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)*

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

ASapp-QSCD (OSB) v1.0

OCSI/CERT/SYS/04/2018/RC

Versione 1.0

24 luglio 2018

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	24/07/2018

2 Indice

3 Elenco degli acronimi

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

ODV Oggetto della Valutazione

PACE Password Authenticated Connection Establishment

PP Profilo di Protezione

QSCD Qualified Signature Creation Device

RAD Reference Authentication Data

RFV Rapporto Finale di Valutazione

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
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

4 Riferimenti

4.1 Criteri e normative

[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 Documenti tecnici

[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 Pro-tocol 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 TCAE160086

[RC] Rapporto di Certificazione “ASapp-QSCD v1.0”, OCSI/CERT/SYS/11/2016/RC, versione 1.0, 12 dicembre 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 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su http://www.sogisportal.eu.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA fino a EAL4.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su http://www.commoncriteriaportal.org.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA fino a EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "ASapp-QSCD v1.0 (based on NXP JCOP3 OSB chip platform)", nome abbreviato "ASapp-QSCD (OSB) v1.0", sviluppato dalla società HID Global.

L'ODV è un prodotto composito e comprende:

- la Piattaforma "NXP JCOP 3 SECID P60 CS (OSB)", già certificata CC dallo Schema olandese a livello EAL5+ (con aggiunta di AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 e ALC_FLR.1) [NSCIB];
- la parte applicativa dell'ODV, un'applet che implementa un Qualified Signature Creation Device (QSCD) conforme al Regolamento del Parlamento Europeo No. 910/2014 [eIDAS];
- la documentazione operativa associata ([INI], [PER] e [USR]).

Pertanto, la valutazione è stata eseguita utilizzando i risultati della certificazione CC della Piattaforma [NSCIB] e seguendo le raccomandazioni contenute nel documento "Composite product evaluation for Smart Cards and similar devices" [CCDB], come richiesto dagli accordi internazionali CCRA e SOGIS.

Il presente Rapporto di Certificazione è stato emesso a conclusione del processo di ri-certificazione di una precedente versione dello stesso ODV (ASapp-QSCD v1.0), già certificata dall'OCSI (Certificato n. 7/17 del 12 dicembre 2017 [RC]).

La versione già certificata si basava sulla variante OSA della piattaforma hardware NXP JCOP3, mentre la nuova versione dell'ODV si basa sulla variante OSB della stessa piattaforma; ciò ha reso necessario procedere a una nuova certificazione dell'ODV.

L'LVS CCLab Software Laboratory ha inizialmente effettuato un'analisi d'impatto delle differenze della nuova versione dell'ODV rispetto a quella già certificata (ASapp-QSCD v1.0), riassumendone i risultati nel documento [IAR]. I valutatori hanno quindi potuto eseguire una nuova valutazione riutilizzando in modo significativo i risultati di quella precedente. In particolare, le attività di valutazione sono state limitate alle classi ASE, AGD, ATE e AVA.

Si noti che le modifiche effettuate hanno comportato anche la revisione del Traguardo di Sicurezza [TDS]. Gli utenti della precedente versione dell'ODV sono quindi invitati a prendere visione anche del nuovo TDS.

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente ODV, per facilità di lettura il presente Rapporto di Certificazione è stato riscritto nella sua interezza, in modo da costituire un documento autonomo associato al nuovo ODV "ASapp-QSCD (OSB) v1.0".

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL4, con aggiunta di ALC_DVS.2 e AVA_VAN.5, in conformità a quanto indicato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione riassume l'esito della valutazione di sicurezza del prodotto "ASapp-QSCD (OSB) v1.0" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

I potenziali acquirenti sono quindi tenuti a consultare il presente Rapporto di Certificazione congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	ASapp-QSCD (OSB) v1.0
Traguardo di Sicurezza	ASapp-QSCD (OSB) v1.0 Security Target, v7, 30 May 2018, reference TCAE160087
Livello di garanzia	EAL4 con aggiunta di ALC_DVS.2 e AVA_VAN.5
Fornitore	HID Global
Committente	HID Global
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 4
Conformità a PP	BSI-CC-PP-0059-2009-MA-01 [BSI-59], BSI-CC-PP-0071-2012 [BSI-71], BSI-CC-PP-0072-2012 [BSI-72]
Data di inizio della valutazione	28 marzo 2018
Data di fine della valutazione	22 giugno 2018

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "ASapp-QSCD (OSB) v1.0" è costituito da una smart card e una parte applicativa programmata per implementare un Qualified Signature Creation Device (QSCD) conforme al Regolamento del Parlamento Europeo No. 910/2014 [eIDAS].

L'ODV è un prodotto composito e comprende:

- la Piattaforma “NXP JCOP 3 SECID P60 CS (OSB)”, già certificata CC dallo Schema olandese a livello EAL5+ (con aggiunta di AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 e ALC_FLR.1) [NSCIB];
- la parte applicativa dell’ODV, un’applet che implementa un Qualified Signature Creation Device (QSCD) conforme al Regolamento del Parlamento Europeo No. 910/2014 [eIDAS];
- la documentazione operativa associata:
    - Initialization Guidance for ASapp-eID Applet [INI]
    - Personalization Guidance for ASapp-eID Applet [PER]
    - Operational User Guidance for ASapp-eID Applet [USR]

Il “cliente” dell’ODV è di solito il fornitore di servizi di firma elettronica, che configura l’ODV come QSCD per i suoi utenti, cioè lo personalizza con l’identità dei singoli utenti/Firmatari e lo distribuisce ai Firmatari stessi.

Il dispositivo QSCD protegge i dati per la creazione della firma elettronica (SCD) durante il suo intero ciclo di vita e può essere usato per generare firme elettroniche esclusivamente dal legittimo utente/Firmatario.

L’ODV comprende tutte le funzionalità di sicurezza necessarie ad assicurare la segretezza dei dati SCD e delle firme elettroniche.

Dopo la preparazione, i dati SCD saranno in uno stato non-operativo; sarà l’utente/Firmatario ad attivare lo stato operativo, dopo aver ricevuto e verificato l’ODV.

7.3.1 Architettura dell’ODV

Per una descrizione maggiormente dettagliata dell’ODV, consultare il capitolo 2 del [TDS]. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti:

7.3.1.1 Generazione della coppia di chiavi SCD/SVD

L’applet QSCD supporta la generazione di coppie di chiavi SCD/SVD nella fase di preparazione da parte del solo Amministratore e nell’uso operativo sia da parte dell’Amministratore, sia da parte del Firmatario. Le chiavi private SCD sono attivate per la creazione della firma all’atto della loro generazione soltanto se generate da parte del Firmatario, altrimenti rimangono non attive fino a quando il Firmatario stesso non le attivi esplicitamente.

Le operazioni di importazione del certificato dall’applicazione per la creazione dei certificati (CGA) e di esportazione della chiave pubblica SVD verso la stessa CGA sono realizzate utilizzando lo stesso canale sicuro per garantire l’integrità della SVD.

Per maggiori dettagli si veda il par. 2.2.2 del [TDS].

7.3.1.2 Creazione della firma

L'applet QSCD supporta la creazione di firme elettroniche utilizzando l'algoritmo RSASSA-PKCS1-v1_5, gli algoritmi SHA-1, SHA-256 conformi a FIPS PUB 180-4 per la generazione degli *hash*, e chiavi di lunghezza pari a 1024, 1280, 1536, o 2048 bit.

La funzione di creazione di firme dell'applet QSCD può accettare come input dall'applicazione per la creazione delle firme (SCA) tutti i seguenti tipi di dati:

- un valore *hash* dei dati da firmare;
- un valore *hash* intermedio di una prima parte dei dati da firmare, completato con la parte restante dei dati stessi;
- i dati completi da firmare non compressi (a patto che la loro lunghezza non superi i 64 bit).

La creazione della firma è consentita solo dopo l'autenticazione dell'utente nel ruolo di Firmatario; ciò garantisce la protezione dell'integrità dei dati da firmare o di una loro rappresentazione unica (DTBS/R) importati dalla SCA. L'esportazione delle chiavi pubbliche, dei certificati e delle firme elettroniche verso la SCA deve essere realizzata utilizzando lo stesso canale fidato.

Per maggiori dettagli si veda il par. 2.2.3 del [TDS].

7.3.1.3 Ciclo di vita dell'ODV

Il ciclo di vita dell'ODV è descritto in termini delle seguenti quattro fasi, ciascuna a sua volta divisa in uno o più passi:

- Fase 1: Sviluppo, composta da:
  - Passo 1) lo sviluppo del circuito integrato e del sistema operativo multi-applicazione Java Card 3 da parte dello sviluppatore del circuito integrato;
  - Passo 2) lo sviluppo dell'applet QSCD da parte dello sviluppatore del software incorporato nel circuito stesso.
- Fase 2: Produzione, composta da:
  - Passo 3) caricamento dell'applet;
  - Passo 4) l'integrazione nel chip di un substrato con antenna, che può essere omessa se i contatti del chip sono scoperti;
  - Passo 5) inizializzazione e configurazione.
- Fase 3: Personalizzazione, comprendente:
  - Passo 6) personalizzazione del documento elettronico per il proprietario.
- Fase 4: Uso operativo, comprendente:

- Passo 7) Preparazione del QSCD;
- Passo 8) Uso operativo del QSCD.

Per maggiori dettagli si veda il par. 2.3 del [TDS].

7.3.2 Caratteristiche di Sicurezza dell'ODV

7.3.2.1 Compatibilità con la Piattaforma

Alcuni aspetti relativi a funzionalità di sicurezza dell'ODV, inclusi obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza organizzative definite nel Traguardo di Sicurezza sono coperti direttamente dalla Piattaforma. Per i dettagli consultare l'Appendice A del [TDS].

7.3.2.2 Funzionalità di sicurezza

L'ODV fornisce le seguenti funzionalità:

- generazione delle chiavi private per la creazione di firme elettroniche (SCD) e le corrispondenti chiavi pubbliche di verifica delle firme stesse (SVD);
- esportazione delle chiavi pubbliche SVD verso la CGA utilizzando un canale sicuro;
- prova dell'identità come QSCD verso entità esterne;
- ricezione e memorizzazione delle informazioni dei certificati (opzionale);
- commutazione del QSCD da uno stato non-operativo a uno di uso operativo;
- nello stato di uso operativo, creazione di firme elettroniche coi seguenti passi:
    a. selezione di una chiave privata SCD se nel QSCD ve ne sono diverse;
    b. autenticazione del Firmatario e verifica della sua intenzione di firmare;
    c. ricezione dei dati da firmare o di una loro rappresentazione univoca (DTBS/R) dalla SCA tramite un canale fidato;
    d. applicazione ai DTBS/R della funzione crittografica di creazione della firma appropriata utilizzando la chiave privata SCD selezionata.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto. Per "cliente" del prodotto si intende il fornitore di servizi di firma elettronica, che ha il compito di distribuire successivamente i singoli prodotti agli effettivi utenti/Firmatari. La documentazione indicata contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità *strict* ai seguenti Profili di Protezione (PP):

- 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 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

Tutti gli SFR sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2]. In particolare, poiché il TDS dichiara stretta conformità a tre PP, sono inclusi anche i componenti estesi definiti in tali PP e precisamente: FPT_EMS da [BSI-59] e FIA_API da [BSI-71].

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Inoltre, trattandosi di un ODV composito, sono state seguite le indicazioni contenute nel documento "Composite product evaluation for Smart Cards and similar devices" [CCDB], come richiesto dagli accordi internazionali CCRA e SOGIS. In particolare, si precisa che i test di intrusione sono stati completati nel mese di maggio 2018, quindi entro 18 mesi da quelli effettuati per la Piattaforma (giugno 2017, periodo di riferimento indicato nei risultati della relativa valutazione [ETR-COMP]).

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS CCLab Software Laboratory.

L'attività di valutazione è terminata in data 22 giugno 2018 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 17 luglio 2018. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS CCLab Software Laboratory e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "ASapp-QSCD (OSB) v1.0" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di ALC_DVS.2 e AVA_VAN.5, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4, con aggiunta di ALC_DVS.2 e AVA_VAN.5.

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

Classi e componenti di garanzia		Verdetto
Delivery procedures	ALC_DEL.1	Positivo
Sufficiency of security measures	ALC_DVS.2	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Advanced methodical vulnerability analysis	AVA_VAN.5	Positivo

Tabella 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "ASapp-QSCD (OSB) v1.0" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 5.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte nel TDS, in particolare quelle compatibili con la Piattaforma hardware dell'ODV (cfr. Appendice A di [TDS]).

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, in Appendice A – Indicazioni per l'uso sicuro del prodotto sono incluse una serie di raccomandazioni relative alla consegna, all'inizializzazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([INI], [PER] e [USR]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna

Poiché l'ODV è di tipo composito, le procedure di consegna prevedono delle interazioni tra lo sviluppatore dell'applicazione (HID Global) e il fornitore della Piattaforma (NXP).

In particolare, il fornitore della Piattaforma implementa l'applicazione nel circuito integrato e attiva il processo di inizializzazione e personalizzazione, con la collaborazione dello sviluppatore dell'applicazione. Il documento così creato, cifrato con un'apposita chiave di trasporto, viene inviato al cliente, cioè il fornitore di servizi di firma elettronica, che ha il compito di distribuire successivamente i singoli prodotti agli effettivi utenti/Firmatari, tramite un corriere espresso di fiducia. Se il documento dovesse perdersi, non potrebbe comunque essere alterato, poiché, dopo che l'applicazione è stata caricata e configurata, è diventato di sola lettura. Infine, il fornitore di servizi di firma elettronica consegna successivamente i singoli documenti agli effettivi titolari direttamente presso la propria sede o inviandoli via posta, in base alle normative locali.

La responsabilità di garantire gli aspetti di sicurezza, integrità, confidenzialità e disponibilità, è a carico dello sviluppatore dell'applicazione HID Global.

Maggiori dettagli sulla procedura di personalizzazione sono contenuti in:

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

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'ODV è preparato per l'uso da parte del Firmatario tramite i seguenti passi:

- generazione di almeno una coppia di chiavi SCD/SVD;
- personalizzazione per il Firmatario memorizzando all'interno dell'ODV stesso:
    a. i dati di autenticazione del Firmatario (RAD);
    b. le informazioni del certificato per almeno una chiave SCD (opzionale).

Dopo la preparazione, la chiave privata SCD non è attiva e quindi l'ODV si trova in uno stato non-operativo. Una volta ricevuto l'ODV, il Firmatario deve verificare tale stato e commutarlo a quello di uso operativo attivando la propria chiave privata SCD.

Quando una chiave privata SCD non è più utilizzata per la creazione di firme elettroniche, deve essere distrutta.

10 Appendice B – Configurazione valutata

L'ODV è il prodotto “ASapp-QSCD v1.0 (based on NXP JCOP3 OSB chip platform)”, nome abbreviato ASapp-QSCD (OSB) v1.0”, sviluppato dalla società HID Global.

L’ODV è un prodotto composito e comprende i seguenti componenti HW/SW, con le rispettive versioni, costituenti la configurazione valutata dell’ODV, come riportato in [TDS], a cui si applicano i risultati della valutazione:

- la Piattaforma “NXP JCOP 3 SECID P60 CS (OSB)”, già certificata CC dallo Schema olandese a livello EAL5+ (con aggiunta di AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 e ALC_FLR.1) [NSCIB], a sua volta costituita da:
    - i circuiti e le connessioni del chip NXP P6022J VB;
    - il Software dedicato con le parti specifiche per i Test e il Supporto;
    - l’Embedded Software (JCOP3 OSB).
- la parte applicativa dell’ODV, un’applet che implementa un Qualified Signature Creation Device (QSCD) conforme al Regolamento del Parlamento Europeo No. 910/2014 [eIDAS];
- la documentazione operativa associata:
    - Initialization Guidance for ASapp-eID Applet [INI]
    - Personalization Guidance for ASapp-eID Applet [PER]
    - Operational User Guidance for ASapp-eID Applet [USR]

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL4, con aggiunta di ALC_DVS.2 e AVA_VAN.5, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura e livello di approfondimento dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

Per l'esecuzione dei test è stato predisposto un apposito ambiente di test presso la sede dell'LVS con il supporto del Committente/Fornitore, che ha fornito le risorse necessarie. In particolare, sono stati predisposti una smart card, un lettore di smart card e un PC, sul quale è stato installato lo strumento di test in ambiente KEOLABS SCRIPTIS.

Prima dell'esecuzione dei test il software è stato installato e configurato seguendo le istruzioni contenute nei documenti [INI], [PER] e [USR], come indicato nel par. 9.2. Inoltre, trattandosi di un ODV composito, sono state seguite le indicazioni contenute nel documento [CCDB]. In particolare, la Piattaforma hardware è stata già certificata e i relativi risultati sono stati riutilizzati dall'LVS, che ha potuto così valutare direttamente l'applicazione software.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Copertura dei test

Il piano di test presentato dal Fornitore si è basato in parte sul seguente documento di riferimento, solitamente utilizzato per prodotti tipo passaporti elettronici e simili:

- 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].

Questo documento è stato utilizzato per i test sul protocollo PACE. Inoltre, come parte principale dell'attività di test, il Fornitore ha progettato autonomamente test aggiuntivi, al fine di dimostrare la completa copertura dei requisiti funzionali (SFR) e delle funzioni di sicurezza.

11.2.2 Risultati dei test

I Valutatori hanno eseguito una serie di test, scelti a campione tra quelli descritti nel piano di test presentato dal Fornitore, verificando positivamente il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

Non sono stati utilizzati strumenti di test particolari, oltre ai componenti dell'ODV che hanno permesso di sollecitare tutte le TSFI selezionate per i test indipendenti.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o inseriti in test più complessi che interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione.

Infine, trattandosi di un ODV composito, sono stati eseguiti anche i test integrativi miranti a verificare il comportamento dell'ODV nel suo complesso, svolgendo le attività integrative previste dalla famiglia ATE_COMP, in base a quanto indicato nel documento [CCDB].

Tutti i test indipendenti eseguiti dai Valutatori hanno dato esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali (cfr. par. 11.1). I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quella indicata nel [TDS], par. 1.5.

In una prima fase, i Valutatori hanno effettuato delle ricerche utilizzando varie fonti di pubblico dominio, quali internet, libri, pubblicazioni specialistiche, atti di conferenze, comprese le varie edizioni dell'ICCC, documenti JIL e CCDB, ecc., al fine di individuare eventuali vulnerabilità note applicabili a tipologie di prodotti simili all'ODV, cioè documenti elettronici eMRTD. Sono state così individuate diverse vulnerabilità potenziali, la maggior parte delle quali, però, si riferiscono alla Piattaforma hardware già certificata EAL5+, e quindi non sfruttabili con potenziali di attacco High, come previsto in AVA_VAN.5.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa, compresa quella della Piattaforma) al fine di evidenziare eventuali ulteriori vulnerabilità potenziali dell'ODV. Da questa analisi, congiuntamente a quella del codice sorgente, i Valutatori hanno effettivamente determinato la presenza di altre vulnerabilità potenziali; anche in questo caso, però, la maggior parte di esse sono state già considerate nel corso della valutazione della Piattaforma, come documentato nel relativo Rapporto Finale di Valutazione [ETR-COMP].

I Valutatori hanno analizzato nel dettaglio le potenziali vulnerabilità individuate nelle due fasi precedenti, per verificare la loro effettiva sfruttabilità nell'ambiente operativo dell'ODV. Quest'analisi ha portato a individuare alcune effettive vulnerabilità potenziali.

I Valutatori hanno quindi progettato dei possibili scenari di attacco, con potenziale di attacco High, e dei test di intrusione per verificare la sfruttabilità di tali vulnerabilità

potenziali candidate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi.

Trattandosi di un ODV composito, sono state eseguite anche le attività integrative previste dalla famiglia AVA_COMP, in base a quanto indicato nel documento [CCDB], al fine di verificare il comportamento dell'ODV nel suo complesso.

Dall'esecuzione dei test di intrusione, i Valutatori hanno effettivamente riscontrato che nessuno scenario di attacco con potenziale High può essere portato a termine con successo nell'ambiente operativo dell'ODV nel suo complesso. Pertanto, nessuna delle vulnerabilità potenziali precedentemente individuate può essere effettivamente sfruttata. Non sono state individuate neanche vulnerabilità residue, cioè vulnerabilità che, pur non essendo sfruttabili nell'ambiente operativo dell'ODV, potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a High.