



TANÚSÍTVÁNY FELÜLVIZSGÁLATI Jegyzőkönyv

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

Tanúsítvány felülvizsgálati eljárás keretében
megvizsgálta

a **HUNG-T-056-2011 TANÚSÍTVÁNYBAN**

foglaltakat, és annak tartalmát összevetette az NMHH által kibocsátott EF-26838-8/2011, EF-26838-9/2011, EF-26838-10/2011, EF-26838-11/2011, EF-26838-12/2011, EF-26838-13/2011 határozataiban foglalt új követelményekkel.

Megállapítja, hogy:

a **nCipher Corporation Ltd.** által fejlesztett

**nShield F3 Ultrasign 32 SCSI,
nShield F3 Ultrasign SCSI,
payShield SCSI és
payShield Ultra SCSI**

**Hardver verziók: nC4032W-150, nC4132W-400,
nC4032W-400, nC4232W-150 és nC4232W-400
firmver verzió: 2.18.15-3**

elektronikus aláírási termék

hitelesítés szolgáltatásra való felhasználási feltételei az alábbiakban módosul

1. SHA-1 vagy annál gyengébb lenyomatoló algoritmus használata 2012 január 1-e után tilos
2. RSA aláírási algoritmus használata esetén a minimális modulus ajánlott mérete (MinModLen) 2048 bit
3. DSA aláírási algoritmus használata esetén az ajánlott minimális p prímhosszúság (pMinLen) 2048 bit, a minimális q prímhosszúság (qMinLen) 224 bit

A Tanúsítvány Felülvizsgálati Jegyzőkönyv regisztrációs száma: **HUNG-FJ-056/1-2011**

Kelt: Budapest, 2011. december 15.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató