



TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Nemzeti Fejlesztési Minisztérium IKF/19519-2/2012-NFM számú Kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy a **SafeNet Inc.** által fejlesztett

Luna® PCI-e 3000, Luna® PCI-e 7000

Hardver verzió: VBD-04-0100

Luna® PCI-e 3000 SFF, Luna® PCI-e 7000 SFF

Hardver verzió: VBD-04-0102

Luna® PCI 3000, Luna® PCI 7000

Hardver verzió: VBD-03-0100

V3.0

Főrmver verziók: 4.7.1(3000) és 4.7.1(7000)

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 rendszervezérlelési kulcsok generálására, tárolására és felhasználására.

Jelen tanúsítvány a HUNG-TJ-065-2014. számú értékelési jelentés alapján került kiadásra.

Készült a NetLock Hálózatbiztonsági és Informatikai Szolgáltató Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-065-2014.**

A tanúsítás kelte: 2014. június 10.

A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2017. június 10.

Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 6 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

Lengyel Csaba
Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

A Luna® PCI-e és Luna® PCI kriptográfiai modul család egy bonyolult kriptográfiai eszköz, melyet fejlesztői úgy terveztek, hogy minél általánosabb feltételek között legyen használható, s a felhasználói igények minél szélesebb körét legyen képes kielégíteni. Ennek megfelelően számos biztonsági tulajdonság konfigurálható (letiltható/engedélyezhető, illetve be/kikapcsolható) az eszközön.

A FIPS 140-2-nek megfelelő módú működtetés (mely a biztonságra helyezi a hangsúlyt, sokszor a hatékonyság és a felhasználói kényelem rovására) számos konfigurációs beállítást megkövetel, s ezek betartása feltétele a tanúsítás érvényességének.

Amennyiben a Luna® PCI-e és Luna® PCI kriptográfiai modul család egy elemét egy minősített hitelesítés-szolgáltató kívánja felhasználni biztonságkritikus tevékenységeihez (az általa kibocsátott tanúsítványok aláírására, időbélyeg válaszai aláírására), 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 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 Luna® PCI-e és Luna® PCI kriptográfiai modul család szolgáltatásait igénybe vevő különböző munkakörök (Security Officer, Crypto Officer, Crypto User) betöltő személyek:

- kompetensek, jól képzettek és megbízhatóak, valamint
- betartják a különböző útmutatók által leírt, kötelező tevékenységeket.

2. A modult csak megfelelően biztonságos operációs rendszerrel és alkalmazói programokkal üzemeltetett, és megfelelő interfésszel ellátott számítógépbe helyezhető.

3. A kriptográfiai modulhoz való fizikai hozzáférést és a kommunikációs kapcsolatokat felügyelet alatt kell tartani.

II. A FIPS 140-2 megfelelésből fakadó érvényességi feltételek

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a Luna® PCI-e és Luna® PCI kriptográfiai modul család megfeleljen a FIPS 140-2 3-as biztonsági szintjének.

4. A FIPS-jóváhagyott módban történő működéshez az alábbi szabálybeállítások szükségesek:

- „Nem FIPS algoritmusok rendelkezésre állnak” lehetőséget le kell tiltani.
- „Hitelesítés megbízható útvonallal” lehetőséget be kell kapcsolni és modult a PED használatával kell inicializálni az SO hitelesítési adatainak megadásához.
- „Kérdés (challenge) nélküli megbízható útvonal művelet” lehetőséget le kell tiltani, ha az aktiválás vagy automatikus aktiválás be van kapcsolva.
- A „Sikertelen kérdés-válasz (challenge-response) validálások számlálása” lehetőséget engedélyezni kell, ha az aktiválás vagy automatikus aktiválás be van kapcsolva.
- Raw RSA műveleteket csak kulcs átvitelre szabad használni FIPS üzemmódban.

III. A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak a Luna® PCI-e és Luna® PCI kriptográfiai modul család felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

5. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság ($MinModLen$): 2048 bit legyen.

6. DSA aláírási algoritmus használata esetén a minimális p prímhosszúság ($pMinLen$) 2048 bit, a minimális q prímhosszúság ($qMinLen$) 224 bit legyen.

7. Az ECDSA aláírási algoritmus használata esetén a következő paraméter feltételek teljesítése szükséges: $qMinLen=256$ SHA256 használata mellett, továbbá $r0Min$ nagyobb, mint 10^4 és $MinClass$ legalább 200, ahol a paraméterek jelölése megfelel az ETSI TS 102 176-1 v 2.1.1 –ben leírtaknak.

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

9. SHA-1 vagy annál gyengébb lenyomatoló algoritmus használata tilos.

10. A minősített tanúsítvány aláírásához használt kulcsot csak minősített tanúsítványok és opcionálisan a kapcsolódó visszavonási státusz adatok (beleértve az azok ellenőrzésére szolgáló tanúsítványt) aláírására szabad használni.

11. Bármilyen, biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a modulnak gondoskodnia kell a kulcs védelméről. Érzékeny kulcsadatok nem védett módon történő tárolása tilos. Minősített tanúsítvány aláíró kulcs csak további biztonsági mechanizmusok alkalmazása esetén tárolható és menthető. Ez megtehető például az alábbiak valamelyikével is:

- az “m az n-ből” technika alkalmazásával, ahol m azon komponensek darabszáma a teljes n komponensből, amelynek ismeretében a kulcs inicializálása sikeresen elvégezhető. A hiba esetén alkalmazandó helyreállításra az $m = 60\% * n$ érték javasolt (azaz ha $n=3$, akkor $m=2$, ha $n=4$ akkor $m=3$, ha $n=5$ akkor $m=3, \dots$).
 - az alábbi módszerrel:
 - a mentés intelligens kártyákra (tokenekre) történnek,
 - a mentés kódolva van a Triple DES vagy AES titkosító algoritmus alkalmazásával,
 - a mentés kódolására alkalmazott titkosító kulcs (Key Encryption Key) legalább két véletlen komponensből van előállítva, s ennek megfelelően legalább két erre felhatalmazott személy együttes jelenléte szükséges a magánkulcs helyreállításához.
12. Az időbélyegzéshez használt aláíró kulcsokat csak időbélyegek aláírására szabad használni.
13. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a HSM modulban) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.
14. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a HSM modulban) történik, biztosítani kell, hogy a modul és az aláírás létrehozó eszköz között biztonságos útvonal legyen. Ennek az útvonalnak forráshitelesítést, sérthetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával.
15. A Tanúsítvány csak az első oldalon megadott hardver és förmver verzióra érvényes. Új förmver verzióra való frissítés csak 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 az NMHH biztonságos elektronikus aláírási termék nyilvántartásába.

IV. Egyéb, az érvényességet befolyásoló megjegyzések

16. 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.
17. Nyilvános források között jelenleg nem található olyan információ, mely befolyásolná a modul biztonságos működését. Ezt a vizsgálatot legalább 3 évente szükséges elvégezni.

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

FIPS 140-2: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-2

ETSI TS 102 176-1 V2.1.1 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

3. számú melléklet

A tanúsításhoz figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

FIPS 140-2 Validation Certificate No. 1350

LEVEL 3 NON-PROPRIETARY SECURITY POLICY FOR Luna® PCI-e 3000, Luna® PCI-e 3000 Short-Form Factor (SFF), Luna® PCI-e 7000, and Luna® PCI-e 7000 SFF Cryptographic Modules, V3.0 /DOCUMENT NUMBER: CR-3093 Revision 7/

FIPS 140-2 Validation Certificate No. 1354

LEVEL 3 NON-PROPRIETARY SECURITY POLICY FOR Luna® PCI 3000 and Luna® PCI 7000 Cryptographic Modules, V3.0 /DOCUMENT NUMBER: CR-2987 Revision 7/