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

Giesecke & Devrient GmbH, Germany
által előállított és forgalmazott

P8WE5032v0G mikrochip-ből, STARCOS SPK 2.3 v 7.0 operációs rendszerből és StarCert v 2.2 digitális aláírás alkalmazásból álló intelligens kártya

elektronikus aláírási termék

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-011-2003. számú értékelési jelentés alapján került kiadásra.
Készült a HunTrust Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-011/2003.**
A tanúsítás kelte: 2003. szeptember 24.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2006. szeptember 24.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a STARCOS 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 STARCOS intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók (aláírók) jól képzettek és megbízhatóak.

2. A STARCOS intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók titokban tartják saját PIN kódjukat.

II. Az ITSEC tanúsításokból fakadó érvényességi feltételek

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

Nincs ilyen feltétel.

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

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

3. A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi feltöltő (padding) algoritmusra kell korlátozni: PKCS#1-es v 1.5

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

5. Bizalmasságot, hitelességet és sértetlenséget biztosító titkos üzenetváltást kell biztosítani (az SSL protokoll aktivizálásával, 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.

6. A kártyatulajdonos sikeres hitelesítését követő aláírások számára vonatkozó korlátot a következőképpen kell konfigurálni:
   - értéke 0 /nincs korlátozás/, ha egy hitelesítés-szolgáltató megbízható környezetében használják az intelligens kártyát, illetve
   - értéke 1 /a korlátozás csak 1 aláírást enged meg egy hitelesítés után/, amennyiben egy magánszemély használja aláírási célból az intelligens kártyát.

7. A globális PIN kódot úgy kell konfigurálni, hogy az SSL mindkét funkcionalitását (hitelesítés és dekódolás) védje.

8. Egy BALE-ként használt STARCOS esetén az adminisztrátor és felhasználó (aláíró) szerepkörök szétválasztásával, valamint az inicializálási, perszonalizálási folyamatoknál alkalmazott programok és rezsim szabályok együttműködésével biztosítani kell a következőket:

   Amennyiben az adminisztrátor generálja az aláírói kulcspár(oka)t:
   1. A generálási folyamat során az „adminisztrátor” hajtson végre egy páronkénti megfelelőség tesztet (az aláíráshoz generált nyilvános – magánkulcs pár összetartozásának ellenőrzését), és csak sikeres eredmény esetén kérhető a nyilvános kulcsra tanúsítvány.
   2. Az „adminisztrátor” biztonságosan (az 5. feltételt betartva, megbízható csatornán keresztül) exportálja a legenerált nyilvános kulcsot tanúsítvány készítés céljából.
   3. A hitelesítés-szolgáltató által elkészített tanúsítványt az adminisztrátor továbbítsa az intelligens kártyának.
   4. Az „adminisztrátor” az 5 digites transzport PIN kód átadásával (nem feltétlenül személyesen, de mindenképp egy biztonságos átadási eljárás keretében) engedélyezze a felhasználó számára az aláírási funkció aktivizálását, s egyúttal (ha még nincs az összes legenerálható kulcspár legenerálva) a további aláírói kulcspárok generálását.
   5. A felhasználó ellenőrizze le a kapott transzport PIN kód hosszúságát, s csak akkor fogadja el, ha az 5 digites. Ekkor az első kártyával kapcsolatos tevékenysége a PIN kód lecserélése legyen, egy legalább 6 digitből álló saját PIN kódra.

   Amennyiben a felhasználó generálja saját aláírói kulcspárj(á/ai)t:
   6. Az „adminisztrátor” az 5 digites transzport PIN kód átadásával (nem feltétlenül személyesen, de mindenképp egy biztonságos átadási eljárás keretében) engedélyezze a felhasználó számára az aláírói kulcspárok generálását, valamint az aláírási funkció későbbi aktivizálását.
   7. A felhasználó ellenőrizze le a kapott transzport PIN kód hosszúságát, s csak akkor fogadja el a kártyát, ha a PIN kód 5 digites. Ebben az esetben az első kártyával kapcsolatos tevékenysége a PIN kód lecserélése legyen, egy legalább 6 digitből álló saját PIN kódra.
   8. Ezt követően a felhasználó generálja le magának aláírói kulcs(á/ai)t, s a folyamat során hajtson végre egy páronkénti megfelelőség tesztet (az aláíráshoz generált nyilvános – magánkulcs pár összetartozásának ellenőrzését). Csak sikeres eredmény esetén kérhető a nyilvános kulcsra tanúsítvány.

9. A felhasználó biztonságosan (az 5. feltételt betartva, megbízható csatornán keresztül) exportálja a legenerált nyilvános kulcsot tanúsítvány készítés céljából.
10. Végül a hitelesítés-szolgáltató által elkészített tanúsítványt a felhasználó küldje át az intelligens kártyára.

9. Az aláíró csak megbízható (host oldali) aláírás-létrehozó alkalmazást használhat.

10. Jelen Tanúsítvány csak a jelenlegi verzióra érvényes:
/P8WE5032v0G chip, SPK 2.3 v 7.0 operációs rendszer, StarCert v 2.2 alkalmazás/

Új chip verzió esetén mind a chip-re, mind az operációs rendszerre és alkalmazásra új tanúsítás szükséges.
Amennyiben csak az operációs rendszer vagy az alkalmazás változik, elég egy olyan új, az operációs rendszerre és az alkalmazásra 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.

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-0158-2001 Certification /for Philips Smart Card Controller P8WE5032V0G/

BSI-DSZ-ITSEC-0158-2001 Certification Report /for Philips Smart Card Controller P8WE5032V0G/

BSI-DSZ-ITSEC-0158 Security Target /Evaluation on Philips P8WE5032 Secure 8-bit Smart Card Controller Version P8WE5032V0G/

T-Systems 02078.TE.12.2001 Certification /Signature Creation Device "Integrated Circuit Card with processor P8WE5032V0G and STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2/

T-Systems-DSZ-ITSEC-04075-2001 Certification Report /STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2/

T-Systems-DSZ-ITSEC-04075-2001 Security Target /StarCert version 2.2 signature application on STARCOS SPK 2.3 version 7.0/

BSI-DSZ-ITSEC-0172-2003 IT-Sicherheitszertifikat /zu STARCOS SPK 2.4 mit Tachograph Card Applikation/

BSI-DSZ-ITSEC-0172-2003 Zertifizierungreport /zu STARCOS SPK 2.4 mit Tachograph Card Applikation/

BSI-DSZ-ITSEC-0172-2003 Sicherheitsvorgaben /zu STARCOS SPK 2.4 mit Tachograph Card Applikation/

A Giesecke & Devrient felelős vezetőinek írásos nyilatkozata arról, hogy a STARCOS SPK 2.3 v7.0 és a STARCOS 2.4 (Tachográf kártya alkalmazással) ugyanazt a megbízható csatornát valósítja meg a "biztonságos adatcsere" funkción keresztül".