Tanúsítási jelentés

Hung-TJ-045-2009

Touch&Sign2048 Version 1.00

intelligens kártya
mint

biztonságos aláírás-létrehozó eszköz

/ST Incard S.r.l./

Verzió:	1.0
Fájl:	Hung-TJ-045-2009_v10.pdf
Minősítés:	Nyilvános
Oldalak:	32

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2009.02.02.	A szerkezet felállítása
v0.9	2009.02.16.	Egyeztetésre kiadott változat
v0.91	**2009.02.20.**	**Egyeztetésre kiadott 2. változat**
v1.0	2009.02.23.	Végleges verzió

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalom

1. Bevezetés

1.1. A tanúsítási jelentés tárgya

Jelen tanúsítási jelentés tárgya a Touch&Sign2048 V1.00 megnevezésű többfunkciós intelligens kártya termék, (a későbbiekben erre a termékre „**Touch&Sign2048 V1.00”-**ként hivatkozunk), s melyet minősített aláírás létrehozásához kívánnak felhasználni mint biztonságos aláírás-létrehozó eszköz (BALE).

A biztonságos aláírás-létrehozó eszközre vonatkozó követelményeket az elektronikus aláírásról szóló 2001. évi XXXV. törvény igen általánosan az alábbi módon fogalmazza meg 1. sz. mellékletében[1]:

1. A biztonságos aláírás-létrehozó eszköznek megfelelő technikai és eljárási eszközökkel biztosítaniuk kell legalább a következőket:

a) az aláírás készítéséhez használt aláírás-létrehozó adat aláírónként biztosan mindig különbözik, s titkossága kellően biztosított,

b) az aktuálisan elérhető technológiával kellő bizonyossággal garantálható, hogy az aláírás készítéséhez használt aláírás-létrehozó adat nem rekonstruálható, megvalósítható annak a jogosulatlan felhasználókkal szembeni védelme, illetve az aláírás nem hamisítható.

Az EU Irányelvek fenti követelményeinek szakmai lebontásaként egy CEN Munkacsoport egyezmény született, mely a Közös szempontrendszer (Common Criteria, ISO/IEC 15408) által definiált védelmi profilok formájában határozta meg a biztonságos aláírás-létrehozó eszközökre vonatkozó részletes funkcionális és garanciális biztonsági követelményeket.

Funkcionalitás szempontjából három különböző BALE típus definiáltak:

- 1-es típus: csak az aláírás-létrehozó / aláírás-ellenőrző adatpárok generálását támogatja, de nem állít elő elektronikus aláírást az általa előállított aláírás-létrehozó adattal,
- 2-es típus: biztosítja az elektronikus aláírás előállítását egy olyan aláírás-létrehozó adat felhasználásával, amelyet egy 1-es típusú BALE-től importál,
- 3-as típus: biztosítja mind az aláírás-létrehozó / aláírás-ellenőrző adatpárok generálását, mind az elektronikus aláírás előállítását az aláírás-létrehozó adattal.

A 3-as típusú BALE-re két Common Criteria szerinti védelmi profil is készült, a garanciális biztonság szempontjából egy szigorú és egy még szigorúbb változat:

- EAL4-es értékelés garancia szint (Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4),
- EAL4+ (emelt szintű) értékelési garancia szint (Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+).

[1] Az idézett rész teljes mértékben megfelel (lévén szó szerinti fordítás) az Európai Parlament és Tanács 1999. december 13-án kelt, az elektronikus aláírásokra vonatkozó 1999/93/EK számú Irányelvének.

A fenti védelmi profilokban megalapozott, megfogalmazott és megindokolt követelményrendszer biztosan helyes szakmai lebontása és részletezése az EU direktíva és a hazai elektronikus aláírás törvény magas szinten megfogalmazott követelményeinek.

A Touch&Sign2048 V1.00 rendelkezik a második védelmi profilnak való megfelelőséget igazoló tanúsítvánnyal.

1.2. A tanúsítási jelentés feladata

Jelen tanúsítási jelentés fő feladatai:

- a Touch&Sign2048 V1.00 vonatkozó tanúsítási eredmények bemutatása,
- a CC tanúsítvány érvényességének, illetve annak megállapítása, hogy a többi kielégítendő funkcionális és biztonsági követelmény teljesülése milyen korlátozásokat, feltételeket támaszt a Touch&Sign2048 V1.00 intelligens kártya 3-as típusú BALE-ként való felhasználására.

1.3. A tanúsítási jelentés hatóköre

Jelen tanúsítási jelentés hatóköre csak a biztonságos aláírás-létrehozó eszközként való felhasználhatóságra és ennek feltétel-rendszerének meghatározására szorítkozik.

Nem terjed ki a Trust&Sign2048 v1.0 egyéb tulajdonságaira (pl. titkosításra való felhasználhatóságára).

1.4. A tanúsítási jelentés szerkezete

A tanúsítási jelentés további szerkezete a következő:

- A 3-as típusú BALE-kre vonatkozó CC szerinti SSCD védelmi profil fontosabb elemei /biztonsági környezet (kivédendő veszélyek és érvényre juttatandó biztonsági szabályok), biztonsági célok, funkcionális és garanciális követelmények/ (2. fejezet).
- A Trust&Sign2048 v1.0 intelligens kártya néhány különleges tulajdonsága (3. fejezet).
- A Trust&Sign2048 v1.0 operációs rendszerére vonatkozó CC tanúsítvány eredményei (4. fejezet).
- A minősített aláírás-létrehozáshoz való alkalmasság megállapítása, valamint az alkalmazás feltételeinek és korlátainak a meghatározása (5. fejezet).
- A jelen tanúsítási jelentéshez figyelembe vett dokumentumok jegyzéke (6. fejezet).
- Az alkalmazott rövidítések jegyzéke (7. fejezet).

2. Egy 3-as típusú BALE-re vonatkozó CC követelmények az SSCD védelmi profil szerint

Az alábbiakban áttekintjük a vonatkozó SSCD védelmi profil fontosabb részeit (a környezetre vonatkozó állításokat, biztonsági célokat, funkcionális és garanciális követelményeket).

2.1. Egy 3-as típusú BALE biztonsági környezete

Védendő értékek:

SCD: aláírás létrehozó adat, azaz a magánkulcs, amelyre az elektronikus aláírási művelethez van szükség. A bizalmasságát kell megőrizni.

SVD: aláírás ellenőrző adat, az SCD-hez kapcsolódó nyilvános kulcs, az elektronikus aláírás ellenőrzéséhez szükséges. Exportálása során a sértetlenségét kell fenntartani.

DTBS és **DTBS-reprezentáció**: az aláírni kívánt adathalmaz, vagy annak valamilyen reprezentációja. Sértetlenségét kell megőrizni.

VAD: Ellenőrző hitelesítési adat: PIN kód vagy biometrikus adat, melyet a végfelhasználó ad meg az aláírási művelet végrehajtása előtt. A bizalmasságát és hitelességét kell fenntartani, ahogyan azt az alkalmazott hitelesítési módszer megkívánja.

RAD: Referencia hitelesítési adat: Referencia PIN kód vagy biometrikus hitelesítési referencia, a végfelhasználó azonosításához és hitelesítéséhez. A sértetlenségét és a bizalmasságát kell megőrizni.

Az SSCD az SCD használatával végrehajtott **aláírás létrehozó funkció**ja: A funkció minőségének fenntartása, hogy hozzájáruljon az elektronikus aláírások jogi érvényességéhez.

Elektronikus aláírás: hamisíthatatlannak kell lenniük.

Szubjektumok

S.User (Felhasználó)
: A TOE végfelhasználója, lehet S.Admin vagy S.Signatory.

S.Admin (Adminisztrátor)
: A TOE inicializálásáért, perszonalizálásáért vagy egyéb TOE adminisztratív funkció végrehajtásáért felelős felhasználó.

S.Signatory (Aláíró)
: A TOE-t működtető felhasználó, aki saját, természetes vagy jogi személy/egyed nevében használja az eszközt.

S.OFFCARD
: Támadó: a TOE-n kívüli, saját céljai elérése érdekében működő ember vagy folyamat. Az S.OFFCARD támadó elsődleges célja az alkalmazás érzékeny információihoz való hozzáférés. A támadóról magas támadási képességet tételezünk fel, és azt, hogy nem ismer egyetlen titkot sem.

2.1.1. Feltételezések

A.CGA Megbízható tanúsítvány-generálási alkalmazás

A CGA az aláíró nevének és az SVD-nek a hitelességét a CSP fokozott biztonságú aláírásával minősített tanúsítványban védi.

A.SCA Megbízható aláírás létrehozó alkalmazás

Az aláíró csak megbízható SCA-t használ. Az SCA elkészíti és a TOE által aláírásra értelmezhető formában elküldi az aláíró által aláírni kívánt adat DTBS-reprezentációját.

2.1.2. A biztonságra irányuló veszélyek

T.Hack_Phys Fizikai támadások a TOE interfészein keresztül

Egy támadó kapcsolatba kerül a TOE interfészekkel, hogy a sebezhetőségeket kihasználja, ami tetszőleges biztonsági kompromittálódáshoz vezet. Ez a veszély minden értéket fenyeget.

T.SCD_Divulg Aláírás létrehozó adat tárolása, másolása és felfedése

Egy támadó a TOE-n kívül tárolhatja, vagy oda másolhatja az SCD-t. Egy támadó felfedheti az SCD-t a TOE-n belüli generálás, tárolás és aláírás létrehozásra történő használat során.

T.SCD_Derive Az aláírás létrehozó adat származtatása

Egy támadó az SCD-re következtet nyilvánosan ismert adatokból, például az SCD-hez tartozó SVD-ből, vagy az SCD-vel létrehozzon aláírásból, vagy egyéb, a TOE-n kívülre továbbított adatból. Ez a veszély az SCD bizalmasságát fenyegeti.

T.Sig_Forgery Az elektronikus aláírás hamisítása

Egy támadó meghamisítja az aláírt adatobjektumot, esetleg annak TOE által létrehozott elektronikus aláírásával együtt, úgy, hogy az aláírt adatobjektum sértetlenségének elvesztését az aláíró vagy egy harmadik fél nem képes észlelni. A TOE által generált aláírás ki van téve olyan szándékos támadásoknak, melyeket magas támadási képességekkel rendelkező szakértők hajtanak végre, és akik magas szintű tudással rendelkeznek a TOE által alkalmazott biztonsági elvekről és módszerekről.

T.Sig_Repud Az aláírások letagadása

Amennyiben egy támadó sikeresen veszélyeztetni tudja az értékek bármelyikét, akkor sérül az elektronikus aláírás letagadhatatlansága. Ennek következménye, hogy az aláíró letagadhatja, hogy az SCD-vel aláírta az adatot az ellenőrzése alatt álló TOE-

vel, még akkor is, ha az aláírás sikeresen ellenőrizhető az aláíró érvényes tanúsítványában szereplő SVD-jével.

T.SVD_Forgery Aláírás ellenőrző adat hamisítása

Egy támadó meghamisítja a TOE által a CGA felé adott SVD-t. Ez az aláíró tanúsítványában szereplő SVD sértetlenségének elvesztését jelenti.

T.DTBS_Forgery A DTBS-reprezentáció hamisítása

Egy támadó módosítja a DTBS-reprezentációt, amit az SCA küldött. Ez által a TOE által aláírásra használt DTBS-reprezentáció nem egyezik meg azzal a DTBS-sel, amit az aláíró aláírni akart.

T.SigF_Misuse Visszaélés a TOE aláírás létrehozó funkciójával

Egy támadó visszaél a TOE aláírás létrehozó funkciójával, hogy olyan adatra hozzon létre aláírt adatobjektumot (SDO), amelyet az aláíró nem akart aláírni. A TOE ki van téve olyan szándékos támadásoknak, melyeket magas támadási képességekkel rendelkező szakértők hajtanak végre, és akik magas szintű tudással rendelkeznek a TOE által alkalmazott biztonsági elvekről és módszerekről.

2.1.3. Szervezeti biztonsági szabályok

P.CSP_QCert Minősített tanúsítvány

A CSP megbízható CGA-t használ az SSCD által generált SVD-hez tartozó minősített tanúsítvány létrehozásához. A minősített tanúsítvány tartalmazza a Direktíva I. függelékében megadott elemeket, azaz többek között az aláíró nevét és a TOE által az aláíró kizárólagos befolyása alatt álló TOE-ben megvalósuló SCD-hez tartozó SVD-t.

P.QSign Minősített elektronikus aláírások

Az aláíró aláírás létrehozó rendszert használ adatok minősített elektronikus aláírással való ellátására. A DTBS-t az aláíró számára az SCA szolgáltatja. A minősített elektronikus aláírás minősített tanúsítványon alapul (Direktíva I. függeléke) és SSCD-vel hozták létre.

P.Sigy_SSCD A TOE mint biztonságos aláírás létrehozó eszköz

A TOE az aláírás létrehozására használt aláírás létrehozó adatot az aláíró kizárólagos ellenőrzése alatt tartja. Az aláírás létrehozására használt SCD (aláírás létrehozó adat) gyakorlatilag csak egyszer fordul elő, azaz egyedinek tekinthető.

2.2. Biztonsági célok

Ez a fejezet a TOE-re és a környezetére vonatkozó biztonsági célokat azonosítja és fogalmazza meg. A biztonsági célok a kinyilvánított szándékot fejezik ki az azonosított veszélyek kivédésre, megfogalmazzák a veszélyek kivédését és megfogalmazzák az azonosított szervezeti biztonsági szabályok és feltételezések betartását.

2.2.1. A TOE által teljesítendő biztonsági célok

OT.EMSEC_Design Fizikai kisugárzás biztonságának megvalósítása

A TOE-t úgy kell tervezni és gyártani, hogy az értelmezhető kisugárzás kibocsátása adott határokon belül maradjon.

OT.Lifecycle_Security Biztonság a teljes életciklusban

A TOE-nak észlelnie kell a hibákat az inicializálás, perszonalizálás és az aktív/rendeltetésszerű használat során. A TOE-nak biztonságos megsemmisítési technikákról kell gondoskodnia az aláírás létrehozó adat (SCD) tekintetében annak újragenerálása esetén.

OT.SCD_Secrecy Az aláírás létrehozó adat bizalmassága

Az aláírás generálására használt aláírás létrehozó adat (SCD) bizalmasságát megfelelő mértékben biztosítani kell a magas támadási képességgel rendelkező támadók által végrehajtott támadások ellen.

OT.SCD_SVD_Corresp Az SVD és SCD összetartozása

A TOE-nak biztosítania kell az SVD és SCD összetartozását. A TOE-nak ellenőriznie kell igény esetén a TOE-ban tárolt SCD és az SVD összetartozását, ha azt a TOE-nak továbbították.

OT.SVD_Auth_TOE A TOE biztosítja az SVD hitelességét

A TOE gondoskodik olyan lehetőségről, mely lehetővé teszi a CGA számára, hogy ellenőrizze az SVD hitelességét, amelyet a TOE exportált.

OT.Tamper_ID Meghamisítás észlelése

A TOE biztosítson olyan rendszertulajdonságokat, amelyek észlelik egy rendszerösszetevő fizikai meghamisítását, és használja ezeket a tulajdonságokat a biztonsági események bekövetkezésének csökkentésére.

OT.Tamper_Resistance Ellenállás a meghamisításnak

A TOE előzze meg vagy álljon ellen bizonyos rendszereszközök és összetevők fizikai meghamisításának.

OT.Init SCD/SVD generálás

A TOE nyújtson biztonsági tulajdonságokat annak biztosítására, hogy az SCD és SVD generálást csak az arra jogosult felhasználók kezdeményezhessék.

OT.SCD_Unique Az aláírás létrehozó adat egyedisége

A TOE-nak biztosítania kell az SCD/SVD kulcspár kriptográfiai minőségét a minősített elektronikus aláíráshoz. Az aláírás generálására használt SCD (aláírás létrehozó adat) gyakorlatilag csak egyszer fordul elő, és nem állítható elő az SVD-ből. A "gyakorlatilag csak egyszer fordul elő" azt jelenti, hogy az egyforma SCD-k előfordulásának esélye elhanyagolhatóan alacsony.

OT.DTBS_Integrity_TOE A DTBS-reprezentáció sértetlenségének ellenőrzése

A TOE-nak ellenőriznie kell, hogy az SCA-tól kapott DTBS-reprezentáció nem módosult-e az SCA és a TOE közötti átvitel során. A TOE-nak biztosítania kell, hogy a DTBS-reprezentációt ő maga sem módosítja. Ez nem mond ellent annak az aláírás létrehozó folyamatnak, amikor a DTBS-hasht a TOE is elkészítheti.

OT.Sigy_SigF Aláírás generáló funkció csak a jogosult aláíró számára

A TOE-nak gondoskodnia kell arról, hogy az aláírás generálási funkció csak a jogosult aláíró számára álljon rendelkezésre, és meg kell védenie az SCD-t mások használatával szemben A TOE-nak ellen kell állnia a magas támadási képességgel végrehajtott támadásoknak.

OT.Sig_Secure Az elektronikus aláírás kriptográfiai biztonsága

A TOE olyan elektronikus aláírásokat generáljon robusztus rejtjelezési technikák alkalmazása által, amelyeket nem lehet hamisítani az SCD ismerete nélkül. Az SCD nem lehet előállítható az elektronikus aláírásából. Az elektronikus aláírásoknak ellen kell állniuk ezen támadásoknak, még a magas támadási képességgel végrehajtott támadásoknak is.

2.2.2. A környezetre vonatkozó biztonsági célok

OE.CGA_QCert Minősített tanúsítványok generálása

A CGA minősített tanúsítványokat generál, amelyek tartalmazzák többek között

- a) a TOE-t használó aláíró nevét,
- b) az aláíró kizárólagos befolyása alatt álló TOE által tartalmazott SCD-hez tartozó SVD-t,
- c) a CSP fokozott biztonságú aláírását.

OE.SVD_Auth_CGA A CGA ellenőrzi az SVD hitelességét

A CGA ellenőrzi, hogy az SSCD-e a kapott SVD küldője, valamint ellenőrzi a kapott SVD sértetlenségét. A CGA ellenőrzi az aláíró SSCD-jében lévő SCD és a minősített tanúsítványban szereplő SVD közötti összetartozást.

OE.HI_VAD A VAD védelme

Ha külső eszköz gondoskodik a humán interfészről a felhasználói hitelesítés során, akkor ennek az eszköznek biztosítania kell a VAD bizalmasságát és sértetlenségét, ahogyan azt az alkalmazott hitelesítési módszer megkívánja.

OE.SCA_Data_Intend Az aláírni kívánt adat

Az SCA

- elkészíti a DTBS-ként bemutatott adat DTBS-reprezentációját, amit az aláíró alá akar írni, a TOE által aláírásra alkalmas formában;
- továbbítja a DTBS-reprezentációt a TOE felé, és lehetővé teszi, hogy a TOE ellenőrizni tudja a DTBS-reprezentáció sértetlenségét;
- hozzácsatolja a TOE által előállított aláírást az adathoz vagy különállóan szolgáltatja azt.

2.3. Egy 3-as típusú BALE funkcionális biztonsági követelményei

Az alábbiakban felsorolt funkcionális biztonsági követelmények kielégítése esetén a BALE:

- kivédi a biztonságra irányuló veszélyeket (2.1.2),
- érvényre juttatja a biztonsági szabályokat (2.1.3), egyúttal
- megvalósítja a biztonsági célokat (2.2).

Az alábbi táblázat összefoglalja a 3-as típusú BALE-kra vonatkozó SSCD védelmi profil funkcionális biztonsági követelményeit.

Funkcióosztályok	Funkció családok és összetevők
Kriptográfiai támogatás	FCS_CKM.1 Kriptográfiai kulcs generálás
	FCS_CKM.4 Kriptográfiai kulcs megsemmisítés
	FCS_COP.1 Kriptográfiai eljárás
A felhasználói adatok védelme	FDP_ACC.1 Részleges hozzáférés ellenőrzés
	FDP_ACF.1 Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés
	FDP_ETC.1 Felhasználói adatok exportálása biztonsági tulajdonságok nélkül
	FDP_ITC.1 Felhasználói adatok importálása biztonsági tulajdonságok nélkül
	FDP_RIP.1 Részleges maradvány információ védelem
	FDP_SDI.2 A tárolt adatok sértetlenségének figyelése és beavatkozás
	FDP_UIT.1 Az adatcsere sértetlensége
Azonosítás és hitelesítés	FIA_AFL.1 A hitelesítési hiba kezelése
	FIA_ATD.1 A felhasználói jellemzők meghatározása
	FIA_UID.1 Az azonosítás időzítése
	FIA_UAU.1 A hitelesítés időzítése
Biztonság kezelés	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
	FMT_MSA.1 A biztonsági jellemzők kezelése
	FMT_MSA.2 Biztonságos biztonsági jellemzők
	FMT_MSA.3 Statikus jellemző inicializálás
	FMT_MTD.1 A biztonsági funkciók adatainak kezelése
	FMT_SMR.1 Biztonsági szerepkörök
Magántitok	---
A biztonsági funkciók megbízható védelme	FPT_AMT.1 Az absztrakt gép tesztelése
	FPT_EMSEC.1 A BALE kisugárzása
	FPT_FLS.1 A biztonságos állapot megőrzése hiba esetén
	FPT_PHP.1 A fizikai támadások passzív észlelése
	FPT_PHP.3. A fizikai támadásokkal szembeni ellenálló képesség
	FPT_TST.1 A biztonsági funkciók tesztelése
Megbízható útvonal /csatorna	FTP_ITC.1 Megbízható csatorna
	FTP_TRP.1 Megbízható útvonal

2.4. Egy 3-as típusú BALE garanciális biztonsági követelményei

Egy 3-as típusú BALE-re vonatkozó, a fejlesztőktől független ellenőrző vizsgálat garancia szintje **EAL 4+** /módszeresen tervezett, vizsgált és átnézett rendszer/.

Az alábbi táblázat összefoglalja az EAL4+ szintű értékelés garanciaosztályait és garancia komponenseit.

Garanciaosztályok	Garancia családok és komponensek az EAL 4 /**EAL4+**/ szintű értékelésénél
A konfiguráció menedzselése	ACM_AUT.1 Részleges konfiguráció menedzselés automatizálás
	ACM_CAP.4 A generálás támogatása és elfogadási eljárások
	ACM_SCP.2 A biztonsági hibákat követő konfiguráció menedzselés
Kiszállítás és üzemeltetés	ADO_DEL.2 A módosítás kimutatása
	ADO_IGS.1 Hardver telepítés, szoftver telepítés, a beindítás eljárásai
Fejlesztés	ADV_FSP.2 Teljesen meghatározott külső interfészek
	ADV_HLD.2 Biztonságot érvényre juttató magas szintű tervezés
	ADV_IMP.1 A biztonsági funkciók részleges kivitelezési dokumentálása
	ADV_LLD.1 Leíró alacsony szintű terv
	ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése
	ADV_SPM.1 Informális biztonsági politika modell
Útmutató dokumentumok	AGD_ADM.1 Az adminisztrátori útmutató
	AGD_USR.1 A felhasználói útmutató
Az életciklus támogatása	ALC_DVS.1 A biztonsági intézkedések azonosítása
	ALC_LCD.1 A fejlesztő által meghatározott életciklus modell
	ALC_TAT.1 Jól meghatározott fejlesztői eszközök
Tesztelés	ATE_COV.2 A teszt lefedettség elemzése
	ATE_DPT.1 A magas szintű terv tesztelése
	ATE_FUN.1 Funkcionális tesztelés
	ATE_IND.2 Független tesztelés - mintán
A sebezhetőség felmérése	**AVA_MSU.3** A nem biztonságos állapotok elemzése és tesztelése
	AVA_SOF.1 Az értékelés tárgya biztonsági funkcióinak erősségértékelése
	AVA_VLA.4 Magas szinten ellenálló

3. A Touch&Sign2048 V1.00 főbb tulajdonságai

A tanúsítási jelentés tárgya a Touch&Sign2048 V1.00 megnevezésű többfunkciós intelligens kártya termék, amelyet a minősített elektronikus aláírások létrehozásában érintett eszközök által igényelt összes képesség biztosítására terveztek.

A Touch&Sign2048 V1.00 funkcionalitása az alábbiakat fedi le:

- Kriptográfiai kulcsok generálása és biztonságos menedzsmentje,
- Biztonságos aláírás létrehozás az aláírandó adatok biztonságos kezelésével,
- Megbízható felhasználók és alkalmazások azonosítása és hitelesítése,
- Adattárolás és védelem a módosítások és/vagy felfedés ellen,
- A TOE és egy megbízható alkalmazás között továbbított érzékeny adatok biztonságos cseréje,
- A TOE és egy megbízható humán interfész eszköz között továbbított érzékeny adatok biztonságos cseréje.

A Touch&Sign2048 V1.00 képes a saját aláíró kulcspárjának létrehozására. Egy jogosult adminisztrátor (Administrator) a CGA használatával kezdeményezi az SCD/SVD generálását, és kérést küld az SSCD felé az SVD exportálásához, a kulcshoz tartozó tanúsítvány generálása céljából. A TOE megőrzi az SVD-t, és mielőtt exportálja a CGA felé a tanúsítvány létrehozás érdekében, megbízható csatornát hoz létre a sértetlenség fenntartása céljából.

Az aláírónak hitelesíteni kell magát az aláírás létrehozás előtt. A hitelesítéshez elküldi a hitelesítő adatát (egy PIN-t) a TOE-nak, az alkalmazott interfész eszköz, azaz egy intelligens kártya olvasó és a TOE között létesülő megbízható útvonalon keresztül. Az intelligens kártya olvasót használja az aláíró és az adminisztrátor is a TOE által tárolt referencia hitelesítő adat (RAD) módosítására, ami a felhasználói PIN ellenőrzésének TOE oldali alapja, továbbá az adminisztrátor használja az aláíró referencia hitelesítő adata zárolásának feloldására, amennyiben erre szükség van.

Az aláírandó adatot (DTBS) vagy annak reprezentációját (DTBSR) az SCA – kizárólag megbízható csatornán keresztül– továbbítja a TOE felé annak érdekében, hogy ezen adatok sértetlensége fennmaradjon. Ugyanez a megbízható csatorna szolgál az aláírt adatobjektum (SDO) visszaadására a TOE-tól az SCA felé (lásd SSCD védelmi profil [11] 2.1 fejezet). A TOE, amikor az SCA kéri, képes generálni egy aláírandó adat reprezentációt (DTBSR) egy hash függvény segítségével, a [15]-ban foglaltaknak megfelelően.

4. A Touch&Sign2048 V1.00 CC tanúsításának eredményei

4.1. Összefoglaló

A tanúsítás alapja a biztonsági előirányzat, amely a tanúsított 3-as típusú SSCD védelmi profilon (1.05 verzió, BSI-PP-0006-2002 [11]) alapul.

A TOE garanciális biztonsági követelményei teljes egészében a Közös szempontok 3. részében szereplő garanciális követelményeken alapulnak (lásd [03], 3. részt a részletekért). A TOE teljesíti az EAL4 szint garanciális követelményeit, az AVA_MSU.3 és AVA_VLA.4 összetevőkkel szigorítva.

A TOE szempontjából lényeges funkcionális biztonsági követelményeket (SFR) a biztonsági előirányzat [08] és [09] 12.1 fejezete írja le. Ezek a követelmények a Közös szempontok (Common Criteria) 2. részéből származnak és vannak köztük újonnan definiáltak is, ezért a TOE kiterjesztett 2. rész megfelelőséget állít.

A TOE IT környezete szempontjából fontos funkcionális biztonsági követelményeket (SFR) a biztonsági előirányzat [08] és [09] 12.3 fejezete írja le.

A TOE funkcionális biztonsági követelményeit az alábbi TOE biztonsági funkciók valósítják meg:

TOE biztonsági funkciói	**Tárgyalt kérdés**
SF.AUTH	Hitelesítési funkciók
SF.RAD	RAD menedzsment
SF.AC	Hozzáférés ellenőrzés
SF.KEY_GEN	Kulcsgenerálás
SF.HASH	Hash számítás
SF.MAC	MAC számítás
SF.SIGN	Kriptográfiai funkciók
SF.SM	Biztonságos üzenetváltás
SF.OBS_A	Megfigyelhetetlenség
SF.INT_A	A TOE logikai sértetlensége
SF.DATA_ERASE	Adatok biztonságos megsemmisítése
SF.TRANSACTION	Konzisztens tranzakciók fenntartása
SF.TEST	Önteszt és naplózás
SF.EXCEPTION	Hibakezelés és kivételkezelés
SF.LIFE_CYCLE	TOE életciklus állapot menedzsment

TOE biztonsági funkciói	Tárgyalt kérdés
SF.HARDWARE	TRNG és fizikai védelem, TOE kriptográfiai támogatás

További részleteket a biztonsági előirányzat [08] és [09] 13.fejezete tartalmaz.

Az állított TOE funkcióerősség „magas” (magas SOF) specifikus funkciókra, ahogyan azt a biztonsági előirányzat [08] és [09] 15.4 fejezete megerősíti. A funkcióerősségi besorolás nem vonatkozik a titkosításra és dekódolásra alkalmas kriptográfiai algoritmusokra.

A TOE által védendő értékeket a biztonsági előirányzat [08] illetve [09] 10.1 fejezete tartalmazza. Ezen értékekből kiindulva a biztonsági előirányzat [08] illetve [09] 10. fejezete feltételezések, veszélyek és szabályzatok által adja meg a biztonsági környezetet.

Ez a tanúsítás a TOE következő konfigurációját fedi le: Touch&Sign2048 V1.00. Erről további részleteket jelen jelentés 8. fejezete tartalmaz.

A tanúsítási eredmények csak a terméknek a tanúsítványban szereplő verziójára vonatkoznak, azzal a feltétellel, hogy jelen tanúsítási jelentésben szereplő minden megszorítás fennáll.

4.2. A TOE azonosítása

Az értékelés tárgyának (TOE) megnevezése: Touch&Sign2048 V1.00 Az alábbi táblázat a TOE értékelésre átadandó elemeit írja le:

Sorszám	Típus	Azonosító	Kibocsátás	Átadás módja
1	HW/SW	A Touch&Sign2048 V1.00 SSCD alkalmazás A Touch&Sign2048 V1.00 eszközkezelők. Az integrált áramkör és annak könyvtárai: ST19WR66I.	N/A	Fizikai átadás
2	DOC	A Touch&Sign2048 V1.00 felhasználói és adminisztrátori útmutató. [12]	A-2, 2007.12.07.	Dokumentum papír vagy elektronikus formában
3	OTHER	A perszonalizációhoz szükséges kulcsok.	N/A	Elektronikus formában megbízható csatornán

A hardver fejlesztőtől való elszállításkor a TOE az inicializálási állapotban van. Az előperszonalizációs állapot a TOE patchingjéből és konfigurálásából áll. A Perso-A

állapot a kártyagyártó számára rendelkezésre álló belső állapot. Az alkalmazás által igényelt összes fájl adminisztrátor által történő létrehozása a Perso-B állapotban történik meg. A TOE a Perso-A állapot végén készül el. A kártyatulajdonoshoz történő szállítás a perszonalizációt végző szervezet felelőssége. A TOE életciklus szakaszainak részletes leírása a biztonsági előirányzat [08] illetve [09] 9.3 fejezetében olvasható, és kifejtése az Útmutatóban [14] található.

A TOE-t az ST Incard S.r.l. gyártási helyszínen inicializálják és elő-perszonalizálják a perszonalizációs központba szállítás előtt. A perszonalizációs központ lehet az ST Incard S.r.l. helyszínen belül, vagy lehet azon kívüli hely.

A belső perszonalizáció esetén a TOE-kat belső szállítási rend szerint továbbítják. A szervezet belső biztonságos területei és a TOE-ban tárolt hitelesítő kulcs nyújtja a biztonságot és garantálja a TOE sértetlenségét.

A külső perszonalizáció esetén a TOE-kat becsomagolják, lepecsételik és egy megbízható futár szállítja a célba. A szállítási dokumentáció, kézikönyv és hitelesítési kulcsok elektronikus formában kerülnek továbbításra megbízható csatorna alkalmazásával (például PGP-vel aláírt és kódolt e-mailben).

4.3. Biztonsági szabályzat

A TOE egy IC, az IC dedikált szoftver és intelligens kártya beépített szoftver összetételéből áll, és biztonságos aláíró eszközként (angol röv: SSCD, magyar röv: BALE) való használatra tervezték, az aláírás létrehozó adat (SCD) generálása és minősített elektronikus aláírások létrehozása céljából.

A biztonsági szabályzatot funkcionális követelmények adott készlete fejezi ki, és a TOE valósítja meg. Az alábbiakat fedi le:

- A TOE interfészeken történő fizikai támadások,
- Az aláírás létrehozó adat tárolása, másolása, felfedése és származtatása egy támadó által,
- Az elektronikus aláírás, az aláírás ellenőrző adat vagy a DTBS reprezentáció hamisítása,
- Aláírások letagadása,
- A TOE aláírás létrehozó funkciójának helytelen használata.

4.4. Feltételezések és a hatókörök kijelölése

A biztonsági előirányzatban megadott feltételezésekkel és a veszélyekkel, valamint a szervezeti biztonsági szabályzatok néhány szempontjával nem foglalkozik maga a TOE. Ezek az aspektusok a TOE környezete által teljesítendő speciális biztonsági célokhoz vezetnek, az alábbi tárgykörökben:

- A CGA megvédi az aláíró nevének és az SVD-nek a hitelességét a minősített tanúsítványban a CSP fokozott biztonságú aláírása által (A.CGA).
- Az aláíró csak megbízható SCA-t használ. Az SCA generálja és továbbítja az aláíró által aláírni kívánt adat DTBS-reprezentációját a TOE által aláírásra alkalmas formátumban (A.SCA).
- A TOE perszonalizációja olyan fizikai és eljárásrendi intézkedések betartásával történik, amelyek biztosítják a TOE perszonalizációs adatok sértetlenségét, bizalmasságát és rendelkezésre állását. A biztonságos

üzenetváltás megteremtéséhez szükséges megbízható csatornák és útvonal kialakítás szimmetrikus kulcsait biztonságos módon importálják és tárolják az SCA és CGA alkalmazások (A.PERSONALIZATION).
- A TOE-t az Adminisztrátori útmutatóban leírtak szerint perszonalizálják és adminisztrálják, amit hozzáértő egyén végez, aki a TOE értékeinek a biztonságáért felelős és megbízható a tekintetben, hogy a jogosultságaival nem él vissza. A TOE adminisztrátor követi a TOE Adminisztrátori útmutatóban foglaltakat a TOE biztonságos megsemmisítése tekintetében, miután a TOE az SC használat vége állapotba került (A.MANAGE).
- A TOE által igényelt pozitív azonosításhoz és hitelesítéshez szükséges információk a TOE felhasználókhoz biztonságos módon kerülnek (A.VAD).

Fentieken túl, a biztonsági előirányzat [08] illetve [09] 10.5 fejezete három szervezeti biztonsági szabályra hivatkozik a védelmi profilból [11].

Ezek meghatározzák, hogy:

- a CSP csak megbízható CGA-t használ az SSCD által generált SVD számára készítendő minősített tanúsítvány generálásához (P.CSP_Qcert),
- az aláíró olyan aláírás létrehozó rendszert használ az adatok minősített elektronikus aláírással való ellátására, amely SSCD-vel előállított minősített tanúsítványon alapul (P.Qsign), valamint
- a TOE az aláírás létrehozásához használt SCD-t az aláíró kizárólagos felügyelete alatt tartja (P.Sigy_SSCD).

4.5. Az architektúrára vonatkozó információk

A TOE Touch&Sign2048 V1.00 olyan többfunkciós intelligens kártya termék, amely 3-as típusú biztonságos aláírás létrehozó eszközt (SSCD) valósít meg egy intelligens kártya integrált áramkörén a vonatkozó védelmi profilnak [11] megfelelően és az alábbiakból áll:

- A Touch&Sign2048 V1.00 SSCD alkalmazás
- A Touch&Sign2048 V1.00 eszközmeghajtók
- Az integrált áramkör és annak könyvtárai ST19WR66I
- Felhasználói és adminisztrátori útmutatók

A Touch&Sign2048 V1.00 terméket egy ST Microelectronics mikrokontrollerre fejlesztették: ST19WR66I ICC, hardver platform 224Kb ROM, 6Kb RAM, 66Kb EEPROM lehetőséggel és kriptográfiai támogatással, és kifejezetten nagy teljesítményű nyilvános és titkos kulcsú algoritmusokon (azaz RSA, DES, TripleDES, AES-128) alapuló biztonságos alkalmazásokra tervezték. A chip tartalmaz egy Moduláris aritmetikai processzort (MAP), amely egy 1088-bites processzor architektúrára épül, valamint egy DES-gyorsítót; mindkettőt a kriptográfiai számítások gyorsítására tervezték.

A hardver tartalmaz továbbá egy valódi véletlen szám generátort (TRNG), amely megfelel mind a FIPS-140-2 [19], mind pedig az AIS 31 [06] P2 osztályának.

A hardver platformot a Francia Séma szerint tanúsították (lásd [18], ST19WR66I Tanúsítási jelentés), és megfelel a PP9806 Intelligens kártya integrált áramkör védelmi profilnak [16].

A TOE hardverből és beágyazott szoftverből áll, melyek több alrendszerben valósulnak meg. Minden bejövő APDU parancsot az „APDU dispatcher” alrendszer kezdeti ellenőrzés alá vesz, majd továbbad a megkívánt funkcionalitásért felelős alrendszer felé, melyek az alábbiak lehetnek:

- Azonosítás és hitelesítés,
- Kulcsgenerálás,
- Aláírás,
- Belső alkalmazás

Ezek az alrendszerek a „Data Protection” alrendszernek alárendelt „File System” alrendszertől kapják a szükséges adatokat, kölcsönhatásban vannak a „Hardware Abstraction Layer” alrendszerrel, amely az IC funkcióit hívja. Minden egyes interfész belépési pontjait a TOE beágyazott szoftver funkciók függvénynevei jelölik (APDU parancsok, ha az interfész kívülről látható), vagy pedig az IC dokumentációra való hivatkozások.

Az IC az „Error Handling” alrendszernek jelzi a hibákat egy biztonságos TOE állapot fenntartása érdekében.

4.6. Dokumentáció

Az értékelt dokumentáció ([14] Touch&Sign2048 V1.00 – User and Administrator Guidance, Version A-2, Date: 2007-12-07, ST Incard) a termékkel együtt kerül a felhasználóhoz. Tartalmazza a TOE biztonságos használatára vonatkozó szükséges információkat a biztonsági előirányzatban foglaltakkal összhangban.

A TOE biztonságos használatára vonatkozó egyéb kötelezettségek és megjegyzések jelen jelentés 5.2. fejezetében olvashatóak.

4.7. IT termék tesztelés

Az értékelt TOE a Touch&Sign2048 V1.00, ami az alábbiakból áll:

- A Touch&Sign2048 V1.00 SSCD alkalmazás
- Touch&Sign2048 V1.00 eszköz meghajtók
- Integrált áramkör és annak könyvtárai ST19WR66I az alábbi azonosítási adatokkal:
  - 0x496E5472: MASK ID - (ASCII code for “InTr”)
  - 0x00010002: ROM Code Version - (ver.01.02)
  - 0x0180: EEPROM package CNS – (Version 1.80)

A teszteket az összetett intelligens kártya termékkel végezték el, amely a 3-as típusú SSCD alkalmazást megvalósító ST Incard S.r.l. által fejlesztett Touch&Sign2048 V1.00 beágyazott szoftverből, az STMicroelectronics ST19WR66I integrált áramkörén lévő eszközmeghajtókból és annak könyvtáraiból áll.

A fejlesztő tesztelte a TOE TSF-jeit, 76 tesztelési stratégia alkalmazásával, amelyeket 681 egyedi tesztesetre bontottak le. A TSF minden tesztelési stratégiája megfelelt az egyedi teszt forgatókönyvek összes tesztjének, így minden TSF-et sikeresen teszteltek a TOE funkcionális specifikációja és magas szintű terve szerint. A fejlesztői teszteredmények megmutatják, hogy a TSF a specifikáltaknak megfelelően működik. A fejlesztői tesztek bizonyítják, hogy a TOE az elvártnak megfelelően működik.

Az értékelő letesztelte mind a 16 TSF-et. Az értékelők megismételték a fejlesztői teszteket és saját teszteket is végrehajtottak mind a 16 TSF-re. Az értékelői TSF részhalmaz tesztelés során a TOE a specifikáltak szerint működött. Az értékelők ellenőrizték a fejlesztői teszteredményeket a fejlesztői tesztelési dokumentáció tesztjeiből származó minta végrehajtásával.

Az értékelők áthatolás tesztelést végeztek a fejlesztői és az értékelői sebezhetőségi elemzésen alapulva. Az értékelő behatolás tesztelése során a TOE a specifikáltaknak megfelelően működött. A TOE tervezett használati környezetében a termék nem mutatott kihasználható sebezhetőséget, amit magas támadási képességgel rendelkező támadók kihasználhatnának, amennyiben minden szükséges intézkedést figyelembe vesznek.

4.8. Az értékelt konfiguráció

A TOE mint 3-as típusú biztonságos aláírás létrehozó eszköz (BALE) kizárólag egy rögzített konfigurációt jelent, melyet a felhasználó nem változtathat meg.

A TOE-hoz egyedi címke kapcsolódik. A címke a TOE OTP (egyszer programozható /one time programmable/) memóriájában tárolódik, és a GET DATA és GET DATA TRACEABILITY parancsokkal olvasható.

Jelen tanúsítás a TOE alábbi konfigurációjára vonatkozik, az alábbi azonosítási adatokkal:

- 0x496E5472: MASK ID - (ASCII code for “InTr”)
- 0x00010002: ROM Code Version - (ver.01.02)
- 0x0180: EEPROM package CNS – (Version 1.80)

A hardver fejlesztőtől való elszállításkor a TOE az inicializálási állapotban van. Az előperszonalizációs állapot a TOE patchingjából és konfigurációjából áll. A Perso-A állapot a kártyagyártó belső használatára tervezett állapot. Az alkalmazás által igényelt összes fájl adminisztrátor által történő létrehozása a Perso-B állapotban történik meg. A TOE a Perso-A állapot végén készül el. A kártyatulajdonoshoz való szállítás a perszonalizációt végző szervezet hatáskörébe tartozik. A TOE-t az ST Incard S.r.l. gyártási helyszínen inicializálják és előperszonalizálják, a perszonalizációs központba szállítás előtt.

4.9. Az értékelés eredményei

4.9.1. CC-specifikus eredmények

Az értékelési technikai jelentést (ETR) [10] a következőknek megfelelően készítették el: a Common Criteria [03] követelményei, a CEM értékelési módszertan [04], a Séma követelményei [05] és minden séma interpretáció (értelmezés) és útmutató (AIS) [06], ahogyan ezek a TOE-ra vonatkoztathatóak.

A CEM értékelési módszertant [04] az EAL4-ig alkalmazták, kiterjesztve a Tanúsítási Testület EAL4 fölötti komponensekre vonatkozó javaslataival, és a termék technológiai jellemzőire vonatkozó speciális útmutatókkal [06] (AIS 34).

Az alábbi technológia-specifikus útmutatót alkalmazták:

- Mivel a TOE értékelése összetett értékelésként történt, az ETR [10] tartalmazza az összetett értékelési tevékenységek eredményeit a CC Kiegészítő dokumentum, „ETR-lite a kompozícióra: A függelék Összetett intelligens kártya értékelés” [06] (AIS 36) dokumentumokban foglaltakkal összhangban.
- Az ETR [10] az alapul szolgáló „ST Microelectronics microcontroller: ST19WR66I" hardver ([18] ”értékelésének „ETR-lite a kompozícióra” dokumentumra épít. Az „ETR-lite a kompozícióra” [12] dokumentumot az ITSEF SERMA Technologies szolgáltatta, a CC kiegészítő dokumentumok, ETR-lite a kompozícióra [06] (AIS 36) foglaltaknak megfelelően, és egy friss újraértékelés során érvényesítették.
- Az intelligens kártyákra vonatkozó speciális módszertan vonatkozásában az AIS 25-t és AIS 26-t (lásd [06]) alkalmazták.

Az értékelés MEGFELELT döntését az alábbi garanciális összetevők támasztják alá:

- Az ASE osztály összes összetevője.
- Az EAL4 csomag összes összetevője, ahogyan azokat a CC-ben meghatározták.
- Az AVA_MSU.3 – „Helytelen használat elemzés” – „A nem biztonságos állapotok elemzése és tesztelése”, és AVA_VLA.4 „Sebezhetőségi elemzés” – „Magas szinten ellenálló” szigorítások a TOE értékeléshez.

Az értékelés megerősítette az alábbiakat:

- PP-megfelelőség áll fenn a 3-as típusú Biztonságos aláírás létrehozó eszköz Védelmi Profillal, 1.05 verzió, BSI-PP-0006-2002 [11];
- A funkcionalitásra: PP megfelelőség áll fenn, és termék specifikus kiterjesztés van CC 2. rész kiterjesztéssel;
- A garanciára: Common Criteria 3. résznek megfelel, emelt EAL4 az AVA_MSU.3 és AVA_VLA.4 összetevőkkel;
- Az alábbi TOE biztonsági funkcionalitás teljesíti az állított funkcióerősséget: SF.AUTH, SF.HASH, SF.SM, SF.HARDWARE. A funkcióerősség értékelés céljából az AIS 20 és AIS 31 sémaértelmezéseket (lásd [06]) vették figyelembe.

Az értékelés eredményei csak a 4.2. fejezetben definiált TOE-ra és a 4.8. fejezetben megadott konfigurációra vonatkoznak.

4.9.2. A kriptográfiai értékelés eredményei

A TOE az alábbi kriptográfiai algoritmusokat használja a biztonsági szabályzat érvényre juttatásához:

- hash függvények: SHA-1 (hardver által biztosított) és SHA-256, az ESW által implementálva. Az SHA-256 az ajánlott.
- rejtjelezési/megoldási algoritmusok: Triple DES 2 vagy 3 kulccsal, AES-128 vagy RSA 1024 és 2048 kulcshosszakkal. A támadásokkal szembeni nagyfokú

ellenálláshoz csak a Triple DES és AES-128 algoritmusok javasoltak szimmetrikus kriptográfiai algoritmusként. A Triple DES esetén a titkos kulcs hosszának 128-bitnek kell lennie (2 kulcs) vagy 192 bitnek (3 kulcs). Az RSA 2048 bit kulcshosszal ajánlott.

A fentiek az alábbi biztonsági funkciókra vonatkoznak:

- – SF.AUTH (Hitelesítési funkciók),
- – SF.KEY_GEN (Kulcs generálás),
- – SF.HASH (Hash számítás),
- – SF.MAC (MAC számítás),
- – SF.SIGN (Kriptográfiai funkciók),
- – SF.SM (Biztonságos üzenetváltás)
- – SF.HARDWARE (TRNG és fizikai védelem, TOE kriptográfiai támogatás).

4.10. A biztonsági előirányzat

A közzététel céljából a TOE biztonsági előirányzata [09] különálló dokumentumként áll rendelkezésre. Ez a végrehajtott értékelés során használt teljes biztonsági előirányzat [08] csökkentett verziója. A csökkentést a vonatkozó CCRA szabályzatban (lásd AIS 35 [06]) foglaltaknak megfelelően hajtották végre.

5. A Tanúsítási jelentés eredménye és érvényességi feltételei

5.1. A Tanúsítási jelentés eredménye

A Touch&Sign2048 V1.00
intelligens kártya termék
/ ST Incard S.r.l./

tanúsítás tárgyát képező verziója

A Touch&Sign2048 V1.00 SSCD alkalmazás
Touch&Sign2048 V1.00 eszköz meghajtók
Integrált áramkör és annak könyvtárai ST19WR66I az alábbi azonosítási adatokkal:

- 0x496E5472: MASK ID - (“InTr” ASCII-kódja)
- 0x00010002: ROM Code Version - (ver.01.02)
- 0x0180: EEPROM package CNS – (Version 1.80)

a tanúsítás érvényességi feltételeinek együttes teljesülése esetén

ALKALMAS

minősített aláírások létrehozására

mint

3-as típusú biztonságos aláírás-létrehozó eszköz.

5.2. Az eredmények érvényességi feltételei

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a Touch&Sign2048 V1.00 intelligens kártya termék BALE-ként való felhasználásának.

5.2.1. Általános érvényességi feltételek

Az alábbi feltételek minden felhasználási mód esetén (tehát a fejlesztő-gyártó cég által igen általánosra tervezett felhasználási kör egészében) szükségesek a megbízható és biztonságos működéshez.

1. A Touch&Sign2048 V1.00 intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók (aláírók) jól képzettek és megbízhatóak.
2. A Touch&Sign2048 V1.00 intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók betartják a felhasználói dokumentáció (Touch&Sign2048 V1.00 – User and Administrator Guidance, Version A-2, Date: 2007-12-07, ST Incard) által a biztonságos használatra vonatkozó ajánlásokat.

5.2.2. Az CC tanúsítás érvényességi feltételei

3. A CGA megvédi az aláíró nevének és az SVD-nek a hitelességét a minősített tanúsítványban a CSP fokozott biztonságú aláírása által (A.CGA).
4. Az aláíró csak megbízható SCA-t használ. Az SCA generálja és továbbítja az aláíró által aláírni kívánt adat DTBS-reprezentációját a TOE által aláírásra alkalmas formátumban (A.SCA).
5. A TOE perszonalizációja olyan fizikai és eljárásrendi intézkedések betartásával történik, amelyek biztosítják a TOE perszonalizációs adatok sértetlenségét, bizalmasságát és rendelkezésre állását. A biztonságos üzenetváltás megteremtéséhez szükséges megbízható csatornák és útvonal kialakítás szimmetrikus kulcsait biztonságos módon importálják és tárolják az SCA és CGA alkalmazások (A.PERSONALIZATION).
6. A TOE-t az Adminisztrátori útmutatóban leírtak szerint perszonalizálják és adminisztrálják, amit hozzáértő egyén végez, aki a TOE értékeinek a biztonságáért felelős és megbízható a tekintetben, hogy a jogosultságaival nem él vissza. A TOE adminisztrátor követi a TOE Adminisztrátori útmutatóban foglaltakat a TOE biztonságos megsemmisítése tekintetében, miután a TOE az SC használat vége állapotba került (A.MANAGE).
7. A TOE által igényelt pozitív azonosításhoz és hitelesítéshez szükséges információk a TOE felhasználókhoz biztonságos módon kerülnek (A.VAD).
8. A CSP csak megbízható CGA-t használ az SSCD által generált SVD számára készítendő minősített tanúsítvány generálásához (P.CSP_Qcert).

9. Az aláíró olyan aláírás létrehozó rendszert használ az adatok minősített elektronikus aláírással való ellátására, amely SSCD-vel előállított minősített tanúsítványon alapul (P.Qsign).
10. A TOE az aláírás létrehozásához használt SCD-t az aláíró kizárólagos felügyelete alatt tartja (P.Sigy_SSCD).
11. A támadásokkal szembeni nagy fokú ellenálláshoz csak a Triple DES és AES-128 algoritmusok használhatóak a hitelesítési folyamatokban. A Triple DES esetén a titkos kulcs hosszának 128-bitnek kell lennie (2 kulcs) vagy 192 bitnek (3 kulcs).
12. A generált SCD/SVD kulcspár hosszának 2048 bitnek kell lennie.
13. Bármilyen hosszú RSA kulcs generáláshoz legalább 5 bit hosszú nyilvános exponens használata szükséges, azaz értéke>=17.
14. A támadásokkal szembeni nagy fokú ellenálláshoz csak a Triple DES és AES-128 algoritmusok javasoltak szimmetrikus kriptográfiai algoritmusként. A Triple DES esetén a titkos kulcs hosszának 128-bitnek kell lennie (2 kulcs) vagy 192 bitnek (3 kulcs).
15. Az SCA által végrehajtott lenyomatkészítés használhatja az SHA-1 vagy SHA-256 algoritmust, de ez utóbbi használata javasolt.
16. A PIN kód értéke nem lehet kevesebb hat jegynél.
17. Az aláírási művelet előtt az aláírónak és az SCA-nak azonosítania és hitelesítenie kell magát.

5.2.3. A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei

Egy minősített aláírásokat létrehozó aláírónak a Touch&Sign2048 V1.00 intelligens kártya felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

18. A BALE-ként használt Touch&Sign2048 V1.00 intelligens kártyának csak egy felhasználója lehet, az aláíró.
19. Az aláírónak meg kell győződnie arról, hogy a kártyát még nem használták. (Ehhez a kibocsájtónak megfelelő útmutatót kell biztosítani.)
20. Az aláírónak a Touch&Sign2048 V1.00 intelligens kártyát biztonságos helyen kell őriznie és a felhasználói hitelesítő adatot titokban kell tartania.
21. A Touch&Sign2048 V1.00 intelligens kártyának használatának lezárulását követően a kártyát meg kell semmisíteni, vagy vissza kell juttatni a kibocsátóhoz.
22. A minősített aláírások létrehozására használt magánkulccsal csak minősített aláírást szabad létrehozni. (Így nem szabad fokozott biztonságú aláírás-létrehozására felhasználni.)

6. Felhasznált dokumentumok

6.1. Termékmegfelelőségi követelményeket tartalmazó dokumentumok

[01] Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

[02] CEN/ISSS ESign Workshop – Expert Group F: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+

6.2. A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

[03] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[04] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[05] BSI certification: Procedural Description (BSI 7125)

[06] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE, specifically:

- AIS 25, Version 3, 6 August 2007 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 2.0, CCDB-2006-04-003, April 2006
- AIS 26, Version 3, 6 August 2007 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 2.3, CCDB-2007-04-001, April 2007
- AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35 ST-lite
- AIS 36, Version 1, 29 July 2002 for: CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2 March 2002
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[07] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[08] Security Target BSI-DSZ-0422-2008, Touch&Sign2048 V1.00 - Security Target, Version A-3, Date 2007-03-29, ST Incard (confidential document)

[09] Security Target BSI-DSZ-0422-2008, Touch&Sign2048 V1.00 - Security Target, Version A-3, Date 2007-03-29, ST Incard (sanitised public document)

[10] Evaluation Technical Report for Touch&Sign2048 V1.00, Version 3, Date 2008-03-05, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (confidential document)

[11] Schutzprofil Secure Signature-Creation Device Type 3, Version 1.05, BSI-PP-0006-2002

[12] ETR-lite for composition ST19WR66D / ST19WR66I (EAL 5+), ITSEF of SERMA Technologies, 12.10.2006 and Surveillance Technical Report ST19WR66I, (EAL 5+), ITSEF of SERMA Technologies 25.02.2008 (confidential document)

[13] Touch&Sign2048 V1.00 –Configuration List, Version A-1, Date: 2008-01-18, ST Incard (confidential document)

[14] Touch&Sign2048 V1.00 – User and Administrator Guidance, Version A-2, Date: 2007-12-07, ST Incard

[15] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 17. Dezember 2007, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[16] Protection Profile PP9806 -Smartcard - Integrated Circuit, version: 2.0, EAL4+, September 1998

[17] ST Microelectronics, Security Target, SMD_ST19WR66_ST_05_001_V01.02

[18] Certification Report 2006/18, ST19WR66I microcontroller, November, 7th 2006, Direction centrale de la sécurité des systèmes d'information

[19] Security Requirements for Cryptographic Modules (FIPS PUB 140-2), NIST, 1999

[20] Certification Report BSI-DSZ-CC-0422-2008 for Touch&Sign2048 Version 1.00 from ST Incard S.r.l.

[21] Kérelem /a tanúsítás elvégzésére/

7. Rövidítések

AES Advanced Encryption Standard (Továbbfejlesztett rejtjelezési szabvány)

APDU Application Protocol Data Unit (intelligens kártyák interfész szabványa lásd ISO/IEC 7816 3. rész)

ATE Garancia osztály Tesztelés

ATE_IND Független tesztelés

ATR Answer to Reset (válasz resetre)

AVA Garancia osztály Sebezhetőségi felmérés

AVA_VLA Sebezhetőségi elemzés

BSI Bundesamt für Sicherheit in der Informationstechnik/ Információbiztonsági Szövetségi Hivatal, Bonn, Germany

BSIG Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG)of 17 December 1990, Bundesgesetzblatt I p. 2834

CCRA Common Criteria Recognition Arrangement (Common Criteria Elfogadási Megállapodás)

CC Common Criteria for IT Security Evaluation

CGA Certification generation application (Tanúsítvány generáló alkalmazás)

CSP Certification-Service provider (Hitelesítés szolgáltató)

DES Data Encryption Standard (Adattitkosítási szabvány)

DOC Documentation / documents (dokumentáció, dokumentumok)

DTBS Data to be signed (Aláírandó adat)

DTBSR Representation of Data to be signed (aláírandó adat reprezentációja)

EAL Evaluation Assurance Level (értékelési garanciaszint)

EEPROM Electronically Erasable Programmable Read Only Memory (elektronikusan törölhető programozható csak olvasható memória)

ESW Embedded Software (beágyazott szoftver)

ETR Evaluation Technical Report (értékelési technikai jelentés)

HW Hardware (hardver)

IC Integrated Circuit (integrált áramkör)

ID Identification number (azonosító szám)

IMP Implementation Representation (megvalósítási reprezentáció)

IT Information Technology (információ technológia)

ITSEF Information Technology Security Evaluation Facility (Információ technológiai biztonsági értékelési keret)

MAC Message Authentication Code (Üzenet hitelesítő kód)

MAP Modular Arithmetic Processor (moduláris aritmetikai processzor)

OE Operational Environment (üzemeltetési környezet)

ODP One Time Programmable (egyszer programozható)

PIN Personal Identification Number (személyi azonosító szám)

PP Protection Profile (védelmi profil)

PW Password (jelszó)

RAD Reference Authentication Data (referencia hitelesítő adat)

RNG Random Number Generator (véletlen szám generátor)

ROM Read Only Memory (csak olvasható memória)

RSA Rivest-Shamir-Adleman Algorithm (RSA algoritmus)

SC Smart Card (intelligens kártya)

SCA Signature creation application (aláírás létrehozó alkalmazás)

SCD Signature creation data (aláírás létrehozó adat)

SDO Signed Data Object (aláírt adatobjektum)

SF Security Function (biztonsági funkció)

SFP Security Function Policy (biztonsági funkció szabályzat)

SFR Security Functional Requirements (funkcionális biztonsági követelmények)

SHA Secure Hash Algorithm (biztonságos hash algoritmus)

SOF Strength of Function (funkcióerősség)

SSCD Secure Signature Creation Device (biztonságos aláírás létrehozó eszköz)

ST Security Target (biztonsági előirányzat)

SVD Signature verification data (aláírás ellenőrző adat)

SW Software (szoftver)

TDES Triple DES

TOE Target of Evaluation (értékelés tárgya)

TRNG True Random Number Generator (valódi véletlen szám generátor)

TSC TSF Scope of Control (TSF hatókör)

TSF TOE Security Functions (TOE biztonsági funkciói)

TSP TOE Security Policy (TOE biztonsági szabályzat)

TT Test Target (tesztelés tárgya)

VAD Verification authentication data (ellenőrző hitelesítési adat)

8. Szószedet

Alapszintű SOF – TOE funkcióerősségi szint, melynél az elemzés megmutatja, hogy a funkció megfelelő védelmet nyújt a TOE biztonságának eseti megsértésével szemben, amit az alacsony támadási képességgel rendelkező támadók követnek el.

Biztonsági előirányzat (Security Target, ST) – Biztonsági követelmények és specifikációk készlete, amelyet egy azonosított TOE értékelésének alapjaként használnak.

Biztonsági funkció (Security Function, SF) – A TOE egy része vagy részei, amelyekre a TSPből származó szabályok szorosan kapcsolódó részhalmazának érvényre juttatása érdekében támaszkodni kell.

Formális – Adott szemantikával bír, szigorú szintaxisú nyelven történő specifikálás, amely jól megalapozott matematikai elveken alapul.

Félformális – Adott szemantikával bíró, korlátozott szintaktikájú nyelven kifejezett.

Funkcióerősség (Strength of Function, SOF) – TOE biztonsági funkció osztályozása, amely azt a minimális befektetést fejez ki, ami feltételezetten ahhoz szükséges, hogy a várt biztonsági működést sikeresen támadják az alapul szolgáló biztonsági mechanizmusok közvetlen támadásával.

Informális – Természetes nyelven kifejezett.

Kiterjesztés – A CC 2. részében nem szereplő funkcionális vagy a 3. részében nem szereplő garanciális követelmény hozzáadása egy PP-hez vagy ST-hez.

Közepes SOF – TOE funkcióerősségi szint, melynél az elemzés megmutatja, hogy a funkció megfelelő védelmet nyújt a TOE biztonságának szándékos és egyértelmű megsértésével szemben, amit a közepes támadási képességgel rendelkező támadók követnek el.

Magas szintű SOF – TOE funkcióerősségi szint, melynél az elemzés megmutatja, hogy a funkció megfelelő védelmet nyújt a TOE biztonságának tervezett és/vagy szervezett megsértésével szemben, amit magas támadási képességgel rendelkező támadók követnek el.

Objektum – TSC-n belüli olyan egyed, amely információt tartalmaz vagy kap és amelyen szubjektumok műveleteket végeznek.

Szigorítás – Egy vagy több garanciális összetevő hozzáadása a CC 3. részéből egy EAL vagy garanciacsomaghoz.

Szubjektum – Olyan egyed a TSC-n belül, aki/ami művelet végrehajtását eredményezi.

Értékelés tárgya (Target of Evaluation, TOE) – Olyan IT termék vagy rendszer, továbbá a kapcsolódó adminisztrátori és felhasználói útmutatók, melyek az értékelés tárgyát képezik.

TOE biztonsági funkciói – TOE hardver, szoftver és förmver eleme halmaza, melyekre a TSP megfelelő érvényre juttatásához alapozni kell.

TOE biztonsági szabályzat – Szabályhalmaz, amely megadja, hogyan kell az értékeket kezelni, védeni és szétosztani a TOE-n belül.

TSF hatóköre – Interakciók összessége, melye a TOE-val vagy azon belül történhetnek, és a TSP szabályainak érvényességi körébe esnek.

Védelmi profil (Protection profile, PP)- Adott felhasználói igényt kielégítő TOE kategóriára vonatkozó biztonsági követelmények megvalósítás-független készlete.