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

TRUST&CA trustworthy system for Certification Service Provider services v2.0

developed by

ProfiTrade 90 Ltd. and 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-036-2007.
Produced on commission of MÁV INFORMATIKA Ltd.

Certificate registration number: **HUNG-T-036-2007.**
Date of certificate: 24.07.2007.
Validity period of the certificate: 24.07.2010.
Annexes: attributes, conditions, requirements and other features on six pages.

HunGuard Kft.
1123 Budapest, Kékgolyó u. 6.
Adószám: 10398221-2-43

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Summary of the main features of TCA v2.0

The TRUST&CA trustworthy system for certification service provider v2.0 (abbr.: TCA system) is a specific electronic signature product that provides different functions regarding certification services.
The TCA system supports the following certification services:
Core (mandatory) services:

- Registration service (achieved outside the scope of the TCA system, its results are used by TCA system);
- Certificate generation service (functionality: initial certificate generation, certificate renewal, certificate refresh), which generates standard X.509 certificates;
- Certificate dissemination service (functionality: certificate export to LDAP, LDAP reconstruction from database);
- Revocation management service (functionality: certificate revocation, certificate suspension, certificate re-validation;)
- Revocation status information service (functionality: CRL publication to LDAP, CRL export to files).

Supplementary (optional) services:

- Provision of signature creation data (SCD) on signature creation device service (functionality: key-pair generation, public key import, certificate export);
- Key escrow for encrypting private keys service (functionality: key escrow);
- Key recovery for encrypting private keys service (functionality: recovery).

The TCA 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 service is achieved by TCA system environment.)

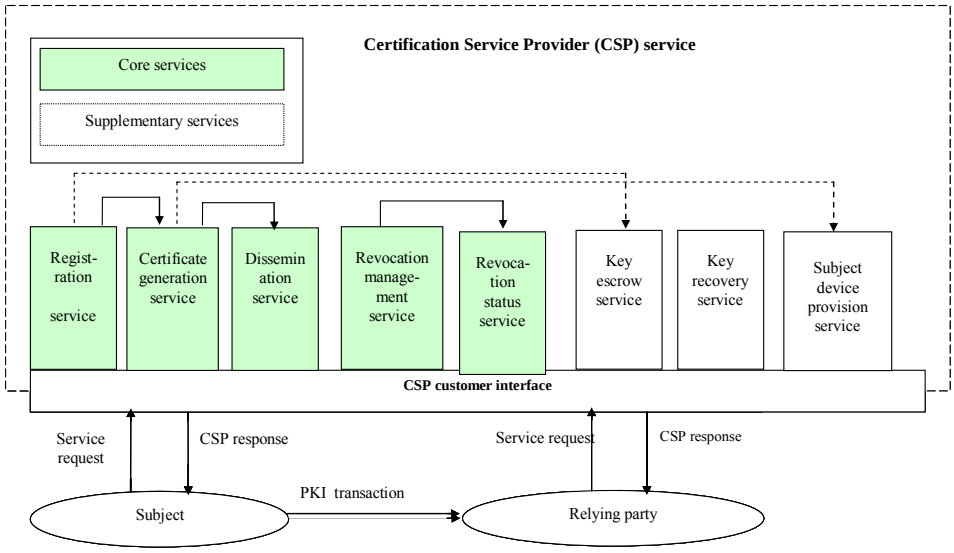

Figure 1. Overall architecture of TCA v2.0

Annex 2

Secure usage conditions

Assumptions for the TCA v2.0 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. 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 TOE and the security of the 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 TOE 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 TOE is not signed by a trusted entity. (A.Malicious Code Not Signed)
7. Administrators, operators, officers, auditors, and other users notify proper authorities of any security issues that impact their systems 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 TOE 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 TOE to counter the perceived threats identified in the security target chapter 3.3. (A.Operating System)

Physical assumptions

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

Annex 2

Other conditions of secure usage

1. Usage in operating environment of TCA system is limited exclusively to the HSM module usage mode; 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.
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 TCA 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 TCA system must be provided by the IT environment.
9. In case of a trustworthy system issuing qualified electronic signing certificates the TCA 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. 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]; [CG3.1]; [D1.1]; [D1.2]; [D2.1]; [RM1.1]; [RM1.4]; [RM1.5]; [RM2.1]; [SP1.1]; [SP1.3]; [SP1.4]; [SP1.5]; [SP1.6]; [SP1.7]; [SP2.1]; [SP3.1]; [SP3.2]

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 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

Standards

RFC3280 Certificate and Certificate Revocation List (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

- TRUST&CA v2.0 Trustworthy system for certification service provider (CSP) service– Security target v1.0
- Configuration management documentation -Trust&CA CSP software v2.0 -v1.0
- Installation manual – Trust&CA CSP Service software v2.0 - v1.0
- TRUST&CA v2.0 Trustworthy system for certification services – Functional specification - v1.0
- TRUST&CA v2.0 0 Trustworthy system for certification services– High level design v1.0
- TRUST&CA v2.0 0 Trustworthy system for certification services – Low level design v1.0
- Conformance analysis - Trust&CA CSP software v2.0 - v1.0
- Administrator's manual – Trust&CA CSP software v2.0 - v1.0
- RA manual – Trust&CA CSP software v2.0 - v1.0
- Development security documentation - Trust&CA CSP software v2.0 - v1.0
- Lifecycle documentation –Trust&CA CSP software v2.0 - v1.0
- Flaw reporting procedures –Trust&CA CSP software v2.0- v1.0
- Developers' tools documentation -Trust&CA CSP software v2.0 - v1.0
- Test documentation – Trust&CA teszt jegyzőkönyv_fin.doc and Trust&CA teszt jegyzőkönyv_fin_nshield.doc
- Test coverage analysis -Trust&CA CSP software v2.0 - v1.0
- Test depth analysis -Trust&CA CSP software v2.0 - v1.0
- Assessment of manuals –Trust& CSP software v2.0 - v1.0
- Analysis of strength of security functions – Trust&CA CSP software v2.0 - v1.0
- Vulnerability assessment – Trust&CA CSP v2.0 - v1.0

Developers-independent documents examined during certification

Evaluation report - TRUST&CA v2.0 trustworthy system for certification services (produced by HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The independent evaluation and certification of TCA v2.0 system has been done according to the methodology of CEM (Common Evaluation Methodology) v2.3.

Evaluation level

EAL4

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