CERTIFICATE REVIEW RECORD

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) and as a product certification authority accredited by the National Accreditation Body by the document No. NAT-6-0048/2011

in Certificate Review Process

examined

the statements included in the

CERTIFICATE HUNG-T-047-2009,

content of which has been compared to the new requirements laid down in resolutions EF-26838-8/2011, EF-26838-9/2011, EF-26838-10/2011, EF-26838-11/2011, EF-26838-12/2011, EF-26838-13/2011 issued by NMHH and states the following:

Usage conditions for certification provider services of

ProtectServer Orange (korábbi nevén CSA8000 Adapter)

hardver verzió: G revizió, Cprov förmver verzió:1.10

electronic signature product
developed by

Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd.

are modified with the following restrictions:

1. Use of SHA-1 or weaker hash algorithm is forbidden after 01 January 2012.
2. Minimal modulus length (MinModLen) should be at least 2048 bits in case of RSA signing algorithm.
3. Minimal p prime length (pMinLen) should be 2048 bits, minimal q prime length (qMinLen) should be 224 bits in case of DSA signature algorithm.

Registration number of this Certificate Review Record: **HUNG-FJ-047/1-2011**
Budapest, 15 December, 2011

LS

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

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 Communications Decree 9/2005. (VII.21)

certifies that

ProtectServer Orange (former name CSA8000 Adapter)

hardware version: G revision, Cprov firmware version:1.10

electronic signature product

manufactured and sold by
Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd
in the case of the realization of all conditions in Annex 1.

is suitable for*

the secure operation of a qualified certification service provider
who provides the following services:

Within the scope of electronic signature certification service:
Generating, storing (qualified) certificate signing keys, signing, saving and recovering (qualified) certificates;
Within the scope of time stamping service:
Generating, storing timestamp signing keys, signing timestamp;
Within the scope of placement of signature creation data in a signature creation device service:
Generating subscriber (signing) key pair;
Within the scope of secure operation of the qualified certification service provider's own information system:
Generating, storing and using infrastructural and reliable management keys.

This certificate was released on the basis of the evaluation report HUNG-TJ-047-2009.
This certificate was released at the request of Netlock Informatics and Network Privacy Services Ltd.

Registration number: **HUNG-T-47/2009.**
Date of the certification: 26 June 2009
Validity of this certification beside yearly revision: 26 June 2012
Annexes: conditions, requirements, documents in seven pages.

SEAL

Endrődi Zsolt
Certification Director:

dr. Szabó István
Managing director

* Considering the fact that both the ETSI TS 102 176-1 V2.0.0 and its resultant decisions HL-21917-9,10,11,12,13,14/2008 by the Hungarian National Communications Authority do not recommend SHA-1 algorithm for electronic signatures from 2009, in case the National Communications Authority prohibits the usage of this algorithm or specific data will be published disclosing the weaknesses of this, then the Certification Authority will withdraw the validity of this certificate.

Annex 1.

Validity conditions of the certificate

CSA 8000 adapter is a sophisticated cryptographic device that was designed for general usage and to satisfy the wide range of user demands. Accordingly many security attributes can be configured in the device.

Operation in FIPS 140-1 mode (which places on security instead of efficiency and user-friendly operation) demands many configuration settings, and complying with these settings are the main conditions of validity.

If the CSA 8000 adapter is used by a qualified certification service provider for its security critical activities (to sign the issued certificates and timestamp responses) it has to comply with further requirements which limit the usability demanding more complementary conditions to be met.

Hereunder we summarize the conditions that collectively form the basis of this certificate's validity.

I. General validity conditions

The following conditions are necessary for every utilization modes (the whole general utilization scope designed by the manufacturer) for reliable and secure operation.

1. Those persons who have different roles in connection with the services of CSA 8000 adapter (Admin, Admin Security Officer, Token Security Officer, Token User):
   - are competent, qualified and reliable;
   - keep the mandatory activities defined by different guides (CSA8000 Adapter Installation Guide, Cprov Installation Guide, Cprov Administration Manual, Cprov Key Management Utility User Manual).

II. Validity conditions arising from FIPS 140-1 conformity

The following conditions are essential for the CSA 8000 adapter to meet FIPS 140-1 Level 3 requirements.

2. Cryptographic functionality in connection with digital signature must be restricted to the following algorithms: **DSA, RSA (PKCS #1), SHA-1**.

3. The following security configurations must be applied:
   - CKF_ENTRUST_READY ("Entrust Compliant" flag) mandatory value: **FALSE**
   - CKF_ALWAYS_SENSITIVE ("No Clear PINs" flag) mandatory value: **TRUE** (SET)
   - CKF_AUTH_PROTECTION ("Session Protection" flag) mandatory value: **TRUE** (SET)
   - CKF_MODE_LOCKED ("Lock Security Mode" flag) mandatory value: **TRUE** (SET)
   - CKF_NO_PUBLIC_CRYPTO ("No Public Cryptography" flag) mandatory value: **TRUE** (SET)

4. During the set up phase new values must be set for HIMKs and the default HIMK values must be cleared.

5. During the set up phase the Administrator role's default user name and password must be changed.

6. Operators must keep their PIN number secret.

7. For every new slot configured the PIN numbers must be at least 4 digits.

III. Complementary conditions for use in qualified certification service

A qualified certification service provider must maintain the following complementary conditions when using the CSA 8000 adapter:

8. Minimal modulus length (MinModLen) must be at least 1020 bit in case of RSA signing algorithm.

9. Minimal p prime length (pMinLen) must be 1024 bit, minimal q prime length must be 160 bit in case of DSA signature algorithm.

10. Only blocks with bit length divisible by 8 can be signed digitally.

11. Those keys which are used to sign qualified certificates are only useable for signing qualified certificates and possibly to sign their certificate revocation lists.

12. The module must take care of key protection when a stored key from a secure cryptographic module is exported. Storing sensitive key data in non-secure mode is prohibited. Storing and saving a qualified certificate signing key is only permitted if other additional security mechanisms are used. This can be done using one of the following:

- "m from n" technique (that is not supported by CSA 8000 but it is later achievable through its standard interface) where m is the quantity of those components from the whole n components which are necessary for the successful initialization of the key. For the recovery from error state the m = 60% * n value is proposed (that is if n=3 then m=2, if n=4 then m=3, if n=5 then m=3, and so on).
- with the following (CSA 8000 supported) methods:
  - saving to a smart card (token),
  - it is encoded by 3DES algorithm,
  - the Key Encryption Key is made from two random components and in compliance with this the simultaneous presence of at least two authorized person is necessary for recovering the private key.

13. Those signing keys that are used for time stamping are only applicable for signing timestamps.

14. In the placement of signature creation data in a signature creation device service if the generation of the subscriber's signing key pair occurs outside the signature creation device (inside the CSA 8000 cryptographic hardware) it must be assured that signing keys for electronic signature are different from other keys, e.g. keys for encryption.

15. In the placement of signature creation data in a signature creation device service if the generation of the subscriber's signing key pair occurs outside the signature creation device (inside the CSA 8000 cryptographic hardware) a secure path between the CSA 8000 cryptographic module and the signature creation device must be assured. This path must assure confidentiality, integrity and authenticity by proper cryptographic mechanisms.

16. This certificate is only valid for the current hardware and firmware version /hardware version: G revision, Cprov firmware version:1.10/. Upgrade of a new firmware version is only applicable if the following requirements are realized:
  - the new firmware version is authenticated by the developer,
  - the new firmware version was evaluated by an accredited laboratory and a new FIPS certificate was released,
  - usability of the new firmware version in qualified certification service is certified by a designated native organization, and the new version is included in the secure signing products register of the Hungarian National Communications Authority.

IV. Other notes that influence validity

17. Certificates issued by the National Institute of Standards and Technology (NIST) are valid until revocation. So hardware, firmware and software products in the certificates are usable in an unchanged form.

18. Those modules which are certified according to FIPS 140-1 are still secure. FIPS 140-1 certificates should not be issued after 26 May 2002.

19. Currently there is no information in public sources that may influence the secure operation of the module. Performing this examination is necessary in every 3 years.

Annex 2.
PRODUCT SUITABILITY REQUIREMENTS
Requirements document

Act XXXV of 2001 on electronic signature

Decree 3/2005. (III.18.) IHM on detailed requirements of services in connection with electronic signature and its service providers

FIPS 140-1: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-1

ETSI TS 101 456 v1.4.3 Policy Requirements for Certification Authorities Issuing Qualified Certificates

ETSI TS 102 176-1 V2.0.0 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

CEN 14167-1:2003 Workgroup Agreement: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

Annex 3.
Documents considered in the certification

Request for the certification

CEN 14167-2:2002 workgroup agreement: Cryptographic Module for CSP Signing Operation – Protection Profile (CMCSO-PP, HSM-PP)

CEN 14167-3:2003 workgroup agreement: Cryptographic Module for CSP Key Genaration Services – Protection Profile (CMCKG-PP, HSM-PP)

FIPS 140-1 Validation Certificate No. 160 /CSA8000 Cryptographic Adapter/

ERACOM: CSA8000 Cryptographic Adapter, Hardware Revision: G, Firmware Version: 1.1, FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

CSA8000 Adapter Installation Guide /Version: A4, Date: 7 May 2001/

Cprov Installation Guide /Version: 3.0, Revision A6, Last Modified: 7 May 2001/

Cprov Administration Manual /Version: 3.0, Revision A7/ May 2001/

Cprov Key Management Utility User Manual /KMU Version: 3.0 Beta, Revision A1/ May 2001/

Eracom Technologies official notification about name change of CSA 8000 Adapter

Frequently Asked Questions for the Cryptographic Module Validation Program