



*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

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. 10/21**

*(Certification No.)*

**Prodotto: IDentity Applet v3.4-p1/QSCD 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+**  
**(AVA\_VAN.5)**

Il Direttore  
(Dott.ssa Eva Spina)

Roma, 11 ottobre 2021



Fino a EAL2 (*Up to EAL2*)



Fino a EAL4 (*Up to EAL4*)





*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-p1/QSCD on NXP JCOP 4 P71**

OCSI/CERT/CCL/07/2021/RC

Versione 1.0

11 ottobre 2021

Questa pagina è lasciata intenzionalmente vuota

## 1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	11/10/2021

## 2 Indice

1	Revisioni del documento .....	5
2	Indice.....	6
3	Elenco degli acronimi .....	8
4	Riferimenti.....	11
4.1	Criteri e normative .....	11
4.2	Documenti tecnici.....	12
5	Riconoscimento del certificato .....	14
5.1	Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA).....	14
5.2	Riconoscimento di certificati CC in ambito internazionale (CCRA).....	14
6	Dichiarazione di certificazione.....	15
7	Riepilogo della valutazione .....	17
7.1	Introduzione.....	17
7.2	Identificazione sintetica della certificazione.....	17
7.3	Prodotto valutato .....	17
7.3.1	Architettura dell'ODV.....	19
7.3.2	Caratteristiche di sicurezza dell'ODV .....	20
7.4	Documentazione .....	22
7.5	Conformità a Profili di Protezione .....	22
7.6	Requisiti funzionali e di garanzia .....	22
7.7	Conduzione della valutazione.....	23
7.8	Considerazioni generali sulla validità della certificazione .....	23
8	Esito della valutazione.....	24
8.1	Risultato della valutazione .....	24
8.2	Attività di garanzia aggiuntive .....	25
8.3	Raccomandazioni.....	26
9	Appendice A – Indicazioni per l'uso sicuro del prodotto.....	27
9.1	Consegna .....	27
9.2	Installazione, inizializzazione e utilizzo sicuro dell'ODV .....	27
10	Appendice B – Configurazione valutata.....	29
11	Appendice C – Attività di Test.....	30

11.1	Configurazione per i Test.....	30
11.2	Test funzionali svolti dal Fornitore .....	30
11.2.1	Approccio adottato per i test .....	30
11.2.2	Copertura dei test.....	31
11.2.3	Risultati dei test .....	31
11.3	Test funzionali ed indipendenti svolti dai Valutatori .....	31
11.4	Analisi delle vulnerabilità e test di intrusione.....	31

### 3 Elenco degli acronimi

<b>AES</b>	Advanced Encryption Standard
<b>API</b>	Application Programming Interface
<b>CC</b>	Common Criteria
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CEM</b>	Common Evaluation Methodology
<b>CGA</b>	Certificate Generation Application
<b>CRS</b>	Certificate Request Signature
<b>CSP</b>	Certification Service Provider
<b>DES</b>	Data Encryption Standard
<b>DPCM</b>	Decreto del Presidente del Consiglio dei Ministri
<b>DTBS/R</b>	Data To Be Signed / Representation
<b>EAL</b>	Evaluation Assurance Level
<b>ECC</b>	Elliptic Curve Cryptography
<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
<b>eIDAS</b>	electronic IDentification Authentication and Signature
<b>eMRTD</b>	Electronic Machine Readable Travel Document
<b>ETR</b>	Evaluation Technical Report
<b>GP</b>	Global Platform
<b>HW</b>	Hardware
<b>IAS-ECC</b>	Identification, Authentication and electronic Signature - European Citizen Card
<b>ICAO</b>	International Civil Aviation Organization
<b>IC</b>	Integrated Circuit
<b>IT</b>	Information Technology
<b>JCOP</b>	Java Card Open Platform
<b>JCRE</b>	Java Card Runtime Environment



<b>JCVM</b>	Java Card Virtual Machine
<b>LGP</b>	Linea Guida Provvisoria
<b>LVS</b>	Laboratorio per la Valutazione della Sicurezza
<b>MMU</b>	Memory Management Unit
<b>NIS</b>	Nota Informativa dello Schema
<b>OCSI</b>	Organismo di Certificazione della Sicurezza Informatica
<b>ODV</b>	Oggetto della Valutazione
<b>OS</b>	Operating System
<b>PIN</b>	Personal Identification Number
<b>PKCC</b>	Public Key Crypto Coprocessor
<b>PP</b>	Profilo di Protezione (Protection Profile)
<b>QSCD</b>	Qualified Signature Creation Device
<b>QTSP</b>	Qualified Trust Service Provider
<b>RAD</b>	Reference Authentication Data
<b>RAM</b>	Random Access Memory
<b>RSA</b>	Rivest, Shamir, Adleman
<b>RFV</b>	Rapporto Finale di Valutazione
<b>SAR</b>	Security Assurance Requirement
<b>SCA</b>	Signature Creation Application
<b>SCD</b>	Signature Creation Data
<b>SFR</b>	Security Functional Requirement
<b>SOGIS</b>	Senior Officials Group Information Systems Security
<b>ST</b>	Security Target
<b>SVD</b>	Signature Verification Data
<b>SW</b>	Software
<b>TDS</b>	Traguardo di Sicurezza
<b>TOE</b>	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 - Accredimento 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-TR] 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] ETR for Composite Evaluation NXP “JCOP 4 P71” – EAL6+, 19-RPT-177, Version 8.0, 25 February 2021
- [IAS-ECC] European Card for e-Services and National e-ID Applications - IAS ECC, Revision 1.0.1, 23 February 2009
- [ICAO-TR] 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-CR3, TÜV Rheinland Nederland B.V., 1<sup>st</sup> March 2021
- [NXP-CR2] Certification Report “NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2)”, BSI-DSZ-CC-1136-2021, BSI - Bundesamt für Sicherheit in der Informationstechnik, 10 February 2021
- [PPQSCD1] EN 419211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation
- [PPQSCD2] EN 419211-4:2013, Protection profiles for Secure signature creation device - Part 4: Device with key generation and trusted communication with certificate generation application
- [RC] Rapporto di Certificazione “IDentity Applet v3.4/QSCD on NXP JCOP 4 P71”, OCSI/CERT/SYS/07/2016/RC, Versione 1.0, 28 ottobre 2020
- [RFV] “ID&Trust IDentity Applet v3.4-p1/QSCD” Evaluation Technical Report, v1, CCLab Software Laboratory, 2 September 2021

[TDS] “Security Target IDentity Applet v3.4-p1/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS”, Version 1.05, ID&Trust Ltd., 28 June 2021

[USR] ID&Trust IDentity Applet Suite User’s Guide, Version 3.4.2, 8 June 2021

## **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-p1/QSCD on NXP JCOP 4 P71", nome abbreviato "IDentity Applet v3.4/QSCD", sviluppato dalla società ID&Trust Ltd.

L'ODV è un dispositivo per la creazione di una firma elettronica qualificata (QSCD) costituito da una smart card a contatto o senza contatto in grado di generare i dati per la creazione di una firma (SCD) e creare firme elettroniche qualificate. L'ODV protegge gli SCD e garantisce che solo un firmatario autorizzato possa utilizzarli.

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/QSCD";
- 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).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (IDentity Applet v3.4/QSCD on NXP JCOP 4 P71), già certificato dall'OCSI (Certificato n. 11/20 del 28 ottobre 2020 [RC]).

In seguito ad alcune modifiche di lieve entità apportate al prodotto da parte del ID&Trust Ltd., è stato necessario procedere a una ri-certificazione dell'ODV. L'aggiornamento dell'ODV si è reso necessario a seguito della richiesta da parte di un cliente della piena conformità con [IAS-ECC] e della relativa convalida dell'implementazione mediante la suite di test KEOLABS.

A tale scopo, il Fornitore ha risolto un problema minore a causa del quale, quando veniva utilizzato un algoritmo di scambio chiavi IAS-ECC, le chiavi di sessione memorizzate venivano eliminate e i diritti di accesso al terminale venivano ripristinati in caso di interruzione del Secure Messaging.

La modifica effettuata esula dall'ambito dell'ODV e non ha alcun impatto sul TSF. L'LVS CCLab Software Laboratory ha ripetuto parte delle attività di valutazione riutilizzando la documentazione e le evidenze già fornite nella precedente valutazione. Le attività di test

funzionali e di analisi di vulnerabilità sono state interamente ripetute.

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente ODV, per facilità di lettura il presente Rapporto di Certificazione è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo ODV "IDentity Applet v3.4/QSCD on NXP JCOP 4 P71".

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 AVA\_VAN.5, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

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



## 7 Riepilogo della valutazione

### 7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "IDentity Applet v3.4/QSCD" 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

<b>Nome dell'ODV</b>	IDentity Applet v3.4-p1/QSCD on NXP JCOP 4 P71
<b>Traguardo di Sicurezza</b>	"Security Target IDentity Applet v3.4-p1/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS", Version 1.05 [TDS]
<b>Livello di garanzia</b>	EAL4 con l'aggiunta di AVA_VAN.5
<b>Fornitore</b>	ID&Trust Ltd.
<b>Committente</b>	NXP Semiconductors Netherlands B.V.
<b>LVS</b>	CCLab Software Laboratory
<b>Versione dei CC</b>	3.1 Rev. 5
<b>Conformità a PP</b>	EN 419 211-2:2013 [PPQSCD1] EN 419 211-4:2013 [PPQSCD2]
<b>Data di inizio della valutazione</b>	28 giugno 2021
<b>Data di fine della valutazione</b>	2 settembre 2021

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/QSCD" è composta da una smart card e da un'applet programmata per implementare un dispositivo per la creazione di una firma elettronica qualificata (QSCD) conforme al Regolamento (UE) n. 910/2014 [eIDAS].

L'ODV implementa la generazione di dati per la creazione di una firma (SCD) e la creazione di firme elettroniche qualificate. Inoltre, l'ODV supporta la propria autenticazione come QSCD nei confronti della CGA (Certificate Generation Application) del prestatore di servizi di certificazione (CSP) e la comunicazione sicura con la CGA per la protezione dei dati di verifica della firma (SVD) generati ed esportati dall'ODV e importati dalla CGA.

L'ODV memorizza gli SCD e i RAD (Reference Authentication Data). L'ODV può memorizzare più istanze di SCD. In questo caso, l'ODV fornisce una funzione per identificare univocamente ogni SCD e la SCA (Signature Creation Application) può fornire un'interfaccia al firmatario per selezionare un SCD da utilizzare nella funzione di creazione della firma del QSCD.

L'ODV protegge la riservatezza e l'integrità degli SCD e ne limita l'uso per la creazione di una firma al titolare. L'ODV comprende tutte le funzionalità di sicurezza necessarie per garantire la riservatezza degli SCD e la sicurezza della firma elettronica. La funzionalità di firma elettronica dell'ODV può essere utilizzata per creare una firma elettronica qualificata conforme a [eIDAS].

L'ODV implementa il protocollo proprietario CRS (Certificate Request Signature) per fornire prova della validità degli SVD alla CGA. Il protocollo CRS consente anche di dimostrare che gli SVD sono connessi all'ODV.

Il protocollo CRS utilizza una coppia di chiavi generata dall'ODV separatamente dalla coppia di chiavi SCD/SVD; all'atto della generazione della coppia di chiavi SCD/SVD, l'ODV firma l'SVD con la chiave privata del CRS. La CGA è quindi in grado di verificare la validità dell'SVD controllando il CRS.

L'ODV può implementare funzioni e requisiti di sicurezza aggiuntivi, ad esempio per la modifica e la visualizzazione dei dati da firmare (DTBS/R), ma questi non rientrano nella politica di sicurezza definita nel Traguardo di Sicurezza [TDS] e non sono coperti 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/QSCD";
- la documentazione operativa associata.

L'utente previsto dell'ODV è il servizio emettitore del QSCD, che prepara l'ODV come QSCD per i suoi utenti, lo personalizza con l'identità del titolare legittimo in qualità di firmatario e lo consegna al firmatario stesso.

Al termine della fase di preparazione, gli SCD devono trovarsi in uno stato non operativo. Dopo aver ricevuto l'ODV, il firmatario deve verificare che questo si trovi nello stato non operativo e modificare lo stato degli SCD in operativo.

### 7.3.1 Architettura dell'ODV

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

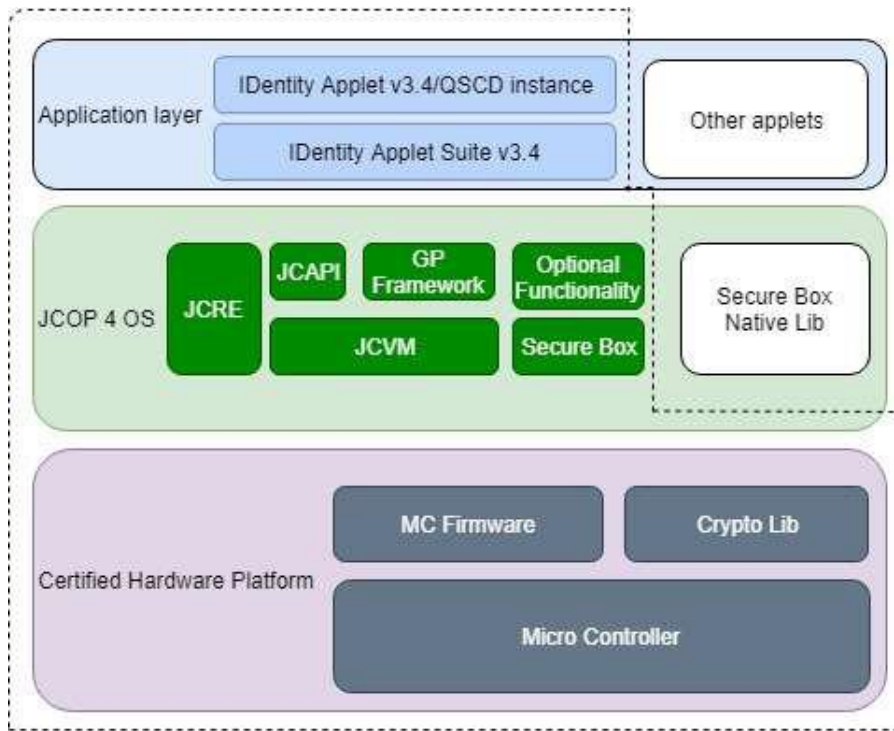


Figura 1 - Ambito logico e confini dell'ODV

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/QSCD.

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 fasi sviluppo, preparazione e uso operativo, è descritto nel par. 1.4.5 del TDS;

- le caratteristiche di sicurezza dell'ODV sono descritte nel par. 1.4.6 del TDS.

## 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. 2.4 del Trattamento di Sicurezza [TDS].

### 7.3.2.2 *Funzionalità QSCD*

L'ODV in qualità di dispositivo per la creazione di firme qualificate (QSCD) prevede i seguenti ambienti operativi distinti:

- L'ambiente di preparazione, in cui interagisce con la CGA di un CSP per ottenere un certificato per gli SVD corrispondenti agli SCD generati dall'ODV. L'ODV esporta gli SVD attraverso un canale sicuro consentendo alla CGA di verificarne l'autenticità. L'ambiente di inizializzazione interagisce ulteriormente con l'ODV per personalizzarlo con il valore iniziale dei RAD.
- L'ambiente di firma, in cui interagisce con il titolare tramite una SCA per firmare i dati dopo averlo autenticato come firmatario legittimo. La SCA fornisce la rappresentazione univoca dei dati da firmare (DTBS/R) come input per la funzione di creazione della firma dell'ODV e ne ottiene la firma elettronica risultante.
- L'ambiente di gestione, in cui interagisce con l'utente o un prestatore di servizi fiduciari qualificati (QTSP) per eseguire operazioni di gestione, ad esempio per reimpostare un RAD bloccato per un firmatario. Un singolo dispositivo, ad esempio un terminale per smart card, può fornire l'ambiente protetto richiesto per le operazioni di gestione e di firma.

L'ODV 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 di una coppia SCD/SVD mediante uno dei seguenti algoritmi di generazione di chiavi crittografiche:
  - RSA con lunghezze di chiave 1024-4096 bit;
  - ECC con lunghezze di chiave 160-521 bit.
- 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 digitali 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 digitali 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.

### 7.3.2.3 Funzioni di sicurezza

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

- **AccessControl:** questa funzione fornisce i controlli di accesso ai dati nel file system e ai dati di inizializzazione, personalizzazione e pre-personalizzazione. Durante le prime fasi del ciclo di vita, quando l'applet potrebbe non essere ancora stata installata, la Piattaforma è responsabile della corretta gestione degli accessi. L'ODV fornisce meccanismi di controllo di accesso che consentono il mantenimento di diversi ruoli di sicurezza (Signatory e Administrator), e le politiche e le funzioni di controllo di accesso.
- **Authenticate:** questa funzione gestisce l'identificazione e l'autenticazione del firmatario e dell'amministratore e impone la separazione dei ruoli. Successivamente all'attivazione o al ripristino dell'ODV nessun utente risulta autenticato. Le azioni mediate dal TSF per conto di un utente richiedono la previa identificazione e autenticazione dell'utente stesso.
- **SecureManagement:** tutti gli attributi di sicurezza vengono modificati in modo sicuro, così da rendere impossibili modifiche non autorizzate. Questa funzione è responsabile della gestione sicura degli attributi, dei dati e delle funzioni di sicurezza.
- **CryptoKey:** questa funzione fornisce il supporto crittografico al TSF, inclusa la generazione sicura di chiavi (coppia di chiavi SCD/SVD), la creazione di firme elettroniche. Inoltre, la funzione CryptoKey fornisce un metodo sicuro di distruzione delle chiavi.
- **AppletParametersSign:** alcuni parametri di configurazione e controllo sono firmati e questa firma viene verificata prima di chiudere la fase di inizializzazione. Solo i parametri non firmati possono essere modificati durante l'inizializzazione. In questo

modo possono essere applicati solamente i profili applicativi (Application Profiles) che sono validati dallo sviluppatore e conformi ai requisiti. In mancanza della corretta verifica delle firme, la fase di inizializzazione non può essere completata raggiungendo lo stato INITIALIZED e la fase di personalizzazione non può essere avviata. Queste firme possono essere verificate durante l'intero ciclo di vita della Identity Applet, rendendo possibile rilevare modifiche non autorizzate mediante l'applicazione di questa funzionalità di sicurezza.

- **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* ai seguenti Profili di Protezione:

- EN 419211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation [PPQSCD1]
- EN 419211-4:2013, Protection profiles for Secure signature creation device - Part 4: Device with key generation and trusted communication with certificate generation application [PPQSCD2]

## 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* ai Profili di Protezione EN 419211-2:2013 [PPQSCD1] e EN 419211-4:2013 [PPQSCD2], sono inclusi anche i seguenti requisiti funzionali estesi dichiarati in tali PP:

- FIA\_API.1 della famiglia FIA\_API: Authentication Proof of Identity
- 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 2021, quindi entro 18 mesi dall'analisi di vulnerabilità effettuata sulla Piattaforma (5 febbraio 2021, 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 2 settembre 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 24 settembre 2021. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

## 7.8 Considerazioni generali sulla validità della certificazione

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

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

## 8 Esito della valutazione

### 8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS CCLab Software Laboratory e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "IDentity Applet v3.4/QSCD" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di AVA\_VAN.5, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

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

Classi e componenti di garanzia		Verdetto
<b>Security Target evaluation</b>	<b>Classe ASE</b>	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
<b>Development</b>	<b>Classe ADV</b>	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
<b>Guidance documents</b>	<b>Classe AGD</b>	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
<b>Life cycle support</b>	<b>Classe ALC</b>	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo
Delivery procedures	ALC_DEL.1	Positivo



Classi e componenti di garanzia		Verdetto
Identification of security measures	ALC_DVS.1	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
<b>Test</b>	<b>Classe ATE</b>	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
<b>Vulnerability assessment</b>	<b>Classe AVA</b>	Positivo
<i>Advanced methodical vulnerability analysis</i>	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
<b>ASE_COMP: Consistency of composite product Security Target</b>	ASE_COMP.1	Positivo
<b>ALC_COMP: Integration of composition parts and consistency check of delivery procedures</b>	ALC_COMP.1	Positivo
<b>ADV_COMP: Composite design compliance</b>	ADV_COMP.1	Positivo
<b>ATE_COMP: Composite functional testing</b>	ATE_COMP.1	Positivo
<b>AVA_COMP: Composite vulnerability assessment</b>	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/QSCD" 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. 2.4).

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 Trapianto 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-p1/QSCD on NXP JCOP 4 P71", nome abbreviato "IDentity Applet v3.4/QSCD", sviluppato dalla società ID&Trust Ltd.

L'ODV è un prodotto composto 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/QSCD" 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 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/QSCD 015A;
- il lettore di smart card Omnikey HID 5022 CL;
- lo strumento di test OpenSCDP, GlobalTester.

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 selezionare correttamente l'applet QSCD, 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-TR];
- 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-TR].

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, "Qualified Signature Creation Device vulnerabilities", "tampering with electronic signature devices", "QSCD") 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 dispositivo di firma elettronica 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 firma 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 firma elettronica. 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 sbloccare un PIN dell'applicazione eSIGN precedentemente bloccato aggirando l'autenticazione richiesta per tale operazione.



- L'attaccante tenta di modificare i dati sensibili dell'applicazione eSIGN necessari per il suo funzionamento corretto e sicuro.
- 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.