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

IBM Corp.

által előállított és forgalmazott

IBM 4758-002 PCI kriptográfiai modul (co-processor)

2-es modell, hardver, Miniboot 0: A verzió, Miniboot 1: A verzió

elektronikus aláírási termék

az 1. számú mellékletben részletezett feltételrendszer teljesülése, valamint a modul 2. és 3. rétegébe biztonságos szoftverek betöltése esetén

megfelel

minősített hitelesítés-szolgáltató által végzett alábbi tevékenységek biztonságos elvégzéséhez:

Elektronikus aláírás hitelesítés szolgáltatás keretén belül:
(Minősített) tanúsítvány aláíró kulcsok generálására, tárolására, (minősített) tanúsítványok aláírására, mentésére és helyreállítására;

Időbélyegzés szolgáltatás keretén belül:
Időbélyegző aláíró kulcsok generálására, tárolására, időbélyegző aláírására;

Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:
Az előfizetői (aláírói) kulcspár generálására;

A minősített hitelesítés-szolgáltató saját informatikai rendszerének biztonságos működtetésén belül:
Infrastrukturális és megbízható rendszervezérlési kulcsok generálására, tárolására és felhasználására.

Jelen tanúsítvány a HUNG-TJ-002-2003, valamint a benyújtott kiegészítő dokumentációkon és értékelésen alapuló HUNG-TJ-006-2003 számú tanúsítási jelentések alapján került kiadásra. Készült a MÁV Informatika Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-002-1/2003.**
A tanúsítás kelte: 2003. március 25.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2006. március 25.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 7 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

Jelen tanúsítvány a HUNG-T-002/2003. számú tanúsítvány érvényességi feltételeinek kiterjesztését tartalmazza, melynek alapja, hogy Megbízó a HUNG-T-002/2003. számú tanúsítvány kiadása után további dokumentációkat nyújtott be, melyekkel az előző tanúsítványban szereplő DSA aláíró algoritmus mellett a modulra az RSA aláíró algoritmus biztonságos alkalmazhatósága is igazolható.

A tanúsítvány érvényességi feltételei

Az IBM 4758-002 egy olyan beavatkozásra reagáló, programozható, kriptográfiai PCI kártya, mely általános célú számítástechnikai környezetet és nagy hatékonyságú kriptográfiai támogatást biztosít. Kriptográfiai funkciók széles választékának megvalósítását támogatja, speciális tervezésű, hardverben megvalósított algoritmusok elérhetővé tételével. Képes szoftvert befogadni, futtatni, egyben megvédeni a betöltött szoftvert és annak titkos adatait, magas támadó potenciállal rendelkező támadók legkülönbözőbb logikai és fizikai támadásával szemben.

A tanúsítás tárgyát képező eszköz a következő fő komponensekből áll:

- hardver /benne: véletlen zaj-generátor, SHA-1-t számító és hatványozó célhardverek, beavatkozást érzékelő, s erre reagáló áramkörök, hardver zárak/,
- Miniboot szoftver /az IBM 4758-002 alapját képező két réteg (0. és 1.), mely az egész eszköz biztonságát és konfigurációját felügyeli/,
- magasabb rendszerszoftver és alkalmazási rétegek (2. és 3. rétegek) kialakításának lehetősége.

Az IBM 4758-002 PCI kriptográfiai koprocesszor hardvere, valamint a 4 egymásra épülő rétegre betölthető szoftver/förmver rendszer alsó két rétege (Miniboot Layer 0, 1) tanúsítvánnyal igazoltan, a legmagasabb 4-es biztonsági szinten kielégíti a FIPS 140-1 követelményeit.

Az utólag az eszközbe tölthető rendszerszoftver és alkalmazás védelmét a hardver és az alsó két réteg támogatja (a 4-es biztonsági szinten tanúsított eszköz biztonságos platformot nyújt biztonságos rendszerszoftverek és alkalmazások védett tárolására és futtatására), amennyiben az alsó két förmver réteg és hardver ezt támogató biztonsági mechanizmusait helyesen alkalmazzák.

A betölthető rendszerszoftverre és alkalmazásra a FIPS tanúsítvány nem vonatkozik. A FIPS 140-1 tanúsítással rendelkező alapkiépítés (hardver, és a szoftver 0. és 1. rétege) önmagában működésképtelen. A 2. és 3. rétegekre töltött szoftverek felelőssége, hogy az alapjukat képező biztonságos platform szolgáltatásait helyesen hívják meg, illetve szabványos, kriptográfia szempontból korrekt, magas szintű interfészt biztosítsanak az IBM 4758-002 eszközt kívülről meghívó alkalmazások számára.

Amennyiben az IBM 4758-002 kriptográfiai modult egy minősített hitelesítés-szolgáltató kívánja felhasználni biztonságkritikus tevékenységeihez (az általa kibocsátott tanúsítványok aláírására, időbélyeg válaszai aláírására, aláírói kulcspárok generálására, stb.), további követelményeknek kell megfelelni kiegészítő feltételek betartását követelve meg.

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

I. Általános érvényességi feltétel

1. Az IBM 4758-002 PCI kriptográfiai koprocesszor telepítése során be kell tartani az „IBM 4758 PCI Cryptographic Coprocessor Installation Manual" által leírt kötelező szabályokat.

II. A FIPS 140-1 megfelelőségből fakadó érvényességi feltételek

Az alábbi feltétel a FIPS 140-1 megfelelőség érdekében elengedhetetlen.

2. A kriptográfiai modul felső (2. és 3.) rétegeiért felelős kriptográfiai tisztviselők (Officer_2, Officer_3) nyilvános kulcsú aláíró algoritmusuknak (mellyel aláírják az alattuk lévő rétegeknek szóló parancsaikat) a **DSA** algoritmust kell választaniuk **(SHA-1** lenyomatoló függvény mellett**)**.

III. A kiegészítő vizsgálatok eredményéből adódó feltételek

3. A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi algoritmusokra kell korlátozni: **DSA és RSA (SHA-1** lenyomatoló függvény mellett**)**.

4. A tanúsítvány címlapján felsorolt, a 2. és 3. rétegekbe betöltött szoftverekkel megvalósított szolgáltatásoknál használható algoritmusok a következők**: DSA és RSA (SHA-1** lenyomatoló függvény mellett**)**.

IV. A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak az IBM 4758-002 felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

5. A DSA aláírási algoritmusra a minimális p prímhosszúság (pMinLen) 1024 bit, a minimális q prímhosszúság (qMinLen) 160 bit legyen.

6. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (MinModLen): 1020 bit legyen. Az aláírás-ellenőrző adat (nyilvános exponens) minimálisan 65537 legyen.

7. Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet**.**

8. A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási listák aláírására szabad felhasználni.

9. Bármilyen, biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a modulnak gondoskodnia kell a kulcs védelméről. Érzékeny kulcsadatok nem védett módon történő tárolása tilos.

10. Az időbélyegzéshez használt aláíró kulcsokat csak időbélyegek aláírására szabad használni.

11. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (az IBM 4758-002 kriptográfiai modulban) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

12. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (az IBM 4758-002 kriptográfiai modulban) történik, biztosítani kell, hogy az IBM 4758-002 kriptográfiai modul és az aláírás létrehozó eszköz között biztonságos útvonal legyen. Ennek az útvonalnak forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával.

13. A Tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes /2-es modell, Miniboot 0.: A verzió, Miniboot 1.: A verzió/. Új förmver verzió feltöltése az alábbi követelmények együttes teljesülése esetén lehetséges:
    - az új förmver verziót a fejlesztő-gyártó cég digitális aláírása hitelesíti,
    - az új förmver verziót értékelte egy FIPS 140 értékeléssel meghatalmazott (akkreditált) laboratórium, s erről egy új FIPS tanúsítvány is készül,
    - az új förmver verzió minősített hitelesítés-szolgáltatáshoz történő felhasználhatóságát egy erre kijelölt hazai tanúsító szervezet megfelelőségi tanúsítványba foglalja, s mint ilyen, az új verzió is bekerül a HIF biztonságos elektronikus aláírási termék nyilvántartásába.

V. A 2. és 3. rétegre betöltendő biztonságos szoftverre vonatkozó feltételek

A FIPS tanúsítványt megalapozó vizsgálat döntő része a hardver védelem erősségére vonatkozott, mely az egész eszköz biztonságilag legkritikusabb része. Ugyanakkor a jelenleg FIPS 140-1 tanúsítvánnyal rendelkező alapkiépítés (hardver, és a szoftver 0. és 1. rétege) önmagában működésképtelen, ezért mindenképpen fel kell tölteni szoftverrel a 2., nagy valószínűséggel a 3. réteget is, ezzel lesz csak teljes a kriptográfiai modul.

A modul 2. és 3. rétegére betöltendő szoftver biztonságosnak tekinthető a következő alternatív feltételek kielégítése esetén:

14/a A modul 2. és 3. rétegét is az IBM által kifejlesztett szoftverekkel töltik fel:
- a 2. rétegre a CP/Q $^{++}$ kontroll programot (mely memória-kezelést, több feladat egyidejű futását, s ezek szinkronizálását biztosítja, C nyelven íródott könyvtárat kínál fel, stb.),
- a 3. rétegre pedig a PKCS #11 szabványos interfészt támogató, IBM alkalmazást.

14/b A 2. és 3. rétegre olyan más programokat töltenek be, melyek rendelkeznek FIPS 140 tanúsítvánnyal, legalább 3-as biztonsági szinten. /Ez az elvárás szerepel az IBM 4758 Model 2 Security Policy 8.2. fejezetben (22. oldal), a modulra adott FIPS tanúsítvány érvényességi feltételei között./ Ebben az esetben be kell tartani a (szoftverre vonatkozó) FIPS tanúsítványban szereplő előírásokat is.

2. számú melléklet

TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK

A követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

16/2001. (IX.1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

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

FIPS 140-1: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-1

ETSI TS 101 456 Policy Requirements for Certification Authorities Issuing Qualified Certificates

CEN 14167-1 munkacsoport egyezmény: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

CEN 14167-2 munkacsoport egyezmény: Cryptographic Module for CSP Signing Operation – Protection Profile (CMCSO-PP, HSM-PP)

CEN 14167-3 munkacsoport egyezmény: : Cryptographic Module for CSP Key Genaration Services – Protection Profile (CMCKG-PP, HSM-PP)

3. számú melléklet

A tanúsításhoz figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

Kérdőív a tanúsítás kérelmezéséhez

FIPS 140-1 Validation Certificate No. 116 /IBM 4758-002 PCI Cryptographic Coprocessor/, ld. Tanúsítvány további melléklete

IBM 4758 Model 2 Security Policy /June 2000/

IBM PCI Cryptographic Coprocessor General Information Manual /Sixth Edition, May 2002/

IBM 4758 PCI Cryptographic Coprocessor Installation Manual /Second Edition, March, 2000/

AZ IBM megfelelőségi nyilatkozata az RSA algoritmus biztonságos megvalósításáról

Értékelő jelentés az RSA algoritmus biztonságos alkalmazhatóságáról. /HUNG-EJ-002-1/2003/.