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
Oberthur Card Systems és Philips Semiconductors GmbH
által kifejlesztett és az
Oberthur Card Systems Kft.
által forgalmazott

CosmopolIC intelligens kártya

/mikrochip: P8WE5033 (verzió: V0G), nyílt Java platform: CosmopolIC (2.1 V4 verzió)/
elektronikus aláírási termék

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

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételeinek figyelembe vételével

biztonságos intelligens kártya platform

mely különböző kriptográfiai szolgáltatást megvalósító alkalmazások (elektronikus aláírást, titkosítást, hitelesítést végző appletek) számára biztosít megbízható kriptográfiai alaptámogatást és védett futtatási környezetet.

Jelen tanúsítvány a HUNG-TJ-006-2003. számú tanúsítási jelentés alapján került kiadásra.
Készült az Oberthur Card Systems Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-006/2003.**
A tanúsítás kelte: 2003. március 27.
A tanúsítvány érvényességi ideje: 2006. március 27.
Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 10 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A CosmopolIC 2.1 V4 legfontosabb biztonsági tulajdonságainak összefoglalása

Az alábbi részletek a HUNG-TJ-006/2003 tanúsítási jelentésből származnak:

1.1 A CosmopolIC intelligens kártya fő komponensei

Az Oberthur Card Systems CosmopolIC 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 CosmopolIC intelligens kártya az alábbi komponensekből áll:

- **mikrochip** (a Philips P8WE5033V0G típusú chip-je),
- **BIOS** (a hardver komponens és az alkalmazások közötti interfész)
- **virtuális gép** (az utólag telepített /letöltött/ alkalmazások számára egységes /operációs rendszertől független/ felületet biztosító, az alkalmazások futtatását végző komponens),
- **API** (jelen esetben a JavaCard 2.1.1 alkalmazás interfész),
- **nyílt platform alkalmazás** (jelen esetben az Open Platform OP 2.0.1, Configuration 1b /benne az alkalmazásokat az intelligens kártyára telepítő, onnan törlő, illetve a külvilággal való kommunikáció biztonságát felügyelő „**Kártyamenedzser**”/
- **rezidens alkalmazás** (parancs irányító)

A fenti komponensek nem tartalmazzák az intelligens kártyára tölthető, azon futtatható alkalmazásokat (ezért használjuk a későbbiekben a CosmopolIC intelligens kártyára a „biztonságos intelligens kártya platform” megnevezést).

1.2 A CosmopolIC intelligens kártya biztonsági tulajdonságai

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

- ***a kivételek (exceptions) kezelése***
  A potenciális támadás vizsgálata automatikusan kivétel jelzést vált ki. Ez az aktuálisan futó folyamatot befejezi (abbahagyja). A következő eseményekkel jelzi a hibát:
  - bejegyzi a biztonsági naplóba, amennyiben a hiba típusa elemezhető a biztonság megsértéseként,
  - a biztonsági kivételt okozó appletet bezárja,

- végrehajtja az applet fejlesztője által megírt kivétel kezelési folyamatot (a JavaCard 2.2.1 Exception Handling szerint),
- egyébként hiba állapottal tér vissza.

- ***a CAP fájl sértetlenségének ellenőrzése***
  A CAP fájlt (vagyis az optimálisan konvertált appletet tartalmazó fájlt) alá kell írni. Az intelligens kártya ellenőrzi ezt az aláírást a CAP (konvertált applet) fájl betöltésekor. Integritás hiba esetén a CAP fájl nem kerül betöltésre.

- ***biztonságos csatorna a külső felhasználókkal kicserélt információk sértetlenségének biztosítására***
  Az adatok, kulcsok és privilégiumok sértetlenségének ellenőrizhetőségét a velük átküldött MAC garantálja. /A kártya kibocsátóval folytatott információcsere biztonsági követelményeit a Kártyamenedzser életciklusa határozza meg. Ez a szolgáltatás (a kártyával kicserélt információk MAC-on alapuló integritásvédelme) az appletek számára is elérhető/.

- ***biztonságos csatorna a külső felhasználókkal kicserélt információk bizalmasságának biztosítására***
  Az adatok és kódok bizalmasságát a DES algoritmussal való titkosítás garantálja. /A kártya kibocsátóval folytatott információcsere biztonsági követelményeit a Kártyamenedzser életciklusa határozza meg. Ez a szolgáltatás (a kártyával kicserélt információk DES-en alapuló titkosítása) az appletek számára is elérhető/.

- ***a kártya kibocsátó (adminisztrátor) hitelesítése***
  Egy biztonságos csatornát kiépítő kommunikációs munkaszakasz kezdetén kötelező a kölcsönös hitelesítés, még mielőtt bármilyen lényeges adat továbbításra kerülne.

- ***Az érzékeny adatok bizalmassága***
  Az intelligens kártya megvédi az alábbi adatok bizalmasságát két (RAM-beli vagy EEPROM-beli) memória blokk összehasonlítása során:
  - PIN értékek,
  - bájt rendezők.

- Az intelligens kártya biztosítja a maradvány információk bizalmasságát:
  - a FAT tábla kezelésével és a hulladékinformáció összegyűjtésével,
  - a deallokálásra kerülő EEPROM törlésével,
  - az allokálásra kerülő átmeneti rendezők törlésével.

- ***tranzakciók védelme (pl. áramkimaradás esetén)***
  Egy tranzakció a hosszú távon tárolt adatok részleges módosítására irányul. Az intelligens kártya erős támogatást ad az elemi tranzakcióknak, a tranzakció előtti állapotok automatikus visszaállítását biztosítva a normálistól eltérő befejezések esetén. Ez védelmet biztosít például az olyan események ellen, amikor áramkimaradás következik be egy tranzakció közben.

Annak érdekében, hogy a PIN kódok ellenőrzését áramkimaradással, illetve egyéb zavarással ne lehessen megkerülni, a PIN kód megadásra rendelkezésre álló kísérletek száma még az összehasonlítás (ellenőrzés) előtt csökkentésre kerül.

- ***ratifikálás***
  Ez a biztonsági funkció:
  - kezeli a PIN kód megadásra még rendelkezésre álló kísérletek számát,
  - lelassítja a kártyakibocsátó (adminisztrátor) hitelesítési idejét,
  - naplóbejegyzésben rögzíti a kártya gyártó sikertelen hitelesítését.

- ***EEPROM kvóta***
  A kártya kibocsátó (adminisztrátor) az appletek számára egy (teljes életciklusukra érvényes) korlátot határozhat meg a felhasználható nem-felejtő memória területre.

- ***Az érzékeny adatok sértetlenségének ellenőrzése***
  Az intelligens kártya ellenőrzi a kriptográfiai kulcsok, hitelesítő adatok (PIN kódok) és az érzékeny applet adatok sértetlenségét. Integritási hiba észlelése esetén hibajelzést ad, az érintett adatot elérhetetlenné teszi, s a folyamatban lévő műveletet megszakítja. Ez a művelet véd az adatok manipulálással történő felfedése ellen.

- ***az objektumok sértetlenségének ellenőrzése***
  Az intelligens kártya felhasználás előtt ellenőrzi a Java objektumok, kártya nyilvántartási adatok (applet azonosító, applet privilégiumok), kulcskészlet verziók és biztonsági napló fájlok sértetlenségét. Integritási hiba észlelése esetén hibajelzést ad, az érintett adatot elérhetetlenné teszi, s a folyamatban lévő műveletet megszakítja.

- ***az appletek sértetlenségének ellenőrzése***
  Egy applet végrehajtása előtt az intelligens kártya ellenőrzi annak sértetlenségét.

- ***a ROM kódok sértetlenségének ellenőrzése***
  Az intelligens kártya ellenőrzi a ROM-ban tárolt kód sértetlenségét:
  - minden reset során (részleges ellenőrzés),
  - a gyártó hitelesítése során az „External Authenticate” parancs segítségével (teljes ellenőrzés).

- ***belső szerepkör kezelés: kártya nyilvántartás***
  Az intelligens kártya kezeli az appletek belső szerepköreit, a kártya nyilvántartásában tárolt privilégiumokon keresztül.

- ***az elindítási folyamat következetessége***
  Az elindítás folyamán az intelligens kártya elnémítja (leállítja) magát a következő hibák esetén:
  - a Kártyamenedzser életciklusának ellentmondó állapot,
  - az EEPROM integritás hibája,
  - a biztonsági napló fájl integritás hibája,
  - a ROM kód integritás hibája,

- a biztonsági napló fájlba írt rekordok száma elér vagy meghalad egy korlátot,
- az opcionális kód terület integritás hibája,
- a véletlenszám generátor blokkolása,
- a kriptográfiai modul hibás működése,
- a FAT tábla integritás hibája,
- kivétel jelzés kiadása.

- ***a biztonsági napló fájl elemzése***
  Ez a funkció azt vizsgálja meg, hogy a biztonsági napló fájlba írt rekordok száma elér-e vagy meghalad-e egy korlátot. Ha igen, lenémítja a kártyát.

- ***biztonsági információ bejegyzése a biztonsági naplóba***
  Olyan kivétel bekövetkezése esetén, melynek típusa a biztonság megsértésének tekinthető, a kivétel típusa, s a kiváltó applet bejegyzésre kerül a biztonsági naplóba.

- ***a kártya gyártó hitelesítése***
  A megszemélyesítés folyamata során kötelező a gyártó hitelesítése a kommunikációs munkaszakasz kezdetén, még mielőtt bármilyen lényeges adat a kártyára kerülne.

- ***A rezidens alkalmazás parancs irányítója***
  A megszemélyesítés folyamata során ez a funkció állapítja meg, hogy a gyártó hitelesítése szükséges-e minden parancsnál.

- ***a kulcs sértetlenségének folyamatos ellenőrzése: kulcsellenőrző érték***
  Ez a funkció egy kulcsellenőrző érték algoritmus használatával a kulcs integritását ellenőrzi, a Visa nyílt platform kártya specifikációnak megfelelően.

- ***a Kártyamenedzser parancs irányítója***
  A Kártyamenedzser kiválasztásakor ez a funkció állapítja meg, hogy a kártya kibocsátó hitelesítése szükséges-e minden parancsnál.
  Egy biztonságos csatorna megnyitása esetén ez a funkció állapítja meg a Kártyamenedzser életciklusa alapján, hogy kötelező-e minden parancsnál a biztonságos üzenetváltás.

- ***a biztonsági napló fájl olvasása***
  Ez a funkció (a kártya kibocsátó sikeres hitelesítését követően) kiolvassa, majd érthető formában kiadja a biztonsági napló fájlt.

- ***Titok generálása***
  Ez egy kettős funkció:
  - véletlenszám generálás: a mikrochip véletlenszám generátorára építve egy véletlen számot állít elő,

- munkaszakasz kulcs generálás: a Kártyamenedzsert érintő valamennyi munkaszakasz kommunikáció biztonságának érdekében munkaszakasz kulcsot állít elő. Az így előállított DES munkaszakasz kulcsokat a biztonságos csatorna műveletihez (bizalmasság és sértetlenség garantálására) használják.

- ***RSA kulcsok generálása***
  Az intelligens kártya appleteket biztosít RSA kulcsgenerálási szolgáltatásra. Ez a szolgáltatás a mikrochip RSA koprocesszorát használja.

- ***DES algoritmus***
  Az intelligens kártya ezt a funkciót a DES hardverrel valósítja meg.

- ***RSA algoritmus***
  Az intelligens kártya ezt a funkciót a FameX koprocesszor segítségével gyorsítja meg.

- ***Tűzfal***
  Ez egy összetett funkció az alábbi funkció elemekkel:
  - applet elkülönítés
    Az intelligens kártya támogatja az appletek és kontextusok (applet környezetek) elkülönítését.
    Az elkülönítés azt jelenti, hogy egy applet nem férhet hozzá egy másik kontextus appletjének mezőihez és objektumaihoz, hacsak a másik applet nem biztosít közvetlenül egy hozzáférési interfészt.
  - JCRE privilégiumok
    Lévén a JCRE kontextus egy rendszer kontextus, speciális előjoga van: a kártya valamennyi objektumának eljárásait elvégezheti. A CosmopolIC intelligens kártya esetén a Kártyamenedzser kontextusa a JCRE kontextus (s így minden kártya objektum eljárásait elvégezheti).
  - JCRE belépési pont
    A JCRE belépési pontok olyan objektumok, melyek tulajdonosa a JCRE kontextus, egyben meg vannak jelölve, mint belépési pont eljárásokat tartalmazók.
    A tűzfal megvédi ezeket a belépési pontokat az appletek felöli eléréstől. Ugyanakkor a belépési pont kijelölés lehetővé teszi ezen objektumok eljárásai számára, hogy bármely kontextusból meghívják.
    A CosmopolIC intelligens kártya JCRE belépési pontjai az APDU objektum és a kártya futásidejű kivétel jelzései (runtime exceptions).
    Ha egy objektum JCRE belépési pont, akkor az applet elkülönítésre vonatkozó általános szabályok eltérnek, megengedve az aktuális kontextus ellenőrzése alatti általános hozzáférést.
  - globális rendezők (arrays)
    A globális rendezők tulajdonosa a JCRE kontextus, de valamennyi kontextusból elérhetők.
    A CosmopolIC intelligens kártya egyetlen globális rendezője az APDU buffer.

Erre a globális rendezőre (APDU buffer) az applet elkülönítésre vonatkozó általános szabályok eltérnek, megengedve az aktuális kontextus ellenőrzése alatti általános hozzáférést.

- megosztható interfész
  A megosztható interfész a megosztott objektumok azonosítására használható. Minden olyan objektumnak, melyet az applet tűzfalon keresztül meg kell osztani, közvetve vagy közvetlenül ezt az interfészt kell alkalmaznia. A tűzfalon keresztül csak a megosztható interfészben meghatározott eljárások érhetők el.
  Ha az applet meghívja a *getPreviousContextAID* parancsot akár magából az appletből, akár egy külső appletből a megosztható interfészen keresztül elérhető eljárásból, a parancs azonosítja meghívóját.

- ***Kulcskészlet verziójának menedzselése***
  Egy kulcskészlet betöltése frissítheti, törölheti vagy kiegészítheti a korábbi kulcskészlet.

- ***Hozzáférés a DES kulcsokhoz***
  A DES kulcsokhoz való hozzáférés megfelel azoknak a szabványoknak, melyeket a JavaCard 2.1.1 API, OP CS, VOP CS dokumentumok tartalmaznak. Ez a hozzáférés megvédi a kulcsot az illetéktelen felfedéstől.

- ***Hozzáférés az RSA kulcsokhoz***
  Az RSA kulcsokhoz való hozzáférés megfelel azoknak a szabványoknak, melyeket a JavaCard 2.1.1 API dokumentum tartalmaz. Ez a hozzáférés megvédi a kulcsot az illetéktelen felfedéstől.

- ***Az átmeneti rendezők kezelése a logikai csatornákban***
  Ez a funkció garantálja az applet(ek)hez tartozó, különböző logikai csatornákban végrehajtott CLEAR_ON_DESELECT átmeneti rendezők elkülönítését.

A fenti biztonsági tulajdonságok építenek a CosmopolIC intelligens kártya alapját képező chip /Philips P8WE5033V0G/ biztonsági tulajdonságaira (melyet a HUNG-TJ-006/2003 tanúsítási jelentés részletesen ismertet)

2. számú melléklet

A biztonságos felhasználás feltételei

1. Felhasználási környezet
Valamennyi érzékeny adat (kulcsok, PIN kódok, appletek) sértetlenségét és/vagy bizalmasságát védeni kell az intelligens kártya külső környezetében történő tárolás és továbbítás során (pl. a szoftver megszemélyesítése vagy az applet betöltése során).

2. Appletek fejlesztése
Az intelligens kártya platform telepítése után a kártyára töltött appletek fejlesztése során az appletek fejlesztésére vonatkozó „programozási útmutató" valamennyi szabályát be kell tartani.

Az appleteket oly módon kell fejleszteni, hogy azok megfelelő védelmet biztosítsanak saját érzékeny adataiknak[1].
Valamennyi utólag a kártyára töltött appletet a JavaCard specifikációknak megfelelő eszközökkel kell összeszerkeszteni, konvertálni és ellenőrizni. Alapvető fontosságú az appletek aláírása (DAP kiszámítása, mellékelése) is ebben a folyamatban.

3. Biztonságos csatorna alkalmazása
Az importált adatok sértetlenségének és bizalmasságának biztosítása érdekében a biztonságos csatornát használva, az adattitkosító funkciót kell alkalmazni.

4. A tanúsított verzió használata
Az applet fejlesztők és a végfelhasználók pontosan a tanúsítás tárgyát képező verziót használják:

- mikrochip: P8WE5033V0G,
- nyílt platform: CosmopolIC (2.1 V4 verzió).

[1] A mikrochip hardver védelmet biztosít a tárolt adatoknak. Az intelligens kártya platform megvédi az egyes appleteket a külvilág, illetve a többi applet irányából induló támadásoktól. Egyik előző komponens sem képes megvédeni ugyanakkor az érzékeny adatokat a saját appletjüktől. (Egy rosszul megírt applet kiadhatja pl. a külvilágnak az általa kezelt bizalmas adatokat.)

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)

A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

Kérdőív a tanúsítás kérelmezéséhez

Certificat 2002/05: CosmopolIC 2.1 v4 JavaCard Open Platform Embedded Software version 1

Certification Report 2002/05: CosmopolIC 2.1 v4 JavaCard Open Platform Embedded Software version 1

CosmopolIC 2.1 v4 JavaCard Open Platform Security Target (EAL4+)

Certificate BSI-DSZ-CC-0199-2002: Philips Smart Card Controller P8WE5033V0G

Certificate Report BSI-DSZ-CC-0199-2002 for Philips Smart Card Controller P8WE5033V0G from Philips Semiconductors GmbH

Security Target Lite BSI-DSZ-CC-0199, version 1.6: Evaluation of the Philips P8WE5033V0G Secure 8-bit Smart Card Controller (EAL5+)

BSI-PP-0002-2001: Smart Card IC Platform Protection Profile (EAL5+)

Oberthur Card Systems: PKCS#11 Cryptoki library for AuthentIC

Oberthur Card Systems: GalactIC version 2.1 V2 Operating System Reference Guide

Oberthur Card Systems: GalactIC version 2.1 V2 Java Card 2.1 Open Platform 2.0.1 Application note Issue 01

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

A tanúsításhoz figyelembe vett, a CosmopolIC intelligens kártya egészére vonatkozó, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 14508 /Common Criteria/ **emelt 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 /

A fenti értékelés felhasználta az intelligens kártya mikrochip-jének korábbi értékelési és tanúsítási eredményeit. Ez még magasabb, **emelt EAL 5**-ös /félformálisan tervezett és vizsgált rendszer/ értékelés garancia szintű volt.

Az emelt szintet az EAL 5 garancia szint által nem megkövetelt alábbi garanciösszetevők kiegészítő megkövetelése és teljesítése jelentette:

- ALC_DVS.2 A biztonsági intézkedések elégségessége /csak EAL6-tól megkövetelt /
- AVA_MSU.3 A nem biztonságos állapotok elemzése és vizsgálata /csak EAL6 -tól megkövetelt /
- AVA_VLA.4 Keményen ellentálló /csak EAL6-tól megkövetelt /

A CosmopolIC intelligens kártya biztonsági funkcióinak értékelt erőssége

A biztonsági funkciók erőssége: **magasszintű.**