Tanúsítási jelentés

Hung-TJ-049-2010

IDOneClassIC Card

ID-One Cosmo 64 RSA v5.4, applet: IDOneClassIC v1.0
platform: P5CT072VOP és
ID-One Cosmo 64 RSA v5.4.1, applet: IDOneCIE v1.01.1
platformok: P5CT072VOP, P5CC072VOP és P5CD072VOP

intelligens kártya
mint

biztonságos aláírás-létrehozó eszköz

/Oberthur Card Systems/

Verzió:	1.0
Fájl:	Hung-TJ-049-2010_v10.pdf
Minősítés:	Nyilvános
Oldalak:	29

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2010.06.30.	A szerkezet felállítása
v0.9	2010.07.12	Belső egyeztetésre kiadott változat
v0.91	2010.07.13	Egyeztetésre kiadott változat
v1.0	**2010.09.30.**	**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 IDOneClassIC Card megnevezésű többfunkciós intelligens kártya termék (ID-One Cosmo 64 RSA v5.4, applet: IDOneClassIC v1.0 platform: P5CT072VOP és ID-One Cosmo 64 RSA v5.4.1, applet: IDOneCIE v1.01.1 platformok: P5CT072VOP, P5CC072VOP és P5CD072VOP) (a későbbiekben erre a termékre „IDOneClassIC Card**”**-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:

[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.

- 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+).

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.

Az IDOneClassIC Card rendelkezik a második védelmi profilnak való megfelelőséget igazoló tanúsítvánnyal [07].

A tanúsítást igénylő szervezet a termék olyan megszemélyesítési eljárással készült terméket használ, mely nem képes a SM (secure messaging) kiépítésére a kártya és a host oldali alkalmazás között.
Ugyanakkor az SM kiépítés részét képezi a CC értékelt termék tanúsítványában foglalt feltételeknek. Következésképp a leszállított termékre nem érvényes a CC tanúsítvány, így ez automatikusan nem tekinthető biztonságos aláírás-létrehozó eszköznek.

A fenti probléma megoldása érdekében a tanúsítást igénylő szervezet egy új biztonsági előirányzatot készített [11], mely a termék (TOE, IDOneClassIC Card) és annak biztonsági környezete között egy új feladat-megosztást, illetve ebből fakadóan egy új felelősség-elhatárolást definiált. Az integritás védelmet igénylő adatok (tanúsítványba foglalandó nyilvános kulcs és hash érték), valamint az integritás és bizalmasság szempontjából megvédendő PIN kód védelmét a környezetre hárította (szabályozás és egyéb rezsim intézkedésekkel).

Ezen új biztonsági előirányzatot a Hunguard Kft értékelési divíziója a korábbi értékelések dokumentumainak felhasználásával és azok tükrében megvizsgálta, majd értékelési jelentést készített.

1.2. A tanúsítási jelentés feladata

Jelen tanúsítási jelentés fő feladatai:

- Az IDOne Classic Card vonatkozó tanúsítási eredmények bemutatása.
- A korábbi CC tanúsítás pozitív eredményei fenntarthatóságának megállapítása a ténylegesen megszemélyesített kártyákra, az új biztonsági előirányzat szerint, illetve annak megállapítása, hogy a többi kielégítendő funkcionális és biztonsági követelmény teljesülése milyen korlátozásokat, feltételeket támaszt a IDOne Classic Card intelligens kártya 3-as típusú BALE-ként való felhasználására.
- Annak megállapítása, hogy az új biztonsági előirányzatban a környezetre megfogalmazott szigorúbb feltételek teljesülése esetén BALE-nek tekinthetők-e a leszállított kártyák.

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 az IDOne Classic Card 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).
- Az IDOne Classic Card intelligens kártya néhány különleges tulajdonsága (3. fejezet).
- Az IDOne Classic Card-ra vonatkozó CC tanúsítvány eredményei (4. fejezet).
- Az IDOne Classic Card hazai értékelésének eredményei (5. fejezet).
- A minősített aláírás-létrehozáshoz való alkalmasság megállapítása, valamint az alkalmazás feltételeinek és korlátainak a meghatározása (6. fejezet).
- A jelen tanúsítási jelentéshez figyelembe vett dokumentumok jegyzéke (7. fejezet).
- Az alkalmazott rövidítések jegyzéke és szószedet (8. és 9. fejezet).

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

Az alábbiakban áttekintjük a vonatkozó SSCD [02] 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 (jelen esetben PIN kód), 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 (jelen esetben PIN kód 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 lennie.

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 ([03] szerint, vagyis a CC v2.3 verziója alapján).

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. Az IDOneClassIC Card főbb tulajdonságai

Az SSCD alkalmazás az alábbi funkciókat biztosítja:

- SCD és SVD generálás – a TOE garantálja az SCD titkosságát;
- Az SCD importálása;
- Az SVD exportálása;
- Aláírás létrehozás;
- Az aláíró PIN-el való hitelesítése: a TOE megőrzi a RAD-t, amelyet a felhasználó által megadott VAD ellenőrzésére használ;
- Megbízható útvonal kialakítása a humán interfész eszközhöz.

A TOE megsemmisíti az SCD-t, amennyiben azt a továbbiakban nem használják aláírás létrehozására. A felhasználási fázisban a TOE lehetővé teszi egy új SCD/SVD pár létrehozását. Az előző SCD-t meg kell semmisíteni az új SCD/SVD pár létrehozása előtt.
A TOE a 3-as típusú SSCD-t valósítja meg, illetve minden olyan SSCD funkciót, amely elektronikus aláírások biztonságos módon történő létrehozásával kapcsolatos.

A kártya az alábbi összetevőkből áll:

- Java kártya technológián JCRE[2], JCVM[3], JCAPI[4] és globális platform[5] technológián alapuló operációs rendszer. Ennek a fő feladatai az alábbiak:
  - Interfész biztosítása az integrált áramkör és az applet között.
  - Az applet számára alapszolgáltatások nyújtása a memóriák és minden szükséges kriptográfiai művelethez való hozzáférés céljából.
  - A kártya globális kezelésének biztosítása (betöltés, telepítés, appletek törlése), valamint a kártya biztonságának ellenőrzése (adat sértetlenség és fizikai támadással szembeni ellenintézkedések).

A betöltési mechanizmus zárolódik az applet betöltése után. Ezért az applet betöltés után nem kezdeményezhető betöltés.

- Az applet egy olyan magas biztonságú termék, amely az alábbi szolgáltatásokat nyújtja:
  - az ISO7816-4 és ISO7816-9 szabványokon alapuló nagy biztonságú és konfigurálható keretrendszer érzékeny és felhasználói adatok tárolására;
  - biztonságos üzenetváltás, az ISO7816-4 szerint;
  - hozzáférés ellenőrzési szabályok dinamikus menedzsmentje;
  - bizalmassági/sértetlenségi (biztonságos üzenetváltás feltételek) beállítások dinamikus menedzsmentje;
  - RSA kulcspár kártyán való generálása (2048 bitig), az ISO7816-8-nak megfelelően;
  - magán (SCD) RSA kulcsok importálása;
  - nyilvános (SVD) RSA kulcsok exportálása;

[2] „Java Card 2.2.1 - Application Programming Interfaces", October 21 2003, Sun Microsystems
[3] "Java Card 2.2.1-JCRE", October 21 2003, Sun Microsystems
[4] "Java Card 2.2.1-Virtual Machine Specifications", October 21 2003, Sun Microsystems
[5] "Global Platform Card Specification", version 2.1.1' March, 2003, Global Platform

- Triple DES alapú hitelesítés, rejtjelezés és megoldás, az ISO7816-4 és ISO7816-8 szabványoknak megfelelően;
- PIN hitelesítés;
- RSA digitális aláírás, az ISO7816-8-nak megfelelően.

4. Az IDOneClassIC Card CC tanúsításának eredményei

4.1. A termék

4.1.1. A termék azonosítása

Az értékelt termék Oberthur Card Systems és a Philips Semiconductors GmbH által fejlesztett «IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4 és applet IDOneClassIC v1.0 P5CT072VOP-re beépítve**».**
Ez a termék egy biztonságos aláírás létrehozó eszköz (SSCD), az alábbi alkotóelemekkel:

- az alapul szolgáló integrált áramkör;
- a Java virtuális gépet (JVM) magába foglaló operációs rendszer;
- az SSCD alkalmazás.

4.1.2. Az értékelt termék jellemzői

A biztonsági előirányzat [05] [06] határozza meg az értékelt terméket, annak értékelt funkcionalitását és működtetési környezetét.
A biztonsági előirányzat megfelel az SSCD [02] védelmi profilnak.

A termék azonosítása

A termék tanúsított verzióját az alábbi elemek azonosítják:

- mikrokontroller azonosító, «Philips T023P», amely a termék felső rétegére kerül, és mikroszkóppal olvasható;
- ROM kód azonosító, «0B6», amely a termék felső rétegére van írva, és mikroszkóppal olvasható;
- applet azonosító (AID), «A0 00 00 00 77 01 00 00 07 10 00 01 00 00 04», az applet betöltéshez megadva.

Biztonsági szolgáltatások

A termék az alábbi fő komponenseket tartalmazza:

- a Platform, ami JavaCard és GlobalPlatform technológiákon alapul, amely elsősorban az alábbi biztonsági szolgáltatásokat nyújtja:
  - az integrált áramkör és az IDOneClassIC applet közötti interfész;
  - alapszolgáltatások az IDOneClassIC applet számára a memóriákhoz és az összes szükséges kriptográfiai művelethez való hozzáféréshez;
  - a kártya globális kezelésének biztosítása (betöltés, telepítés és appletek törlése), valamint a kártya biztonságának ellenőrzése (adat sértetlenség és fizikai támadással szembeni ellenintézkedések);
  - az IDOneClassIC betöltése után a betöltő mechanizmus zárolása (miáltal az IDOneClassIC betöltése után nem kezdeményezhető további betöltés).

- az IDOneClassIC Applet, amely az alábbi fő biztonsági szolgáltatásokat nyújtja:

- titkos és nyilvános RSA aláíró kulcsok generálása (SCD: aláírás létrehozó adat, SVD: aláírás ellenőrző adat);
- titkos RSA aláíró kulcs (SCD) importálása;
- nyilvános RSA aláíró kulcs (SVD) exportálása;
- aláírás létrehozás;
- az aláíró PIN-nel történő hitelesítése.

Architektúra

A terméket az alábbi összetevők alkotják:

- a Philips Semiconductors GmbH által fejlesztett és gyártott P5CT072VOP mikrokontroller;
- az Oberthur Card Systems által fejlesztett JavaCard operációs rendszer, melynek alkotóelemei:
  - ID-One Cosmo 64 RSA v5.4 (GOP ID MX 64) platform, beágyazva a ROM mikrokontrolleren (BIOS/VM címke : build33, Platform címke : Platform RefV87, Rezidens alkalmazás címke : GOP64_20051014) ;
  - az RSA SFM opcionális kód, az EEPROM mikrokontrollerbe ágyazva (verzió: r1.0, címke Liv20060310) ;
- az SSCD alkalmazás: IDOneClassIC, melyet az Oberthur Card Systems fejlesztett, és a perszonalizációs fázisban töltődik be (IDOneClassIC v1.0).

Életciklus

A termék életciklusát az alábbi szakaszok alkotják:

IC fejlesztés és gyártás

1. fázis:
   OS fejlesztés
   Applet fejlesztés
2. fázis:
   IC fejlesztés a dedikált szoftverrel
   IC adatbázis kialakítás
   IC fotomaszk gyártás
3. fázis
   IC gyártás
   IC tesztelés és előperszonalizáció

Intelligens kártya fejlesztés és gyártás

4. fázis
   IC csomagolás
   Tesztelés
5. fázis
   Intelligens kártya termék befejező folyamat
   Tesztelés
6. fázis
   Perszonalizáció és applet betöltés
   Tesztelés
7. fázis
   Intelligens kártya termék végfelhasználás
   Életciklus folyamat vége

A terméket az **Oberthur Card Systems** fejlesztette.

A BSI által tanúsított mikrokontrollert a Philips Semiconductors GmbH fejlesztette és gyártotta.
Az értékelési folyamatban a termék perszonalizálóját „termék adminisztrátornak", a terminált pedig, amelyen az aláíró a kártyát használja, „termék felhasználónak" tekintették.

4.2. Az értékelés

Az értékelést a **Common Criteria 2.3 verziója** [03] alapján végezték, a Common Evaluation Methodology [04] előírásai szerint.
Az EAL4 szint fölötti garanciális komponensek esetén az értékelők saját értékelési módszereket követtek, melyek összhangban állnak a DCSSI által validált AIS34[6]-el.
Az intelligens kártyákkal kapcsolatos sajátosságok tekintetében a CC IC[7] és CC AP[8] dokumentumok szolgáltak útmutatóul.

Az értékelést a komponens-összetétel sémának megfelelően végezték el, ahogyan azt az ETR-lite for composition, Version 1.0, March 2002. útmutató leírja, annak megállapítása érdekében, hogy a már korábban tanúsított mikrokontroller szoftver integrálásából nem származik-e biztonsági gyengeség.

Ezért a P5CTT072VOP mikrokontrollernek az ALC_DVS.2, AVA_MSU.3 és AVA_VLA.4 komponensekkel szigorított EAL5 szinten való értékelésének eredményei a BSI-PP-0005-200T2 védelmi profilnak megfelelnek. A szóban forgó mikrokontrollert 2006. március 28-án tanúsították a BSI-DSZ-CC-0348-2006 hivatkozási szám alatt.

Az értékelés a CNS kártyatermék értékelési eredményeire épít, amelyet 2006. szeptember 15-én tanúsítottak a 2006/13[9] azonosítóval.
Az értékelési technikai jelentés [08], amelyet a DCSSI-nek 2007. január 24-én adtak be, részletezi az értékelők által végrehajtott munkát és megállapítja, hogy minden értékelési feladat eredménye „**megfelelt**".

[6] Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004
[7] Application of CC to Integrated Circuit
[8] Application of Attack Potential to Smartcards
[9] Certification report 2006/13 - Carte CNS : composant P5CT072VOP masqué par la plate-forme JavaCard GOP ID MX 64 et embarquant l'application CNS 1.0.7, 15 September 2006 SGDN/DCSSI

4.3. Tanúsítás

A 4.1. fejezetben azonosított, illetve az értékelés technikai jelentésében [08] leírt értékelést az érvényben lévő szabályoknak és szabványoknak megfelelően végezték el, egy akkreditált értékelő szervezettől megkívánt hozzáértéssel és elfogulatlansággal. Az elvégzett munka lehetővé tette CC tanúsítvány, valamint a hozzá tartozó tanúsítási jelentés [07] kibocsátását.

A tanúsítvány bizonyítja, hogy az értékelésre beadott "IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4 és IDOneClassIC v1.0 a P5CT072VOP-re ágyazott applet" teljesíti a biztonsági előirányzatában [05] meghatározott biztonsági követelményeket, a megemelt EAL4 értékelési garanciaszinten.

Korlátozások

A tanúsított termék felhasználójának tekintetbe kell vennie a biztonsági előirányzatban megadott, működtetési környezetre vonatkozó biztonsági célokat, valamint az útmutatóban [09] leírt ajánlásokat, különös tekintettel az alábbiakra:

- a nyilvános aláíró kulcs (SVD) és a titkos aláíró kulcs (SCD) közötti megfeleltetés (OE.SCD_SVD_Corresp);
- a titkos aláíró kulcs (SCD) biztonságos továbbítása az SSCD-k között (OE.SCD_Transfer);
- az aláírás létrehozó adat egyedisége (OE.SCD_Unique);
- minősített tanúsítványok létrehozása (OE.CGA_Qcert);
- a CGA ellenőrzi az SVD hitelességét (OE.SVD_Auth_CGA);
- az ellenőrző hitelesítő adat (VAD) védelme (OE.HI_VAD);
- az aláírandó adat (OE.SCA_Data_Intend).

4.4. Tanúsítvány karbantartás

4.4.1. A karbantartott termék azonosítása

A garanciakarbantartás [10] alá eső termék az Oberthur Card Systems és a Philips Semiconductors GMBH által fejlesztett IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4.1 és applet IDOneClassIC v1.01.1 a P5CT072VOP, P5CC072VOP és P5CD072VOP komponensekre beépítve

A terméken az applet a DF 65 tag-el küldött GET DATED paranccsal azonosítható, a válasz negyedik és ötödik byte-ja ekkor 10 11, ami megfelel az ID One Co v1.01.1-nek.

Ugyanilyen módon, a platform és a mikroáramkör azonosításához a GET DATED parancsot a DF 52 tag-el kell elküldeni, ekkor a válasz harmadik és negyedik byte-ja E9 20, ami a platform ID One Cosmo v5.4.1-et jelenti, a kilencedik byte pedig az alábbi módon azonosítja a mikroáramkört:

- 10 a P5CC072 esetén;
- 11 a P5CT072 esetén;
- 15 a P5CD072 esetén.

A garancia-karbantartás alá eső termék, három szakaszban végrehajtott módosítások után:
- egy R3 javítás a V5.4-ben;
- egy applet módosítás a V5.4-ben;
- egy alkalmazás maszkolva a V5.4.1-en.

A változtatások egyike sem okozott lényeges hatást a TOE-ra

4.5. A tanúsítvány elfogadása

4.5.1. Európai elismerés (SOG-IS)

A tanúsítványt a SOG-IS[10] megállapodásban foglaltaknak megfelelően állították ki.

A SOG-IS által 1999-ben létrehozott Európai Elfogadási Megállapodás lehetővé teszi az aláíró országok részéről az ITSEC és Common Criteria tanúsítványok elfogadását. Az európai elfogadás az ITSEC E6 és a CC EAL7 szintekig alkalmazható. A megállapodás hatáskörébe eső tanúsítványok az alábbi jelöléssel kerülnek kibocsátásra:

4.5.2. Nemzetközi CC elfogadás (CCRA)

Jelen tanúsítványt a CCRA[11] megállapodásban foglaltaknak megfelelően állították ki.

A Common Criteria Elfogadási Megállapodás lehetővé teszi az aláíró országok számára a Common Criteria tanúsítványok elfogadását. A kölcsönös elfogadás a CC EAL4 szintig és az ALC_FLR család vonatkozásában áll fenn.

[10] «Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[11] Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.

5. Az IDOne Classic Card hazai értékelésének eredményei

5.1. A termék azonosítása

Az értékelés tárgya a [07] szerint tanúsított és a [10] szerint tanúsítvány karbantartott IDONClassIC Card olyan perszonalizációs eljárás után kiadott verziója, ami SM (secure messaging) kiépítésére nem alkalmas, így az SSCD védelmi profilban megfogalmazott alábbi két biztonsági cél teljesítésére nem képes:

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.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.

Nem alkalmas továbbá az alábbi, működtető környezetre vonatkozó biztonsági cél támogatására sem:

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.

5.2. Az értékelés összefoglaló eredménye

Az értékelés fő következtetése az alábbi:
az IDOneClassIC Card megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az értékelés egyéb következtetései az alábbiak:

- **A korábbi CC értékelés pozitív eredményei fenntarthatók a ténylegesen megszemélyesített kártyákra, az új biztonsági előirányzat szerint.**
- **Az új biztonsági előirányzatban a környezetre megfogalmazott szigorúbb feltételek teljesülése esetén (lásd 5.3) a leszállított kártyák 3. típusú BALE-nek tekinthetők.**

5.3. Feltételek

Az értékelés fenti következtetései az alábbi (az eredeti biztonsági előirányzat feltételein túlmutató) feltételek teljesülésén múlnak:

Módosított környezeti biztonsági célok:

OE.SVD_Auth /Az SVD hitelessége/
A működtetési környezet biztosítja a TOE által a CGA felé exportált SVD sértetlenségét. A CGA ellenőrzi az összetartozást az aláíró SSCD-jében lévő SCD és a hitelesítés-szolgáltató (CSP) tanúsítvány-generáló funkciója számára adott inputban lévő SVD között.

OE.HI_VAD_NOSM /A VAD védelme/
Ha külső eszköz gondoskodik a humán interfészről a felhasználói hitelesítés során, akkor a működtetési környezetnek biztosítania kell a VAD bizalmasságát és sértetlenségét, ahogyan azt az alkalmazott hitelesítési módszer megkívánja.

Új környezeti biztonsági célok:

OE.SSCD_Prov_Service /AZ SSCD ellátó szolgáltatás által biztosított hiteles SSCD/
Az SSCD ellátó szolgáltatás hiteles eszközöket kezel, amelyek a jogosult felhasználó, mint aláíró számára elkészítendő TOE-kat valósítanak meg; perszonalizálja és kibocsátja az SSCD-ként funkcionáló TOE-t az aláírónak.

OE.DTBS_Protect /Az SCA megvédi az aláírandó adatot /
A működtetési környezet biztosítja, hogy a DTBS/R nem módosítható az SCA és a TOE közötti átvitel során.

OE.Signatory /Az aláíróra vonatkozó biztonsági kötelezettségek/
Az aláíró meggyőződik arról, hogy az SSCD ellátó szolgáltatástól kapott SSCD-ben tárolt SCD még nem használták. (Ehhez a kibocsájtónak megfelelő útmutatót biztosít.) Az aláíró a TOE-t felügyelete alatt tartja és bizalmasan kezeli a VAD-jét.

6. A Tanúsítási jelentés eredménye és érvényességi feltételei

6.1. A Tanúsítási jelentés eredménye

Az IDOneClassIC Card
intelligens kártya termék
/ Oberthur Card Systems /

tanúsítás tárgyát képező verziója

ID-One Cosmo 64 RSA v5.4, applet: IDOneClassIC v1.0
platform: P5CT072VOP
és
ID-One Cosmo 64 RSA v5.4.1, applet: IDOneCIE v1.01.1
platformok: P5CT072VOP, P5CC072VOP és P5CD072VOP

a tanúsítás érvényességi feltételeinek együttes teljesülése esetén

ALKALMAS

minősített aláírások létrehozására

mint

3-as típusú biztonságos aláírás-létrehozó eszköz.

6.2. Az eredmények érvényességi feltételei

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele az IDOneClassIC Card intelligens kártya termék BALE-ként való biztonságos felhasználásának.

6.2.1. 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. Az IDOneClassIC Card intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók (aláírók) jól képzettek és megbízhatóak.
2. Az IDOneClassIC Card intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók betartják a felhasználói dokumentáció által a biztonságos használatra vonatkozó ajánlásokat.

6.2.2. Az CC tanúsítás érvényességi feltételei

3. A CGA minősített tanúsítványokat generál, amelyek tartalmazzák többek között: a) a TOE-t használó aláíró nevét[12], b) az aláíró kizárólagos befolyása alatt álló TOE által tartalmazott SCD-hez tartozó SVD-t, c) a CSP fokozott biztonságú aláírását. (OE.CGA_QCert)
4. 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.SVD_Auth_CGA)
5. 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.HI_VAD)
6. Az SCA: a) elkészíti a DTBS-ként bemutatott adat DTBS-reprezentációját, amit az aláíró alá akar írni, a TOE által aláírásra alkalmas formában; b) továbbítja a DTBS-reprezentációt a TOE felé, és lehetővé teszi, hogy a TOE ellenőrizni tudja a DTBS-reprezentáció sértetlenségét; c) hozzácsatolja a TOE által előállított aláírást az adathoz vagy különállóan szolgáltatja azt. (OE.SCA_Data_Intend)
7. A generált SCD/SVD RSA kulcspár ajánlott mérete 2048 bit. Ettől kisebb, de 1020 bitnél nagyobb RSA kulcspár 2011. szeptember 24-ig használható feltéve, hogy a Hatóság ezt határozatban hamarabb meg nem tiltja.
8. Bármilyen hosszú RSA kulcs generáláshoz legalább 5 bit hosszú nyilvános exponens használata szükséges, azaz értéke>=17.

[12] A név lehet álnév is, de ezt a tényt a minősített tanúsítványban jelezni kell.

9. A felhasználó a PIN kód értékét ne válassza hat jegynél rövidebbre.
10. Az aláírási művelet előtt az aláírónak és az SCA-nak azonosítania és hitelesítenie kell magát.

6.2.3. Az SM (Secure messaging) elhagyásának feltételei

11. Amennyiben az IDOneClassIC Card intelligens kártyát úgy perszonalizálták, hogy az SM (secure messaging) kiépítésre nem képes, akkor a biztonságos környezet kialakításának szükségességéről a végfelhasználót (aláírót) a kártyát kibocsájtó hitelesítés szolgáltatónak egyértelműen tájékoztatni kell.
12. A működtetési környezet biztosítja a TOE által a CGA felé exportált SVD sértetlenségét. A CGA ellenőrzi az összetartozást az aláíró SSCD-jében lévő SCD és a hitelesítés-szolgáltató (CSP) tanúsítvány-generáló funkciója számára adott inputban lévő SVD között. (OE.SVD_Auth)
13. Ha külső eszköz gondoskodik a humán interfészről a felhasználói hitelesítés során, akkor a működtetési környezetnek biztosítania kell a VAD bizalmasságát és sértetlenségét, ahogyan azt az alkalmazott hitelesítési módszer megkívánja. (OE.HI_VAD_NOSM)
14. Az SSCD ellátó szolgáltatás hiteles eszközöket kezel, amelyek a jogosult felhasználó, mint aláíró számára elkészítendő TOE-kat valósítanak meg; perszonalizálja és kibocsátja az SSCD-ként funkcionáló TOE-t az aláírónak. (OE.SSCD_Prov_Service)
15. A működtetési környezet biztosítja, hogy a DTBS/R nem módosítható az SCA és a TOE közötti átvitel során. (OE.DTBS_Protect)
16. Az aláíró meggyőződik arról, hogy az SSCD ellátó szolgáltatástól kapott SSCD-ben tárolt SCD még nem használták. (Ehhez a kibocsájtó megfelelő útmutatót biztosít.) Az aláíró a TOE-t felügyelete alatt tartja és bizalmasan kezeli a VAD-jét. (OE.Signatory)

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

Egy minősített aláírásokat létrehozó aláírónak az IDOneClassIC Card intelligens kártya felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

17. A BALE-ként használt IDOneClassIC Card intelligens kártyának csak egy felhasználója lehet, az aláíró.
18. Az IDOneClassIC Card intelligens kártyának használatának lezárulását követően a kártyát meg kell semmisíteni, vagy vissza kell juttatni a kibocsátóhoz.
19. A minősített aláírások létrehozására használt magánkulccsal csak minősített aláírást szabad létrehozni. (Így nem szabad fokozott biztonságú aláírás-létrehozására felhasználni.)

7. Felhasznált dokumentumok

7.1. 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+

7.2. A tanúsítási jelentésben hivatkozott 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] IDOneClassIC CARD Security Target, ref. FQR: 110 3517, edition 4, 16/01/07

[06] IDOne™ ClassIC Card V1.0 Public Security Target (eredeti biztonsági előirányzat kivonat)

[07] Certification Report 2007/02 (IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4 and applet IDOneClassIC v1.0 embedded on P5CT072VOP) (eredeti tanúsítási jelentés)

[08] az eredeti CC értékelési jelentés megismerésének lehetősége
- ANTERAK project: Evaluation Technical Report, ref. ANTERAK_ETR_V1.2, version 1.2, 24/01/07

[09] az eredeti termék telepítési, adminisztrátori és felhasználói dokumentációi:
- IDOneClassIC Guidance, ref. FQR : 110 3558, édition: 1 du 20/11/06
- Software Requirement Specification, ref. 066771 00 SRS, édition 1-AB du 23/11/06

[10] Rapport de Maintenance ANSSI-CC-2007/02-M02

[11] IDOne Classic Card SSCD Type 3 Proprietary Security Target (új biztonsági előirányzat)

[12] Különbségek az IDOne Classic Card Public Security Target és az IDOne Classic Card SSCD Type 3 Proprietary Security Target között (az eredeti és az új biztonsági előirányzat összehasonlítása)

[13] NETLOCK ID-ONE CLASSIC File Structure and Access Conditions (a Netlock Kft. számára leszállított kártyák megszemélyesítésének részletei)

[14] IDOne Classic Card SSCD Type 3 ÉRTÉKELÉSI JELENTÉS v1.0 Készítette Hunguard Kft.

[15] Kérelem /a tanúsítás elvégzésére/

8. Rövidítések

ACM (Assurance: Configuration management)	Konfiguráció kezelés értékelése
ADO (Assurance: Delivery and operation)	Szállítás és üzemeltetés értékelése
ADV (Assurance: Development)	Fejlesztés értékelése
AGD (Assurance: Guidance documents)	Útmutató dokumentumok értékelése
ALC (Assurance: Life cycle support)	Életciklus támogatás értékelése
ASE (Assurance: Security Target)	Biztonsági előirányzat értékelése
ATE (Assurance: Tests)	Tesztelés értékelése
AVA (Assurance:Vulnerability assessment)	Sebezhetőségi elemzés értékelése
CC (Common Criteria)	Közös szempontok
CGA (Certification generation application)	Tanúsítvány-létrehozó alkalmazás
CEM (Common Evaluation Methodology)	Közös értékelési módszertan
CSP (Certificate Service Provider)	Hitelesítés-szolgáltató
DTBS (Data to be Signed)	Aláírandó adat
DTBS/R (DTBS Representation)	Aláírandó adat reprezentáció
EAL (Evaluation Assurance Level)	Értékelési garanciaszint
ETR (Evaluation Technical Report)	Értékelési jelentés
IC (Integrated Circuit)	Integrált áramkör
IT (Information Technology)	Információ technológia, informatika
PIN (Personal Identification Number)	Személyi azonosító szám
PP (Protection Profile)	Védelmi profil
SCA (Signature Creation Application)	Aláírás-létrehozó alkalmazás
SCD (Signature Creation Data)	Aláírás-létrehozó adat
SM (Secure Messaging)	Biztonságos üzenetváltás
SSCD (Secure Signature Creation Device)	Biztonságos aláírás-létrehozó eszköz (BALE)
ST (Security Target)	Biztonsági előirányzat
SVD (Signature Verification Data)	Aláírás ellenőrző adat
TOE (Target of Evaluation)	Értékelés tárgya

9. Szószedet

biztonsági cél
Szándéknyilatkozat azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági szabályzatoknak és feltételezésnek való megfelelésről.

biztonsági előirányzat
Biztonsági követelmények és előírások olyan összessége, amelyet valamilyen adott tárgy értékelésének alapjaként használnak.

biztonsági funkció
Az értékelés tárgyának olyan része vagy részei, amelyben meg kell bízni ahhoz, hogy a vonatkozó biztonsági szabályzatból egy szorosan összefüggő szabályhalmaznak érvényt lehessen szerezni.

biztonsági funkció szabályzata
A biztonsági funkció által érvényre juttatott biztonsági szabályzat.

értékelés
A biztonsági előirányzat, illetve az értékelés tárgyának felmérése meghatározott szempontrendszer (a CC módszertana) alapján.

értékelés tárgya
Az az informatikai termék vagy rendszer, valamint a hozzá kapcsolódó adminisztrátori és használati útmutatók, amelyre az értékelés irányul.

értékelési garanciaszint
A CC. 3 rész olyan garancia összetevőiből álló csomag, amelyek egy-egy pontot képviselnek a CC előre meghatározott garanciális skáláján.

értékelési séma
Olyan igazgatási és szabályozási keret, amely szerint az értékelő szervezet egy adott közösségben alkalmazza a CC-t.

értékelő szervezet
Az a testület, amely egy adott közösség keretein belül az úgynevezett értékelési séma révén valósítja meg a CC-t.

felhasználó
Az a személy, aki a TOE (értékelés tárgya) szolgáltatásait igénybe kívánja venni.

termék
Informatikai szoftver, förmver és/vagy hardver által alkotott csomag, amely adott használatra vagy különböző rendszerekbe való beépítésre tervezett funkciókészletet szolgáltat.

védelmi profil
Megvalósítástól független, olyan biztonsági követelményrendszer az értékelés tárgyainak egy kategóriájára, amely adott fogyasztói igényeket elégít ki.