# 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
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 for netHSM
kriptográfiai hardver eszköz

**tanúsítás tárgyát képező verziója:**

Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3

**elektronikus aláírási termék**
*az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén*

## megfelel

**a 2001. évi XXXV. törvényben szereplő**
**minősített elektronikus aláírások létrehozására alkalmazható**

**„3-as típusú biztonságos aláírás-létrehozó eszköz”-nek.**

Jelen tanúsítvány a HUNG-TJ-062-2013 számú tanúsítási jelentés alapján került kiadásra.
Készült a Mezőgazdasági és Vidékfejlesztési Hivatal megbízásából.
A tanúsítvány regisztrációs száma: **HUNG-T-062-2013.**
A tanúsítás kelte: 2013. szeptember 23.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2016. szeptember 23.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 7 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató:

Lengyel Csaba
Ügyvezető igazgató

# 1. számú melléklet

## A tanúsítvány érvényességi feltételei

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a Tanúsítvány érvényességének.

Feltételek az előkészítés szakaszában:

1. Inicializálás során az alábbi lépéseket kell elvégezni:
   a) Gyári alapállapotba hozás (Initialise)
   b) Firmware verzió ellenőrzése (New Enquiry, elvárt verziószám 2.33.60)
   c) Hosszú távú kulcs generálása (Generate KLF).
   d) Hosszú távú kulcs nyilvános felének exportálása (GetLongTermKey)

2. A Security World létrehozása során az alábbi opciókat kell beállítani:

| | |
|---|---|
| • Cipher suite: AES | key blobok titkosítása AES-sel |
| • Key recovery: No | nincs kulcs helyreállítás |
| • ACS (K and N): (N=K=2) | titokmegosztás van a 2 NSO (adminisztrátor) között |
| • pass phrases: YES | az adminisztrátor hitelesítéséhez jelmondat is kell |
| • FIPS 140-2 level 3 compliance: YES | FIPS 140-2 level 3 üzemmód |
| • FTO: NO | csak nCipher kártya használható |
| • Remote Operator: YES | az aláírónak távolról is hozzá kell férnie a netHSM-hez |
| • OCS replacement: NO | NSO ne tudjon magánkulcsot menteni, klónozni, átruházni |
| • Pass phrase replacement: NO | NSO ne tudjon jelmondatot visszaállítani |
| • Nonvolatile memory (NVRAM) options: NO | a key-blob tárolható a kriptográfiai hardver eszközön kívül |
| • Security World SEE options: NO | az SEE (nCipher Secure Execution Engine) használatának tiltása |
| • Real-time clock (RTC) options: NO | az RTC (Real-time clock) használatának tiltása |
| • Security World replacement options: NO | NSO ne tudjon Security World-öt-t klónozni |

3. Az Operator Card Set-ek (OCS) létrehozása a kártyatulajdonosok (operátorok, aláírók) jelenlétében az alábbi beállításokkal történjen:

| | |
|---|---|
| • OCS (K and N): (N=K=1) | nincs titokmegosztás az aláíróknál |
| • pass phrases: YES | hitelesítéshez jelmondat is kell |
| • formal FIPS 140-2 level 3 compliance: YES | FIPS 140-2 level 3 üzemmód |
| • OCS persistent: YES | csak olvasóba helyezett kártya mellett lehet aláírást kezdeményezni |
| • remotely-readable: YES vagy NO | YES esetén a kártya távolról is olvasható |
| • Time-outs: nincs feltétel | |
| • pass phrase replacement: NO | az NSO ne állíthassa vissza az aláíró jelmondatát |
| • felhatalmazás kulcspár generálására | NSO tanúsítvánnyal engedélyt ad |

4. Amennyiben az OCS létrehozása során engedélyezésre került a távoli kártya olvasás (remotely-readable: YES) akkor miniHSM alkalmazása szükséges az aláírói végponton. Az alkalmazott miniHSM-re teljesülniük kell az alábbiaknak:

- érvényes FIPS 140-2 level 3 szerinti tanúsítvánnyal rendelkezzen,
- a jelen tanúsítvány tárgyát képező HSM verzióval (nShield F3 500 for netHSM, hardver verzió: nC4033P-500N, förmver verzió: 2.33.60-3) kliens üzemmódban együttműködésre képes szoftver/förmver verzióval legyen ellátva.

5. A létrehozott operátorok (aláírók) kulcspár generálása az alább lépésekből álljon:

a) Kulcspár generálás /cél: aláírás, aktivizáló: kizárólag saját maga, algoritmus: RSA, kulcsméret: minimum 2048, key recovery: nem/,
b) Nyilvános kulcs exportálása,
c) QCA-hoz továbbítás /vagy az aláíró viszi be személyesen a nyilvános kulcsát, vagy egy RO személyesen felügyeli a nyilvános kulcs exportálását/,
d) A QCA ellenőrzi a nyilvános kulcs hitelességét /azaz a nyilvános kulcs sértetlen, az aláíró rendelkezik a nyilvános kulcshoz tartozó, megfelelő magánkulccsal, a kulcspárt egy BALE generálta /,
e) A QCA minősített tanúsítványt generál /amely tartalmazza többek között az aláíró nevét, a nyilvános kulcsot, a QCA fokozott biztonságú aláírását/,
f) A generált minősített tanúsítvány visszajuttatása az aláíró szoftverhez.

6. A 2-es feltételben szereplő ACS titokmegosztás ( ACS (K and N): N=K=2) érvényesítése az alábbi módon történjen:

- az egyik NSO kártyája és jelmondata az üzemeltetőknél marad,
- a másik NSO kártyája és leírt, borítékba zárt jelmondata egy közjegyzőhöz kerül, a szükséges OCS-ek létrehozását és legenerálását követően haladéktalanul, az auditor jelenlétében.

7. Amennyiben a jövőben új aláírói végpont (miniHSM) telepítésére lesz szükség, a titokmegosztás érvényesítése az alábbi módon történhet:
- az auditor jelenlétében felveszik a közjegyzőtől a második NSO kártyát és a hozzá tartozó jelmondatot tartalmazó borítékot,
- az auditor jelenlétében és a két NSO közreműködésével megtörténik az új aláírói végpont létrehozása,
- a második NSO kártyája és leírt, borítékba zárt jelmondata haladéktalanul visszakerül a közjegyzőhöz, az auditor jelenlétében.

8. Az nShield F3 500 for netHSM készüléken, illetve az alkalmazott miniHSM-en az auditor (ld. 19. feltétel) helyezzen el az eszköz felnyitását egyértelműen bizonyító, egyedi azonosítóval rendelkező „tamper-detecting" jelzést.

Feltételek az aláíró szoftver oldalán:

9. Az nShield F3 500 for netHSM-et meghívó (a környezet részét képező) aláíró szoftver kezelje le az nShield F3 500 for netHSM által visszajelzett sikertelen hitelesítési kísérleteket, és kényszerítse ki az alábbiakat:
- az első sikertelen kísérlet után iktasson be egy *t* (*t* konfigurálható vagy fix, legalább 1 sec értékű) késleltetést a következő kísérlet felkínálásáig,
- minden későbbi sikertelen kísérlet után növelje kétszeresére ezt a késleltetést,
- sikeres hitelesítés után állítsa vissza *t* alapértékét.

10. A környezet részét képező aláíró szoftver kényszerítse ki, hogy a jelmondat legalább 8 karakterből álljon, valamint betűt és számot is tartalmazzon.

11. A környezet részét képező aláíró szoftver:
- ellenőrizze, hogy a gyártó által szállított PKCS#11 vagy egyéb (Microsoft CSP, Java) driver-rel kommunikál,
- készítse el az aláírandó adatként bemutatott adat DTBS-reprezentációját (legalább SHA256 vagy SHA512 hash képét) a netHSM által aláírásra alkalmas formában,
- továbbítsa a DTBS-reprezentációt a netHSM felé,
- csatolja a netHSM által előállított aláírást az adathoz.

12. A környezet részét képező aláíró szoftver:
- minden aláírandó dokumentum csomag indítása esetén kötelezően kérje be az OCS jelszót, és authentikálja az OCS-t (ezen keresztül az aláírót), és ha az OCS nincs jelen, ne induljon el (azaz minden csomag indítása előtt kötelezően új munkamenetet építsen fel),
- az aláírások elkészültét követően azonnal szakítsa meg a munkamenetet a netHSM-mel.

Feltételek a működtetés szakaszában:

13. Az nShield F3 500 for netHSM környezete olyan fizikai védelem alatt álljon, mely megakadályozza a bekapcsolt, működő nShield F3 500 for netHSM speciális eszközökkel való manipulálását, fizikai támadását.
Amennyiben a netHSM (például lopás miatt) kikerül ebből a védett környezetből, valamennyi a rendszerben generált magánkulcshoz tartozó aláíró tanúsítványt haladéktalanul vissza kell vonatni, a netHSM-et pedig újra kell inicializálni.

14. A netHSM készüléken vagy a miniHSM-en az auditor által elhelyezett „tamper-detecting" jelzés sértetlenségét rendszeresen ellenőrizni kell. Amennyiben a jelzés sérült, a rendszer által kezelt aláíró kulcsokhoz tartozó tanúsítványokat vissza kell vonni, és magát az eszközt újra kell inicializálni.

15. Az aláíró vigyázzon a hitelesítéséhez szükséges eszközére (nCipher smart card), kizárólag a miniHSM-hez vagy az nShield F3 500 for netHSM-hez való hozzáféréskor használja azt, védett környezetben. Az aláírások jóváhagyását, az aláírások megkezdését követően haladéktalanul vegye ki az olvasóból, és tartsa személyes felügyelete alatt. Amennyiben a hitelesítéshez szükséges eszköz kikerül az aláíró ellenőrzése alól, az általa generált magánkulcshoz tartozó tanúsítványt haladéktalanul vissza kell vonatnia.

16. Az aláíró vigyázzon a hitelesítéséhez szükséges tudására (pass phrase), értékét senkinek se fedje fel, illetve a OCS-t biztonságos helyen őrizze.

17. Az aláíró magánkulcsok key blob-ok formájában, AES256-tal titkosítva vannak tárolva az nShield F3 500 for netHSM-en kívül. Amennyiben egy ilyen key blob helyreállíthatatlanul megsemmisül, új magánkulcsot kell generálni, a megsemmisült kulcshoz tartozó tanúsítványt pedig vissza kell vonatni.

18. A minősített aláírások létrehozására használt magánkulccsal kizárólag minősített elektronikus aláírást szabad létrehozni.

19. Az nShield F3 500 for netHSM eszközzel csak olyan rendszerben lehet minősített elektronikus aláírást előállítani, amely rendszer jelen tanúsítványban lévő 1.-12. feltételeknek való megfelelését az informatika biztonsági szakterület jogszabályban rögzített vagy nemzetközi mértékadó követelményen alapuló technológiai értékelési követelményrendszere alapján

- akkreditált értékelő szervezet a megfelelő akkreditált eljárásrendben értékelte, és
- ennek alapján akkreditált tanúsító szervezet a megfelelő akkreditált eljárásrendben tanúsította.

# 2. számú melléklet
## TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK
## A követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

Az Európai Parlament és Tanács 1999/93/EK Irányelv (1999. december 13.) az elektronikus aláírásra vonatkozó közösségi keretfeltételekről.

CWA 14169, Secure signature-creation devices “EAL 4+”, March 2004

CWA 14355, Guidelines for the implementation of Secure Signature-Creation Devices, March 2004

Protection Profile — Secure Signature-Creation Device - Type 3, March 2004 (Prepared By: ESIGN Workshop - Expert Group F)

# 3. számú melléklet
## A tanúsításhoz figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

nShield F3 500 for netHSM biztonságos aláírás-létrehozó eszköz /Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3/ ÉRTÉKELÉSI JELENTÉS v1.0 /netHSM_SSCD_ETR_v1.0.doc/

FIPS 140-2 Validation Certificate –nShield F3 500, nShield F3 500 for NetHSM and nShield F3 10 PCI by nCipher Corporation Ltd. (When operated in FIPS mode) 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 Version: 2.2.3 3 June 2008

nCipher Security Officer's Guide

Technical Reference Manual

nCipher netHSM Technical Architecture – White Paper

nShield – User Guide for Windows Version: 7.1