TANÚSÍTVÁNY (E-HT11F1-TAN.SSCD) MELLÉKLETE

Dokumentumazonosító	**TAN-SSCD-01.ME-01**	
Projektazonosító	**E-HT11F1**	**Huntrust Kft. BALE 1. felülvizsgálat 2011**
MATRIX tanúsítási igazgató	**Szádeczky Tamás**	
Kelt	**Budapest, 2011. szeptember 7.**	
…….. MATRIX tanúsítási igazgató		

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

A HUNTRUST Informatikai Kutató, Fejlesztő, Tanácsadó és Szolgáltató Kft. (továbbiakban HUNTRUST) kifejlesztette az IDentity Applet JAVA Card Appletet, amelynek 2.20 verziója az NXP J2A040, J3A040 és J3A081 v2.4.1 R3 platformján, a JAVA kártyával együtt biztonságos aláírás létrehozó eszközként működik, amelynek felülvizsgálatára a HUNTRUST megbízta a MATRIX-ot.

A MATRIX áttanulmányozta az HUNTRUST által átadott fejlesztői dokumentumokat, elemezte a kötelezően betartandó és az önként vállalt normatíváknak való megfelelést. A fejlesztő által biztosított alkalmazás segítségével ellenőrizte a fejlesztő által átadott és teszt jegyzőkönyvben is rögzített tesztesetek eredményét és a fejlesztőktől független teszteket is végzett.

Az értékelés tárgya a TEST IAS ECC 1.36 tesztspecifikációban meghatározott tesztsorozaton esett át, amelyen bizonyítást nyert a megfelelése.

Az elvégzett vizsgálatokról részletes jelentések készültek, amelyekből a vizsgálat és a felhasználás körülményeire vonatkozó legfontosabb információkat jelen melléklet tartalmazza.

2 AZ ÉRTÉKELÉS TÁRGYA

Megnevezés: „Huntrust Kft. által kifejlesztett IDentity Applet ver 2.20 azonosítójú alkalmazásból és NXP J2A040, J3A041, J3A081 v2.4.1 R3 Secure Smart Card Controllerekből álló intelligens kártya"

2.1 Az értékelés tárgyát képező eszközök és dokumentációk

TÍPUS	TÁRGY	VERZIÓ	MEGJELENÉS
Hardver / Szoftver	NXP J3A040 and J2A040 Secure Smart Card Controller Revision 3 including ROM mask and EEPROM patch	Mask ID: 33h (51) Mask name: NX011C Patch ID: x1h ("x" változó) Target ID: 00h(SmartMX)	Chipkártya
Hardver / Szoftver	NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Revision 3 including ROM mask and EEPROM patch	Mask ID: 34h (52) Mask name: NX011D Patch ID: x1h ("x" változó) Target ID: 00h (SmartMX)	Chipkártya
Hardver	NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B	V0B	Chipkártya
Hardver	NXP P5Cx081V1A Secure Smart Card Controller	V1A	Chipkártya
Hardver	NXP P5CD041V1A Secure Smart Card Controller	V1A	Chipkártya
Szoftver	IDentity Applet	2.20	Elektronikus állomány
Dokumentum	IDentity Applet User's Guide	2.20.1	Elektronikus állomány (PDF)
Dokumentum	IDentity Applet Administrator's Guide	2.20.1	Elektronikus állomány (PDF)
Dokumentum	IDentity Applet Initialization and Configuration	2.20.1	Elektronikus állomány (PDF)
Dokumentum	IAS ECC – European card for e-Services and National e-ID applications	1.0.1	Elektronikus állomány (PDF)
Dokumentum	European card for e-Services and National e-ID applications TEST IAS ECC Identification Authentication Signature European Citizen Card Test Description	1.36	Elektronikus állomány (PDF)
Dokumentum	Certification Report BSI-DSZ-CC-0730-2011 for NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH	1.0	Elektronikus állomány (PDF)
Dokumentum	Certification Report BSI-DSZ-CC-0675-2011 for NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH	1.0	Elektronikus állomány (PDF)
Dokumentum	Certification Report BSI-DSZ-CC-0404-2007 for NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification	1.0	Elektronikus állomány (PDF)
Dokumentum	Certification Report BSI-DSZ-CC-0555-2009 for NXP Smart Card	1.0	Elektronikus állomány (PDF)

	Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A,P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification		
Dokumentum	Certification Report BSI-DSZ-CC-0710-2010 for Crypto Library V2.6 on P5CD040V0B /P5CC040V0B / P5CD020V0B / P5CC021V0B /P5CD012V0B from NXP Semiconductors Germany GmbH	1.0	Elektronikus állomány (PDF)
Dokumentum	Certification Report BSI-DSZ-CC-0633-2010 for Crypto Library V2.7 on P5CD081V1A /P5CC081V1A / P5CN081V1A / P5CD041V1A /P5CD021V1A / P5CD016V1A from NXP Semiconductors Germany GmbH	1.0	Elektronikus állomány (PDF)

Fejlesztő és a felülvizsgálat megrendelője:

HUNTRUST Informatikai Kutató, Fejlesztő, Tanácsadó és Szolgáltató Kft.
1117 Budapest, Infopark, Gábor Dénes utca 2. D. ép. 1. em.

3 FUNKCIONÁLIS LEÍRÁS

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 2.20 verziója az NXP J2A040, J3A041, J3A081 v2.4.1 R3 Secure Smart Card Controller-eken lett megvalósítva, ami egy NXP SmartMX Integrált áramkör JCOP 2.4.1 R3 Java Card Operációs rendszerrel. Az integrált áramkörök típustól függően csak kontaktusos vagy kontaktusos és érintésmentes csatoló felületeket is támogatnak.

A chipkártyás kontrollerek a BSI által kiállított EAL5+ CC tanúsítvánnyal rendelkeznek, a vonatkozó ST megfelel a PP/0303 Védelmi Profilnak.

Az ÉT applikáció egy biztonságos környezetben kerül telepítésre és megszemélyesítésre, és a kártyabirtokosok – a megszemélyesítéskori konfiguráció függvényében – ismert, megbízható (non-hostile environment), illetve nem megbízható környezetben (hostile environment) 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 2048 bites RSA és az SHA-256 algoritmusokat és a fejlesztő vizsgálatai alapján megfelel az európai állampolgári kártya (European Citizen Card – CEN/TS 15480-2), az ISO/IEC 7816-3/4/8/9 és az ISO/IEC 24727-2 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 alkotóelemekből épül fel.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

Az ÉT megfelel az alábbi követelményeknek:

- Kötelezően betartandó normatívák
  - 2001. évi XXXV. törvény az elektronikus aláírásról,
  - 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről;
  - Megfelelés az algoritmikus követelményeknek
    Nemzeti Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917/2008 határozata.
- Önként vállalt normatívák
  - MATRIX által vizsgált megfelelés
    - 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
    - Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,
  - Fejlesztő, vagy más szervezetek által igazolt megfelelés
    - ISO/IEC 7816-3/4/8/9
    - EN 14890-1/2
    - CEN/TS 15480-2
    - ISO/IEC 24727-2

- IAS-ECC 1.0.1
- PKCS#1

Az aláírási termék megfelel a fenti követelményeknek a 4.2 pontban leírt működési környezetben az alábbi feltételek teljesülése mellett:

- A tanúsítás kizárólag a bevizsgált rendszerre vonatkozik, bárminemű változtatás esetén a módosított verzióra jelen tanúsítás érvénytelen.

- Nem képezi a tanúsítás tárgyát a program működési környezete, így az
  - operációs rendszer,
  - a felhasznált külső szoftver modulok illetve programok,
  - a működéshez szükséges hardver elemek.

4.2 Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése, amelynek betartása a felhasználó felelőssége.

4.2.1 Megszemélyesítés és technikai környezet

Jelen tanúsítvány az NXP J2A040, J3A041, J3A081 v2.4.1 R3 Secure Smart Card Controllereken futó IDentity Applet ver 2.20 elektronikus aláírás alkalmazásból álló BALÉ-ra vonatkozik.

A hitelesítés szolgáltatónak (HSZ) a biztonságos megszemélyesítéshez szükséges valamennyi biztonsági intézkedést dokumentálnia kell a saját biztonsági előírásában foglaltak szerint.

A JCOP v2.4.1 és az IDentity Applet dokumentációiban leírt komplettírozási-, inicializálási- és megszemélyesítési folyamatoktól nem szabad eltérni. Ezen folyamatok garantálják a működési hibák kiküszöbölését és ezért a HSZ biztonsági koncepciójának részét kell képezniük.

Az ÉT-t használó egyéb alkalmazások nem képezik jelen hitelesítés tárgyát.

4.2.2 A termék használata

Működés közben a megfelelő termék használat érdekében az alábbi előírásoknak kell megfelelni:

A hitelesítés-szolgáltatóra vonatkozó általános előírások:

- A hitelesítés-szolgáltató köteles megismerni és betartani a vonatkozó dokumentációkban (IDentity Applet ver 2.20 és JCOP v2.4.1 kézikönyvei) foglalt szabályokat.

- A hitelesítés-szolgáltató köteles betartani a hatóság algoritmusokra és paramétereire vonatkozó hatályos határozatát.

- A hitelesítés-szolgáltatónak folyamatosan figyelnie kell az algoritmikus követelmények változásait, és szükség esetén fel kell készülnie a használat módjának megváltoztatására, vagy extrém esetben az eszközök tömeges cseréjére.

Amennyiben az ÉT-t minősített elektronikus aláírások létrehozására kívánják felhasználni, teljesíteni kell az alábbi követelményeket:

- 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.'

- 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.'

- A hitelesítés-szolgáltató köteles tartózkodni azon személy aláírás-létrehozó adatainak a tárolásától, illetve másolásától, akinek kulcskezelési szolgáltatásokat nyújtott;

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

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

- 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

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

A végfelhasználókra vonatkozó általános követelmények:

- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt úgy használja és tárolja, hogy a visszaélés és manipulálás megakadályozható legyen.

- Az aláíró kulcs birtokosa az aláírás létrehozó funkciót kizárólag olyan adatok vonatkozásában alkalmazhatja, amelyek integritását és hitelességét garantálja.

- Az aláíró kulcs birtokosa az aláírás létrehozó eszközre vonatkozó aktivizáló adatait (pl. PIN) bizalmasan kezelje.

- Az aláíró kulcs birtokosa rendszeres időközönként módosítsa az aláírás létrehozó eszközre vonatkozó aktivizáló adatait.

- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt kizárólag az elektronikus aláírásról szóló törvény előírásainak megfelelő aláírás alkalmazás komponenssel együtt alkalmazhatja.

- Ha a BALE konfiguráció különbséget tud tenni megbízható és nem megbízható aláírási környezet között, akkor a BALE felhasználó felelőssége a környezet megbízhatóságának megállapítása.

- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt kizárólag olyan aláírás alkalmazás komponenssel használhatja, amely a törvény előírásainak megfelelően képes a felhasználó által értelmezhető formában megjeleníteni az aláírandó dokumentumot.

- Az aláíró kulcs birtokosának be kell tartania a vonatkozó dokumentációkban (IDentity Applet ver 2.20 és JCOP v2.4.1 kézikönyvei) foglalt felhasználókra vonatkozó szabályokat.

A védelemre vonatkozó általános követelmények:

- Az aláírási termék használatát biztosító rendszer által tartalmazott hardver, szoftver és firmware elemeket megfelelően kell védeni az illetéktelen fizikai módosítások ellen.

- Az aláírási termék által használt kommunikációs csatornákat megfelelően védeni kell az illetéktelen fizikai módosítások ellen.

- Az aláírási termék által használt kommunikációs csatornákat megfelelő módon védeni kell az illetéktelen lehallgatás ellen. Lehallgatás alatt logikai (pl. kémprogramok) és fizikai (EMC) módszerekkel végzett adatgyűjtés értendő.

- A program telepítő készletét nem módosítható, biztonságos adathordozón kell a felhasználónak átadni.

- A telepítést csak a megfelelően előkészített, biztonságos környezetben szabad megkezdeni az átadott adathordozó segítségével, a telepítési útmutatóban rögzített lépések pontos betartásával.

- Az eredeti adathordozó felhasználásával rendszeresen ellenőrizni kell a számítógépre telepített program integritását.

4.3 Algoritmusok és kapcsolódó paraméterek

Az elvégzett vizsgálatok alapján összefoglalásként megállapítható, hogy a TOE által támogatott alábbi kriptográfiai algoritmuskészlet 2012 végéig jelenlegi ismereteink szerint megfelelően biztonságos marad:

- sha256 lenyomatképző függvény;

- emsa-pkcs1-v2.1 vagy iso9796-din-rn feltöltő algoritmus;

- RSA aláíró algoritmus 2048 bites kulccsal;

- rsagen1 kulcsgeneráló algoritmus;

- trueran véletlenszám generátor.

Bár az sha1 lenyomatképző függvény és a min. 1024 bites RSA kulcs használata jelenleg még nem tiltott, de a támadási módszerek fejlődésével fel kell készülni a gyengébb algoritmusok és paraméterek használatának megszüntetésére. A szolgáltatónak és a felhasználónak folyamatosan figyelnie kell a felhasználható kriptográfiai algoritmusokkal kapcsolatos határozatokat, és az elektronikus aláírás használata során a megfelelő algoritmusokat kell használniuk.

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

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 tömeges cseréjére.

4.4 Értékelési módszertan

Az értékelés nyelvezete a Közös Szempontrendszerben meghatározott, az értékelés módszertanának alapját a Közös Szempontrendszerhez használt módszertani ajánlás képzi. A tanúsítás teljes módszertani leírása a TTKK-45011-2 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv Az elektronikus aláírási termékek megfelelőségének tanúsítására című dokumentumban található.

A fejlesztő által a vizsgálatra átadott részletes dokumentumok elemzése és az elvégzett független működési tesztek eredményeit szakterületi audit jelentésekben foglaltuk össze, amelyek főbb megállapításait és az azokban megfogalmazott környezeti követelményeket tartalmazza az értékelési jelentés és a tanúsítvány melléklete (jelen dokumentum).

4.5 Biztonsági szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy a HUNTRUST által fejlesztett 2. pontban azonosított BALE megfelel a MATRIX által vizsgált normatív dokumentumokban foglalt követelményeknek a vizsgált környezetben.

A megfelelőségre vonatkozó megállapítást a témakör biztonságát érintő jelentős tudományos felfedezés, illetve új verzió kiadása esetén felül kell vizsgálni.

5 RÖVIDÍTÉSEK

Rövidítés	Tartalom
ALA	Aláírás Létrehozó Alkalmazás
BALE	Biztonságos Aláírás-Létrehozó Eszköz
CC	(Common Criteria) MSZ ISO/IEC 15408. Az informatikai biztonság értékelésének közös szempontrendszere
EASZ	Elektronikus Aláírási Szabályzat
TOE	Target of Evaluation – az ÉT eredeti, angol nyelvű megfelelője
ÉT	Értékelés Tárgya

Dokumentum vége