Tanúsítvány száma
E-IDS18T_TAN-QSCD

Érvényesség kezdete
2019.04.11.

Érvényesség vége
2020.04.26.

Tanúsítvány

Termék megnevezése:

Minősített elektronikus aláírást létrehozó eszköz

ID&Trust Kft. által fejlesztett 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 inteligens kártya

A MATRIX Kft.* tanúsítja, hogy az

IdomSoft Zrt.

1134 Budapest, Tüzér utca 41.

által sponzorált és az

ID&Trust Kft.

1117 Budapest, Gábor Dénes utca 2. Infopark D épület

által benyújtott dokumentációk és az értékelés eredménye alapján
a fenti termék

megfelel

az alábbi

normatív dokumentumban foglalt követelményeknek:

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 és II. melléklete, valamint a vonatkozó a Bizottság (EU) 2016/650 (2016. április 25.) Végrehajtási határozat a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról.
A Végrehajtási határozatban felsorolt védelmi profilok közül a következő került alkalmazásra:
EN 419211-2:2013 Biztonságos aláírás-létrehozó eszköz védelmi profilja 2. rész: Kulcsgenerálós eszközök
A Védelmi Profil és a kapcsolódó Biztonsági előirányzat a következő normatíváknak felel meg:
ISO/IEC 15408 Informatika Biztonságtechnika Az informatikai biztonságértékelés szempontjai, 1-3. Rész az alábbiak szerint:
- ISO/IEC 15408-1:2009 Informatika Biztonságtechnika Az informatikai biztonságértékelés szempontjai, 1. rész. ISO, 2009
- ISO/IEC 15408-2:2008 Informatika Biztonságtechnika Az informatikai biztonságértékelés szempontjai, 2. rész. ISO, 2008
- ISO/IEC 15408-3:2008 Informatika Biztonságtechnika Az informatikai biztonságértékelés szempontjai, 3. rész. ISO, 2008

A vizsgálat módszertana a következő normatíváknak megfelelő:
ISO/IEC 18045:2008 Informatika Biztonságtechnika Az informatikai biztonságértékelés módszertana, és annak alkalmazott értelmezéséről a tanúsító által kialakított TTKK-17065 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv dokumentum

MATRIX
MINŐSÍTETT TERMÉK

A tanúsító szervezet nevében:

Einetter Lajos
ügyvezető igazgató
2019.04.05.

A Tanúsítvány a mellékletével együtt érvényes.
*A MATRIX Kft. (2040 Budaörs, Szabadság út 290.) a BM/1990-8/2018. iktatószámú Határozatban a belügyminiszter által kijelölt tanúsító szervezet.

TANÚSÍTVÁNY (E-IDS18T_TAN-QSCD) MELLÉKLETE

Dokumentumazonosító	**TAN-QSCD.ME-01**	
Projektazonosító	**E-IDS18T**	**IdomSoft Zrt. MALE tanúsítás 2018**
MATRIX tanúsítási igazgató	**Molnár Ádám**	
Kelt	**Budaörs, 2019. április 5.**	

.....

MATRIX tanúsítási igazgató

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

Az IdomSoft Zrt. (továbbiakban: IDOMSOFT) a következő termék – az ID&Trust által fejlesztett IDentity Applet Suite 3.2 verziójú alkalmazásból és az NXP J2E120_M65, J3E120_M65, J2E082_M65 és J3E082_M65 v2.4.2 R3 platformon alkalmazható, a Java kártyával együtt minősített elektronikus aláírást létrehozó eszközként működő – esetében a korábban kiadott E-IDNT15T_TAN-SSCD tanúsítvány lejáratát megelőzően annak újra tanúsításával bízta meg a MATRIX-ot.

A MATRIX felhasználta a korábbi tanúsítási anyagokat és áttanulmányozta az átadott fejlesztői dokumentumokat, elemezte a kötelezően betartandó normatíváknak való megfelelést a fejlesztő által átadott és teszt jegyzőkönyvben is rögzített tesztesetek eredményét.

Az elvégzett értékelésről részletes jelentések készültek, amelyekből az értékelés 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 Controllerből 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 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)
Dokumentum	ID&Trust Security Target for Secure signature creation device	V3.2.01.	Elektronikus állomány (PDF)

A tanúsítás megrendelője:

Név: IdomSoft Zrt.
Cím: 1134 Budapest, Tüzér utca 41.

A termék fejlesztője:

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

3 FUNKCIONÁLIS LEÍRÁS

Az Értékelés Tárgya egy chipkártyán megvalósított MALE, 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.

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;
- ÉT 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 az RSA, a 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 eIDAS 910/2014 EU rendelet II. melléklet *A minősített elektronikus aláírást létrehozó eszközökre vonatkozó követelmények*ben foglaltaknak.

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

- 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 (Továbbiakban: eIDAS);

- A Bizottság (EU) 2016/650 végrehajtási határozata (2016. április 25.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó eletronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és a 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról;

- ISO/IEC 18045:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés módszertana.

- Az ISO/IEC 18045:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés módszertanban nem meghatározott értelmezési kérdések kapcsán a TTKK-17065 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv dokumentum tartalmaz további információkat.

- ISO/IEC 15408 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 1–3. rész az alábbiak szerint:

- ISO/IEC 15408-1:2009 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 1. rész. ISO, 2009

- ISO/IEC 15408-2:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 2. rész. ISO, 2008

- ISO/IEC 15408-3:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 3. rész. ISO, 2008

- EN 419 211-2:2013 Biztonságos aláírás-létrehozó eszköz védelmi profilja 2. rész:Kulcsgeneráló eszközök

– 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,

– A 2.1 fejezetben hivatkozott ID&Trust Security Target for Secure signature creation device v3.2.01. dokumentumban foglalt működési környezetre (4.2 Security Objectives for Operational Enviroment) vonatkozó követelmények betartása mellett.

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 MALE-ra vonatkozik.

A bizalmi szolgáltatónak (BSZ) 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:

- IDentity Applet User's Guide 3.2.18,
- IDentity Applet Administrator's Guide 3.2.19,
- IDentity Applet Initialization and Configuration 3.2.03,

dokumentációiban leírt komplettírozási-, inicializálási- és megszemélyesítési folyamatoktól nem szabad eltérni. Ezen folyamatok garantálják a biztonságos működést és ezért a BSZ biztonsági koncepciójának részét kell képezniük.

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

4.2.2 A termék használata

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

A bizalmi szolgáltatóra vonatkozó általános előírások:

- A bizalmi szolgáltató köteles betartani a hatóság algoritmusokra és paramétereire vonatkozó hatályos határozatát.
- A bizalmi 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 bizalmi szolgáltató köteles az eIDAS 910/2014 EU rendelet II. mellékletében meghatározott feltételeknek megfelelni.

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 normatív dokumentumokban foglaltaknak:

- 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;

- A Bizottság (EU) 2016/650 végrehajtási határozata (2016. április 25.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó eletronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és a 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról;

- 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 eIDAS rendelet előírásainak megfelelő aláírás alkalmazás komponenssel együtt alkalmazhatja.

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

- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt kizárólag olyan aláírás alkalmazás komponenssel használhatja, amely az eIDAS rendelet II. mellékletének 2. pontjában foglalt 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 értékelés 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 módszertanának alapját az ISO/IEC 15408-hoz használt módszertan képzi. Az értékelés nyelvezete az ISO/IEC 15408-ban meghatározott. A tanúsítás teljes módszertani leírása a TTKK-17065 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv című dokumentumban található.

A fejlesztő által az értékelésre 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).

A fejlesztő által átadott részletes dokumentumok vizsgálatának módszertana a következő normatíváknak megfelelő:

ISO/IEC 18045:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés módszertana. A módszertanban nem meghatározott értelmezési kérdések kapcsán a TTKK-17065 azonosítójú Terméktanúsítási Minőségügyi Kézikönyv dokumentum tartalmaz további információkat.

A Védelmi Profil és a kapcsolódó Biztonsági előirányzat a következő normatíváknak felel meg:

ISO/IEC 15408 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 1–3. rész az alábbiak szerint:

- ISO/IEC 15408-1:2009 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 1. rész. ISO, 2009

- ISO/IEC 15408-2:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 2. rész. ISO, 2008

- ISO/IEC 15408-3:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 3. rész. ISO, 2008

4.5 Biztonsági szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy az ID&Trust által fejlesztett 2. pontban azonosított MALE 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
MALE	Minősített Elektronikus Aláírást Létrehozó Eszköz
TOE	Target of Evaluation – az ÉT eredeti, angol nyelvű megfelelője
ÉT	Értékelés Tárgya

Dokumentum vége