MINŐSÍTETT TERMÉK

Tanúsítvány

Tanúsítvány száma: E-IDNT15T_TAN-SSCD
Kelt: 2016. április 11.

Gyártó/Megbízó:ID&Trust Kft.
Címe: 1117 Budapest,
Gábor Dénes utca 2.,
Infopark D. ép.

A termék megnevezése:

Minősített elektronikus aláírás létrehozására alkalmas biztonságos aláírás létrehozó eszköz

A MATRIX Kft. tanúsítja, hogy*
a benyújtott dokumentációk és elvégzett vizsgálatok alapján az

ID&Ttrust Kft. által kifejlesztett
IDentity Applet Suite Version 3.2 azonosítójú alkalmazásból és
NXP J2E120_M65 / J3E120_M65 / J2E082_M65 / J3E082_M65
v2.4.2 R3 Secure Smart Card Controllerekből álló
intelligens kártya
megfelel

az alábbi normatív dokumentumokban foglalt követelményeknek:

- 2001. évi XXXV. törvény az elektronikus aláírásról;
- Nemzeti Média- és Hírközlési Hatóság E-Szolgáltatás-felügyeleti Osztály EF/26838-10/2011 határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően;
- az Európai Parlament és a Tanács 1999/93/EK Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről (hatályok kívül helyezve 2016. július 1-től);
- Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről;

Berki Csaba József
Tanúsítási igazgató

Einetter Lajos
Ügyvezető igazgató

Érvényes: 2019. április 10-ig
Melléklet: 8 oldal

*A MATRIX Kft. a IKF/23900-3/2015-NFM számú Kijelölési Okiratban a nemzeti fejlesztési miniszter által kijelölt tanúsító szervezet.

TANÚSÍTVÁNY (E-IDNT15T_TAN-SSCD) MELLÉKLETE

Dokumentumazonosító	**TAN-SSCD.ME-01**	
Projektazonosító	**E-IDNT15T**	**ID&Trust Kft. BALE tanúsítás 2015**
MATRIX tanúsítási igazgató	**Berki Csaba József**	
Kelt	**Budaörs, 2016. április 11.**	

.....

MATRIX tanúsítási igazgató

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

Az ID&Trust Kft. (továbbiakban IDANDTRUST) kifejlesztette az IDentity Applet Suite Java Card Appletet, amelynek 3.2 verziója az NXP J2E120_M65, J3E120_M65, J2E082_M65 és J3E082_M65 v2.4.2 R3 platformján, a Java kártyával együtt biztonságos aláírás létrehozó eszközként működik, amelynek felülvizsgálatára az IDANDTRUST megbízta a MATRIX-ot.

A MATRIX áttanulmányozta az IDANDTRUST 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.

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

2 AZ ÉRTÉKELÉS TÁRGYA

Megnevezés: „ID&Trust Kft. által kifejlesztett IDentity Applet Suite Version 3.2 azonosítójú alkalmazásból és NXP J2E120_M65, J3E120_M65, J2E082_M65 és J3E082_M65 v2.4.2 R3 Secure Smart Card Controllerekből álló intelligens kártya"

2.1 Az értékelés tárgyát képező eszközök és dokumentációk

TÍPUS	TÁRGY	VERZIÓ	MEGJELENÉS
Hardver / Szoftver	NXP J2E120_M65 és J3E120_M65 Secure Smart Card Controller Revision 3 including ROM mask and EEPROM patch	Mask ID: T0BCKRY6 Mask name: mask65 Patch ID: 3 Target ID: JCOP 2.4.2 R3	Chipkártya
Hardver / Szoftver	NXP J2E082_M65 és J3E082_M65 Secure Smart Card Controller Revision 3 including ROM mask and EEPROM patch	Mask ID: T0BGEAE6 Mask name: mask65 Patch ID: 3 Target ID: JCOP 2.4.2 R3	Chipkártya
Hardver	NXP Secure Smart Card Controller P5Cx128V0v, P5Cx145V0v	V0B	Chipkártya
Szoftver	IDentity Applet Suite	3.2	Elektronikus állomány
Dokumentum	IDentity Applet User's Guide	3.2.18	Elektronikus állomány (PDF)
Dokumentum	IDentity Applet Administrator's Guide	3.2.19	Elektronikus állomány (PDF)
Dokumentum	IDentity Applet Initialization and Configuration	3.2.03	Elektronikus állomány (PDF)
Dokumentum	File System IDentity SSCD	v3.2.02	Elektronikus állomány (PDF)
Dokumentum	NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65 and J2E082_M65 Secure Smart Card Controller Revision 3	NSCIB-CC-13-37760-CR	Elektronikus állomány (PDF)
Dokumentum	NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software	BSI-DSZ-CC-0858-2013	Elektronikus állomány (PDF)
Dokumentum	Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s)	BSI-DSZ-CC-0750-V2-2014	Elektronikus állomány (PDF)

Fejlesztő és a tanúsítás megrendelője:

Név: ID&Trust Kft.
Cím: 1117 Budapest, Gábor Dénes utca 2. / Infopark D. ép.

3 FUNKCIONÁLIS LEÍRÁS

Az Értékelés Tárgya egy chipkártyán megvalósított BALE, amely képes aláírás létrehozó adatok generálására, 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 Suite 3.2 verziója az NXP J3E120_M65, J2E120_M65, J3E082_M65 és J2E082_M65 v2.4.2 R3 Secure Smart Card Controller-eken lett megvalósítva, ami egy NXP SmartMX Integrált áramkör JCOP 2.4.2 R3 Java Card Operációs rendszerrel. Az integrált áramkörök típustól függően csak kontaktusos, csak érintésmentes, vagy kontaktusos és érintésmentes (duál interfészes) csatoló felületeket is támogatnak.

A chipkártyás kontrollerek a BSI által kiállított EAL5+ CC tanúsítvánnyal rendelkeznek, a vonatkozó ST megfelel a BSI-CC-PP0035-2007 Védelmi Profilnak.

Az ÉT életciklusa szempontjából az alábbi környezeti feltételeknek kell megfelelni:

- ÉT applikáció telepítése: az integrált áramkör gyártásakor, vagy biztonságos környezetben;
- ÉT konfigurálása: biztonságos környezetben;
- ÉT megszemélyesítése: biztonságos környezetben vagy biztonságos környezetből kiépített biztonságos csatornán keresztül;
- BALE működési fázis: a kártyabirtokosok az ÉT-t – a konfiguráció függvényében – ismert, megbízható (non-hostile environment), illetve nem megbízható környezetben (hostile environment) fogják használni.

Az ÉT alapját képező JCOP 2.4.2 R3 egy multi-applikációs platform, amely megfelelő jogosultságokkal rendelkező entitások számára lehetővé teszi további alkalmazások kártyára történő feltöltését a kártya kibocsátása során, vagy az után is.

Az ÉT egy multi-funkciós chipkártya platform elektronikus azonosítási feladatok ellátására, amely támogatja a 2048 bites RSA, 192-320 bites ECDSA 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.
  - Nemzeti Média és Hírközlési Hatóság E-Szolgáltatás-felügyeleti osztály EF/26838-x/2011 határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően;

- Önként vállalt normatívák
  - MATRIX által vizsgált megfelelés
    - Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről (hatályon kívül helyezve 2016. július 1-től);
    - Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről;
  - Fejlesztő, vagy más szervezetek által igazolt megfelelés
    - ISO/IEC 7816-4/8/9
    - ISO/IEC 14443
    - 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 J3E120_M65, J2E120_M65, J3E082_M65 és J2E082_M65 v2.4.2 R3 Secure Smart Card Controllereken futó IDentity Applet Suite Version 3.2 elektronikus aláírás alkalmazásból álló BALE-ra vonatkozik.

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

A JCOP v2.4.2 és az IDentity Applet Suite dokumentációiban leírt komplettírozási-, inicializálási- és megszemélyesítési folyamatoktól nem szabad eltérni. Ezen folyamatok garantálják a biztonságos működést 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 Suite Version 3.2 és JCOP v2.4.2 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 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 140-2, 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 Suite Version 3.2 és JCOP v2.4.2 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 algoritmuskészletek::

- SHA256 lenyomatképző függvény;
- PKCS#1 v1.5, PKCS#1 v2.0 PSS feltöltő algoritmus;
- RSA aláíró algoritmus 2048 bites kulccsal;
- rsagen1 kulcsgeneráló algoritmus;
- ECDSA aláíró algoritmus 192-320 bites kulccsal;
- ECC kulcsgeneráló algoritmus;
- trueran véletlenszám generátor.

A TOE felhasználójának folyamatosan figyelnie kell az algoritmikus követelmények változásait, és szükség esetén fel kell készülnie a használat módjának megváltoztatására, vagy extrém esetben az eszköz 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-17065 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv című dokumentumban található.

A fejlesztő által a vizsgálatra átadott részletes dokumentumok elemzése és értékelés eredményeit szakterületi 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 ID&Trust által fejlesztett 2. pontban azonosított BALE megfelel a MATRIX által értékelt 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

Rövidítés	Tartalom
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