TANÚSÍTVÁNY (E-MS12T_TAN.BALE) MELLÉKLETE

Dokumentumazonosító	**TAN.BALE.ME-01**	
Projektazonosító	**E-MS12T**	**Microsec Kft. BALE tanúsítás 2012**
MATRIX tanúsítási igazgató	**Hornyák Gábor**	
Kelt	**Budapest, 2012. május 22.**	
…….. MATRIX tanúsítási igazgató		

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

A Microsec Kft. minősített elektronikus aláírás hitelesítés-szolgáltató. 2012. elején a Microsec megkeresésére szakmai egyeztetések kezdődtek a Gemalto által fejlesztett BALE tanúsítása tárgyában. A MATRIX a projekt során azt tekintette át, hogy szükséges-e a Francia Információs Rendszerek Nemzeti Biztonságának Nemzeti Ügynöksége által kiadott DCSSI-2009/07 Tanúsítvány kiadása óta eltelt idő technikai fejlődése kapcsán új vizsgálatokat elvégezni a MATRIX tanúsítvány kiadásához, illetve azt, hogy a Magyarországon hatályos jogi feltételrendszernek a termék megfelel-e.

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

2 AZ ÉRTÉKELÉS TÁRGYA

Megnevezés: Gemalto által gyártott és forgalmazott MultiApp ID Citizen 72K (Általános konfiguráció) IAS Classic v3.0 elektronikus aláírási programot támogató JC/GP MultiApp v1.1 platformmal maszkolt S3CC91C komponens, intelligens kártya

2.1 Az értékelés tárgyát képező eszközök és dokumentációk

TÍPUS	TÁRGY	VERZIÓ	MEGJELENÉS
Hardver / Szoftver	Gemalto által gyártott és forgalmazott MultiApp ID Citizen 72K (Általános konfiguráció) IAS Classic v3.0 elektronikus aláírási programot támogató JC/GP MultiApp v.1.1 platformmal maszkolt S3CC91C komponens,intelligens kártya.	Get Data paranccsal azonosíthatóan: Card Identity Data = B0 85 13 1D1 01 04 42 50 00 C8 00 00 00 00 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 00 00 00 00 ; Gemalto Family Name: Java Card: B0h ; Gemalto OS Name: MultiApp ID v1.1: 85h ; Gemalto Mask Number: MSA081: 13h ; Gemalto Product Name: IAS generic configuration: 1Dh ; Gemalto Flow version: 01h ; Gemalto filter set: Filter 01, version 4: 04h ; Chip Manufacturer: Samsung: 4250h ; Chip version: S3CC91C: 00C8h.	Chipkártya
Dokumentum	BSI-PP-0005-2002 hivatkozási számú ([PP0005) „Secure Signature-Creation Device Type 2”	1.04.	Elektronikus állomány (pdf)
Dokumentum	BSI-PP-0006-2002 hivatkozási számú (PP0006) „Secure Signature-Creation Device Type 3”.	1.05.	Elektronikus állomány (pdf)
Dokumentum	Gemalto Multiapp Platform Public Security Target	2009 Public	Elektronikus állomány (pdf)
Dokumentum	IAS Konfigurációs lista	1.1	Elektronikus állomány (pdf)
Dokumentum	Platform Adminisztrátori és Felhasználói kézikönyv	1.2	Elektronikus állomány (pdf)
Dokumentum	IAS Classic Adminisztrátori és felhasználói kézikönyv	1.1	Elektronikus állomány (pdf)
Dokumentum	MultiApp ID Combi és származtatott termékei Referencia Kézikönyv	1.0	Elektronikus állomány (pdf)
Dokumentum	IAS Classic Applet V3 Referencia Kézikönyv	1.0	Elektronikus állomány (pdf)
Dokumentum	MultiApp ID Citizen 72K eszköz francia tanúsítványa és melléklete	DCSSI-2009/07	Elektronikus állomány (pdf)
Dokumentum	MultiApp ID Citizen 72K Értékelési Jelentés Lite	1.0	Elektronikus állomány (pdf)

Fejlesztő és a felülvizsgálat megrendelője:

Fejlesztő:

Gemalto La vigie, Avenue du Jujubier Z.I. Athelia IV., 13705 La Ciotat, Franciaország	**Samsung** Electronics La Boursidière, RN186, Bat. Jura BP202, 92357 Le Plessis Robinson Franciaország

Megrendelő: Microsec Kft. 1022 Budapest, Marcibányi tér 9.

3 FUNKCIONÁLIS LEÍRÁS

Az Értékelés Tárgya a MultiApp ID Citizen 72K (MultiApp ID Citizen 72K), általános felhasználásra kialakított konfigurációja szerint. A termék hivatkozási száma „IAS Classic v3.0 / MultiApp v1.1 T1006974 on S3CC91C rev.0”. Ez a chipkártya 2. és 3. típusú biztonságos elektronikus aláírást létrehozó eszközként (SSCD) való felhasználásra készült.

A kártya egyik alkotóeleme egy 0. változatú S3CC91C biztonsági mikrokontroller. Ezt a TORNADO kriptográfiai társprocesszorral valamint egy TORNADO RSA 3,5S könyvtárral felszerelt, Samsung Electonics gyártmányú, 16 bites RISC mikrokontrollert a BSI 2007 szeptemberében tanúsította [Certif_IC] a BSI-DSZ-CC-0451-2007 számon. A kártya másik alkotóeleme, a Gemalto által a Java Card v2.2.1 és Global Platform c2.1 specifikációinak megfelelően kifejlesztett, 1.1. változatú Java MultiApp nyílt platform, mely tartalmaz egy operációs rendszert, az S3CC91C komponensbe van beágyazva. Ez a program több segédprogramot is tartalmaz, melyeket a Gemalto az alatta levő programtól függetlenül fejlesztett ki. Ezeket a segédprogramokat ROM-ba vagy EEPROM-ba telepítették. A ROMon tárolt 3.0 változatú IAS Classic segédprogram a termék legfontosabb segédprogramja, és elektronikus aláírási szolgáltatásokat biztosít.

A termék több egyéb beágyazott segédprogramot is tartalmaz. Csak az IAS Classic segédprogram kerül azonosításra. Ez után a termék különböző módokon konfigurálható, úgy, hogy egyéb segédprogramokat is azonosítanak rajta. A nem azonosított és nem is azonosítható segédprogramokat inaktívvá teszik.

Az értékelés nem terjedt ki az összes azonosítható segédprogramra, azonban a sebezhetőség vizsgálatakor ezek is figyelembe vételre kerültek. A jelen tanúsítványnak megfelelő konfigurációban az azonosítható segédprogramok kizárólag a ROM-on tárolt három segédprogram - MPCOS, OATH és Biomatch C API & Cryptomanager. A ROM-on tárolt egyéb segédprogramok inaktiválásra kerülnek, és az EEPROM-on nincs semmilyen más segédprogram.

Az ÉT applikáció egy biztonságos környezetben kerül telepítésre és megszemélyesítésre, és a kártyabirtokosok – a megszemélyesítéskori konfiguráció függvényében – ismert, megbízható, 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 multiapplikációs platform,

amely lehetővé tenné a megfelelő jogosultságokkal rendelkező entitások számára a kibocsátás után további alkalmazások feltöltését a kártyára.

A kártyán a minősített aláíró kulcsokon kívül más kulcsok is lehetnek. A kulcstároló helyek a következő

- minősített aláíró kulcs hely
- egyéb kulcs hely – ez használható fokozott biztonságú aláírásra, authentikációra, titkosításra is.

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

o 2001. évi XXXV. törvény az elektronikus aláírásról;

az eszköz megfelel a törvényben foglalt követelményeknek, és alkalmas a 6.§-ban foglalt alábbi szolgáltatások nyújtásához:

- elektronikus aláírás hitelesítés-szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás),

- időbélyegzés,

- aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése,

- elektronikus archiválás szolgáltatás.

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

o Megfelelés az algoritmikus követelményeknek
Nemzeti Média- és Hírközlési Hatóság E-Szolgáltatás-felügyeleti osztály EF/26838-x/2011határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően

– Önként vállalt normatívák

o Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről

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

- Fejlesztő vagy más szervezetek által igazolt megfelelőség:
  - ISO/IEC 15408 v.2.3 Az informatikai biztonságértékelés közös szempontjai
    - megfelelési szint: EAL4+ (ADV_IMP.2, ALC_DVS.2 , AVA_MSU.3, AVA_VLA.4)
  - BSI-PP0005-2002: SSCD, 2. típus, 1.04 változat
  - BSI-PP0006-2002: SSCD, 3. típus, 1,05 változat

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

- A tanúsítás kizárólag a tanúsítványon megjelölt rendszerre vonatkozik, bárminemű változtatás esetén a módosított verzióra jelen tanúsítás érvénytelen.
- Nem képezi a tanúsítás tárgyát a program működési környezete, így:
  - a felhasznált külső szoftver modulok illetve programok,
  - a működéshez szükséges egyéb 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

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

A referencia kézikönyvekben és az adminisztrátori valamint felhasználói útmutatókban foglaltatktól nem szabad eltérni a folyamat során.

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 referencia kézikönyvekben és az adminisztrátori valamint felhasználói útmutatókban foglaltaktól nem szabad eltérni a folyamat során.

- 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 aláíráslétrehozó eszközben történt elhelyezése után az aláírás létrehozó eszközön kívüli magánkulcsot biztonságos módon meg kell semmisíteni. A minősített aláírások létrehozatalára használt magánkulccsal csak minősített elektronikus aláírás hozható létre.

- 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;

A végfelhasználókra vonatkozó általános követelmények:

- Az aláíró felelőssége, hogy a kártyán lévő aláíró magánkulcsokat kizárólag aláírás készítésére használja.

- 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.

- A MATRIX javasolja, hogyaz aláíró kulcs birtokosa az aláírás létrehozó eszközt 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 aláírónak be kell tartania az átvett Felhasználói dokumentációban foglalt előírásokat.

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.

- Aláíráskor a PIN kódot biztonságos módon kell eljuttatni a kártyába. E követelmény teljesíthető például biztonságos (ún. Class 2) kártyaolvasó segítségével. Ha a felhasználó nem biztonságos kártyaolvasó segítségével hozza létre az aláírást, gondoskodnia kell a PIN kód védelméről. Például ne használja az eszközt általa nem ismert helyen.

- Az eszköz olyan módon is használható BALE-ként, minősített elektronikus aláírás készítésére, hogy az aláírandó dokumentumból a hash-t a PC számítja ki, és csak ezt a hash-t juttatja el a kártyának.

4.3 Algoritmusok és kapcsolódó paraméterek

Az alábbi kitételek csak a felhasználó által használni kívánt minősített aláíró kulcsokra vonatkoznak.

Az elvégzett vizsgálatok alapján összefoglalásként megállapítható, hogy a TOE által támogatott alábbi kriptográfiai algoritmuskészlet 2017 végéig jelenlegi ismereteink szerint megfelelően biztonságos marad:

Az eszköz által alkalmazott, az NMHH határozatának megfelelő algoritmusok a következők:

- Lenyomatképző algoritmus:
  - SHA–256 lenyomatképző algoritmus PKCS#1 v2.x feltöltő algoritmussal
- Aláíró algoritmus:
  - RSA (1024-2048) aláíró algoritmus
- választható feltöltő algoritmusok:
  - ISO 9796–2 feltöltő algoritmus
  - PKCS#1 v2.x feltöltő algoritmus
- Kulcs-előállítási algoritmus:
  - RSAGEN1
- Véletlenszám-generálási módszer:
  - trueran

A MATRIX a kiadott NMHH határozat alapján a 2048 bites kulcshosszt ajánlja használatra, az NMHH dokumentáció alapján az 1024 bites kulcshossz már nem ajánlott, az 1536 bites pedig csak 2012-ig garantálható biztonságú.

Az ÉT felhasználójának folyamatosan figyelnie kell az algoritmikus követelmények változásait, és szükség esetén fel kell készülnie a használat módjának megváltoztatására, vagy extrém esetben az eszközök 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 tanúsítási eljárás során elvégzett, fejlesztőktől független értékelő vizsgálat az MSZ ISO/IEC 15408 szabványban meghatározott EAL4 + szinthez hasonló tartalmú és mélységű volt, ami a lehető legnagyobb garanciát biztosítja a fejlesztő számára a tervezői fázisban alkalmazott pozitív biztonsági megközelítésből anélkül, hogy a már meglévő és alapos fejlesztői gyakorlatot lényegesen megváltoztatná.

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.

4.5 Biztonsági szint

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

A megfelelés biztonsági garancia szintje a Common Criteria értékelési rendszere szerinti **EAL 4**+ (ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4) szinttel ekvivalens, ami a fejlesztőktől függetlenül garantált biztonság kiemelt szintjét jelenti.

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