CERTIFICATE REVIEW RECORD

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. IKF/19519-2/2012-NFM of the Ministry of National Development based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21) and as a product certification authority accredited by the National Accreditation Body by the document No. NAT-6-0048/2011

in Certificate Review Process
examined
the statements included in the
CERTIFICATE
HUNG-T-037-2007
and its supplementary documents:
HUNG-TK-037/1-2009,
HUNG-TK-037/2-2010 and
HUNG-TK-037/3-2012
Certificate Maintenance Records and states the following:

NCA TWS trustworthy system for Certification Service Provider services v2.10.1

developed by

NETLOCK Informatics and Network Privacy Services Ltd.

has been under permanent assurance maintenance during the certification period and evidence submitted due to modifications justified that the validity of the certificate can be extended. Thus the certification authority
extends the validity of the certificate referenced above until 27 August, 2016
maintaining functionality described in Annex 1 and considering terms regarding the secure usage conditions in Annex 2 of the certificate.
This certificate applies to v2.6.0, v2.8.1, v2.9.0 and v2.10.1 versions of NCA TWS.
Registration number of this Certificate Review Record: **HUNG-FJ-037/2-2013**
Budapest, 15 August, 2013

LS

Endrődi Zsolt	Lengyel Csaba
Certification director	Managing director

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) and as a product certification authority accredited by the National Accreditation Body by the document No. NAT-6-0048/2011

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 v2.10.1

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-037/3-2012**

Budapest, 14 March 2012

PH.

Endrődi Zsolt Certification director	dr. Szabó István Managing director

CERTIFICATE REVIEW 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 Review Process
examined
the statements included in the
CERTIFICATE
HUNG-T-037-2007
and its supplementary documents:
HUNG-TK-037/1-2009
HUNG-TK-037/2-2010
Certificate Maintenance Records and states the following:

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

developed by

NETLOCK Informatics and Network Privacy Services Ltd.

has been under permanent assurance maintenance during the certification period and evidence submitted due to modifications justified that the validity of the certificate can be extended.
Thus the certification authority extends the validity of the certificate referenced above until 27 August, 2013
maintaining functionality described in Annex 1 and considering terms regarding the secure usage conditions in Annex 2 of the certificate.

Registration number of this Certificate Review Record: **HUNG-FJ-037/1-2010**
Budapest, 27 August, 2010

LS

Endrődi Zsolt	dr. Szabó István
Certification director	Managing director

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

CERTIFICATE MAINTENANCE RECORD

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 113/2007 of the Minister of the Ministry of Economy and Transport 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 v2.8.1

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-037/1-2009**

Budapest, 25 February 2009

PH.

Endrődi Zsolt Certification director	dr. Szabó István Managing director

CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 113/2007 of the Minister of the Ministry of Economy and Transport of the Republic of Hungary
based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

certifies

that the

NCA TWS trustworthy system for Certification Service Provider services v2.6.0

developed by

NETLOCK Informatics and Network Privacy Services Ltd.

with functionality laid down in Annex 1
and with the secure usage conditions listed in Annex 2

passes the requirements

for applications operating in trustworthy system for qualified certification service provider and for not qualified certification service provider, according to the Act XXXV of 2001.

This certificate has been issued on the basis of the certification report No. HUNG-TJ-037-2007.
Produced on commission of NETLOCK Informatics and Network Privacy Services Ltd.

Certificate registration number: **HUNG-T-037-2007.**
Date of certificate: 27.08.2007.
Validity period of the certificate: 27.08.2010.
Annexes: attributes, conditions, requirements and other features on six pages.

L.S.

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Summary of the main features of NCA v2.6.0

The NCA v2.6.0 (NCA system) is a specific electronic signature product that provides different functions regarding certification services.

NCA system v2.6.0 receives service messages and commands from calling applications, checks their permissions (if applicable) and executes them. The system supports the following certification services:

Core services (in all modes of operation):

- Registration service,
- Certificate generation service,
- Certificate dissemination service,
- Revocation management service (CRL, OCSP),
- Revocation status information service.

Supplementary services (in certain modes of operation):

- Time-stamping service,
- General signature service (GSU),
- Key escrow for encrypting private keys service,
- Key recovery for encrypting private keys service.

The NCA system is capable of executing the requests for certificate issuance based on checks and process control commands defined in its configuration, with or without human interference. It is also capable of handling the whole life cycle of requests and later of certificates, from the registration of request (pre-request), through the key generation and compilation of data in the checked certificate (pre-certificate) to the certificate issuance, and suspension or revocation of certificates. It is able to give accurate details (e.g. statistics, certain status and information) in different life cycle phases for the operators, auditors and for the external world, in a form which can be interpreted by human users (HTML pages, e-mails) or machines (CRL, OCSP or defined protocols).

The audit logs of the NCA system ensures full control of events and the tracebility of activities.

The NCA system can be configured using a wide variety of parameters, and provide for the capability of monitoring of running services.

It is suitable for activation of different HSM modules available via PKCS#11 interface, and through this capability for calling the execution of cryptographic functions. In the certified configurations the HSM means exclusively the following hardware cryptographic module:

- ProtectServer Orange (earlier Eracom CSA 8000).

The security target of the NCA system makes a conformance claim to the protection profile Certificate Issuing and Management Components Family of Protection Profiles (CIMC-PP) Version 1.0 /Security Level 3/.

Annex 2

Secure usage conditions

Assumptions for the NCA v2.6.0 IT environment
The following assumptions (also specified in the Security Target) are made for the IT environment:

Personnel assumptions

1. Audit logs are required for security-relevant events and must be reviewed by the system auditor. (A.Auditors Review Audit Logs)
2. An authentication data (password and PIN) management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (A.Authentication Data Management)
3. Competent administrators, operators, officers and auditors will be assigned to manage the TOE and the security of the information it contains. (A.Competent Administrators, Operators, Officers and Auditors)
4. All administrators, operators, officers, and auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated. (A.CSP)
5. Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility). (A.Disposal of Authentication Data)
6. Malicious code destined for the TOE is not signed by a trusted entity. (A.Malicious Code Not Signed)
7. Administrators, operators, officers, auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data. (A.Notify Authorities of Security Issues)
8. General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks. (A.Social Engineering Training)
9. Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner. (A.Cooperative Users)

Connectivity assumptions

10. The operating system has been selected to provide the functions required by the TOE to counter the perceived threats identified in the security target chapter 3.3. (A.Operating System)

Physical assumptions

11. The system is adequately physically protected against loss of communications i.e., availability of communications. (A.Communications Protection)
12. The TOE hardware, software, and firmware critical to TOE security policy (TSP) enforcement will be protected from unauthorized physical modification. (A.Physical Protection)

Annex 2

Other conditions of secure usage

1. In case of qualified certification service provision only the following modes of operations shall be configured: CWAmode=1, QualifiedMode=1 and CertificateMode= sign.
2. In case of non-qualified certification services, but which are under the effect of the Electronic Signature Act 2001, only the following modes of operations shall be configured: CWAmode=1, QualifiedMode=0 and CertificateMode= sign.
3. The IT environment must support the generation of trusted time (with independent time sources and synchronization programme).
4. In case of qualified certification .service and time-stamping service provision the IT environment must synchronize the trusted time to a time value that is within the Co-ordinated Universal Time (UTC) with one second.
5. The IT environment must provide for the appropriate HSM module (e.g. ProtectServer Orange) usage, and the enforcement of the usage conditions established during HSM module certification.
6. The IT environment must provide for a trusted channel between the remote users and the NCA system (e.g. it must enforce the usage of SSL connection for the web-server available for remote users).
7. The IT environment must provide for the possibility of checking the root certificate's hash in order to guarantee the correctness of the certificate issued by the certification service provider, by providing information through a trusted path.
8. Yearly change of infrastructure and control keys must be checked by IT and non-IT procedures.
9. IT and non-IT procedures must be applied to trusted checking of data shipped in certificate requests sent to the certificate provider.
10. Status modifications applied in NCA system must be compliant with the policies of the certification service provider.
11. During the usage of NCA system exclusive usage of the applicable certificate profiles must be provided.
12. In case of qualified certification service provision the Owner field of the CSP's certificate must contain the country code.
13. The certification service provider must provide that requests for revocation and/or suspension are processed in such a way that the maximum duration from the request to the status information change does not exceed the 24 hours.
14. Checks must be made on algorithms applied in NCA system in a timely manner that they are compliant with the requirements laid down in ETSI TS 102 176-1.
15. IT and non-IT procedures must be enforced in order to achieve the following requirements: [SO2.1]; [SO2.2]; [SO2.3]; [KM1.3]; [KM2.4]; [KM3.1]; [KM5.1]; [KM5.2]; [KM5.3]; [KM6.3]; [KM6.6]; [CG2.3]; [RM1.4]; [RM2.1]; [TS2.2]; [TS4.2]

Annex 3

Product conformance requirements
Documents containing requirements and standards

Requirements

Act XXXV of 2001 of the Republic of Hungary on electronic signature

CEN CWA 14167-1:2003 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

MSZ CWA 14167-1:2006 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

ETSI TS 101 862 v1.3.3 Qualified Certificate profile

ETSI SR 002 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

Standards

RFC 2560	Online Certificate Status Protocol - OCSP
RFC3161	Time-Stamp Protocol (TSP)
RFC3280	Certificate and Certificate Revocation List (CRL) Profile
PKCS #11 v2.11	Cryptographic Token Interface Standard
PKCS #12 v1.0	Personal Information Exchange Information Standard

Annex 4

Further information on the certification procedure

Developers' documents examined during certification

- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – SECURITY TARGET v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services - CONFIGURATION MANAGEMENTDOCUMENTATION v1.1
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – DEVELOPMENT SECURITY DOCUMENTATIONv1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – LIFECYCLE DOCUMENTATION v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – FLAW REPORTING PROCEDURES v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – SECURITY POLICY MODEL v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – FUNCTIONAL SPECIFICATION v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – CLIENT FUNCTIONS AND CONSOLE COMMANDS v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – STRUCTURE OF CONFIGURATION FILES v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – HIGH LEVEL DESIGN v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – LOW LEVEL DESIGN v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – CONFORMANCE ANALYSIS v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – DEVELOPERS' TOOLS DOCUMENTATION v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – DEVELOPERS' TESTS RESULTS
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – TEST COVERAGE ANALYSIS v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – TEST DEPTH ANALYSIS v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – ASSESSMENT OF GUIDANCE DOCUMENTATION v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – ANALYSIS OF STRENGTH OF FUNCITON v1.0
- NCA TWS v2.6.0 - NCA Trustworthy system for Certification Service Provider services – VULNERABILITY ANALYSIS v1.0

Developers-independent documents examined during certification

Evaluation report - NCA TWS 2.6.0 trustworthy system for certification services v1.0 (produced by HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The independent evaluation and certification of NCA v2.6.0 system has been done according to the methodology of CEM (Common Evaluation Methodology) v2.3.

Evaluation level

EAL4 + (augmented with assurance component ALC_FLR.2 Flaw reporting procedures).