Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

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. 12/20

(Certification No.)

Prodotto: IDentity Applet v3.4/eIDAS on NXP JCOP 4 P71

(Product)

Sviluppato da: ID&Trust Ltd.

(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, ATE_DPT.2, AVA_VAN.5)

Il Direttore
(Dott.ssa Eva Spina)

Roma, 28 ottobre 2020

Firmato digitalmente
da Eva Spina
Data: 2020.10.29
09:46:43 +01'00'

Common Criteria

SOGIS IT SECURITY CERTIFIED

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

IDentity Applet v3.4/eIDAS on NXP JCOP 4 P71

OCSI/CERT/SYS/08/2016/RC

Versione 1.0

28 ottobre 2020

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	28/10/2020

2 Indice

1 Revisioni del documento 5
2 Indice 6
3 Elenco degli acronimi 8
4 Riferimenti 10
4.1 Criteri e normative 10
4.2 Documenti tecnici 11
5 Riconoscimento del certificato 13
5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA) 13
5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA) 13
6 Dichiarazione di certificazione 14
7 Riepilogo della valutazione 16
7.1 Introduzione 16
7.2 Identificazione sintetica della certificazione 16
7.3 Prodotto valutato 17
7.3.1 Architettura dell'ODV 18
7.3.2 Caratteristiche di sicurezza dell'ODV 19
7.4 Documentazione 23
7.5 Conformità a Profili di Protezione 24
7.6 Requisiti funzionali e di garanzia 24
7.7 Conduzione della valutazione 25
7.8 Considerazioni generali sulla validità della certificazione 25
8 Esito della valutazione 27
8.1 Risultato della valutazione 27
8.2 Attività di garanzia aggiuntive 28
8.3 Raccomandazioni 29
9 Appendice A – Indicazioni per l'uso sicuro del prodotto 30
9.1 Consegna 30
9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV 30
10 Appendice B – Configurazione valutata 32
11 Appendice C – Attività di Test 33

11.1 Configurazione per i Test 33
11.2 Test funzionali svolti dal Fornitore 33
11.2.1 Approccio adottato per i test 33
11.2.2 Copertura dei test 34
11.2.3 Risultati dei test 34
11.3 Test funzionali ed indipendenti svolti dai Valutatori 34
11.4 Analisi delle vulnerabilità e test di intrusione 35

3 Elenco degli acronimi

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
API	Application Programming Interface
BAC	Basic Access Control
CAN	Card Access Number
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
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic IDentification Authentication and Signature
eMRTD	Electronic Machine Readable Travel Document
ETR	Evaluation Technical Report
GP	Global Platform
HW	Hardware
ICAO	International Civil Aviation Organization
IC	Integrated Circuit
IT	Information Technology
JCOP	Java Card Open Platform
LDS	Logical Data Structure
LGP	Linea Guida Provvisoria

LVS	Laboratorio per la Valutazione della Sicurezza
MRZ	Machine-Readable Zone
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OS	Operating System
PACE	Password Authenticated Connection Establishment
PACE-CAM	PACE with Chip Authentication Mapping
PACE-GM	PACE with Generic Mapping
PIN	Personal Identification Number
PP	Profilo di Protezione (Protection Profile)
QSCD	Qualified Signature Creation Device
RSA	Rivest, Shamir, Adleman
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SCD	Signature Creation Data
SFR	Security Functional Requirement
SOGIS	Senior Officials Group Information Systems Security
ST	Security Target
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-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

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

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[eIDAS] “Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE”, Gazzetta ufficiale dell’Unione europea L 257, 28 agosto 2014

[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

[ADM] ID&Trust Identity Applet Suite Administrator's Guide, Version 3.4.1, 31 July 2020

[BSI-TR1] BSI Technical Guideline 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, 6 April 2014

[BSI-TR2] BSI Technical Guideline TR-03105 Part 3.3: Test Plan for eID-Cards with Advanced Security Mechanisms - EAC 2, Version 1.03, 24 September 2010

[BSI-TR2A] Amendment to BSI TR-03105 Part 3.3, Release 3, 04 June 2012

[BSI-TR3] BSI Technical Guideline TR-03105 Part 3.4: Test plan for eID-Cards with eSign-application acc. to BSI TR-03117, Version 1.0, 01 April 2010

[DEL] ID&Trust Documents, Common Criteria Evaluation, IDentity Applet V3.4 Delivery Documentation, V0.02, 10 February 2020

[ETR-COMP] Evaluation Technical Report for Composition NXP JCOP 4 P71 - EAL6+, 19-RPT-177, Version 7.0, 19 March 2020

[ICAO-9303] International Civil Aviation Organization (ICAO) Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015

[ICAO-TR1] International Civil Aviation Organization (ICAO) Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, 15 April 2014

[ICAO-TR2] International Civil Aviation Organization (ICAO) Technical Report, Radio Frequency Protocol and Application Test Standard for eMRTD Part 3 – Tests for Application Protocol and Logical Data Structure, Version 2.10, 7 July 2016

[JIL-COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[NXP-CR1] Certification Report "NXP JCOP 4 P71", NSCIB-CC-180212-CR2, TÜV Rheinland Nederland B.V., 20 March 2020

[NXP-CR2] Certification Report "NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library", BSI-DSZ-CC-1040-2019-MA-01, BSI - Bundesamt für Sicherheit in der Informationstechnik, 4 March 2020

[PP-056] BSI-CC-PP-0056-V2-2012, Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012

[PP-068] BSI-CC-PP-0068-V2-2011-MA-01, Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22 July 2014

[PP-086] BSI-CC-PP-0086, Protection Profile - Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2 PP), Version 1.01, 20 May 2015

[PP-087] BSI-CC-PP-0087, Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP), version 1.01, 20 May 2015

[PPSSCD] EN 419211-2:2013, Common Criteria Protection Profiles for Secure Signature Creation Device - Part 2: Device with key generation (BSI-CC-PP-0059-2009-MA-02)

[RFV] “ID&Trust IDentity Applet v3.4 /eIDAS” Evaluation Technical Report, v4, CCLab Software Laboratory, 14 October 2020

[TDS] “Security Target ID&Trust IDentity Applet v3.4/eIDAS – Electronic Identity Card with PACE-GM, PACE-CAM, Extended Access Control v1 and v2, Restricted Identification and Active Authentication”, Version 1.02, ID&Trust Ltd., 13 October 2020

[TR-03110-1] BSI TR-03110-1, Advanced Security Mechanisms forMachine Readable Travel Documents and eIDAS Token - Part 1: eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015

[TR-03110-2] BSI TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 21 December 2016

[TR-03110-3] BSI TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3: Common Specifications, Version 2.21, 21 December 2016

[TR-03110-4] BSI TR-03110-4, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 4: Applications and Document Profiles, Version 2.21, 21 December 2016

[USR] ID&Trust Identity Applet Suite User’s Guide, Version 3.4.1, 4 August 2020

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 https://www.sogis.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 per tutti i componenti di garanzia 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 EAL2, 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 https://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 "IDentity Applet v3.4/eIDAS on NXP JCOP 4 P71", nome abbreviato "IDentity Applet v3.4/eIDAS", sviluppato dalla società ID&Trust Ltd.

L'ODV è una smart card senza contatto con installata l'applet IDentity Applet Suite v3.4 configurata come IDentity Applet/eIDAS. L'ODV è un documento elettronico con tre applicazioni (ePassport, eID e eSign) conformi agli standard eIDAS pertinenti e fornisce tutti i protocolli di sicurezza necessari (PACE, EAC1 ed EAC2).

L'ODV è un prodotto composito e comprende:

- La Piattaforma sottostante dell'ODV: "NXP JCOP 4 P71", sviluppata da NXP Semiconductors Germany GmbH;
- La parte applicativa dell'ODV: "IDentity Applet v3.4/eIDAS";
- la documentazione operativa associata.

Pertanto, la valutazione è stata eseguita utilizzando i risultati della certificazione CC della Piattaforma [NXP-CR1] e seguendo le raccomandazioni contenute nel documento "Composite product evaluation for Smart Cards and similar devices" [JIL-COMP], 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).

La valutazione è di fatto iniziata nel 2016 su un ODV denominato "IDentity Applet v3.3/eIDAS on NXP JCOP 3 SECID P60 OSB Smart Card", basato sulla piattaforma JCOP 3. Durante la valutazione, il Committente ha deciso di aggiornare l'ODV alla piattaforma JCOP 4. Il nuovo ODV "IDentity Applet v3.4/eIDAS" ha esattamente le stesse funzionalità della versione 3.3 ma sulla piattaforma aggiornata. Pertanto, l'LVS CCLab Software Laboratory ha potuto utilizzare come base i risultati della valutazione in corso della versione 3.3.

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 e/o utilizzatori. 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 l'aggiunta di ALC_DVS.2, ATE_DPT.2 e AVA_VAN.5, in conformità a quanto

riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in ID&Trust Identity Applet Suite User's Guide [ADM];

- ID&Trust Identity Applet Suite Administrator's Guide [USR].

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 specifica l'esito della valutazione di sicurezza del prodotto "IDentity Applet v3.4/eIDAS" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato 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	IDentity Applet v3.4/eIDAS on NXP JCOP 4 P71
Traguardo di Sicurezza	"Security Target ID&Trust IDentity Applet v3.4/eIDAS – Electronic Identity Card with PACE-GM, PACE-CAM, Extended Access Control v1 and v2, Restricted Identification and Active Authentication", Version 1.02 [TDS]
Livello di garanzia	EAL4 con l'aggiunta di ALC_DVS.2, ATE_DPT.2 e AVA_VAN.5
Fornitore	ID&Trust Ltd.
Committente	NXP Semiconductors Netherlands B.V.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	BSI-CC-PP-0087 [PP-087] EN 419211-2:2013 [PPSSCD] BSI-CC-PP-0056-V2-2012 [PP-056] BSI-CC-PP-0086 [PP-086] BSI-CC-PP-0068-V2-2011-MA-01 [PP-068]
Data di inizio della valutazione	6 settembre 2016
Data di fine della valutazione	14 ottobre 2020

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 "IDentity Applet v3.4/eIDAS" è un circuito integrato (chip) senza contatto contenente i componenti per un documento di viaggio leggibile a macchina (MRTD), programmato secondo la Logical Data Structure (LDS) definita in [ICAO-TR1], che fornisce una soluzione eID altamente configurabile, in grado di soddisfare diversi requisiti applicativi anche all'interno di una singola istanza dell'applet. L'ODV è un documento elettronico con tre applicazioni conformi agli standard eIDAS pertinenti ([TR-03110-1], [TR-03110-2], [TR-03110-2]):

1. applicazione ePassport (passaporto elettronico);
2. applicazione eID (identità elettronica);
3. applicazione eSign (firma elettronica).

Sulla base del documento tecnico del BSI [TR-03110-4], l'ODV distingue tra le seguenti configurazioni:

- European Passport;
- Identity Card with Protected MRTD Application;
- Identity Card with EU-compliant MRTD Application.

Per maggiori informazioni sulle possibili configurazioni si consulti il par. 1.4.5 del TDS.

L'ODV fornisce anche tutti i protocolli di sicurezza necessari: PACE, EAC1 e EAC2. L'ODV può anche supportare funzionalmente il protocollo BAC, ma questo non rientra nella politica di sicurezza definita dal Traguardo di Sicurezza [TDS] e non è coperto dalla configurazione valutata dell'ODV.

L'ODV è un prodotto composito e comprende:

- La Piattaforma sottostante dell'ODV: "NXP JCOP 4 P71", sviluppata da NXP Semiconductors Germany GmbH, certificata CC a livello EAL6 con l'aggiunta di ASE_TSS.2 e ALC_FLR.1 [NXP-CR1]; questa comprende:
    a) Micro Controller (un controllore per smart card sicuro della famiglia SmartMX3 di NXP);
    b) IC Dedicated Software (Micro Controller Firmware e Crypto Library);
    c) IC Embedded Software JCOP 4 (Java Card Virtual Machine, Runtime Environment, Java Card API);
    d) Global Platform (GP) Framework;
- La parte applicativa dell'ODV: "IDentity Applet v3.4/eIDAS";
- la documentazione operativa associata.

L'utente previsto dell'ODV è l'ente emettitore del documento elettronico, che è responsabile della distribuzione delle smart card ai rispettivi titolari.

7.3.1 Architettura dell'ODV

L'ODV "IDentity Applet v3.4/eIDAS" è un prodotto composito risultante dall'unione degli elementi seguenti:

- la parte fisica del documento di viaggio, formata da un supporto in carta e/o plastica e un chip. Presenta dati leggibili a vista, inclusi, ma non limitati a, i dati personali del titolare del documento di viaggio:
    - i dati anagrafici nella pagina corrispondente sulla superficie del documento di viaggio;
    - i dati stampati nella Machine-Readable Zone (MRZ);
    - la foto del titolare.
- La parte logica del documento di viaggio, ossia i dati del titolare del documento di viaggio memorizzati secondo la Logical Data Structure (LDS) sul circuito integrato senza contatto, come specificato da ICAO in [ICAO-TR1]. Presenta dati leggibili senza contatto, inclusi, ma non limitati a, i dati personali del titolare del documento di viaggio:
    - I dati elettronici nella Machine-Readable Zone Data (digital MRZ data);
    - la foto digitalizzata del titolare;
    - i dati biometrici di riferimento (impronte digitali e/o immagini dell'iride);
    - altri dati in conformità alla LDS;
    - il Document Security Object (SO_D).

La Figura 1 mostra l'ambito logico e i confini dell'ODV.

L'ODV è un prodotto composito e la linea tratteggiata indica l'intero ODV. La piattaforma hardware certificata sottostante e il sistema operativo JCOP 4 sono contrassegnati in viola e in verde. La casella blu contrassegna lo strato applicativo. La ID&Trust IDentity Applet Suite v3.4 può essere caricata nella memoria Flash. Durante la fase di inizializzazione viene creata un'istanza dell'applet che, al termine di una serie di passaggi di configurazione, risulterà personalizzata come IDentity Applet v3.4/eIDAS.

Per una descrizione dettagliata dell'ODV si consulti il Traguardo di Sicurezza [TDS]; in particolare:

- le parti fisica e logica dell'ODV sono descritte nel par. 1.4.2 del TDS;
- il ciclo di vita dell'ODV, che si compone delle quattro fasi sviluppo, produzione, personalizzazione del documento elettronico e uso operativo, è descritto nel par. 1.4.3 del TDS, unitamente alle operazioni consentite agli utenti e agli amministratori per ciascuna fase;

- le caratteristiche dell'Applet sono descritte nel par. 1.4.5 del TDS.

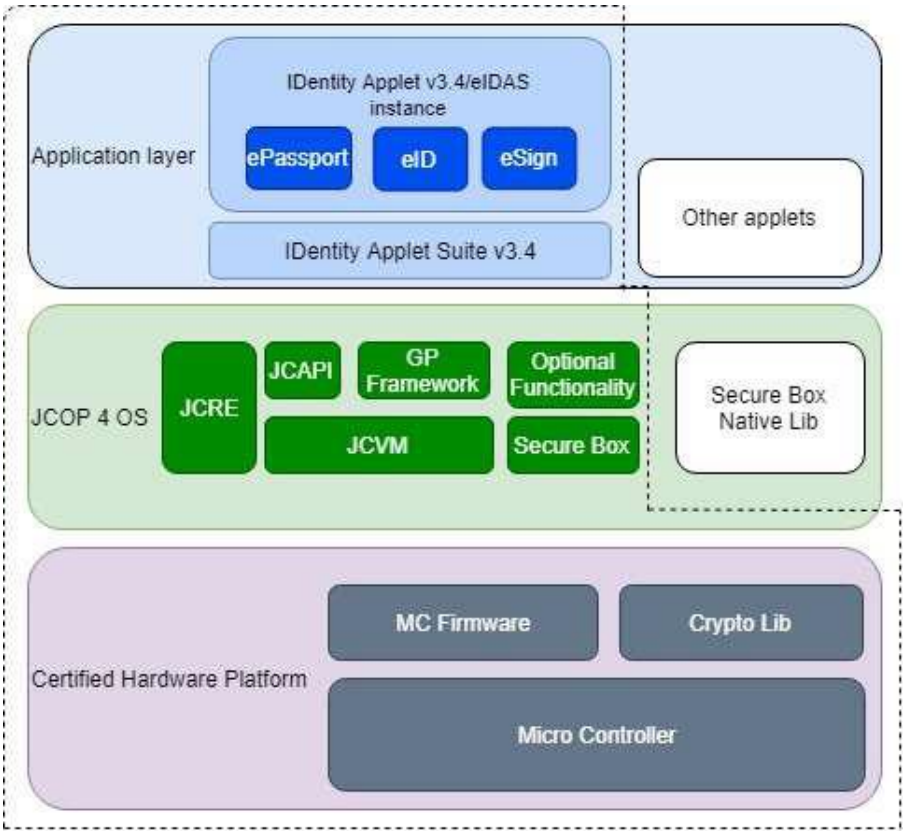

Figura 1 - Ambito logico e confini dell'ODV

7.3.2 Caratteristiche di sicurezza dell'ODV

7.3.2.1 Compatibilità con la Piattaforma

Alcuni aspetti relativi alle funzionalità di sicurezza dell'ODV, inclusi obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, sono coperti direttamente dalla Piattaforma. Per i dettagli consultare il par. 2.5 del Traguardo di Sicurezza [TDS].

7.3.2.2 Funzionalità ePassport (PACE)

PACE è un protocollo di scambio di chiavi Diffie-Hellman autenticato con password che fornisce una comunicazione sicura e l'autenticazione basata su password del chip eMRTD e del sistema di ispezione. PACE instaura un sistema sicuro di scambio messaggi (Secure Messaging) tra un chip eMRTD e un sistema di ispezione basato su password deboli (corte). Il contesto di sicurezza viene stabilito nel Master File. Il protocollo consente al chip eMRTD di verificare che il sistema di ispezione sia autorizzato ad accedere ai dati memorizzati ed ha le seguenti caratteristiche:

- fornisce chiavi di sessione complesse indipendentemente dalla robustezza della password;
- l'entropia delle password utilizzate per autenticare il sistema di ispezione può essere molto bassa.

PACE utilizza chiavi derivate dalle password mediante una funzione di derivazione di chiave. La chiave può essere derivata dalla Machine-Readable Zone (MRZ) o dal Card Access Number (CAN).

PACE supporta le seguenti mappature:

- Generic Mapping;
- Integrated Mapping;
- Chip Authentication Mapping.

L'implementazione di PACE di IDentity Applet v3.4/eIDAS utilizza i comandi READ BINARY, MSE: SET AT, GENERAL AUTHENTICATE.

Passaggi del protocollo Password Authenticated Connection Establishment:

- Il sistema di ispezione invia all'ODV un comando READ BINARY seguito da un comando MSE: SET AT (comando MANAGE SECURITY ENVIRONMENT con funzione SET Authentication Template).
- Come risultato di una catena di comandi GENERAL AUTHENTICATE, l'ODV genera in modo casuale e uniforme un *nonce*, lo cifra con la password condivisa precedentemente definita e invia il testo cifrato al sistema di ispezione.
- Il sistema di ispezione recupera il testo in chiaro mediante la password condivisa.
- L'ODV e il sistema di ispezione si scambiano dati aggiuntivi per la mappatura del *nonce*. Ad esempio, per il Generic Mapping vengono scambiate chiavi pubbliche effimere, mentre per l'Integrated Mapping l'ODV invia un ulteriore *nonce* al sistema di ispezione.
- Sia l'ODV, sia il sistema di ispezione calcolano i parametri di dominio effimero, eseguono uno scambio di chiavi Diffie-Hellman anonimo basato sui tali parametri e generano il segreto condiviso. Durante lo scambio di chiavi Diffie-Hellman, l'ODV controlla se le due chiavi pubbliche differiscono. Quindi vengono derivate le chiavi di sessione e l'ODV e il sistema di ispezione si scambiano e verificano il *token* di autenticazione.

Per i protocolli Diffie-Hellman e Diffie-Hellman a curva ellittica PACE utilizza gli algoritmi di cifratura 3DES o AES con lunghezza di chiave 112, 128, 192 o 256 bit. IDentity Applet v3.4/eIDAS utilizza esclusivamente curve ellittiche su campi primi con punti non compressi.

7.3.2.3 Funzionalità eID

La funzionalità dichiarata Extended Access Control 2 include il protocollo PACE sopra descritto e anche i seguenti protocolli conformi a [TR-03110-2]:

- *Chip Authentication Version 2*:
  Il Chip Authentication Protocol è un protocollo di scambio chiavi Diffie-Hellman effimero-statico che fornisce comunicazioni sicure e autenticazione unilaterale del

chip MRTD.
La versione 2 di questo protocollo fornisce autenticazione esplicita del chip MRTD, mediante verifica del *token* di autenticazione, e autenticazione implicita dei dati archiviati mediante Secure Messaging utilizzando la nuova chiave di sessione.
Se la Chip Authentication viene eseguita correttamente, il Secure Messaging viene riavviato utilizzando le chiavi di sessione derivate. In caso contrario, il Secure Messaging prosegue utilizzando la chiave di sessione stabilita in precedenza (PACE).

- *Terminal Authentication Version 2*:
  Il Terminal Authentication Protocol è un protocollo *challenge-response* a due mosse che fornisce autenticazione unilaterale esplicita del terminale.
  La Terminal Authentication consente al chip MRTD di verificare che il terminale sia autorizzato ad accedere ai dati sensibili. Poiché il terminale potrà in seguito accedere a dati sensibili, tutte le ulteriori comunicazioni dovranno essere protette in modo appropriato. La Terminal Authentication autentica quindi anche una chiave pubblica effimera scelta dal terminale che verrà utilizzata per instaurare il Secure Messaging col protocollo Chip Authentication Version 2. Il chip MRTD dovrà comunque vincolare i diritti di accesso del terminale al Secure Messaging instaurato mediante la chiave pubblica effimera autenticata del terminale.
  Se la Terminal Authentication viene eseguita con successo, il chip MRTD dovrà consentire l'accesso ai dati sensibili memorizzati in base all'effettiva autorizzazione del terminale autenticato. Il chip MRTD dovrà tuttavia limitare i diritti di accesso del terminale al Secure Messaging instaurato mediante la chiave pubblica effimera autenticata, ovvero il chip MRTD confronterà la rappresentazione compressa della chiave pubblica effimera del terminale, ricevuta come parte dell'autenticazione del terminale, con la rappresentazione compressa della chiave pubblica effimera fornita dal terminale come parte dell'autenticazione del chip. Il chip MRTD non deve accettare più di un'esecuzione della Terminal Authentication nella stessa sessione.

- *Restricted Identification*:
  Il Restricted Identification Protocol è un protocollo di scambio chiavi statico Diffie-Hellman che genera un identificatore specifico di settore del chip MRTD con le seguenti proprietà:
  - all'interno di ogni settore l'identificatore specifico di settore di ogni chip MRTD è univoco;
  - tra due settori qualsiasi, è impossibile da un punto di vista computazionale collegare gli identificatori specifici di settore di qualsiasi chip MRTD.

  L'identificatore specifico di settore viene utilizzato per (ri)identificare il chip MRTD all'interno di ciascun settore. La Chip Authentication e la Terminal Authentication devono essere state eseguite correttamente prima di utilizzare la Restricted Identification.
  Lo stato di sicurezza del chip MRTD non è influenzato dalla Restricted Identification.

7.3.2.4 Funzionalità QSCD

L'ODV in qualità di dispositivo per la creazione di firme qualificate (QSCD) è una combinazione di hardware e software configurata per creare, utilizzare e gestire in modo

sicuro i dati per la creazione di una firma (SCD). Il QSCD protegge gli SCD durante il loro intero ciclo di vita, facendo in modo che questi vengano utilizzati in un processo di creazione della firma esclusivamente dal loro titolare. Il QSCD comprende tutte le caratteristiche di sicurezza necessarie a garantire la riservatezza degli SCD e la sicurezza della firma elettronica, mediante le seguenti funzionalità:

- generazione degli SCD e dei corrispondenti SVD (Signature Verification Data);
- esportazione degli SVD mediante canale sicuro verso la CGA per la generazione del certificato;
- dimostrazione dell'identità dell'ODV come QSCD nei confronti di entità esterne;
- (opzionale) ricezione e memorizzazione delle informazioni sul certificato;
- commutazione dell'ODV da uno stato non operativo a uno stato operativo;
- nello stato operativo, creazione di firme elettroniche mediante i seguenti algoritmi crittografici:
    - RSASSA-PKCS1-v1_5 o RSASSA-PSS con lunghezze di chiave 2048-4096 bit;
    - ECDSA con lunghezze di chiave 160-521 bit.

Le firme elettroniche vengono create mediante i seguenti passaggi:

- selezione di un SCD se più SCD sono presenti nel QSCD;
- autenticazione del firmatario e determinazione della sua intenzione di firmare;
- ricezione del DTBS/R;
- applicazione al DTBS/R di una funzione crittografica adatta per la creazione di una firma utilizzando l'SCD selezionato.

La IDentity Applet v3.4/eIDAS esegue la creazione di firme elettroniche qualificate utilizzando i comandi "PSO: Hash" e "PSO: Compute Digital Signature". Il servizio viene eseguito in due passi. Il primo esegue l'ultimo round dell'*hash* parziale, mentre il secondo realizza il calcolo della firma elettronica sull'intero *hash* calcolato grazie al calcolo dell'ultimo round.

Fasi della creazione di una firma qualificata:

- L'IFD (Interface Device) esegue il calcolo dell'*hash* parziale sul messaggio M. I risultati del calcolo sono i seguenti:
    - PartialHash(M);
    - Counter(M);
    - RemainingMessage(M).
- L'IFD invia i dati di *hash* parziali alla scheda a circuito integrato e richiede il calcolo del round finale dell'*hash* utilizzando il comando "PSO: Hash".

- La scheda a circuito integrato inizializza il contesto di *hashing* con i dati in ingresso risultanti dal calcolo dell'*hash* parziale, quindi termina l'*hash* sull'ultimo blocco di dati, rendendo disponibile il valore Hash(M).

- L'IFD richiede il calcolo della firma utilizzando il comando "PSO: Compute Digital Signature".

- La scheda calcola la firma con la chiave privata selezionata e restituisce il risultato.

7.3.2.5 Funzioni di sicurezza

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il par. 7.1 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **AccessControl**: l'ODV fornisce i meccanismi di controllo di accesso che consentono il mantenimento dei diversi ruoli di sicurezza (Manufacturer, Personalisation Agent, Country Verifying Certification Authority, Document Verifier, Terminal, PACE Terminal, EAC2 o EAC1 Terminal a seconda della configurazione, Electronic Document Holder), e le politiche e le funzioni di controllo di accesso.

- **Authenticate**: l'ODV supporta diversi meccanismi per autenticare gli utenti, i terminali e per dimostrare l'autenticità del documento elettronico. I meccanismi e i protocolli supportati si basano sugli standard ICAO e BSI [ICAO-TR1], [ICAO-9303], [TR-03110-1], [TR-03110-2] e [TR-03110-3].

- **SecureManagement**: l'ODV gestisce in maniera sicura gli attributi, i dati e le funzioni di sicurezza. Inoltre, l'ODV limita l'uso dei comandi disponibili in ogni fase del proprio ciclo di vita.

- **CryptoKey**: l'ODV utilizza svariati servizi crittografici, come la creazione e la verifica di una firma elettronica, la crittografia asimmetrica e simmetrica, la generazione di numeri casuali e la gestione completa delle chiavi. Inoltre, la funzione CryptoKey fornisce la funzionalità di messaggistica sicura all'ODV.

- **AppletParametersSign**: l'ODV verifica la propria integrità in ognuna delle fasi del proprio ciclo di vita.

- **Platform**: copre le funzionalità di sicurezza basate su quelle della libreria crittografica certificata e della Piattaforma IC certificata.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

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. 8.3 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità *strict* al seguente Profilo di Protezione:

- BSI-CC-PP-0087, Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP), version 1.01, 20 May 2015 [PP-087]

Questo PP definisce i requisiti di sicurezza per una smart card programmata in conformità ai documenti tecnici [TR-03110-1] e [TR-03110-2]. La smart card può contenere una o più applicazioni. Nel suo insieme, la smart card programmata viene chiamata documento elettronico.

Il PP BSI-CC-PP-0087 dichiara a sua volta conformità *strict* ai seguenti PP:

- EN 419211-2:2013, Common Criteria Protection Profiles for Secure Signature Creation Device - Part 2: Device with key generation (BSI-CC-PP-0059-2009-MA-02) [PPSSCD]

- BSI-CC-PP-0056-V2-2012, Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012 [PP-056]

- BSI-CC-PP-0086, Protection Profile - Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2 PP), Version 1.01, 20 May 2015 [PP-086]

Poiché gli ultimi due PP sopra elencati dichiarano conformità *strict* al PP [PP-068], il PP BSI-CC-PP-0087 dichiara implicitamente conformità *strict* al seguente PP:

- BSI-CC-PP-0068-V2-2011-MA-01, Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22 July 2014 [PP-068]

Poiché il PP BSI-CC-PP-0087 dichiara conformità *strict* ai PP sopra elencati, il Traguardo di Sicurezza [TDS] dichiara a sua volta implicitamente conformità *strict* agli stessi PP.

La dichiarazione di conformità del TDS copre la parte della politica di sicurezza per l'applicazione eSign dell'ODV, corrispondente alla politica di sicurezza definita in [PPSSCD], ed è quindi applicabile nel caso in cui l'applicazione eSign è operativa.

7.6 Requisiti funzionali e di garanzia

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

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2].

Considerando che il Traguardo di Sicurezza dichiara conformità *strict* al Profilo di Protezione BSI-CC-PP-0087 [PP-087], sono inclusi anche tutti i requisiti funzionali estesi dichiarati in tale PP:

- FIA_API.1 della famiglia FIA_API: Authentication Proof of Identity
- FAU_SAS.1 della famiglia FAU_SAS: Audit data storage
- FCS_RND.1 della famiglia FCS_RND: Generation of random numbers
- FMT_LIM.1 e FMT_LIM.2 della famiglia FMT_LIM: Limited capabilities and availability
- FPT_EMS.1 della famiglia FPT_EMS: TOE Emanation

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, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

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" [JIL-COMP], come richiesto dagli accordi internazionali CCRA e SOGIS. In particolare, si precisa che i test di intrusione sono stati completati nel mese di agosto 2020, quindi entro 18 mesi dall'analisi di vulnerabilità effettuata sulla Piattaforma (31 maggio 2019, data del più vecchio "ETR for Composition" indicato nei rapporti di certificazione della Piattaforma [NXP-CR1] and [NXP-CR2]).

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 14 ottobre 2020 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 16 ottobre 2020. 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 ID&Trust Identity Applet Suite User's Guide [ADM];

- ID&Trust Identity Applet Suite Administrator's Guide [USR].

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 "IDentity Applet v3.4/eIDAS" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di ALC_DVS.2, ATE_DPT.2 e AVA_VAN.5, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in ID&Trust Identity Applet Suite User's Guide [ADM];

- ID&Trust Identity Applet Suite Administrator's Guide [USR].

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, ATE_DPT.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

Classi e componenti di garanzia		Verdetto
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
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: security enforcing modules	*ATE_DPT.2*	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 Attività di garanzia aggiuntive

Il documento di supporto obbligatorio “Composite product evaluation for Smart Cards and similar devices” [JIL-COMP] include requisiti di garanzia aggiuntivi specifici per questa tipologia di ODV composito.

Il documento definisce i raffinamenti ai requisiti di garanzia esistenti necessari per la valutazione di un prodotto composito. L’obiettivo di queste sotto-attività è definire con precisione i compiti del Valutatore per le diverse parti della valutazione di un ODV composito.

La Tabella 2 riassume i verdetti finali di ciascuna attività di garanzia specifica per la composizione svolta dall’LVS secondo quanto richiesto da [JIL-COMP].

Attività di garanzia specifiche per la composizione		Verdetto
ASE_COMP: Consistency of composite product Security Target	ASE_COMP.1	Positivo
ALC_COMP: Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1	Positivo
ADV_COMP: Composite design compliance	ADV_COMP.1	Positivo
ATE_COMP: Composite functional testing	ATE_COMP.1	Positivo
AVA_COMP: Composite vulnerability assessment	AVA_COMP.1	Positivo

Tabella 2 – Verdetti finali per le attività di garanzia specifiche per la composizione

8.3 Raccomandazioni

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

Si raccomanda ai potenziali acquirenti del prodotto "IDentity Applet v3.4/eIDAS" 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 cap. 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 dell'organizzazione e le ipotesi descritte rispettivamente nel par. 3.3 e nel par. 3.4 del TDS, in particolare quelle compatibili con la Piattaforma (si veda [TDS] par. 2.5).

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 ([ADM], [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 un prodotto composito, le procedure di consegna comportano interazioni tra lo sviluppatore dell'applicazione (ID&Trust Ltd.) e il produttore della piattaforma (NXP).

Le procedure di consegna tra ID&Trust e NXP prevedono quanto segue:

1. Lo sviluppatore (ID&Trust) realizza una nuova versione di IDentity Applet v3.4.

2. Dopo una fase di testa interna, la nuova versione viene rilasciata da ID&Trust e memorizzata nel sistema di gestione delle configurazioni dello sviluppatore.

3. La nuova versione di IDentity Applet v3.4 viene inviata a NXP.

4. NXP carica l'applet nel chip della Piattaforma.

La Piattaforma sottostante fornisce diverse funzioni di sicurezza per proteggere IDentity Applet v3.4 durante il trasporto tra le diverse entità coinvolte.

NXP offre due modalità di consegna del prodotto:

1. Ritiro ("Collection"): il cliente ritira il prodotto presso il sito di NXP.

2. Spedizione ("Shipment"): il prodotto viene inviato da NXP al cliente. Per garantire che non venga manomesso durante la consegna, il prodotto viene consegnato in pacchi sigillati con un nastro adesivo speciale. Il nastro è stampato con numeri consecutivi e presenta speciali caratteristiche adesive che rendono visibile qualsiasi manipolazione. Nel pacco è incluso un modulo da restituire a NXP a cura del cliente per informare il produttore che il pacco ricevuto non era danneggiato.

Entrambi i metodi di consegna garantiscono che il cliente riceva un prodotto autentico. Inoltre, il cliente può utilizzare una chiave crittografica speciale (Transport Key) per autenticare il chip.

Maggiori dettagli sulle procedure di consegna dell'ODV sono contenuti nel documento ID&Trust's IDentity Applet V3.4 Delivery Documentation [DEL].

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, i seguenti documenti contengono informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il

funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- ID&Trust Identity Applet Suite User's Guide [ADM];
- ID&Trust Identity Applet Suite Administrator's Guide [USR].

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "IDentity Applet v3.4/eIDAS on NXP JCOP 4 P71", nome abbreviato "IDentity Applet v3.4/eIDAS", sviluppato dalla società ID&Trust Ltd.

L'ODV è un prodotto composito e comprende i seguenti componenti HW/SW, che rappresentano la configurazione valutata dell'ODV, come riportato in [TDS], a cui si applicano i risultati della valutazione:

- La Piattaforma "NXP JCOP 4 P71", sviluppata da NXP Semiconductors Germany GmbH, certificata CC a livello EAL6 con l'aggiunta di ASE_TSS.2 e ALC_FLR.1 [NXP-CR1]; questa comprende:
    e) Micro Controller (un controllore per smart card sicuro della famiglia SmartMX3 di NXP);
    f) IC Dedicated Software (Micro Controller Firmware e Crypto Library);
    g) IC Embedded Software JCOP 4 (Java Card Virtual Machine, Runtime Environment, Java Card API);
    h) Global Platform (GP) Framework;
- La parte applicativa dell'ODV: "IDentity Applet v3.4/eIDAS" configurata come applicazione eMRTD;
- la documentazione operativa associata:
    - ID&Trust Identity Applet Suite User's Guide [ADM];
    - ID&Trust Identity Applet Suite Administrator's Guide [USR].

Il firmware del microcontrollore della Piattaforma e il software dedicato IC sono coperti dalla seguente certificazione: "NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library" [NXP-CR2].

Per maggiori dettagli, consultare il par. 1.4 del Traguardo di Sicurezza [TDS].

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, ATE_DPT.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 di queste attività è stato predisposto un ambiente di test presso la sede dell'LVS. Il Fornitore ha messo a disposizione dei Valutatori tutte le risorse necessarie per i test ad eccezione dello strumento di test e del lettore di schede.

In particolare, la configurazione di test dei Valutatori comprendeva:

- un esemplare dell'ODV su smart card identificato come IDentity Applet v3.4.7470/eIDAS;
- il lettore di smart card HID Omnikey 5x21 CL0;
- lo strumento di test OpenSCDP with Eclipse 2018-12.

Prima dell'esecuzione dei test, l'applicazione software è stata inizializzata e configurata in accordo alla documentazione operativa indicata nel par. 9.2 ([ADM] e [USR]). Il Fornitore ha messo a disposizione uno script di personalizzazione per l'installazione dell'ODV. I Valutatori sono stati in grado di installare correttamente l'ODV sulla Piattaforma sottostante. I Valutatori sono riusciti a leggere correttamente i dati dell'applet eID, a riprova che la scheda era stata installata correttamente e si trovava in uno stato noto.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

Il piano di test presentato dal Fornitore si è basato in gran parte sui seguenti documenti tecnici di riferimento del settore:

- ICAO Technical Report, Radio Frequency Protocol and Application Test Standard for eMRTD Part 3 - Tests for Application Protocol and Logical Data Structure, Version 2.10 [ICAO-TR2];
- BSI Technical Guideline 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, 6 April 2014 [BSI-TR1];

- BSI Technical Guideline TR-03105 Part 3.3: Test Plan for eID-Cards with Advanced Security Mechanisms - EAC 2, Version 1.03, 24 September 2010 [BSI-TR2];
- Amendment to BSI TR-03105 Part 3.3, Release 3, 04 June 2012 [BSI-TR2A];
- BSI Technical Guideline TR-03105 Part 3.4: Test plan for eID-Cards with eSign-application acc. to BSI TR-03117, Version 1.0, 01 April 2010 [BSI-TR3].

Inoltre, il Fornitore ha progettato in maniera indipendente ulteriori test proprietari al fine di dimostrare la copertura completa dei requisiti funzionali (SFR) e delle funzioni di sicurezza.

11.2.2 Copertura dei test

I Valutatori hanno esaminato il piano di test presentato dal Fornitore e hanno verificato la completa copertura dei requisiti funzionali (SFR) e delle TSFI descritte nelle specifiche funzionali.

11.2.3 Risultati dei test

I Valutatori hanno eseguito una serie di test, scelti a campione tra quelli descritti nel piano di test presentato dal Fornitore, allo scopo di verificare la ripetibilità e la riproducibilità sia dei test standard di settore, sia di quelli proprietari. I Valutatori hanno confrontato i risultati ottenuti da questi test con i risultati attesi definiti nelle specifiche di test del Fornitore, verificandone la piena corrispondenza.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

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

Il TSF include un gran numero di interfacce, cosa che rende poco pratico testarle tutte rigorosamente. Pertanto, i Valutatori hanno deciso di concentrarsi sulla verifica dell'immutabilità dei dati essenziali memorizzati nell'ODV, utilizzando una strategia di campionamento per testare le seguenti interfacce:

- PUT DATA
- Test approfonditi per tutte le possibili TSFI non documentate

I Valutatori hanno verificato i risultati effettivi dei test e ne hanno riscontrato la coerenza con i risultati attesi.

Inoltre, considerando che l'ODV è un prodotto composito, i Valutatori hanno verificato il comportamento dell'ODV nel suo complesso, svolgendo le attività aggiuntive specificate dalla famiglia ATE_COMP, conformemente al documento [JIL-COMP], tenendo anche in considerazione gli obblighi e le raccomandazioni per il Valutatore dell'applet inclusi nel documento "ETR for Composition" [ETR-COMP] della Piattaforma.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività i Valutatori hanno lavorato sullo stesso campione dell'ODV già utilizzato per le attività dei test funzionali, verificando che la configurazione di test fosse congruente con la versione dell'ODV in valutazione.

Poiché l'ODV è un prodotto composito, i Valutatori hanno svolto le attività aggiuntive specificate dalla famiglia AVA_COMP, conformemente al documento [JIL-COMP], ed hanno esaminato i risultati dell'analisi di vulnerabilità nel documento "ETR for Composition" [ETR-COMP] per verificare che potessero essere riutilizzati per la valutazione composita dell'applet.

I Valutatori hanno utilizzato due diversi approcci: è stata impiegata una strategia di campionamento per testare le funzionalità di un sottoinsieme di TSFI invece di testare tutte le interfacce, ed è stato implementato ed eseguito un attacco a forza bruta per scoprire eventuali API non documentate. Considerando che si tratta di un prodotto composito, i Valutatori hanno verificato il comportamento dell'ODV nel suo complesso.

La prima fase dell'analisi di vulnerabilità è consistita nella raccolta di informazioni sull'ODV. Come prima cosa, sono state condotte svariate ricerche da fonti pubbliche con diverse combinazioni di parole chiave (ad esempio, "Electronic ID vulnerabilities", "penetration testing electronic travel documents", "electronic passport security flaws", "eID") per identificare le falle e le vulnerabilità dell'ODV di pubblico dominio. In questa fase sono stati esaminati anche database pubblici di vulnerabilità e pubblicazioni tecniche di ricerca. Le vulnerabilità note pubblicamente sono risultate obsolete o rilevanti solo per la Piattaforma sottostante, che non rientra nell'ambito della valutazione. Al termine di questa fase, i Valutatori hanno concluso che la tecnologia delle smart card è ben documentata e un potenziale attaccante è in grado di comprendere a fondo il funzionamento di un passaporto elettronico sulla base degli standard di riferimento del settore e delle informazioni disponibili pubblicamente sulle smart card. La documentazione dell'ODV non è disponibile pubblicamente (cioè, non è reperibile sul sito Web del produttore). Questa informazione è stata considerata rilevante per il calcolo del potenziale di attacco. Sulla base delle informazioni pubblicamente disponibili, non è stata individuata alcuna vulnerabilità nota rilevante per l'ODV.

In una seconda fase, i Valutatori hanno analizzato la documentazione del produttore allo scopo di familiarizzare con l'ODV e con le sue funzionalità di identificazione elettronica, ed identificare potenziali superfici di attacco. Come accennato in precedenza, non è disponibile pubblicamente alcuna documentazione sul sito Web del produttore. I Valutatori hanno esaminato le funzionalità dell'ODV sulla base della documentazione e utilizzando gli strumenti forniti dal produttore della piattaforma sottostante per interagire con le interfacce dell'ODV. Durante questa fase, i Valutatori hanno identificato possibili vettori di attacco relativi a possibili interfacce non documentate. In considerazione della tipologia di prodotto dell'ODV e della rigorosa standardizzazione nel settore delle smart card, i Valutatori si sono concentrati sulle potenziali vulnerabilità e sui test relativi all'implementazione delle funzionalità di autenticazione. Sulla base delle informazioni raccolte, i Valutatori hanno stabilito che le vulnerabilità potenziali legate all'autenticazione dovessero essere oggetto di indagine.

Una volta raccolte tutte le informazioni necessarie sull'ODV e sulle potenziali vulnerabilità, i Valutatori hanno realizzato un piano di test suddiviso in diversi scenari di attacco per

soddisfare i requisiti di AVA_VAN.5. Per ogni scenario di attacco è stato calcolato l'esatto potenziale di attacco, considerando che le informazioni pubblicamente disponibili sulle smart card sono molto dettagliate, ricche e relativamente facili da apprendere.

Una volta definiti gli scenari di attacco, i Valutatori hanno condotto test di penetrazione sulle funzionalità dell'ODV per identificare eventuali vulnerabilità sfruttabili.

I Valutatori hanno definito i seguenti scenari di attacco:

- L'attaccante tenta di effettuare una verifica del PIN forzata attraverso un canale non sicuro. Se l'attacco venisse condotto con successo, si avrebbero a disposizione nuove superfici di attacco in quanto i dati sensibili e relativi alla sicurezza potrebbero essere intercettati utilizzando attacchi di tipo *man-in-the-middle*.

- L'attaccante tenta di modificare dati sensibili e non modificabili nell'applicazione. Se l'attacco venisse condotto con successo, verrebbero violati i necessari protocolli di sicurezza, rendendo il bersaglio non conforme agli standard eIDAS pertinenti in quanto possibile oggetto di contraffazione.

- L'attaccante scopre un'interfaccia non documentata. Questa interfaccia potrebbe costituire un'ulteriore superficie di attacco.

Sulla base degli scenari di attacco sopra descritti, i Valutatori hanno quindi tentato di penetrare la protezione dell'ODV mediante test di intrusione.

I risultati dei test sono stati documentati con dettagli sufficienti per la loro ripetibilità e i risultati sono stati anche raccolti in una tabella per motivi di chiarezza.

I test di intrusione eseguiti non hanno permesso di identificare vulnerabilità dell'ODV sfruttabili con potenziale di attacco High.

Durante le visite al sito del Fornitore, i Valutatori hanno eseguito un'analisi del codice sorgente concentrandosi prevalentemente sull'implementazione delle funzionalità di autenticazione e sulle contromisure applicate contro gli attacchi di tipo *side channel* e *fault injection*.

Sulla base delle informazioni disponibili, i Valutatori non hanno individuato vulnerabilità residue, ovvero vulnerabilità che potrebbero essere sfruttate solo da attaccanti con potenziale di attacco superiore a High.