TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Gazdasági és Közlekedési Miniszterének 113/2007 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy az

SafeNet Inc.

által előállított és forgalmazott

Luna CA³ kriptográfiai token

hardver verzió: 2, förmver verzió: 3.102

elektronikus aláírási termék

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

a) minősített hitelesítés-szolgáltató által végzett alábbi tevékenységek biztonságos elvégzéséhez**:**

Elektronikus aláírás hitelesítés szolgáltatás keretén belül:

minősített tanúsítvány aláíró kulcsok generálására, tárolására, mentésére és helyreállítására, valamint minősített tanúsítványok aláírására;

Időbélyegzés szolgáltatás keretén belül:

időbélyegző aláíró kulcsok generálására, tárolására és időbélyegző aláírására;

A minősített hitelesítés-szolgáltató saját informatikai rendszerének biztonságos működtetésén belül:

infrastrukturális és megbízható rendszervezérlési kulcsok generálására, tárolására és felhasználására;

b) fokozott biztonságú elektronikus aláírás létrehozásához,

melyhez megbízható kriptográfiai alaptámogatást és védett futtatási környezetet biztosít**.**

Jelen tanúsítvány a HUNG-TJ-040-2008. számú tanúsítási jelentés alapján került kiadásra.
Készült a Miniszterelnöki Hivatal Elektronikuskormányzat-központ megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-040-2008.**
A tanúsítás kelte: 2008. 02. 13.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2011. 02. 13.
Mellékletek: feltételek, követelmények, dokumentumok, összesen: 6 oldalon.

PH.

Tanúsítási igazgató:
Endrődi Zsolt

Ügyvezető igazgató
dr. Szabó István

1. számú melléklet

A tanúsítvány érvényességi feltételei

A Luna CA^3 modul 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 be, illetve ki rajta.

A FIPS 140-1-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 CA^3 modult 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 CA^3 modul szolgáltatásait igénybe vevő különböző munkaköröket (Security Officer, User) betöltő személyek:
   - kompetensek, jól képzettek és megbízhatóak, valamint
   - betartják a különböző útmutatók (Luna® PKI HSM Installation Guide, Luna® PKI HSM Planning & Integration Guide) által leírt, kötelező tevékenységeket.

II. A FIPS 140-1 megfelelőségből fakadó érvényességi feltételek

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a Luna CA^3 token megfeleljen a FIPS 140-1 3-as biztonsági szintjének.

2. A biztonságos működéshez csak a tokenhez tartozó alkatrészeket, szoftvereket szabad használni. Ezek a következők:
   - Chrysalis-ITS® dual-slot Luna® Dock PC Card Reader
   - Luna® Pin Entry Device (PED)
   - PED Kulcsok (Datakey® Device)
   - Enabler (termékkonfiguráló) szoftver
   - Cryptographic API Software

3. A Token Szabályzat Vektor (TPV) bitjeit a következő beállításokkal kell használni:
- TPV_USER_ZEROIZE = 1
- TPV_USER_FW_UPDATE = 0
- TPV_M_OF_N_ACTIVATION = 1
- TPV_KEY_ATTRIB_LOCK = 1
- TPV_KEY_SINGLE_FUNCTION = 0
- TPV_SIGNING_KEY_LOCAL = 1
- TPV_DISABLE_CLONING_BY_USER = 1

4. Mind a Security Officer, mind a User szintű felhasználók generálásánál 6 jegyű PIN kódot kell megadni a PED-en keresztül.

5. Az N-ből M aktiválás beállításakor M és N értékeket, úgy kell megválasztani, hogy $M \geq 2$ és $N \geq M$. Ezt az SO és a User jogosultságú felhasználók generálásakor is figyelembe kell venni.

6. Ha a Luna CA^3 tokent többet nem használják, azt olyan módon kell megsemmisíteni vagy tárolni, hogy semmilyen áramköréhez ne lehessen hozzáférni úgy, hogy abból használható információt lehessen kinyerni.

7. A tokenhez mind fizikai, mind hálózati értelemben csak arra felhatalmazott személyek illetve folyamatok férhetnek hozzá, a token által meghatározott protokollon keresztül.

8. A tokent olyan helyen kell működtetni, ahol nem lehet kitéve erős elektromágneses sugárzásnak, így kikerülve azt, hogy egy rosszindulatú személy megváltoztathassa a token adatait.

III. A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak a Luna CA^3 modul felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

9. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (MinModLen): 1020 bit legyen.

10. DSA aláírási algoritmus használata esetén a minimális p prímhosszúság (pMinLen) 1024 bit, a minimális q prímhosszúság (qMinLen) 160 bit legyen.

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

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

13. 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 (melyet a Luna CA^3 modul támogat), 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,…).
- az alábbi módszerrel:
  - a mentés intelligens kártyákra (tokenekre) történnek,
  - a mentés kódolva van a triple-DES 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.

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

15. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a Luna CA^3 kriptográfiai hardverben) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

16. A Tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes / Hardver verzió: 2, Förmver verzió: 3.102/. Új förmver verzió upgradje 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 NHH biztonságos elektronikus aláírási termék nyilvántartásába.

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 v1.3.1 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

3. számú melléklet
A tanúsításhoz figyelembe vett egyéb dokumentumok

Kérelem a tanúsítás elvégzésére/

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 Generation Services – Protection Profile (CMCKG-PP, HSM-PP)

FIPS 140-1 Validation Certificate No. 214 /Luna CA^3/

Luna® Token Security Policies /Luna CA^3 v3/ Document Number CR-1356

HUNG-TJ-21-2004 Tanúsítási jelentés