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 a
SchumbergerSema és Infineon Technologies AG
által kifejlesztett és a
SchumbergerSema
által forgalmazott

JavaCard 32K CRISTAL intelligens kártya

/mikrochip: SLE66CX322P (GC A23 verzió), operációs rendszer: GEOS (SC_V3.0.0 verzió), aláírás-létrehozó alkalmazás: CRISTAL (AC_V1.0.0 verzió)/
aláírás-létrehozó eszköz

az 1. számú mellékletben áttekintett biztonsági tulajdonságokkal és funkcionalitással, valamint

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételeinek figyelembe vételével

megfelel

a 2001. évi XXXV. törvényben szereplő
minősített elektronikus aláírások létrehozására alkalmazható
„3-as típusú biztonságos aláírás-létrehozó eszköz”-ként

Jelen tanúsítvány a HUNG-TJ-005-2003. számú tanúsítási jelentés alapján került kiadásra.
Készült a RITA Részvénytársaság megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-005/2003.**
A tanúsítás kelte: 2003. február 17.
A tanúsítvány érvényességi ideje: 2006. február 17.
Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen: 7 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A JAVACARD 32K CRISTAL legfontosabb biztonsági tulajdonságainak összefoglalása

A SchlumbergerSema Cyberflex nevű intelligens kártyája egy multiapplikációs Java Card. Megfelel mind a Java Card, mind a (Visa) Open Platform specifikációjának. A kártyán megvalósított virtuális gép különböző operációs rendszereket, s ezeken futó különböző alkalmazásokat támogat.

A JavaCard 32K CRISTAL intelligens kártya ennek a Cyberflex JavaCard-nak egy olyan speciális megvalósítása, mely az alábbi három fő komponensből áll:

- mikrochip (az Infineon SLE66CX322P típusú chip-je, mely valamennyi Cyberflex alapját képezi),
- operációs rendszer (a GEOS általános operációs rendszer, mely egyike a Cyberflex intelligens kártyákba ágyazható operációs rendszereknek),
- aláírás-létrehozó alkalmazás (a CRISTAL nevű alkalmazás, mely egy a Cyberflex intelligens kártyára tölthető, azon futtatható alkalmazás).

Jelen tanúsítás a Cyberflex ezen speciális megvalósítására vonatkozik.

Funkcionalitás szempontjából három különböző biztonságos aláírás-létrehozó eszköz (BALE) típus lett definiálva:

- 1-es típus: csak az aláírás-létrehozó / aláírás-ellenőrző adatpárok generálását támogatja, de nem állít elő elektronikus aláírást az általa előállított aláírás-létrehozó adattal,
- 2-es típus: biztosítja az elektronikus aláírás előállítását egy olyan aláírás-létrehozó adat felhasználásával, amelyet egy 1-es típusú BALE-től importál,
- 3-as típus: biztosítja mind az aláírás-létrehozó / aláírás-ellenőrző adatpárok generálását, mind az elektronikus aláírás előállítását az aláírás-létrehozó adattal

A JavaCard 32K CRISTAL intelligens kártya 2-es és 3-as típusú BALE-ként egyaránt működtethető. A két típus a megszemélyesítési- kulcsgenerálási folyamatok, valamint a tanúsítás érvényességi feltételei szempontjából jelentősen különböznek egymástól. Jelen tanúsítás a JavaCard 32K CRISTAL intelligens kártya 3-as típusú BALE-ként való alkalmazhatóságára vonatkozik.

A JavaCard 32K CRISTAL intelligens kártya alábbi biztonsági tulajdonságait érintette az értékelés, majd az ezt követő (francia séma alapján végzett) tanúsítás:

- **az intelligens kártya öntesztelése**
  /Minden munkaszakasz kezdetén a biztonsági funkciók tesztelik a RAM-ot az IC-t és ezek környezetét. Kérésre a biztonsági funkciók tesztelik az EEPROM-ot és a véletlen generátort is./

- **biztonsági események detektálása**
  /Az intelligens kártya jelzi az alábbiakra vonatkozó hibákat: üzenet formátum, adat sértetlenség, környezeti feltételek elfogadható tartományból való kitérése, életciklus állapottal való összeférhetetlenség./
- **memória munkaterületek maradvány információ védelme**
  /Az intelligens kártya törli munka memória területeit minden munkaszakasz kezdetén, illetve minden érzékeny adatra vonatkozó erőforrás kiosztás (allokáció) és erőforrás visszavétel (deallokáció) előtt./
- **tárolt adatok sértetlenségének ellenőrzése**
  / Az intelligens kártya ellenőrzi a kriptográfiai kulcsok, hitelesítő adatok és az aláírandó adat reprezentáns sértetlenségét. Integritási hiba észlelése esetén hibajelzést ad, az érintett adatot elérhetetlenné teszi, s a folyamatban lévő műveletet megszakítja./
- **a műveletek és adatok megfigyelhetetlensége**
  /Az intelligens kártya elrejti a külső megfigyelés elől az érzékeny adatokat továbbításuk és feldolgozásuk során./
- **az intelligens kártya menedzselése**
  /Az intelligens kártya belső folyamatainak végrehajtása a kártya felhasználója által küldött megfelelő kezelő utasítások által irányítható. A kezelő utasítások üzenetei megfelelnek az ISO 7816 szabványban előírtaknak. Az intelligens kártya ellenőrzi mind az utasítás formátumát, mind az utasítás kód és megadott paramétereinek konzisztenciáját. Ellenőrzésre kerül, az utasítások sorrendjének helyessége, illetve az adott életciklusban történő végrehajthatósága. Csak az ellenőrzésen sikeresen átesett utasítások hajtódnak végre./
- **kulcsok generálása**
  /Az intelligens kártya 1024 bites RSA aláíró kulcspárt generál. (A kulcspár nyilvános összetevőjét szükség esetén képes előállítani a magánkulcs és a modulus alapján). Az intelligens kártya 112 bites triple DES munkaszakasz kulcsokat generál a VOP szabványnak megfelelő módon (a megbízható csatorna kiépítéséhez). /
- **aláírás létrehozása**
  /Az intelligens kártya a kívülről kapott, vagy a kártyán tárolt adat lenyomatot (hash értéket) a PKCS #1 szabványnak megfelelően aláírja, 1024 bites RSA magánkulcsot használva. Az aláírás funkciót csak az előzetesen sikeresen hitelesített felhasználó aktivizálhatja./
- **adatok lenyomatolása**
  /Az intelligens kártya a kívülről kapott, vagy a kártyán lévő adatokra lenyomatot (hash értéket) készít SHA-1 algoritmust használva. A kártya arra is képes, hogy befejezze a lenyomatolási folyamatot egy közbülső hash értékből kiindulva, az ehhez utólag fogadott adatokkal./
- **MAC kontrollösszeg képzése és ellenőrzése**
  /Az intelligens kártya MAC kontrollösszeget képez, illetve ellenőriz, 112 bites triple DES kulcs felhasználásával./

- **megbízható csatorna kiépítése a külvilággal**
  /Az intelligens kártya képes megbízható csatornát kiépíteni. A külső fél hitelességét egy olyan kölcsönös hitelesítési eljárással ellenőrzi, mely MAC-on alapuló kriptográfiai értéket használ. Egy belső számláló (3-ra) korlátozza a hitelesítési kísérleteket. Ez a funkció titkosítja és dekódolja a megbízható csatornán átküldött üzeneteket, illetve dekódolja a kívülről (a munkaszakasz kulcsok kialakításához) kapott kulcsokat 112 bites triple DES kulcsokat használva./
- **PIN kódok kezelése**
  /Az intelligens kártya ellenőrzi a PIN kód kezelésével kapcsolatos valamennyi műveletet, köztük az aláíró hitelesítését, a PIN előállítását, ellenőrzését és módosítását./
- **hozzáférés ellenőrzés**
  /Az intelligens kártya hozzáférés ellenőrzés funkciója ellenőrzi, hogy teljesülnek-e a hozzáférés feltételei a következő műveleteknél: az adminisztrátor általi magánkulcs generálás és PIN kód létrehozás, illetve az aláíró általi PIN kód csere, nyilvános kulcs export és aláírás./
- **életciklus kontroll**
  /Az intelligens kártya garantálja saját életciklusának megfelelő menedzselését. Folyamatosan ellenőrzi életciklus állapota sértetlenségét, megállapítja az aktuális fázist és állapotot, illetve szükség esetén a következő állapotra vagy fázisra módosít. A fázisok módosítása visszafordíthatatlan folyamat./
- **biztonsági jellemzők meghatározhatósága**
  /Az intelligens kártya az alábbi biztonsági jellemzők kezelését teszi lehetővé:

Jellemző (attribútum)	érték
Szerep	adminisztrátor / aláíró
Magán-nyilvános kulcspár kezelés	felhatalmazott / nem felhatalmazott
Nyilvános kulcs biztonságos importálásának engedélyezettsége	igen / nem
Magánkulcs működtetése (aláírás)	igen / nem
Aláírandó adat küldése egy felhatalmazott aláírás-létrehozó alkalmazástól	igen / nem

  /
- **a mikrochip biztonsági tulajdonságainak menedzselése**
  /Az intelligens kártya biztosítja mikrochip-je biztonsági tulajdonságainak menedzselését. Ez magában foglalja a chip állapotának vizsgálatát, biztonsági események generálását és tárolását, a chip védőburkának sérülése esetén a sérülés komolyságától függő intézkedések foganatosítását, a véletlen időgenerálás kontrollálását./
- **biztonságos állapotba való visszatérés**
  /Az intelligens kártya garantálja, hogy a megelőző biztonságos állapotába kerüljön vissza, ha az alábbiak valamelyike bekövetkezik: korlátnál alacsonyabb áramerősség, korlátnál magasabb feszültség, órafrekvencia kiesése a megengedett (alsó és felső korlátok közötti) tartományból, integritás hiba./

2. számú melléklet

A biztonságos felhasználás feltételei

A JavaCard 32K CRISTAL intelligens kártya adott alkalmazását úgy fejlesztették, hogy (a sokkal általánosabb kriptográfiai funkcionalitást is támogató mikrochip-je, illetve több felhasználói alkalmazás futtatására alkalmas platformja) pontosan megfeleljen a viszonyítási alapként tekintett védelmi profil követelményeinek.
Ez jelentősen leegyszerűsíti a feltételek meghatározását. Nem szükséges például külön elemezni és áttekinteni a mikrochip tanúsítványának érvényességi feltételeit, hiszen azt a későbbi értékelő/tanúsító szervezetek figyelembe vették (teljesítettnek nyilvánították, vagy saját feltételeik közé is beépítették).

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a tanúsítvány érvényességének.

I. A tanúsítás viszonyítási alapját képező védelmi profilból adódó érvényességi feltételek

1. Az adminisztrátor kövesse az adminisztrátori útmutatót

Az adminisztrátornak be kell tartania a JavaCard 32K CRISTAL intelligens kártya inicializálásához, megszemélyesítéséhez és adminisztrálásához biztosított adminisztrátori útmutató[1] valamennyi előírását[2].

2. Megbízható tanúsítvány-létrehozó alkalmazást kell használni

Csak minősített hitelesítés-szolgáltató által működtetett tanúsítvány-létrehozó alkalmazást szabad használni a nyilvános kulcs tanúsítványba foglalásához. Az ilyen tanúsítvány kellő biztonsággal megvédi a minősített tanúsítványban szereplő felhasználói név és aláírás-ellenőrző adat hitelességét a minősített hitelesítés-szolgáltató aláírásával.

3. Az aláíró kövesse a felhasználói útmutató előírásait

Az aláírónak követnie kell a JavaCard 32K CRISTAL intelligens kártya által biztosított felhasználói útmutató[3] valamennyi előírását[4].
/Különösen fontos az alábbiak betartása:
A felhasználónak (aláírónak) titokban kell tartania saját PIN kódját./

4. Megbízható aláírás-létrehozó alkalmazást használjanak

Az aláíró csak megbízható aláírás-létrehozó alkalmazást használhat.
Az aláírás-létrehozó alkalmazás állítja elő és küldi át az aláíró által alá írni kívánt adatokat (vagy annak reprezentánsát, részlegesen vagy teljesen lenyomatolt képét) a JavaCard 32K CRISTAL intelligens kártyára, az aláíráshoz megfelelő formában.

---

[1] Administration manual: RUBIS (MRD06GI003072 v.1.3)
[2] Az alábbiakban azért nem részletezzük ezen előírásokat, mert egy nem nyilvános dokumentum tartalmazza azokat /Administration manual: RUBIS/
[3] User manual: RUBIS (MRD06GI003073 v.1.1)
[4] Az alábbiakban azért nem részletezzük ezen előírásokat, mert egy nem nyilvános dokumentum tartalmazza azokat /User manual: RUBIS/

II. A hazai jogszabályokból adódó érvényességi feltételek

Nincsenek járulékos követelmények.
Ennek egyik oka, hogy a JavaCard 32K CRISTAL intelligens kártya minden kategóriában támogat egy a 2/2002. (IV. 26.) MeHVM irányelv l. számú mellékletében felsorolt „elfogadott kriptográfiai algoritmust”:

- aláíró algoritmus: **RSA (1024 bites kulcsmérettel)**
- kulcs létrehozási algoritmus: **valódi véletlen**
- feltöltő módszer: **PKCS #1 (emsa-pkcs-v1_5)**
- lenyomat- (hash) függvény: **SHA-1**

A másik ok az, hogy a JavaCard 32K CRISTAL intelligens kártya (pontosabban annak CRISTAL alkalmazása) csak a fenti elfogadott kriptográfiai algoritmusok meghívását teszi lehetővé, nincs szükség tehát a kiválasztható sokféle algoritmus közül megtiltani néhány nem elfogadott algoritmussal való felhívását.

III. Egyéb érvényességi feltételek

5. A megbízható csatorna kialakításában közreműködő kulcsokat a host oldalon is védeni kell

Az intelligens kártya és a host oldal közötti kölcsönös hitelesítés egy közös titok ismeretén alapul. Ezt a titkot (statikus kulcsot) a host oldalon is kellő biztonsággal meg kell védeni az illetéktelen felfedés ellen.

6. Megfelelő hosszú PIN kódot használjanak

A JavaCard 32K CRISTAL intelligens kártya **legfeljebb 8 hosszú PIN kód**ot támogat, megadott értékét bájtos alakban kezeli. 3 egymást követő sikertelen hitelesítési kísérlet (téves PIN kód megadás) után a kártya alkalmazás blokkolja valamennyi felhasználói funkcióját. Ahhoz, hogy magas fokú védelem legyen biztosítva **minimálisan 4 jegyű, véletlenszerű PIN kódot kell használni**. A szakirodalom szerint erősen ajánlott a véletlen próbálgatáson alapuló illetéktelen hitelesítési kísérletek sikere ellen annak valószínűségét az 1/1000000-od valószínűség közelébe leszorítani, mely a PIN kód jelkészletétől függő módon az alábbi alsó hosszúság korlátot jelenti a PIN kódra: számjegyek alkalmazása esetén: 6; hexadecimális karakterek alkalmazása esetén: 5; általános klaviatúra használata esetén (kis és nagy betűk, számjegyek): 4 karakter.

7. Pontosan a tanúsított verziót használják

A tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes[5] /mikrochip: SLE66CX322P (GC A23 verzió), operációs rendszer: GEOS (SC_V3.0.0 verzió), aláírás-létrehozó alkalmazás: CRISTAL (AC_V1.0.0 verzió)/.

[5] A tanúsítás érvényes marad, ha a CRISTAL alkalmazás mellé egy másik alkalmazást töltenek az intelligens kártyára.

3. 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+

Smartcard IC Platform Protection Profile (BSI-PP-0002)

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

a) A tanúsításhoz figyelembe vett egyéb dokumentumok

- Kérelem /a tanúsítás elvégzésére/
- Kérdőív a tanúsítás kérelmezéséhez
- Certification Report BSI-PP-0006-2002: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+
- SSI: Rapport de certification 2002/07: JavaCard 32K CRISTAL (référence M256LCAC2)
- SchlumbergerSema: JavaCard 32K, Common Criteria/ISO 15408 Security Target (Public version, EAL4+)
- BSI: Certification Report BSI-DSZ-CC-0169-2002: Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 6 m148a23
- Infineon Technologies AG: SLE66CX322P with RSA2048 / m1484 Security Target (version 1.0.5)
- Administration manual: RUBIS (MRD06GI003072 v.1.3)
- User manual: RUBIS (MRD06GI003073 v.1.1)

b) A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

A tanúsításhoz figyelembe vett, a JavaCard 32K CRISTAL intelligens kártya egészére vonatkozó, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 14508 /Common Criteria/ emelt szintű **EAL 4-es** /módszeresen tervezett, vizsgált és átnézett rendszer/ volt.

Az emelt szintet az EAL 4 garancia szint által nem megkövetelt alábbi garanciösszetevők kiegészítő megkövetelése és teljesítése jelentette:

- ADV_IMP.2 Az értékelés tárgya biztonsági funkcióinak kivitelezése /csak EAL5-től megkövetelt/
- ALC_DVS.2 A biztonsági intézkedések elégségessége /csak EAL6-tól megkövetelt /
- AVA_VLA.4 Keményen ellentálló /csak EAL6-tól megkövetelt /

c) A JavaCard 32K CRISTAL intelligens kártya biztonsági funkcióinak értékelt erőssége

A biztonsági funkciók erőssége: **magasszintű.**