TANÚSÍTVÁNY KARBANTARTÁS Jegyzőkönyv

HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Miniszterelnöki Hivatalt Vezető Miniszterének 001/2010 számú Kijelölési okiratával kijelölt tanúsító szervezet

Tanúsítvány karbantartás eljárás keretében

a **HUNG-T-037-2007 TANÚSÍTVÁNY állításait**

kiterjeszti

a

NetLock Hálózatbiztonsági és Informatikai Szolgáltató Kft.

által továbbfejlesztett alábbi verzióra:

NCA TWS megbízható rendszer hitelesítés-szolgáltatáshoz v2.9.0

a fent nevezett tanúsítvány
1. számú mellékletében áttekintett funkcionalitással, valamint
a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vétele mellett.

A Karbantartási Jegyzőkönyv regisztrációs száma: **HUNG-TK-037/2-2010**
Kelt: Budapest, 2010. május 31.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

Az NCA v2.9.0 és a HUNG-T-037-2007 tanúsítványban szereplő 2.6.0-ás verzió közötti jelentősebb bővülések

Operációs rendszer

A szerver (NCAADM) és a kliensek (NCACLI USR és NCACLI ADM) az értékelt kiépítésekben az alábbi operációs rendszereken futottak:

2.6.0-ás verziótól:

Ssz	Operációs rendszer
1	MS Windows XP SP2
2	Solaris 9
3	Slackware 10.1 (Linux)

2.9.0-ás verziótól:

Ssz	Operációs rendszer
4	Windows Server 2003 R2 Standard Edition Service Pack 2
5	Solaris 10 (Opensolaris SunOS opensolaris 5.11 snv_125 sun4u sparc sun4u)
6	CentOS 5.4 (Linux 2.6.18-164.11.1.el5PAE #1 SMP Wed Jan 20 08:16:13 EST 2010 i686 i386 GNU/Linux, a CentOS által karban tartott biztonsági frissítésekkel)

HSM

Az NCA rendszer képes együttműködni az informatikai környezet részét képező FIPS 140 szerint tanúsított kriptográfiai hardver modulokkal. Az értékelt kiépítésekben az alábbi kriptográfiai hardver modulokkal működött együtt:

2.6.0-ás verziótól:

Ssz	HSM
1	PSO - ProtectServer Orange (Eracom CSA 8000, Hardware 71.00 (G), HSM middleware: Cprov 3.10 CSA8000 PKCS11 felület)

2.9.0-ás verziótól:

Ssz	HSM
2	PSG - ProtectServer Gold (Safenet PSG, Hardware 66.00 (B), Firmware 2.04, HSM middleware: Cprov 3.30 PSG PKCS11 felület)
3	LUNA- Safenet LUNA PCI HSM (Firmware 4.6.1, HSM middleware: Chrystoki/0.6 LUNA PKCS11 felület)

Kriptográfiai algoritmusok

Az NCA rendszer az alábbi jóváhagyott kriptográfiai algoritmusokat támogatja:

2.6.0-ás verziótól:

Ssz	Kriptográfiai algoritmus	Felhasználási terület	azonosító / minimális kulcshossz	Támogatás	Szabvány
1	SHA1	lenyomat generálás	-	openssl	FIPS 180-2
2	RSA	végfelhasználói aláírás	1024 bit	PSO HSM	FIPS 180-2
3	RSA	Root CA által kiadott CA tanúsítványok / CA által kiadott végfelhasználói tanúsítványok / időbélyeg válaszok / OCSP válaszok aláírása és ellenőrzése	2048 bit	PSO HSM	FIPS 186-2
4	DES, 3DES	titkosítás és dekódolás	56/168 bit	PSO HSM	FIPS 186-2
5	AES	titkosítás és dekódolás	128 bit	PSO HSM	FIPS 197

2.9.0-ás verziótól:

Ssz	Kriptográfiai algoritmus	Felhasználási terület	azonosító/ minimális kulcshossz	Támogatás	Szabvány
6	SHA256	lenyomat generálás	-	openssl	FIPS 180-2
7	ECC	végfelhasználói aláírás	secp224r1 (RSA hossz megfeleltetés: 2048 bit)	PSG HSM LUNA HSM	FIPS 186-2
8	ECC	Root CA által kiadott CA tanúsítványok / CA által kiadott végfelhasználói tanúsítványok / időbélyeg válaszok / OCSP válaszok aláírása és ellenőrzése	sect283r1 (RSA hossz megfeleltetés: 3456 bit)	LUNA HSM	FIPS 186-2
9	ECC	Root CA által kiadott CA tanúsítványok / CA által kiadott végfelhasználói tanúsítványok / időbélyeg válaszok / OCSP válaszok aláírása és ellenőrzése	secp384r1 (RSA hossz megfeleltetés: 7680 bit)	PSG HSM	FIPS 186-2