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

Info&AA
v1.0
Attribute Service Provider Software

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 applications operating in trustworthy system of certification service providers according to the Act XXXV of 2001.

This certificate has been issued on the basis of the certification report No. HUNG-TJ-050-2010.
Produced on commission of InfoScope Ltd.

Certificate registration number: **HUNG-T-050-2010.**
Date of certificate: 27.08.2010.
Validity period of the certificate: 27.08.2013.
Annexes: attributes, conditions, requirements and other features on eight pages.

L.S.

Endrődi Zsolt	dr. Szabó István
Certification director	Managing director

Annex 1

Summary of the main features of Info&AA v1.0

The Info&AA v1.0 is a specific electronic signature product that provides different attribute service functions.
Info&AA v1.0 supports the following attribute services:

a) attribute registration service,

b) attribute certificate request service,

c) attribute certificate generation service,

d) attribute certificate dissemination service,

e) attribute certificate revocation management service,

f) attribute certificate revocation status information service

The Info&AA v1.0 implements the following functions as part of these services:

- attribute certificate generation (generation of attribute certificates according to the X.509 and RFC 3281 standards which are linked to existing PKI certificates),
- attribute certificate revocation management (revocation, suspension or reactivation of published attribute certificates),
- attribute certificate revocation status information service (generation of ACRLs according to X.509 and RFC 5280 containing revoked and suspended attribute certificates and their publishing to LDAP).

Users of the Info&AA v1.0 system are: operators and administrators of the attribute service provider.

Annex 2

Secure usage conditions

Security objectives for the IT environment of the Info&AA v1.0 (also listed in the Security Target):

1. Capable management of the TOE must be provided by assigning competent persons to the trustworthy roles to manage the TOE and the security of the information it contains. (OE.Competent Administrators, Operators, Officers and Auditors)
2. Faults of staff in trustworthy roles should be prevented by providing adequate guidance documentation for them on securely configuring and operating the TOE (OE.Administrators, Operators, Officers and Auditors guidance documentation).
3. It must be ensured that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE. (OE.Cooperative Users)
4. All staff members in trustworthy roles shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated. (OE.CPS)
5. Proper authorities must be notified of any security issues that impact their systems to minimize the potential for the loss or compromise of data. (OE.Notify Authorities of Security Issues)
6. Training for staff in trustworthy roles must be provided in techniques to thwart social engineering attacks. (OE.Social Engineering Training)
7. It must be ensured that users change their authentication data (their passwords, activating numbers, PINs) at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) through enforced authentication data management. (OE.Authentication Data Management)
8. Proper disposal of authentication data and associated privileges must be provided after access has been removed (e.g., job termination, change in responsibility). (OE.Disposal of Authentication Data)
9. Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security. (OE.Installation)
10. The IT-environment of the TOE must use such an operating system which provides domain separation and non-bypassability of the security functions. (OE.Operating System)
11. Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security. (OE.Physical Protection)
12. The system must be protected against a physical attack on the communications capability by providing adequate physical security. (OE.Communication Protection)
13. Appropriate integrity protection must be provided for user data and software. (OE.Integrity protection of user data and software)

14. Integrity protection must be provided to detect modifications to firmware, software, and backup data. (OE.Detect modifications of firmware, software, and backup data)
15. Malicious code prevention procedures and mechanisms must be applied. (OE.Procedures for preventing malicious code)
16. Automated notification (or other responses) must be implemented to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent. (OE.React to detected attacks)
17. Inspection of downloads/transfers must be required. (OE.Require inspection for downloads)
18. A trusted path must be provided between the user and the system. A trusted path must be provided to security-relevant (TSF) data in which both end points have assured identities. (OE.Trusted Path)
19. It must be ensured that security-relevant software, hardware, and firmware are correctly functioning through features and procedures. (OE.Validation of security function)
20. The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and validated cryptographic modules must be used. (OE.Cryptographic functions)
21. Data assets must be protected when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users. (OE.Data import/export)
22. Periodic integrity checks must be provided on both system and software. (OE.Periodically check integrity)

23. Security-relevant events must be identified and monitored, and must be reviewed by system auditors at a frequency rate sufficient to address risks (OE.Auditors Review Audit Logs).
24. Audit records must be protected against unauthorized access, modification, or deletion to ensure accountability of user actions. (OE.Protect stored audit records)
25. Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events. (OE.Respond to possible loss of stored audit records)
26. Authentic time value must be provided to time-dependent certification services and to ensure that the sequencing of audit events can be verified. (OE.Time stamps)

27. Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code. (OE.Object and data recovery free from malicious code)
28. The secure state of the system must be preserved in the event of a secure component failure and/or the system must be recovered to a secure state. (OE.Preservation/trusted recovery of secure state)
29. Sufficient backup storage and effective restoration must be provided to ensure that the system can be recreated. (OE.Sufficient backup storage and effective restoration)

30. Tools and techniques must be used during the development phase which ensure that security is designed into the TOE. Flaws during the operational phase must be detected and resolved. (OE.Lifecycle security)

31. The vendor repairs security flaws that have been identified by a user. (OE.Repair identified security flaws)

Other conditions of secure usage

32. Usage in operating environment of Info&AA system is limited exclusively to the operational mode supported by the HSM module; software mode supports only testing purposes.
33. The system must only be used by identification and authentication by a hardware token.
34. In the operating system the Code Signing checking must be set as a mandatory check, for automatic integrity checking of executable files signed by Code Signing.
35. Proper administrative measures must be applied in order to generate the security-critical InfoAA.sso system file. These measure must provide for the following:
    a. Private keys linked to the SSO certificates must be generated in such tokens that guarantee that the private key can not be disclosed and protect the key from the unauthorized access.
    b. The file InfoAA.sso must be generated in the presence of the system auditor in order to guarantee the double human control.
    c. The auditor must produce a report about the generation of the InfoAA.sso file. The report should contain the time of generation, types of tokens used, their identification data and data regarding the token holders.
36. Proper administrative measures must be followed during the issue of the SO, PO and RO rights. These measure must provide for
    a. Private keys linked to the SO, PO and RO certificates must be generated in such tokens that guarantee that the private key can not be disclosed and protect the key from the illegitimate access.
    b. The SSO must produce a report about the issue of SO right, and the SO must make a report about the issue of the SSO, PO and RO rights. The report should contain the time of generation, types of tokens applied, their identification data and data regarding the token holders.
37. The system administrator must provide that the users can not access other components with execution right than that they have to use in normal operational mode.
38. The system administrator has to check the correct load of the ACRL profiles at every system start.

Conditions resulting from the confoormance to the MSZ CWA 14167-1 requirements

39. The IT environment must provide and manage the system administrator, system operator and system auditor roles.
40. The IT environment must provide for usage of applicable HSM module in order to store the private key used for the signing of the attribute certificates, and for maintaining the usage terms determined during the certification of the HSM module.
41. For audit events that are occurred due to auditing storage failure, IT and non-IT procedures must be enforced.
42. Verification of digital signatures on audit records (i.e. justification of audit log integrity) must be ensured by the IT environment.
43. Confidentiality of data in the attribute certificate requests must be provided in the IT-environment.
44. Periodically it must be checked that the algorithms applied in Info&AA system meet the requirements of the document „Secure algorithms" [1]
45. IT and non-IT procedures must be enforced in order to achieve the following requirements:
    [[SO2.1]; [SO2.2]; [SO2.3]; [SO3.1] NQCA; [SA1.2]; [KM1.2]; [KM1.3]; [KM1.4]; [KM1.7]; [KM3.1]; [KM4.1]; [KM4.2]; [KM5.1; [KM5.2]; [KM5.3]; [KM5.4]; [KM6.1]; [KM6.2]; [KM6.3]; [KM6.4]; [KM6.5]; [KM6.6]; [AA2.1]; [AA2.2]; [AA4.1]; [AA4.2]; [AA5.1]; [AA6.1]; [AA8.1]; [AR1.1]; [AR1.2]; [AR1.3]; [AR1.4]; [AR2.1]; [AR3.1]; [BK1.1]; [BK1.2]; [BK1.3]; [BK2.1] NQCA; [BK2.2]; [BK3.1]; [BK3.2]; [R1.1]; [R1.2]; [R1.4]; [R1.5] QCA; [R1.6]; [R2.1]; [CG2.2]; [D1.1]; [D1.2]; [D2.1]; [RM1.1]; [RM1.4]; [RM1.5]; [RM2.1];

[1] Annex 3.: ETSI SR 002 176-1 v2.0.0

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 14167-1:2003 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

MSZ CWA 14167-1:2006 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

ETSI SR 002 176-1 v2.0.0 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

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

Attribute service provider software (Info&AA) v1.0 – **Security target** (v1.0)
Installation guide - Info&AA Attribute certificate issuing software v1.0 (v1.0)
Overview of trustworthy roles - Info&AA Attribute certificate issuing software v1.0 (v1.0)
InfoAA Administrators' manual (v1.0)
InfoAA RA manual (v1.0)
InfoAA Policy Manager manual (v1.0)
Security architecture - Attribute service provider software (Info&AA) v1.0 (v1.0)
Functional specification - Attribute service provider software (Info&AA) v1.0 (v1.0)
TOE design - Attribute service provider software (Info&AA) v1.0 (v1.0)
Implementation representation - Attribute service provider software (Info&AA) v1.0 (v1.0)
Configuration list - Attribute service provider software (Info&AA) v1.0 (v1.0)
Configuration management documentation - Attribute service provider software (Info&AA) v1.0 (v1.0)
Development security - 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 service provider software (Info&AA) v1.0 (v1.0)
Target of evaluation suitable for testing (v1.0)
Attribute service provider software (Info&AA) v1.0 **Test plan** (v1.0)
Attribute service provider software (Info&AA) v1.0 **Test documentation** (v1.0)
Attribute service provider software (Info&AA) v1.0 **Test coverage analysis** - ATE_COV.2 (v1.0)
Attribute service provider software (Info&AA) v1.0 **Test depth analysis** - ATE_DPT.2 (v1.0)

Developers-independent documents examined during certification

Evaluation report – Info&AA v1.0 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 Info&AA v1.0 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"