*Ministero dello Sviluppo Economico*

*Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione*

OCSI

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. 3/17

*(Certification No.)*

**Prodotto:** **ASapp-eID-BAC v1.0**
*(Product)*

**Sviluppato da:** **HID Global / Arjo Systems**
*(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)**

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 20 settembre 2017

Common Criteria

SOGIS

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

*Ministero dello Sviluppo Economico*

*Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione*

Organismo di Certificazione della Sicurezza Informatica

# Rapporto di Certificazione

# ASapp-eID-BAC v1.0

OCSI/CERT/SYS/09/2016/RC

Versione 1.0

20 settembre 2017

Questa pagina è lasciata intenzionalmente vuota

# 1 Revisioni del documento

| Versione | Autori | Modifiche | Data |
|---|---|---|---|
| 1.0 | OCSI | Prima emissione | 20/09/2017 |
| | | | |

# 2 Indice

1 Revisioni del documento ....5
2 Indice ....6
3 Elenco degli acronimi ....8
4 Riferimenti ....9
5 Riconoscimento del certificato ....11
5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA) ....11
5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA) ....11
6 Dichiarazione di certificazione ....12
7 Riepilogo della valutazione ....13
7.1 Introduzione ....13
7.2 Identificazione sintetica della certificazione ....13
7.3 Prodotto valutato ....13
7.3.1 Architettura dell'ODV ....14
7.3.2 Caratteristiche di Sicurezza dell'ODV ....14
7.4 Documentazione ....15
7.5 Conformità a Profili di Protezione (PP) ....15
7.6 Requisiti funzionali e di garanzia ....16
7.7 Conduzione della valutazione ....16
7.8 Considerazioni generali sulla validità della certificazione ....17
8 Esito della valutazione ....18
8.1 Risultato della valutazione ....18
8.2 Raccomandazioni ....19
9 Appendice A – Indicazioni per l'uso sicuro del prodotto ....20
9.1 Consegna ....20
9.2 Inizializzazione e utilizzo sicuro dell'ODV ....20
10 Appendice B – Configurazione valutata ....21
11 Appendice C – Attività di Test ....22
11.1 Configurazione per i Test ....22
11.2 Test funzionali svolti dal Fornitore ....22
11.2.1 Copertura dei test ....22

11.2.2 Risultati dei test .....23
11.3 Test funzionali ed indipendenti svolti dai Valutatori .....23
11.4 Analisi delle vulnerabilità e test di intrusione .....23

# 3 Elenco degli acronimi

**BAC** Basic Access Control

**CC** Common Criteria

**CCRA** Common Criteria Recognition Arrangement

**CEM** Common Evaluation Methodology

**DPCM** Decreto del Presidente del Consiglio dei Ministri

**EAL** Evaluation Assurance Level

**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

**PP** Profilo di Protezione

**RFV** Rapporto Finale di Valutazione

**SAR** Security Assurance Requirement

**SFR** Security Functional Requirement

**SW** Software

**TDS** Traguardo di Sicurezza

**TOE** Target of Evaluation

**TSF** TOE Security Functionality

**TSFI** TOE Security Functionality Interface

# 4 Riferimenti


[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

[BSI-55] BSI-CC-PP-0055-2009, Machine Readable Travel Document with ”ICAO Application”, Basic Access Control, Version 1.10, 25 March 2009

[BSI-TR] BSI TR-03105 Part 3.2: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EACv1) Tests for security implementation, version 1.4.1, April 2014

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

[ETR-COMP] ETR for Composite Evaluation NXP JCOP 3 SECID P60 (OSA) – PL 2/5 – EAL5+, Brightsight, v1.0, 21 December 2016

[ICAO-P10] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

[ICAO-P11] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015, Part 11: Security Mechanisms for MRTDs

[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-eID Applet Initialization Guidance Version 1.0, 14 March 2017, reference TCAE160083

[NSCIB] Certification Report for “NXP JCOP 3 SECID P60 (OSA) PL2/5”, 21 December 2016, ref. NSCIB-CC-16-99111-CR2

[PER] ASapp-eID Applet Personalization Guidance Version 1.0, 14 March 2017, reference TCAE160084

[RFV] “ASapp-eID Machine Readable Electronic Document - Basic Access Control” Evaluation Technical Report, v3.0, 17 August 2017

[TDS] “ASapp-eID Machine Readable Electronic Document - Basic Access Control” Security Target, v7, 15 August 2017, reference TCAE160088

[USR] ASapp-eID Applet Operational User Guidance Version 1.2, 7 July 2017, reference TCAE160075

# 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-eID Machine Readable Electronic Document - Basic Access Control", nome abbreviato "ASapp-eID-BAC v1.0", sviluppato dalla società HID Global / Arjo Systems.

L'ODV è un prodotto composito e comprende:

- la Piattaforma "NXP JCOP 3 SECID P60 (OSA) – PL 2/5", nome abbreviato "JCOP3 SECID P60", 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 conforme al documento ICAO Doc 9303 ([ICAO-P10] and [ICAO-P11]);
- 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.

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 per avere piena consapevolezza del problema di sicurezza affrontato. 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, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B 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-eID-BAC 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-eID-BAC v1.0 |
| **Traguardo di Sicurezza** | ASapp-eID-BAC v1.0 Security Target, v7, 15 August 2017, reference TCAE160088 |
| **Livello di garanzia** | EAL4 con aggiunta di ALC_DVS.2 |
| **Fornitore** | HID Global / Arjo Systems |
| **Committente** | HID Global / Arjo Systems |
| **LVS** | Systrans Software Laboratory - CCLAB |
| **Versione dei CC** | 3.1 Rev. 4 |
| **Conformità a PP** | BSI-CC-PP-0055-2009 [BSI-55] |
| **Data di inizio della valutazione** | 20 settembre 2016 |
| **Data di fine della valutazione** | 2 agosto 2017 |

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-eID-BAC v1.0" è un documento elettronico costituito da una smart card programmata in base ai requisiti e alle raccomandazioni prescritti dall'International Civil Aviation Organization in ICAO Doc 9303 [ICAO-P10].

Le comunicazioni tra il terminale e il chip sono protette tramite il Basic Access Control (BAC), secondo quanto prescritto dal Profilo di Protezione “Machine Readable Travel Document with ICAO Applet Basic Access Control” (BAC PP) [BSI- 55].

L'ODV è un prodotto composito e comprende:

- la Piattaforma “NXP JCOP 3 SECID P60 (OSA) – PL 2/5”, nome abbreviato "JCOP3 SECID P60", 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 conforme al documento ICAO Doc 9303 ([ICAO-P10] and [ICAO-P11]);
- 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 l’Ente emettitore (Stato o altra Organizzazione) del documento elettronico, che ha il compito di distribuire successivamente i singoli documenti agli effettivi titolari, dopo avervi memorizzato i loro dati personali, quali, ad es., dati biografici, foto, ecc.

Il documento elettronico può essere visto come costituito da una parte “fisica” (cartacea o plastica, con relativo chip), che consente di verificare visivamente i dati personali del titolare, e da una parte ”logica”, in cui gli stessi dati sono memorizzati secondo una Logical Data Structure (LDS) come specificato in [ICAO-P10].

L’autenticità e l’integrità del documento elettronico e dei relativi dati sono garantiti dall’Ente emettitore. In particolare, la parte fisica del documento, identificata da un numero univoco, è protetta con specifiche misure di sicurezza fisiche, logiche e organizzative, mentre la parte logica è garantita dalla firma digitale dello stesso Ente emettitore.

### 7.3.1 Architettura dell'ODV

Per una descrizione maggiormente dettagliata dell’ODV, consultare il [TDS]; in particolare:

- le parti, fisica e logica, dell’ODV sono descritte nel par. 1.4.2;
- il ciclo di vita dell’ODV è costituito da quattro fasi: sviluppo, produzione. personalizzazione e uso operativo, descritte in dettaglio nel par. 1.5, incluse le operazioni permesse ad utenti ed amministratori in ciascuna di esse.

### 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*

Le funzionalità di sicurezza implementate dall'ODV sono organizzate in servizi di sicurezza, descritti in dettaglio nel par. 7.1 del [TDS]. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti:

- **Agents Identification & Authentication**: l'accesso alle funzioni e ai dati dell'ODV è consentito soltanto a utenti autenticati; il meccanismo di autenticazione dipende dal sistema utilizzato per l'uso operativo.

- **Data exchange with Secure Messaging**: per lo scambio dei dati tra l'ODV e il sistema di ispezione, viene creato un canale di comunicazione sicuro, sul quale i dati viaggiano cifrati con chiavi di sessione, in modo che l'ODV sia in grado di verificare l'integrità e l'autenticità dei dati ricevuti.

- **Access Control of stored Data Objects**: l'accesso ai dati sensibili (di utente e delle TSF) è consentito in base ai diritti di accesso definiti durante la fase di Personalizzazione, che consentono anche di differenziare i ruoli degli utenti.

- **Life cycle management**: le fasi del ciclo di vita dell'ODV sono fissate in maniera univoca e irreversibile nel seguente ordine: produzione, personalizzazione e uso operativo.

- **Software integrity check of TOE's assets**: l'ODV non consente di analizzare né modificare il software durante l'uso operativo.

- **Security features provided by the hardware**: l'ODV beneficia di un insieme di funzionalità di sicurezza fornite dalla Piattaforma certificata.

## 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 l'Ente emettitore (Stato o altra Organizzazione) del documento elettronico, che ha il compito di distribuire successivamente i singoli documenti agli effettivi titolari. La documentazione indicata contiene le informazioni richieste per l'inizializzazione, 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 (PP)

L'ODV è strettamente conforme al Profilo di Protezione (PP):

- BSI-CC-PP-0055-2009 [BSI-55], che definisce gli obiettivi di sicurezza e i requisiti delle smart card con o senza contatto utilizzate per documenti di viaggio elettronici (MRTD) protette tramite il controllo di accesso Basic Access Control (BAC).

Poiché l'ODV è un documento elettronico di uso generale, nel TDS sono stati rimossi tutti i riferimenti ai documenti di viaggio utilizzati nel PP. Per lo stesso motivo, l'acronimo "MRTD" è stato sostituito da "e-Document", il termine "travel document" da "e-Document" o "electronic document" e "traveler" da "user" o "presenter".

## 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 un PP [BSI-55], sono inclusi anche i componenti estesi definiti in tale PP e precisamente: FAU_SAS, FCS_RND, FMT_LIM e FPT_EMSEC.

## 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 nella Linea Guida Provvisoria [LGP3] e nella Nota Informativa 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 luglio 2017, quindi entro 18 mesi da quelli effettuati per la Piattaforma (dicembre 2016, 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 Systrans CCLAB.

L'attività di valutazione è terminata in data 2 agosto 2017 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 30 agosto 2017. 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 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-eID-BAC 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, 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.

| **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 | ALC_CMC.4 | Positivo |

| Classi e componenti di garanzia | | Verdetto |
|---|---|---|
| automation | | |
| Problem tracking CM coverage | ALC_CMS.4 | Positivo |
| 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 |
| Focused vulnerability analysis | AVA_VAN.3 | 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-eID-BAC 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. 4.2 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 HW dell'ODV (cfr. [TDS], Appendice A).

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, l'Appendice A include 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 i potenziali acquirenti 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 / Arjo Systems) 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 l'Ente emettitore (Stato o altra Organizzazione) del documento elettronico, 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, l'Ente emettitore consegna 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 / Arjo Systems.

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 Inizializzazione e utilizzo sicuro dell'ODV

L'inizializzazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo in accordo agli obiettivi di sicurezza indicati nel [TDS], devono avvenire seguendo le istruzioni contenute nelle apposite sezioni dei seguenti documenti:

- Initialization Guidance for ASapp-eID Applet [INI];
- Personalization Guidance for ASapp-eID Applet [PER];
- Operational User Guidance for ASapp-eID Applet [USR].

# 10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "ASapp-eID Machine Readable Electronic Document - Basic Access Control", nome abbreviato "ASapp-eID-BAC v1.0", sviluppato dalla società HID Global / Arjo Systems.

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 (OSA) – PL 2/5", nome abbreviato "JCOP3 SECID P60", 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 OSA).
- la parte applicativa dell'ODV, un'applet conforme al documento ICAO Doc 9303 ([ICAO-P10] and [ICAO-P11]);
- 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, 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 gran parte sui seguenti documenti di riferimento, solitamente utilizzati 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 Pro-tocol and Logical Data Structure, version 2.10, July 2016 [ICAO-TR];
- BSI TR-03105 Part 3.2: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EACv1) Tests for security implementation, version 1.4.1, April 2014 [BSI-TR].

In aggiunta, il Fornitore ha progettato autonomamente altri 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. 1.4.

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, riferite alla Piattaforma hardware già certificata EAL5+, e quindi non sfruttabili con potenziale di attacco Enhanced-Basic, come previsto in AVA_VAN.3.

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 erano state già considerate nel corso della valutazione della Piattaforma, come documentato nel relativo Rapporto Finale [ETR-COMP].

I Valutatori hanno quindi 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 Enhanced-Basic, 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 Enhanced-Basic 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 Enhanced-Basic.