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 AC SDK
v1.0.0.6
Attribute Certificate Validation SDK

developed by
InfoScope Ltd.

with functionality laid down in Annex 1

and with the secure usage conditions listed in Annex 2

passes the requirements

for development of electronic signature products according to the Act XXXV of 2001.

This certificate has been issued on the basis of the certification report No. HUNG-TJ-051-2010.
Produced on commission of InfoScope Ltd.

Certificate registration number: **HUNG-T-051-2010.**
Date of certificate: 27.08.2010.
Validity period of the certificate: 27.08.2013.
Annexes: attributes, conditions, requirements and other features on five pages.

L.S.

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Summary of the main features InfoSigno AC SDK v1.0.0.6

InfoSigno AC SDK is a software development library that supports checking the validity of attribute certificates.

Services provided by InfoSigno AC SDK are:

- loading of standard attribute certificate;
- validity checking of attribute certificate which covers the following sub-functions:
  - processing the public key certificates linked to the AC, validation of certificate paths, processing of CRLs and OCSPs;
  - verification of signatures on the certificates (verification of digital signatures on public key certificates contained in the certification path and on the attribute certificate);
  - processing the certificate revocation lists (ACRL) for attribute certificates;
- mapping of attribute certificate components to .NET objects;
- providing access to all fields in the attribute certificate.

The InfoSigno AC SDK takes into consideration the following standards and recommendations during processing of attribute certificates:

- RFC 3281: An Internet Attribute Certificate Profile for Authorization
- RFC 4476: Attribute Certificate (AC) Policies Extension
- ITU-T X.509-2000 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

The **InfoSigno ACTest** is a web application based on the functions of InfoSigno AC SDK and it supports the checking and testing of all services provided by InfoSigno AC SDK.

Annex 2

Secure usage conditions

Security objectives for the IT environment of the InfoSigno AC SDK v1.0.0.6 (also listed in the Security Target):

1. The operating system of the host platform shall provide separated contexts of execution for the various tasks which it performs. In addition, the following security measures shall be implemented: the host platform must be protected from viruses; the data exchange between the host platform and other IT elements via an open network must be controlled by a firewall; the access to the administration functions of the host platform must be restricted to the administrators of the platform (thereafter the “Host administrator”). The user account must be different from the Host administrator account; the installation and the update of the software of the host platform must be under the control of the Host administrator; the operating system of the host platform must not allow the execution of untrusted applications. Application note: The role of Host administrator is distinct from the role of Security administrator of the TOE. (OE.Host_Platform)
2. The environment of the TOE must provide the validation data necessary to the verification of the signatures and the attribute certificate. (OE.Validation_Data_Provision)
3. The environment of the TOE must provide to the Security administrator the means of controlling the integrity of the services and of the parameters of the TOE. (OE.Services_Integrity)
4. The security administrator of the TOE shall be trusted, shall be trained with the use of the TOE and shall have the means necessary to adequately do his activity. (OE.Trusted_Security_Administrator)
5. The IT environment of the TOE must provide the necessary IT environment for testing (ACTest) in order to store the user data needed for the tests. (OE.AC_CheckFrame)

Other conditions of secure usage

6. Technical and procedural measures must be applied in the operational environment of InfoSigno AC SDK in order to assure that the InfoSigno AC SDK development library and all components interacting with the signature generation, signature verification processes are implemented in a secure area.

Annex 3

Product conformance requirements

Documents containing requirements and standards

Requirements

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

CEN CWA 14171: 2004 General guidelines for electronic signature verification

Standards

RFC 3281: An Internet Attribute Certificate Profile for Authorization

RFC 4476: Attribute Certificate (AC) Policies Extension

ITU-T X.509-2000 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Annex 4

Further information on the certification procedure

Developers' documents examined during certification

InfoSigno AC SDK v1.0.0.6 (+ ACTest v1.0.1.4) Attribute certificate validation SDK– **Security target** (v1.0)
ACTest test website installation guide (v1.0)
ACTest testprogramme user guide (v1.0)
Security architecture - Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)
Functional specification - Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
TOE design- Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)
Implementation representation - Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)
Configuration list - Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
Configuration management documentation - Attribute service provider software (Info&AA) v1.0 (v1.0)
Development security documentation- Attribute service provider software (Info&AA) v1.0 (v1.0)
Lifecycle documentation - Attribute service provider software (Info&AA) v1.0 (v1.0)
Development tools documentation - Attribute service provider software (Info&AA) v1.0 (v1.0)
Infoscope Development conventions, C#, C/C++ (v1.01)
Delivery procedures - Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
ACTest testprogramme documentation - Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 +ACTest v1.0.1.4) (v1.0)
Test coverage analysis - ATE_COV.2 Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4) (v1.0)
Test depth analysis - ATE_DPT.2 Attribute certificate validation SDK (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)
Target of evaluation suitable for testing

Developers-independent documents examined during certification

Evaluation report – InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4 trustworthy system for certification services v1.0 (Produced by Hunguard Ltd.)

Method of independent assessment checking the requirement compliance

The independent evaluation and certification of InfoSigno AC SDK v1.0.0.6 system has been done according to the methodology of MIBÉTS (Hungarian Scheme for Information Technology Security Evaluation and Certification).

Evaluation level

MIBÉTS High (EAL4)

Documents about methodology used during evaluation

- Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 1: Introduction and general model
- Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 2: Security functional components
- Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 3: Security assurance components
- Common Methodology for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2)
- MSZ/ISO/IEC 15408:2003 – Information technology – Security technology – Common Criteria of Information Security Evaluation
- KIB (Information Technology Committee for Public Services) Recommendation No 28. „Certification methodology for products"