TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005.(VII. 21.) IHM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 002/2006 számú kijelölési okiratával kijelölt terméktanúsító szervezet

tanúsítja,

hogy az

IBM Corp.

által előállított és forgalmazott

a CP/Q++ kontroll programmal működtetett IBM 4758 /PCI cryptographic Coprocessor/ kriptográfiai modul

hardver modell: 2, Miniboot 0: A verzió, Miniboot 1: A verzió, CP/Q++: 2.41

elektronikus aláírási termék

az 1. számú mellékletben részletezett feltételrendszer teljesülése 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-046-2009. számú értékelési jelentés alapján került kiadásra.
A tanúsítványt a MÁV INFORMATIKA Zrt. kérésére állítottuk ki.
A tanúsítvány regisztrációs száma: **HUNG-T-046/2009.**
A tanúsítás kelte: 2009. március 30.
A tanúsítvány érvényességi ideje az 1. számú melléklet IV/15. pontja alapján: 2009. december 31.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 7 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

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, a 4 egymásra épülő rétegre betölthető szoftver/förmver rendszer alsó két rétege (Miniboot Layer 0, 1), valamint a 2., alkalmazási réteg, mely CP/Q++ alkalmazást tartalmazza, tanúsítvánnyal igazoltan, 3-as biztonsági szinten kielégíti a FIPS 140-1 követelményeit.

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, melyek a felhasználhatóságot tovább korlátozzák, 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 feltételek a FIPS 140-1 megfelelőség érdekében elengedhetetlenek.

2. A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi algoritmusokra kell korlátozni: **DSA, RSA, SHA-1**.

3. A hardvert a következőkkel kell feltölteni:
   - A FIPS 140 értékelt Miniboot-ot az 1. rétegbe.
   - A FIPS 140 értékelt CP/Q++-t a 2. rétegbe. A réteg 'tulajdonos azonosítója' (owner identifier) 2 kell, hogy legyen. Működő rendszerben 6-os azonosítót nem szabad használni.

4. A külső External User felhasználónak meg kell vizsgálnia, hogy van-e valami FIPS 140 által megkövetelt megkötés a 3. rétegben futó alkalmazás felhasználásával kapcsolatban.

III. 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. Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet

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

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

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

10. 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.

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 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.

12. A Tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes /2-es modell, Miniboot 0.: A verzió, Miniboot 1.: A verzió, CP/Q++: 2.41/. 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.

IV. Egyéb, az érvényességet befolyásoló megjegyzések

13. A National Institute of Standards and Technology (NIST) által kibocsátott tanúsítványok visszavonásig érvényesek. Így a tanúsítványokban szereplő hardver, förmver és szoftver konfigurációk változatlan formában használhatók.

14. A FIPS 140-1 szerint tanúsított modulok továbbra is biztonságosnak tekinthetők. A FIPS 140-1 szerinti tanúsítványok azonban 2002. május 26. után nem adhatók ki.

15. Nyilvános forrásban jelenleg két olyan támadás található, melyek a modul biztonságát veszélyeztetik. Az egyik a modulban tárolt 3DES kulcs kinyerésére, a másik a banki alkalmazásokban használt PIN kódok kinyerésére irányul.

    Az első támadás a rosszul megvalósított jogosultságkezelés eredménye, melynek során a modulban tárolt 3DES kulcsot lehet viszonylag egyszerűen kinyerni. A támadás kivédése a tanúsításra kerülő 2.41-es CP/Q++ verzióban már implementálásra került. További védelmet nyújtanak a minősített hitelesítés-szolgáltatóknál megvalósított fizikai biztonsági intézkedések, hiszen a támadás végrehajtásához a modulhoz való fizikai hozzáférés szükséges.

    A Bugtraq 6901 azonosítóval ellátott hiba abban az esetben jelentkezik, ha a modult banki környezetben használják. Ekkor a bankkártyák PIN kódjainak visszafejtésére van lehetőség a támadás végrehajtásához. Ez a támadás a minősített hitelesítés-szolgáltatók működését nem érinti, a megfelelő fizikai biztonsági intézkedések védelmet nyújtanak a támadás ellen.

    A fenti két támadás tehát nem érint minősített hitelesítés-szolgáltatóknál való működést, ugyanakkor a Nemzeti Hírközlési Hatóság nemzetközi követelményeken alapuló HL-21917-9,10,11,12,13,14/2008. számú határozataiban az SHA-1 lenyomat képző algoritmust csak 2009 év végéig ajánlja tanúsítványok aláírásában felhasználásra. Mivel az IBM 4758---002 HSM a dokumentációk szerint az SHA-1 algoritmust alkalmazza, a tanúsító szervezet a kiadott tanúsítvány érvényességi idejét 2009. december 31-ben korlátozza.

V. Az IBM 4758-002 3. rétegére betöltendő biztonságos szoftverre vonatkozó feltételek

A FIPS tanúsítványt megalapozó vizsgálat döntő része a hardver védelem erősségére vonatkozott, mely az egész eszköz biztonságilag legkritikusabb része. Nagy valószínűséggel a 3. réteget is fel kell tölteni szoftverrel, ezzel lesz csak teljes a kriptográfiai modul.

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

16. Az IBM 4758-002 modul 3. rétegét is az IBM által kifejlesztett szoftverekkel töltik fel:
    - a 3. rétegre a PKCS #11 szabványos interfészt támogató, IBM alkalmazást.

17. A 3. rétegre olyan más programokat töltenek be, melyek rendelkeznek FIPS 140 tanúsítvánnyal, legalább 3-as biztonsági szinten. /Ez az elvárás szerepel a Security Policy for the Security Module with CP/Q++ part of the IBM 4758 PCI Cryptographic Coprocessor Model 002 14. oldalán, 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

3/2005. (III. 18.) IHM 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 v1.4.3 Policy Requirements for Certification Authorities Issuing Qualified Certificates

ETSI TS 102 176-1 V2.0.0 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

CEN 14167-1:2003 Munkacsoport Egyezmény: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

HL-21917-9,10,11,12,13,14/2008. számú NHH határozat a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről

3. számú melléklet

A tanúsításhoz figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

FIPS 140-1 Validation Certificate No. 116 /IBM 4758-002 PCI Cryptographic Coprocessor/ (visszavont)

FIPS 140-1 Validation Certificate No. 345 /Security Module with CP/Q++/

IBM 4758 Model 2 Security Policy /June 2000/

Security Policy for the Security Module with CP/Q++ part of the IBM 4758 PCI Cryptographic Coprocessor Models 002 and 023 (PCICC)

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

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

Mike Bond, Piotr Zielinski, Decimalisation table attacks for PIN cracking, http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-560.pdf

Mike Bond, Richard Clayton, Extracting a 3DES key from an IBM 4758, http://www.cl.cam.ac.uk/~rnc1/descrack/

Frequently Asked Questions for the Cryptographic Module Validation Program