Certificate

HUNGUARD Informatics and IT R&D and General Service Provider Ltd.
as a certification authority assigned by the assignment document No. 002/2004 of the Minister of The Ministry of Informatics and Communication of the Republic of Hungary and based on the Decree 15/2001. (VIII. 27.) of the Minister of the Prime Minister's Office

certifies

that the

NLCAPI3 v3.2.0 cryptographic module

developer function library suitable for developing electronic signature applications

developed by the

NetLock Informatics and Network Privacy Services Ltd.

with functionality written down in Appendix 1
and with the secure usage conditions listed in Appendix 2

passes the requirements

for generating and verifying advanced and qualified electronic signatures and for requesting and verifying time-stamps applicable to developing standard and secure applications, according to the Act XXXV of 2001 of the Republic of Hungary on electronic signature

This certificate has been issued on the basis of the certification report of HUNG-TJ-027-2005.
Produced on commission of NetLock Informatics and Network Privacy Services Ltd.
Certificate registration number: **HUNG-T-027-2005.**
Date of certificate: 20.06.2005.

Validity period of certificate: 20.06.2008.
Appendices: attributes, conditions, requirements and other features on five pages.

L.S.

Endrődi Zsolt
certification director

dr. Szabó István
managing director

Appendix 1

Summary of the main attributes of NLCAPI3 v3.2.0

NLCAPI3 v3.2.0 is a programme library providing electronic signature functionality for application developers.
NLCAPI3 v3.2.0 is based on entirely on the Crypto API of the Windows operating system, and significantly simplifies its usage. It uses Microsoft's or other vendors' CSP through the Crypto API in order to access the functionality of the signature-creation device. The message-digest procedures are also the functions of the Crypto API. It uses the functions of OpenSSL 0.9.7d to check the certification path.
The NLCAPI3 v3.2.0 provides programming interface for cryptographic module developers to create electronic signatures, to verify electronic signatures, to handle certificates and time-stamps. The main attributes are:

- Signature formats used:
  - PKCS7 (RFC2315);
  - XMLDSIG (RFC3275);
  - XADES-BES, XADES-T, XADES-C, XADES-XL, XAdES-A, multiple XAdES-A (ETSI 101903)
  - proprietary NetLock format (not documented)
- Time-stamp management based on RFC3161
- MD5 and SHA1 message digest procedures
- Managing X509 certificates and CLRs, in Windows certificate repository or in BASE64 coded PEM and DER formats
- Certificate validation based on RFC3280.
- Supported certificate extensions:
  - Key Usage
  - Basic Constraints
  - CRL Distribution Points
  - Qualified Certificate Statement (ETSI TS 101 862)

Appendix 2

Secure usage terms

Here we summarise those mandatory conditions that must be maintained and that have effect on the validity of this certificate. These terms contribute to the security of the signatures that are managed by electronic signature applications developed by the NLCAPI3 v3.2.0 cryptographic module.

Term 1: *The NLCAPI3 v3.2.0 cryptographic module does not support the self-issued certificates. Neither does it support the validation of the certificate paths in those cases when CRLs are validated by other certificate than the end-user certificates. Therefore it should be used only in such environments where there is not self-issued certificate in the certificate path, and where the CRL and end-user certificate must be validated using the same CA certificate.*

Term 2: *Technical and procedural measures should be done in the operational environment of the signature creation application developed by the NLCAPI3 v3.2.0 cryptographic module in order to ensure that the signature creation process could not be interfered with untrusted system and application processes, peripheral devices and communication channels that are not needed for the operation of the signature creation application.*

Term 3: *The MD5 message digest algorithm should not be used when creating advanced or qualified electronic signatures.*

Term 4: *Though the NLCAPI3 v3.2.0 cryptographic module contains self-protection function, in its operational environment technical and procedural measures should be done in order to ensure the followings:*

- *signature creation application and other signature creation components invoked by it should be protected from viruses, and*
- *signature creation components accidentally infected by viruses should be securely recovered.*

Term 5: *Technical and procedural measures should be done in the operational environment of the NLCAPI3 v3.2.0 cryptographic module to protect the integrity of the functional components of the NLCAPI3 v3.2.0 cryptographic module from intruders' activity.*

Term 6: *Technical and procedural measures should be done in the operational environment of the NLCAPI3 v3.2.0 cryptographic module in order to ensure that the NLCAPI3 v3.2.0 cryptographic module and all components interacting with the signature creation and signature verification processes are implemented in a secure area.*

Appendix 3

Product compliance requirements

Documents containing requirements and standards

Requirements

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

CEN/ISSS/E-Sign; Area G1 14170:2004 Workgroup Agreement: Security Requirements for Signature Creation System

CEN/ISSS/E-Sign; Area G2 14171:2004 Workgroup Agreement: Procedures for Electronic Signature Verification

CEN/ISSS/E-Sign; Area V 14172-4:2001 Workgroup Agreement: Signature Creation Application and Procedures for Electronic Signature Verification

ETSI TS 101 733 v1.4.0 Electronic Signature Formats

ETSI TS 101 862 v1.3.2 Qualified Certificate profile

ETSI SR 002 176 v1.1.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures

ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)

Standards

CAPI	Microsoft Cryptographic Application Interface
PKCS#1	RSA Cryptographic Standard /RFC2313/
RSA	Rivest-Shamir-Adleman (public key crypto-system) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/

RFC3061 Time-Stamp Protocol (TSP)

RFC3275 XML Digital Signatures (XMLDSig)

RFC3280 Certificate and Certificate Revocation List (CRL) Profile

PKCS #7: Cryptographic Message Syntax Standard

Appendix 4

Other features of the certification process

Developers' documents examined during the certification:

- Request for certification
- NLCAPI 3 function specification v1.0
- NLCAPI 3 high level design v1.0
- NLCAPI 3 user guide
- NLCAPI 3 test documentation v1.0

Documents considered during the certification, independent from the developers

- Evaluation report on the NLCAPI3 V3.2.0 cryptographic module, which module serves as a programming library suitable for developing electronic signature creation and verification applications (Produced by HunGuard Ltd.)

Assurance level of the analysis checking the compliance with requirements

The assurance level of the developer-independent verification process taken into consideration while making this certification report is similar to **EAL3** of the ISO 15408 /Common Criteria/. (EAL3 provides medium security, independently assured from the developers.)
An evaluation report has been made as a summary of the examination that was conducted independently from the developers.

This certification report is mainly based on the developers' evidence and the results included and documented in the evaluation report.
The evaluation has covered the following assurance classes:

- development
- guidance documents
- tests

During evaluation, apart from the above, developer-independent sample has been tested and penetration tests have taken place.