Reference: 2020-37-INF-3429- v1
Target: Público
Date: 18.03.2021

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2020-37**
TOE	**Secure Element Protection Profile - GPC_SPE_174, version 1.0**
Applicant	**9865186 - GlobalPlatform, Inc.**

References

[EXT-6150] Certification Request

[EXT-6546] Evaluation Technical Report

Certification report of the Protection Profile Secure Element Protection Profile - GPC_SPE_174, version 1.0, as requested in [EXT-6150] dated 22/07/2020, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-6546] received on 17/02/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the Protection Profile Secure Element Protection Profile - GPC_SPE_174, version 1.0.

A Protection Profile (PP) defines an implementation-independent set of IT security requirements for a category of products, which are intended to meet common consumer needs for IT security. Product certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued but the results from a PP certification can be re-used for the Security Target evaluation within a product evaluation when conformance to the PP has been claimed.

Developer/manufacturer: GlobalPlatform, Inc.

Sponsor: GlobalPlatform, Inc.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Assurance Package claimed in the PP: Common Criteria v3.1 R5 Part 3 conformant
EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5.

Evaluation end date: 19/02/2021.

Expiration Date[1]: 18/03/2031.

All the assurance components APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1 and APE_REQ.2 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied as defined by the Common Criteria v3.1 R5 and the Common Evaluation Methodology v3.1 R5. The Assurance Package claimed in the Protection Profile is Common Criteria v3.1 R5 Part 3 conformant EAL 4 augmented by ALC_DVS.2 Sufficiency of security measures and AVA_VAN.5 Advanced methodical vulnerability analysis.

Considering the obtained evidences during the instruction of the certification request of the Protection Profile Secure Element Protection Profile - GPC_SPE_174, version 1.0, a positive resolution is proposed.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

PROTECTION PROFILE SUMMARY

Secure Element Protection Profile - GPC_SPE_174, version 1.0 defines a mandatory core Protection Profile (PP), and optional functional packages and PP-Modules for Secure Elements (SEs) implementing Java Card specifications [JCVM], [JCAPI], [JCRE] and GlobalPlatform Card Specification with Amendments [GPCS et al.]. Typical SE form factors include smartcards, eUICCs, and eSEs.

The mandatory core PP defines the security problem, objectives, and requirements for SEs by extending the Java Card PP [PP-JC] to address the security functionality defined in [GPCS et al.]. This includes:

- Card and application life cycle management
- Privileges Management
- Trusted Framework
- Secure communication covering all Secure Channel Protocols (SCPs).

The six optional functional packages defined in chapters 8 to 13 of the Protection Profile address the following GlobalPlatform privileges assigned to the Security Domains (SDs) or Applications in the card to permit changes to the card content:

- Ciphered Load File Data Block
- Global Services
- Cardholder Verification Method (CVM)
- Delegated Management
- DAP Verification
- Mandated DAP Verification.

GlobalPlatform Amendments B, D, E, F, and G are addressed as part of the core PP. Additionally, four optional PP-Modules are defined in chapters 14 to 17 of the Protection Profile to cover Confidential Card Content Management [Amd A], Contactless Services [Amd C], Executable Load File Upgrade [Amd H], and Secure Element Management Service [Amd I]. The Contactless Activation and Contactless Self Activation privileges are covered within the PP-Module for Contactless Services. A fifth PP-Module defined in chapter 18 addresses the post-issuance OS update capability.

The SE evaluation may be performed as a composite evaluation [CC-Comp] on top of a certified IC compliant with [PP-0084] or on top of a certified Java Card System compliant with [PP-JC].

The allowed SE PP-Configurations consist of the core PP with any of the packages and any subset of PP-Modules. The SE PP section 2.8 provides instructions for selecting the appropriate packages and PP-Modules depending on the implemented GlobalPlatform privileges and amendments.

SECURITY ASSURANCE REQUIREMENTS

The Protection Profile was evaluated with all the evidence required to fulfil the following assurance components according to Common Criteria v3.1 R5:

- APE_INT.1 PP introduction
- APE_CCL.1 Conformance claims
- APE_SPD.1 Security problem definition
- APE_OBJ.2 Security objectives
- APE_ECD.1 Extended components definition
- APE_REQ.2 Derived security requirements

SECURITY FUNCTIONAL REQUIREMENTS

Secure Element Protection Profile - GPC_SPE_174, version 1.0 provides the set of Security Functional Requirements (SFRs) the TOE to be certified has to enforce in order to fulfil the security objectives. One group of SFRs covers the Java Card System and comes from [PP-JC] (see section 7.1.1 of PP), while the other group of SFRs is added and covers GlobalPlatform Card Specification with Amendments [GPCS et al] and OS update (see section 7.1.2 for the core PP, sections 8.4, 9.4, 10.4, 11.4 and 12.4 for the optional packages and sections 14.4, 15.4, 16.4, 17.4 and 18.4 for the optional PP-Modules)..

IDENTIFICATION

Protection Profile Identification: Secure Element Protection Profile - GPC_SPE_174, version 1.0

Evaluation Level: Common Criteria v3.1 R5 assurance components APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1 and APE_REQ.2.

Assurance Package claimed in the PP: Common Criteria v3.1 R5 Part 3 conformant

EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5.

SECURITY POLICIES

The Secure Element Protection Profile - GPC_SPE_174, version 1.0 defines a set of security policies assuring the fulfilment of different standards and security demands. The detail of these policies is documented in section 4.4 Organisational Security Policies (OSP) for the core the Protection Profile, sections 8.2, 11.2 and 12.2for the optional packages for the PP and sections 14.2, 16.2 and 18.2 for the optional PP-Modules defined.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The Secure Element Protection Profile - GPC_SPE_174, version 1.0 section 4.5 Assumptions defines the assumptions and constraints to the conditions used to assure the security properties and functionalities compiled by the TOEs compliant to the core PP. Functional packages do not add any assumption, and PP-Modules added assumptions are defined in 17.2 and 18.2. These assumptions shall be applied during the evaluation of TOE compliant with this PP in order to determine if the identified vulnerabilities are applicable and can be exploited.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not constitute a riskfor the TOEs compliant with Secure Element Protection Profile - GPC_SPE_174, version 1.0, although the agents implementing attacks have a high attack potential according to AVA_VAN.5 assurance component and provided the usage assumptions and the organisational security policies are fulfilled.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the core Protection Profile are defined in section 4.3 Threats and sections 8.2, 10.2 and 11.2 for the optional packages for the PP and sections 15.2, 16.2, 17.2 and 18.2 for the optional PP modules defined.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The TOEs compliant with Secure Element Protection Profile - GPC_SPE_174, version 1.0 require the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are defined in section 5.2 Security Objectives for the Operational Environment for the core PP and sections 8.3, 11.3 and 12.3 for the optional packages for the PP and sections 17.3 and 18.3 for the optional PP modules defined.

EVALUATION RESULTS

The product Secure Element Protection Profile - GPC_SPE_174, version 1.0 has been evaluated against the Common Criteria v3.1 R5 and the Common Evaluation Methodology v3.1 R5.

All the assurance components required by the evaluation level APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1 and APE_REQ.2 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1 and APE_REQ.2, as defined by the Common Criteria v3.1 R5 and the Common Evaluation Methodology v3.1 R5.

The Assurance Package claimed in the Protection Profile is Common Criteria v3.1 R5 Part 3 conformant EAL 4 augmented by ALC_DVS.2 Sufficiency of security measures and AVA_VAN.5 Advanced methodical vulnerability analysis.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the usage of the Protection Profile are provided. These have been collected along the evaluation process and are detailed to be considered when using the PP.

- For sake of modularity, this PP has extracted different optional features as independent Packages and PP-Modules. It is expected that ST writers will include combinations between different packages and PP-Modules depending on the functionalities implemented by the future TOE.
- The PP-Configuration consisting of the core SE PP, all the PP-Modules and all the packages has been evaluated as a single PP using APE assurance family, which in this context is equivalent to ACE. Moreover, no dependency was observed between PP-Modules and/or packages, which imply that the evaluation results apply to all the PP-Configurations composed of the core SE PP and a subset of the PP-Modules and packages.
- The evaluation team makes the following security recommendations:
    - The user of the PP has to carefully follow the recommendations of supported cryptographic algorithms as defined in [GP Crypto] and [SOGIS_ACM]. Note that according to [GP Crypto], Legacy use algorithms are valid of until 2023 and that they should not be used for any new products/specifications (even though some products may already be in the market).

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of Secure Element Protection Profile - GPC_SPE_174, version 1.0, a positive resolution is proposed.

The certifier provides the following recommendations:

- A user of the PP shall carefully consider and apply all Application Notes included in the PP.
- PP consumers should observe the recommendations provided in Table 2-1 of section 2.3.2 Secure Communication Management and Protocols of the PP when selecting the Secure Channel Protocols and the cryptographic algorithms in the elaboration of the Security Target.
- A cryptographic assessment was not part of the PP evaluation. Neither the strength nor the suitability for use in a distinct TOE has been evaluated. When writing a Security Target

claiming conformance to this PP, the author shall chose cryptographically strong algorithms and operation modes.

- PP consumers should observe the instructions for ST Authors in section 2.8 of the PP and wants to remark that the ST shall conform to the core PP and optionally the ST shall identify all the claimed functional packages and PP-Modules.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
eSE	Embedded Secure Element
ETR	Evaluation Technical Report
eUICC	Embedded Universal Integrated Circuit Card
OC	Organismo de Certificación
SE	Secure Element
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[SOGIS_ACM] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, version 1.2. January 2020. SOG-IS Crypto Working Group.

[CC-Comp] Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018. Joint Interpretation Library.

[JCAPI] Application Programming Interface, Java Card™ Platform, versions 2.2 through 3.1.

[JCVM] Virtual Machine Specification, Java Card™ Platform, versions 2.2 through 3.1.

[JCRE] Runtime Environment Specification, Java Card™ Platform, versions 2.2 through 3.1.

[GPCS et al.] GlobalPlatform Card Specification and Amendments: [GPCS], [Amd A], [Amd B] , [Amd C] , [Amd D] , [Amd E] , [Amd F] , [Amd G] , [Amd H] and [Amd I]

[GPCS] GlobalPlatform Technology Card Specification v2.3.1, March 2018. Document Reference: GPC_SPE_034

[Amd A] GlobalPlatform Card

Confidential Card Content Management

Card Specification v2.3 – Amendment A v1.2 or latest applicable version

Document Reference: GPC_SPE_007

[Amd B] GlobalPlatform Card

Remote Application Management over HTTP

Card Specification v2.2 – Amendment B v1.1.3 or latest applicable version

Document Reference: GPC_SPE_011

[Amd C] GlobalPlatform Card Technology

Contactless Services

Card Specification v2.3 – Amendment C v1.3 or latest applicable version

Document Reference: GPC_SPE_025

[Amd D] GlobalPlatform Card Technology

Secure Channel Protocol '03'

Card Specification v2.3 – Amendment D v1.2 or latest applicable version

Document Reference: GPC_SPE_014

[Amd E] GlobalPlatform Card Technology

Security Upgrade for Card Content Management Card Specification v2.3 – Amendment E v1.1 or latest applicable version

Document Reference: GPC_SPE_042

[Amd F] GlobalPlatform Card

Secure Channel Protocol '11'

Card Specification v2.3 – Amendment F v1.2.1 or latest applicable version

Document Reference: GPC_SPE_093

[Amd G] GlobalPlatform

Opacity Secure Channel

Card Specification v2.3 – Amendment G v1.0 or latest applicable version

Document Reference: GPC_SPE_106

[Amd H] GlobalPlatform Card

Executable Load File Upgrade

Card Specification v2.3 – Amendment H v1.1 or latest applicable version

Document Reference: GPC_SPE_120

[Amd I] GlobalPlatform Technology

Secure Element Management Service

Card Specification v2.3 – Amendment I v1.0 or latest applicable version

Document Reference: GPC_SPE_121

[GP Crypto] GlobalPlatform Technology Cryptographic Algorithm Recommendations v1.0 or latest applicable version

Document Reference: GP_TEN_053

[PP-JC] BSI-CC-PP-0099-V2-2020 – Java Card System - Open Configuration Protection Profile Version 3.1, April 2020

[PP-0084] BSI-CC-PP-0084-2014 - Security IC Platform Protection Profile, Rev 1.0, 13 January 2014

PROTECTION PROFILE DOCUMENT

Along with this certification report, the complete Protection Profile is available in the Certification Body:

- Secure Element Protection Profile - GPC_SPE_174, version 1.0. 17 February 2021. GlobalPlatform, Inc.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this Protection Profile is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this Protection Profile is recognized under CCRA for all assurance components.