners.

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV® trademark is owned by EMVCo LLC.

Contents

Tables

Figures

Introduction

This document provides detailed information related to the Visa testing submission process and the testing requirements for mobile proximity payment products. The intent of the document is to identify the forms and documents needed to correctly submit products for testing. The document also identifies testing requirements and process that are applied to specific mobile proximity payment products that a vendor may submit.

Audience

This document is intended for vendors submitting the following mobile proximity payment product configurations to Visa for testing:

- Embedded Secure Element (eSE)
- Wearable Product

Key Terms

Term	Definition
CCPS Antenna	The antenna in the mobile product which facilitates the (EMV®) contactless proximity communication for Visa payment transaction.
Delta testing	A delta test is the difference between the testing performed for the original product versus a newer test plan
Embedded Secure Element (eSE)	The secure element embedded in the mobile product where the VMPA applet resides
EMVCo	EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions. It accomplishes this by managing and evolving the EMV® Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Today there are EMV® Specifications based on contact chip, contactless chip, common payment application (CPA), card personalization, and tokenization. This work is overseen by EMVCo's six member organizations—American Express, Discover, JCB, MasterCard, UnionPay, and Visa.
Handset	Another term for a mobile device, usually a mobile phone handset

Term	Definition
microSD	An extended and removable memory card which may integrate a Secure Element. A memory card integrating a Secure Element may be plugged into a mobile handset.
Mobile Application	The interface that manages the interactions between the handset user and the VMPA applet. Also referred to as Visa Mobile Application or wallet.
Mobile Device	A portable electronic device with contactless and wide area communication capabilities. Mobile devices include mobile phones and other consumer electronic devices
Near Field Communications	A short range contactless proximity technology based on ISO/IEC 18092, which provides for ISO/IEC 14443 compatible communications
Performance Testing	A set of tests to assess the performance of the mobile product to perform a transaction
Regression testing	A subset of testing
Secure Element	A tamper resistant module, capable of hosting applications in a secure manner
User Interface	Input and output components on a mobile device, for example, display, keyboard and touch screen.
VMPA	Visa Mobile Payment Application—Visa Mobile Contactless Payment application hosted in the Secure Element
VMPA Applet	A software application developed to [VMCPS] and [MA] that resides on a Secure Element in a mobile device.
Mobile Wearable Product	An NFC-based wearable form factor that can be worn on the body.

Abbreviations and Terminology

Abbreviation	Terminology
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
AS	Approval Services
ASTA	Approval Services Testing Agreement
ATS	Answer to Select
CLF	Contactless Front-end

Abbreviation	Terminology
CPS	Card Personalization Specification
CCPS	EMVCo Contactless Communication Protocol Specification
DES	Data Encryption Standard
ETSI	European Telecommunication Standards Institute
GP	GlobalPlatform
HCE	Host-based Card Emulation
HCI	Host Controller Interface, defined by ETSI TS 102 622
IAL	Impact Assessment Letter
IC	Integrated Circuit
ICCN	Integrated Circuit Certificate Number
ICS	Implementation Conformance Statement
ISD	Issuer Security Domain
LoQ	Letter of Qualification
NFC	Near Field Communications
OS	Operating System
OTA	Over the Air
PCN	Platform Certificate Number
POS	Point of Sale
QA	Quality Assurance
RF	Radio Frequency
SCO	Supported Configuration Options
SE	Secure Element
TTIA	Test Tool Interface Application
UAT	User Acceptance Testing
UI	User Interface
(U)SIM	Universal Subscriber Identification Module
VDPS	Visa Digital Partner Services
VMPA	Visa Mobile Payment Application
VMCPS	Visa Mobile Contactless Payment Specification

Contact Information

Visa Approval Services is responsible for managing the accreditation and various other processes described in this guide. They are the single point of contact within Visa for vendors seeking testing and laboratories seeking accreditation. The vendor or the testing laboratory may contact Visa Approval Services at any time.

Email:	ApprovalServices@visa.com
Websites:	**Visa Digital Partner Services (VDPS)** **(https://digitalpartnerservices.visaonline.com)**
US Postal Address: • Product samples for interoperability and performance testing	**Visa International Approval Services** **900 Metro Center Boulevard** **Mail Stop M3-2NW** **Foster City, CA 94404** **United States** **Mailroom Contact : +1 650 432-8822**

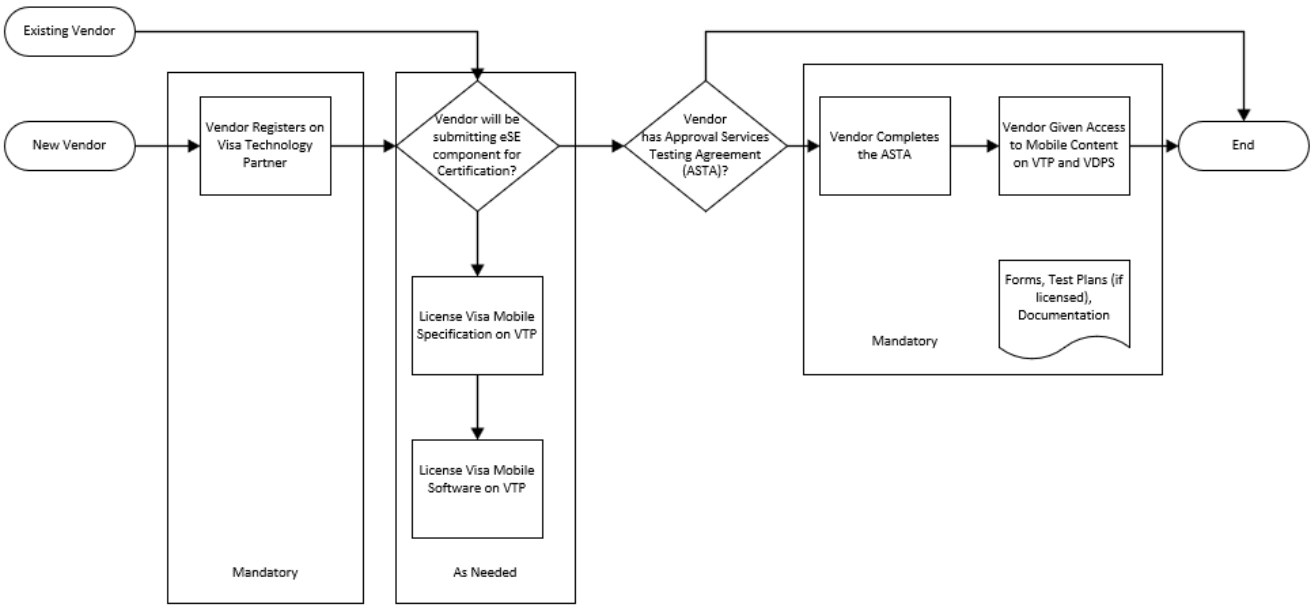
Scope and Assumptions

The design of a mobile product with a payment application may vary significantly between vendors and products, so it is necessary to make certain assumptions regarding common functionality in order to perform testing on a mobile product while minimizing the effort and cost of testing. These assumptions include but are not limited to the following:

- The mobile product complies with all required EMVCo and Visa contactless specifications and Visa testing requirements.
- An approved mobile payment applet developed to Visa Mobile Contactless Payment Specification (hence forth referred to as "VMPA applet") will reside on a GlobalPlatform compliant secure element physically separated from the low level contactless analogue interface component. Based on the product configuration digital functionality may or may not be separated from the secure element.
- The secure element complies with GlobalPlatform (GP) specifications and may be directly connected to the proximity communication antenna (in this case, no separate contactless digital interface component).
- Products that are not developed to the GP specifications are outside the scope of this document.
- Testing for compliance does not include testing of the user interface application (commonly referred to as a wallet).
- The antenna and low level analogue interface components may be powered by the host product's battery.
- A wearable product shall be in an operational state. It shall be able to perform a payment transaction without any remote activation of controls.
- For testing purposes, it shall be possible to remotely activate the contact and the contactless interface via defined commands sent to a client application. Refer to VMPA Test Tool Interface Requirements (Book 6) and Guidance for Visa Mobile and Wearable Products TTIA.
- This document does not address additional Visa regional business requirements that may be required prior to deployment.

1 Vendor Registration, Licensing and Testing Agreement

Figure 1-1: Vendor Registration, Licensing and Testing Agreement Process



All mobile payment product manufacturers must register on the Visa Technology Partner (VTP) website and have executed the appropriate testing agreement before they are eligible to submit a product for testing.

Vendors who are submitting a wearable product must contact the Visa Ready Program. Please contact Visa Ready at VisaReadyDigitalPlat@visa.com or go to Visa Ready Digital Payment Portal.

A vendor that submits a product for Visa compliance testing is not required to license Visa mobile specifications or mobile software from Visa if:

- The product does not include a secure element, or
- The product includes a secure element, but the vendor does not and will not have the keys to access the security domain where the Visa-developed Visa Mobile Payment Application (VMPA) resides.

Secure element suppliers and vendors who will be submitting products with a secure element and have the keys to the security domain where the Visa-developed VMPA applet resides must license the applicable Visa mobile specifications and software. Licensing is handled by the VTP.

A Visa-recognized laboratory (hereafter referred to in this document as "laboratory") may only accept mobile payment products for official compliance testing from vendors authorized by Visa. Vendors wishing to perform debug "QA" testing at a laboratory do not need prior authorization from Visa.

The definitions for seeking to become a Visa mobile payment product vendor are described below:

Table 1–1: Definitions of Visa Mobile Payment Product Vendor

Vendor	Definition
Chip/OS Component Supplier	The entity that supplies Chip/OS packages must have executed the necessary agreements with Visa to allow it to submit chip/OS component packages (in an ID1 card format) directly to Visa for testing
Secure Element Supplier	The entity that provides the final Secure Element product and takes responsibility for the entire package: operating system, application, embedding of module and, when applies, the inlay/antenna
Mobile Product Supplier	The entity that manufactures a mobile product capable of hosting the Secure Element and performing a Visa mobile contactless transaction
Mobile Wearable Supplier	The entity that manufactures the mobile wearable final form factor, capable of hosting an embedded inlay and performing a Visa mobile contactless transaction.

1.1 Specifications and Requirements

Vendors are responsible for licensing and developing their products to comply with the appropriate specifications and requirements. The major relevant documents are listed in the table below. This list is not exhaustive of all specifications and requirements that may be used in the development of a Visa-compliant mobile payment product. The vendor developing a mobile payment product is ultimately responsible for obtaining all specifications and requirements relevant to the mobile payment product it submits for testing and compliance

Table 1–2: Documentation Acronyms

Document Acronym	Document Title
[EMV_ICCN]	EMVCo Integrated Circuit Certificate Number
[EMV_SEWG]	EMVCo Security Evaluation Process
[EMV-CCP]	EMV® Contactless Communication Protocol Specification. Also known as Book D
[ETSI-001]	ETSI TS 102 613 UICC - Contactless Front-end (CLF) Interface; part 1 physical and data link layer characteristics
[MA]	Multi-Access Specification for VMPA
[SIM-PROF]	SIM Profile Requirements for Functional Testing
[VCSP]	Visa Chip Security Program – Security Testing Process
[VMCPS]	Visa Mobile Contactless Payment Specification
[VMPA_TP]	Visa Mobile Contactless Payment Specification Functional Testing Requirements

2 Mobile Testing Overview

Visa oversees testing of mobile proximity payment products that will be used to conduct Visa "payWave" payment transactions to ensure that they comply with Visa, GlobalPlatform and EMVCo specifications and requirements.

Mobile products subject to such testing include, but are not limited to:

- Secure Elements
- Mobile Wearable Products

Depending on the configuration of the product submitted the testing process may involve:

- Analog and Digital (EMVCo Contactless Level 1)
- Visa Cross Testing / Interoperability testing
- Visa Mobile Payment Application testing (VMPA) including any extension
- Secure Element Platform Functional testing (GP)
- Secure Element Platform Security testing (EMV® PCN)
- Secure Element Visa Chip Security Program testing (VCSP)

If the mobile product meets Visa's testing requirements, Visa issues a Compliance Letter to the vendor. Visa's compliance recognition applies worldwide unless geographic restrictions are specified in the Compliance Letter.

Note: The process described in this document does not approve vendors; it only denotes that a tested mobile product is compliant to Visa specifications and requirements.

Note: A Compliance Letter is not transferable from one vendor's product to another product or from one vendor to another vendor.

2.1 Products Accepted for Testing

This document covers the following configurations of mobile products for compliance testing:

- Embedded Secure Element Component (alone /on board)
- Mobile Wearable Product

Note: For information relating to non NFC-based wearables and inlays, please refer to the Visa Chip Card Testing and Approval Requirements on the VDPS.

Visa will decide in its sole discretion whether to accept alternative configurations of mobile products for testing. Vendors should contact their regional Visa representative to determine if Visa will accept their alternative mobile product configuration. The Vendor must provide a complete description of the alternative mobile product to aid Visa in its decision-making.

2.2 Mobile Component Overview

To simplify the description of the testing program, the mobile product is divided into component zones. These component zones identify areas within a mobile product that perform different aspects of proximity "Visa Contactless" mobile payment. The configurations and components within these zones are subject to this testing program. Five zones have been identified and are described in the following sections. Following the zone descriptions are diagrams showing some of the common mobile component configurations of zones, components, and the interfaces between these zones and components.

2.2.1 A: Secure Element Component

This component known as a Secure Element (SE) could also be identified by various names for the different form factor/product such as embedded Secure Element (eSE), or removable SE. This component hosts the VMPA applet.

2.2.2 B: Contactless Interface Component

This component mainly performs the conversion of interfaces from an analogue signal to digital contact based link such as Single Wire Protocol (SWP) and Host Controller Interface (HCI). As a most common implementation, the contactless interface component is expected to be a Near Field Communication device.

This module may incorporate a router to direct the contactless communication to various Secure Elements on the handset and to the handset itself. In this case, the functionality of the component extends beyond interface conversion.

In some cases, the Secure Element component (A) may be capable of receiving analogue signals with an ability of analyzing them to the digital (contactless protocol) level. In such configurations, there is no component B.

2.2.3 C: Proximity Communication Antenna

This component captures and transmits Radio Frequency (electromagnetic field) analogue signals with an external device such as a contactless-enabled POS terminal.

2.2.4 D: Handset Device

This component incorporates the previously described components as well as others related to the mobile wireless network. It also hosts the handset part of the Visa Proximity Mobile Payment Application, such as the user interface application (referred to as the wallet).

2.2.5 E: Mobile Application

This component is the software application resident on the mobile device that consumers use to interact with their mobile device to access a product or a service. For Visa cloud-based payments, Mobile Applications typically include, but are not necessarily limited to, mobile banking applications or mobile wallet applications.

2.2.6 MA: Mobile Wearable Product

This component is a peripheral unit to a mobile device. It may or may not be physically connected to the mobile device.

2.2.7 Interaction between Components

Although the mobile product components must go through testing that is required for Visa, Visa testing focuses on the secure element (hosting the VMPA applet) and the contactless interface components.
The tests that are performed and the tests that are out of scope are described in this document.

The following diagrams represent possible arrangements of components in a mobile product. The diagrams indicate areas tested, areas not tested, and interfaces that may be exercised during testing.

The following diagrams are shown in different colors, which signify the following:

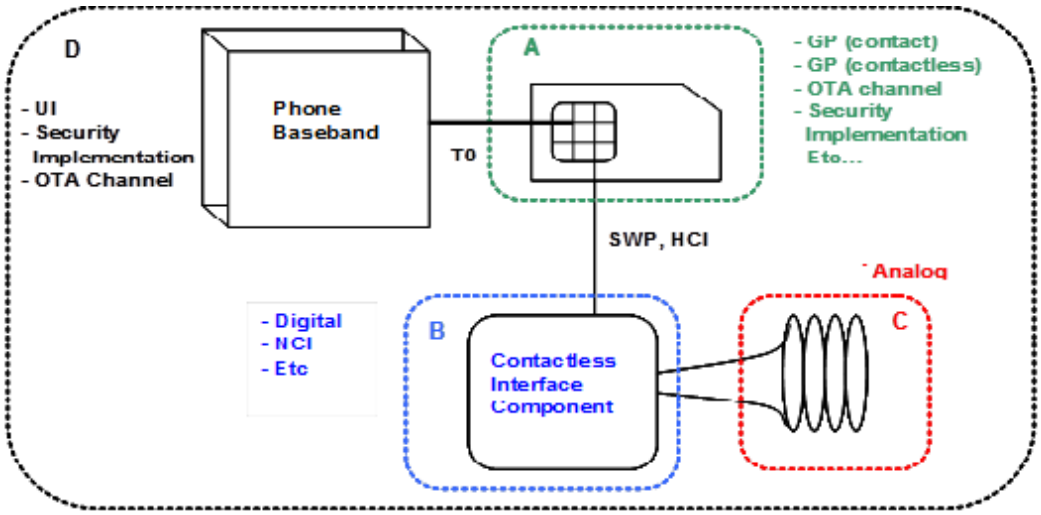
- **Green**: indicates the Secure Element component and some of the technologies that may be implemented in that component

- **Blue**: indicates the Contactless Interface component and some of the technologies that may be implemented in that component
- **Red**: indicates the Proximity Communication Interface component and some of the technologies that may be implemented in that component
- **Black**: indicates the Handset component and some of the technologies that may be implemented in that component
- **Orange**: indicates the mobile application component and some of the technologies that may be implemented in that component.

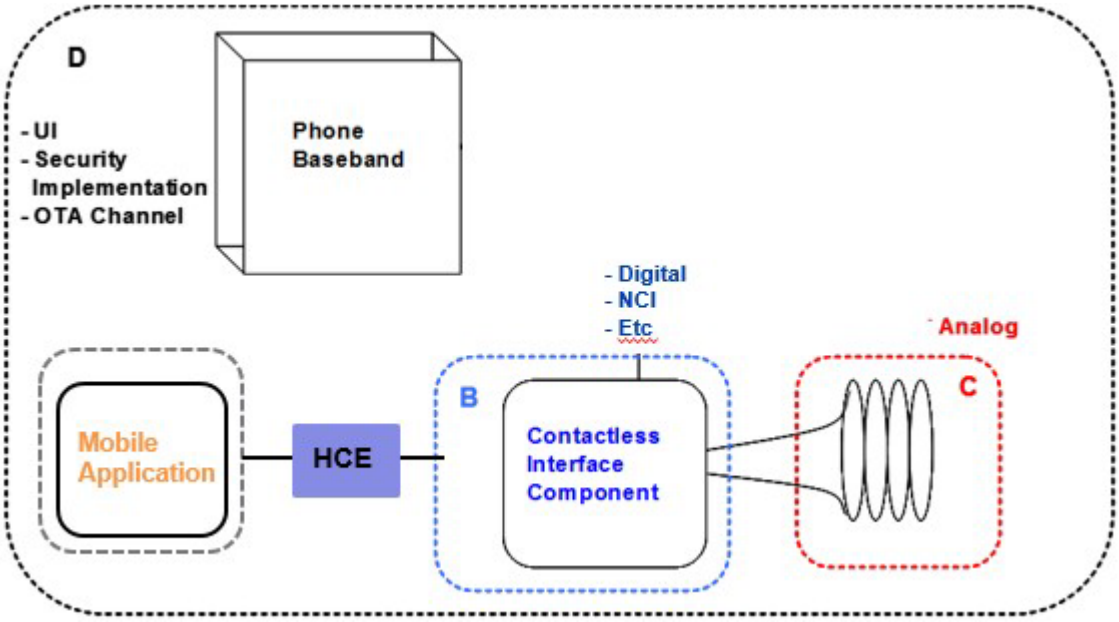
The figures that follow show the component zones A, B, C, D, E, MA that are subjects of the testing and compliance process. These diagrams are simplified models used to represent what is usual and expected in today's mobile payment products. These diagrams are not based on any specific mobile payment product.

2.3 Mobile Component Descriptions

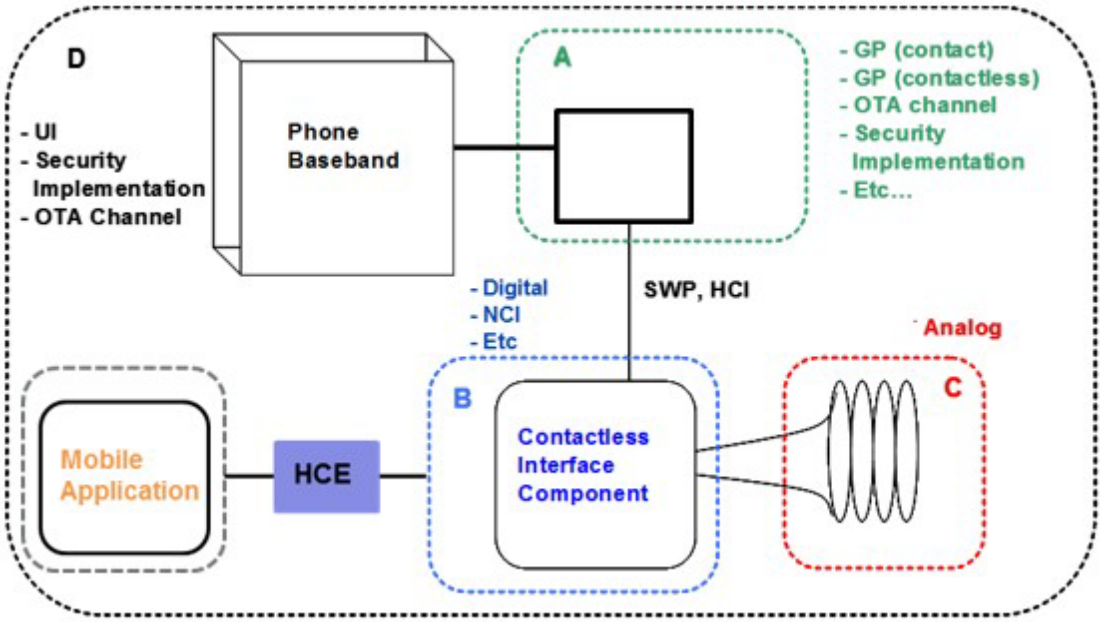
2.3.1 Components with a Secure Element



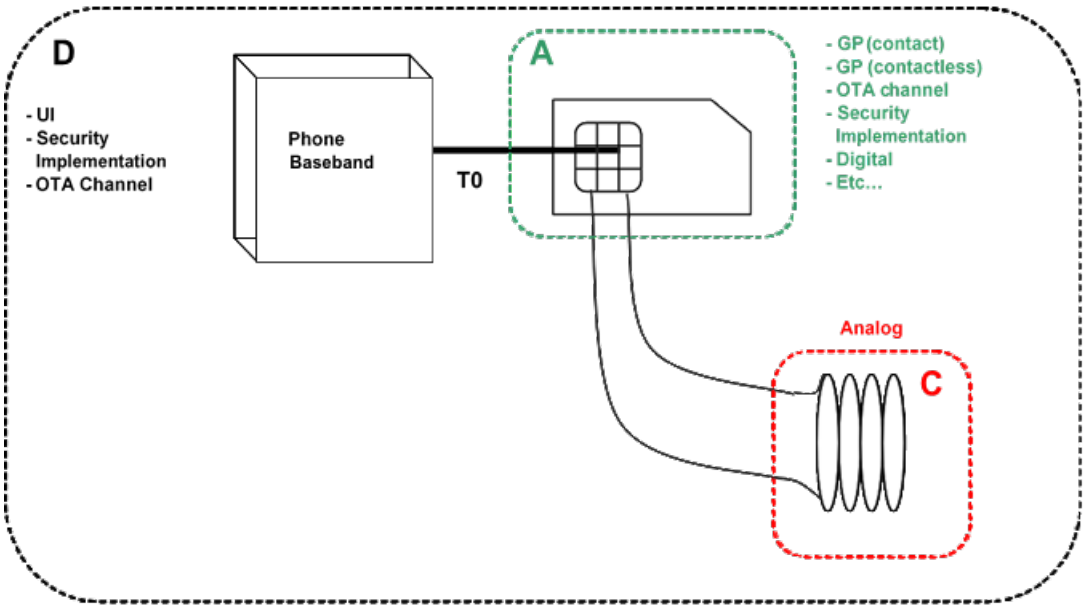
2.3.2 Components with Host-based Card Emulation (HCE) Capability



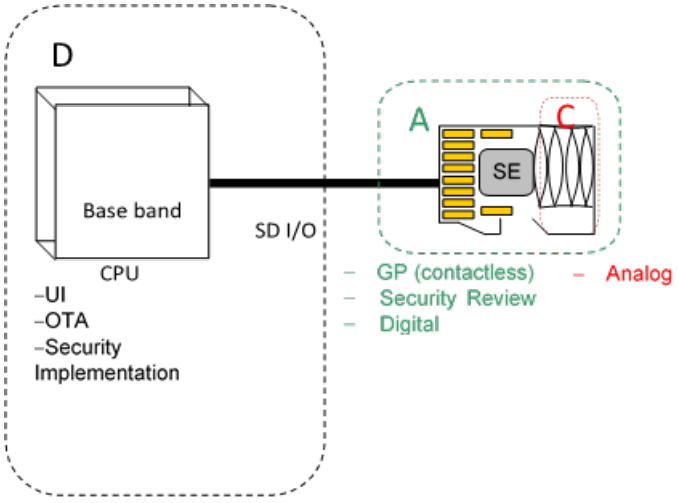
2.3.3 Components with a Secure Element and Host-based Card Emulation (HCE) Capability



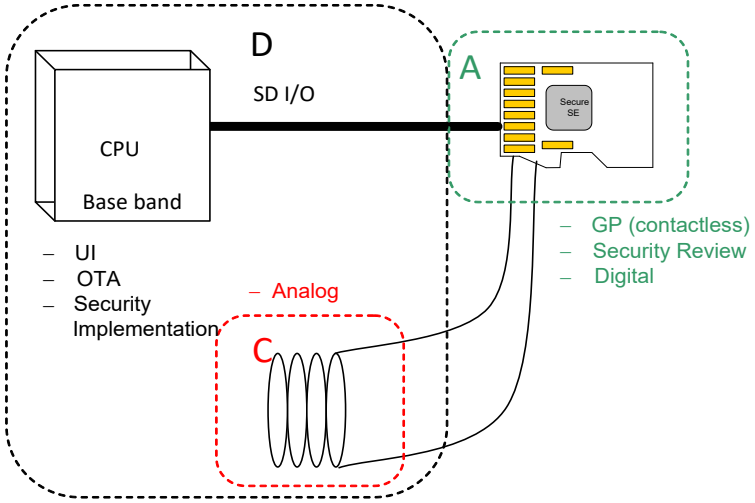
2.3.4 Components without a Contactless Interface Component



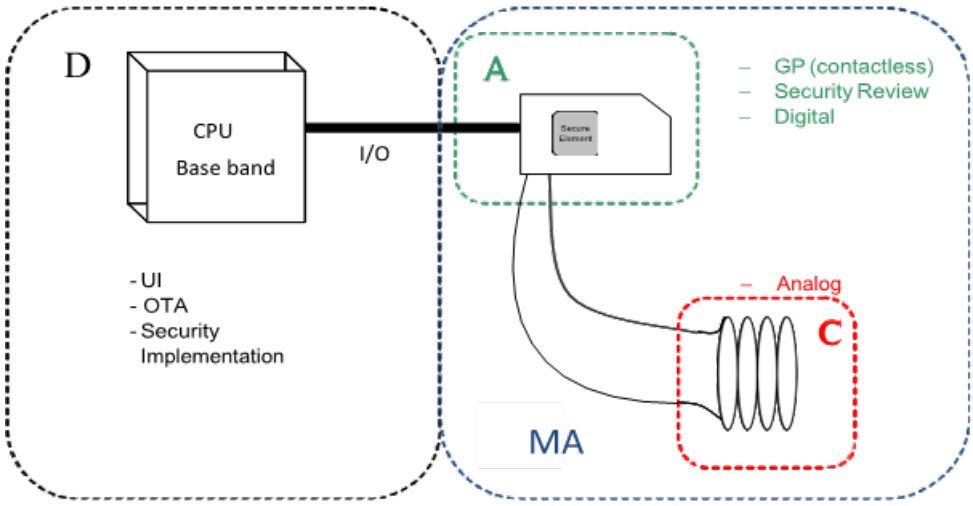
2.3.5 Components with a Removable microSD with Internal Antenna



2.3.6 Components with a Removable microSD with Antenna in the Handset



2.3.7 Components with a Mobile Wearable with a Secure Element



2.4 Embedded Secure Element (eSE) Component

A vendor can submit a secure element for testing that is developed according to GlobalPlatform specifications.

Prior to submitting the eSE for testing the vendor must ensure that the chip is listed on EMVCo's Approved Chips List and the platform is listed on EMVCo's Approved Platforms List. See Section 3.0 regarding Security Testing.

The Visa Compliance Letter will address the product's ability to host a VMPA applet and complete a Visa payWave payment transaction. At the very minimum, platforms must support the GlobalPlatform configurations for secure elements. All other functionality (e.g. Single Wire Protocol (SWP) interface) is out of scope of Visa's compliance testing. It is the vendor's responsibility to ensure proper compliance to the respective standards issued by other organizations such as ETSI.

2.4.1 Visa Token Service (VTS) Compatibility Requirements for Secure Element Products

A secure element implementation that intends to connect to the Visa Token Service (VTS) must meet requirements defined by Visa Ready.

Any secure element implementation that intends to connect to the VTS can only use a Visa Approved Secure Element that is compatible with VTS. The requirements below for mobile and wearable products outline these compatibility constraints. If you have approved products that do not meet these requirements, please consider updating them to become VTS compatible.

Product Requirements :

- Products must support GlobalPlatform (GP) card specification 2.3 Amendment 'A' scenario #1 with a RSA key size of 2048 bits.
- Product must use a Visa-approved VMPA applet located on VDPS.
- Additional VTS requirements may be applicable. For additional information, please contact VisaReadyDigitalPlat@visa.com.

2.4.2 Embedded Secure Element (eSE) Component

This configuration is of a stand-alone embedded secureelement (eSE).

Table 2–1: Scope of the Tests for Embedded Secure Element (eSE) Component

Test Type	Test Extent	Zone Subject to Testing	Supporting Specification(s)
Cross-Testing / Interoperability Testing	eSE: Not Applicable	-	-
Visa Application Testing	Applicable	A	[VMCPS]
GP Platform Functional Testing	Applicable	A	Refer to GlobalPlatform
Platform Certification Testing	Applicable	A	Refer to EMVCo
Visa Security Testing	Applicable	A	[VCSP]

Note: If the configuration includes built-in contactless digital protocol technology, digital testing is required.

2.5 Wearable Products

A mobile wearable product is a form factor that can be worn on the body, such as a wrist watch or bracelet. A wearable may or may not rely on a mobile handset to complete a Visa payWave transaction. It is assumed that a wearable is not physically connected to another device such as a handset and can be tested as a standalone product independent of any specific external device.

Wearables can take advantage of reduced testing if they leverage a compliant mobile inlay.

The proximity communication antenna may be the original design from the inlay or modified to fit into the physical dimensions of the wearable. Mobile inlays are expected to be embedded into the final design of the wearable and cannot be removed by the consumer.

Table 2–2: Scope of the Tests for wearable products

Test Type	Test Extent	Zone Subject to Testing	Supporting Specification(s)
Analog	Applicable	A + C	[EMV®-CCP]
Digital	Applicable	A + C	[EMV®-CCP]
Cross-Testing	Applicable	-	-
Visa Application Testing	Applicable	A	[VMCPS]
GP Platform Functional	Applicable	A	Refer to GlobalPlatform
Platform Certification	Applicable	A	Refer to EMVCo
Visa Security Testing	Applicable	A	[VCSP]

If utilizing a tested and compliant inlay only analog and cross testing is required.

2.6 Component Specification and Compliance

The components described in this document are developed based on specifications defined by various standards bodies such as GlobalPlatform or EMVCo.

Visa acknowledges that some of these organizations have developed a compliance program for their respective specification and Visa will incorporate those programs into Visa's compliance process. Among these various compliance programs, certain plans exist that grant testing laboratories the following:

- The right to perform the tests
- The authority to provide test results
- The authority to certify the component

3 Security Testing

Security testing is required for the secure element hosting the VMPA applet. It is not applicable to other components of a mobile product, such as the NFC device containing the contactless interface components.

Security testing goes beyond the functional testing to help determine whether the secure element is vulnerable to 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 conducted testing, knowledge of the particular application(s), and past experience with similar products. The Visa Chip Security Program (VCSP) seeks to minimize the cost and time spent in performing evaluation work and, where possible, to avoid duplication of effort. A copy of the VCSP process document can be downloaded from theVisa Digital Partner Services.

The VMPA applet must only be loaded on a secure element that has successfully undergone and passed EMVCo's security evaluation process. Visa will accept new mobile product submission only if the platform and the underlying IC holds a valid EMVCo Platform Certificate Number (PCN) and an Integrated Circuit Certificate Number (ICCN), respectively.

The VMPA applet residing on the EMVCo approved platform must successfully complete a Visa composite security evaluation (e.g., platform with VMPA applet) by a Visa recognized security lab. As required level of assurance, it must achieve "High" JIL attack potential rating against state of the art attacks.

The security testing laboratory must verify that the final product properly protects Visa assets, taking into account the result of the platform security evaluation as documented in the Shared Evaluation Report (SER) and the accompanying security guidelines. These documents described what security mechanisms are implemented by the platform and the scope of previously performed security testing. They provide mandatory security requirements and highlights areas of potential concern. The overall goal here is to obtain assurance that the composition of the VMPA applet and the platform sufficiently protects Visa assets against state of the art attacks.

Any pre-loaded or future (post-issuance) application loaded on the secure element must not impact the security of the Visa payment application assets. Each application is recommended to pass the latest byte code verifier and must meet all requirements in the latest platform security guidance documents.

Note: Visa composite security evaluation can be authorized once the EMVCo platform security evaluation has started. However, it will only be reviewed and approved once the PCN is officially granted by EMVCo and after verification by Visa that the composite evaluation done is consistent with the final result of the platform evaluation.

Conducting the composite security evaluation while the PCN is pending has associated

risks (e.g. if not subsequently approved or requires update on the platform, etc.). Visa will not be responsible for any risks, costs or delays associated with a pending PCN.

For More Information

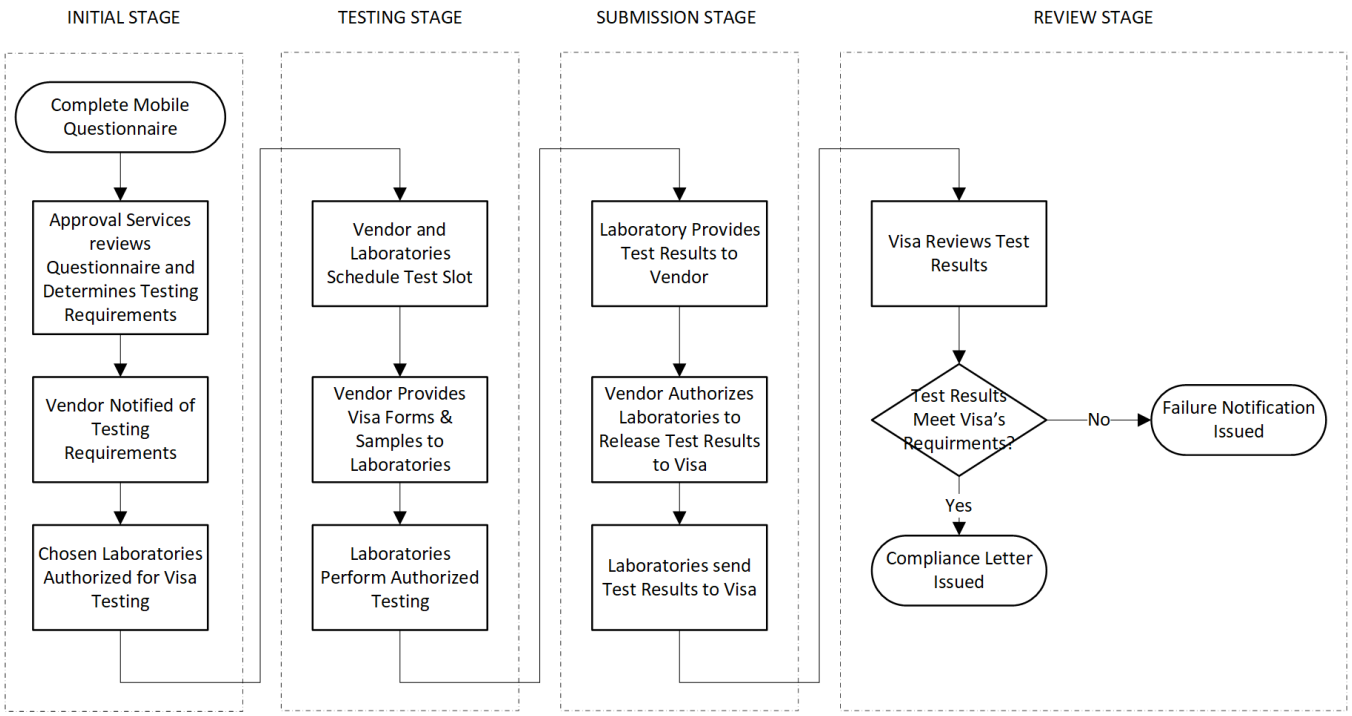
For detailed information on the EMVCo 'IC' and 'Platform' Security Evaluation process, please see EMVCo Security Evaluation Process document available at www.emvco.com, or contact the EMVCo Security Evaluation Secretariat at securityevaluation@emvco.com with any questions about the process.

For further information on the Visa chip security testing process, please refer to the *"Visa Chip Security Program – Security Testing Process"* document on the VDPS

4 Certification Process, Laboratories and Documentation

4.1 Certification Process Overview

Figure 4-1: Product Submission and Compliance Testing Process



4.2 Certification Areas By Organization

To reduce the duplication of testing for vendors, Visa's program utilizes testing and certification programs offered by EMVCo and GlobalPlatform.

Depending on the configuration and technical specifications of the mobile product, Visa may require the product to have been certified by those organizations prior to submitting the product to Visa.

Visa's program covers Secure Elements and wearables thereof, with different testing requirements for each. See Appendix C for testing requirements by product configuration.

EMVCo's certification programs cover chips and platforms used for Secure Elements, whether

embedded or removable and Host-based Card Emulation (HCE). In addition, they offer Contactless EMV Level 1 testing for handsets.

GlobalPlatform's certification program covers functional platform qualification for Secure Elements, whether embedded or removable.

Furthermore, a product being tested by more than one organization may also be performed in parallel (e.g. Visa testing, GlobalPlatform testing), again at the request of the vendor and at their own risk.

The following table shows which areas of testing each organization qualifies:

4.3 EMVCo Mobile Product Level 1 Testing

Visa requires products to receive an EMVCo issued Letter of Approval in lieu of testing requirements managed by Visa, if EMVCo offers the testing.

If the EMVCo Letter of Approval is not available at the time of the product submission to Visa, the vendor is responsible for providing the Letter of Approval before Visa will determine whether the product meets Visa's requirements and issue a Compliance Letter.

***Note**: Visa does not issue a Compliance Letter for a product with an EMVCo Letter of Approval that does not require additional L2 testing required by Visa.*

Vendors are required to provide the EMVCo Level 1 ICS with the Letter of Approval.

If Visa requires other testing on the submitted product, this may be done in parallel with the EMVCo process.

Visa will continue to accept EMVCo's process as they continue to expand the scope of products accepted.

4.3.1 Obtaining Visa Test Package for EMVCo Testing

Visa only provides the Test package for EMVCo testing to product providers who are registered with EMVCo.

If the product provider is not registered, they must reach out to EMVCo to begin the process. Once the registration is complete, the product provider must contact Approval Services requesting the Visa test package for EMVCo testing. Visa will request that product provider completes a license agreement with Visa. In addition, they must also provide their PGP key because the package will be encrypted.

4.4 GlobalPlatform Qualification Testing

A vendor can submit a secure element for testing that is developed according to GlobalPlatform (GP) specifications.

GlobalPlatform manages the platform functional testing for GP platforms.

Visa only accepts official GP test results performed by a GP-qualified laboratory. Self-testing results are not accepted as proof of specification compliance.

Vendors shall provide a Supported Configuration Options (SCO) number and Letter of Qualification (LoQ) from GP to Visa in support of their Visa submission process.

Visa requires Secure Elements to have the SCO and LoQ issued by GlobalPlatform prior to the issuance of the Visa Compliance Letter.

Vendors who are unable to receive a Letter of Qualification (LoQ) from GP because their product does not support all mandatory GP requirements may request a Compliance Assessment Report (CAR) from GP.

Visa will only review a final GP CAR. As an exception process, vendors who provide a GP CAR to Visa where the product meets Visa's minimum functional platform requirements may be eligible to receive a Compliance Letter from Visa without a Letter of Qualification (LoQ) from GP.

More information about the GlobalPlatform compliance testing process can be found on its website at http://www.globalplatform.org/.

4.5 Cross Testing

Visa performs cross testing (also referred to as interoperability testing). Cross testing is part of the official testing process and the performance during this testing will be part of the final compliance consideration. Products that fail to communicate with multiple terminals may not be eligible for compliance.

***Note**: Visa is not permitted to disclose information about the terminals used to obtain the cross testing results.*

EMVCo also offers cross testing, referred to as terminal interoperability testing, as part of its mobile product level 1 type approval process. Visa accepts an EMVCo Letter of Approval in lieu of cross testing.

4.6 Test Plans and Test Tools

Test plans and commercial test tools with associated test scripts are available to assist vendors in conducting quality assurance (QA) testing prior to submitting the product for official testing. These test tools are not intended as a replacement for Visa testing.

Successful completion of all the test scripts by the vendor does not imply compliance, nor does it duplicate Visa's full testing process.

Visa reserves the right to develop and run additional tests that are not defined as part of the current test plans or tools. Visa testing may include subjecting the product to additional physical and situation- specific tests as needed.

Commercial test tools and test scripts are available from test tool suppliers. Vendors must have licensed the Visa mobile specification and software before acquiring the mobile test tools.

Information about Visa test tools can be found at Visa Digital Partner Services (VDPS)

Information about EMVCo test tools can be found at www.emvco.com.

Information about GlobalPlatform test tools can be found at www.globalplatform.org.

The following Visa test plan is available on the Visa Digital Partner Services (VDPS) to licensed users:

- Visa Mobile Payment Application (VMPA)

Before requesting a test plan, the following agreements need to be executed with Visa:

- All applicable Visa Technology License Agreements. Technology licensing is handled on the Visa Technology Partner website.
- Approval Services Testing Agreement (ASTA)

Possession and use of these materials are subject in all respects to the terms of the ASTA.

Test plans and test scripts are subject to enhancements and modifications at any time. Test plan revisions will be accumulated and made available to vendors with new releases as determined by Visa. It is the vendor's responsibility to ensure that they have the most current test plan available. Vendors should contact their tool supplier to obtain any test script updates. Test case updates are published in the query application on the Visa Technology Partner website, available to authorized users only.

Visa grants permission to use the test plans solely for purposes of QA testing for use in connection with a Visa payment application. Visa may revoke its permission at any time for any or no reason. Possession and use of these materials are subject in all respects to the terms of the ASTA or documentation license agreement. Test plans and all intellectual property subsisting therein are the property of Visa. THESE MATERIALS ARE PROVIDED ON AN "AS IS" BASIS "WITH ALL FAULTS. VISA DISCLAIMS ALL WARRANTIES PERTAINING TO THESE MATERIALS, EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR PURPOSES, OR NON INFRINGEMENT.

4.7 Test Laboratories

The list of Visa-Recognized Laboratories is available on the Visa Digital Partner Services (VDPS).

Testing will not begin until the laboratory has received all required items. If any required item is incorrect or non-functioning, the test slot may be delayed.

Please contact the Laboratory for pricing and to arrange scheduling of testing.

When testing is complete, the Laboratory will provide the vendor with a report outlining the test results.

The vendor is required to grant authorization for the Laboratory to provide the test reports to Approval Services.

Approval Services will evaluate the test results and provide the vendor with information about the usability of the product in Visa deployments.

4.8 Starting the Product Submission Process

Before submitting any mobile product for testing, vendors must execute the current Approval Services Testing Agreement (ASTA) with Approval Services.

Additionally, vendors will also need to execute any agreements required by the Laboratory that performs the testing.

Once the legal agreements have been executed, vendors are eligible to submit the necessary paperwork to start the testing process.

A questionnaire is required by Approval Services to start the product submission process.

The following table lists the forms required for product testing. All the Visa forms are available on the Visa Digital Partner Services (VDPS) websites. All information must be provided in English.

Note: Some forms may be combined into a single document.

Table 4–1: Documentation Required for Testing and Evaluation

Forms	Description
Mobile Secure Element Questionnaire	Information regarding the submission of a mobile secure element product for testing. Allows Visa to determine whether the mobile secure element product is eligible for submission.
Exhibit A: Request for Testing Services and Request for Compliance Form	Establishes Visa's right to review testing results submitted by the Vendor, following testing at a Laboratory. Vendors who have signed the ASTA May 2018 or newer version no longer need to provide this form. An official request to release test reports to Visa so that Visa can begin the review and compliance process for a product tested at the Laboratory.
Implementation Conformance Statement (ICS)	A vendor must provide detailed information regarding the Visa payment application, platform, or interface. A separate ICS is needed for each type of functional testing performed.
Single Production Batch Confirmation Form	Declares that the secure elements supplied to the laboratories and Approval Services are all from the same production batch and are identical without modifications. Only required for configurations involving secure elements.

Table 4–2: Additional Documentation Required for Testing and Evaluation

Forms	Description
GlobalPlatform Letter of Qualification (or Conformance Assessment Report) and Support Configuration Options Number	Vendors whose product has gone through GlobalPlatform functional testing shall provide the long version of the Letter of Qualification (LOQ) including any Conformance Assessment Report (if applicable) and the Supported Configuration Options (SCO) Number. See section 4.4.
EMVCo Platform Certificate	Vendors whose product has gone through EMVCo platform security testing shall provide a copy of the certificate if the platform is not published on EMVCo's Approved Platforms List on their website.
EMVCo Letter of Approval	Vendors whose product that has gone through EMVCo Mobile Product Level1 Type Approval process shall provide a copy of the Letter of Approval including the associated EMVCo ICS.

5 Submission of Testing Materials for Functional Testing

This section details the materials that the vendor must submit to the laboratory for Visa functional testing. Refer to **Appendix C** for detailed requirements by product configuration.

5.1 Requirements for Product Submission

5.1.1 For All Product Configurations

Products submitted for testing must be in the final configuration that will be deployed commercially. The exception is Embedded Secure Element (eSE) Components, which are accepted for testing prior to embedding in a commercial product.

All debugging code must be removed from the product before it is submitted for testing. Failure to remove this code will cause the product to fail testing.

5.1.2 For Secure Elements

Secure Elements must contain a Visa-approved VMPA applet and PPSE applet, pre-installed and personalized.

Secure elements containing a Visa-developed VMPA applet shall be provided as follows:

- the VMPA applet loaded, Container installed as defined in [VMPA_TP]
- SIM profile configured as described in [SIM-PROF]
- A Proximity Payment System Environment (PPSE) applet installed and configured.
- The ICS form shall accurately represent the personalization of the samples.

EMV® Common Personalization Specification is required to personalize the VMPA applet. If the mobile product allows multiple application instances with pre-personalized images, the documentation must also explain how to select among the different applications with specific instruction on how to obtain the application image(s) needed for Visa's testing requirements.

Products should be clearly marked with the Visa Reference Number, the VMPA applet version and build number, and mobile image the VMPA applet was personalized with.

The Single Production Batch Confirmation form must be completed, printed and included in the package sent to the Laboratory

5.1.3 Wearable Products

The vendor must include all cables and batteries required to operate the product including detailed operating instructions and how to configure the device for NFC communication.

Products should be marked to show the location of the zero point. If the product is intended to be used in a defined orientation and/or presentment, this information must be communicated to Approval Services and the laboratory as part of the product submission.

Products should be clearly marked with its assigned Visa Reference Number.

A user guide detailing how to operate the product and access the payment application must be provided.

Vendors who are submitting a product utilizing an embedded secure element (eSE) and have not licensed the Visa specifications and mobile software should consult with their embedded secure element provider on providing VMPA installed and personalized for testing a completed VMPA ICS form, and a Test Tool Interface Application.

If there are any changes to the product after the testing authorization has been sent Approval Services is required to be notified and the testing requirements to be reassessed. If samples have been sent to the Laboratory, new samples are required to be resent to **all** Laboratories.

- The vendor must provide the laboratory with at least two samples for testing.
- The vendor must provide Approval Services with at least two samples for cross testing.

5.1.4 Shipping

Vendors shall indicate, either directly on the product samples or on the shipping documentation, the Visa Reference Number of the product(s) being tested and contained in the shipment.

The shipper is responsible for completing and providing all required US Customs forms, including FCC Form 740 if required. The shipper shall be liable for any and all costs associated with releasing an impounded shipment seized by US Customs due to missing or incomplete paperwork.

Note: Testing will not begin until the laboratory has received all required items. If any required item is incorrect or non-functioning, the test slot may be delayed.

Vendors have six months from the date Approval Services authorized the laboratory testing to submit all test results to Approval Services for review.

After testing is complete, the Laboratory and/or Visa will retain the tested components for any subsequent testing that may be required.

5.2 Testing eSE Product Over Contact Interface

Testing eSE Product Over Contact Interface

Vendors must supply the Test Tool Interface Application (TTIA) to access the eSE in mobile or wearable product over the contact interface. The TTIA enables personalization for functional and transaction testing on eSE products. Visa does not supply a generic TTIA. Visa supplies the requirements to build a TTIA.

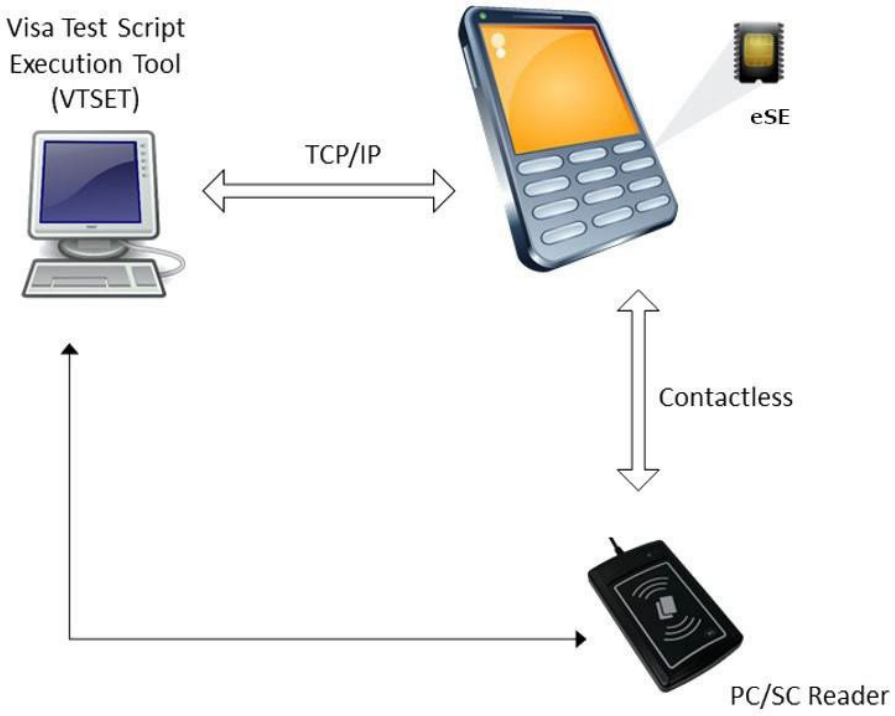
Personalization of eSE involves card content management according to GlobalPlatform specifications. The TTIA host must provide the tester a means to issue commands to the eSE product.

The TTIA host must also provide a means for the tester to view and analyze responses sent from the eSE product back to the test tool client.

The TTIA host must also provide a means to log all of the commands and responses sent during a test session.

The TTIA host must provide a means to save the log as a file and provide a means to print the log from the current test session or from a file saved from a previous test session.
The TTIA shall provide a means so that the Visa Test Script Execution Tool is able to establish a connection. Please refer to VMPA Test Tool Interface Requirements (Book 6) and Guidance for Visa Mobile and Wearable Products TTIA document for detailed information.

Figure 5-1: TTIA with Embedded Secure Element (eSE)



5.3 Utilizing Test Results between Products

Vendors may have the opportunity to leverage functional test reports from previously certified components and products. A product that uses shared test results may be eligible for reduced testing.

If Visa discovers a defect in a previously certified product, all vendors involved in the sharing consent to Visa's communication of all relevant information to each affected vendor and its customers, including an explanation of the nature of the defect and products at issue.

Shared test results are only permitted under and are subject to the following conditions:

- All vendors involved in the sharing have signed the appropriate agreements allowing results to be shared.
- The components being leveraged have been tested and certified by Visa with no issues.
- The components being leveraged are not already sharing test results from another product.
- A product using shared results will be tied to the original product
- The new product will receive the same expiration date as the product from which the results are shared.
- If for any reason the original product is not renewed, any product sharing testing results will not be renewed either.
- If the original product is revoked, then all products sharing testing results will be revoked.
- If the original product is modified and/or updated, then all products sharing testing results may require additional testing.

Note: If a product is submitted for full testing, it receives an independent certification and its expiration date is not tied to any other product.

5.4 Utilizing Test Results between Products

Vendors may have the opportunity to leverage functional test reports from previously certified components and products. A product that uses shared test results may be eligible for reduced testing.

If Visa discovers a defect in a previously certified product, all vendors involved in the sharing consent to Visa's communication of all relevant information to each affected vendor and its customers, including an explanation of the nature of the defect and products at issue.

Shared test results are only permitted under and are subject to the following conditions:

- All vendors involved in the sharing have signed the appropriate agreements allowing results to be shared.
- The components being leveraged have been tested and certified by Visa with no issues.
- The components being leveraged are not already sharing test results from another product.
- A product using shared results will be tied to the original product
- The new product will receive the same expiration date as the product from which the results are shared.
- If for any reason the original product is not renewed, any product sharing testing results will not be renewed either.
- If the original product is revoked, then all products sharing testing results will be revoked.
- If the original product is modified and/or updated, then all products sharing testing results may require additional testing.

Note: If a product is submitted for full testing, it receives an independent certification and its expiration date is not tied to any other product.

6 Compliance Letters

This section describes the process that vendors must follow in order to obtain a Compliance Letter for a mobile payment product.

6.1 Legal Conditions and Restrictions

Visa's determination that a product complies with its specifications only applies to products that are identical to the product tested by one of Visa's recognized laboratories or by Visa. A product should not be considered compliant to Visa's requirements, nor promoted as compliant, if any aspect of the product is different from the specimen that was tested by a laboratory or by Visa, even if the product conforms to the basic product description contained in the Compliance Letter. For example, even though a product contains components, applications or operating systems that have the same name or model number as those tested by one of Visa's recognized laboratories or by Visa, but the product is not identical to the features previously tested by one of Visa's recognized laboratories or by Visa, the product should not be considered or promoted as compliant to Visa's requirements.

Visa's Compliance Letter is granted solely in connection with a specific product and to the submitting vendor. A Compliance Letter may not be assigned, transferred or sublicensed, either directly or indirectly, by operation of law or otherwise. Only vendors that have received a Visa Compliance Letter for a mobile payment product may claim that they have a Compliance Letter.

No mobile payment product manufacturer, chip supplier, or other third party may refer to a product, service or facility as "compliant" or as having a "Compliance Letter", nor otherwise state or imply that Visa has, in whole or part, found the product to be compliant to Visa's requirements in any aspect of a manufacturer, or supplier, or its products, services or facilities, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with Visa, or in a Compliance Letter provided by Visa Approval Services. All other references to Visa's "Compliance Letter" or "compliance" are strictly prohibited by Visa.

When given, Visa's Compliance Letter is provided by Visa to reflect certain security and operational characteristics important to Visa's systems as a whole, but does not, under any circumstances, include any endorsement or warranty regarding the functionality, quality or performance of any particular product or service. Visa does not warrant any products or services provided by third parties. A Compliance Letter does not, under any circumstances, include or imply any product warranties from Visa, including, without limitation, any implied warranties of merchantability, fitness for purpose or non- infringement, all of which are expressly disclaimed by Visa. All rights and remedies regarding products and services that have received a Visa Compliance Letter shall be provided by the party providing such products or services, and not by Visa. Unless otherwise agreed in writing by Visa, all

property and services contemplated in this document that Visa provides to any person or entity are provided on an "as-is" basis, "with all faults" with no warranties whatsoever. Visa specifically disclaims any implied warranties of merchantability, fitness for purpose or non-infringement.

The issuance of the Compliance Letter is conditioned upon the vendor having executed all necessary agreements with Visa, including without limitation, all applicable license agreements with Visa and shall be of no force and effect unless such agreements have been executed prior to the issuance of the letter.

Visa performs limited testing to ascertain a product's compliance with any required specifications and may perform interoperability testing with other compliant or approved products. Visa's limited testing program is not designed to ensure the proper functioning of vendor's compliant product in all potential conditions in which it may be used. Visa's Compliance Letter does not include or imply any guarantees, assurances or warranties that the compliant product will operate in all settings or in combination with any other compliant or approved product.

6.2 Requesting a Compliance Letter

Visa will consider issuing a Compliance Letter only for mobile payment products that have successfully passed testing at a Visa-recognized laboratory and that support Visa's mobile payment product requirements.

Approval Services ensures that all agreements, tests, and reviews have taken place at a laboratory including:

- All mobile payment products destined for use in Visa mobile payment projects have passed all testing as identified in this document.
- All required documentation for the mobile payment products tested at a laboratory must be completed by the vendor and submitted to Visa for verification.

At the vendor's request, products that are submitted to Visa to perform cross testing that do not successfully pass cross testing may be returned to the vendor.

Note – Visa does not issue a Compliance Letter for products with an EMVCo Letter of Approval that do not require additional testing required by Visa.

6.3 Compliant Products List

In addition to the issuance of the Compliance Letter, the mobile product will be listed on either the public or private Visa Approval Services Mobile Compliant Products List, as chosen by the vendor. The public list is published on the Visa Digital Partner Services (VDPS).

7 Secure Element Lifecycle and Wearable Expiry Date

This section describes the requirements and the process of the secure element lifecycle management policy and the expiration date for a wearable product.

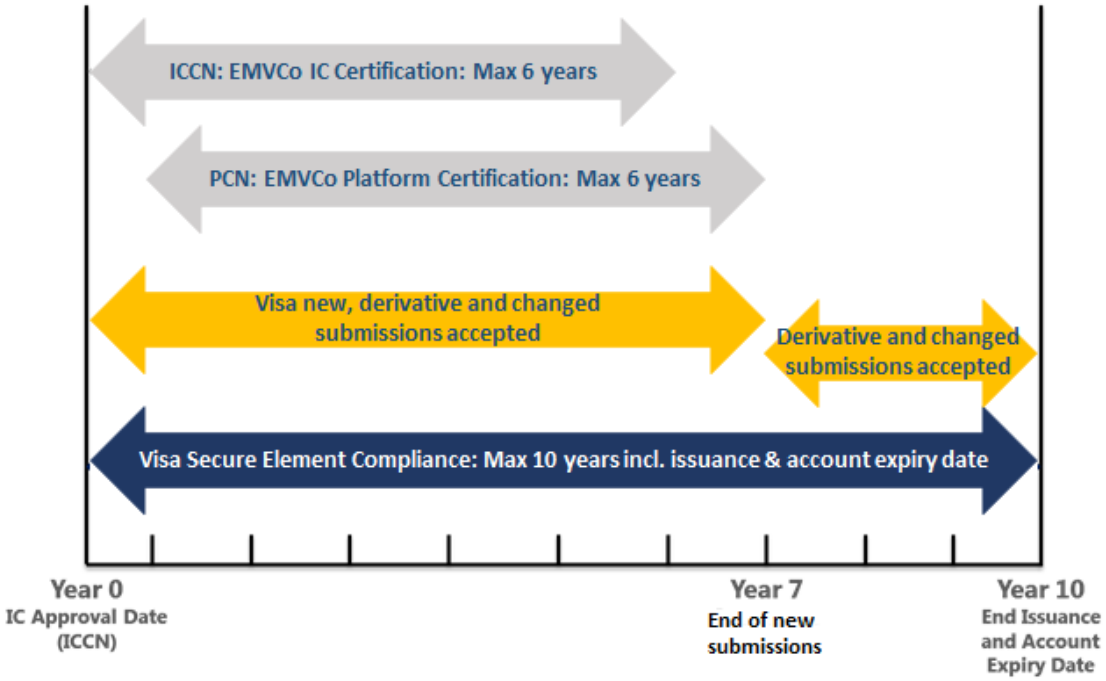
7.1 Secure Element Lifecycle Management

The secure element lifecycle management policy applies to all secure element form factors including removable[1] and embedded secure element (eSE) products.

Upon compliance of a secure element product, the compliance recognition end date assigned on the compliance letter will be based on the issue date of the underlying ICCN from EMVCo. The compliance recognition end date is defined as the **ICCN issue date + 10 years,** matching the date the Issuer must set the account expiration date for the Visa Mobile payment account.

When the compliance recognition end date of a secure element has been reached, the product will no longer be recognized as compliant and will be removed from the Visa Approval Services Mobile Compliant Products List.

Figure 7-1: Secure Element Lifecycle Management Policy



7.2 Tokenized Wearables Approval Expiration Date

Upon compliance of the tokenized wearable with an embedded secure element, the compliance recognition end date assigned on the compliance letter will be the **approval date plus 6 years** or the approval expiration date of the secure element, whichever is earlier.

The compliance letter will be sent to Visa Ready. The vendor will need to work with Visa Ready to complete the final wearable approval.

7.3 General Conditions and Exceptions

Visa does not offer renewals for mobile products.

If problems are identified with the product after receiving a Compliance Letter, Visa reserves the right to revoke its compliance recognition at any time.

Visa reserves the right to amend this policy without prior notice. The effective date of any such change will be communicated to vendors.

A Appendix A

A.1 Revision History

Version	Date	Description
4.1	May 2015	Added HCE testing information: Section 2, Section 5, Appendix B, Appendix C
5.1	October 2015	Updated Section 4.2 Updated Section 4.8 Updated Appendix B
5.2	December 2015	Updated Appendix B: Added base product testing requirements and updated derivatives testing requirements
5.3	February 2016	Minor editorial updates Section 7.2 Updated
5.4	June 2016	Updated Appendix B: Updated testing requirements based on Visa Chip Bulletin 13 4th edition and implementation of the second phase of EMVCo Mobile Product Level 1 Type Approval Testing. Minor editorial updates.
5.5	June 2019	Editorial updates Revised Test Matrix
5.6	July 2021	Removed Handsets and MicroSD Removed HCE test configurations Removed VTKPM Editorial updates Update Test Matrix
5.7	October 2022	Corrections, clarifications and updates Added Tokenized Wearables approval expiration date
6.0	June 2024	Removed UICC

B Appendix B

B.1 Testing Requirements for Changes to a Compliant Mobile Product

B.1.1 Appendix Structure

This appendix lists the testing requirements for base mobile products and changes to a compliant mobile product.

If a vendor wants to make a change that is not listed, contact ApprovalServices@visa.com to determine which process may be utilized.

B.1.2 Limits to Change Process

A change to ROM of the approved product's secure element is considered a new submission and testing is required. The security lab must provide an Impact Assessment Letter (IAL) to Approval Services defining the scope of the security evaluation.

Vendors that have received a Compliance Letter from Visa identifying issues in the specification deviation / comments sections may not use this process to make changes to a product. Vendors must correct the issue(s) identified in the Compliance Letter before submitting the next version of the product for testing.

B.1.3 Paper Approval Process

No functional or security testing is required.

Exhibit A – Request for Testing Services form must be completed, signed and provided to Approval Services if the vendor has not executed a version of the ASTA that is May 2018 or newer.

B.2 Testing Requirements

B.2.1 Secure Elements

This table is only a guideline and additional testing may be required depending on the test results.

Table B–1: Base Product Testing Requirements – Secure Elements

#	Base Product Configuration	EMVCo Contactless Level 1	Cross Testing	VMPA	GP LOQ	EMVCo PCN	Visa Security Testing	Notes
1	Embedded Secure Element (eSE) Component	None	None	Full	Yes	Yes	IAL/ Security testing	-

Table B–2: Derivative Testing Requirements - Secure Elements

#	Product Configuration	Derivation	EMV Contactless Level 1	VMPA	GP LOQ	EM VCo PCN	Visa Security Testing	Compliance Letter	Notes
1	All	Updating VMPA applet to a higher specification version	None	Full or Regression*	No	No	IAL	Yes	Security testing may be required in addition to the Impact Assessment Letter (IAL) from the security testing laboratory. *to be determined by AS
2	All	Addition of new applications (OTA or pre-issuance)	None	None	No	No	None	No	New application(s) must pass latest Oracle Byte Code Verifier and comply with latest Platform Security Guidance Documents.
3	All	Change to CREL/P PSE parameters (e.g. change Type A SAK from 28 to 20)	None	Transaction	No	No	None	No	Same PCN and ROM mask.
4	All	Different EEPROM or Flash memory size	None	None	No	No	None	No	-
5	All	Security patch	TBD	TBD	TBD	Yes	IAL	Yes	Security testing may be required dependent on the Impact Assessment Letter (IAL).

B.2.2 Wearable Products

This table is only a guideline and additional testing may be required depending on the test results.

Product submissions that are comprised of a wearable with another component, such as an embedded secure element (eSE), are subject to the aggregated testing requirements for each component making up the product being submitted. Therefore, a wearable with an embedded secure element (eSE) shall be subject to the testing requirements for both the wearable and the embedded secure element (eSE) component.

The scope of testing is dependent on whether the wearable product is or is not leveraging components from previously compliant inlay or secure element. Therefore, this section will be broken into three scenarios, (i) wearable product is not leveraging any component from a compliant product and (ii) wearable product is leveraging an embedded secure element (eSE) component.

Table B–3: Mobile Wearable Base Product Testing Requirements – without leveraging previously approved Mobile Secure Elements

#	Base Product Configuration	EMVCo Contactless Level 1	Cross Testing	VMPA	GP LOQ	EMVCo PCN	Visa Security Testing	Notes
1	Wearable with internal antenna & Embedded Secure Element (eSE)	EMVCo LOA	EMVCo LOA	Full	Yes	Yes	IAL/ Security testing	Wearable does not support Host-based Card Emulation (HCE).
2	Wearable only supporting HCE	EMVCo LOA	EMVCo LOA	None	No	No	See notes*	Wearable does not support an eSE. *Requires review of the design by Security team to define testing requirements.
3	Wearable supporting more than one execution environment(EE)	EMVCo LOA	Full on 1st EE and None of add'l EE	Full, for eSE	Yes	Yes	IAL/ Security testing	If eSE, see Section B.2.2 for the additional requirements for eSE component.

Table B–4: Mobile Wearable Base Product Testing Requirements – leveraging previously approved Secure Elements

#	Base Product Configuration	EMVCo Contactless Level 1	Cross Testing	VMPA	Notes
1	Wearable with internal antenna & Embedded Secure Element (eSE)	EMVCo LOA	EMVCo LOA	Transaction	Wearable does not support Host-based Card Emulation (HCE).
2	Wearable supporting more than one execution environment	EMVCo LOA	EMVCo LOA	Transaction if eSE supported else none.	-

B.2.3 Derivative Testing Requirements – Mobile Wearables

Multiple changes will result in the aggregation of each applicable test requirement for the changes.

Card emulation is defined as any level 1 PICC parameters defined in EMVCo Contactless Communication Protocol Specification - Book D, or any settings that include, but not limited to, NFC controller clock settings, or proximity payment antenna performance (NFC).

Product submissions comprising of a wearable and another component, such as an embedded secure element (eSE), are subject to the aggregated testing requirements for each component making up the product and all changes being made to those components.

Table 17: This table defines the acceptable changes for a Base Product to be eligible as a derivative. Visa recognizes EMVCo's certification process for Mobile Level 1 testing. The list below is not exhaustive but provides examples of commonly submitted change requests. If a Vendor wants to make a change that is not listed below, they should contact Approval Services to determine which process the Vendor may utilize.

Test requirements for the EMVCo Certification process for Mobile Level 1 can be found in Appendix A of the EMV Mobile Product Level 1 Type Approval. Vendors can obtain the latest version of the document at www.emvco.com

Table B–5: Derivative Testing Requirements – Mobile Wearable Matrix

#	Derivation	EMVCo equivalent REF	Cross Testing	VMPA	Compliance Letter	Notes
1	Wearable Size and/orShape Changes	CH11	None	None	Yes	Size and/or shape of the wearable changed and impacts the thickness or distance of antenna from surface. Testing dependent on details of changes.
2	Wearable Material Changes	CH11	None	Transaction	Yes	Materials (with metallic composition added) changed.
3	Wearable Material Changes	NA	None	None	No	Materials (with non-metallic composition added) changed.
4	Proximity Payment Antenna Changes (materials or design)	CH1	Full	Transaction	Yes	Driving electronics are identical to original antenna and no change of tuning.
5	Different Proximity Payment Antenna Manufacturer or Antenna Manufacturing Site	MIN05	None	None	No	Antenna materials and design are unchanged.
6	NFC Controller Firmware Change	CH4	None	Transaction	Yes	Card emulation affected. Digital Only
7	NFC Controller Firmware Change	CH2	None	Transaction	Yes	Card emulation affected. Analogue only

#	Derivation	EMVCo equivalent REF	Cross Testing	VMPA	Compliance Letter	Notes
8	NFC Controller Firmware Change	MIN02	None	Transaction	No	Card emulation not affected. Same vendor, identical NFC controller. Additional presentments of #7.
9	Wearable Software Change	CH5	None	Transaction	Yes	Card emulation affected or major OS version change. Impact to digital functionality only.
10	Wearable Software Change	New or Base product	None	Transaction	Yes	Card emulation affected or major OS version change. Impact to analogue and digital functionality. Treated as a base product
11	Wearable Software Change	MIN01	None	None	No	Card emulation not affected or not a major OS version change.
12	Change of Battery (materials or size)	CH8	Full	None	Yes	Proximity payment antenna not in battery.
13	Change of Battery (materials or size)	CH9	Full	None	Yes	Proximity payment antenna in battery. Treated as a base product.
14	Change of Battery (different capacity with no impact to battery dimensions)	Min03	None	None	No	-

#	Derivation	EMVCo equivalent REF	Cross Testing	VMPA	Compliance Letter	Notes
15	Contactless Level1 Specification Version	New or Base product	Full	Full	Yes	Treated as a base product.
16	Change of Execution Environment (addition of HCE)	CH15	NA	NA	NA	Contact Visa Ready. Wearable is already compliant for SE transactions. Requirements subject to change based on OS version.
17	Change of Execution Environment (addition of SE)	CH15	None	Transaction	Yes	Wearable is already compliant for Host-based Card Emulation (HCE). Secure Element is embedded and previously approved.

C Appendix C

C.1 Submission Requirements

The vendor is required to provide the items listed below for Visa functional testing. For GlobalPlatform testing submission requirements refer to the GlobalPlatform site. For EMVCo testing submission requirements refer to the EMVCo site.

Vendors submitting wearable products must contact Visa Ready. Visa retains all mobile samples. The samples could be retained up to 8 years after Approval date. After the retention period, Visa will contact the mobile provider determine if they would like the sample returned or securely destroyed.

Note: Visa reserves the right to conduct additional testing on any products that have gone through the testing and compliance process. The number of samples stated is the minimum required. Additional samples may be required or provided upon request.

Table C–6: Embedded Secure Element Component (Without a Handset)

Test Description	Labs	Form Factor	Number of Samples Required for Testing	Personalization Profile
GlobalPlatform Testing	External Lab	-	Refer to GlobalPlatform	Refer to GlobalPlatform
VMPA Testing including any extension	External Lab	Secure Elements (as a Dual Interface ID1)	10	Not Applicable
-	-	eSE circuit board	1 testing board with 5 eSE chips	-

To test the Embedded Secure Element (eSE) in contactless mode, it will be necessary to supply a form factor that permits Contactless Level 1 communication with the Secure Element and compatible with the test tools through a Test Tool Interface Application.

Table C–7: Wearable Product

Test Description	Labs	Number of Samples Required for Testing	Personalization Profile
Contactless Level 1 Testing: Analog Digital	External Lab	2	1 Type A with Mobile00 AND 1 Type B with Mobile00
VMPA Testing including any extension	External Lab	2 with TTIA	VMPA is pre-installed and personalized with Mobile00 on one, and Mobile30 on the other. The type (A, B and A &B) is not important for this test, so is left to vendor discretion.
Cross Testing/ Performance Testing	Visa Lab	2	Type A&B with Mobile00.