TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 15/2001.(VIII. 27.) MeHVM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 006/2002 számú kijelölési okiratával kijelölt terméktanúsító szervezet

tanúsítja,

hogy az

nCipher Corporation Ltd.

által előállított és forgalmazott

nShield F3 PCI*, *az nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI hardver kriptográfiai modul

hardver verzió: nC4032P-150, nC4032P-300, nC4132P-300, förmver verzió: 2.0.0, 2.0.2.

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, 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.

Jelen tanúsítvány a HUNG-TJ-013-2003. számú tanúsítási jelentés alapján került kiadásra.
Készült a Hewlett-Packard Magyarország Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-013/2004.**
A tanúsítás kelte: 2004. március 17.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2007. március 17.
Mellékletek: feltételek, követelmények, dokumentumok, összesen: 8 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

Az nShield F3 PCI /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ adapter 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 PCI /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ adaptert 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 PCI /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ kriptográfiai modul szolgáltatásait igénybe vevő különböző munkaköröket (nCipher Security Officer, Junior Security Officer, User) betöltő személyek:
   - kompetensek, jól képzettek és megbízhatóak, valamint
     - betartják a különböző útmutatók (Getting Started Guide, nShield User Guide) által leírt, kötelező tevékenységeket.

II. A FIPS 140-1 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 által engedélyezett alkalmazásnak el kell végeznie a következő szolgáltatásokat, melyekről részletesen az nCipher Security Officer's Guide-ban és a Technical Reference Manualban lehet olvasni.

2. A modul inicializálása

1. Be kell állítani az inicializációs kapcsolót és újraindítani a modult.
2. Az Initialise parancs segítségével el kell érni az Inicializációs állapotot.
3. Egy kulcspárt kell generálni, mely a Security Officer kulcs lesz.
4. Egy logikai tokent[1] kell generálni, mely a Security Officer kulcsát védi.
5. Ennek a logikai tokennek egy vagy több megosztását fizikai vagy szoftver tokenekre (pl. smart card) kell írni.
6. A Security Officer titkos kulcsát key blobként[2] 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 level 3 szintű működéshez legalább a következő jelzőket be kell állítani:
    - 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 key blobokat biztonságosan kell tárolni
10. További modul kulcsok generálhatók a felhasználócsoportok megkülönböztetésére.
11. Ettől kezdve lehet munkakulcsokat generálni és a felhasználó engedélyezést elvégezni.
12. Ki kell kapcsolni az inicializációs kapcsolót és újraindítani a modult.

Megjegyzés: az nCipher grafikus programja, a KeySafe, valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzik.

- A KeySafe használatánál be kell állítani a StrictFIPS 140 jelzőt.
- 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 modulban tárolt kulcsot.

[1] Logikai token: egy 3DES kulcs, mely a key blobokat védi.
[2] Key blob: az nShield modul a merevlemezen titkosított formában tárolja a kulcsokat. Ezt a formát key blobnak hívják.

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 működési szabályzatát.
5. Ki kell kapcsolni az inicializációs kapcsolót és újraindítani a modult.

Ezen működés után a modult megfelelően inicializálni kell, mielőtt FIPS módban működhetne.

Megjegyzés: az nCipher grafikus programja, a KeySafe, valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzik.

4. Új felhasználó létrehozása

1. Egy logikai tokent kell készíteni.
2. Ennek a tokennek egy vagy több megosztását hardver vagy szoftver tokenekre kell írni.
3. Minden kulcsot, mely szükséges a felhasználónak, key blobként exportálni kell ezen tokenekhez tartozóan.
4. Meg kell adni a felhasználó titkos jelszavát és a key blobját.

Megjegyzés: az nCipher grafikus programja, a KeySafe, valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzik.

5. Felhasználó felhatalmazása kulcskészítésre

1. Új kulcsot kell készíteni, olyan Access Control List[3] (ACL) alatt, mely engedélyezi a UseAsSigningKey kapcsolót. Ezt csak felhatalmazott felhasználó engedélyezheti.
2. Ezt a kulcsot key blobként kell exportálni a felhasználó tokenéhez tartozóan.
3. Az nCipher Security Officer által aláírt tanúsítványt kell generálni, mely
   - tanúsítóként ennek a kulcsnak a lenyomatát tartalmazza,
   - engedélyezi a GenerateKey vagy a GenerateKeyPair működéseket attól függően, hogy mely kulcstípus szükséges,
   - amennyiben a felhasználónak szüksége van kulcstárolásra, engedélyezi a MakeBlob működést, de kizárólag a saját tokenjeikre.
4. Át kell adni a felhasználónak a key blobját és a tanúsítványát.

Megjegyzés: az nCipher grafikus programja, a KeySafe, valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzik.

6. Felhasználó felhatalmazása Junior Security Officerként való működésre

1. Egy logikai tokent kell generálni, mely védi a Junior Security Officer kulcsát.

[3] Access Control List: meghatározza, hogy milyen kulccsal milyen kriptográfiai művelet hajtható végre.

2. Ennek a tokennek egy vagy több megosztását hardver vagy szoftver tokenekre kell írni.
3. Egy új kulcspárt kell generálni,
    - melynek titkos kulcsa olyan ACL-ben van, mely engedélyezi a Sign és a UseAsSigningKey működést,
    - nyilvános kulcsa pedig olyan ACL-ben van, mely engedélyezi az ExportAsPlainText működést.
4. A Junior Security Officer titkos kulcsát key blobként kell exportálni ezen tokenhez tartozóan.
5. A Junior Security Officer nyilvános kulcsát nyílt szövegként kell exportálni.
    - Olyan tanúsítványt kell készíteni, melyet az nCipher Security Officerének kulcsával írnak alá, és tartalmazza ennek a kulcsnak a lenyomatát, mint tanúsító,
    - felhatalmaz a GenerateKey és a GeneratKeyPair működésre,
    - felhatalmaz a GenerateLogicalToken, WriteShare és a MakeBlob működésre, de csak bizonyos modulkulcsokra vonatkozólag.
6. Át kell adni a Junior Security Officernek a szoftver tokenjét, a jelszavát, a key blobját és a tanúsítványát.

Megjegyzés: az nCipher grafikus programja, a KeySafe, valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzik.

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 key blobba.
4. A felhasználó innentől minden olyan szolgáltatást el tud érni, mi a kulcs ACL-jében le van írva.

Megjegyzés: az nCipher grafikus programja, a KeySafe, valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzik.

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 a felhatalmazott kulcsot betölteni a key blobból.
3. A 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.

Megjegyzés: az nCipher grafikus programja, a KeySafe, valamint a new-world parancssori program ezeket a lépéseket automatikusan elvégzik.

III. A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak az nShield /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ 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 az nShield F3 PCI /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ 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 (az nShield F3 PCI /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ kriptográfiai hardverben) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

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 F3 PCI /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ kriptográfiai modulban) történik, biztosítani kell, hogy az nShield F3 PCI /nShield F3 Ultrasign PCI és az nShield F3 Ultrasign 32 PCI/ kriptográfiai modul és az aláírás létrehozó eszköz között biztonságos útvonal legyen. Ennek az útvonalnak forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával.

17. A Tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes /hardver verzió: nC4032P-150, nC4032P-300, nC4132P-300, förmver verzió: 2.0.0, 2.0.2./. 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

16/2001. (IX.1.) MeHVM 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 Policy Requirements for Certification Authorities Issuing Qualified Certificates

CEN 14167-1 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/

Kérdőív a tanúsítás kérelmezéséhez

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

FIPS 140-2 Validation Certificate No. 297 /nShield F3 PCI Cryptographic Adapter/

The nShield modules security policy /nShield F3 PCI, nshield F3 PCI Ultrasign v1.2.40/

Getting Started Guide /Version: 4.1.53, Date: 26 July 2002/

nShield User Guide Windows /Version: 4.7.51, Date: 1 August 2002/

Microsoft Windows Server 2003 PKI and deploying the nCipher nShield Hardware Security Module /Version: 1.0, Date: 15 December 2003/