Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 7/18

(Certification No.)

Prodotto: **ASapp-QSCD (OSB) v1.0**
(Product)

Sviluppato da: **HID Global**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_DVS.2, AVA_VAN.5)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 24 luglio 2018

Common Criteria

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

ASapp-QSCD (OSB) v1.0

OCSI/CERT/SYS/04/2018/RC

Version 1.0

24 July 2018

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	24/07/2018

2 Table of contents

3 Acronyms

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CGA Certificate Generation Application

DPCM Decreto del Presidente del Consiglio dei Ministri

DTBS/R Data To Be Signed/Representation

EAL Evaluation Assurance Level

eIDAS Electronic IDentification, Authentication and Signature

eMRTD Electronic Machine Readable Travel Document

HW Hardware

ICAO International Civil Aviation Organization

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

OCSI Organismo di Certificazione della Sicurezza Informatica

PACE Password Authenticated Connection Establishment

PP Protection Profile

QSCD Qualified Signature Creation Device

RAD Reference Authentication Data

RFV Rapporto Finale di Valutazione (Evaluation Technical Report)

SAR Security Assurance Requirement

SCA Signature Creation Application

SCD Signature Creation Data

SFR Security Functional Requirement

SVD Signature Verification Data

SW	Software
TDS	Traguardo di Sicurezza (Security Target)
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

4 References

4.1 Criteria and regulations

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[BSI-59] Protection profiles for secure signature creation device – Part 2: Device with key generation, v2.0.1, January 2012, BSI-CC-PP-0059-2009-MA-01 [BSI-59]

[BSI-71] Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, November 2012, BSI-CC-PP-0071-2012

[BSI-72] Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, November 2012, BSI-CC-PP-0072-2012

[CCDB] CCDB-2015-12-001, Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, Version 1.4, December 2015

[eIDAS] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 2014

[ETR-COMP] Evaluation Technical Report for Composition NXP JCOP 3 SECID P60 CS (OSB) – EAL5+, Brightsight, NSCIB-CC-98209, Version 2.0, 17 July 2017

[IAR] Impact Analysis Report: “ASapp-eID and ASapp-QSCD Applets”, version: 2, 15 November 2017, reference TCAE170098

[ICAO-TR] ICAO: Machine Readable Travel Documents – Technical Report – RF Protocol and Application Test Standard for EMRTD – Part 3: Tests for Application Protocol and Logical Data Structure, version 2.10, July 2016

[INI] ASapp-QSCD Applet Initialization Guidance Version 1.1, 25 April 2018, reference TCAE160085

[NSCIB] Certification Report for NXP JCOP 3 SECID P60 CS (OSB)”, 1 August 2017, ref. NSCIB-CC-98209-CR

[PER] ASapp-QSCD Applet Personalization Guidance Version 1.1, 25 April 2018, reference TCAE 160086

[RC] Certification Report for “ASapp-QSCD v1.0”, OCSI/CERT/SYS/11/2016/RC, version 1.0, 12 December 2017

[RFV] ASapp-QSCD (OSB) Evaluation Technical Report, v1, 22 June 2018

[TDS] ASapp-QSCD (OSB) Security Target, v7, 30 May 2018, reference TCAE160087

[USR] ASapp-QSCD Applet Operational User Guidance Version 1.3, 25 April 2018, reference TCAE160076

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on http://www.sogisportal.eu.

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

This certificate is recognized under SOGIS-MRA up to EAL4.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on http://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “ASapp-QSCD v1.0 (based on NXP JCOP3 OSB chip platform)”, short name “ASapp-QSCD (OSB) v1.0”, developed by HID Global.

The TOE is a composite product and comprises:

- the Platform “NXP JCOP 3 SECID P60 CS (OSB)”, certified under The Netherland CC Scheme at EAL5+ (augmented with AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1) [NSCIB];
- the Application Part of the TOE, an applet implementing a Qualified Signature Creation Device (QSCD) compliant with European Parliament Regulation No. 910/2014 [eIDAS];
- the associated guidance documentation ([INI], [PER], and [USR]).

Therefore, the evaluation has been conducted using the results of the Platform CC certification [NSCIB] and following the recommendations contained in the document “Composite product evaluation for Smart Cards and similar devices” [CCDB], as required by the international agreements CCRA and SOGIS.

This Certification Report was issued at the conclusion of the re-certification of an earlier version of the same TOE (ASapp-QSCD v1.0), already certified by OCSI (Certificate no. 7/17 of 12 December 2017 [RC]).

The already certified version was based on the NXP JCOP3 chip platform, variant OSA, while the new version of the TOE is based on the variant OSB of the same chip platform, so making necessary to proceed to a new TOE certification.

The LVS CCLab Software Laboratory has initially carried out an impact analysis of the differences with respect to the already certified version (ASapp-QSCD v1.0), summarizing the results in the document [IAR]. On this basis, the evaluators were able to conduct a new evaluation with a significant re-use of the previous evaluation results. In particular, the evaluation activities were limited to the classes ASE, AGD, ATE and AVA.

Note that the changes have also led to the revision of the Security Target [TDS]. Customers of the TOE are therefore advised to take also into account the new ST.

While the considerations and recommendations already expressed for the previous TOE remain valid, for the sake of simplicity this Certification Report has been rewritten in its entirety, so to constitute an independent document associated with the new TOE "ASapp-QSCD (OSB) v1.0".

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated

by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [TDS]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with ALC_DVS.2 and AVA_VAN.5, according to the information provided in the Security Target [TDS] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “ASapp-QSCD (OSB) v1.0” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [TDS], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	ASapp-QSCD (OSB) v1.0
Security Target	ASapp-QSCD (OSB) v1.0 Security Target, v7, 30 May 2018, reference TCAE160087
Evaluation Assurance Level	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
Developer	HID Global
Sponsor	HID Global
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 4
PP conformance claim	BSI-CC-PP-0059-2009-MA-01 [BSI-59], BSI-CC-PP-0071-2012 [BSI-71], BSI-CC-PP-0072-2012 [BSI-72]
Evaluation starting date	28 March 2018
Evaluation ending date	22June 2018

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [TDS] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of TOE; for a detailed description, please refer to the Security Target [TDS].

The TOE “ASapp-QSCD (OSB) v1.0” is a combination of a smart card and an applet programmed for implementing a Qualified Signature Creation Device (QSCD) compliant with European Parliament Regulation No. 910/2014 [eIDAS].

The TOE is a composite product and comprises:

- the Platform “NXP JCOP 3 SECID P60 CS (OSB)”, certified under The Netherland CC Scheme at EAL5+ (augmented with AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1) [NSCIB];
- the Application Part of the TOE, an applet implementing a Qualified Signature Creation Device (QSCD) compliant with European Parliament Regulation No. 910/2014 [eIDAS];
- the associated guidance documentation.
  - Initialization Guidance for ASapp-eID Applet [INI]
  - Personalization Guidance for ASapp-eID Applet [PER]
  - Operational User Guidance for ASapp-eID Applet [USR]

The intended customer of the product is the QSCD provisioning service, who prepares the TOE as QSCD for its users, personalizes the TOE with the identity of the legitimate user as Signatory and delivers it to the Signatory itself.

The QSCD protects the Signature Creation Data (SCD) during its whole life cycle as to be used in a signature creation process solely by its Signatory.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature.

After preparation, the SCD shall be in a non-operational state. Upon receiving a TOE, the Signatory shall verify its non-operational state and change the SCD state to operational.

7.3.1 TOE Architecture

For a detailed description of the TOE, consult sect. 2 of the Security Target [TDS]. The most significant aspects are summarized below.

7.3.1.1 Generation of SCD/SVD pairs

The QSCD applet supports the generation of SCD/SVD pairs in the QSCD preparation phase only by the Administrator, as well as in the QSCD operational use phase by both the Administrator and the Signatory. SCD keys are activated for signature creation at the time of their generation only in case they are generated by the Signatory, otherwise they are not active until the Signatory explicitly activates them.

The import of certificate info from the CGA and the export of the SVD to the CGA are supported over the same trusted channel to ensure the SVD integrity.

For more detail see sect. 2.2.2 of [TDS].

7.3.1.2 Signature creation

The QSCD applet supports digital signature creation with signature creation algorithm RSASSA-PKCS1-v1_5, hash algorithms SHA-1, SHA-256 compliant with FIPS PUB 180-4, and keys of 1024, 1280, 1536, or 2048 bits.

The signature creation function of the QSCD applet can take all of the following types of data as input from the SCA:

- a hash value of the data to be signed;
- an intermediate hash value of a first part of the data to be signed, complemented with the remaining part of such data;
- the data to be signed themselves (provided their length is not larger than 64 bytes).

Signature creation is only allowed after the authentication of the user in the Signatory role; this guarantees the protection of integrity of data to be signed or a unique representation thereof (DTBS/R) imported from the SCA. The export of public keys, certificate info, and digital signatures to the SCA must occur over the same trusted channel.

For more detail see sect. 2.2.3 of [TDS].

7.3.1.3 TOE life cycle

The TOE life cycle is described in terms of the following four life cycle phases, each divided in one or more steps:

- Phase 1: Development, composed of:
  - Step 1) the development of the integrated circuit and of the multi-applications operating system Java Card 3 by the IC Manufacturer;
  - Step 2) the development of the QSCD applet by the Embedded Software Developer.
- Phase 2: Manufacturing, composed of:
  - Step 3) loading the applet;
  - Step 4) the embedding of the chip in a substrate with an antenna, that may be omitted if the IC contacts are exposed;
  - Step 5) the Initialization and configuration.
- Phase 3: Personalization, comprising:
  - Step 6) personalization of the e-Document for the holder.
- Phase 4: Operational Use, comprising:
  - Step 7) QSCD Preparation;
  - Step 8) QSCD Operational Use.

For more detail see sect. 2.3 of [TDS].

7.3.2 TOE security features

7.3.2.1 Platform compatibility

Some aspects related to security features of the TOE, including security objectives, assumptions, threats and organizational security policies, defined in the Security Target, are covered directly by the Platform. For details see Appendix A of [TDS].

7.3.2.2 Security features

The TOE provides the following functions:

- to generate Signature Creation Data (SCD) and the corresponding Signature Verification Data (SVD);
- to export the SVD for certification to the CGA over a trusted channel;
- to prove the identity as QSCD to external entities;
- to, optionally, receive and store certificate info;
- to switch the QSCD from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data with the following steps:
    a. select an SCD if multiple are present in the QSCD;
    b. authenticate the Signatory and determine its intent to sign;
    c. receive data to be signed, or a unique representation thereof (DTBS/R) from the SCA over a trusted channel;
    d. apply an appropriate cryptographic signature creation function to the DTBS/R using the selected SCD.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product. The intended customer of the product is the QSCD provisioning service, who is in charge of delivering the product to the legitimate user as Signatory.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [TDS].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [TDS] claims strict conformance to the following Protection Profiles:

- Protection profiles for secure signature creation device – Part 2: Device with key generation, v2.0.1, January 2012, BSI-CC-PP-0059-2009-MA-01 [BSI-59];
- Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, November 2012, BSI-CC-PP-0071-2012 [BSI-71];
- Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, November 2012, BSI-CC-PP-0072-2012 [BSI-72].

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

Please refer to the Security Target [TDS] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

All the Security Functional Requirements (SFR) have been selected or derived by extension from CC Part 2 [CC2]. In particular, considering that the Security Target claims strict conformance to three PPs, all extended components from such PPs are included: FPT_EMS from [BSI-59] and FIA_API from [BSI-71].

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

Therefore, considering that the TOE is a composite product, the evaluation has been conducted following the recommendations contained in the document “Composite product evaluation for Smart Cards and similar devices” [CCDB], as required by the international agreements CCRA and SOGIS. In particular, the penetration tests have been completed in May 2018, within 18 months from the Platform vulnerability analysis (June 2017, the reference date indicated in the relevant evaluation [ETR-COMP]).

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [TDS]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 22 June 2018 with the issuance by LVS of the Evaluation Technical Report [RFV], which was approved by the Certification Body on 17 July 2018. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [TDS], with reference to the operating environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [RFV] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE “ASapp-QSCD (OSB) v1.0" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_DVS.2 and AVA_VAN.5, with respect to the security features described in the Security Target [TDS] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with ALC_DVS.2, AVA_VAN.5.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass

Assurance classes and components		Verdict
Delivery procedures	ALC_DEL.1	Pass
Sufficiency of security measures	ALC_DVS.2	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Advanced methodical vulnerability analysis	AVA_VAN.5	Pass

Table 1 – Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product "ASapp-QSCD (OSB) v1.0" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [TDS].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 5.2 of the Security Target [TDS]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the TDS are respected, particularly those compatible with the Platform HW (see Appendix A of [TDS]).

This Certification Report is valid for the TOE in the evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([INI], [PER], and [USR]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

Since the TOE is a composite product, the delivery procedures entail interactions between the application developer (HID Global) and the Platform manufacturer (NXP).

In particular, the platform manufacturer implements the application in the integrated circuit and activates the process of initialization and customization, with the cooperation of the application developer. The document just created, encrypted with a special transport key, is delivered to the customer, i.e. the QSCD provisioning service, who is in charge of delivering the product to the legitimate user as Signatory, by a trusted express courier. If the document is lost, however, it cannot be altered, since, after the application is loaded and configured, it becomes read-only. Finally, the QSCD provisioning service delivers the individual cards to the legitimate users personally at its official site, or sending by post, according to the local regulations.

The application developer HID Global is responsible for the maintenance of the security aspects (integrity, confidentiality, availability).

More detail on such a procedure are contained in:

- Initialization Guidance for ASapp-eID Applet [INI]
- Personalization Guidance for ASapp-eID Applet [PER]

9.2 Installation, initialization and secure usage of the TOE

The TOE is prepared for the Signatory's use by:

- generating at least one SCD/SVD pair, and
- personalizing for the Signatory by storing in the TOE:
    a. the Signatory's Reference Authentication Data (RAD),
    b. optionally, certificate info for at least one SCD in the TOE.

After preparation, the SCD is not active and the TOE shall be in a non-operational state. Upon receiving the TOE, the Signatory shall verify its non-operational state and change it to the operational use explicitly activating the SCD.

If the use of an SCD is no longer required, then it shall be destroyed.

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “ASapp-QSCD v1.0 (based on NXP JCOP3 OSB chip platform)”, short name ASapp-QSCD (OSB) v1.0”, developed by HID Global.

The TOE is a composite product and comprises the following HW/SW components, representing the evaluated configuration of the TOE, as reported in [TDS], to which the evaluation results apply:

- the Platform “NXP JCOP 3 SECID P60 CS (OSB)”, certified under The Netherland CC Scheme at EAL5+ (augmented with AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1) [NSCIB], which in turn consists of:
    - the circuitry of the e-Document’s chip NXP P6022J VB;
    - the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software;
    - the IC Embedded Software (JCOP3 OSB).
- the Application Part of the TOE, an applet implementing a Qualified Signature Creation Device (QSCD) compliant with European Parliament Regulation No. 910/2014 [eIDAS];
- the associated guidance documentation.
    - Initialization Guidance for ASapp-eID Applet [INI]
    - Personalization Guidance for ASapp-eID Applet [PER]
    - Operational User Guidance for ASapp-eID Applet [USR]

11 Annex C – Test activity

This annex describes the task of both the evaluators and the developer in testing activities. For the assurance level EAL4, augmented with ALC_DVS.2 and AVA_VAN.5, such activities include the following three steps:

- evaluation of the tests performed by the developer in terms of coverage and level of detail;
- execution of independent functional tests by the evaluators;
- execution of penetration tests by the evaluators.

11.1 Test configuration

For the execution of these activities a test environment has been arranged at the LVS site with the support of the developer, which provided the necessary resources. In particular, the test configuration consists of the test card, a test card reader connected to the test PC, running the test cases, developed for KEOLABS SCRIPTIS environment.

Before the tests, the software application has been initialized and configured in accordance with the guidance documentation ([INI], [PER], and [USR]), as indicated in sect. 9.2.

Moreover, considering that the TOE is a composite product, the recommendations contained in the document [CCDB] have been followed. In particular, the hardware platform has already been certified and the results were reused from LVS, who was able to directly evaluate the software application.

11.2 Functional tests performed by the developer

11.2.1 Test coverage

The test plan presented by the developer has been partly based on the following reference document, normally used for products such as electronic passports and similar:

- ICAO: Machine Readable Travel Documents – Technical Report – RF Protocol and Application Test Standard for EMRTD – Part 3: Tests for Application Protocol and Logical Data Structure, version 2.10, July 2016 [ICAO-TR].

This was applied for PACE tests. In addition, as the main part of the testing the developer designed independently other additional tests in order to demonstrate the complete coverage of the functional requirements SFR and of the security functions.

11.2.2 Test results

The evaluators executed a series of tests, a sample chosen from those described in the test plan presented by the developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the evaluators

Therefore, the evaluators have designed independent testing to verify the correctness of the TSFI.

They did not used testing tools in addition to the specific components of the TOE that allowed to check all TSFI selected for independent testing.

In the design of independent tests, the evaluators have considered aspects that in the developer test plan were not present, or ambiguous, or inserted in more complex tests, which covered a mix of interfaces but with a level of detail not adequate.

The evaluators also designed and executed some tests independently from similar tests of the developer, based only on the evaluation documentation.

Finally, considering that the TOE is a composite product, the behavior of the TOE as a whole has been verified, carrying out the additional activities specified in the family ATE_COMP, according to the document [CCDB].

All independent tests performed by evaluators generated positive results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see sect. 11.1)

The evaluators have first verified that the test configurations were consistent with the version of the TOE under evaluation, that is indicated in the [TDS], sect. 1.5.

In a first phase, the evaluators have conducted researches using various sources in the public domain, such as Internet, books, publications, conference proceedings, including the various editions of ICCC, JIL and CCDB documents, etc., in order to identify known vulnerabilities applicable to types of products similar to the TOE, i.e. electronic documents eMRTD. They identified several potential vulnerabilities, most of which, however, refer to the hardware platform already certified EAL5+, and therefore not exploitable with the High potential attack corresponding to AVA_VAN.5.

In a second step, the evaluators examined the evaluation documentation (Security Target, functional specification, TOE design, security architecture and operational documentation, including the Platform) to identify any additional potential vulnerabilities of the TOE. From this analysis, together with the source code examination, the evaluators have actually determined the presence of other potential vulnerabilities; however, also in this case, most of them were already considered during the evaluation of the Platform, as documented in the relevant final Evaluation Technical Report [ETR-COMP].

The evaluators have analyzed in detail the potential vulnerabilities identified in the two previous steps, to ensure their effective exploitability in the TOE operating environment. This analysis led to identify some actual potential vulnerabilities.

Therefore, the evaluators have designed some possible attack scenarios, with High attack potential, and penetration tests to verify the exploitability of the potential candidate vulnerabilities. The penetration tests have been described with sufficient detail for their

repeatability using for this purpose test sheets, also used, appropriately compiled with the results, as the report of the tests themselves.

Moreover, considering that the TOE is a composite product, the behavior of the TOE as a whole has been verified, carrying out the additional activities specified in the family AVA_COMP, according to the document [CCDB].

On the basis of the penetration tests, the evaluators have actually found that no attack scenario with potential High can be completed successfully in the operating environment of the TOE as a whole. Therefore, none of the previously identified potential vulnerabilities can be exploited effectively. They have not identified residual vulnerabilities, i.e. vulnerabilities that, although not exploitable in the operating environment of the TOE, could be exploited only by an attacker with attack potential beyond High.