CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 113/2007 of the Minister of the Ministry of Economy and Transport of the Republic of Hungary
based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

certifies

that the

InfoCA trustworthy system for Certification Service Provider services v2.5

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 for qualified certification service provider and for not qualified certification service provider, according to the Act XXXV of 2001

This certificate has been issued on the basis of the certification report No. HUNG-TJ-048-2009.
Produced on commission of MÁV INFORMATIKA Ltd.

Certificate registration number: **HUNG-T-048-2009.**
Date of certificate: 19.08.2009.
Validity period of the certificate: 19.08.2012.
Annexes: attributes, conditions, requirements and other features on six pages.

L.S.

Endrődi Zsolt Certification director	dr. Szabó István Managing director

Annex 1

Summary of the main features of InfoCA v2.5

The InfoCA trustworthy system for certification service provider v2.5 (abbr.: InfoCA system) is a specific electronic signature product that provides different functions regarding certification services.

The InfoCA system supports the following certification services:

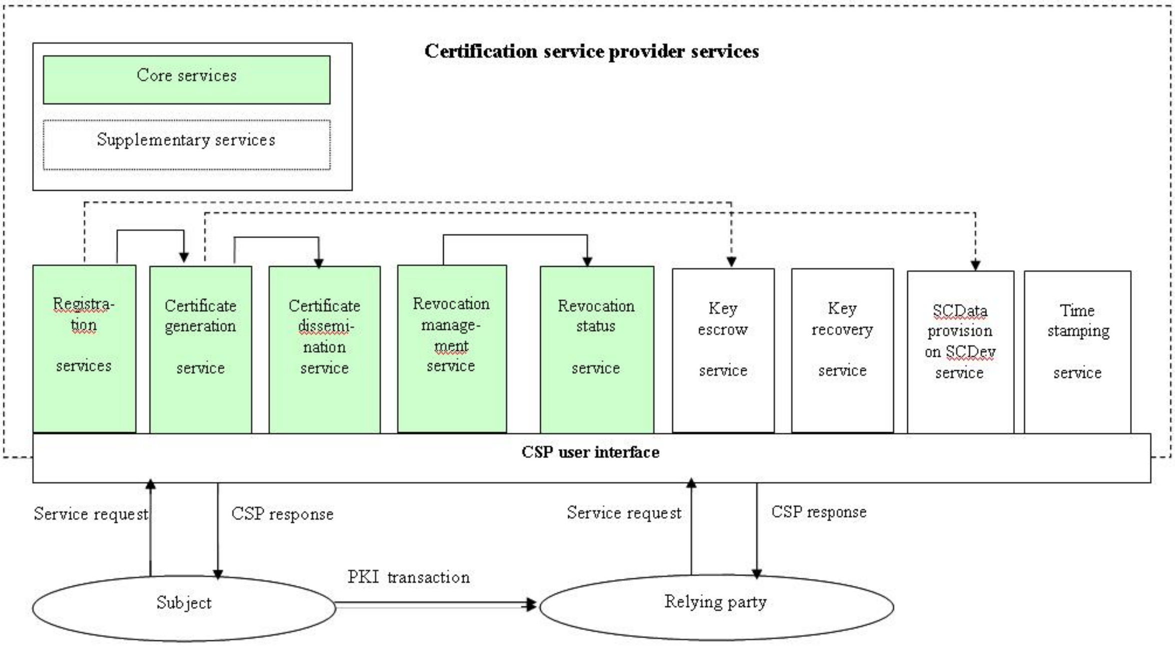
Core (mandatory) services:

- Registration service (achieved outside the scope of the InfoCA system, though its results are used by the InfoCA system);
- Certificate generation service;
- Certificate dissemination service;
- Revocation management service;
- Revocation status information service (CRL, OCSP).

Supplementary (optional) services:

- Key escrow for encrypting private keys service;
- Key recovery for encrypting private keys service.
- Provision of signature creation data (SCD) on signature creation device service (outside the InfoCA system);
- Time-stamping service.

The InfoCA system has been basically designed to function as a certification service provider’s trustworthy system, which implements (core and supplementary) certification services provided by the CA, or gives technical support for the implementation, as it is depicted in figure 1. (Note that the registration and provision of SCD on signature creation device services are achieved by InfoCA system environment.)



1. ábra Az InfoCA v2.5 általános felépítése

Annex 2

Secure usage conditions

Assumptions for the InfoCA v2.5 IT environment

The following assumptions (also specified in the Security Target) are made for the IT environment:

Personnel assumptions

1. Audit logs are required for security-relevant events and must be reviewed by the system auditor. (A.Auditors Review Audit Logs)
2. In the operational environment of the InfoCA an authentication data (password and PIN) management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (A.Authentication Data Management)
3. Competent administrators, operators, officers and auditors will be assigned to manage the InfoCA and the security of information it contains. (A.Competent Administrators, Operators, Officers and Auditors)
4. All administrators, operators, officers, and auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the InfoCA is operated. (A.CSP)
5. Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility). (A.Disposal of Authentication Data)
6. Malicious code destined for the InfoCA is not signed by a trusted entity. (A.Malicious Code Not Signed)
7. Administrators, operators, officers, auditors, and other users should notify proper authorities of any security issues that impact the InfoCA system to minimize the potential for the loss or compromise of data. (A.Notify Authorities of Security Issues)
8. General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks. (A.Social Engineering Training)
9. Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the InfoCA and are expected to act in a cooperative manner. (A.Cooperative Users)

Connectivity assumptions

10. The operating system has been selected to provide the functions required by the InfoCA to counter the perceived threats identified in the security target chapter 3.3. (A.Operating System)

Physical assumptions

11. The InfoCA system is adequately physically protected against loss of communications i.e., loss of the availability of communications. (A.Communications Protection)
12. The InfoCA hardware, software, and firmware critical to TOE security policy (TSP) enforcement will be protected from unauthorized physical modification. (A.Physical Protection)

Other conditions of secure usage

1. Usage in operating environment of InfoCA system is limited exclusively to the operational mode supported by the HSM module; software mode supports only testing purposes.
2. The IT environment must provide and manage the system administrator , system operator and system auditor roles.
3. The IT environment (operating system) must provide for protection of printed PINs as sensitive residual data produced for internal and external users.
4. The IT environment must provide for usage of applicable HSM module, and maintaining the usage terms determined during the certification of the HSM module.
5. The IT environment must provide for the possibility of checking the root certificate's hash in order to guarantee the correctness of the certificate, by providing information through a trusted path.
6. During InfoCA system operation the exclusive usage of proper certificate profiles must be ensured.
7. In case of a trustworthy system issuing electronic signing certificates the key escrow function must be disabled in the signing certificate profiles.
8. Integrity of the executable files of the InfoCA system must be provided by the IT environment.
9. In case of a trustworthy system issuing qualified electronic signing certificates the InfoCA system must be installed by "noreq" version of ExitConfig.dll.
10. For logging events that are done due to auditing storage failure, IT and non-IT procedures must be enforced.
11. Verification of digital signatures on audit events (i.e. justification of audit log integrity) must be ensured by the IT environment.
12. Confidentiality of information exchanged between RA and CA subsystems must be ensured by the IT environment.
13. Validity of certificates to be renewed must be ensured by IT and non-IT procedures.
14. The IT environment must establish trusted channel between the OCSP subsystem and the CA subsystem, and must ensure that the OCSP subsystem responses the actual status of the certificate under processing.
15. Periodically it must be checked that the algorithms applied in InfoCA system meet the requirements of the document „Secure algorithms" [1]".
16. IT and non-IT procedures must be enforced in order to achieve the following CWA-14167-1 requirements:
    [M1.4] QCA ;[SO2.1]; [SO2.2]; [SO2.3] ;[SO3.1] QCA; [SO3.1] NQCA; [IA2.2] QCA; [SA1.2]; [KM1.2]; [KM1.3]; [KM1.4]; [KM1.7]; [KM2.4]; [KM2.6]; [KM3.1]; [KM3.2] QCA; [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; [BK2.1] QCA; [BK2.2]; [BK3.1]; [BK3.2]; [R1.1]; [R1.2]; [R1.3] QCA; [R1.4]; [R1.5] QCA; [R1.6]; [R2.1]; [R3.1]; [CG1.2]; [CG1.3]; [CG2.1]; [CG2.2]; [CG2.3]; [CG2.4]; [CG3.1]; [D1.1]; [D1.2]; [D2.1]; [RM1.1]; [RM1.4]; [RM1.5]; [RM2.1]; [RS2.2], [TS1.1], [TS2.1], [TS2.2], [TS4.2], [TS4.3], [TS4.4], [TS4.6], [TS6.1], [SP1.1]; [SP1.3]; [SP1.4]; [SP1.5]; [SP1.6]; [SP1.7]; [SP2.1]; [SP3.1]; [SP3.2]

[1] See 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 TS 101 862 v1.3.3 Qualified Certificate profile

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 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol

RFC 3161 X.509 Internet Public Key Infrastructure - Time-Stamp Protocol

RFC 5280: X.509 Internet Public Key Infrastructure - Certificate and CRL Profile

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

- InfoCA v2.5 Trustworthy system for certification service provider (CSP) service - Security target - v1.1
- Installation manual v1.8 – InfoCA CSP software, v2.5
- Administrators' guide v1.11 – InfoCA CSP software, v2.5
- RA manual – Trust&CA CSP software v2.0 (unchanged since the previous certification)-v1.0
- InfoCA v2.5 Trustworthy system for certification services – Functional specification -v1.1
- InfoCA v2.5 Trustworthy system for certification services – High level design -v1.1
- InfoCA v2.5 Trustworthy system for certification services – Low level design-v1.1
- InfoCA v2.5 Trustworthy system for certification services - Conformance analysis -v1.1
- InfoCA v2.5 Trustworthy system for certification services – Security policy model -v1.1
- InfoCA v2.5 Trustworthy system for certification services – Configuration management documentation -v1.2
- InfoCA v2.5 Trustworthy system for certification services - Development security documentation - v1.1
- InfoCA v2.5 Trustworthy system for certification services - Developers' tools documentation -v1.1
- InfoCA v2.5 Trustworthy system for certification services - Lifecycle documentation - v1.1
- InfoCA v2.5 Trustworthy system for certification services - Flaw reporting procedures -v1.1
- Test documentation (test records): TJ_090511_OCSP.rtf (OCSP, software); TJ_090609_OCSP.rtf (OCSP, Luna with HSM); TJ_090710_OCSP.rtf (OCSP, nShield with HSM); TJ_090511_TSS.rtf (TimeStamp, software); TJ_090526_TSS.rtf (TimeStamp, Luna with HSM); TJ_090710_TSS.rtf (TimeStamp, nShield with HSM)-
- InfoCA v2.5 Trustworthy system for certification services - Test coverage analysis -v1.1
- InfoCA v2.5 Trustworthy system for certification services - Test depth analysis -v1.1
- InfoCA v2.5 Trustworthy system for certification services – Analysis of guides -v1.1
- InfoCA v2.5 Trustworthy system for certification services - Vulnerability assessment -v1.1
- Analysis of Strength of security -v1.0 – Trust&CA CSP software v2.0 (unchanged since the previous certification)

Developers-independent documents examined during certification

Evaluation report - InfoCA v2.5 trustworthy system for certification services v1.1 (produced by HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The independent evaluation and certification of InfoCA v2.5 system has been done according to the methodology of CEM (Common Evaluation Methodology) v2.3.

Evaluation level

EAL4+ (augmented by ALC_FLR.2 Flaw reporting procedures)

Documents about methodology used during evaluation

- MSZ/ISO/IEC 15408:2003 Information technology – Security technology – Common Criteria of Information Security Evaluation
- Common Criteria for Information Technology Security Evaluation (CC) Part 1: Introduction and general model - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 2: Security functional requirements - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 3: Security assurance requirements - Version 2.3, August 2005
- Common Methodology for Information Security Evaluation (CEM), Version 2.3, August 2005