TANÚSÍTVÁNY (E-HT09T_TAN-01.ST) MELLÉKLETE

Dokumentumazonosító	TAN-01.ST.ME-01	
Projektazonosító	E-HT09T	Huntrust Kft. 2009.
MATRIX tanúsítási igazgató	Dr. Szőke Sándor	
MATRIX tanúsító	Hornyák Gábor	
Kelt	Budapest, 2009. december 22.	
..... MATRIX tanúsítási igazgató	..... MATRIX tanúsító részéről	

TARTALOMJEGYZÉK

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

2009. elején a HUNTRUST Kft. megkeresésére szakmai egyeztetések kezdődtek a HUNTRUST által fejlesztett BALE tanúsítása tárgyában. Az egyeztetések során körvonalazódtak a tanúsítás feltételei, a tanúsítást HUNTRUST két egymásra épülő lépésben kívánja elvégeztetni:

- BALE Biztonsági Előirányzat tanúsítása;
- BALE tanúsítása a Common Criteria követelményrendszere szerint kifejlesztett dokumentáció és az eszközön végzett független tesztek alapján.

A projekt első fázisában MATRIX a Biztonsági Előirányzat vizsgálatát végezte el. Az elvégzett vizsgálatok alapján MATRIX megállapította a Biztonsági Előirányzat megfelelőségét és kiállította az E-HT09T_TAN-01.ST azonosítójú tanúsítványt és annak jelen mellékletét.

A tanúsítvány melléklete a tanúsítás főbb körülményeit és érvényességének feltételeit foglalja össze.

2 A VIZSGÁLAT KÖRÜLMÉNYEI

2.1 A vizsgált Biztonsági Előirányzat megnevezése

- Huntrust IDentity Applet Biztonsági Előirányzat Ver. 1.0.

2.2 A vizsgálathoz a fejlesztő által átadott dokumentációk

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Dokumentáció	IDentity v1.0 SSCD Security Target	1.0	2009. szeptember 2.	elektronikus
Dokumentáció	Fejlesztő nyilatkozata a biztonsági körülményekről		2009. december 2.	papír

2.3 A vizsgálat megrendelője

A vizsgálat megrendelője megegyezik a Biztonsági Előirányzat fejlesztőjével. A fejlesztő:

- HUNTRUST Kft.
- 1029 Budapest, Turul köz 51.

2.4 A Biztonsági Előirányzat azonosítása

ST címe	IDentity v1.0 SSCD Security Target
ST referencia	ST-J3A080-CC-IDentity-V1
ST verzió	1.0

Dátum	2009. december 15.
Szerző	Szabó Tamás
Fejlesztő	Szabó Tamás
Termék típus	Java Card applet
Termék neve	IDentity v1.0
TOE neve	J3A080-CC-IDentity-V1
TOE verzió	1.0
TOE platform	NXP J3A080 v2.4.1
TOE hardver	P5CD080V0B
CC verzió	Common Criteria for Information Technology Security Evaluation Version 2.3 Final of August 2005 - Part 1: CCMB 2005-08-001 - Part 2: CCMB 2005-08-002 - Part 3: CCMB 2005-08-003
PP megfelelés	Protection Profile: Secure Signature-Creation Device Type 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Identification: PP0005b Protection Profile: Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Identification: PP0006b

2.5 ST áttekintése

A vizsgált ST célja, hogy az 1999/93 EU direktíva [1] III. mellékletében előírtaknak megfelelő funkcionális és biztonsági követelményeket fogalmazzon meg az 'IDentity Applet' elektronikus aláírás alkalmazás számára. A Biztonsági Előirányzat az SSCD Type 2 [6] és az SSCD Type 3 [7] Védelmi Profilokon alapul. Két fő konfiguráció létezik:

1. A teljesen SSCD PP megfelelő verzióban kötelezően létrehozandó a megbízható csatorna az SSCD és az Aláírás létrehozó alkalmazás (SCA) között.

2. Eltér az SSCD PP követelményeitől annyiban, hogy a megbízható csatorna az SSCD és az SCA között létrehozható, de nincs kikényszerítve. Ebben az esetben megkülönböztet megbízható és nem megbízható aláírási környezetet az aláírás létrehozó applikáció szempontjából. Megbízható környezetben a megbízható csatorna létrehozása nem követelmény. Nem megbízható környezetben minősített aláírás csak a megbízható csatorna létrehozása esetén állítható elő. A megbízható csatorna sikeres létrehozásáról a kártyabirtokos értesítést kap egy üzenet kijelző szolgáltatáson (Display Message mechanism) keresztül. Annak megállapítása a kártyabirtokos feladata, hogy egy környezet megbízhatónak tekinthető-e.

A Biztonsági Előirányzat egy aláírás létrehozó adatok és minősített elektronikus aláírások létrehozására szolgáló Biztonságos Aláírás Létrehozó Eszköz biztonsági követelményeit határozza meg. Az Értékelés Tárgya egyéb funkciókat és biztonsági követelményeket is megvalósíthat, mint például az aláírandó adatok megjelenítése és szerkesztése, de ezek a hozzáadott funkciók és biztonsági követelmények nem képezik a vizsgált Biztonsági Előirányzat tárgyát.

Az Értékelés Tárgya egy chipkártyán megvalósított BALE, amely képes aláírás létrehozó adatok generálására és importálására, valamint minősített elektronikus aláírások létrehozására. Az Értékelés Tárgya megvédi az aláírás létrehozó adatokat és biztosítja, hogy azokat csak az arra feljogosított aláíró használhassa.

Az IDentity applet egy NXP J3A080 v2.4.1 Secure Smart Card Controller-en lett megvalósítva, ami egy NXP SmartMX Integrált áramkör JCOP 2.4.1 Java Card Operációs rendszerrel. Az NXP SmartMX P5CD080V0B Smart Card Controller Integrált áramkör kontaktusos és érintésmentes csatoló felületeket is támogat.

A chipkártyás kontroller a BSI által kiállított EAL5+ CC tanúsítvánnyal rendelkezik [10], a vonatkozó ST [9] megfelel a PP/0303 [8] Védelmi Profilnak.

Az ÉT applikáció egy biztonságos környezetben lesz telepítve és megszemélyesítve, és a kártyabirtokosok – a megszemélyesítéskori konfiguráció függvényében – ismert, megbízható (hostile environment), illetve nem megbízható környezetben fogják használni. A chipkártya operációs rendszer betöltő mechanizmusa a megszemélyesítés után blokkolva lesz, így a kibocsátás után nem lehet további alkalmazást telepíteni a kártyára, bár az ÉT maga egy multi-applikációs platform, amely lehetővé tenné a megfelelő jogosultságokkal rendelkező entitások számára a kibocsátás után további alkalmazások feltöltését a kártyára.

Az ÉT egy multi-applikációs chipkártya platform elektronikus azonosítási feladatok ellátására, amely támogatja a max 2048 bites RSA és az SHA-256 algoritmusokat és megfelel az európai állampolgári kártya (European Citizen Card [11]) és az ISO 24727 [12] szabványoknak a tekintetben, hogy megvalósítja valamennyi kötelező funkciót és az opcionális funkciók egy részét.

Az ÉT megfelel az EU Irányelv 2. cikk 2. pontja által definiált, a fokozott biztonságú elektronikus aláírással szemben támasztott alábbi követelményeknek:

a) egyértelműen kapcsolódik az aláíróhoz;

b) képes azonosítani az aláírót;

c) olyan eszközökkel készült, amelyek folyamatosan az aláíró felügyelete alatt állnak,

d) úgy kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása felfedhető.

Az Értékelés Tárgya hardver és szoftver alkotó elemekből épül fel.

2.6 CC megfelelés

Az ST megfelel az alábbi Common Criteria követelményeknek:

- CC Version 2.3 Part 2 [3] (az SSCD PP [7] és a CC Version 2.3 Part 3 [4] dokumentumokban megfogalmazott kiegészítésekkel);
- SSCD Type 2 Protection Profile [6];

- SSCD Type 3 Protection Profile [7].

Az ST garanciaszintje EAL4 az alábbi kiterjesztésekkel:

- AVA_MSU.3 A nem biztonságos állapotok elemzése és vizsgálata;
- AVA_VLA.4 Keményen ellenálló.

A TOE biztonsági funkcionális követelményeinek funkcióerőssége minimálisan 'felső szintű' (SOF-high).

3 ELVÉGZETT VIZSGÁLATOK

3.1 Megfelelés a kötelezően betartandó normatíváknak

- 2001. évi XXXV. törvény az elektronikus aláírásról [13];
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [15];
- Megfelelés az algoritmikus követelményeknek
  Nemzeti Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917-x/2008 határozata [16].

3.2 Megfelelés az önként vállalt normatíváknak

- Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről [1];
- 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről [14];
- PP0005b – Protection Profile — Secure Signature-Creation Device Type 2 – EAL 4+ – Version: 1.04, 25 July 2001 [6];
- PP0006b – Protection Profile — Secure Signature-Creation Device Type 3 – EAL 4+ – Version: 1.05, 25 July 2001 [7];
- Common Criteria Version 2.3 Part 2 [3] (az SSCD PP [7] és a CC Version 2.3 Part 3 [4] dokumentumokban megfogalmazott kiegészítésekkel).

3.3 Biztonsági körülmények, környezet

A vizsgálat során MATRIX azt értékelte az átadott dokumentációk alapján, hogy a fejlesztés módszertana és a használt informatikai környezet megfelelő-e az adott dokumentum biztonságos kifejlesztéséhez.

4 A VIZSGÁLAT MÓDSZERTANA

MATRIX a fejlesztő által választott CC verziónak megfelelően az alábbi módszertan szerint végezte el a vizsgálatokat:

- Common Methodology for Information Technology Security Evaluation
  - CCMB-2005-08-004 - Evaluation methodology, August 2005., Version 2.3 [5].

5 MEGFELELŐSÉG KINYILVÁNÍTÁSA

5.1 Megfelelőség

Az elvégzett vizsgálatok alapján MATRIX megállapította, hogy a HUNTRUST által elkészített és vizsgálatra átadott 'Huntrust IDentity Applet Biztonsági Előirányzat Ver. 1.0.' Biztonsági Előirányzat megfelel a kötelező érvényű és a fejlesztő által önként vállalt normatíváknak az 3. pont szerinti részletezésben. A dokumentum vizsgálata során bizonyítást nyert, hogy a dokumentum konzisztens és műszaki szempontból helyes, ezért alkalmas arra, hogy a tervezett elektronikus aláírási termékhez követelményeket rögzítsen. A megfelelés igazolásaként MATRIX kiállította az E-HT09T_TAN-01.ST azonosítójú tanúsítványt.

5.2 Felhasználási kör

A vizsgált Biztonsági Előirányzat elsősorban a biztonságos aláírás létrehozó eszköz fejlesztői számára szolgál útmutatóként, de hasznos információt tartalmaz az ST alapján kifejlesztendő BALE felhasználói számára is.

5.3 Az érvényesség feltétele

A TOE akkor lesz használható minősített elektronikus aláírások előállítására, ha a fejlesztése és felhasználása során betartják az alábbi feltételeket:

EAT:

- Az ST alapján létrehozott ÉT akkor tekinthető a törvény szerinti biztonságos aláírás-létrehozó eszköznek, ha ezt egy *az informatikáért felelős miniszter által kijelölt, illetve a laboratóriumok, a tanúsító és ellenőrző szervezetek akkreditálásáról szóló 1995. évi XXIX. törvény szerinti szakmai akkreditáló bizottságok által akkreditált és tanúsításra jogosult szervezetek, illetőleg a (Eat.) 7. § (3) bekezdése szerinti tanúsító szervezet által kiadott igazolás* tanúsítja, továbbá az ÉT *megfelel az igazolásban megjelölt egyéb követelményeknek*.

- Az ÉT fejlesztőjének részletes dokumentációt kell előállítania a Hitelesítés szolgáltató részére, amely pontosan meghatározza, hogy az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése során milyen feltételeket kell betartani annak érdekében, hogy az Értékelés Tárgya megfeleljen az EAT 16/A § (1)-(5) követelményeinek és felhasználható legyen Fokozott biztonságú illetve Minősített elektronikus aláírások létrehozására.

- Az ÉT tanúsítása során a Tanúsítónak meg kell vizsgálnia, hogy az ÉT megfelel-e az aktuális kriptográfiai algoritmikus és paraméter követelményeknek, és a kiállítandó

Tanúsítvány érvényességének feltételéül kell szabni a tanúsítvány érvényességének idejére a kriptográfiai algoritmikus és paraméter követelmények figyelését.

- Az ÉT tanúsítványát a tanúsító szervezetnek be kell jelentenie a nyilvántartást vezető Hatóságnak.

IHM rendelet:

- Az ÉT fejlesztőjének részletes dokumentációt kell előállítania a Hitelesítés szolgáltató részére, amely pontosan meghatározza, hogy az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése során milyen feltételeket kell betartani annak érdekében, hogy az Értékelés tárgya megfeleljen az IHM rendelet 40 § (1)-(5) követelményeinek és felhasználható legyen Fokozott biztonságú illetve Minősített elektronikus aláírások létrehozására.

MeHVM irányelv:

- (105) A külső kulcsgenerálás esetén a Hitelesítés Szolgáltató által betartandó előírás: ’*A megbízható rendszerek nem rendelkezhetnek olyan funkcióval, amely lehetővé tenné az előfizető magán aláíró kulcsának mentését vagy letétbe helyezését.’*

- (138) A Hitelesítés Szolgáltatónak a tanúsítvány kiadása során be kell tartania az alábbi követelményt ’*Amennyiben az aláíró kulcspárt nem a HSZ hozza létre, a tanúsítvány kérelmi eljárásnak igazolnia kell, hogy az ügyfél a tanúsításra bemutatott nyilvános kulcshoz tartozó magán kulcsot birtokolja.*’

- Amennyiben az aláírói kulcspár előállítása az aláírás-létrehozó eszközön kívül történik, teljesülniük kell az alábbi követelményeknek:

  (226) ’a kulcspárt előállító kriptográfiai eszköznek tanúsítvánnyal igazoltan meg kell felelnie az alábbi szabványok, szabványjellegű dokumentumok legalább egyikének:
  a) FIPS 140-1, 3-as szint,
  b) CEN HSM PP,
  C) CEN SSCD PP.’

  (227) ’a kulcspárt biztonságos módon kell az aláírás-létrehozó eszközbe juttatni, az alábbi értelemben: a kriptográfiai eszköz és az aláírás létrehozó eszköz között biztonságos útvonalnak kell lennie, melynek forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával’

  (228) ’a kulcspárnak az aláírás-létrehozó eszközben történt elhelyezése után az aláírás-létrehozó eszközön kívüli magánkulcsot biztonságos módon meg kell semmisíteni.’

- (1. melléklet) Az ST és az ÉT tanúsítása során a Tanúsítónak meg kell vizsgálnia, hogy az ÉT megfelel-e az aktuális kriptográfiai algoritmikus és paraméter követelményeknek, és a kiállítandó Tanúsítvány érvényességének feltételéül kell szabni a tanúsítvány érvényességének idejére a kriptográfiai algoritmikus és paraméter követelmények figyelését.

EU irányelv:

- II. MELLÉKLET

  A minősített tanúsítványokat kiállító hitelesítés-szolgáltatóra vonatkozó követelmények.

  A hitelesítés-szolgáltató köteles:

  j) tartózkodni azon személy aláírás-létrehozó adatainak a tárolásától, illetve másolásától, akinek kulcskezelési szolgáltatásokat nyújtott;

Algoritmikus követelmények:

A TOE által támogatott alábbi kriptográfiai algoritmuskészlet 2012 végéig jelenlegi ismereteink szerint megfelelően biztonságos marad:

- sha256 lenyomatképző függvény;
- emsa-pkcs1-v1.5, iso9796-ds2 vagy iso9796-ds3 feltöltő algoritmus;
- RSA aláíró algoritmus 2048 bites kulccsal;
- rsagen1 kulcsgeneráló algoritmus;
- trueran véletlenszám generátor.

Új eszköz és alkalmazás fejlesztésénél javasolt az sha256 lenyomatképző függvény és a 2048 bites RSA kulcs használata.

Az sha1 lenyomatképző függvény és a min. 1024 bites RSA kulcs használata jelenleg nem tiltott, így a felhasználó dönthet ezek alkalmazásáról is.

A javasoltnál gyengébb kriptográfiai algoritmus vagy paraméter felhasználása a támadási módszerek fejlődése miatt fokozott kockázattal jár.

A TOE felhasználójának folyamatosan figyelnie kell az algoritmikus követelmények változásait, és szükség esetén fel kell készülnie a használat módjának megváltoztatására, vagy extrém esetben az eszközök tervezettnél korábbi tömeges cseréjére.

6 HIVATKOZÁSOK

[1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 1999/93/EK IRÁNYELVE (1999. december 13.) az elektronikus aláírással kapcsolatos közösségi keretrendszerről;

[2] Common Criteria for Information Technology Security Evaluation
- CCMB-2005-08-001 - Part 1: Introduction and general model, August 2005., Version 2.3;

[3] Common Criteria for Information Technology Security Evaluation
- CCMB-2005-08-002 - Part 2: Security functional requirements, August 2005., Version 2.3;

[4] Common Criteria for Information Technology Security Evaluation
- CCMB-2005-08-003 - Part 3: Security assurance requirements, August 2005., Version 2.3;

[5] Common Methodology for Information Technology Security Evaluation - CCMB-2005-08-004 - Evaluation methodology, August 2005., Version 2.3;

[6] PP0005b – Protection Profile — Secure Signature-Creation Device Type 2 – EAL 4+ – Version: 1.04, 25 July 2001;

[7] PP0006b – Protection Profile — Secure Signature-Creation Device Type 3 – EAL 4+ – Version: 1.05, 25 July 2001;

[8] PP/0303 – Minimal Configuration Protection Profile, Version 1.1, May 2006 – Smartcard Integrated Circuit, version: 2.0 EAL4+;

[9] Security Target Lite BSI-DSZ-CC-0515, NXP J3A080 v2.4.1 Secure Smart Card Controller Rev. 01.06 – December 2008;

[10] Certification Report BSI-DSZ-CC-0515-2009, NXP J3A080 v2.4.1 Secure Smart Card Controller (JCOP c2.4.1);

[11] CEN/TS 15480-2 – Identification card systems - European Citizen Card - Part 2: Logical data structures and card services;

[12] ISO/IEC 24727-2 – Identification cards — Integrated circuit card programming interfaces — Part 2: Generic card interface;

[13] 2001. évi XXXV. törvény az elektronikus aláírásról;

[14] 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről;

[15] 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről;

[16] Nemzeti Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917-x/2008 határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően.

7 RÖVIDÍTÉSEK

Rövidítés	Magyarázat
BALE	Biztonságos Aláírás Létrehozó Eszköz
BE	Biztonsági Előirányzat - egy megvalósítandó termék biztonsági rendszerterve
CC	Common Criteria - MSZ ISO/IEC 15408. Az informatikai biztonság értékelésének közös szempontrendszere
EAT	2001. évi XXXV. törvény az elektronikus aláírásról
ÉT	Értékelés Tárgya – az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza

Rövidítés	Magyarázat
PP	Protection Profile – a Védelmi Profil eredeti, angol elnevezése
SCA	Signature-Creation Application – aláírás létrehozó alkalmazás angol rövidítése
SSCD	Secure Signature-Creation Device – a BALE angol elnevezése
ST	Security Target – a Biztonsági Előirányzat eredeti, angol elnevezése
TOE	Target Of Evaluation – az Értékelés Tárgya eredeti, angol elnevezése
VP	Védelmi Profil – egy megvalósítandó termék általános, technológia-független leírása, követelményrendszere

Javított változat 2010. 09. 17. Szádeczky Tamás

Dokumentum vége