CERTIFICATE MAINTENANCE RECORD

HUNGUARD Informatics and IT R&D and General Service Provider Ltd as a certification authority assigned by the assignment document No. 001/2010 of the Minister of the Prime Minister's Office of the Republic of Hungary based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

in Certificate Maintenance Process

extends

the claims of the T-037-2007 CERTIFICATE
for the following version developed by

NetLock Informatics and Network Privacy Services Ltd

NCA TWS trustworthy system for Certification Service Provider services v2.9.0

with the functionality listed in annex 1 and
with the secure usage conditions contained in annex 2
of the referenced certificate.

Registration number of the Maintenance Record: **HUNG-TK-037/2-2010**

Budapest, 31 May 2010

PH.

Endrődi Zsolt Certification director	dr. Szabó István Managing director

Annex

Significant differences between this NCA version 2.9.0 and version 2.6.0 registered in HUNG-T-037-2007

Operating system

In the evaluated configurations the server (NCAADM) and clients (NCACLI USR and NCACLI ADM) have been executed on the following operating systems:

From version 2.6.0:

	Operating system
1	MS Windows XP SP2
2	Solaris 9
3	Slackware 10.1 (Linux)

From version 2.9.0:

	Operating system
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, with security patch provided by CentOS)

HSM

The NCA system is able to cooperate with cryptographic hardware modules certified according to FIPS 140, which belong to the IT environment. In the evaluated configurations the NCA version 2.9.0 have operated with the following cryptographic hardware modules:

From version 2.6.0:

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

From version 2.9.0:

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

Cryptographic algorithms:

The NCA supports the following approved cryptographic algorithms:

From version 2.6.0:

	Cryptographic algorithm	Usage	ID/minimal key length	Support	Standard
1	SHA1	hash generation	-	openssl	FIPS 180-2
2	RSA	end user signature	1024 bit	PSO HSM	FIPS 180-2
3	RSA	CA certificates issued by Root CA/ End user certificates issued by CA/ Signing and verifying time-stamp responses/ OCSP responses	2048 bit	PSO HSM	FIPS 186-2
4	DES, 3DES	encryption and decryption	56/168 bit	PSO HSM	FIPS 186-2
5	AES	encryption and decryption	128 bit	PSO HSM	FIPS 197

From version 2.9.0:

	Cryptographic algorithm	Usage	ID/minimal key length	Support	Standard
6	SHA256	hash generation	-	openssl	FIPS 180-2
7	ECC	end user signature	secp224r1 (complying with RSA length 2048 bit)	PSG HSM LUNA HSM	FIPS 186-2
8	ECC	CA certificates issued by Root CA/ End user certificates issued by CA/ Signing and verifying time-stamp responses/ OCSP responses	sect283r1 (complying with RSA length 3456 bit)	LUNA HSM	FIPS 186-2
9	ECC	CA certificates issued by Root CA/ End user certificates issued by CA/ Signing and verifying time-stamp responses/ OCSP responses	secp384r1 (complying with RSA length 7680 bit)	PSG HSM	FIPS 186-2