Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISZTERELNÖK

Honvédelmi és Nemzetbiztonsági Főtitkárság Információs

Rendszerek Nemzetbiztonsági Hivatala

ANSSI-CC-2018/24 tanúsítási jelentés

IAS „Classic” V4.4.2 MOC szerverrel, verziószám: v1.1, V4.0.1 „MultiApp”-on

Párizs, 2018. június 11.

Az Információs Rendszerek
Nemzetbiztonsági Hivatalának
vezérigazgatója

Guillaume POUPARD
[EREDETI PÉLDÁNY ALÁÍRÁSSAL ELLÁTVA]

SÉCURITÉ CERTIFICATION

Tájékoztatás

E jelentés olyan dokumentumot kíván szolgáltatni a megrendelőknek, amely lehetővé teszi számukra, hogy a jelentésben meghatározott használati és üzemeltetési feltételek között igazolják a termék értékelt verziója által kínált biztonsági szintet. A jelentés célja továbbá, hogy a termék potenciális vevője számára meghatározza az értékelés és a tanúsítás tárgyát képező feltételeket, amelyek alapot adnak az általa történő használathoz és üzemeltetéshez. Ezért a tanúsítási jelentést - amely leírja a veszélyeket, a környezetre vonatkozó feltevéseket és a feltételezett alkalmazási feltételeket - az értékelt felhasználói és adminisztrátori útmutatóval, valamint a termék biztonsági céljával együtt kell értelmezni annak érdekében, hogy a felhasználó biztonsági céljainak függvényében tudja értékelni a termék megfelelőségét.

A tanúsítás önmagában nem minősül az Információs Rendszerek Nemzetbiztonsági Hivatala (a továbbiakban francia rövidítés szerint ANSSI, agence nationale de la sécurité des systèmes d'information) általi ajánlásnak, és nem szavatolja, hogy a tanúsított termék teljes mértékben mentes a működési sérülékenységektől.

A jelentéssel kapcsolatos minden levelezést a következő névre és címre kell eljuttatni:

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification (Honvédelmi és Nemzetbiztonsági
Főtitkárság, Információs Rendszerek Nemzetbiztonsági
Hivatala, Tanúsító Központ)
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

A jelen dokumentum másolása engedélyezett, annak megváltoztatása és kivonatolása nélkül

Tanúsítási jelentés azonosítószáma

ANSSI-CC-2018/24

Termék neve

IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1

Termék azonosítószáma/verziója

IAS alkalmazás verziója: 4.4.2 MOCA
szerver alkalmazás verziója: 1.1
Java Card MultiApp platform verziója: 4.0.1

Védelmi profilnak való megfelelőség

Védelmi profilok biztonságos aláírás-létrehozó eszközhöz:

2. rész: Kulcsgenerálást tartalmazó eszköz, v2.0.1, BSI-CC-PP-0059-2009-MA-01;
3. rész: Kulcsimportálást tartalmazó eszköz, v1.0.2, BSI-CC-PP-0075-2012;
4. rész: Eszköz kiterjesztés kulcsgenerálással és tanúsítványgeneráló alkalmazással való megbízható kommunikációval, v1.0.1, BSI-CC-PP-0071-2012;
5. rész: Eszköz kiterjesztés kulcsgenerálással és aláírásgeneráló alkalmazással való megbízható kommunikációval, v1.0.1, BSI-CC-PP-0072-2012;
6. rész: Eszköz kiterjesztés kulcsimportálással és aláírásgeneráló alkalmazással való megbízható kommunikációval, v1.0.4, BSI-CC-PP-0076-2013.

Értékelési szempontok és verzió

Közös szempontok verzió: 3.1 frissítés: 5

Értékelési szint

EAL 5 +

ALC_DVS.2, AVA_VAN.5

Fejlesztő

Gemalto	Infineon Technologies AG
6, rue de la Verrerie, **92197 Meudon cedex,** **Franciaország**	**AIM CC SM PS – Am Campeon 1-12,** **85579 Neubiberg, Németország**

Megrendelő

Gemalto

6, rue de la Verrerie, 92197 Meudon cedex, Franciaország

Értékelő központ

Serma Safety & Security

14 rue Galilée, CS 10055, 33615 Pessac Cedex, Franciaország

Alkalmazandó elismerési megállapodások

CCRA

SOG-IS

E tanúsítvány EAL2 szintű elismerésnek felel meg

Előszó

A tanúsítás

Az információtechnológiai termékek és rendszerek által kínált biztonsági tanúsítást a 2002. április 18-i 2002-535 sz. módosított rendelet szabályozza. E rendelet a következőket írja elő:

- A **tanúsítási jelentéseket** az Információs Rendszerek Nemzetbiztonsági Hivatala dolgozza ki. A jelentések kifejtik az ajánlott biztonsági célkitűzések jellemzőit. Magukban foglalhatnak minden olyan tájékoztatást, amelyet a szerkesztők hasznosnak találnak megemlíteni. A megrendelők választása szerint adhatók ki harmadik személynek vagy hozhatók nyilvánosságra (7. cikk).
- A Miniszterelnök által kibocsátott **tanúsítványok** igazolják, hogy a termékek vagy rendszerek értékelésre bocsátott példánya megfelel a meghatározott biztonsági jellemzőknek. Igazolják továbbá, hogy az értékeléseket a hatályban lévő szabályok és standardok szerint, a szükséges szakértelemmel és pártatlansággal folytatták le (8. cikk).

A tanúsítási eljárások megtalálhatók a www.ssi.gouv.fr. weblapon.

Tartalomjegyzék

1. A termék

1.1. A termék ismertetése

Az értékelt termék az „IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1” alkalmazás (fejlesztő: *GEMALTO* társaság), M7892 G12 mikrovezérlőbe (gyártó: *INFINEON TECHNOLOGIES AG*. társaság).

A termék biztonságos aláírás-létrehozó eszközként (SSCD)[1] való használatra lett tervezve.

1.2. A termék leírása

1.2.1. Bevezetés

Az értékelt terméket, annak biztonsági funkcióit és üzemeltetési környezetét a biztonsági cél [ST] határozza meg.

E cél megfelel a *Biztonságos aláírás-létrehozó eszköz védelmi profiljainak* [PP-SSCD-2.rész], [PP-SSCD-3.rész], [PP-SSCD-4.rész], [PP-SSCD-5.rész] és [PP-SSCD-6.rész].

1.2.2. Biztonsági szolgáltatások

A termék által nyújtott fő biztonsági szolgáltatások a következők:

- a Java Card platform szolgáltatásai nyitott konfigurációban vagy a MultiApp V4.0.1 platform szolgáltatási zárt konfigurációban, tanúsítási szám: ANSSI-CC-2017/76 (lásd [CER-PLF]);
- SCD aláírás-létrehozó adatok (*Signature Creation Data*) importálása megbízható csatornán keresztül;
- SCD / SVD párok in situ generálása (*Signature Verification Data*);
- elektronikus aláírások generálása;
- aláírás-ellenőrzési adatok (SVD) exportálása CGA-ba (*Certification Generation Application*);
- aláírás hitelesítés PIN-kóddal vagy biometrikus ujjlenyomat-adatokkal (BioPIN);
- adminisztrátori hitelesítés (kölcsönös hitelesítés);
- védett adatok hozzáférési feltételeinek integritása, SCD és RAD (*Reference Authentication Data*);
- aláírandó adatok integritása, DTBS (*Data To Be Signed*);
- olvasott adatok integritásának és titkosságának védelme a „*Secure Messaging”* mechanizmus segítségével.

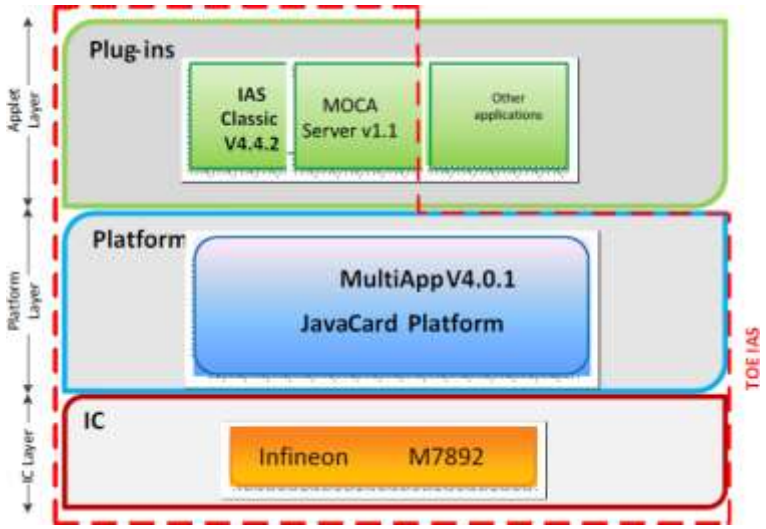
1.2.3. Architektúra

A termék a következő alkotóelemekből épül fel:

- a korábban tanúsított M7892 G12 alkotóelem (lásd [CER-IC]);

1 *Secure Signature Creation Device.*

- a korábban tanúsított Card MultiApp V4.0.1 platform (lásd [CER- PLF]);
- „IAS Classic V4.4.2” alkalmazás, melyet adatai elektronikus aláírása céljából bocsátunk a felhasználó rendelkezésére;
- „MOCA server V1.1” alkalmazás a *Match On Card* megvalósítására.



1. ábra: Az „IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1” termék architektúrája

A termék a *GEMALTO* által kifejlesztett kriptográfiai könyvtáron alapul.

A jelen értékelés körén kívüli Java alkalmazások is letölthetők a JavaCard MultiApp V4.0.1 platformra, ezeknek meg kell felelniük a [PLF_BADR] és [PLF_SADR] útmutatóknak.

1.2.4. A termék azonosítása

A termék alkotóelemei a konfigurációs listán [CONF] vannak feltüntetve.

A termék tanúsított verziójának beazonosítását a CPLC-n végzett GET DATA paranccsal a termék a jelenlévő elemek megadásával válaszol (lásd [GUIDES]):

- Az IAS Classic alkalmazás azonosítása:
  - a ‘C**0**’ tag lehetővé teszi az IAS kisalkalmazás azonosítószámának lehívását: **49 41 53 20 43 6C 61 73 73 69 63 20 76 34** (IAS Classic v4 ASCII-ben);
  - a ‘C**1**’ tag lehetővé teszi az IAS kisalkalmazás verziójának lehívását: **34 2E 34 2E 32 2E 41** (verzió: 4.4.2.A ASCII-ben).

- A MOC Server alkalmazás azonosítása:
  - az ‘A**0**’ tag lehetővé teszi a „MOC Server” alkalmazás azonosítószámának lehívását: **4D 4F 43 41 20 53 45 52 56 45 52 20 31 2E 31** (MOCA Server 1.1 ASCII-ben);
  - az ‘A**1**’ tag lehetővé teszi a „MOC Server” alkalmazás verziójának lehívását: **31 2E 31 2E 31 41** (verzió: 1.1.1A ASCII-ben).

1.2.5. Életciklus

Az értékelés köre a 1-5 szakaszokra korlátozódik, amelyek az 1. és 2. fázisnak, vagyis a fejlesztési és gyártási fázisoknak felelnek meg, a védelmi profilban [PP-0084] leírtak szerint.

Az életciklus leírását a biztonság cél [ST] 2.3.2 fejezete tartalmazza.

Az 1. és 2. szakasz a termék fejlesztésének felel meg, ami a következőket foglalja magában:
- a beágyazott szoftver, vagyis a *firmware* alkotóelemhez kapcsolódó szoftver, az operációs rendszer, a *JAVACARD* rendszer, a dokumentáció, a *kisalkalmzások* és a platform egyéb szoftverelemeinek fejlesztése;
- a komponens fejlesztése.

A 3. és 4. szakasz a termék a komponens gyártását és csomagolását tartalmazza (*packaging*).

A 5. szakasz a beágyazott szoftver betöltését foglalja magában (a *firmware* kivételével, amely már a 3. szakaszban el van rejtve a komponensben. Megjegyzendő, hogy a kártya szállítási vagy kibocsátási pontja az 5. szakasz végén áll elő.

Az 1-5. szakaszok tehát a TOE felépítésének felelnek meg. Ezek a jelen értékelésben a 2. és 3. szakaszok esetében a komponens értékelési eredményeinek újbóli felhasználásával lettek figyelembe véve. A mikrovezérlő fejlesztési és gyártási telephelyeinek részletes megjelölését a [CER-IC] azonosítószámú tanúsítási jelentés tartalmazza.

A termék fejlesztése a következő telephelyeken történik:

Gemalto Meudon 6 Rue de la Verrerie 92190 Meudon, Franciaország	Gemalto Singapore 12 Ayer Rajah Crescent Singapor 139941, Szingapúr
Gemalto Gémenos Avenue du Pic de Bretagne 13881 Gémenos, Franciaország	Gemalto La Ciotat Avenue du Jujubier, ZI Athelia IV 13705 La Ciotat, Franciaország
ATOS Paris (Aubervilliers / Croissy) 4 rue des Vieilles Vignes 77 183 Croissy-Beaubourg, Franciaország	ATOS Bydgoszcz – (ATOS Poland) Biznes Park, ul. Kraszewskiego 1 85-240 Bydgoszcz, Lengyelország
Gemalto Barcelona Poligono lndustrial Llevant CL Llevant 12, 08150 Parets del Valles, Barcelona, Spanyolország	Gemalto Montgomeryville 101 & 106 Park Drive Montgomeryville, PA 18 936 Egyesült Államok
Gemalto Curitiba Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, PR Brazília	Gemalto Vantaa Myllynkivenkuja 4, Vantaa, Finnország, FI-01620
Gemalto Tczew Ul. Skarszewska 2 33-110 Tczew, Lengyelország	Gemalto Pont Audemer Z.l. Saint Ulfrant rue de Saint Ulkfrant 27500 Pont Audemer, Franciaország

A mikrovezérlő fejlesztési és gyártási telephelyeinek részletes megjelölését a komponens tanúsítási jelentése tartalmazza (lásd [CER-IC]).

A [PLF_AGD_OPE] útmutató ajánlásokat is ad a kártya MultiApp V4.0.1 operációs rendszerén keresztül lehívható jövőbeli alkalmazások szállítására vonatkozóan.
Ezen felül a [PLF_BADR] és [PLF_SADR] útmutatók a kártyára letöltendő alkalmazások fejelsztési szabályait írják le; míg a [PLF_GTO_VA] és [PLF_THIRD_VA] útmutatók az ellenőrző hatóság által alkalmazandó hitelesítési szabályokat határozzák meg.

1.2.6. Az értékelt konfiguráció

A tanúsítás a „MOC Server 1.1 alkalmazást magában foglaló, nyílt Java Card MultiApp V4.0.1 platformra épülő, rejtett M7892 G12 komponenst tartalmazó IAS Classic V4.4.2 alkalmazásra vonatkozik, az 1.2.3 Architektúra fejezetben leírtak szerint.

A jelen értékelés keretében használt Java Card platformok az M7892 G12 mikrovezérlőből származó SLE78CLFX400**V**PHM komponensen vannak elrejtve.

A termék nyitott konfigurációjának értékelésére az [OPEN] szerint került sor: a termék nyitott „particionált” platformnak felel meg. Az új alkalmazások letöltését minden esetben az auditált folyamatok szerint kell elvégezni, a jelen tanúsítás jelentés 3.2 fejezetében bemutatott kikötések figyelembe vételével.

2. Az értékelés

2.1. Értékelési szempontrendszerek

Az értékelés elvégzésére a **Közös szempontok verzió: 3.1 frissítés: 5** [CC] és a CEM kézikönyvben meghatározott értékelési módszertan [CEM] szerint került sor.

Azon biztonsági alkotóelemek esetében, amelyek a [CEM] kézikönyvben nem szerepelnek, az értékelő központ ANSSI által jóváhagyott saját módszereit alkalmazták.

A chipkártyák sajátosságainak figyelembe vétele érdekében a [JIWG IC] és a [JIWG AP] útmutatók kerületek alkalmazásra. Így az AVA_VAN szint meghatározása a [JIWG AP] útmutatóban található értékelő skála alapján történt. Emlékeztetőül megjegyzendő, hogy ez az értékelő skála magasabb követelményeket támaszt, mint az egyéb kategóriájú termékekre (például szoftver termékekre) használt standard módszer [CC] szerinti értékelő skála.

2.2. Értékelési munkálatok

Az összetett értékelés elvégzésére a [COMP] útmutató alkalmazásával került sor, ami lehetővé tette annak ellenőrzését, hogy a szoftver integrálásával nem jelent meg hiányosság a már másutt tanúsított platformon [CER-PLF].

Az ANSSI-nek 2018. május 22-én átadott technikai értékelő jelentés részletesen leírja az értékelő központ által megvalósított értékelési munkálatokat és igazolja, hogy minden egyes értékelési feladat elvégzése
„sikeres”.

2.3. A kriptográfiai mechanizmusok értékelése az ANSSI technikai referencia-dokumentációja alapján

A kriptográfiai mechanizmusok értékelésére az ANSSI technikai referencia-dokumentációja [REF] alapján került sor. A kapott eredmények elemzési jelentés tárgyát [ANA-CRY] képezték.

Egyes elemzett kriptográfiai mechanizmusok nem felelnek meg az AINSI technikai referencia-dokumentációjának [REF], ezek nevezetesen a következők:

- az S_ENC munkamenetkulcs használata az SCP01 és SCP02 protokollokhoz kapcsolódó különböző kriptográfiai mechanizmusok során;
- az [AGD_PRE] 3.6 bekezdésében említett mechanizmusok, ha az ugyanebben a bekezdésben említett ajánlások szigorú betartása nem valósul meg.

A továbbfejlesztett minősítési folyamat keretében a CESTI elvégezte a kriptográfia megvalósulásának értékelését. Az eredményeket a független értékelő a sérülékenységi elemzés során vette figyelembe, és ezek alapján a célzott AVA_VAN.5 szinten nem mutatható ki működési sérülékenység.

2.4. A randomizer elemzése

A végtermák által használt fizikai jellegű véletlenszám-generátor értékelése a mikrovezérlő értékelésének (lásd [CER-IC]) keretében valósult meg.

Ezen felül az ANSSI kriptográfiai referencia-dokumentációjában ([REF]) előírtaknak megfelelően, a véletlenszám-generátor kimenete kriptográfiai jellegű újrafeldolgozáson megy keresztül (lásd [CER- PLF]).
Az eredményeket a független értékelő a sérülékenységi elemzés során vette figyelembe, és ezek alapján a célzott AVA_VAN.5 szinten nem mutatható ki működési sérülékenység.

3. A tanúsítás

3.1. Következtetés

Az értékelés lefolytatására a hatályban lévő szabályok és standardok szerint került sor, engedélyezett értékelő központok számára előírt a szükséges szakértelemmel és pártatlansággal. Az elvégzett értékelési munkálatok lehetővé teszik a 2002-535 rendelet szerinti tanúsítás kibocsátását.

Ez az tanúsítvány igazolja, hogy az értékelésre beterjesztett M7892 G12 komponensen elrejtett „IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1” termék teljesíti a biztonsági céljában [ST] meghatározott biztonsági jellemzőket az ALC_DVS.2 és AVA_VAN.5 alkotóelemek EAL 5 + értékelési szintjén.

3.2. Felhasználási korlátok

E tanúsítvány a jelen tanúsítási jelentés 1.2 fejezetében meghatározott termékre vonatkozik.

A tanúsított termék felhasználójának ellenőriznie kell, hogy az operációs környezet megfelel-e a biztonsági célban [ST] meghatározott biztonsági célkitűzéseknek, és követnie kell a szállított útmutatókban [GUIDES] található ajánlásokat, így nevezetesen a következőket:

- a termékre letöltött minden alkalmazásnak meg kell felelnie a platform ([PLF_BADR] és [PLF_SADR]) fejlesztési korlátainak;
- az ellenőrző hatóságoknak a [PLF_GTO_VA] és [PLF_THIRD_VA] útmutatókat kell alkalmazniuk;
- A termékre letöltött minden alkalmazás letöltésekor aktiválni kell a védelmet a [PLF_AGD_PRE] utasításai szerint;
- az SCP03 protokoll használatát kell előnyben részesíteni az SCP01 és SCP02 protokollokkal szemben, melyek használata nem javasolt. Azonban ha e két protokoll használata szükségesnek bizonyulna, ezt fizikailag biztonságos környezetben kell megtenni, a kicserélt adatok rejtjelezésével (lásd [AGD_PRE_OPE] 2.1.1 és 2.1.4 cikk).

3.3. A tanúsítvány elismerése

3.3.1. Európai elismerés (SOG-IS)

E tanúsítvány kibocsátása a SOG-IS megállapodás [SOG-IS] feltételeivel történik.

A 2010-es kölcsönös elismerésről szóló európai SOG-IS megállapodás lehetővé teszi, hogy az ITSEC tanúsítványokat és a Közös szempontokat a megállapodást aláíró országok [1] elismerjék. A chipkártyák és hasonló eszközök esetében az európai elismerés ITSEC E6 emelt szintig és CC EAL7 szintig alkalmazandó, amennyiben a CC függőségek teljesülnek. A megállapodás keretében elismert tanúsítványok a következő márkajelzéssel kerülnek kibocsátásra:

3.3.2. Nemzetközi elismerés közös szempontjai (CCRA)

E tanúsítvány kibocsátása a CCRA megállapodás [CCRA] feltételeivel történik.

A „Common Criteria Recognition Arrangement” lehetővé teszi, hogy a tanúsítványokat és a Közös szempontokat a megállapodást aláíró országok[2] elismerjék.
Az elismerés a CC EAL2 szintű biztonsági alkotóeleméig, valamint az ALC_FLR családig alkalmazandó.
A megállapodás keretében elismert tanúsítványok a következő márkajelzéssel kerülnek kibocsátásra:

1 A SOG-IS megállapodás aláíró országainak listája megtalálható a megállapodás weboldalán: .www.sogis.org 2 A CCRA megállapodás aláíró országainak listája megtalálható a megállapodás weboldalán: .www.commoncriteriaportal.org

1. sz. Melléklet - A termék értékelési szintje

Osztály	Család	Alkotóelemek biztonsági szintenként							A termékre meghatározott biztonsági szint	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Alkotóelem megnevezése
ADV Fejlesztés	ADV_ARC		1	1	1	1	1	1	1	Biztonsági architektúra leírása
	ADV_FSP	1	2	3	4	5	5	6	5	Teljes félformális funkcionális specifikáció hibákra vonatkozó kiegészítő információkkal
	ADV_IMP				1	1	2	2	1	Implementáció TSF érvényesülés
	ADV_INT					2	3	3	2	Megfelelő belső felépítés
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	4	Félformális moduláris dizájn
AGD Felhasználói útmutatók	AGD_OPE	1	1	1	1	1	1	1	1	Működési felhasználói útmutató
	AGD_PRE	1	1	1	1	1	1	1	1	Előkészítő eljárások
ALC Életciklus támogatása	ALC_CMC	1	2	3	4	4	5	5	4	Támogatás, elfogadási eljárások és automatizálás
	ALC_CMS	1	2	3	4	5	5	5	5	CM lefedési eszközök fejlesztése
	ALC_DEL		1	1	1	1	1	1	1	Átadási eljárások
	ALC_DVS			1	1	1	2	2	2	Biztonsági intézkedések elégségessége
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	1	Fejlesztő által meghatározott Életciklus modell
	ALC_TAT				1	2	3	3	2	Végrehajtási standardoknak való megfelelés
ASE Biztonsági cél értékelése	ASE_CCL	1	1	1	1	1	1	1	1	Megfelelőségi állítások
	ASE_ECD	1	1	1	1	1	1	1	1	Kiterjesztett alkotóelemek meghatározása
	ASE_INT	1	1	1	1	1	1	1	1	ST bevezetés
	ASE_OBJ	1	2	2	2	2	2	2	2	Biztonsági célok
	ASE_REQ	1	2	2	2	2	2	2	2	Származtatott biztonsági követelmények
	ASE_SPD		1	1	1	1	1	1	1	Biztonsági probléma meghatározása
	ASE_TSS	1	1	1	1	1	1	1	1	TOE összefoglaló specifikáció
ATE Tesztelés	ATE_COV		1	2	2	2	3	3	2	Lefedettségi elemzés
	ATE_DPT			1	1	3	3	4	3	Tesztelés: moduláris dizájn
	ATE_FUN		1	1	1	1	2	2	1	Funkcionális tesztelés
	ATE_IND	1	2	2	2	2	2	3	2	Független fél általi tesztelés: minta
AVA Sérülékenységek értékelése	AVA_VAN	1	2	2	3	4	5	5	5	Részletes módszertani sérülékenységi elemzés

2. sz. Melléklet - Az értékelt termék dokumentumhivatkozásai

[ST]	Az értékelés hivatkozott biztonsági célja - MultiApp V4.0.1: IAS EN Core & Extensions Security Target (IAS EN Alap és kiterjesztett biztonsági cél), azonosítószám: D1433429, verzió: 1.6, 2018. május 4., *GEMALTO*. A közzétételi igényekhez a következő biztonsági cél megadására és jóváhagyására került sor a jelen értékelés keretében: - IAS Classic V4.4.2 with MOC Server 1.1 on MultiApp V4.0.1 Security Target Lite, azonosítószám: D1433429, verzió: 1.6p, *GEMALTO*.
[RTE]	Technikai értékelő jelentés: - Evaluation Technical Report (Technikai értékelő jelentés) - CASSIDY-I Projekt, azonosítószám: CASSIDY-I_ETR_v1.1 / 1.1, verzió: 1.1, 2018. május 22., *SERMA SAFETY & SECURITY*.
[ANA-CRY]	Cryptographic Mechanisms Evaluation Report (Kriptográfiai mechanizmusok értékelési jelentése) - CASSIDY I Projekt, azonosítószám: CASSIDY-I_IAS_cryptography_v1.2/1.2, verzió: 1.2, 2018. május 22., *SERMA SAFETY & SECURITY*.
[CONF]	A termék konfigurációs listája: - MultiApp V4.0.1: ALC LIS document (ALC LIS dokumentum)– IAS Classic v4.4.2, azonosítószám: D1439244, verzió: 1.5, 2018. május 4., *GEMALTO*.

[ÚTMUTATÓK]:	
[AGD_PRE_OPE]	- MultiApp V4.0.1: AGD OPE and PRE document (AGD OPE és PRE dokumentum) - IAS v4.4.2, verzió: 1.3, azonosítószám: D1438665, 2018. április 12., *GEMALTO*;
[AGD_PRE]	- Card Personalization Specification requirement for SSCD security evaluation IAS Classic v4.4 (Kártya személyre szabásra vonatkozó specifikáció követelményei az „IAS Classic v4.4 SSCD biztonsági értékeléséhez), verzió: 1.2, azonosítószám: WG.RND.5.0026, 2018. január 22., *GEMALTO*;
[AGD-OPE-IAS]	- IAS Classic Applet V4.4, Reference Manual (Referencia-kézikönyv), azonosítószám: D1387713J, 2017. szeptember 26., *GEMALTO*; - BioPIN Manager V2.0 – Reference Manual (Referencia-kézikönyv), azonosítószám: D1290692C, 2016. október 26., *GEMALTO* ; - IAS Classic Applets – Personalization Profiles Guides (IAS Classic Kisalkalmazások – Profil testreszabási útmutató), azonosítószám: D1203913G, 2017. április 27., *GEMALTO*;
[GUIDES_PLF]:	
[PLF_BADR]	- Rules for applications on Multiapp certified product (Multiapp tanúsítvánnyal rendelkező termékekre vonatkozó alkalmazások szabályai); azonosítószám: D1390963, verzió: 1.2, 2017 novembere, *GEMALTO*;
[PLF_SADR]	- Guidance for secure application development on Multiapp platforms (Útmutató a biztonságos alkalmazásfejlesztéshez Multiapp platformokon), azonosítószám: D1390326, verzió: A01, 2016 februárja, *GEMALTO*;
[PLF_GTO_VA]	- Verification process of Gemalto non sensitive applet (A Gemalto nem érzékeny kisalkalmazásának ellenőrzési folyamata), azonosítószám: D1390670, verzió: A01, 2016. február, *GEMALTO*;
[PLF_THIRD_VA]	- Verification process of Third Party non sensitive applet (Harmadik fél nem érzékeny kisalkalmazásának ellenőrzési folyamata), azonosítószám: D1390671, verzió: A01, 2016. február, *GEMALTO*;
[PLF_AGD_PRE]	- MultiApp V4.0.1 AGD_PRE dokumentum - Javacard Platform, azonosítószám: D1431347, verzió: 1.0, 2017. szeptember 28., *GEMALTO*;
[PLF_AGD_OPE]	- MultiApp V4.0.1 Javacard Platform AGD_OPE dokumentum, azonosítószám: D1432683, verzió: 1.1, 2017. szeptember 28., *GEMALTO*.
[PP-SSCD-Part2]	Protection profiles for secure signature creation device (Védelmi profilok biztonságos aláírás-létrehozó eszközhöz) – 2. rész: Device with key generation (Kulcsgenerálást tartalmazó eszköz), azonosítószám: prEN 14169-2:2012, verzió: 2.0.1, 2012. január 23. *A BSI (Bundesamt für Sicherheit in der Informationstechnik) által fenntartva 2012. február 21-én BSI-CC-PP-0059-2009-MA-01 azonosítószám alatt.*
[PP-SSCD-Part3]	Protection profiles for secure signature creation device (Védelmi profilok biztonságos aláírás-létrehozó eszközhöz) – 3. rész: Device with key import (Kulcsimportálást tartalmazó eszköz), azonosítószám: prEN 14169-3:2012, verzió: 1.0.2, 2012. július 24. *A BSI által tanúsítva 2012. szeptember 27-én BSI-CC-PP- 0075-2012 azonosítószám alatt.*

[PP-SSCD-Part4]	Protection profiles for secure signature creation device (Védelmi profilok biztonságos aláírás-létrehozó eszközhöz) – 4. rész: Extension for device with key generation and trusted communication with certificate generation application (Eszköz kiterjesztés kulcsgenerálással és tanúsítványgeneráló alkalmazással való megbízható kommunikációval), azonosítószám: prEN 14169-4:2012, verzió: 1.0.1, kelt 2012. november 14-én. *A BSI által tanúsítva 2012. december 12-én BSI-CC-PP- 0071-2012 azonosítószám alatt.*
[PP-SSCD-Part5]	Protection profiles for secure signature creation device (Védelmi profilok biztonságos aláírás-létrehozó eszközhöz) – 5. rész: Extension for device with key generation and trusted communication with certificate generation application (Eszköz kiterjesztés kulcsgenerálással és aláírásgeneráló alkalmazással való megbízható kommunikációval), azonosítószám: prEN 14169-5:2012, verzió: 1.0.1, kelt 2012. november 14-én. *A BSI által tanúsítva 2012. december 12-én BSI-CC-PP- 0072-2012 azonosítószám alatt.*
[PP-SSCD-Part6]	Protection profiles for secure signature creation device (Védelmi profilok biztonságos aláírás-létrehozó eszközhöz) – 6. rész: Extension for device with key generation and trusted communication with certificate generation application (Eszköz kiterjesztés kulcsimportálással és aláírásgeneráló alkalmazással való megbízható kommunikációval), azonosítószám: prEN 14169-6:2013, verzió: 4.0.1, kelt 2013. április 3-án. *A BSI által tanúsítva 2013. április 16-án BSI-CC-PP- 00712013 azonosítószám alatt.*
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages (Védelmi profil, biztonsági IC platform védelmi profilbővítési csomagokkal), verzió: 1.0, 2014. január 13. *A BSI (Bundesamt für Sicherheit in der Informationstechnik) által tanúsítva BSI-PP-0084-2014 azonosítószám alatt.*
[CER-PLF]	JavaCard MultiApp V4.0.1 platform- PACE nyitott, rejtett konfigurációval az M7892 G12 alkotóelemen. *Az ANSSI által tanúsítva 2017. december 18-án ANSSI-CC- 2017/76 azonosítószám alatt.*
[CER-IC]	Tanúsítási jelentés, azonosítószáma: BSI-DSZ-CC-0891-V2-2016, tanúsítás tárgya: Infineon Security Controller M7892 Design Steps D11 és G12 RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01 opcióval és eszközkészlettel v2.03.008 könyvtárak, v2.02.010 szimmetrikus crypto-könyvtár és specifikus IC dedikált szoftver (firmware) az Infineon Technologies AG-től. A BSI (Bundesamt für Sicherheit in der Informationstechnik) által tanúsítva 2016. december 20-án BSI-DSZ-CC-0891-V2-2016 azonosítószám alatt.

3. sz. Melléklet - A tanúsításhoz kapcsolódó hivatkozások

2002. április 18-i 2002-535 sz. módosított rendelet az információtechnológiai termékek és rendszerek által kínált biztonság értékeléséről és biztonságáról.	
[CER/P/01]	ANSSI-CC-CER-P-01 eljárás - Az információtechnológiai termékek, rendszerek, védelmi weboldalak és profilok által kínált biztonság közös tanúsítási szempontjai, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation (Az információtechnológia biztonsági értékelésének közös szempontjai): - 1. rész: Introduction and general model (Bevezetés és általános modell), 2017 áprilisa, verziószám: 3.1, frissítés: 5, azonosítószám: CCMB-2017-04-001; - 2. rész: Security functional components (Funkcionális biztonsági alkotóelemek), 2017 áprilisa, verziószám: 3.1, frissítés: 5, azonosítószám: CCMB-2017-04-002; - 3. rész: Security assurance components (Biztonsági alkotóelemek), 2017 áprilisa, verziószám: 3.1, frissítés: 5, azonosítószám: CCMB-2017-04-003;
[CEM]	Common Methodology for Information Technology Security (Az információtechnológia közös biztonsági módszertana): Evaluation Methodology (Értékelési módszertan), 2017 áprilisa, verziószám: 3.1, frissítés: 5, azonosítószám: CCMB2017-04-004;
[JIWG IC]	Mandatory Technical Document - The Application of CC to Integrated Circuits (Kötelező műszaki dokumentáció - CC alkalmazása integrált áramköröknél), verziószám: 3.0, 2009 februárja.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smartcards (Kötelező műszaki dokumentáció - Támadási potenciál alkalmazása intelligens kártyákra), verziószám: 2.9, 2013 januárja.
[COMP] *	Mandatory Technical Document - Composite product evaluation for Smart Cards and similar devices (Kötelező műszaki dokumentáció -Intelligens kártyák és hasonló eszközök összetett termékértékelése), verziószám: 1.2, 2012 januárja.
[OPEN]	Certification of „Open” smart card products („Open” intelligens kártyák tanúsítása), verziószám: 1.1 (kísérleti használatra), 2013. február 4.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Megállapodás a közös szempontokon alapuló tanúsítványok elismeréséről az informatikai biztonság területén), 2014. július 2.
[SOG-IS]	„Mutual Recognition Agreement of Information Technology Security Evaluation Certificates” (megállapodás az információtechnológia biztonsági értékelésének kölcsönös elismeréséről), verziószám: 3.0, 2010. január 8., Irányítóbizottság.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques (Kriptográfiai mechanizmusok - A kriptográfiai mechanizmusok kiválasztására és méretezésére vonatkozó szabályok és ajánlások), verziószám: 2.03, 2014. február 21., csatolva az Általános biztonsági hivatkozási dokumentációhoz (RGS_B1), lásd www.ssi.gouv.fr.

*SOG-IS dokumentum; a CCRA elismerésére vonatkozó megállapodás keretében az egyenértékű CCRA segéddokumentációt kell alkalmazni.