CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 002/2006 of the Minister of the Ministry of Informatics and Communication (MIC) of the Republic of Hungary
based on the MIC Decree 9/2005. (VII.21)

certifies

that the

MultiSigno V3 SDK /3.0.1 r249/

electronic signature development kit

developed by

Grepton Informatics PLC.

with functionality written down in Annex 1

and with conditions regarding the secure usage listed in Annex 2

passes the requirements

for the development of secure applications meeting the applicable standards for creating and verifying qualified electronic signatures 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 No. HUNG-TJ-033-2006.
Produced on commission of Grepton Informatics PLC.
Certificate registration number: **HUNG-T-033-2006.**
Date of certificate: 09.06.2006.
Validity period of the certificate: 09.06.2009.
Annexes: attributes, conditions, requirements and other features on six pages.

LS

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Overview of the main features of MultiSigno v3.0.1

The MultiSigno v3.0.1 is a development kit for implementing standard-compliant (based on X.509 standard) public key-enabled applications. Public key services supported by the development kit are:

- creating advanced electronic signature with RSA/1024 algorithm and key size, with private key stored in PKCS#12 file, in a self-developed certificate store or in cryptographic hardware device;
- creating qualified electronic signature with RSA/1024 algorithm and key size with the use of SSCD;
- verifying electronic signatures together with services for certification path building and validation;
- producing hash value for the signature creation with SHA-1, SHA-256, SHA-384 or SHA-512 algorithms;
- symmetric (AES/ECB and CBC, 3DES/CBC, RC2/CBC) and asymmetric (RSA, PKCS#1 v1.5) encryption and decryption;
- time stamping (request and verification).

Based on this with MultiSigno v3.0.1 such applications can be developed that are capable of providing for confidentiality, integrity, authentication and non-repudiation services on the grounds of PKI technology.

MultiSigno v3.0.1 development library supports the following public key services:

- It securely manages keys, trust points and certificates.
- It accepts and processes X.509 v3 public key certificates.
- It is capable of obtaining the necessary certificates and revocation data.
- It verifies the validity of every certificate based on procedures specified in the X.509 standard [ISO 9594-8] including the revocation checks.
- It accesses accurate and trusted time-source for the purpose of the verification of certificates, revocation data and dates and times of application data.
- In case of the creation of qualified electronic signatures it works together with the SSCD necessary for creating qualified electronic signatures which device is certified on the grounds of the requirements by Hungarian law. In case of advanced electronic signatures it is capable of secure handling of standard software key storing files or cryptographic hardware device.
- It collects, stores and maintains data necessary for the verification of the signatures in the future.
- It is capable of automatic selection from several private encryption keys when implementing public key decryption.
- Generation of HAES-Ready XAdES signature format.

Annex 2

Secure usage terms

Assumptions for the MultiSigno v3.0.1 IT environment

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

1. Authorised users (application developers) are trusted to perform their assigned functions (AE.Authorized_Users).
2. MultiSigno v3.0.1 is properly installed and configured (AE.Configuration).
3. In case of creation of advanced electronic signatures the cryptographic functions called by MultiSigno v3.0.1 (OpenSSL v0.9.8) are trusted to implement the expected cryptographic functionality (AE.Crypto_Module). In case of creation of qualified electronic signatures the MultiSigno v3.0.1 environment contains one or more SSCD(s), registered and certified by the National Communication Authority (NCA), that is/are store(s) and protect(s) the signatory's private key and implement(s) the digital signature operation (AE.Crypto_Module).
4. The attack potential against MultiSigno v3.0.1 is assumed to be low (AE.Low).
5. The MultiSigno v3.0.1 environment is protected from physical access (AE.Physical_Protection).
6. The certificate and certificate revocation information is available to the MultiSigno v3.0.1 (AE.PKI_Info).
7. The MultiSigno v3.0.1 environment provides accurate system time with required precision in GMT format (AE.Time).
8. The MultiSigno v3.0.1 environment provides access to the time-stamping provider (AE.TimeStamp).

Further conditions regarding the secure usage

1. The MultiSigno v3.0.1 development library does not support self-issued certificates. Neither does it support automatic policy management nor CRL distribution based on LDAP, nor delta CRLs. Therefore it can be used in such environments where self-issued certificate cannot be found in the certificate path. It should not be used in environments where Policy should be handled automatically, the CRL distribution is based on LDAP or delta CRLs are applied.
2. Technical and procedural measures should be applied in the operational environment of the signature application using MultiSigno v3.0.1 development kit 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.
3. Changing of password of the PKCS#12 file or the token device should be provided in the operational environment of MultiSigno v3.0.1.
4. Technical and procedural measures should be applied in the operational environment of MultiSigno v3.0.1 development library 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.
5. Technical and procedural measures should be applied in the operational environment of MultiSigno v3.0.1 development library in order to protect the integrity of functional components of MultiSigno v3.0.1 and so to prevent damages done by attackers.
6. Technical and procedural measures should be applied in the operational environment of MultiSigno v3.0.1 development library in order to assure that the MultiSigno v3.0.1 development library and all of its components interacting with signature creation, signature verification processes are implemented in a secure area.

Annex 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 Working Group Agreement: Security Requirements for Signature Creation System

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

CEN/ISSS/E-Sign; Area V 14172-4:2001 Working Group Agreement: Signature Creation Application and Procedures 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 v1.2.1 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/

RFC3161 Time-Stamp Protocol (TSP)

RFC3275 XML Digital Signatures (XMLDSig)

RFC3280 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

Annex 4

Further information on the certification procedure

Developers' documents examined during certification

- Security Target v1.0
- Functional specification v1.0
- High level design v1.0
- Low level design v1.0 (MultiSigno SDK Documentation v3.0.1)
- Implementation v3.0.1
- Compliance analysis v1.0
- Test documentation v1.0
- Test coverage documentation v1.0
- Test depth documentation v1.0
- Guide documentations (MultiSIgno 3.0 Manual) 28.04.2006.
- Configuration management v1.0
- Development security v1.0
- Life cycle documentation v1.0
- Development tools v1.0
- Misuse analysis of developers' guide v1.0
- Vulnerability analysis v1.0
- Program charts v1.0.0
- MultiSigno 3 – Design documentation – Implementation model 06.01.2006.
- MultiSigno 3 - Design documentation – Use cases implementation 06.01.2006.
- Logical architecture for MultiSigno 3 design documentation 06.01.2006.
- MultiSigno 3.0 Specification v2.0
- MultiSigno 3.0 Manual 28.04.2006.

Developers-independent documents examined during certification

Evaluation report on MultiSigno V3 SDK electronic signature development kit v3.0.1 /r249/ v1.0 (HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The evaluation of MultiSigno v3.0.1has been done according to the Hungarian IT Security and Evaluation Scheme (MIBÉTS) methodology. MIBÉTS acknowledges the concepts, principles and criteria of the Common Criteria (MSZ ISO/IEC 15408:2002) for the technological evaluation of information systems and products.

Evaluation level

High (EAL4)

Documents about methodology used during evaluation

- MIBÉTS Publication No 1: General model of National MIBÉTS scheme /v0.95, February 2005/,
- MIBÉTS Publication No 2: Procedures of evaluation and certification /v0.95, February 2005/,
- MIBÉTS Publication No 3: Evaluation methodology 1 – Evaluation methodology of the Security Target /v0.95, February 2005/,
- MIBÉTS Publication No 3: Evaluation methodology 4- Evaluation methodology of the high assurance level /v0.95, February 2005/.