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

Luna CA^3 cryptographic token

hardware version: 2, firmware version: 3.102
manufactured and distributed by
SafeNet Inc.

electronic signature product

in case of fulfilment of criteria detailed in Annex 1

is suitable for

a) the secure operation of the following activities of a **qualified certification service provider**:

Within the scope of electronic signature certification service:

Generating, storing, saving and recovering qualified certificate signing keys, and signing qualified certificates;

Within the scope of time stamping service:

Generating and storing timestamp signing keys, and signing timestamps;

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.

b) generating advanced electronic signatures:

providing trustworthy base cryptographic support and secure runtime environment.

This certificate has been issued on the basis of the certification report HUNG-TJ-040-2008.
Produced on commission of The Hungarian Prime Minister's Office Electronic Government Centre.
Registration number: **HUNG-T-040-2008.**
Date of the certification: February 13, 2008
Validity of this certificate in case of yearly revision: February 13, 2011
Annexes: conditions, requirements, documents in six pages.

LS

Endrődi Zsolt	dr. Szabó István
Certification director	Managing director

Annex 1

Validity conditions of this certificate

The Luna CA^3 module is a complex cryptographic device that was designed for general usage and to satisfy a wide range of user needs. Accordingly, many security attributes can be configured on/off in the device.

Operation in FIPS 140-1 mode (which focuses on security at the expense of efficiency and user-friendly operation) requires several configuration settings, and complying with these settings is the basic condition of validity.

If the Luna CA^3 module is used by a qualified certification service provider for its security-critical activities (to sign the issued certificates and timestamp responses) then it has to meet further requirements which limit the usability by demanding other supplementary conditions to be met.

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

I. General validity conditions

The following conditions are necessary for every usage mode (for the whole general utilization scope designed by the manufacturer) in order to provide for reliable and secure operation.

1. Individuals assigned to different roles (Security Officer, User) using Luna CA^3 cryptographic module's services
   - are competent, well-trained and reliable, and
   - follow the mandatory activities defined in different guides (Luna® PKI HSM Installation Guide, Luna® PKI HSM Planning & Integration Guide).

II. Validity conditions due to FIPS 140-1 conformance

The following conditions are crucial so that Luna CA^3 token can comply with FIPS 140-1 Level 3 security.

2. For the secure operation only components and software elements shipped with the token must be used. These are:
   - Chrysalis-ITS® dual-slot Luna® Dock PC Card Reader
   - Luna® Pin Entry Device (PED)
   - PED Keys (Datakey® Device)
   - Enabler (product configuration) software
   - Cryptographic API Software

3. Bits of Token Policy Vector (TPV) must be set as detailed here:
- TPV_USER_ZEROIZE = 1
- TPV_USER_FW_UPDATE = 0
- TPV_M_OF_N_ACTIVATION = 1
- TPV_KEY_ATTRIB_LOCK = 1
- TPV_KEY_SINGLE_FUNCTION = 0
- TPV_SIGNING_KEY_LOCAL = 1
- TPV_DISABLE_CLONING_BY_USER = 1

4. Generating both *Security Officer* and *User* role users 6-length PIN code must be set using PED.

5. Activating „M from N" M and N must be set that $M \geq 2$ and $N \geq M$. This must be taken into account when generating SO and User security level users.

6. In case the Luna CA^3 token is not used any more, it must be destroyed or stored in a way that any of its circuits cannot be accessed and interpretable information cannot be obtained from it.

7. Only authorised persons and processes can access the token both physically and via network, through the protocol specified by the token.

8. The token must be operated in environments where it is not exposed to strong electromagnetic emanation, so preventing that malicious attackers could modify token data.

III. Supplementary conditions for qualified certification service provision

For a qualified certification service provider the following supplementary conditions must be met during Luna CA^3 modul usage:

9. In case of RSA signing algorithm the minimal modulus length (`MinModLen`) must be at least 1020-bit.

10. In case of DSA signature algorithm the minimal p prime length (`pMinLen`) must be 1024-bit, minimal q prime length must be 160-bit.

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

12. Keys used to sign qualified certificates are only usable for signing qualified certificates and possibly to sign their certificate revocation lists.

13. 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 techniques:

- "m from n" technique (which is supported by Luna CA^3 module) 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),
  - saved data is encoded by Triple-DES encryption algorithm,
  - the Key Encryption Key is made from two random components and in compliance with this the simultaneous presence of at least two authorized persons is necessary to recover the private key.

14. Signing keys used for time stamping are only applicable for signing timestamps.

15. If the generation of the subscriber's signing key pair occurs outside the signature creation device (inside Luna CA^3 cryptographic hardware) during the placement of signature creation data within the signature creation device service, then it must be assured that signing keys for electronic signature are different from other keys, e.g. keys for encryption.

16. This certificate is only valid for the current hardware and firmware version (Hardware version: 2, firmware version: 3.102) Upgrade to new firmware version can be done in case of joint fulfilment of the following conditions:

- the new firmware version is authenticated by digital signature of developer/manufacturer company;
- the new firmware version has been evaluated by an (accredited) laboratory authorised to do FIPS 104 evaluations and a new FIPS certificate has been issued on it;
- the usability of the new firmware version for qualified certification service is certified by a designated Hungarian certification authority, and as such the new version will be listed in the secure electronic signature products registry of the Hungarian National Communications Authority.

Annex 2
PRODUCT CONFORMANCE REQUIREMENTS
Requirements document

Act XXXV of 2001 of the Republic of Hungary on electronic signature

Decree 3/2005. (III.18.) IHM on detailed requirements for 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 140-1: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-1

ETSI TS 101 456 v1.3.1 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

Further documents considered during certification

Request for certification

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

CEN 14167-3 Workgroup Agreement: Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP, HSM-PP)

FIPS 140-1 Validation Certificate No. 214 /Luna CA^3/

Luna® Token Security Policies /Luna CA^3 v3/ Document Number CR-1356

HUNG-TJ-21-2004 Certification Report