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 Communications Decree 9/2005. (VII.21)

certifies that

eSign Toolkit v2.1.0.2

development kit for qualified electronic signatures

developed by
Noreg Information Security Ltd

with functionality laid down in Annex 1

and with the secure usage conditions listed in Annex 2

passes the requirements

**for the development of secure applications meeting the applicable standards for creating and verifying advanced and qualified electronic signatures
according to the Act XXXV of 2001.**

This certificate has been issued on the basis of the certification report No. HUNG-TJ-043-2008.
Produced on commission of Noreg Information Security Ltd.

Certificate registration number: **HUNG-T-043-2008.**
Date of certificate: 01.12.2008.
Validity period of the certificate: 01.12.2011.
Annexes: attributes, conditions, requirements and other features on six pages.

LS

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Main features of eSign Toolkit v2.1.0

eSign Toolkit v2.1.0 function library has the following features:

- able to generate standard format electronic signatures (XAdES v1.2.2 and XAdES-EPES, XAdES-T, XAdES-C and XAdES-XL complying with MELASZ-ready v1.0; and CMS complying with RFC 3852),
- able to verify standard format electronic signatures (XAdES v1.2.2 and XAdES-EPES, XAdES-T, XAdES-C and XAdES-XL complying with MELASZ-ready v1.0; and CMS complying with RFC 3852),
- able to handle X.509 v3 certificates and certificate paths (based on RFC5280),
- is suitable for generating time-stamp requests and verification of time-stamp responses (operating together with time-stamping service providers fulfilling RFC 3161 standard)),
- able to query revocation information (CRL and OCSP) from certification service providers (from distribution points set in the certificate),
- able to operate with different signature-creation devices (SCDs) and secure signature-creation devices (SSCDs).

eSign Toolkit v2.1.0 is a function library made for software developers, and provides public key services written in language C and designed for using in a closed system. Its functionality covers services to generate and verify electronic signatures; for the verification to process validation information, to build certification path, to check the validity of certificates and of revocation information; to request and to verify time-stamps, to request and verify OCSPs.

eSign Toolkit v2.1.0 is based upon the functions of OpenSSL, uses these functions during operation; it implements most of its cryptographic functionality via these interfaces. The handling of cryptographic tokens is done through PKCS#11.

The DLL has interface that can be called from different programming language environments and it can be purchased in software development package.

Annex 3

Secure usage conditions

The positive result of the evaluation is based on the fulfilment of the following conditions:

- assumptions derived from the security target (assumptions regarding the IT environment that are necessary for the security of the TOE),
- conditions that are necessary for the compliance with CWA 14170 and CWA 14171 requirements,
- other secure usage conditions.

Assumptions for the eSign Toolkit v2.1.0IT environment

The following assumptions (also specified in the Security Target) are made for the IT environment:

1. Authorised users (application developers) are trusted to correctly perform their assigned functions (AE.Authorized_Users).
2. eSign Toolkit v2.1.0 development kit is properly installed and configured (AE.Configuration).
3. The cryptographic functions called by eSign Toolkit v2.1.0 (e.g. OpenSSL) securely implements the cryptographic functions called by eSign Toolkit v2.1.0. In case of qualified electronic signatures the environment of eSign Toolkit v2.1.0 contains one (or more) SSCD(s) –registered and certified by the Hungarian National Communications Authority– and this (these) SSCD(s) store(s) and protect(s) the private key of the signatory and performs the digital signature process (AE.Crypto_Module).
4. In the development environment eSign Toolkit v2.1.0 is protected from unauthorised physical access (AE.Physical_Protection).
5. The certificate and certificate revocation information are available to eSign Toolkit v2.1.0 (AE.PKI_Info)
6. The environment provides accurate system time with required precision in GMT format (AE.Time).
7. eSign Toolkit v2.1.0 environment provides access to the time-stamping provider (AE.TimeStamp).

Conditions necessary for the compliance with CWA 14170 and CWA 14171 requirements

No 1 CWA condition (for F_ISV_3 functional requirement)
eSign Toolkit v2.1.0 function library –when verifying the certificate path– operates according to the shell model, i.e. each certificate validity period must be within the validity period of the issuing certificate validity period. It does not support the verification of certificate paths where the issued CRL is not complete. Therefore it must be applied only in such environments where an issued certificate is not valid further than its issuing certificate, and the CRL issued for the certificates is complete.

No 2 CWA condition (for S_SCA_9 security requirement)
Management, operational and technological measures should be applied in the operational environment of signature application developed by eSign Toolkit v2.1.0 function library in order to assure that non-trusted system and application processes, peripheral devices and communication channels not necessary for signature creation applications should not be able to interfere with the signature process.

No 3 CWA condition (for S_SCA_12 security requirement)
eSign Toolkit v2.1.0 function library store text/xml type as content type. Therefore eSign Toolkit v2.1.0 can be used to sign only data that comply with this format.

No 4 CWA condition (for S_I/O_1 security requirement)
eSign Toolkit v2.1.0 does not have self-protection functionality, so management, operational and technological measures should be applied in its operational environment in order to provide for the following:

a. viruses will not damage the signature application and other signature components used by it, and
b. signature components accidentally infected by viruses will be recovered correctly.

No 5 CWA condition (for S_I/O_2 security requirement)
Management, operational and technological measures should be applied in the operational environment of eSign Toolkit v2.1.0 in order to protect the integrity of functional components of eSign Toolkit v2.1.0 and so to prevent damages done by attackers.

No 6 CWA condition (for S_VER_1 security requirement)
Management, operational and technological measures should be applied in the operational environment of eSign Toolkit v2.1.0 in order to assure that all of the components of eSign Toolkit v2.1.0 interacting with signature creation or signature verification processes are implemented in a secure area.

Further secure usage conditions

eSign Toolkit v2.1.0 has the following two modes of operation:

- qualified electronic signature creation mode (environment variable „QualifiedSignature” is not 0);
- advanced electronic signature creation mode (environment variable „QualifiedSignature” is 0)

No 1 other condition
In case of generating qualified electronic signatures the „qualified electronic signature creation mode” must be set using the „QualifiedSignature” environment variable by setting it to the proper value.

Annex 3

Product compliance requirements

Documents containing requirements and standards

Requirements

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

CEN CWA 14170:2004 Working Group Agreement: Security Requirements for Signature Creation System

CEN CWA 14171:2004 Working Group Agreement: General guidelines for electronic signature verification

ETSI TS 101 733 v1.6.3 CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 862 v1.3.3 Qualified Certificate profile

ETSI SR 002 176-1 2.0.0 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

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

Standards

RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/
RFC 2560	X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999
RFC3161	Time-Stamp Protocol (TSP)
RFC3275	XML Digital Signatures (XMLDSig)
RFC3852	Cryptographic Message Syntax (CMS)
RFC5280	Certificate and Certificate Revocation List (CRL) Profile
PKCS#1	RSA Cryptographic Standard /RFC2313/
PKCS #11 v2.11	Cryptographic Token Interface Standard
PKCS #12 v1.0	Personal Information Exchange Information Standard
MELASZ-ready v1.0	Unified MELASZ format for electronic signatures v1.0, February 2006

Annex 4

Further information on the certification procedure

Developers' documents examined during certification

- Requests for certification
- Security Target v1.0
- Configuration management documentation v1.0
- Development security documentation v1.0
- Noregpki2.Dll – Developers' documentation 2.1.0.2
- Test documentationv1.0
- Test coverage documentation v1.0
- Test depth documentation v1.0
- High level design v1.0
- Compliance analysis v1.0
- Vulnerability assessment v1.0
- NoregPKI2.dll, NoregPKI2.h 2.1.0.2

Developers-independent documents examined during certification

Evaluation report on "eSign Toolkit for qualified electronic signatures v2.1.0" v1.0 (by HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The evaluation of eSign Toolkit v2.1.0 development toolkit has been done according to methodology of the Hungarian Information Technology Security Evaluation and Certification Scheme /MIBÉTS/. MIBÉTS acknowledges the concepts, terminology and criteria of Common Criteria ISO/IEC 15408:2005 as a normative standard for the security evaluation of IT products and systems.

Evaluation level

Advanced (EAL3)

Documents about methodology used during evaluation

- ISO/IEC 15408:2005 Information technology — Security techniques — Evaluation criteria for IT security (Part 1,2,3)
- ISO/IEC 18045:2005 Information technology — Security techniques — Methodology for IT security evaluation
- Recommendation No 25 of Committee on Public Administration IT (KIB): Hungarian Information Security Recommendations – Hungarian Information Technology Security Evaluation and Certification Scheme (v1.0, June 2008) – Guidance No 5: EVALUATION METHODOLOGY