Reference: 2024-50-INF-4652- v1
Target: Limitada al expediente
Date: 09.03.2026

Created by: I008
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-50**
TOE	**Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0**
Applicant	**9865186 - GlobalPlatform, Inc.**
References	

[EXT-9325] Solicitud de certificación

[EXT-9760] 2025-08-11_2024-50_ETR_vM1

Certification report of the product Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0, as requested in [EXT-9325] dated 04/10/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9760] received on 11/08/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0.

A Protection Profile (PP) / a PP-Configuration 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) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Assurance Package claimed in the PP: CC:2022 Release 1 conformant EAL 4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5.

Evaluation end date: 31/10/2025

Expiration Date[1]: 21/12/2030

All the assurance components APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, APE_REQ.2, ACE_INT.1, ACE_CCL.1, ACE_SPD.1, ACE_OBJ.2, ACE_ECD.1, ACE_REQ.2, ACE_MCO.1 and ACE_CCO.1 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 CC:2022 Revision 1 and the CEM:2022 Revision 1. The Assurance Package claimed in the PP and PP-Configuration is CC:2022 Revision 1 conformant EAL 4 augmented by ALC_DVS.2 Sufficiency of security measures, ALC_FLR.2 Flaw remediation procedures 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 and extensions (Functional packages, PP-

[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.

Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0, a positive resolution is proposed.

SUMMARY

The Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0 defines the Secure Element Protection Profile (SE PP), the SE PP-Modules and the SE PP-Configurations for Secure Elements (SEs) implementing Java Card specifications [JCVM], [JCAPI], [JCRE] and GlobalPlatform Card Specification with selected Amendments [GPCS & Amds]. SE form factors include smartcards, eUICCs, and eSEs.

The SE PP extends the security problem, security objectives and security requirements defined in [PP-JC]. It is structured in two parts: a core, called the “core SE PP” in the rest of the document, and six optional functional packages. The identification, the TOE overview and the conformance claims of the SE PP are defined in section 1.1 and chapters 2 and 3, respectively.

Chapters 4 to 6 define the “core SE PP”, which addresses the security functionality defined in the Card Specification [GPCS] and in the amendments Remote Application Management over HTTP [Amd B], Secure Channel Protocol '03' [Amd D], Secure Channel Protocol '11' [Amd F], and Opacity Secure Channel [Amd G].

In addition to the functionality already available in the Java Card PP, the SE PP offers:

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

Chapters 7 to 12 define functional packages, which address the GlobalPlatform privileges that can optionally be assigned to Security Domains (SDs) and Applications to permit changes to the card content:

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

The SE PP-Modules defined in Chapters 13 to 16 address additional optional functionality: 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. Chapter 17 defines the SE PP-Module addressing the (post-issuance) OS update capability.

Chapter 18 defines the allowed SE PP-Configurations, which consist of the SE PP and any subset of PP-Modules. The SE PP, PP-Modules and PP-Configurations claim conformance to the same assurance level, i.e. EAL 4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5.

The SE PP and PP-Configurations constitute the reference for the evaluation of GlobalPlatform-enabled Java Card SEs. An SE evaluation conforming to the SE PP or to an SE PP-Configuration should be performed as a composite evaluation [CC-Comp] using the COMP assurance package defined in [CC5], where the base component is either a certified IC, a certified 3S in SoC or a certified Java Card Platform, conforming to [PP-0084], [PP-0117] or [PP-JC], respectively.

The SE PP, PP-Modules and PP-Configurations have been developed in the framework of the GlobalPlatform SE Security Working Group.

SECURITY ASSURANCE REQUIREMENTS

The PP and PP-Configuration was evaluated with all the evidence required to fulfil the following assurance components according to CC:2022 Revision 1:

- 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 Security requirements
- ACE_INT.1 PP-Module introduction
- ACE_CCL.1 PP-Module conformance claims
- ACE_SPD.1 PP-Module Security problem definition
- ACE_OBJ.2 PP-Module Security objectives
- ACE_ECD.1 PP-Module extended components definition
- ACE_REQ.2 PP-Module security requirements
- ACE_MCO.1 PP-Module consistency
- ACE_CCO.1 PP-Configuration consistency

SECURITY FUNCTIONAL REQUIREMENTS

Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0 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 6.1.1 of PP), while the other group of SFRs is added and covers GlobalPlatform Card Specification with Amendments [GPCS & Amds] and OS update (see section 6.1.2 for the core PP, sections 7.4, 8.4, 9.4, 10.4, 11.4 and 12.4 for the functional packages and sections 13.5, 14.5, 15.5, 16.5 and 17.5 for the PP-Modules).

IDENTIFICATION

Protection Profile Identification: Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0

SE PP Functional Packages:

- Functional Package for 'Ciphered Load File Data Block (CLFDB)'
- Functional Package for 'Global Services (GS)'
- Functional Package for 'Cardholder Verification Method (CVM)'
- Functional Package for 'Delegated Management (DM)'
- Functional Package for 'DAP Verification (DAP)'
- Functional Package for 'Mandated DAP Verification (MDAP)'

SE PP-Modules

- PP-Module for 'Amendment A: Confidential Card Content Management (CCCM)',
- PP-Module for 'Amendment C: Contactless Services (CTL)'
- PP-Module for 'Amendment H: Executable Load File Upgrade (ELFU)'
- PP-Module for 'Amendment I: Secure Element Management Services (SEMS)'
- PP-Module for 'OS Update'

SE PP-Configurations

- Master SE PP-Configuration, ref. GPC_SPE_174[194.195.196.197.198]
- Subset SE PP-Configuration, ref. GPC_SPE_174[x1...xn] (where n is the number of components of the PP-Configuration, xi belongs to {194,195,196,197,198}, and xi is different from xj for any i and j).

Evaluation Level: CC:2022 Revision 1 assurance components APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, APE_REQ.2, ACE_INT.1, ACE_CCL.1, ACE_SPD.1, ACE_OBJ.2, ACE_ECD.1, ACE_REQ.2, ACE_MCO.1 and ACE_CCO.1.

Assurance Package claimed in the PP: CC:2022 Release 1 conformant EAL 4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5.

SECURITY POLICIES

The Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0 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 PP, sections 7.2, 10.2, 11.2 and 12.2 for the functional packages for the PP and sections 13.3, 15.3 and 17.3 for the PP-Modules defined.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0 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 16.3 and 17.3. These assumptions shall be applied during the evaluation of TOEs 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 suppose a risk for the product Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0, although the agents implementing attacks have the attack potential according to the AVA_VAN.5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

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, sections 7.2, 9.2, 10.2, 11.2 and 12.2 for the functional packages for the PP and sections 14.3, 15.3, 16.3 and 17.3 for the PP-Modules defined.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The TOEs compliant with Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0 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 SE PP, sections 7.3, 10.3, 11.3 and 12.3 for the functional packages for the PP and sections 16.4 and 17.4 for the PP-modules defined.

EVALUATION RESULTS

The Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0 has been evaluated against the CC:2022 Revision 1 and the CEM:2022 Revision 1.

All the assurance components APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, APE_REQ.2, ACE_INT.1, ACE_CCL.1, ACE_SPD.1, ACE_OBJ.2, ACE_ECD.1, ACE_REQ.2, ACE_MCO.1 and ACE_CCO.1 have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation as defined by the CC:2022 Revision 1 and the CEM:2022 Revision 1.

The Assurance Package claimed in the PP and PP-Configuration is CC:2022 Revision 1 conformant EAL 4 augmented by ALC_DVS.2 Sufficiency of security measures, ALC_FLR.2 Flaw remediation procedures and AVA_VAN.5 Advanced methodical vulnerability analysis.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Secure Element Protection Profile and extensions (Functional packages, PP-Modules and PP-Configurations) (SE PP) - GPC_SPE_174, version 2.0, a positive resolution is proposed.

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 protection profile:

[JCAPI] Application Programming Interface, Java Card™ Platform, version 3.2, Oldest Accepted Version:2.2

[JCVM] Virtual Machine Specification, Java Card™ Platform, version 3.2, Oldest Accepted Version:2.2

[JCRE] Runtime Environment Specification, Java Card™ Platform, version 3.2, Oldest Accepted Version:2.2

[GPCS & Amds] The following GlobalPlatform Technology specifications:

[GPCS] Card Specification

[Amd A] Confidential Card Content Management

[Amd B] Remote Application Management over HTTP

[Amd C] Contactless Services

[Amd D] Secure Channel Protocol '03'

[Amd F] Secure Channel Protocol '11'

[Amd G] Opacity Secure Channel

[Amd H] Executable Load File Upgrade

[Amd I] Secure Element Management Service

[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, Document Reference: GPC_SPE_007

[Amd B] GlobalPlatform Card Remote Application Management over HTTP Card Specification v2.3.1 – Amendment B v1.2, Oldest Accepted Version: Amendment B v1.1.3, Document

Reference: GPC_SPE_011

[Amd C] GlobalPlatform Card Technology Contactless Services Card Specification v2.3 – Amendment C v1.3, Document Reference: GPC_SPE_025

[Amd D] GlobalPlatform Card Technology Secure Channel Protocol '03' Card Specification v2.3 – Amendment D v1.2, Document Reference: GPC_SPE_014

[Amd F] GlobalPlatform Card Secure Channel Protocol '11' Card Specification v2.3.1 – Amendment F v1.4, Oldest Accepted Version: Amendment F v1.2.1, Document Reference: GPC_SPE_093

[Amd G] GlobalPlatform Opacity Secure Channel Card Specification v2.3 – Amendment G v1.0, Document Reference: GPC_SPE_106

[Amd H] GlobalPlatform Card Executable Load File Upgrade Card Specification v2.3 – Amendment H v1.1, Document Reference: GPC_SPE_120

[Amd I] GlobalPlatform Technology Secure Element Management Service Card Specification v2.3.1 – Amendment I v1.1, Oldest Accepted Version: Amendment I v1.0, Document Reference: GPC_SPE_121

[PP-JC] BSI-CC-PP-0099-V3-2024 – Java Card System – Open Configuration Protection Profile Version 3.2, July 2024

[PP-0084] Security IC Platform Protection Profile, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014

[PP-0117] Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0117-V2-2022, Version 1.8, 23 October 2023

[CC:2022] Common Criteria for information Technology Security Evaluation, Parts 1 to 5, CC:2022 Revision 1, November 2022

[CC1] Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model,CC:2022 Revision 1, November 2022, reference CCMB-2022-11-001

[CC2] Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements, CC:2022 Revision 1 Part 2 November 2022, reference CCMB-2022-11-002

[CC3] Common Criteria for information Technology Security Evaluation, Part 3: Security assurance components, CC:2022 Revision 1, November 2022, reference CCMB- 2022-11-003

[CC5] Common Criteria for information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC:2022 Revision 1, November 2022, reference

CCMB-2022-11-005

[CEM] Common Evaluation Methodology, CEM:2022 Revision 1, November 2022, reference CCMB-2022-11-006

[CC-Comp] Composite product evaluation and certification, version 1.6, April 2024

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.eu.

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

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 recognized under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components selected.