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 **Thales e-Security Ltd.** által fejlesztett

nShield F3 6000e /Hw: nC4033E-6K0/,
nShield F3 1500e /Hw: nC4033E-1K5/,
nShield F3 500e /Hw: nC4033E-500/,
nShield F3 10e /Hw: nC4033E-030/,
nShield F3 6000e for nShield Connect /Hw: nC4033E-6K0N/,
nShield F3 1500e for nShield Connect /Hw: nC4033E-1K5N/ és
nShield F3 500e for nShield Connect /Hw: nC4033E-500N/

förmver verzió: 2.38.4-3 és 2.38.7-3

elektronikus aláírási termék

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

minősített vagy nem 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, visszavonási státusz adatok aláírására;

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

Jelen tanúsítvány a HUNG-TJ-069-2014. számú értékelési jelentés alapján került kiadásra.
Készült a Digitoll Informatikai és Szolgáltató Kft. megbízásából.
A tanúsítvány regisztrációs száma: **HUNG-T-069-2014**
A tanúsítás érvényesség kezdete: 2014. december 01.
A tanúsítvány érvényesség vége: 2017. december 01.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 6 oldalon.
Kelt Budapest, 2014. december 01.

PH.

Endrődi Zsolt
Tanúsítási igazgató:

Lengyel Csaba
Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

Az nShield F3 PCIe 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 be, illetve ki rajta.

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 az nShield F3 PCIe kriptográfiai modul család egy elemét egy minősített vagy nem 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. Az nShield F3 PCIe kriptográfiai modul család szolgáltatásait igénybe vevő különböző munkaköröket (nCipher Security Officer, Junior Security Officer, User) betöltő személyek:
   - kompetensek, jól képzettek és megbízhatóak, valamint
   - betartják a különböző útmutatók által leírt, kötelező tevékenységeket.

II. A FIPS 140-2 megfelelőségből fakadó érvényességi feltételek

2. Az nShield F3 PCIe kriptográfiai modul család egy elemét, hogy a FIPS 140-2 3-as biztonsági szintjének megfelelően működjön, az alábbi módon kell inicializálni:

   a. Állítsuk az üzemmód kapcsolót inicializálási pozícióba és indítsuk újra a modult.
   b. A KeySafe grafikus interfész vagy a parancssoros new-world eszközt használatával specifikálni kell az Adminisztrátori kártyakészletben lévő kártyák számát, és a használandó rejtjelezés algoritmust, a Triple-DES-t vagy AES-t. Annak garantálása céljából, hogy a modul 3-as szint üzemmódba kerüljön, az alábbiakat kell tenni:
      - a KeySafe-el válasszuk: „Strict FIPS 140 Mode”=Yes.
      - a new-world-el adjuk meg a –F-et a parancssorban
   c. Az eszköz kéri a kártyákat és minden kártyához a jelszót.
   d. Az összes kártya létrehozása után, állítsuk az üzemmód kapcsolót működési pozícióba, és indítsuk újra a modult.

Amennyiben egy modult 3-as szinten inicializáltak

- a KeySafe megjeleníti a „Strict FIPS 140-2 Mode”=Yes szöveget az modul információs paneljén.
- a parancssoros Enquiry eszköz tartalmazza a StrictFIPS-et a modul állapotjelzői között.

III. A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak az nShield F3 PCIe kriptográfiai modul család felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

3. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (MinModLen): 2048 bit legyen.
4. DSA aláírási algoritmus használata esetén a minimális p prímhosszúság (pMinLen) 2048 bit, a minimális q prímhosszúság (qMinLen) 224 bit legyen.
5. 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.
6. Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet
7. SHA-1 vagy annál gyengébb lenyomatoló algoritmus használata tilos.
8. 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.
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. 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,…).
   - 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.
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 (a 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 (a kriptográfiai modulban) történik, biztosítani kell, hogy a 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 az első oldalon megadott hardver és förmver verzióra érvényes. 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 NMHH biztonságos elektronikus aláírási termék nyilvántartásába.

IV. Egyéb, az érvényességet befolyásoló megjegyzések

14. 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.
15. Nyilvános források között jelenleg nem található olyan információ, mely befolyásolná a modul biztonságos működését. Ezt a vizsgálatot legalább 3 évente szükséges elvégezni.

HUNGUARD

2. számú melléklet
TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK
A követelményeket tartalmazó dokumentumok

Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról

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 Workgroup Agreement: 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. 1197

The nShield security policy / v2.5.4/