TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 15/2001.(VIII. 27.) MeHVM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 006/2002 számú kijelölési okiratával kijelölt terméktanúsító szervezet

tanúsítja,

hogy az

ORGA Kartensysteme GmbH, Germany
által előállított

SLE66CX320P mikrochip-ből és MICARDO v2.1 operációs rendszerből álló elektronikus aláírási termék

/ hardver verzió: SLE66CX320P/m1421b25,
szoftver verzió: v2.1 64/32 R1.0 /

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

a 2001. évi XXXV. törvényben szereplő
minősített elektronikus aláírások létrehozására alkalmazható

„3-as típusú biztonságos aláírás-létrehozó eszköz”-nek

Jelen tanúsítvány a HUNG-TJ-009-2003. számú értékelési jelentés alapján került kiadásra.
Készült a beültetést és forgalmazást végző Pénzjegynyomda Rt. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-009/2003.**
A tanúsítás kelte: 2003. július 10.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2006. július 10.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 9 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

Az SLE66CX320P mikrochip-ből és a MICARDO v2.1 operációs rendszerből álló (MICARDO) intelligens kártya egy bonyolult kriptográfiai eszköz, melyet fejlesztői úgy terveztek, hogy minél általánosabb feltételek között legyen használható, s a felhasználói igények minél szélesebb körét legyen képes kielégíteni. Ennek megfelelően számos biztonsági tulajdonság konfigurálható be, illetve ki rajta.

Amennyiben a MICARDO intelligens kártyát minősített aláírások létrehozására kívánják felhasználni, olyan biztonsági követelményeknek kell megfelelni, melyek a felhasználhatóságot korlátozzák, különböző feltételek betartását követelik meg.

Tovább bonyolítja a helyzetet, hogy a MICARDO intelligens kártya nem támogat kártyán tárolt végrehajtható kódokból álló alkalmazásokat, az alkalmazásokat kizárólag a host oldalról kiadott, szabványos (és az operációs rendszer által támogatott, értelmezett és a chip segítségével végrehajtott) parancsok megfelelő sorozatával lehet megvalósítani. Ez a filozófiai megközelítés bizonyos szempontból növeli a felhasználhatóság rugalmasságát, ugyanakkor számos biztonsági veszélyt is okoz, mivel
a host oldalról akár nem biztonságos konfigurálások is beállíthatók, elérhetők. Ezen veszélyek megnyugtató kivédése (legalább a felhasználói fázisra) további szigorításokat, extra feltételeket kíván meg.

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a MICARDO intelligens kártya BALE-ként való felhasználásának.

I. Általános érvényességi feltételek

Az alábbi feltételek minden felhasználási mód esetén (tehát a fejlesztő-gyártó cég által igen általánosra tervezett felhasználási kör egészében) szükségesek a megbízható és biztonságos működéshez.

1. A MICARDO intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók (aláírók) jól képzettek és megbízhatóak.

2. A MICARDO intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók betartják a különböző útmutatók **(**döntően a MICARDO Public Chip Card Operating System v2.1 User Manual**)** által előírt, alábbi kötelező tevékenységeket:
   - a tulajdonosok titokban tartják saját PIN kódjukat,
   - az aláírók PIN kód hosszúsága legalább 6 digit legyen,
   - a PIN kódokat nem szabad megjeleníteni a terminálon adatbevitel közben,

3. A külvilág és az intelligens kártya közötti bizalmas adatcsere esetén titkos üzenetváltást kell megvalósítani (a parancsra és válaszára megvalósított MAC képzéssel és kódolással).
4. A külvilágban tárolt (hitelesítéshez vagy titkosításhoz használt) kulcsok titkosságáért a felhasználók felelősek. Számukra a következők erősen ajánlottak:
   - a kulcsokat tartalmazó adatterületeket védeni kell az illetéktelen kiolvasás és módosítás ellen,
   - a kulcsokat kompromittálódásuk esetén azonnal cserélni vagy blokkolni kell ,
   - kulcsok továbbítása az intelligens kártyára mindig titkos üzenettel történjen.

II. Az ITSEC tanúsításokból fakadó érvényességi feltételek

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a MICARDO v2.1 intelligens kártya megfeleljen az ITSEC E4-es biztonsági szintjének.

5. A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi algoritmusra kell korlátozni: **RSA (1024 bites kulcsméret, PKCS #1-es aláírás formátum, SHA-1 lenyomatképzés)**[1].

6. A MICARDO és a külvilág közötti titkos üzenetváltáshoz a **Triple DES** algoritmust alkalmazzák **(**a MICARDO által támogatott 112 bites kulcsméretben).

III. A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei

Egy minősített aláírásokat létrehozó aláírónak a MICARDO felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

7. A BALE-ként használt MICARDO intelligens kártyának csak egy felhasználója lehet, az aláíró[2].

8. A minősített aláírások létrehozására használt magánkulcsot érvényességének lejárta után az első lehetséges alkalommal törölni kell[3].

9. A minősített aláírások létrehozására használt magánkulcs hozzáférési szabályait úgy kell beállítani a perszonalizálás folyamatában, hogy a későbbiekben azzal a felhasználó (aláíró) csak aláírni tudjon. (Ne lehessen titkosításra /pontosabban dekódolásra/ vagy hitelesítésre felhasználni.)

10. A minősített aláírások létrehozására használt magánkulcsot ne lehessen menteni.

---

[1] Mert az ITSEC értékelés csak erre az algoritmusra vonatkozott, bár a chip támogatja a DSA aláíró algoritmust is.

[2] A MICARDO v2.1 képes több (vég)felhasználót is kezelni egy kártyán.

[3] Amennyiben új tanúsítvány kérelme vagy más célból az aláíró eszközével megjelenik a hitelesítés-szolgáltatónál, az adminisztrátor felelőssége (mert csak neki van jogosultsága rá) a kártyán lévő, már érvénytelen magánkulcsok fizikai megsemmisítése (törlése).

11. A minősített aláírások létrehozására használt magánkulccsal csak minősített aláírást szabad létrehozni. (Így nem szabad fokozott biztonságú aláírás-létrehozására felhasználni.)

12 Bizalmasságot, hitelességet és sértetlenséget biztosító titkos üzenetváltást kell biztosítani (a Triple DES algoritmus felhasználásával) a következő esetekben:
- az aláírandó adatreprezentáns intelligens kártyára küldésekor (aláírás céljából),
- a nyilvános kulcs intelligens kártyáról való fogadásakor (tanúsítványba foglalás céljából).
- kezdeti felhasználói hitelesítéskor (a PIN kód vagy a jelszó megadásához),
- a hitelesítési adatok (PIN kód vagy jelszó) cseréjéhez.

13 A biztonsági attribútumok inicializálásakor biztosítani kell az alábbiakat:
- A retry counter alapértéke 3 legyen.
- A retry counter reset-elési funkciójához csak az adminisztrátornak legyen joga.

14. Egy BALE-ként használt MICARDO esetén az adminisztrátor és felhasználó (aláíró) szerepkörök szétválasztásával, valamint az inicializálási, perszonalizálási folyamatoknál alkalmazott programok és rezsim szabályok együttműködésével biztosítani kell a következőket:
1. az „aláíró” vagy az „adminisztrátor” generálja az aláírói kulcspárt, ennek felhasználását pedig az „adminisztrátor” engedélyezze,
2. a folyamat során az „adminisztrátor” végrehajt egy páronkénti megfelelőség tesztet (az aláíráshoz generált nyílt – magánkulcs pár összetartozásának ellenőrzését), és csak sikeres eredmény esetén adható ki tanúsítvány, illetve maga a BALE,
3. az „aláíró” vagy az „adminisztrátor” exportálja a legenerált nyilvános kulcsot tanúsítvány készítés céljából,
4. csak az „aláíró” aktivizálhatja magánkulcsát (aláírásra),
5. a sikeres folyamat végén a felhasználónak (aláírónak) átadott intelligens kártyára teljesül, hogy minden biztonsági attribútum biztonságos értéket vesz fel, s így hagyja el a hitelesítés-szolgáltató védett környezetét (a felhasználói környezetben ez a későbbiekben már nem változtatható meg)
/Azon elvárás, hogy minden biztonsági attribútum biztonságos értéket vesz fel, magában foglalja az alábbi követelményeket is:
   - a PIN kódokat megfelelő hozzáférési szabályokkal védve, biztonságosan tárolják az intelligens kártyán,
   - valamennyi digitális aláírással kapcsolatos parancs végrehajtása csak sikeres jelszó alapú felhasználói azonosítás és hitelesítés után legyen lehetséges (a megfelelő fájlok „sikeres jelszó alapú felhasználói hitelesítés után” hozzáférési feltétel beállításával)./
6. technikai vagy rezsim intézkedésekkel biztosítani kell, hogy egy már kulcsokkal ellátott, de még nem az aláíró személyes felügyelete alá tartozó intelligens kártyával harmadik személy ne élhessen vissza jogosulatlanul.

15. A hitelesítés-szolgáltató által működtetett, inicializálást, perszonalizálást végző, esetenként nem biztonságos attribútum beállításokat is működtető alkalmazásra egy a fejlesztőktől független, elektronikus aláírás termékek biztonsági értékelésére/tanúsítására felhatalmazott szervezet értékelési eredménye állapítsa meg, hogy az alkalmazás kielégíti a 7. - 10., valamint a 12. - 14. feltételeket.[4]

16. Az aláíró csak megbízható aláírás-létrehozó alkalmazást használhat.

17. A Tanúsítvány csak a jelenlegi verzióra érvényes
/chip: SLE66CX320P / m1421b25, operációs rendszer: v 2.1 64/32 R1.0/

    Új chip verzió esetén mind a chip-re, mind az operációs rendszerre új tanúsítás szükséges.
    Amennyiben csak az operációs rendszer változik, elég egy olyan új, az operációs rendszerre vonatkozó tanúsítás, mely a régi chip verziót megnevezi.
    Mindkét fenti esetben szükséges az új verzió BALE-ként való felhasználhatóságát egy erre kijelölt hazai tanúsító szervezettel ismételten tanúsíttatni.

[4] A 15. feltétel indoklása:
A MICARDO intelligens kártya nem támogat kártyán tárolt végrehajtható kódokból álló alkalmazásokat, az alkalmazásokat kizárólag a host oldalról kiadott, szabványos (és az operációs rendszer által támogatott, értelmezett és a chip segítségével végrehajtott) parancsok megfelelő sorozatával lehet megvalósítani.
Ez a filozófiai megközelítés bizonyos szempontból növeli a felhasználhatóság rugalmasságát, ugyanakkor számos biztonsági veszélyt is okoz, mivel a host oldalról akár nem biztonságos konfigurálások is beállíthatók, elérhetők. Még az elektronikus aláírásról szóló 2001. évi XXXV. törvény 1. sz. mellékletében a biztonságos aláírás-létrehozó eszközre vonatkozó igen általános követelmények is sérülhetnek, nemcsak az SSCD védelmi profil elvárásai:

- az aláírás készítéséhez használt aláírás-létrehozó adat titkossága is sérülhet
- az aláírás-létrehozó adat jogosulatlan felhasználókkal szembeni védelme sem biztosított.

/Például egy kulcs pár generálására a felhasználói kézikönyv az alábbi, egymást követő lépéseket javasolja:

1. új könyvtár létrehozása az adatfájlok számára (dedikált fájlok, valamint megfelelő strukturális információkkal feltöltött elemi fájlok),
2. az új adatmezők feltöltése,
3. a hozzáférési jogok módosítása (ezt követően a magánkulcs információkhoz nem lehetséges a hozzáférés),
4. kulcs generálása,
5. a nyilvános kulcs kiolvasása

A felhasználói útmutató is felhívja a figyelmet arra, hogy amennyiben a fenti 3. lépés kimarad, a magánkulcs módosítható vagy olvasható marad!/
A fenti (igen súlyos) veszélyek megnyugtató kivédése indokolja a szolgáltató által használt alkalmazásra vonatkozó szigorító feltételt.

2. számú melléklet

TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK

A követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

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

CEN/ISSS ESign Workshop – Expert Group F: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+

ITSEC: Information Technology Security Evaluation Criteria, version 1.2 (1991)

ITSEM: Information Technology Security Evaluation Manual, version 1.0 (1993)

3. számú melléklet

A tanúsításhoz figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

Kérdőív a tanúsítás kérelmezéséhez

BSI-DSZ-ITSEC-0175-2002 Certification
/Smart Card IC SLE66CX320P / m1421b25/

BSI-DSZ-ITSEC-0175-2002 Certification Report
/Smart Card IC SLE66CX320P / m1421b25/

TUVIT-DSZ-ITSEC-9126-2001 Certification
/MICARDO Public Version 2.1 64/32 R1.0/

TUVIT-DSZ-ITSEC-9126-2001 Certification Report
/Smart Card Operating System MICARDO Public Version 2.1 64/32 R1.0/

ORGA: MICARDO Public Chip Card Operating System v2.1 User Manual