CERTIFICATE

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)

certifies

that the

InfoSigno PKI SDK
electronic signature application development kit
for qualified electronic signatures
v3.0.1 (build 9)

developed by

ARGEON Informatics Services Provider 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-055-2011.
Produced on commission of ARGEON Informatics Services Provider Ltd.

Certificate registration number: **HUNG-T-055-2011.**
Date of certificate: 04.03.2011.
Validity period of the certificate: 04.03.2014.
Annexes: attributes, conditions, requirements and other features on six pages.

LS

Endrődi Zsolt	dr. Szabó István
Certification director	Managing director

Annex 1

Main features of InfoSigno v3.0.1

InfoSigno v3.0.1 is a development kit for implementing standard-compliant (based on X.509 standard) public key-enabled applications. The previous version of the product is the InfoSigno for Developers registered under No. HUNG-T031-2006, but the new product version has been changed significantly in functionality, technology and also in the product name. Public key services supported by the development kit are:

- Generating advanced and qualified electronic signature with algorithm parameters supported by the Crypto API, using private key stored in Windows certificate-repository, in a software token or a cryptographic hardware device.
- Verifying electronic signatures together with services for certification path building and validation with RSA algorithm support.
- Producing hash value for the signature creation with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms.
- Request and verification of time stamps.
- Request and verification of revocation information (CRL, OCSP).

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

InfoSigno v3.0.1 development library has 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 RFC 5280 including revocation checks;
- It accesses accurate and trusted time-source for the purpose of the verification of date and time information of certificates, revocation data and application data;
- It collects, stores (embedding into the signature structure) data necessary for the verification of the signatures in the future;
- It supports XAdES-EPES, -T, -C, -X, -X-L, and -A electronic signature formats.

Annex 2

Secure usage terms

The validity of this certificate depends on the fulfilment of the environmental assumptions listed in the Security Target.

The following objectives laid down also in the Security Target apply to the IT environment:

Conditions regarding both generation and verification of electronic signatures

OE.Host_Platform
The host platform which the TOE has been installed on should be under the direct control of the signatory/verifier or under the control of an organisation that guarantees for the signatory/verifier that the following security measures are maintained.
The host operating system should identify the signatory/verifier during system start-up.
The host operating system should provide separate execution environment for applications running on it and

- the host is protected from viruses;
- the communication between the host platform and other IT components with open network connections should be protected by a firewall;
- access to administrator functions of the host platform should be restricted to the platform administrators (“host administrators”). The user account must be different from the host administrator account.
- installation and software update for the host platform should be under the control of the host administrator;
- the host operating system must prevent execution of untrusted applications
- the host shall provide accurate system time.

OE.Document_Presentation
One or more presentation application(s) should be run on the host platform on which the TOE is installed and these applications:

- accurately display the document to be signed/to be verified, or
- warn the signatory about possible compatibility problems between the viewer application and the properties of the document.

In case the document to be signed already contains signatures, the TOE environment should enable the signatory to know at least the identity of previous signatories, or, at best to verify the validity of these signatures.

OE.Trusted_Security_Administrator
The signatory/verifier are trusted persons, they are trained to use the TOE and have the necessary means to do their tasks. The security administrator of the host platform must be a trusted person, and shall have the means necessary to perform his job.

OE.Signature_Policy_Origin
The signatory should check the authenticity of origin of the signature policies before these have been imported to the TOE.

Conditions exclusively for electronic signature generation

OE.SCDev
The SCDev should be capable to generate digital signature on the data received from the TOE.
The SCDev must authenticate the signatory and enable him to activate the private key corresponding to the selected certificate.
The SCDev is responsible for the protection of the signatory's data. The following data shall be stored and used in a secure manner by the SCDev:

- data related to the generation of the signature:
  - the private key(s) of the signatory (confidentiality and integrity);
  - the actual certificate(s) or a reference to the certificate(s) of the signatory (integrity);
  - the private key/certificate correspondence (integrity)
- data related to the authentication of the signatory:
  - the authentication data of the signatory (integrity and confidentiality)
  - the correspondence between the authentication data and the private key/certificate pair (integrity).

OE.TOE/SCDev_Communications
The software and/or hardware components providing the interface between the TOE and the SCDev shall be able to manage (to open/close) a trusted channel guaranteeing the integrity and the exclusiveness of the communication.

OE.Signatory_Authentication_Data_Protection
The software/hardware components enabling the signatory to authenticate himself to the SCDev in order to activate the private key corresponding to the selected certificate, shall guarantee the confidentiality and the integrity of the authentication data during their input and during their transfer to the SCDev.

OE.Signatory_Presence
The signatory should be present from the point of time of his explicit claim to generate electronic signature on the documents until he activates his private key by entering his authentication data.

Conditions exclusively for electronic signature verification

OE.Validation_Data_Provision
The TOE environment should provide the validation data for the electronic signature verification.

Condition due to the compliance requirements to CWA 14170 and CWA 14171
The InfoSigno PKI SDK should be used only such environments in which the CRLs and end-user certificates must be verified with the same CA certificate; and should be operated under a signature policy that applies the following X.509 v3 certificate extensions at most:

- ExtendedKeyUsage,
- KeyUsage,
- BasicConstraints,
- CRLDistributionPoints,
- SubjectAlternativeName,
- IssuerAlternativeName,
- OCSP No check - id-pkix-ocsp-nocheck,
- OCSP AuthorityInfoAccess,
- QC statement.

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 workgroup agreement: Security Requirements fro Signature Creation System

CEN CWA 14171:2004 workgroup agreement: General guidelines for electronic signature verification

Protection Profile - Electronic Signature Creation Application (DCSSI-PP-2008/05)

Protection Profile - Electronic Signature Verification Module (DCSSI-PP-2008/06)

ETSI TS 102 176-1 v2.0.0 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

Unified MELASZ format for electronic signatures v2.0 (MELASZ Ready2, MMM-001: 2008, v2.0)

Standards

RFC 2560: PKIX - Online Certificate Status Protocol – OCSP

RFC 3161 PKIX - Time-Stamp Protocol

RFC 5280 PKIX - Certificate and Certificate Revocation List (CRL) Profile

SHS Secure Hash Standard /FIPS PUB 180-3/

PKCS#1 RSA Cryptography Standard v2.1, June 2002

Annex 4

Further information on the certification procedure

Developers' documents examined during certification

- Security Target InfoSigno_biztonsagi_eloiranyzat_v1.00.doc v1.00
- Installation manual InfoSigno_Telepitesi_kezikonyv_v1.1.doc v1.1
- Developers' documentation InfoSigno_Fejlesztoi_v1.4.doc v1.4, InfoSigno.chm v3.0.1
- Operational manual InfoSigno_PKI_SDK_Uzemeltetesi_kezikonyv_v1.2.doc v1.2
- Security architecture InfoSigno_biztonsagi_szerkezet_v1.00.doc v1.00
- Functional specification InfoSigno_funkcionalis_specifikacio_v1.00 v1.00
- TOE design InfoSigno_TOE_terv_v1.00.doc v1.00
- Implementation representation InfoSigno_megvalositas_reprezentacio_v1.00.doc v1.00
- Source code developed by Argeon
- Configuration list InfoSigno_konfiguracio_lista_v1.00.doc v1.00
- Configuration management InfoSigno_konfiguracio_kezeles_v1.00 v1.00
- Development security InfoSigno_fejlesztes_biztonsag_v1.00.doc v1.00
- Lifecycle specification InfoSigno_eletciklus_meghatarozas_v1.00 v1.00
- Development tools InfoSigno_fejlesztesi_eszkozok_v1.00 v1.00
- Delivery procedures in „Installation manual" Chapter 1, Section 1.1
- TOE suitable for testing InfoSigno.dll v3.0.1.9
- Test documentation in Chapter 3 in Test coverage analysis
- Test coverage analysis InfoSigno_teszt_lefedettseg_v1.00.doc v1.00
- Test depth analysis InfoSigno_teszt_melyseg_v1.00.doc v1.00

Developers-independent documents examined during certification

Evaluation report: Infoprove v3.0.1 electronic signature application + InfoSigno v3.0.1 electronic signature application development kit for qualified electronic signatures v1.0 (by HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The independent evaluation and certification of InfoSigno v3.0.1 has been done according to the methodology of MIBÉTS.

Evaluation level

MIBÉTS high (conforming to CC EAL4)

Documents about methodology used during evaluation

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.
- [Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.
- KIB (Information Technology Committee for Public Services) recommendation No 28. „Evaluation methodology for products"