GLOBALPLATFORM®

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

GlobalPlatform Card
Composition Model
Security Guidelines for Basic Applications

Version 2.0

Public Release

November 2014

Document Reference: GPC_GUI_050

Contents

Tables

1 Introduction

GlobalPlatform Card Composition Model [Comp Model] defines a composition model for the evaluation of composite products. A composite product consists of an open platform, one or more Sensitive Applications, and optionally one or more Basic Applications.

A Sensitive Application is an application that requires formal security certification by an Evaluation Scheme such as Common Criteria or EMVCo.

A Basic Application is an application that is not required to be certified.

This document proposes a minimal set of guidelines for Basic Applications intended to mitigate potential security risks introduced by Basic Applications.

Note: ***Guidance for Sensitive Applications*** shall include the rules of this guide (as well as others specific to Sensitive Applications).

1.1 Audience

The guidelines in this document are intended for use by:

- **Platform Developers**
- **Product Issuers**, **Secure Element Issuers**, **Mobile Network Operators** (**MNOs**), and other entities that control a multi-application product
- **Application Developers**
- **Application Issuers**
- **Verification Authorities**
- **Evaluation Schemes** (initially Common Criteria and EMVCo)

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://www.globalplatform.org/specificationsipdisclaimers.asp. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

Documents denoted with a “[P]” following the specification names are typically freely accessible to the public. Documents denoted with an “[R]” may be under restricted distribution by the publishing entity, typically available to members of the publishing entity or by paying a fee.

Table 1-1: Normative References

Standard / Specification	Description	Ref
GlobalPlatform Card Composition Model [P]	GlobalPlatform Card Composition Model v1.1, June 2012	[Comp Model]

Standard / Specification	Description	Ref
Java Card [P]	Go to the following website for Java Card™ documentation:[1] http://www.oracle.com/technetwork/java/javacard/overview/index.html	[Java Card]
Life Cycle for GlobalPlatform Products [P]	GlobalPlatform Card – Overview of Complete Life Cycle for GlobalPlatform Products v1.0, November 2014	[Life Cycle]

Table 1-2: Informative References

Standard / Specification	Description	Ref
Java Card System Open Configuration Protection Profile [P]	Java Card™ System – Open Configuration Protection Profile, Version 2.6, 19 April 2010, Certificate: ANSSI-CC-PP-2010/03. Java Card Protection Profile for Java Card Classic platforms in an open configuration.	[JCS OCPP]
Java Card Off-Card Byte Code Verifier [P]	Java Card™ 2.2 Off-Card Verifier, White Paper, Sun Microsystems v1.0, June 2002	[JC OCV]
JIL Application of Attack Potential to Smartcards [P]	Common Criteria Supporting Document: Application of Attack Potential to Smartcards, Version 2.8 (CCDB-2012-04-002, v2.8)	[JIL]
EMVCo Security Evaluation Process [P]	EMV Security Guidelines (EMVCo Security Evaluation Process) v4.0, December 2010	[E Sec Gd]
EMVCo Approvals & Certification Process Updates [P]	All process update bulletins, including: Bulletin nº6, ICCN and PCN Product Renewal Policy Update, November 2011 Bulletin nº5, Platform Evaluation & Process update, Bulletin nº3, EMVCo – Evaluation review fees Bulletin nº2, EMVCo – Product renewal and reuse of evaluation evidence Bulletin nº9, Platform Security Guidance Update	[E Bulletins]
EMVCo CPA Secure Implementation Guidelines [R]	EMVCo CPA Secure Implementation Guidelines, Version 1, January 2007	[E CPA Impl]
EMVCo Java Card & GlobalPlatform Guidelines [R]	EMVCo Security Guidelines for Java Card & Global Platform Implementations including Mobile Payments	[E JC GP]

[1] Java Card is a trademark of Oracle and/or its affiliates.

Standard / Specification	Description	Ref
Common Criteria for Information Technology Security Evaluation [P]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Re-published as an ISO Standard; see ISO 15408. Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012	[ISO 15408]
Common Criteria Composite Evaluation [P]	Common Criteria Supporting Document: Composite Product Evaluation for Smart Cards and Similar Devices, Version 1.2, April 2012	[CC CEval]
Common Criteria Statement on Reuse of Evaluation Results and Evidence [P]	Common Criteria Supporting Document: Information Statement on Reuse of Evaluation Results and Evidence, 26 October 2002 (2002-08-009-002)	[CC Reuse]
Common Criteria ETR for Composition [P]	Common Criteria Supporting Document: ETR template for composite evaluation of Smart Cards and similar devices, Version 1.0, Revision 1, September 2007 (CCDB-2007-09-002)	[CC ETR]

1.4 Terminology and Definitions

Table 1-3: Terminology and Definitions

Term	Definition
Application	A Java Card applet and related libraries intended to be executed on top of a platform.
Application Developer	An entity responsible for development of an application. This entity may also be the Application Issuer.
Application Issuer	An entity responsible for the security of an application.
Basic Application	A Java Card Application: • that does not have a negative impact on the certification status of the product onto which it will be loaded, • that should have been verified to meet a set of basic security rules, and • that therefore may reside on a card along with one or more Sensitive Applications.
Certificate	Formal document issued by an Evaluation Scheme acknowledging that a component or product has demonstrated sufficient assurance of security; the outcome of a successful evaluation.
Certification	Validation that the results of an evaluation meet the required assurance level.
Certified Platform	A platform that has achieved a Security Certification (that is, that has been issued a security certificate) by an Evaluation Scheme.

Term	Definition
Common Criteria	The Common Criteria for Information Technology Security Evaluation and the companion Common Methodology for Information Technology Security Evaluation are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that: • Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance. • Supporting documents are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies. • The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation. All the signatories of the CCRA recognize these certificates.
Common Criteria (CC) Certification	IT security certification as described in Common Criteria for Information Technology Security Evaluation, also known as ISO 15408 [ISO 15408].
Composite Product	A Secure Element that consists of an Open Platform and one or more applications. See also *GlobalPlatform Composite Product*.
Composition	See *GlobalPlatform Composition*.
Composition Model	See *GlobalPlatform Composition Model*.
EMVCo	The entity that manages, maintains, and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, extending to new payment devices as well, such as contactless and mobile payment.[2] EMVCo acts as the security certification entity for Integrated Circuit (IC), Platform and IC Card (ICC) payment products. EMVCo is currently owned by American Express, Discover, JCB, MasterCard, UnionPay, and Visa.
EMVCo Certification	The EMVCo confirmation that a product successfully completed the EMVCo security evaluation process and has been issued a Certificate with a Certificate Number.
ETR for Composition	An Evaluation Technical Report (ETR) to be exchanged between laboratories, summarizing the evaluation results and providing recommendations for possible future compositions (see Common Criteria ETR for Composition [CC ETR]).
Evaluation	The process of verifying that an IT product satisfies a given set of requirements based on a well-established methodology. In the context of this document, the IT product is a Secure Element or part of it and the evaluation methodology is used for a security evaluation.

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

Term	Definition
Evaluation Scheme	An organization or network of organizations (Certification Body) that oversees the security evaluation process and issues certificates for products or product components that have demonstrated sufficient assurance of security.
GlobalPlatform Composite Product	A Composite Product for which certification has been obtained using the GlobalPlatform Composition Model.
GlobalPlatform Composite Product Issuer	An entity that issues a GlobalPlatform Composite Product and is responsible for the security of the product during the entire product life cycle.
GlobalPlatform Composition	A process to combine applications and Certified Platforms which results in a Composite Product.
GlobalPlatform Composition Model	A model for the evaluation of GlobalPlatform Composite Products, described in [Comp Model].
Guidance for Sensitive Applications	A set of rules and recommendations designed to ensure the secure usage of the platform by a Sensitive Application; an output of the Platform Certification step described in [Life Cycle].
Java Card	A technology that allows Java-based applications (applets) to be run securely on smart cards and similar small memory footprint devices.
Multi-Application Product	A product consisting of a platform and two or more Basic and/or Sensitive Applications.
Open Platform	A Platform is the collective name for the integrated circuit (IC) hardware with its dedicated software, Operating System (OS), Run Time Environment (RTE) and Platform environment on which one or more applications can be executed. An open platform allows the addition, deletion, or modification of applications.
Original Platform	A platform on which an application has been certified. This term is used in the context of describing the *portability* of an application from this *original platform* to a *target platform*.
Platform	The integrated circuit (IC) hardware with its dedicated software, Operating System (OS), Run Time Environment (RTE), and Platform environment, on which one or more applications can be executed.
Platform Developer	The entity responsible for the development of a platform. This entity may also sponsor the platform evaluation.
Platform Security Guidance	A set of rules and recommendations for the secure usage of the platform by an application. In Common Criteria, these rules and recommendations are identified as Operational User Guidance (AGD_OPE) in [ISO 15408].
Portability	The ability of an application to run on multiple platforms.
Product Issuer	See *GlobalPlatform Composite Product Issuer*.
Scheme	See *Evaluation Scheme*.

Term	Definition
Secure Element	A tamper resistant component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models. Such a Secure Element may exist in any form factor such as UICC, embedded SE, smartSD, smart microSD, etc.
Security Certification	Certification based on security rules and recommendations that are defined by the certification scheme (e.g. EMVCo or CC schemes).
Security Guidance	See *Platform Security Guidance.*
Sensitive Application	A Java Card application that requires formal Security Certification by an Evaluation Scheme such as Common Criteria or EMVCo.
Target Platform	A platform receiving a new application as part of a GlobalPlatform Composition. See also *Original Platform.*
Verification Authority	An entity that checks that all required certifications are current for Sensitive applications and that Basic Applications have been appropriately Validated and manages the storage of the downloadable format.

1.5 Abbreviations and Notations

Table 1-4: Abbreviations

Abbreviation	Meaning
AGD	Guidance Documents (Common Criteria)
CAP	Converted Applet
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CPA	Common Payment Application (EMVCo)
CVM	Cardholder Verification Method
ETR	Evaluation Technical Report
ICAO	International Civil Aviation Organization
IT	Information Technology
JIL	Joint Interpretation Library (of the JIWG in the European CC Scheme)
JIWG	Joint Interpretation Working Group
MNO	Mobile Network Operator. Also referred to as Carrier.
SIM	Subscriber Identity Module
UICC	Universal Integrated Circuit Card

1.6 Revision History

Table 1-5: Revision History

Date	Version	Description
June 2012	1.0	Public Release
November 2014	2.0	Removed classification of rules as mandatory or recommended. Eliminated selected rules based on feedback.

2 Scope and Considerations

2.1 Scope

The guidelines defined in this document apply to any Basic Application that is to be loaded on a Composite Product that has been certified by an Evaluation Scheme (in the current version of the GlobalPlatform Composition Model, either Common Criteria or EMVCo). Any Java Card with GlobalPlatform technology is within the scope of this document, including SIM cards, payment cards, and identity cards.

This document formulates general guidelines. Application and platform specific guidelines may exist in addition to the guidelines in this document (defined by, e.g., ICAO or EMVCo).

2.1.1 Objective

The objective of this document is to define industry best practices that Basic Applications should meet in order to demonstrate that they are safe to be downloaded on a certified product. This will allow vendors to re-use test results and evaluation reports to avoid duplication of effort and cost. It will also reduce redundancies and inconsistencies in security testing.

Therefore, this document provides a set of guidelines for use by:

- **Platform Developers** – who need to ensure that the Platform Security Guidance documents that they develop for Basic Applications and for Sensitive Applications meet these guidelines
- **Product Issuers**, **Secure Element Issuers**, **Mobile Network Operators** (**MNOs**), and other entities that control a multi-application product – who need to ensure that loading a Basic Application will not impact the existing certification of a card
- **Application Developers** – who need to ensure that the applications they develop respect the certification requirements of the targeted platform products
- **Application Issuers** – who need to ensure that the applications they support comply with these guidelines
- **Verification Authorities** – who will verify that a Basic Application complies with these guidelines
- **Evaluation Schemes** (initially Common Criteria and EMVCo) – who may use this document to identify limitations on the Basic Applications that may be loaded with the Sensitive Applications that they evaluate

The main intent of this document is to provide sufficient and enough guidelines for basic application development. Unfortunately today, the platform may require that Basic Applications be checked against additional rules before loading.

For a specific product, the application developer may request the Platform Security Guidance documents, if they exist for the Basic Application being developed. These documents are generally available only under NDA.

2.1.2 Exclusions

This document:

- Does not provide guidelines for the platform or for any native code that may be part of the Java Card platform.
- Does not address administration of the card.
- Does not discuss details of the validation process to determine whether a Basic Application follows the guidelines provided. For information, see [Comp Model].

2.2 Considerations

As described in [Comp Model], validation of a Basic Application is split into activities related to the certificate of the platform and activities that are common to all platforms. The purpose of the validation is to ensure that a Basic Application does not negatively impact the security of a platform or of a Sensitive Application on a platform.

The guidelines in this document are selected to aid in the common activities of the validation process. By following these guidelines, a Basic Application should already provide a reasonable assurance that it will not pose a security risk to a Sensitive Application, even before considering the security features provided by the platform.

It is assumed that the target platform is a Certified Platform and provides an implementation compliant to the Java Card specifications from Oracle [Java Card].

Basic Applications may consist of applet code, library code, or both. The guidelines should be applied to both applet and library code.

3 Guidelines

This chapter contains the guidelines for Basic Applications. Each rule contains a rationale and the suggested inputs for validation of the rule.

- A Basic Application that fails to meet a rule presents a potential risk for the security of the product. This risk has to be managed by the Product Issuer, which may decide after further analysis that the application may be loaded.

Inputs

The discussion of each rule identifies the inputs required to verify that the Basic Application meets the rule. The total list of inputs required by the guidelines in this chapter is as follows:

- The export files of the target platform
- The CAP file of the Basic Application
- The export file of the Basic Application

3.1 Development

3.1.1 Shared Resources

Rule	If the Basic Application uses shared libraries: • The major version of the shared library found on the target platform shall be equal to the major version number of the library that has been used for generation of the CAP file for the Basic Application. • The minor version of the shared library found on the target platform shall be equal to or higher than the minor version number of the library that has been used for generation of the CAP file for the Basic Application.
Rationale	Using older versions of the shared libraries may introduce incompatibility and security issues.
Input	CAP file and export files of the target platform

3.1.2 Versioning

Rule	When the Basic Application provides a shared library, the versioning policy shall be: • At least the minor version changes if there are changes to the implementation of the exported methods. • If the signature of a method changes, the major version shall be incremented.
Rationale	Changes to the shared libraries may introduce incompatibility and security issues.
Input	CAP file and export file of the Basic Application

3.1.3 PIN Usage

Rule	A Basic Application shall not provide any command using GlobalPlatform CVM functions. It shall not offer the ability to unblock the CVM, reset the CVM try counter, or change the CVM value.
Rationale	To prevent the Basic Application from causing misuse of the GlobalPlatform CVM.
Input	CAP file of the Basic Application

3.2 Conversion and Packaging

The conversion and packaging phase of the Basic Application takes the binary output of the development phase and converts it into a format suitable for loading onto the target platform. This phase includes bytecode verification procedures, adding signatures, and defining operational parameters for deployment.

3.2.1 Bytecode Verification Tools

Rule	A Basic Application shall be compliant with the Java Card specifications and shall **successfully pass** bytecode verification using tools from Oracle or from the Platform Developer of the target platform. The tools used for bytecode verifications shall be the latest version available.
Rationale	To ensure that the Basic Application complies with Java Card specifications (structural constraints and type constraints). Having to pass the **latest** bytecode verification process by Oracle or the Platform Developer limits the impact of bugs in earlier versions of the bytecode verifier.
Input	CAP file of the Basic Application Export files of the targeted platform