Fordítás

ZÁRADÉK

Amely tanúsítja, hogy jelen fordítást az Enviroclean Hungary Kft. - Fordítóiroda készítette. Igazoljuk, hogy a fordítás, valamint a nekünk eredetiként felmutatott és a fordításhoz csatolt anyag, tartalmában mindenben megegyezik.

ENVIROCLEAN HUNGARY KFT. FORDÍTÓ-IRODA

ENVIROCLEAN HUNGARY KFT. FORDÍTÓ-IRODA

A fordítás eredetiségét igazolom:

Szökröny Tamás
Ügyvezető

ENVIROCLEAN HUNGARY KFT. FORDÍTÓ-IRODA

Budapest, 2010. október 20.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISZTERELNÖK

Nemzetvédelmi Főtitkárság

Informatikai rendszerek biztonsági főigazgatósága

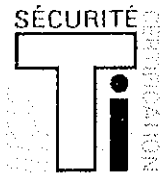
DCSSI-2009/07 Tanúsítási jelentés
MultiApp ID Citizen 72K
(Generic configuration)

S3CC91C alkotóelem JC/GP platform maszkkal
MultiApp v1.1 IAS Classic v3.0 elektronikus aláírási applettel

Párizs, 2009. április 23.

Informatikai rendszerek biztonsági főigazgatója

[HIVATALOS ALÁÍRÁS]



Figyelmeztetés

A jelentés célja, hogy olyan dokumentumot szolgáltasson a megbízók számára, amely tanúsítja a termék biztonsági szintjét a jelentésben meghatározott felhasználási vagy alkalmazási feltételek esetén. A potenciális vevő számára megadja azokat a feltételeket, amelyek mellett használhatja vagy alkalmazhatja a terméket, és amelyek megfelelnek a termék értékelése és tanúsítása során megadott feltételeknek. A jelentést ezért a kezelési és felhasználási kézikönyvvel együtt kell áttanulmányozni, a termék biztonsági célkitűzéseinek beazonosításával, amelyek pontosan meghatározzák a környezeti feltételezéseket és veszélyforrásokat, valamint a tervezett felhasználási feltételeket, így lehetővé teszik a felhasználó számára annak eldöntését, hogy a termék alkalmas-e saját biztonsági célkitűzéseinek elérésére.

A tanúsítvány önmagában nem jelent ajánlást az informatikai rendszerek biztonsági főigazgatósága részéről (DCSSI) és nem garantálja, hogy a tanúsítás tárgyát képező termék teljesen hibamentes.

Kérjük, hogy a jelentéssel kapcsolatos leveleket az alábbi címre küldjék:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

A tanúsítási jelentés hivatalos jelölése **DCSSI-2009/07**
A termék neve **MultiApp ID Citizen 72K** **(Generic configuration)**
A termék jelölése / verziója **T1003982 referencia** **S3CC91C alkotóelem, 0. felülvizsgálat, JC/GP platform maszkkal** **MultiApp 1.1 verzió, az IAS Classic 3.0 verzió elektronikus aláírás applettel**
Védelmi profil megfelelőség **BSI-PP0005-2002: SSCD 2. típus 1.04 verzió** **BSI-PP0006-2002: SSCD 3. típus 1.04 verzió**
Értékelési szempontok és verzió Közös Szempontok 2.3 verzió az ISO 15408:2005 szabvány alapján
Értékelési szint EAL 4 emelt szint ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4
Fejlesztők **Gemalto** **La Vigie, Avenue du Jujubier** **Z.I. Athelia IV, 13705 La Ciotat, Franciaország** **Samsung Electronics** **La Boursidière, RN186, Bat. Jura BP202,** **92357 le Plessis Robinson, Franciaország**
Megrendelő **Gemalto** **La Vigie, Avenue du Jujubier** **Z.I Athelia IV, 13705 La Ciotatm Franciaország**
Értékelő központ **Serma Technologies** **30 avenue Gustave Eiffel, 33608 Pessac, Franciaország** **Tel: +33 (0)5 57 26 08 75, mél: e.francois@serma.com**
Elismerésről szóló egyezmények **CCRA** **SOG-IS** IT Security Certified **A termék EAL4 szintű elismeréssel rendelkezik.**

Előszó

Tanúsítás

A termék és az informatikai technológiai rendszerek biztonsági tanúsítási eljárását a 2002. április 18-i 2002-535 számú rendelet szabályozza, amely megjelent a Francia Köztársaság közlönyében. A rendelet kimondja:

- Az informatikai rendszerek biztonsági főigazgatósága dolgozza ki a tanúsítási jelentéseket. Ezek a jelentések határozzák meg az elérni kívánt biztonsági célokat. Tartalmazzák mindazokat a figyelmeztetéseket, amelyeket a jelentések összeállítói a biztonság érdekében szükségesnek tartanak. A vevők döntik el, hogy a jelentést harmadik személyek számára hozzáférhetővé teszik-e, illetve, hogy nyilvánosságra hozzák-e (7. cikkely).
- A Miniszterelnök által kiadott tanúsítványok igazolják, hogy az értékelés tárgyát képező termékek vagy rendszerek megfelelnek a biztonsági specifikációknak. Azt is tanúsítják, hogy az értékeléseket a hatályos normáknak és szabályoknak megfelelően bonyolították le az elvárt szakértelemmel és pártatlansággal (8. cikkely).

A tanúsítási eljárás hozzáférhető az interneten: www.ssi.gouv.fr.

Tartalomjegyzék

1. A Termék

1.1 A termék leírása

A vizsgált termék a *MultiApp ID Citizen 72K* kártya generikus konfigurációja. A termék azonosítója „ IAS Classic v3.0 / MultiApp v.1.1 T1003982 on S3CC91C rev.0". A chipkártya 2 és 3 típusú elektronikus aláírás biztonságos létrehozásához használható (SSCD).

A kártya egy biztonságos ellenőrző mikroprocesszorból áll: S3CC91C rev.0. A RISC 16 bites ellenőrző mikroprocesszor fel van szerelve egy TORNADO kriptográfiai processzorral és egy TORNADO RSA 3.5S Samsung Electronics gyártmányú könyvtárral, amelyet 2007 szeptemberében a BSI tanúsított [Certif_IC] a BSI-DSZ-CC-0451-2007 referencia alapján. Tartozik hozzá egy nyílt Java MultiApp 1.1 verziójú platform, amelyet a Gemalto fejlesztett ki a Java Card v2.2.1 és Global Platform v2.1 specifikációinak megfelelően, ez tartalmaz egy operációs rendszert az S3CC91C elembe építve. A platform több appletet is támogat, ezeket is a Gemalto fejlesztette ki, az előbb említett alkotóelemtől függetlenül. Az appletek a ROM-ra vagy az EEPROM-ra vannak telepítve. A ROM-on tárolt IAS 3.0 Classic verzió a termék fő appletje, ez szolgáltatja az elektronikus aláírási szolgáltatásokat.

A termék több appletet is tartalmaz. Csak az IAS Classic applet van inicializálva. A termék a különböző konfigurációk alapján diverzifikálható (1.2.5 pont), a többi applet inicializálásával. Ha egy applet nincs inicializálva és nem is lehet inicializálni, dezaktiválva van.

Az összes inicializálható applet nem volt az értékelés tárgya, de mégis figyelembe vettük őket, hogy a termék gyengeségeit megtaláljuk.

A jelen tanúsítvány tárgyát képező konfiguráció (1.2.5. pont) csak a ROM-on tárolt három appletet határozza meg: MPCOS, OATH és Biomatch C API & Crytomanager. A ROM többi appletje nem aktív, az EEPROM-on pedig egyetlen applet sincs.

1.2 A vizsgált termék leírása

A biztonsági cél [ST] meghatározza a vizsgált terméket, annak funkcióit és felhasználási környezetét.
A biztonsági cél az alábbi védelmi profiloknak felel meg:

- „Secure Signature-Creation Device Type 2 Version: 1.04" BSI-PP-0005-2002 referencia [PP0005];
- „Secure Signature- Creation Device Type 3 Version: 1.05" BSI-PP-0006-2002 referencia [PP0006];

1.2.1 A termék beazonosítása

A termék tanúsított változata a konfigurációs listában felsorolt összetevők alapján azonosítható [CONF]. Az azonosító elemek elérhetők a „Get Data" parancs segítségével. Az értékek között találjuk az alábbiakat:

- Card Identity Data = B0 85 13 1C 01 04 42 50 00 C8 00 00 00 00 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 00 00 00 00;
- Gemalto Family Name: Java Card: B0h;
- Gemalto OS Name: MultiApp ID v1.1:85h;
- Gemalto Mask Number: MSA081:13h;
- Gemalto product Name: IAS CC configuration: 1Ch;
- Gemalto Flox version: 01h;
- Gemalto filter set: Filter 01, version 4:04h;
- Chip Manufacturer: Samsung: 4250h;
- Chip version: S3CC91C: 00C8h;

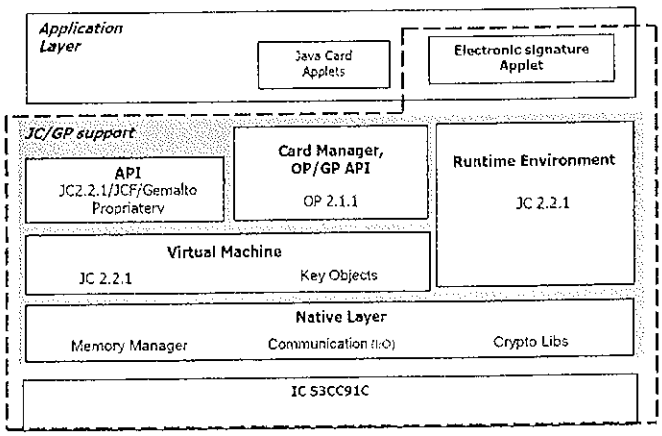
Az azonosítókhoz rendelt értékek a termék felhasználói kézikönyvében szerepelnek (GUIDEST).

1.2.2 Biztonsági szolgáltatások

A termék rendelkezik az elektronikus aláíráshoz kapcsolódó biztonsági funkciókkal és ezek használatát csak a biztonságos kommunikációs csatornákon keresztül biztosítja. A szoftver rendelkezik a „aláírások biztonságos létrehozását célzó eszközzel" (SSCD), amely lehetővé teszi aláírások létrehozási adatainak generálását és importálását (SCD), az aláírások ellenőrzését (SVD) és minősített elektronikus aláírások létrehozását. A termék védi az SVD-ket és csak engedélyezett felhasználókra korlátozza a használatukat.

1.2.3 Felépítés

A termék felépítését az alábbi 1. ábra mutatja.



1. ábra – A termék felépítése

A termék egy chipkártya, amely az alábbi elemekből áll:

- S3CC91C rev.0 egység RSA Tornado 3.5S kriptográfiai könyvtárral;
- nyitott platformú OS, JavaCard/GlobalPlatform: MultiApp, 1.1 verzió, JCVM-mel felszerelve;
- IAS Classic v3.0 applet elektronikus aláíráshoz és adataihoz;
- egyéb inicializálható appletek, amelyek nem tartoznak az értékelés hatáskörébe.

1.2.4 Életciklus

A termék életciklusa több szakaszból áll, ezeket a fejlesztők különböző telephelyeken dolgozták ki.

A fejlesztésben résztvevő egységek a következők:

- Gemalto Meudon: kutatási-fejlesztési központ, itt dolgozták ki az OS-t, a Java Card platformot, az IAS Classic appletet, és itt tervezték meg az előbeállításokat;
- Samsung Electronics Giheung (wafer line 6, Korea): az IC tervezése és gyártása.

A Gemalto többi telephelye is részt vett a termékfejlesztés egyéb szakaszaiban:

- Gemalto Gémenos és Pont-Audemer: gyártó telepek (back-up), amelyek a mikro-modulokká történő összeállítást végzik;
- Gemalto Vantaa és Gémenos: gyártó telepek (back-up), amelyek az összeállítást és az előbeállítást végzik.

A telephelyeket auditáltatták (2.2), hogy garantálni lehessen az ALC_DVS minőségbiztosítási feltételek betartását.

A vizsgálat tárgyát képező termékfejlesztési eljárási szakaszok leírása a következő (2. ábra):

1. szakasz (Gemalto Meudon):
   - a beépített szoftver fejlesztése

2. szakasz (Samsung Giheung)[1]:
   - a integrált áramkör és a beépített szoftver tervezése
   - az ügyfélkód kezelése
   - az adatok előkészítése a maszkhoz
   - a maszkok gyártása

3. szakasz (Samsung Giheung):
   - a mikro-áramkör gyártása
   - tesztelés
   - a szilícium lemez csiszolása és levágása (*wafers*).

[1] A Samsung a maszkok gyártását alvállalkozókkal is végeztetheti. A Samsung S3CC91C rev.0 alkotóelem életciklusával kapcsolatos részletek a BSI hitelesítési jelentésben olvashatók (referencia: BSI-DSZ-CC-0451-2007).

4. szakasz (Gemalto Gémenos / Pont-Audemer):
- a chipek összeállítása mikro-modulokká

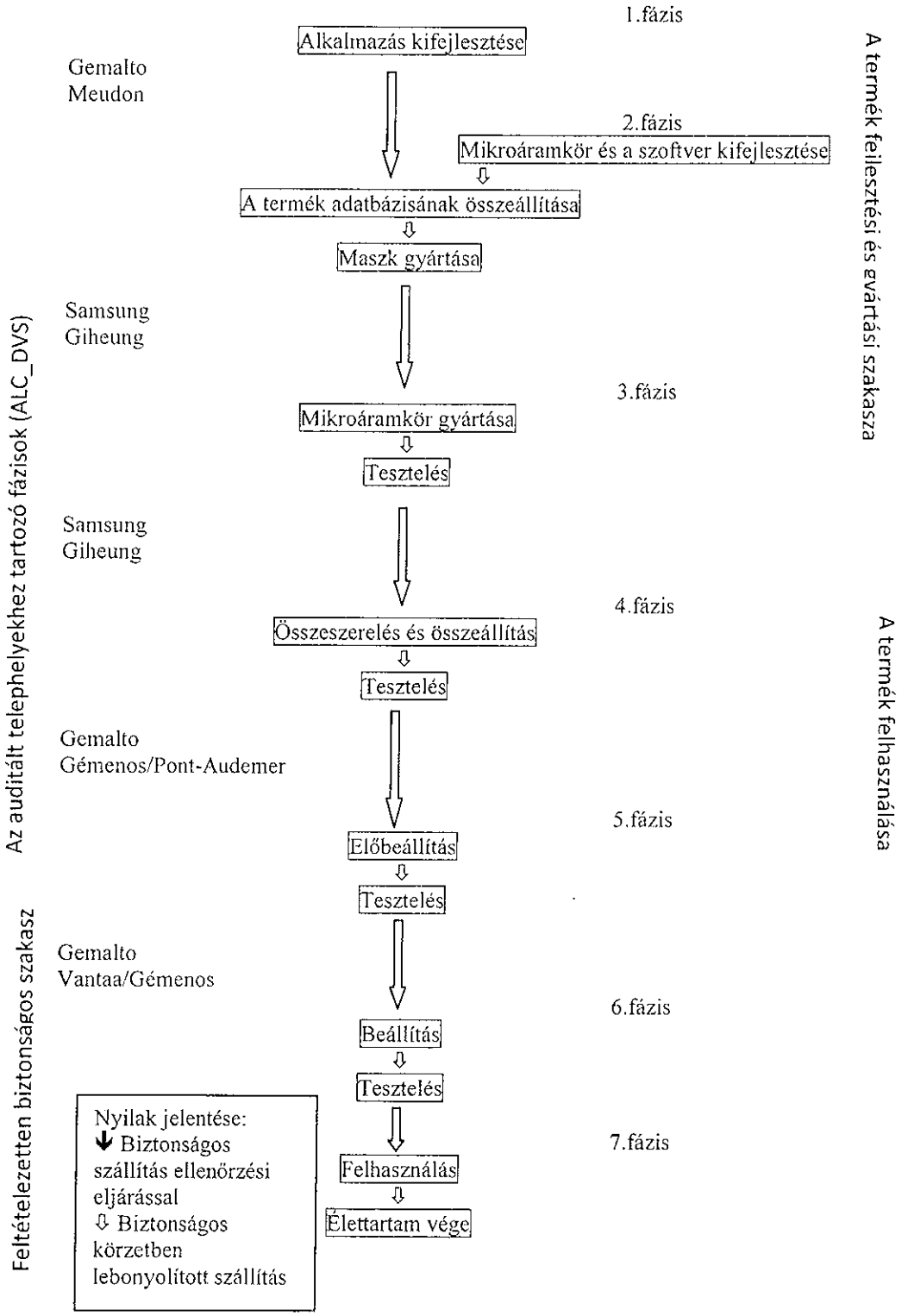
5. szakasz (Gemalto Vantaa / Gémenos):
- összeállítás (*packaging*)
- előbeállítások és egy esetleges patch betöltése az EEPROM-ba

6. szakasz (értékelésen kívül)
- személyre szabás

Az egyes fejlesztési fázisok közötti átmenetek során titkos adatok átadására kerül sor, ezek lehetnek logikai adatok (tervezési adatok, forráskódok) vagy fizikai adatok (fejlesztési fázisban lévő termékminta).

Az alábbi műveletek biztonságát kell garantálni:
- az alkalmazás fejlesztője által használt útmutató és szoftver (1. fázist megelőzően);
- a beépített szoftver kódja a mikroprocesszor gyártója számára (1. és 2. fázis között);
- a maszk gyártója számára szükséges adatok (a 2. fázis során: alvállalkozás);
- maszkok a mikroprocesszor gyártója számára (2. és 3. fázis között);
- mikroprocesszorok az összeszerelő és összeállító egység számára (3. és 4. fázis között),
- kártyák az előbeállításokhoz (4. és 5. fázis között);
- előbeállított kártyák a beállításokhoz (5. és 6. fázis között).

Az életciklus alapján a vizsgált termék az 5. szakaszból, az előbeállításból kilépő termék. Az azt követő ciklusokat lefedi a termék kézikönyve [GUIDES].



2. ábra – A termék életciklusa

1.2.5 Vizsgált konfiguráció

A vizsgált, generikus konfiguráció neve *Generic configuration.* A konfiguráció inicalizálja az IAS Classic appletet, ugyanakkor három másik applet inicializálását is lehetővé teszi: MPCOS, OATH és Biomatch C API & Cryptomanager. A ROM többi appletje nem aktív, az EEPROM-on pedig nincsenek appletek.

A hitelesítés a termék alábbi funkcióira vonatkozik:

IC funkciók:

- véletlenszerű generálás (DRNG)
- kriptográfiai eszközök:
  - TDES processzor
  - TORNADO processzor (az RSA-t gyorsítja 2048 bit-re)
- RSA Tornado 3.4S könyvtár (a gyártásnál opcionálisan beépíthető, a Gemalto nem használja)
- ISO7816 interface
- memória védelem (MPU)
- hozzáférési ellenőrzés
- védelem a rejtett csatornákon keresztül adatkiszivárogtatás és kifigyeléses támadások ellen
- a környezeti feltételek megsértése elleni védelem
- a tesztelési és a normál üzemmód megfordíthatóságának megakadályozása

Java Card platform funkciói:

- az alkalmazások biztonságos telepítése
- tűzfal (az alkalmazások egymástól történő leválasztását is lehetővé teszi)
- az érzékeny eszközök épségének ellenőrzése
- a kriptográfia implementációja (Gemalto könyvtár RSA-1024 2048 bitre, RSA CRT, SHA-1 és SHA-256)
- kulcsok kezelése
- biztonságos kommunikáció
- hitelesítés
- az érzékeny eszközök védelmének kezelése az adatkiszivárogtatás és a fizikai támadások ellen
- ellenintézkedések implementációja az OS-en belül a kifigyeléses támadások és a hiba-injektálások ellen.

IAS Classic (SSCD2 & SSCD3) applet funkciói

- hitelesítések kezelése
- műveletek és hozzáférés ellenőrzésének kezelése
  - aláírások létrehozása
  - aláírások létrehozási és ellenőrzési adatainak generálása
  - aláírások létrehozási adatainak tárolása és importálása

    - aláírások ellenőrzési adatainak exportálása
- kriptográfia kezelése
- érzékeny adatok épségének kezelése
- biztonságos kommunikáció kezelése

2. Értékelés

2.1 Értékeléssel kapcsolatos referenciák

A értékelést a **Közös Szempontok 2.3 verziója** [CC] alapján és a CEM [CEM] kézikönyvben megadott értékelési módszerek alapján végeztük.
Az EAL4 felső szintű biztonsági elemek esetében az értékelő központ által használt, a DCSSI által jóváhagyott és a dokumentummal [AIS 34] kompatibilis módszereket alkalmaztunk.
A chipkártyák jellemzőinek kiértékeléséhez az [CC IC] és a [CC AP] kézikönyvet használtuk.

2.2 Értékelési munka

A felépítés értékelését a [COMP] kézikönyv alapján végeztük annak ellenőrzésére, hogy semmiféle hiba nem került a rendszerbe, amikor a szoftvert telepítették a már hitelesített mikroprocesszorra [Certif_IC].

Az értékelés során figyelembe vettük az „S3CC91C, rev.0 RSA Tornado 3.5S könyvtárral felszerelt" mikroprocesszor értékelésének eredményeit [RTE_IC], az ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 és az AVA_VLA.4 alkotóelemek megnövelt EAL4 biztonsági szintjén, a biztonsági célnak megfelelően [ST_IC], amely a BSP-PP-0002-2001 referencia védelmi profilon alapul [PP-0002]. A mikroprocesszort a BSI hitelesítette 2007. szeptember 10-én, BSI-DSZ-CC-0451-2007 szám alatt [Certif_IC].

Az értékelés ugyanakkor támaszkodott a korábbi tanúsítási eljárásokban elvégzett értékelések eredményeire [2008/04], (hasonló termék, de más a HW alkotó elem és az OS), [2008-45], (EAC útlevél). Az eredmények újrafelhasználása elsősorban a fejlesztési környezet, a konfiguráció kezelőrendszere és a szállítási eljárások terén történt, valamint a CESTI Serma Technologies és a német CESTI Tüv-IT által a telephelyekkel kapcsolatban elvégzett audit terén.

A DCSSI számára 2009. január 8-án átadott műszaki értékelési jelentés [RTE] részletesen leírja az értékelési központ által elvégzett munkát és tanúsítja, hogy valamennyi értékelési feladat sikerrel járt.

2.3 A kriptográfiai mechanizmusok ellenállásának elemzése

A DCSSI nem elemezte a kriptográfiai mechanizmusok ellenállását.

3. A tanúsítás

3.1 Konklúzió

Az értékelést a hatályban lévő szabályok és normák betartásával végeztük, a hivatalos értékelő központoktól elvárt kompetenciával és pártatlansággal. Az értékelési eredmények alapján kiadható a tanúsítvány a 2002-535. rendelet alapján.

A tanúsítvány igazolja, hogy a vizsgálat tárgyát képező *MultiApp ID Citizen 72K (Generic configuration)* termék megfelel a biztonsági célkitűzésben [ST] a megnövelt EAL4 szinthez előírt biztonsági jellemzőknek.

3.2 Felhasználási korlátok

A jelen tanúsítvány a jelentés 1.2 pontjában leírt termékre vonatkozik.

A tanúsítvánnyal rendelkező termék felhasználója köteles ellenőrizni, hogy a 4.2 pontban leírt biztonsági célkitűzésben [ST] meghatározott környezeti biztonsági feltételek adottak és követnie kell a használati kézikönyvben található ajánlásokat [GUIDES].

3.3 A tanúsítvány elismerése

3.3.1 Európai elismerés (SOG-IS)

A jelen tanúsítványt a SOG-IS [SOG-IS] egyezményben megszabott feltételek mellett adtuk ki.

Az 1999-es európai SOG-IS egyezmény lehetővé teszi, hogy az egyezményt aláíró országok[2] kölcsönösen elismerjék az ITSEC tanúsítványokat és a Közös Szempontokat. Az európai elismerés az ITSEC E6 és CC EAL7 szintekig terjed. Az egyezmény keretében elismert tanúsítványokon a következő jelzés szerepel:

[2] A SOG-IS egyezmény aláírói: Németország, Spanyolország, Finnország, Franciaország, Görögország, Olaszország, Norvégia, Hollandia, Egyesült Királyság és Svédország.

3.3.2 *Nemzetközi elismerés a Közös Szempontok alapján (CCRA)*

A jelen tanúsítványt a CCRA [CC RA] egyezményben megszabott feltételek mellett adtuk ki.

A „Common Criteria Recognition Arrangement" egyezmény lehetővé teszi, hogy az egyezményt aláíró országok[3] kölcsönösen elismerjék a Közös Szempontok alapján kiadott tanúsítványokat. Az elismerés a CC EAL4 biztonsági szintű alkotó elemekre és az ALC_FLR termékcsaládokra vonatkozik. Az egyezmény keretében elismert tanúsítványokon a következő jelzés szerepel:

[3] A CCRA egyezmény aláírói: Németország, Ausztrália, Ausztria, Kanada, Dánia, Spanyolország, Egyesült Államok, Finnország, Franciaország, Görögország, Magyarország, India, Izrael, Olaszország, Japán, Malajzia, Norvégia, Új-Zéland, Pakisztán, Hollandia, Koreai Köztársaság, Cseh Köztársaság, Egyesült Királyság, Szingapúr, Svédország és Törökország.

A termék értékelési szintje

Osztály	Család	Alkotó elemek biztonsági szint szerint							A termékhez elvárt biztonsági szint	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Alkotóelem neve
ACM Konfiguráció kezelése	ACM_AUT				1	1	2	2	1	Partial CM automation
	ACM_CAP	1	2	3	4	4	5	5	4	Configuration support and acceptance procedures
	ACM_SCP			1	2	3	3	3	2	Problem tracking CM coverage
ADO Szállítás és működés	ADO_DEL		1	1	2	2	2	3	2	Detection of modification
	ADO_IGS	1	1	1	1	1	1	1	1	Installaation, generation and start-up procedures
ADV Fejlesztés	ADV_FSP	1	1	1	2	3	3	4	2	Fully defined external interfaces
	ADV_HLD		1	2	2	3	4	5	2	Security enforcing high-level design
	ADV_IMP				1	2	3	3	2	Implementation of the TSF
	ADV_INT					1	2	3		
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	1	Informal correspondence demonstration
	ADV_SPM				1	3	3	3	1	Informal TOE security policy model
AGD Használati kézikönyvek	AGD_ADM	1	1	1	1	1	1	1	1	Administrator guidance
	AGD_USR	1	1	1	1	1	1	1	1	User guidance
ALC Életciklus	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
ATE Tesztek	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	1	Testing: high-level design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Gyengeségek becslése	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	3	Analysis and testing of insecure states
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evalution
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

A vizsgált termékkel kapcsolatos hivatkozások

[2008/04]	Tanúsítási jelentés: - MultiApp ID CIE/CNS SSCD Ellenőrző mikroegység SLE66CX680PE -A13, CIE/CNS alkalmazási maszkkal Referencia: DCSSI-2008/04, 2008. március 13. SGDN/DCSSI
[2008/45]	Tanúsítási jelentés: - eTravel EAC termékek, 1.1 verzió (01 02 verzió) P5CD080 és P5CD144 alkotóelemeken Referencia: DCSSI-2008/45, 2008. december 18. SGDN/DCSSI
[Certif_IC]	Tanúsítási jelentés: - S3CC91C 16-bit RISC Microcontroller for Smart Card, 0. verzió Referencia: BSI-DSZ-CC-0451-2007 BSI
[RTE_IC]	ETR-Lite for composition: - ETR-LITE S3CC91C 2.0 verzió, 2007. augusztus 28. Tüv-IT/BSI
[ST_IC]	Ellenőrző mikroegység biztonsági célpontja - Security Target of S3CC91C 16-bit RISC Microcontroller for Smart Cards 1.0 verzió, 2007. augusztus 9. Samsung Electronics
[ST]	Platform referencia biztonsági célpontja az értékeléshez: - Adriatic Platform Security Target 1.5 verzió, referencia D10777228, 2008 Gemalto Applet referencia biztonsági célpontja az értékeléshez: - Adriatic IAS Classic Security Target, Generic Configuration 1.6 verzió, referencia D1077227_Generic, 2008 Gemalto
[RTE]	Műszaki értékelési jelentés: - Evaluation Technical Report - Project: Adriatic IAS, Referencia: ADRIATIC-IAS_ETR_v.1.0/1.0 Serma Technologies
[CONF]	A konfigurációs lista az alábbi dokumentumokból áll: - Adriatic IAS Configuration List 1.1 verzió, referencia D1109385 Gemalto
[GUIDES]	A termék vezérlési és használati kézikönyve - Platform Adminisztrator's and user's guide 1.2 verzió, referencia: D1077605 Gemalto - IAS Classic Adminisztrator's and user's guide 1.1 verzió, referencia: D1077604

	Gemalto Reference Manual: - IAS Classic Applet v3, Reference Manual referencia: DOC116499E Gemalto - MultiApp ID Combi and Derives Products, Reference Manual referencia: DOC116422A Gemalto Az S3CC91C alkotóelemmel kapcsolatos ajánlások: - Application Note DRNG Software 2.0 verzió Samsung Electronics - Application Note RSA Crypto Library with TORNADO V3.5S 1.10 verzió Samsung Electronics - Security Application Note, S3CC91C 1.2 verzió Samsung Electronics
[PP0002]	Protection Profile - Smart Card IC Platform 1.0 verzió, *BSI tanúsítvánnyal, BSI-PP-0002-2001 számmal.*
[PP0005]	Protection Profile - Secure Signature- Creation Device Type 2, 1.04 verzió, 2001. július 25. *BSI tanúsítvánnyal (Bundesamt für Sicherheit in der Informationstechnik), BSI-PP-0005-2002 számmal.*
[PP0006]	Protection Profile - Secure Signature- Creation Device Type 3, 1.05 verzió, 2001. július 25., *BSI tanúsítvánnyal, BSI-PP-0006-2002 számmal.*

A tanúsítással kapcsolatos hivatkozások

2002. április 18-i, az informatikai rendszerek és termékek által nyújtott biztonsági értékelésének vizsgálatáról és tanúsításáról szóló 2002-535. számú rendelet	
[CER/P/01]	CER/P/01 az információs technológiai rendszerek és termékek által nyújtott biztonsági szolgáltatások tanúsítási eljárása, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: 1. rész: Bevezetés és általános modell 2005. augusztus, 2.3 verzió, referencia: CCM-2005-08-001; 2. rész: Biztonsági funkciókkal kapcsolatos elvárások 2005. augusztus, 2.3 verzió, referencia: CCM-2005-08-002; 3. rész: Biztonság biztosításával kapcsolatos elvárások 2005. augusztus, 2.3 verzió, referencia: CCM-2005-08-003; A Közös Szempontrendszer 2.3 verziójának tartalma megegyezik az ISO/IEC 15408:2005 Nemzetközi Szabvány tartalmával.
[CEM]	Common Methodolody for Information Technology Security Értékelés: Értékelési módszerek 2005. augusztus, 2.3 verzió, referencia: CCM-2005-08-004 A CEM 2.3 verziójának tartalma megegyezik az ISO/IEC 18045:2005 Nemzetközi Szabvány tartalmával.
[CC IC]	Common Criteria Supporting Document- Mandatory Technical Document - The Application of CC to Integrated Circuits referencia: CCDB-2006-04-003, 2.0 verzió, felülvizsgálat 1, 2006. április
[CC AP]	Common Criteria Supporting Document- Mandatory Technical Document - Application of attack potential to smart-cards referencia: CCDB-2008-04-001, 2.5 verzió, felülvizsgálat 1, 2008. április
[COMP]	Common Criteria Supporting Document- Mandatory Technical Document - Composite product evaluation for smart cards and similar devices referencia: CCDB-2007-09-001, 1.0 verzió, felülvizsgálat 1, 2007. szeptember
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2000. május
[SOG-IS]	"Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", 2.0 verzió, 1999. április, Management Committee of Agreement Group
[REF-CRY]	Kriptográfiai mechanizmusok - A normál erősségű kriptográfiai mechanizmusok méretezésével és kiválasztásával kapcsolatos szabályok és ajánlások 1.10 verzió, 2006. december 19., referencia: 2741/SGDN/DCSSI/SDS/Crypto
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, 1.00 verzió, 2004. június 1. BSI (Bundesamt für Sicherheit in der Informationstechnik)