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 a **nCipher Corporation Ltd.** által előállított és forgalmazott

nShield F3 Ultrasign PCI /Hw: nC4033P-300/
nShield F3 Ultrasign 32 PCI, /Hw: nC4132P-300/
nCipher F3 PCI for NetHSM, /Hw: nC4032P-300N/
payShield Ultra PCI Hw: /nC4232P-300/
payShield Ultra PCI for NetHSM /Hw: nC4232P-300N/
nShield F3 PCI /Hw: nC4032P-150/
payShield PCI, és /Hw: nC4232P-150/
nShield Lite, /Hw: nC4032P-10/
förmver verzió: 2.22.6-3

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-039-2007. számú értékelési jelentés alapján került kiadásra.
Készült a Microsec Számítástechnikai Fejlesztő Kft. megbízásából.
A tanúsítvány regisztrációs száma: **HUNG-T-039-2007.**
A tanúsítás kelte: 2007. december 13.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2010. december 13.
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 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 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 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 PCI /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ adapter megfeleljen a FIPS 140-2 3-as biztonsági szintjének.

Az nCipher használatára feljogosított alkalmazásnak az alábbi szolgáltatásokat kell végrehajtania.

2. A modul inicializálása

1. Be kell állítani az inicializációs kapcsolót és újra kell indítani a modult.
2. Az Initialise parancs segítségével el kell érni az Inicializációs állapotot.
3. Egy kulcspárt kell generálni, amely a Security Officer kulcsa lesz.
4. Egy logikai tokent kell létrehozni, mely a Security Officer kulcsát védi.
5. Ennek a logikai tokennek egy vagy több megosztását szoftver tokenekre kell írni.

6. A Security Officer magán kulcsát kulcsblobként exportálni kell ezen tokenhez tartozóan.
7. A Security Officer nyilvános kulcsát nyílt szövegként kell exportálni.
8. A Set Security Officer szolgáltatás segítségével be kell állítani a modul Security Officer kulcsát és a működési szabályzatát. A FIPS-140 3-as szintű működéshez legalább a következő állapotjelzőket kell beállítani:
   - · NSOPerms_ops_ReadFile
   - · NSOPerms_ops_WriteFile
   - · NSOPerms_ops_EraseShare
   - · NSOPerms_ops_EraseFile
   - · NSOPerms_ops_FormatToken
   - · NSOPerms_ops_GenerateLogToken
   - · NSOPerms_ops_SetKM
   - · NSOPerms_ops_RemoveKM
   - · NSOPerms_ops_StrictFIPS140
9. A tokeneket és a kulcsblobokat biztonságosan kell tárolni.
   További modul kulcsok generálhatók a felhasználócsoportok megkülönböztetésére.
   Ettől az állapottól kezdve lehet munkakulcsokat generálni és a felhasználó engedélyezést elvégezni.
10. El kell távolítani az inicializációs kapcsolót és újra kell indítani a modult.

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

A KeySafe használatánál be kell állítani a StrictFIPS 140 állapotjelzőt.

A new-world program használatánál a –F kapcsolót kell használni.

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 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 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. E művelet hitelesítést igényelhet.
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 ponttól kezdve minden olyan szolgáltatást el tud érni, amely a kulcs ACL-jében le van írva.

5. A Security Officer szerepkörhöz be kell tölteni ezzel az eljárással a Security Officer 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 által szolgáltatott tanúsítvánnyal meg kell adni ezt a tanúsítványt a GenerateKey, a GenerateKeyPair és a MakeBlob parancsokhoz.

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 kriptográfiai modul család 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. 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 2.0.0 –ben leírtaknak.
12. Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet
13. A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási listák aláírására szabad felhasználni.
14. 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.

15. Az időbélyegzéshez használt aláíró kulcsokat csak időbélyegek aláírására szabad használni.
16. 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 kriptográfiai adapter modulban) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.
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 kriptográfiai adapter modulban) történik, biztosítani kell, hogy az nShield 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.
18. 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 NHH biztonságos elektronikus aláírási termék nyilvántartásába.

IV. Egyéb, az érvényességet befolyásoló megjegyzések

19. 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.
20. 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

2/2002 (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

FIPS 140-2: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-2

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 14167-2:2002 munkacsoport egyezmény: Cryptographic Module for CSP Signing Operation – Protection Profile (CMCSO-PP, HSM-PP)

CEN 14167-3:2003 munkacsoport egyezmény: : Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP, HSM-PP)

FIPS 140-2 Validation Certificate No. 674

The nShield security policy /nShield and payShield modules v2.0.7/