TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Miniszterelnöki Hivatalt Vezető Miniszterének 001/2010 számú Kijelölési okiratával kijelölt tanúsító szervezet és mint a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet

tanúsítja,

hogy az **nCipher Corporation Ltd.** által előállított és forgalmazott

nShield F3 500,
nShield F3 500 for netHSM, és
nShield F3 10 PCI

Hardver verziók: nC4033P-500, nC4033P-500N és nC4033P-10, Build Standard N

förmver verziók: 2.33.60-3

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-059-2011. számú értékelési jelentés alapján került kiadásra.
Készült a MÁV INFORMATIKA Zrt. megbízásából.
A tanúsítvány regisztrációs száma: **HUNG-T-059-2011.**
A tanúsítás kelte: 2011. december 15.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2014. december 15.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 8 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató:

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

Az nShield F3 500 kriptográfiai adapter 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 500 kriptográfiai adapter 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. Az nShield F3 500 kriptográfiai adapter 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

Az alábbi feltételek ahhoz elengedhetetlenek, hogy az nShield F3 500, nShield F3 500 for netHSM, és nShield F3 10 modulok megfeleljenek a FIPS 140-2 3-as biztonsági szintjének..

Az nCipher használatára feljogosított alkalmazásnak az alábbi szolgáltatásokat kell végrehajtania.

2. A modul inicializálása

1. Állítsuk az üzemmód kapcsolót inicializálási pozícióba és indítsuk újra a modult.
2. 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

3. Az eszköz kéri a kártyákat és minden kártyához a jelszót.
4. 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 parancsosors Enquiry eszköz tartalmazza a **StrictFIPS**-et a modul állapotjelzői között.

3. A modul visszaállítása gyári állapotba

Ez az állapot törli a Security Officer kulcsát, a modul aláíró kulcsát és minden, betöltött modul kulcsot.

1. Be kell állítani az az inicializációs kapcsolót és újraindítani a modult.
2. Az **Initialise** parancs segítségével el kell érni az Inicializációs állapotot.
3. Egy véletlen értéket kell a Security Officer kulcsának lenyomataként betölteni.
4. A Set Security Officer szolgáltatás segítségével be kell állítani a modul Security Officer kulcsát és a modul működési szabályzatát.
5. Ki kell kapcsolni az inicializációs kapcsolót és újra kell indítani a modult.
6. Ezután a művelet után a modult megfelelően inicializálni kell mielőtt FIPS-jóváhagyott módban lehetne használni.

Az nCipher által biztosított grafikus felhasználói interfész (KeySafe), valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzik.

4. Új felhasználó létrehozása

1. Készíteni kell egy logikai tokent.
2. Ennek a tokennek egy vagy több megosztását szoftver tokenekre kell írni.
3. A felhasználó által igényelt minden kulcs típus esetén, exportálni kell a kulcsot kulcsblobként ezzel a tokennel.
4. Meg kell adni a felhasználó titkos jelszavát és a kulcsblobját.

Az nCipher által biztosított grafikus felhasználói interfész (KeySafe), valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzi.

5. Felhasználó felhatalmazása kulcskészítésre

1. Új kulcsot kell készíteni, olyan hozzáférés ellenőrzési listával (ACL-el), mely csak a **UseAsSigningKey** kapcsolót engedélyezi.
2. Ezt a kulcsot kulcsblobként kell exportálni a felhasználó tokenéhez tartozóan.
3. Az nCipher Security Officer által aláírt tanúsítványt kell generálni, mely
4. tanúsítóként ennek a kulcsnak a lenyomatát tartalmazza;
5. engedélyezi a **GenerateKey** vagy a **GenerateKeyPair** műveleteket attól függően, hogy milyen kulcstípus szükséges;
6. amennyiben a felhasználónak szüksége van kulcstárolásra, engedélyezi a **MakeBlob** műveletet, de kizárólag a saját tokenre.
7. Át kell adni a felhasználónak a kulcsblobját és a tanúsítványát.

Az nCipher által biztosított grafikus felhasználói interfész (KeySafe), valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzi.

6. Felhasználó felhatalmazása Junior Security Officerként való működésre

1. Egy logikai tokent kell generálni, mely védi a Junior Security Officer kulcsát.
2. Ennek a tokennek egy vagy több megosztását szoftver tokenekre kell írni.
3. Egy új kulcspárt kell generálni,
4. melynek titkos kulcsának ACL-je engedélyezi a **Sign** és a **UseAsSigningKey** működést,
5. nyilvános kulcsának ACL-je pedig engedélyezi az **ExportAsPlainText** műveletet.
6. A Junior Security Officer titkos kulcsát kulcsblobként kell exportálni ezen tokenhez tartozóan.
7. A Junior Security Officer nyilvános kulcsát nyílt szövegként kell exportálni. ·
8. Olyan tanúsítványt kell készíteni, melyet az nCipher Security Officerének kulcsával írnak alá, és tartalmazza ennek a kulcsnak a lenyomatát mint tanúsító,
9. engedélyezi a **GenerateKey** és a **GeneratKeyPair** műveleteket,
10. felhatalmaz a **GenerateLogicalToken**, **WriteShare** és a **MakeBlob** tevékenységekre, de ez korlátozható adott modulkulcsra.
11. Át kell adni a Junior Security Officernek a szoftver tokenjét, a jelszavát, a kulcsblobját és a tanúsítványát.

Az nCipher által biztosított grafikus felhasználói interfész (KeySafe), valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzi.

7. A felhasználó azonosítása a tárolt kulcs használatához

1. A **LoadLogicalToken** szolgáltatás segítségével helyet kell csinálni a logikai tokennek.
2. A **ReadShare** szolgáltatás segítségével minden megosztást be kell olvasni a logikai tokenről.
3. A **LoadBlob** szolgáltatás segítségével a kulcsot be kell tölteni a kulcsblobból.
4. A felhasználó ettől a pontttól kezdve minden olyan szolgáltatást el tud érni, mi a kulcs ACL-jében le van írva.
5. A Security Officer szerepkör tölti be ezzel az eljárással a Security Offcier kulcsot. A Security Officer kulcsa ezután használható tanúsítványokban további műveletek engedélyezésére.

Az nCipher által biztosított grafikus felhasználói interfész (KeySafe), valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzi.

8. A felhasználó azonosítása új kulcs készítéséhez

1. Amennyiben a felhasználói token még nincs betöltve, a fenti módon kell azt megtenni.
2. A **LoadBlob** szolgáltatás segítségével kell az engedélyezési kulcsot betölteni a kulcsblobból.
3. A visszakapott **KeyId** segítségével lehet aláírói kulcs tanúsítványt készíteni.
4. A Security Officer tanúsítványával aláírt tanúsítványt kell készíteni a **GenerateKey**, a **GenerateKeyPair** és a **MakeBlob** parancs segítségével.

Az nCipher által biztosított grafikus felhasználói interfész (KeySafe), valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzi.

III. A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak az nShield F3 500 kriptográfiai modul család felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

9. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (MinModLen): 2048 bit legyen.
10. DSA aláírási algoritmus használata esetén a minimális p prímhosszúság (pMinLen) 2048 bit, a minimális q prímhosszúság (qMinLen) 224 bit legyen.
11. 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 –ban leírtaknak.
12. Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet
13. SHA-1 vagy annál gyengébb lenyomatoló algoritmus használata 2012. január 1-e után tilos.
14. A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási információk, illetve ezek kibocsátásához szükséges tanúsítványok aláírására szabad felhasználni.
15. 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.
16. Az időbélyegzéshez használt aláíró kulcsokat csak időbélyegek aláírására szabad használni.
17. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (az nShield F3 500 kriptográfiai adapter modulban) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.
18. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó

eszközön kívül (az nShield F3 500 kriptográfiai adapter modulban) történik, biztosítani kell, hogy az nShield F3 500 kriptográfiai adapter modul és az aláírás létrehozó eszköz között biztonságos útvonal legyen. Ennek az útvonalnak forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával.

19. 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

20. 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.
21. 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 V2.0.0 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/

FIPS 140-2 Validation Certificate No. 966

nShield security policy nShield F3 500, nShield F3 500 for netHSM and nShield F3 10 PCI in FIPS 140-2 level 3 mode /v2.2.3/

nCipher Security Advisory No. 12

nCipher Security Advisory No. 13

nCipher Security Advisory No. 14