E-HITELES FORDÍTÁS | E-CERTIFIED TRANSLATION

Az 1x1 Fordítóiroda nevében ezúton igazoljuk, hogy a mellékelt fordítás a szintén mellékelt eredeti szöveggel tartalmilag megegyezik.	On behalf of 1x1 Translations we do hereby certify that the translation attached is a true and accurate rendition of the original text as attached.

Kelt: Budapesten, 2021. augusztus 17. Issued in: Budapest, on 17 August 2021

e-SZIGNO secured trusted site	TÁJÉKOZTATÁS	E dokumentum elektronikus aláírással lett ellátva. A jelen dokumentum kinyomtatva is bizonyító erejű okiratnak minősül.
	INFORMATION	This document was electronically signed. A printout of this document has the probative force of an authentic document.

1x1 FORDÍTÓIRODA 1x1

Csobay-Novák Tamás

1x1 TRANSLATIONS

Tel.: +36 70 33 24 905
Skype: onebyonetranslation
@ info@1x1forditoiroda.hu
Web: www.1x1forditoiroda.hu

Gazdaságfejlesztési Minisztérium
Híradástechnikai és Információbiztonsági Főigazgatóság Felsőfokú Hírközlési és Informatikai Intézet

OCSI
Organismo di Certificazione della Sicurezza Informatica

Az IKT-rendszerek és -termékek biztonsági értékelésének és tanúsításának nemzeti rendszere (2003. október 30-i DPCM - 2004. április 27-i G.U. n. 93)

11/20.sz. tanúsítvány
(Certification No.)

Termék: **IDentity Applet v3.4/QSCD on NXP JCOP 4 P71**
(Product)

Fejlesztő: **ID&Trust Ltd.**
(Developed by)

Az ebben a tanúsítványban feltüntetett termékről megállapították, hogy megfelel az ISO/IEC 15408 (Common Criteria) v. 3.1. szabvány követelményeinek a megbízhatósági szint tekintetében:

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)

Az Igazgató
(Dott.ssa Eva Spina)

Róma, 2020. október 28.

Eva Spina digitális aláírásával. Dátum: 2020.10.28. 16:57:39 +01'00'

Common Criteria

EAL2-ig *(Up to EAL2)*

EAL4-ig *(Up to EAL4)*

Ezt az oldalt szándékosan üresen hagytuk

Gazdaságfejlesztési Minisztérium

Híradástechnikai és Információbiztonsági Főigazgatóság Felsőfokú Hírközlési és Informatikai Intézet

Organismo di Certificazione della Sicurezza Informatica

Tanúsítási jelentés

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

OCSI/CERT/SYS/07/2016/RC

1.0 verzió

2020. október 28.

Ezt az oldalt szándékosan üresen hagytuk

1 A dokumentum felülvizsgálata

Verzió	Szerzők	Módosítások	Dátum
1.0	OCSI	Első kiadás	2020. október 28.

2 Tartalomjegyzék

3 A betűszavak jegyzéke

AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria (Közös Kritériumok)
CCRA	Arrangement on the Recognition of Common Criteria (Közös Kritériumok elismeréséről szóló megállapodás)
CEM	Common Evaluation Methodology (közös értékelési módszertan)
CGA	Certificate Generation Application
CRS	Certificate Request Signature
CSP	Certification Service Provider
DES	Data Encryption Standard
DPCM	Decreto del Presidente del Consiglio dei Ministri (A Minisztertanács elnökének rendelete)
DTBS/R	Data To Be Signed / Representation
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
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	Hardver
ICAO	International Civil Aviation Organization
IC	Integrated Circuit
IT	Information Technology
JCOP	Java Card Open Platform
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine

LGP	Linea Guida Provvisoria (Ideiglenes irányelv)
LVS	Laboratorio per la Valutazione della Sicurezza (Biztonságértékelő laboratórium)
MMU	Memory Management Unit
NIS	Nota Informativa dello Schema (A rendszer tájékoztatója)
OCSI	Organismo di Certificazione della Sicurezza Informatica (IT-biztonsági tanúsító testület)
ODV	Oggetto della Valutazione (Az értékelés tárgya)
OS	Operating System (Operációs rendszer)
PIN	Personal Identification Number (Személyi azonosító szám)
PKCC	Public Key Crypto Coprocessor
PP	Profilo di Protezione (Protection Profile)
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
RAD	Reference Authentication Data
RAM	Random Access Memory
RSA	Rivest, Shamir, Adleman
RFV	Rapporto Finale di Valutazione (Végső értékelő jelentés)
SAR	Security Assurance Requirement
SCD	Signature Creation Data (aláírást létrehozó adat)
SFR	Security Functional Requirement
SOGIS	Senior Officials Group Information Systems Security
ST	Security Target
SVD	Signature Verification Data
SW	Szoftver
TDS	Traguardo di Sicurezza (Biztonsági célkitűzés)
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

4 Hivatkozások

4.1 Kritériumok és előírások

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, 3.1 verzió, 5. felülv., 2017. április

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, 3.1 verzió, 5. felülv., 2017. április

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, 3.1 verzió, 5. felülv., 2017. április

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

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, 3.1 verzió, 5. felülv., 2017. április

[eIDAS] „Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről”, az Európai Unió Hivatalos Lapja L 257, 2014. augusztus 28.

[LGP1] Az informatikai rendszerek és termékek biztonsági értékelésének és tanúsításának nemzeti rendszere - A nemzeti rendszer általános leírása - Ideiglenes iránymutatások - 1. rész - LGPI 1.0 verzió, 2004. december

[LGP2] Az informatikai rendszerek és termékek biztonságának nemzeti értékelési és tanúsítási rendszere - Az LVS-ek akkreditációja és az asszisztensek képzése - Ideiglenes iránymutatás - 2. rész - LGP2 1.0 verzió, 2004. december

[LGP3] Az informatikai rendszerek és termékek biztonsági értékelésének és tanúsításának nemzeti rendszere - Értékelési eljárások - Ideiglenes iránymutatások - 3. rész - LGP3, 1.0 verzió,
2004. december

[NIS1] IT-biztonsági tanúsító testület, A rendszerre vonatkozó 1/13. sz. tájékoztató - Az LGP1 módosításai, 1.0. verzió, 2013. november

[NIS2] IT-biztonsági tanúsító testület, A rendszerre vonatkozó 2/13. sz. tájékoztató - Az LGP2 módosításai, 1.0. verzió, 2013. november

[NIS3] IT-biztonsági tanúsító testület, A rendszerre vonatkozó 3/13. sz. tájékoztató - Az LGP3 módosításai, 1.0. verzió, 2013. november

[SOGIS] „Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, 3-as verzió, 2010. január

4.2 Műszaki dokumentumok

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

[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-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

[PPQSCD1] EN 419211-2:2013, Biztonságos aláírás-létrehozó eszköz védelmi profilja - 2. rész: Kulcsgeneráló eszköz

[PPQSCD2] EN 419211-4:2013, Biztonságos aláírás-létrehozó eszköz védelmi profilja - 4. rész: Tartozék kulcsgeneráló eszközökhöz és megbízható csatorna tanúsítványgeneráló alkalmazáshoz

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

[TDS] “Security Target IDentity Applet v3.4/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS”, Version 1.02, ID&Trust Ltd., 13 October 2020

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

5 A tanúsítvány elismerése

5.1 A CC tanúsítványok európai szintű elismerése (SOGIS-MRA)

Az európai kölcsönös elismerési megállapodás (SOGIS-MRA, 3. változat, [SOGIS]) 2010. áprilisában lépett hatályba, és a Közös Kritériumok (CC) alapján kiadott tanúsítványok kölcsönös elismeréséről rendelkezik az EAL4 értékelési szintig bezárólag valamennyi informatikai termék esetében. Bizonyos műszaki területekhez tartozó termékek esetében az elismerés az EAL4 feletti értékelési szinteken is lehetséges.

Az aláíró országok és a legmagasabb elismerést élvező műszaki területek legfrissebb listája, valamint egyéb részletek a https://www.sogis.eu/ honlapon találhatók.

A tanúsítványra nyomtatott SOGIS-MRA logó jelzi, hogy az aláíró országok a megállapodás feltételei alapján elismerik a tanúsítványt.

Ezt a tanúsítványt a SOGIS-MRA minden garanciális elemre vonatkozóan elismeri az EAL4 szintig.

5.2 A CC tanúsítványok nemzetközi szintű elismerése (CCRA)

A CC alapján kiállított tanúsítványok kölcsönös elismeréséről szóló nemzetközi megállapodás (Közös Kritériumok elismeréséről szóló megállapodás, [CCRA]) jelenlegi változatát 2014. szeptember 8-án hagyták jóvá. Ez az EAL4 szintig az "együttműködő" védelmi profiloknak (cPP) megfelelő CC-tanúsítványokra vagy az EAL2 szintig a megbízhatósági összetevőkön alapuló tanúsítványokra vonatkozik, a hibaelhárítási család (ALC_FLR) lehetséges kiegészítésével.

Az aláíró országok és az "együttműködő" védelmi profilok (cPP) frissített listája és egyéb részletek a következő címen érhetők el https://www.commoncriteriaportal.org/.

A tanúsítványra nyomtatott CCRA-logó azt jelzi, hogy az aláíró országok a megállapodás feltételei szerint elismerik a tanúsítványt.

Ezt a bizonyítványt a CCRA az EAL2 szintig ismeri el.

6 Tanúsítási nyilatkozat

Az értékelés tárgya (ODV) az ID&Trust Ltd. által kifejlesztett „IDentity Applet v3.4/QSCD on NXP JCOP 4 P71”, rövidítve „IDentity Applet v3.4/QSCD”.

Az ODV egy olyan minősített elektronikus aláírás-létrehozó eszköz (QSCD), amely egy érintkező vagy érintkezés nélküli intelligens kártyából áll, amely képes az aláírást létrehozó adatok előállítására (SCD) és minősített elektronikus aláírások létrehozására. Az ODV védi az SCD-ket és biztosítja, hogy csak az arra jogosult aláíró használhassa azokat.

Az ODV egy összetett termék, és a következőket tartalmazza:

- Az ODV mögöttes platformja: „NXP JCOP 4 P71”, amelyet az NXP Semiconductors Germany GmbH fejlesztett ki;
- Az ODV alkalmazási része: „IDentity Applet v3.4/QSCD”;
- a kapcsolódó üzemeltetési dokumentáció.

Ezért az értékelést a platform CC tanúsítványának [NXP-CR1] eredményei alapján, valamint a „Composite product evaluation for Smart Cards and similar devices” [JIL-COMP] dokumentumban foglalt ajánlásokat követve végezték el, a CCRA és a SOGIS nemzetközi megállapodásokban előírtaknak megfelelően.

Az értékelést az informatikai ágazatban a rendszerek és termékek biztonságának értékelésére és tanúsítására szolgáló nemzeti rendszer által meghatározott és az ideiglenes iránymutatásokban [LGP1, LGP2, LGP3], valamint a rendszer tájékoztató jegyzeteiben [NIS1, NIS2, NIS3] megfogalmazott követelményekkel összhangban végezték el. A rendszert a 2003. október 30-i miniszterelnöki rendelettel (G.U. n.98, 2004. április 27.) létrehozott IT-biztonsági Tanúsító Testület irányítja.

Az értékelés valójában 2016-ban kezdődött egy „IDentity Applet v3.3/SSCD on NXP JCOP 3 SECID P60 OSB Smart Card” nevű ODV-n, amely a JCOP 3 platformon alapul. Az értékelés során az ügyfél úgy döntött, hogy az ODV-t a JCOP 4 platformra frissíti. Az új ODV „IDentity Applet v3.4/QSCD” pontosan ugyanazokkal a funkciókkal rendelkezik, mint a 3.3-as verzió, de a frissített platformon. Ezért az LVS CCLab szoftverlaboratóriuma a 3.3-as verzió folyamatban lévő értékelésének eredményeit használhatta alapul.

Az értékelés célja, hogy garantálja az ODV hatékonyságát a Biztonsági célkitűzés [TDS] elérésében, amelyet a potenciális vásárlók és/vagy felhasználók számára ajánlott elolvasni. Az értékelési folyamathoz kapcsolódó tevékenységeket a Közös Kritériumok 3. részével [CC3] és a közös értékelési módszertannal [CEM] összhangban végezték.

- Megállapítást nyert, hogy az ODV megfelel a CC v 3.1 3. részének az EAL4 biztonsági szintre vonatkozó követelményeinek, az AVA_VAN.5 kiegészítéssel,

a Biztonsági célkitűzésben [TDS] és az ID&Trust Identity Applet Suite felhasználói kézikönyvben [ADM] szereplő követelményekkel összhangban;

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

B melléklet – ennek a Tanúsítási Jelentésnek az értékelt konfigurációja.

A Tanúsítási Jelentés közzététele megerősíti, hogy az értékelési folyamatot a Közös Kritériumok - ISO/IEC 15408 értékelési kritériumainak ([CC1], [CC2], [CC3]) és a Közös Kritériumok elismeréséről szóló megállapodásban [CCRA] meghatározott eljárásoknak megfelelően hajtották végre, és hogy nem találtak kihasználható sebezhetőséget. A tanúsító szervezet azonban ezzel a dokumentummal nem fejezi ki az ODV semmiféle támogatását vagy népszerűsítését.

7 Az értékelés összefoglalása

7.1 Bevezetés

Ez a Tanúsítási Jelentés az "IDentity Applet v3.4/QSCD" termék Közös Kritériumok szerinti biztonsági értékelésének eredményét tartalmazza, és célja, hogy útmutatást nyújtson a potenciális vásárlók és/vagy felhasználók számára annak megítéléséhez, hogy az ODV biztonsági jellemzői megfelelnek-e a saját igényeiknek.

Ezt a Tanúsítási Jelentést a Biztonsági célkitűzéssel [TDS] együtt kell áttanulmányozni, amely meghatározza a funkcionális és garanciális követelményeket, valamint a tervezett felhasználási környezetet.

7.2 A tanúsítás összefoglalás azonosítása

Az ODV neve	IDentity Applet v3.4/QSCD on NXP JCOP 4 P71
Biztonsági célkitűzés	„Security Target IDentity Applet v3.4/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS”, Version 1.02 [TDS]
Garanciális szint	EAL4 az AVA_VAN.5 hozzáadásával
Beszállító	ID&Trust Ltd.
Megbízó	NXP Semiconductors Netherlands B.V.
LVS	CCLab Software Laboratory
CC verziója	3.1 Felülv. 5
A Pp-nek való megfelelőség	EN 419 211-2:2013 [PPQSCD1] EN 419 211-4:2013 [PPQSCD2]
Az értékelés kezdetének időpontja	2016. szeptember 6.
Az értékelés végének időpontja	2020. október 14.

A tanúsítási eredmények csak a terméknek a jelen Tanúsítási Jelentésben megjelölt változatára vonatkoznak, és feltéve, hogy a Biztonsági célkitűzésben [TDS] leírt környezeti feltételezések teljesülnek.

7.3 Az értékelt termék

Ebben a bekezdésben az ODV főbb funkcionális és biztonsági jellemzőit foglaljuk össze; részletes leírásért kérjük, olvassa el a Biztonsági célkitűzést [TDS].

Az ODV "IDentity Applet v3.4/QSCD" egy intelligens kártyából és egy olyan appletből áll, amely a 910/2014/EU rendeletnek [eIDAS] megfelelő minősített elektronikus aláírás-létrehozó eszköz (QSCD) megvalósítására van beprogramozva.

Az ODV átülteti a gyakorlatba az aláírást létrehozó adatok (SCD) generálását és a minősített elektronikus aláírások létrehozását. Ezenkívül az ODV támogatja saját maga QSCD-ként való hitelesítését a bizalmi szolgáltató (CSP) tanúsítvány-létrehozó alkalmazásával (CGA) szemben, valamint a CGA-val folytatott biztonságos kommunikációt az ODV által generált és exportált, valamint a CGA által importált aláírás-hitelesítési adatok (SVD) védelme érdekében.

Az ODV tárolja az SCD-ket és a RAD-okat (Referencia hitelesítési adatok). Az ODV az SCD-k több példányát is tárolhatja. Ebben az esetben az ODV funkciót biztosít az egyes SCD-k egyedi azonosításához, az aláírás-létrehozó alkalmazás (SCA) pedig interfészt biztosíthat az aláíró számára, hogy kiválaszthassa a QSCD aláírás-létrehozási funkcióban használandó SCD-t.

Az ODV védi az SCD-k titkosságát és integritását, és azoknak az aláírás létrehozására való felhasználást a jogosultra korlátozza. Az ODV tartalmazza az összes olyan biztonsági funkciót, amely az SCD-k titkosságának és az elektronikus aláírás biztonságának biztosításához szükséges. Az ODV elektronikus aláírási funkciói felhasználhatók az [eIDAS]-nak megfelelő minősített elektronikus aláírás létrehozására.

Az ODV a saját CRS (Certificate Request Signature) protokollját alkalmazza az SVD-k érvényességének igazolására a CGA számára. A CRS protokoll azt is bizonyítja, hogy az SVD-k kapcsolatban állnak az ODV-vel.

A CRS protokoll az SCD/SVD kulcspártól elkülönítve az ODV által generált kulcspárt használja; az SCD/SVD kulcspár generálásakor az ODV az SVD-t a CRS magánkulccsal írja alá. A CGA ezután a CRS ellenőrzésével tudja ellenőrizni az SVD érvényességét.

Az ODV további biztonsági funkciókat és követelményeket is megvalósíthat, például az aláírandó adatok szerkesztésére és megjelenítésére (DTBS/R), de ezek nem részei a Biztonsági célkitűzésben [TDS] meghatározott biztonsági politikának, és nem tartoznak az értékelt ODV-konfiguráció hatálya alá.

Az ODV egy összetett termék, és a következőket tartalmazza:

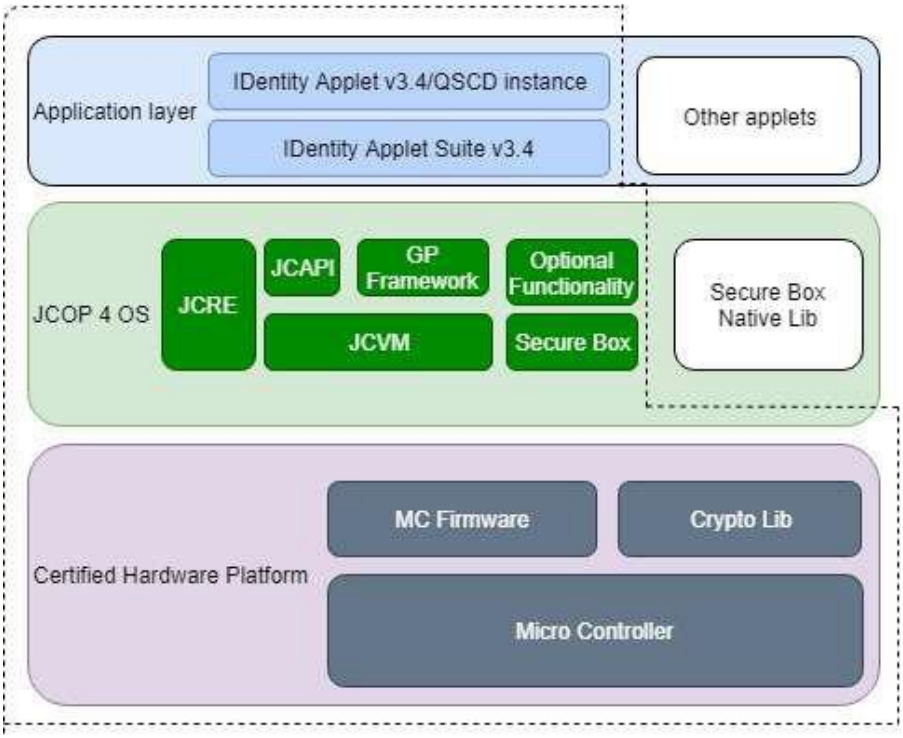
- Az ODV mögöttes platformja: „NXP JCOP 4 P71”, melyet az NXP Semiconductors Germany GmbH fejlesztett ki, CC EAL6 szintű tanúsítással, ASE_TSS.2 és ALC_FLR.1 [NXP-CR1] kiegészítéssel; ez az alábbiakat tartalmazza:
    a) Micro Controller (az NXP SmartMX3 családjába tartozó biztonságos intelligens kártyavezérlő);
    b) IC Dedicated Software (Micro Controller Firmware és Crypto Library);
    c) IC Embedded Software JCOP 4 (Java Card Virtual Machine, Runtime Environment, Java Card API);
    d) Global Platform (GP) Framework;
- Az ODV alkalmazási része: „IDentity Applet v3.4/QSCD”;
- a kapcsolódó üzemeltetési dokumentáció.

Az ODV rendeltetésszerű felhasználója a QSCD-kibocsátó szolgálat, amely az ODV-t QSCD-ként elkészíti a felhasználók számára, személyre szabva azt a jogos tulajdonos, mint aláíró személyazonosságával, és eljuttatja az aláíróhoz.

Az előkészítési szakasz végén az SCD-nek nem működőképes állapotban kell lenniük. Az aláírónak, miután megkapta az ODV-t, ellenőriznie kell, hogy az ODV ne legyen működőképes állapotban és az SCD-k státuszát működőképesre kell módosítania.

7.3.1 Az ODV felépítése

Az 1. ábra mutatja az ODV logikai hatókörét és határait.



1. ábra - Az ODV logikai hatóköre és határai

Az ODV egy összetett termék és a szaggatott vonal a teljes ODV-t jelzi. Az alatta lévő tanúsított hardverplatform és a JCOP 4 operációs rendszer lila és zöld színnel vannak jelölve. A kék doboz az alkalmazási réteget jelöli. Az ID&Trust IDentity Applet Suite v3.4 betölthető a flashmemóriába. Az inicializálási fázisban létrejön az applet egy példánya, amely egy sor konfigurációs lépés végén IDentity Applet v3.4/QSCD néven kerül személyre szabása.

Az ODV részletes leírásával kapcsolatban tekintse meg a Biztonsági célkitűzéseket [TDS]; különös tekintettel a következőkre:

- az ODV fizikai és logikai részeinek leírása a TDS 1.4.2 bekezdésében található;
- az ODV életciklusának leírása, amely a fejlesztési, előkészítési és üzemeltetési fázisokból áll, a TDS 1.4.5 bekezdésében található;

- az ODV biztonsági jellemzőinek leírása a TDS 1.4.6 bekezdésében található.

7.3.2 Az ODV biztonsági jellemzői

7.3.2.1 A platformmal való összeférhetőség

Az ODV biztonsági funkcióinak egyes aspektusait, beleértve a biztonsági célkitűzéseket, feltételezéseket, fenyegetéseket és a szervezet biztonsági politikáit, közvetlenül a platform fedezi. A részletekkel kapcsolatban olvassa el a Biztonsági célkitűzés [TDS] 2.4 bek.

7.3.2.2 QSCD funkcionalitás

Az ODV, mint minősített aláírás-létrehozó eszköz (QSCD) a következő, egymástól elkülönülő működési környezetekkel rendelkezik:

- Az előkészítő környezet, ahol kölcsönhatásba lép a CSP CGA-vel, hogy tanúsítványt kapjon az ODV által generált SCD-nek megfelelő SVD-hez. Az ODV egy biztonságos csatornán keresztül exportálja az SVD-ket, lehetővé téve a CGA számára hitelességük ellenőrzését. Az inicializálási környezet további kölcsönhatásba lép az ODV-vel, hogy testre szabja azt az SVD-k kezdeti értékével.

- Az aláírási környezet, ahol egy SCA-n keresztül kölcsönhatásba lép a tulajdonossal az adatok aláírásához, miután jogos aláíróként hitelesítette a tulajdonost. Az SCA az aláírandó adatok egyedi reprezentációját (DTBS/R) adja meg bemenetként az ODV aláírás-létrehozó funkciójához, és eredményül megkapja az elektronikus aláírást.

- A kezelési környezet, ahol a felhasználóval vagy egy minősített bizalmi szolgáltatóval (QTSP) lép kapcsolatba a kezelési műveletek elvégzéséhez, például egy aláíró blokkolt RAD-jának visszaállítása érdekében. Egyetlen eszköz, pl. egy intelligens kártyaterminál, biztosíthatja a szükséges biztonságos környezetet az irányítási és aláírási műveletekhez.

Az ODV az aláírás-létrehozási adatok (SCD) biztonságos létrehozására, használatára és kezelésére konfigurált hardver és szoftver kombinációja. A QSCD megóvja az SCD-ket azok teljes életciklusa alatt, biztosítva, hogy azokat csak a tulajdonosuk használhassa fel az aláírás-létrehozási folyamatban. A QSCD tartalmazza az összes olyan biztonsági funkciót, amely az SCD-k titkosságának és az elektronikus aláírás biztonságának biztosításához szükséges, az alábbi funkciók révén:

- SCD/SVD pár létrehozása az alábbi rejtjelkulcskulcs-generáló algoritmusok egyikével:
  - RSA 1024-4096 bit hosszúságú kulcsokkal;
  - ECC 160-521 bit hosszúságú kulcsokkal.

- az SVD-k biztonságos csatornán keresztül történő exportálása a CGA-be a tanúsítványok előállításához;

- az SB-nek, mint a QSCD identitásának bizonyítása külső szervezetek felé;

- (nem kötelező) a tanúsítványinformációk fogadása és tárolása;

- az ODV nem üzemképes állapotból üzemképes állapotba való átkapcsolása;
- működési állapotban digitális aláírások létrehozása a következő kriptográfiai algoritmusok használatával:
    - RSASSA-PKCS1-v1_5 vagy RSASSA-PSS 2048-4096 bit hosszúságú kulcsokkal;
    - ECDSA 160-521 bit hosszúságú kulcsokkal.

A digitális aláírások a következő lépéseken keresztül jönnek létre:

- egy SCD kiválasztása, ha a QSCD-ben több SCD van jelen;
- az aláíró hitelesítése és aláírási szándékának megállapítása;
- a DTBS/R fogadása;
- egy olyan kriptográfiai függvény alkalmazása a DTBS/R-re, amely alkalmas az aláírás létrehozására a kiválasztott SCD felhasználásával.

7.3.2.3 Biztonsági funkciók

Az ODV biztonsági funkcióinak részletes leírását lásd a Biztonsági célkitűzés [TDS] 7.1 bekezdésében. A legfontosabb szempontokat az alábbiakban soroljuk fel:

- **AccessControl**: ez a funkció biztosítja a fájlrendszerben lévő adatokhoz, valamint az inicializálási, személyre szabási és a személyre szabás előtti adatokhoz való hozzáférés ellenőrzését. Az életciklus korai szakaszában, amikor az alkalmazást még nem telepítették, a Platform felelős a megfelelő hozzáférés kezeléséért. Az ODV olyan hozzáférés-vezérlési mechanizmusokat biztosít, amelyek lehetővé teszik a különböző biztonsági szerepkörök (aláíró és rendszergazda), valamint a hozzáférés-vezérlési irányelvek és funkciók fenntartását.
- **Authenticate**: ez a funkció kezeli az aláíró és a rendszergazda azonosítását és hitelesítését, és biztosítja a szerepek szétválasztását. Az ODV aktiválása vagy alaphelyzetbe állítása után a felhasználó nincs hitelesítve. A TSF által a felhasználó nevében közvetített műveletekhez a felhasználó előzetes azonosítása és hitelesítése szükséges.
- **SecureManagement**: minden biztonsági attribútumot biztonságosan módosítanak, így nincs lehetőség illetéktelen módosítások elvégzésére. Ez a funkció felelős az attribútumok, adatok és biztonsági funkciók biztonságos kezeléséért.
- **CryptoKey**: ez a funkció kriptográfiai támogatást nyújt a TSF számára, beleértve a biztonságos kulcsgenerálást (SCD/SVD kulcspár) és az elektronikus aláírások létrehozását. Ezenkívül a CryptoKey funkció biztonságos módszert biztosít a kulcsok megsemmisítésére.
- **AppletParametersSign**: aláír néhány konfigurációs és vezérlési paramétert és az aláírást az inicializálási fázis lezárása előtt ellenőrzi. Az inicializálási szakasz során csak a nem aláírt paramétereket lehet módosítani. Így

csak a fejlesztő által hitelesített és a követelményeknek megfelelő alkalmazási profilok (Application Profiles) alkalmazhatók. Az aláírások megfelelő ellenőrzése nélkül az inicializálási fázis nem fejezhető be az INITIALIZED állapot elérésével, és a személyre szabási fázis nem indítható el. Ezek az aláírások az IDentity Applet teljes életciklusa alatt ellenőrizhetők, így a biztonsági funkció alkalmazásával lehetővé válik a jogosulatlan módosítások felderítése.

- **Platform**: a tanúsított kriptográfiai könyvtár és a tanúsított IC-platform biztonsági funkcióira épülő biztonsági funkciókat látja el.

7.4 Dokumentáció

Az A függelékben - Útmutató a termék biztonságos használatához meghatározott dokumentációt a termékkel együtt kapja meg a vásárló.

A megadott dokumentáció tartalmazza az ODV inicializálásához, konfigurálásához és biztonságos használatához szükséges információkat a Biztonsági célkitűzésnek [TDS] megfelelően.

Ezenkívül be kell tartani ennek a jelentésnek a 8.3 bekezdésében foglalt, az ODV biztonságos használatára vonatkozó ajánlásokat is.

7.5 A védelmi profiloknak való megfelelés

A Biztonsági célkitűzés [TDS] *szigorúan* megfelel az alábbi Védelmi profiloknak:

- MSZ EN 419211-2:2013, Biztonságos aláírás-létrehozó eszköz védelmi profilja - 2. rész: Kulcsgenerálós eszközök [PPQSCD1]

- MSZ EN 419211-4:2013, Biztonságos aláírás-létrehozó eszköz védelmi profilja - 4. rész: Tartozék kulcsgeneráló eszközökhöz és megbízható csatorna tanúsítványgeneráló alkalmazáshoz [PPQSCD2]

7.6 Funkcionális és garanciális követelmények

Az összes garanciális követelményt (SAR) a CC 3. részéből [CC3] választották ki.

Az összes funkcionális követelményt (SFR) a CC 2. részéből [CC2] választották ki.

Tekintettel arra, hogy a Biztonsági célkitűzés *szigorúan* megfelel az MSZ EN 419211-2:2013 [PPQSCD1] és MSZ EN 419211-4:2013 [PPQSCD2] Védelmi profiloknak, beletartoznak az említett PP-kben meghatározott alábbi kibővített funkcionális követelmények is:

- a FIA_API család FIA_API.1: Authentication Proof of Identity

- az FPT_EMS család FPT_EMS.1: TOE Emanation

A Biztonsági célkitűzés [TDS], amelyre a teljes leírás és az alkalmazási megjegyzések tekintetében hivatkozunk, meghatározza az OVD-re vonatkozó összes biztonsági célkitűzést, az e célkitűzésekkel szembeni fenyegetéseket, az SFR-eket és az e célkitűzéseket megvalósító biztonsági funkciókat.

7.7 Az értékelés lefolytatása

Az értékelést az informatikai ágazatban a rendszerek és termékek biztonságának értékelésére és tanúsítására szolgáló nemzeti rendszer által meghatározott és az Ideiglenes iránymutatásokban [LGP3], valamint a Rendszer tájékoztató jegyzeteiben [NIS3] megfogalmazott követelményekkel összhangban végezték el. Az értékelést a fentieken kívül a Common Criteria Recognition Arrangament [CCRA] követelményeinek megfelelően végezték.

Ezenkívül, mivel egy összetett ODV-ről van szó, a CCRA és a SOGIS nemzetközi megállapodásokban előírtaknak megfelelően követték a „Composite product evaluation for Smart Cards and similar devices" [JIL- COMP] dokumentumban rögzített útmutatásokat. Különösen azt kell megjegyezni, hogy a behatolási teszteket 2020. augusztusában, tehát a platformon elvégzett sebezhetőségi elemzéstől számított 18 hónapon belül fejezték be (2019. május 31., a [NXP-CR1] és [NXP-CR2] platform tanúsítási jelentésében feltüntetett „ETR for Composition" legrégebbi dátuma).

Az értékelés célja, hogy bizonyosságot nyújtson az OVD hatékonyságáról a vonatkozó Biztonsági célkitűzésben [TDS] megfogalmazott állítások teljesítéséhez, amelyet a potenciális vásárlóknak érdemes elolvasniuk. Kezdetben a Biztonsági célkitűzést értékelték azért, hogy az megfelelő alapot biztosítson a CC-szabvány követelményei szerinti értékeléshez. Az ODV-t ezután a Biztonsági célkitűzésben megfogalmazott kijelentések alapján értékelték. Az értékelés mindkét szakaszát a CC 3. rész [CC3] és a CEM [CEM] szerint végezték.

A tanúsító szervezet felügyelte az LVS CCLab szoftverlaboratórium által végzett értékelés lefolytatását.

Az értékelési tevékenység 2020. október 14-én fejeződött be azzal, hogy az LVS kiadta a végső értékelési jelentést [RFV], amelyet a tanúsító szervezet 2020. október 16-án hagyott jóvá. Ezt követően a tanúsító szervezet kiadta ezt a Tanúsítási Jelentést.

7.8 A tanúsítás érvényességével kapcsolatos általános megfontolások

- Az értékelés a Biztonsági célkitűzésben [TDS] bejelentett biztonsági funkciókat vizsgálta, az ott meghatározott működési környezetre való hivatkozással. Az értékelést az ID&Trust Identity Applet Suite felhasználói kézikönyvében [ADM] leírtak szerint konfigurált ODV-n végeztük;

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

B függelék – Értékelt konfiguráció. A potenciális vásárlóknak azt javasoljuk, hogy ellenőrizzék, hogy megfelel-e elvárásaiknak, és vegyék figyelembe az ebben a Tanúsítási Jelentésben megfogalmazott ajánlásokat.

A tanúsítás nem garantálja a sebezhetőségek hiányát; továbbra is fennáll annak a valószínűsége (a valószínűség annál kisebb, minél nagyobb a garanciaszint), hogy a tanúsítvány kiadása után kihasználható sebezhetőségeket fedeznek fel. Ez a Tanúsítási Jelentés a tanúsító szervezetnek a kiadás időpontjában levont következtetéseit tükrözi. A (potenciális és tényleges) vásárlókat felkérjük, hogy a jelen Tanúsítási Jelentés kiadása után rendszeresen ellenőrizzék az új sebezhetőségeket, és ha a sebezhetőségek az ODV működési környezetében kihasználhatók, akkor a gyártóval ellenőrizzék, hogy

a biztonsági frissítéseket kifejlesztették-e, és hogy ezeket a frissítéseket értékelték és tanúsították-e.

8 Az értékelés kimenetele

8.1 Az értékelés eredménye

- Az LVS CCLab szoftverlaboratórium által készített Végső értékelő jelentés [RFV] és a tanúsításhoz szükséges dokumentumok elemzését követően, az elvégzett értékelési tevékenységekre tekintettel, a tanúsító csoport tanúsága szerint az OCSI arra a következtetésre jutott, hogy az "IDentity Applet v3.4/QSCD" ODV megfelel a Közös Kritériumok 3. részében [CC3] az EAL4 megbízhatósági szintre előirányzott követelményeknek, kiegészítve az AVA_VAN.5 kiegészítéssel, a biztonsági célrendszerben [TDS] megadott biztonsági funkciókkal és az ID&Trust Identity Applet Suite felhasználói kézikönyvben [ADM] megadott értékelt konfigurációval kapcsolatban;

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

B függelék – Értékelt konfiguráció.

Az 1. táblázat összefoglalja az LVS által végzett egyes tevékenységek végső értékelését a [CC3] biztosíthatósági követelményei alapján, az EAL4 biztosíthatósági szintre vonatkozóan, az AVA_VAN.5 kiegészítéssel.

Garanciaosztályok és összetevők		**Vélemény**
Biztonsági célkitűzés vizsgálata	**ASE osztály**	Pozitív
Conformance claims	ASE_CCL.1	Pozitív
Extended components definition	ASE_ECD.1	Pozitív
ST introduction	ASE_INT.1	Pozitív
Security objectives	ASE_OBJ.2	Pozitív
Derived security requirements	ASE_REQ.2	Pozitív
Security problem definition	ASE_SPD.1	Pozitív
TOE summary specification	ASE_TSS.1	Pozitív
Fejlesztés	**ADV osztály**	Pozitív
Security architecture description	ADV_ARC.1	Pozitív
Complete functional specification	ADV_FSP.4	Pozitív
Implementation representation of the TSF	ADV_IMP.1	Pozitív
Basic modular design	ADV_TDS.3	Pozitív
Használati kézikönyvek	**AGD osztály**	Pozitív
Operational user guidance	AGD_OPE.1	Pozitív
Preparative procedures	AGD_PRE.1	Pozitív
Életciklus támogatás	**ALC osztály**	Pozitív

Garanciaosztályok és összetevők		Vélemény
Production support, acceptance procedures and automation	ALC_CMC.4	Pozitív
Problem tracking CM coverage	ALC_CMS.4	Pozitív
Delivery procedures	ALC_DEL.1	Pozitív
Identification of security measures	ALC_DVS.1	Pozitív
Developer defined life-cycle model	ALC_LCD.1	Pozitív
Well-defined development tools	ALC_TAT.1	Pozitív
Tesztek	**ATE osztály**	Pozitív
Analysis of coverage	ATE_COV.2	Pozitív
Testing: basic design	ATE_DPT.1	Pozitív
Functional testing	ATE_FUN.1	Pozitív
Independent testing - sample	ATE_IND.2	Pozitív
Sebezhetőségek becslése	**AVA osztály**	Pozitív
Advanced methodical vulnerability analysis	*AVA_VAN.5*	Pozitív

1. táblázat - A garanciakövetelményekre vonatkozó végleges ítéletek

8.2 További garanciális tevékenységek

A „Composite product evaluation for Smart Cards and similar devices” [JIL-COMP] című kötelező támogató dokumentum további, az ilyen típusú összetett ODV-re jellemző további garanciakövetelményeket tartalmaz.

A dokumentum meghatározza az összetett termék értékeléséhez szükséges meglévő megbízhatósági követelmények finomításait. Ezen altevékenységek célja, hogy pontosan meghatározzák az értékelő feladatait az összetett ODV értékelésének különböző részeire vonatkozóan.

A 2. táblázat összefoglalja az LVS által a [JIL-COMP] által előírtaknak megfelelően elvégzett egyes összetétel-specifikus megbízhatósági tevékenységek végső ítéleteit.

Összetétel-specifikus garanciális tevékenységek		Végső ítélet
ASE_COMP: Consistency of composite product Security Target	ASE_COMP.1	Pozitív
ALC_COMP: Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1	Pozitív
ADV_COMP: Composite design compliance	ADV_COMP.1	Pozitív
ATE_COMP: Composite functional testing	ATE_COMP.1	Pozitív
AVA_COMP: Composite vulnerability assessment	AVA_COMP.1	Pozitív

2. táblázat - Az összetétel-specifikus biztosítási tevékenységekre vonatkozó végleges ítéletek

8.3 Ajánlások

A Tanúsító Szervezet következtetései a 6. Fejezetben olvashatók (Tanúsítási nyilatkozat).

Az „IDentity Applet v3.4/QSCD” termék potenciális vásárlóinak azt javasoljuk, hogy a Jelentést elolvasva pontosan értelmezzék a tanúsításnak a Biztonsági célkitűzések [TDS] vonatkozásában meghatározott alkalmazási körét.

Az ODV-t a Biztonsági célkitűzés [TDS] 4.2. szakaszában meghatározott, az üzemeltetési környezetre vonatkozó biztonsági célkitűzésekkel összhangban kell használni. Feltételezhető, hogy abban az üzemeltetési környezetben, amelyben az OVD-t elhelyezik, betartják a szervezet biztonsági szabályzatát és a TDS 3.3., illetve 3.4. bekezdésében leírt feltételezéseket, különös tekintettel azokra, amelyek a Platformmal kompatibilisek (lásd a [TDS] 2.4 bek.).

Ez a Tanúsítási Jelentés kizárólag az értékelt konfigurációjú ODV-re érvényes; különösen az A függelék - az Útmutató a termék biztonságos használatához - tartalmaz a termék átadására, inicializálására és biztonságos használatára vonatkozó javaslatokat, az ODV-vel együtt szállított üzemeltetési dokumentációban ([ADM], [USR]) megtalálható útmutatásoknak megfelelően.

9 A függelék - Útmutató a termék biztonságos használatához

Ez a függelék a termék potenciális vásárlója számára különösen fontos észrevételeket tartalmaz.

9.1 Szállítás

Mivel az ODV egy összetett termék, a szállítási eljárások az alkalmazásfejlesztő (ID&Trust Ltd.) és a platformgyártó (NXP) közötti kölcsönös viszony függvénye.

Az ID&Trust és az NXP közötti szállítási eljárások a következők:

1. A fejlesztő (ID&Trust) elkészíti az IDentity Applet v3.4 új verzióját.

2. A belső tesztelési fázist követően az ID&Trust kiadja az új verziót, és azt a fejlesztő konfigurációkezelő rendszerében tárolja.

3. Az IDentity Applet v3.4 új verzióját elküldi az NXP-nek.

4. Az NXP betölti az appletet a Platform chipbe.

Az alapul szolgáló platform számos biztonsági funkciót biztosít az IDentity Applet v3.4 védelme érdekében a különböző érintett szervezetek közötti szállítás során.

Az NXP kétféle termékszállítási módot kínál:

1. Átvétel („Collection”): az ügyfél átveszi a terméket az NXP telephelyén.

2. Szállítás („Shipment”): A terméket az NXP elküldi az ügyfélnek. Annak érdekében, hogy a terméket szállítás közben ne lehessen megbabrálni, a terméket speciális ragasztószalaggal lezárt csomagokban kerül szállításra. A szalag folyamatos számokkal van nyomtatva, és speciális ragasztási jellemzőkkel rendelkezik, amelyek láthatóvá teszik az illetéktelen beavatkozásokat. A csomagban található egy nyomtatvány, amelyet az ügyfélnek vissza kell küldenie az NXP-nek, hogy tájékoztassa a gyártót arról, hogy a kapott csomag nem sérült.

Mindkét szállítási mód biztosítja, hogy az ügyfél eredeti, hamisítatlan terméket kapjon. Ezenkívül az ügyfél egy speciális kriptográfiai kulcsot (Transport Key) használhat a chip hitelesítéséhez.

Az ODV kézbesítési eljárásaival kapcsolatos további részletek az ID&Trust IDentity Applet V3.4 Delivery Documentation [DEL] című dokumentumában olvashatók.

9.2 Az ODV telepítése, inicializálása és biztonságos használata

Az ODV telepítését, konfigurálását és üzemeltetését a termékkel együtt a vevőnek átadott útmutató dokumentáció megfelelő szakaszaiban található utasításoknak megfelelően kell elvégezni.

Különösen az alábbi dokumentumok tartalmaznak az ODV biztonságos inicializálására,

működési környezetének előkészítésére és az

ODV biztonságos működésére vonatkozó, a Biztonsági célkitűzéssel [TDS] összhangban álló részletes információkat:

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

10 BB függelék – Értékelt konfiguráció

Az értékelés tárgya (ODV) az ID&Trust Ltd. által kifejlesztett „IDentity Applet v3.4/QSCD on NXP JCOP 4 P71”, rövidítve „IDentity Applet v3.4/QSCD”.

Az ODV egy összetett termék, és a következő HW/SW komponensekből áll, amelyek az ODV értékelt konfigurációját képviselik, a [TDS] szerint, amelyre az értékelési eredmények vonatkoznak:

- Az „NXP JCOP 4 P71” platform, amelyet az NXP Semiconductors Germany GmbH fejlesztett ki, CC EAL6 szintű tanúsítással rendelkezik, ASE_TSS.2 és ALC_FLR.1 [NXP-CR1] kiegészítéssel; ez az alábbiakat tartalmazza:
    e) Micro Controller (az NXP SmartMX3 családjába tartozó biztonságos intelligens kártyavezérlő);
    f) IC Dedicated Software (Micro Controller Firmware és Crypto Library);
    g) IC Embedded Software JCOP 4 (Java Card Virtual Machine, Runtime Environment, Java Card API);
    h) Global Platform (GP) Framework;
- Az ODV alkalmazási része: eMRTD alkalmazásként konfigurált „IDentity Applet v3.4/QSCD”;
- a kapcsolódó üzemeltetési dokumentáció:
    - ID&Trust Identity Applet Suite User’s Guide [ADM];
    - ID&Trust Identity Applet Suite Administrator’s Guide [USR].

A Platform mikrovezérlő firmware-je és a dedikált IC-szoftver a következő tanúsítással rendelkezik: “NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library” [NXP-CR2].

Bővebb részletekért olvassa el a Biztonsági célkitűzés [TDS] 1.4 bekezdésében foglaltakat.

11 C Melléklet - Tesztelés

Ez a függelék ismerteti az értékelőknek és a szállítónak a tesztelési tevékenységekre vonatkozó kötelességvállalását. Az EAL4 megbízhatósági szint esetében, az AVA_VAN.5 kiegészítésével, ezek a tevékenységek három lépést foglalnak magukban:

- értékelés a szállító által elvégzett tesztek lefedettsége és mélysége szempontjából;
- az Értékelők által elvégzett független funkcionális tesztek;
- az Értékelők által elvégzett behatolási tesztek.

11.1 Konfiguráció a teszteléshez

Az LVS telephelyén tesztkörnyezetet alakítottak ki ezeknek a tevékenységeknek az elvégzéséhez. A beszállító a tesztekhez szükséges összes eszközt biztosította az értékelők számára, a teszteszköz és a kártyaolvasó kivételével.

Az Értékelők tesztkonfigurációja különösen a következőket tartalmazta:

- az IDentity Applet v3.4.7470/QSCD néven azonosított intelligens kártyán lévő ODV egy példányát;
- a HID Omnikey 5x21 CL0 intelligens kártyaolvasót;
- az OpenSCDP az Eclipse 2018-12 teszteszközt.

A tesztek elvégzése előtt a szoftveralkalmazást inicializálták és konfigurálták az ([ADM] és [USR]) 9.2 bekezdésében megnevezett üzemeltetési dokumentációnak megfelelően. A Szállító az ODV telepítéséhez személyreszabási szkriptet biztosított. Az Értékelőknek sikerült helyesen telepíteniük az OVD-t az alapul szolgáló platformra. Az Értékelőknek sikerült helyesen kiválasztaniuk a QSCD-appletet, ami bizonyította, hogy a kártyát helyesen telepítették, és ismert állapotban volt.

11.2 A Beszállító által végzett funkcionális tesztek

11.2.1 A tesztekhez alkalmazott megközelítés

A beszállító által bemutatott vizsgálati terv nagyrészt az alábbi műszaki referenciadokumentumokon alapult:

- 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].

Ezenkívül a beszállító önállóan további saját teszteket tervezett a funkcionális követelmények (SFR) és a biztonsági funkciók teljes lefedettségének bizonyítása érdekében.

11.2.2 A tesztek fedettsége

Ezenkívül a beszállító önállóan további saját teszteket tervezett, hogy bizonyítsa a funkcionális előírásokban leírt funkcionális követelmények (SFR) és TSFI-k teljes fedettségét.

11.2.3 Teszteredmények

Az Értékelők a beszállító vizsgálati tervében leírtak közül véletlenszerűen kiválasztott teszteket végeztek, hogy ellenőrizzék mind az ipari szabványos, mind a saját fejlesztésű tesztek megismételhetőségét és reprodukálhatóságát. Az Értékelők összehasonlították ezeknek a teszteknek az eredményeit a beszállító tesztelési specifikációiban meghatározott elvárt eredményekkel, és meggyőződtek arról, hogy azok teljes mértékben megegyeznek.

11.3 Az Értékelők által végzett funkcionális és független tesztek

Ezt követően az értékelők független teszteket terveztek a TSFI helyességének ellenőrzésére.

A TSF nagyszámú interfészt tartalmaz, ami miatt nem célszerű mindegyiket szigorúan tesztelni. Ezért az értékelők úgy döntöttek, hogy az ODV-ben tárolt alapvető adatok megváltoztathatatlanságának ellenőrzésére összpontosítanak, és mintavételi stratégiát alkalmaznak a következő interfészek tesztelésére:

- PUT DATA
- Az összes lehetséges dokumentálatlan TSFI-re vonatkozó alapos tesztelés

Az Értékelők ellenőrizték a tényleges vizsgálati eredményeket, és megállapították, hogy azok megfeleltek a várt eredményeknek.

Ezen kívül, tekintettel arra, hogy az ODV egy összetett termék, az értékelők az ATE_COMP család által meghatározott további tevékenységek révén, a [JIL-COMP] dokumentummal összhangban ellenőrizték az ODV egészének viselkedését, figyelembe véve a platform „ETR for Composition” dokumentumában [ETR-COMP] szereplő, az applet értékelőre vonatkozó kötelezettségeket és ajánlásokat is.

11.4 Sebezhetőségi elemzés és behatolásvizsgálat

Ezeknek a tevékenységek az elvégzéséhez az értékelők a funkcionális tesztelési tevékenységekhez már használt ODV ugyanazon mintapéldányát használták, ellenőrizve, hogy a tesztkonfiguráció összhangban van-e az ODV értékelés alatt álló változatával.

Mivel az ODV egy összetett termék, az értékelők az [JIL-COMP] dokumentummal összhangban elvégezték az AVA_COMP család által meghatározott további tevékenységeket, és megvizsgálták az „ETR for Composition” [ETR-COMP] dokumentumban szereplő sebezhetőségi elemzés eredményeit, hogy meggyőződjenek arról, hogy azok újra felhasználhatók-e az applet összetett értékeléséhez.

Az értékelők két különböző megközelítést alkalmaztak: az összes interfész tesztelése helyett mintavételi stratégiát alkalmaztak a TSFI egy részhalmaza funkcionalitásának tesztelésére, valamint nyers erővel végrehajtott támadást hajtottak végre, hogy felderítsék a dokumentálatlan API-ket. Tekintettel arra, hogy ez egy összetett termékről van szó, az értékelők az ODV egészének viselkedését vizsgálták.

A sebezhetőségi elemzés első szakasza az ODV-vel kapcsolatos információk összegyűjtéséből állt. Első lépésként különféle keresést végeztünk nyilvános forrásokban különböző kulcsszavak kombinációival (pl. „Qualified Signature Creation Device vulnerabilities", „tampering with electronic signature devices", „QSCD") a nyilvánosságra került ODV hibák és sebezhetőségek azonosítása érdekében. Ebben a szakaszban a sebezhetőségek nyilvános adatbázisa és a műszaki kutatási kiadványok is vizsgálat tárgyát képezték. A nyilvánosan ismert sebezhetőségek elavultnak bizonyultak, vagy csak az alapul szolgáló Platformra vonatkoztak, amely nem képezi az értékelés tárgyát. Ennek a szakasznak a végén az Értékelők arra a következtetésre jutottak, hogy az intelligens kártyák technológiája jól dokumentált, és egy potenciális támadó az iparági referenciaszabványok és az intelligens kártyákkal kapcsolatos nyilvánosan elérhető információk alapján teljes mértékben képes megérteni egy elektronikus aláíró eszköz működését. Az ODV dokumentáció nem nyilvános (azaz nem érhető el a gyártó honlapján). Ezt az információt lényegesnek tekintették a támadási potenciál kiszámítása szempontjából. A nyilvánosan elérhető információk alapján nem találtak az ODV-re vonatkozó ismert sebezhetőséget.

Második lépésben az értékelők elemezték a gyártó dokumentációját, hogy megismerjék az ODV-t és annak elektronikus aláírási funkcióit, valamint, hogy azonosítsák a lehetséges támadási területeket. Mint korábban említettük, a gyártó honlapján nem érhető el dokumentáció. Az Értékelők a dokumentáció alapján és az alapul szolgáló platform gyártója által az ODV-interfészekkel való interakcióhoz biztosított eszközök segítségével vizsgálták az ODV működését. Ebben a fázisban az Értékelők azonosították az esetleges dokumentálatlan interfészekhez kapcsolódó lehetséges támadási vektorokat. Figyelembe véve az ODV termék típusát és az intelligens kártyák iparágának szigorú szabványosítását, az értékelők az elektronikus aláírási funkciók megvalósításával kapcsolatos potenciális sebezhetőségekre és tesztelésre összpontosítottak. Az összegyűjtött információk alapján az Értékelők megállapították, hogy a hitelesítéssel kapcsolatos lehetséges sebezhetőségeket meg kell vizsgálni.

Miután összegyűjtötték az ODV-re és a potenciális sebezhetőségekre vonatkozó összes szükséges információt, az értékelők az AVA_VAN.5 követelményeinek megfelelő, több támadási forgatókönyvre osztott teszttervet készítettek. Minden egyes támadási forgatókönyvhöz kiszámították a pontos támadási potenciált, figyelembe véve, hogy az intelligens kártyákra vonatkozó, nyilvánosan elérhető információk nagyon részletesek, gazdagok és viszonylag könnyen megismerhetők.

A támadási forgatókönyvek meghatározását követően az Értékelők behatolásteszteket végeztek az ODV funkcióin, hogy felderítsék az esetlegesen kihasználható sebezhetőségeket.

Az Értékelők a következő támadási forgatókönyveket határozták meg:

- A támadó megpróbálja feloldani egy korábban zárolt eSIGN alkalmazás PIN-kódját az ilyen művelethez szükséges hitelesítés megkerülésével.

- A támadó megpróbálja módosítani az eSIGN alkalmazás megfelelő és biztonságos működéséhez szükséges érzékeny adatokat.

- A támadó felfedez egy dokumentálatlan interfészt. Ez az interfész további támadási felületet jelenthet.

A fent leírt támadási forgatókönyvek alapján az értékelők ezután behatolási tesztek segítségével megpróbáltak behatolni az ODV védelmébe.

A vizsgálatok eredményeit kellő részletességgel dokumentálták a megismételhetőség érdekében, és az áttekinthetőség kedvéért az eredményeket táblázatban is összefoglalták.

Az elvégzett behatolási tesztek nem azonosítottak egyetlen kihasználható, nagy támadási potenciállal rendelkező ODV sebezhetőséget sem.

A Beszállító telephelyén tett látogatások során az Értékelők elvégezték a forráskód elemzését, elsősorban a hitelesítési funkciók megvalósítására, valamint az oldalcsatornás *(side channel)* és hibainjekciós (*fault injection*) támadások ellen alkalmazott ellenintézkedésekre összpontosítva.

A rendelkezésre álló információk alapján az értékelők nem azonosítottak fennmaradó, azaz olyan sebezhetőségeket, amelyeket csak olyan támadók használhatnának ki, akiknek a támadási potenciálja High-nál magasabb.

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. 11/20

(Certification No.)

Prodotto: IDentity Applet v3.4/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, 28 ottobre 2020

Fino a EAL2 *(Up to EAL2)*

Common Criteria

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/QSCD on NXP JCOP 4 P71

OCSI/CERT/SYS/07/2016/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

3 Elenco degli acronimi

AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CGA	Certificate Generation Application
CRS	Certificate Request Signature
CSP	Certification Service Provider
DES	Data Encryption Standard
DPCM	Decreto del Presidente del Consiglio dei Ministri
DTBS/R	Data To Be Signed / Representation
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
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
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine

LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MMU	Memory Management Unit
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OS	Operating System
PIN	Personal Identification Number
PKCC	Public Key Crypto Coprocessor
PP	Profilo di Protezione (Protection Profile)
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
RAD	Reference Authentication Data
RAM	Random Access Memory
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-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] Evaluation Technical Report for Composition NXP JCOP 4 P71 - EAL6+, 19-RPT-177, Version 7.0, 19 March 2020

[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-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

[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

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

[TDS] "Security Target IDentity Applet v3.4/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS", Version 1.02, ID&Trust Ltd., 13 October 2020

[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/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).

La valutazione è di fatto iniziata nel 2016 su un ODV denominato "IDentity Applet v3.3/SSCD 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/QSCD" 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 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/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

Nome dell'ODV	IDentity Applet v3.4/QSCD on NXP JCOP 4 P71
Traguardo di Sicurezza	"Security Target IDentity Applet v3.4/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS", Version 1.02 [TDS]
Livello di garanzia	EAL4 con l'aggiunta di 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	EN 419 211-2:2013 [PPQSCD1] EN 419 211-4:2013 [PPQSCD2]
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/QSCD" è composte 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.

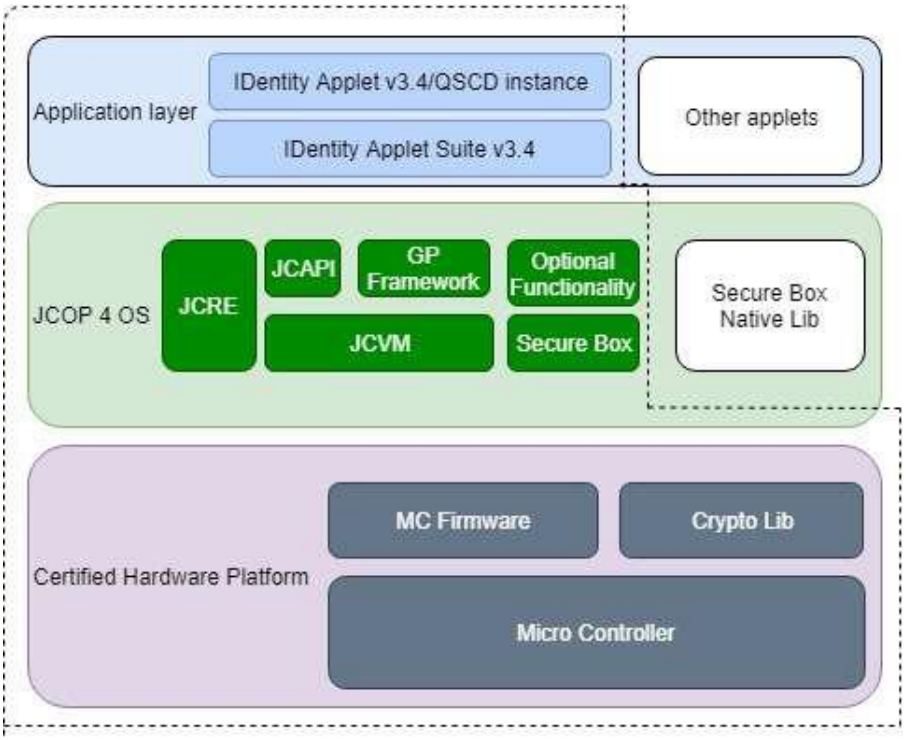


Figura 1 - Ambito logico e confini dell'ODV

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 Traguardo 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 Traguardo 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 sicure 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 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/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 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 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
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
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Advanced methodical vulnerability analysis	*AVA_VAN.5*	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

8.2 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/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 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/QSCD on NXP JCOP 4 P71", nome abbreviato "IDentity Applet v3.4/QSCD", 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/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;
- 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 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.