CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 002/2006 of the Minister of the Ministry of Informatics and Communication (MIC) of the Republic of Hungary based on the MIC Decree 9/2005. (VII.21)

certifies that

CryptoServer 2000

hardware version: 1.0.2.0, firmware version:1.0.0.2
electronic signature product

manufactured and sold by

Utimaco Safeware AG

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-035-2006.
This certificate was released at the request of Safesoft Ltd.

Registration number: **HUNG-T-035-2006.**
Date of the certification: 7 December 2006
Validity of this certification beside yearly revision: 7 December 2009
Annexes: conditions, requirements, documents in 7 pages.

SEAL

Endrődi Zsolt
Certification Director

dr. Szabó István
Managing director

Annex 1.

Validity conditions of the certificate

Utimaco CryptoServer 2000 module 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 140-2 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 Utimaco CryptoServer 2000 module 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 Utimaco CryptoServer 2000 module (Cryptographic User, Administrator):
   - are competent, qualified and reliable;
   - keep the mandatory activities defined by different guides (CryptoServer 2000 - Administrator's Guide for CryptoServer in FIPS-Mode).

II. Validity conditions arising from FIPS 140-2 conformity

The following conditions are essential for the CryptoServer 2000 module to meet FIPS 140-2 Level 3 requirements.

For the setup and first personalization of CryptoServer 2000 the following services must be done, as described in the CryptoServer 2000 Administrator's Guide for CryptoServer in FIPS-Mode document.

2. The preconditions must be fulfilled.

CryptoServer 2000 module must be in personalization mode and initialized state.

Furthermore all firmware modules that are mandatory in FIPS mode are needed and properly signed with the customer specific Initialization Key. The required modules are the followings:

- SMOS: file ‘smos.mtc’, version 1.0.3.7
- CMDS: file ‘cmds.mtc’, version 1.0.5.0
- UTIL: file ‘util.mtc’, version 1.0.6.0
- ADM: file ‘adm.mtc’, version 1.0.2.0
- DB: file ‘db.mtc’, version 1.0.1.1
- VDES: file ‘vdes.mtc’, version 1.0.0.3
- VRSA: file ‘vrsa.mtc’, version 1.0.3.3
- AES: file ‘aes.mtc’, version 1.0.0.0
- HASH: file ‘hash.mtc’, version 1.0.1.0
- LNA: file ‘lna.mtc’, version 1.0.3.0
- ASN1: file ‘asn1.mtc’, version 1.0.1.1
- CSI: file ‘csi.mtc’, version 1.0.0.3
- FIPS140: file ‘fips140.mtc’, version 1.0.0.2

Furthermore the smart card with CryptoServer’s Initialization Key is available.

3. In order to be able to administrate the CryptoServer, it is a basic requirement that the customer-specific Initialization Key is loaded.

4. Perform a GetState command. The CryptoServer should be in initialized state and the alarm state should be ‘off’.

5. For further personalization of the CryptoServer the private part of the customer specific Initialization Key (which is usually on the smart card) is needed.

6. Set the CryptoServer’s clock with the BLSetRTC command.

7. Load the base firmware modules (SMOS, CMDS, ADM and UTIL, as MTC files) using the BLLoadFile command.

8. Start the base firmware modules with the StartOS command.ű

9. Verify if the CryptoServer is now in operational state using the GetState command.

10. Load all other firmware modules that are listed above with the LoadFile command.

11. Verify whether the CryptoServer is now in FIPS mode and is not in any error state (using the GetState command).

III. Complementary conditions for use in qualified certification service

A qualified certification service provider must maintain the following complementary conditions when using the Utimaco CryptoServer 2000 module:

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

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

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

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

16. 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 Utimaco CryptoServer 2000) 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 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.

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

18. 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 Utimaco CryptoServer 2000 module) it must be assured that signing keys for electronic signature are different from other keys, e.g. keys for encryption.

19. 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 Utimaco CryptoServer 2000 module) a secure path between the Utimaco CryptoServer 2000 module and the signature creation device must be assured. This path must assure confidentiality, integrity and authenticity by proper cryptographic mechanisms.

20. This certificate is only valid for the current hardware and firmware version /hardware version: 1.0.2.0, firmware version:1.0.0.2/. 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.

21. Because of the vulnerability of MD5 hashing algorithm the usage of this algorithm is prohibited in the operation of the Certification Authority.

IV. Other notes that influence validity

22. 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.

23. 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

Directive 2/2002 (IV.26) MeHVM on security requirements of qualified electronic signature services and its service providers

FIPS 140-2: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-2

ETSI TS 101 456 v1.3.1 Policy Requirements for Certification Authorities Issuing Qualified Certificates

ETSI TS 102 176-1 V1.2.1 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

Questionnaire 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 140-2 Validation Certificate No. 543 / Utimaco CryptoServer 2000/

CryptoServer Security Policy /Version 1.1.4, Doc. No.: 2004-0007, 9th May 2005/

CryptoServer 2000 Administrator's Guide for CryptoServer in FIPS-Mode /Version 1.0.2, Doc. No.: 2004-0002, 26th January 2005/