



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

InfoSigno for Developers v1.0.0 r119
development kit for qualified electronic signature applications

developed by

Argeon Business Services Ltd.

*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-031-2006.
Produced on commission of Argeon Business Services Ltd.

Certificate registration number: **HUNG-T-031-2006.**

Date of certificate: 29. 05. 2006.

Validity period of the certificate: 29. 05. 2009.

Annexes: attributes, conditions, requirements and other features on six pages.

L S

Endródi Zsolt
Certification director

dr. Szabó István
Managing director



Annex 1

Overview of the main features of InfoSigno v1.0.0

InfoSigno v1.0.0 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 electronic signatures;
- verifying electronic signatures together with services for certification path building and validation;
- asymmetric (for key transfer) and symmetric (for data transfer) encryption and decryption;
- time stamping (request and verification).

Based on this the InfoSigno v1.0.0 supports the development of a wide range of applications that are capable of provision of confidentiality, integrity, authentication and non-repudiation services on the grounds of PKI technology.

The InfoSigno v1.0.0 development library supports the following public key services:

- It securely manages key, 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 all certificates based on procedures specified in RFC 3280 with the conditions determined in Annex 2, including the revocation checks.
- It handles accurate and trusted time-source based on RFC 3161 for 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.
- Digital signature algorithm: RSA 1024, hash algorithm: SHA-1 with padding pkcs1-v1.5.
- Generation of XAdES-C signature format.
- 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.



Annex 2

Secure usage terms

Assumptions for the InfoSigno v1.0.0 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. InfoSigno v1.0.0 is properly installed and configured (AE.Configuration).
3. In case of creation of advanced electronic signatures the cryptographic functions called by InfoSigno v1.0.0 (OpenSSL) are trusted to implement the expected cryptographic functionality (AE.Crypto_Module).
4. In case of creation of qualified electronic signatures the InfoSigno v1.0.0 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 implements the digital signature operation (AE.Crypto_Module).
5. The InfoSigno v1.0.0 environment is protected from physical access (AE.Physical_Protection).
6. The certificate and certificate revocation information is available to the InfoSigno v1.0.0 (AE.PKI_Info).
7. The InfoSigno v1.0.0 environment provides accurate system time with required precision in GMT format (AE.Time).
8. The InfoSigno v1.0.0 environment provides access to the time-stamping provider (AE.TimeStamp).

Further conditions regarding the secure usage

1. The InfoSigno v1.0.0 cryptographic module does not support self-issued certificates, nor does support certificate path verification when CRLs are verified with certificate other than the end certificates. The InfoSigno v1.0.0 makes binary comparison for the issuer and owner match during building certificate path. Therefore it can be used in such environments where self-issued certificate cannot be found in the certificate path, the CRLs and end certificates are validated with the same CA certificate and in the certificate path the issuer-owner match is a binary match.
2. Technical and procedural measures should be applied in the operational environment of the signature application using InfoSigno v1.0.0 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 SCDev should be provided in the operational environment of InfoSigno v1.0.0.



4. Technical and procedural measures should be applied in the operational environment of InfoSigno v1.0.0 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 InfoSigno v1.0.0 development library in order to protect the integrity of functional components of InfoSigno v1.0.0 and so to prevent damages done by attackers.
6. Technical and procedural measures should be applied in the operational environment of InfoSigno v1.0.0 development library in order to assure that the InfoSigno v1.0.0 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 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

CEN CWA 14172-4:2001 Working Group Agreement: Signature-creation application and general guidelines for electronic signature verification

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

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

- Request for certification
- Security Target v1.0
- Functional specification v1.0
- High level design v1.0
- Low level design v1.0
- Compliance analysis v1.0
- Test documentation v1.0
- Test coverage documentation v1.0
- Test depth documentation v1.0
- Developers' guide v1.0
- Configuration management v1.0
- Development security v1.0
- Life cycle documentation v1.0
- Development tools v1.0
- Misuse analysis of developers' guide v1.0
- Strength of function analysis v1.0
- Vulnerability analysis v1.0

Developers-independent documents examined during certification

Evaluation report on InfoSigno for Developers development kit for qualified electronic signatures v1.0 (HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The evaluation of InfoSigno v1.0.0 has 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/.