# TANÚSÍTVÁNY
# FELÜLVIZSGÁLATI JEGYZŐKÖNYV

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft (1123 Budapest, Kékgolyó u. 6.) a 9/2005. (VII.21.) IHM rendelet alapján, mint a Nemzeti Fejlesztési Minisztérium IKF/1262-1/2016-NFM számú Kijelölési okiratával kijelölt tanúsító szervezet

tanúsítvány felülvizsgálati eljárás keretében megvizsgálta a

HUNG-T-062-2013 TANÚSÍTVÁNYBAN

foglaltakat, és a mellékletben szereplő érvényességi feltételek teljesítése mellett

**az nCipher Corporation Ltd.**

által előállított és forgalmazott

**nShield F3 500 for netHSM**

kriptográfiai hardver eszköz termék tanúsítás tárgyát képező

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

**mint elektronikus aláírási termék megfelelőségére vonatkozó**

HUNG-T-062-2013 tanúsítványának érvényességét

- figyelembe véve a tanúsítás óta eltelt időszakban nyilvános forrásokban megjelent információkat, valamint a jogbiztonságból adódó elvárásokat -

kiterjeszti 2019. szeptember 23-ig.

A Tanúsítvány Felülvizsgálati Jegyzőkönyv regisztrációs száma: **HUNG-FJ-062/1-2016**

*Kelt: Budapest, 2016. június 20.*

PH.

Endrődi Zsolt
Tanúsítási igazgató

Szűcs Ákos Balázs
Ügyvezető igazgató

# 1. számú melléklet

## Érvényességi feltételek

### 1. Korábbi feltételek érvényessége

Teljesítendő a HUNG-T-062-2013 számú tanúsítvány 1. számú mellékletében szereplő, a biztonságos felhasználásra vonatkozó feltételrendszer.

### 2. Új feltétel

A multifunkciós (elektronikus aláírás létrehozás, - ellenőrzés, kulcs-generálás, kulcsvédelem,…) nShield F3 500 for netHSM termék elektronikus aláírási kulcspár generálására 2016. június 20-tól 2019. szeptember 23-ig maximum 20 db. RSA2048 kulcspár generálása engedélyezett.

Az eszközzel – mint tanúsított termékkel – 2016. június 20-tól új rendszer implementálása nem megengedett.

**Indokolás**

A HUNG-T-062-2013 számú tanúsítvány alapjául szolgáló Tanúsítási jelentés felhasználta az nShield F3 500 for netHSM termék 966-os számú FIPS 140-2 tanúsítását. A felhasznált FIPS tanúsítvány 2016.01.31-én átkerült a „Historical List[1]" nyilvántartásba azzal a kikötéssel, hogy a véletlenszám generálása 2016-tól nem felel meg a módosított követelményeknek. A termék Security Policy dokumentuma tartalmazza, hogy az RNG algoritmusa FIPS-186-2 -nek megfelelő. A korlátozó előírás összhangban van a SP-800-131A Revision1 (Nov. 2015) dokumentummal, (ld. Table 3.), mely elavultnak, majd nem engedélyezettnek minősíti a nevezett RNG algoritmusokat (általános felhasználásra). A nyilvánosan elérhető információk között nem elérhetők konkrét gyengeségek.

A „Historical List" bevezetőjében szerepel, hogy az eszköz használatát a szervezetek kockázati megítélésére bízza. Kockázat-értékelésünk szerint kevés számú véletlen bit generálására az eszköz megfelelő.

A fenti indokok miatt került korlátozásra a termékkel generálható RSA2048 bites kulcsok száma, és az új rendszerben való alkalmazhatóság.

[1] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-historical.htm