CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. IKF/19519-2/2012-NFM of the Ministry of National Development based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

certifies

that the

mySigno API 3.1
electronic signature application development kit
v3.1

developed by

InfoScope 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 initial verification of advanced electronic signatures according to the Act XXXV of 2001.

This certificate has been issued on the basis of the certification report No. HUNG-TJ-66-2014.
Produced on commission of InfoScope Informatics Services Provider Ltd.

Certificate registration number: **HUNG-T-66-2014**
Validity start date of the certificate: 31 October 2014
Validity end date of the certificate: 31 October 2017
Annexes: attributes, conditions, requirements and other features on six pages.

Budapest, 31 October 2014

LS

Endrődi Zsolt
Certification director

Lengyel Csaba
Managing director

HUNGUARD

Annex 1

Main features of mySigno API 3.1

mySigno API 3.1 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:

- Generating advanced electronic signature with algorithm parameters supported by the Crypto API, using private key stored in a software token.
- Verifying initially electronic signatures together with services for certification path building and validation with RSA 2048 algorithm support.
- Producing hash value for the signature creation with SHA-256 algorithms.

Based on this such applications can be developed with mySigno API 3.1 that are capable of providing for confidentiality, integrity, authentication and non-repudiation services on the grounds of PKI technology.

The main security features of mySigno API 3.1 are:

- biometric data is produced from the handwritten signature and the result is unambiguously bound to the signed document in such a way that guarantees protection from unauthorized usage and access;
- integrity and authenticity of the package containing the bit image of the handwritten signature, the biometric data derived from the handwritten signature and the documents bound to this handwritten signature are guaranteed (by creating advanced electronic signature and by the initial verification of it);
- the package containing the handwritten signature and the advanced electronic signature are encrypted before transmitting to the server;
- at startup it verifies the validity of the advanced electronic signature placed on the server side configuration file.

The mySigno API 3.1 electronic signature creation is embedded in a system that has other functionality which enables the creation and processing of handwritten signatures for the users.

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.Trusted_Security_Admin

Administrators performing the installation tasks, which are outside the TOE scope and must be accomplished before the mySigno API 3.1 usage, are trusted, are trained to use MySigno API 3.1, and possess the necessary tools to perform their job.

OE.UserGuide

The human agent using the client is trained, and is aware of all the rules which derive from the device physical features and which guarantee the secure usage.

OE.Trusted_EnvCode

The application calling the mySigno API 3.1 security functions and the library implementing the functions called by mySigno API 3.1 are trusted regarding that they meet the security requirements which are formulated as IT environment assumptions in this Security Target.

OE.Packet_Viewers

Both the client device and the server IT environment contain such outer viewer applications which are capable of presenting all the formats that can be included in the package (which are determined by the signature policy). The IT environments of signature creation client and the server application performing the signature verification are able to handle and present exactly the same formats; moreover, these outer applications operate with the same configuration settings on both sides. These outer viewer applications are outside the TOE scope.

OE.Separation_and_Exclusion

In the environment where the signature creation and verification take place the TOE processes are protected from the harmful interference of other processes. Only one mySigno API 3.1 module instance should be loaded by host applications at a time.

OE.Services_Integrity

The environment of the mySigno API 3.1 (that is the calling host application, the operation system) must provide tools which can be applied to verify the integrity of the mySigno API 3.1 services and parameters.

OE.Protected_Verification_Environment

Protected environment must be provided on the server side and a verification application as well, in order to conclude disputed cases emerging subsequently in connection with a handwritten signature.

In the protected environment the verification application must be able to restore the biometric data of the handwritten signature bound to the document and this process must be done in the joint presence of a given number of key guards. At the same time it must be able to verify the validity of the digital signature of the package and the integrity of the document with the handwritten signature, after which a forensic handwriting examiner can be able to decide whether the handwritten signature derives from the person in question.

OE.Host_CLIENT_Machine

The host platform which the mySigno API 3.1 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;
- 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.
- the host operating system must prevent execution of untrusted applications

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.

Condition due to the compliance requirements to CWA 14170 and CWA 14171

Only such an outer viewer must be used that informs the signer that other signed data are embedded int he signer’s document, it is not able to modify the data and is capable of syntax verification of the formats it handles including the recognition of active codes and the warning function when an active code has modified the data.

The mySigno API 3.1 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.

HUNGUARD

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

ETSI TS 102 176-1 v2.1.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

Standards

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 INFOSCOPE_mySigno_ST_v1.0.5.doc v1.0.5
- Security Target Lite INFOSCOPE_mySigno_ST_v1.0.6_lite.pdf v1.0.6
- Installation manual INFOSCOPE_mySigno_telepitesi_v3.3 v3.3
  INFOSCOPE_mySigno_fejlesztoi_v3.3.docx v3.3
  mySigno 2010 P2 Quickstart v4.2.docx v4.2
- Developers' documentation INFOSCOPE_mySigno_fejlesztoi_v3.3.docx v3.3
- Operational manual INFOSCOPE_mySigno_fejlesztoi_v3.3.docx v3.3
- Security architecture INFOSCOPE_mySigno_FS_v1.4.4.docx v1.4.4
- Functional specification INFOSCOPE_mySigno_FS_v1.4.4.docx v1.4.4
- TOE design INFOSCOPE_mySigno_HLD_v311.docx v3.1.1
- Configuration list mySigno_konfiguracio_lista_v3.2.doc v3.2
- Configuration management INFOSCOPE_mySigno_konfiguracio_kezeles_v3.1.docx v3.1
- Development security INFOSCOPE_mySigno_DVS_v1.0.docx v1.00
- Lifecycle specification INFOSCOPE_mySigno_eletciklus_meghatarozas_v3.1.docx v3.1
- Delivery procedures in „Installation manual" Chapter 1, Section 1.1
- Test documentation INFOSCOPE_mySigno_Test_Documentation_v1.2 v1.2
- Test coverage analysis INFOSCOPE_mySigno_Test_Documentation_v1.2 v1.2
- Test depth analysis INFOSCOPE_mySigno_Test_Documentation_v1.2 v1.2

Developers-independent documents examined during certification

Evaluation report: mySigno API 3.1 electronic signature application development kit v1.0 (by HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The independent evaluation and certification of mySigno API 3.1 has been done according to the methodology of MIBÉTS.

Evaluation level

MIBÉTS moderate (conforming to CC EAL3)

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"