CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. IKF/19519-2/2012-NFM of the Ministry of National Development based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

certifies that

Luna® PCI-e Cryptographic Module
Hardware version: VBD-05-0100, VBD-05-0101 and VBD-05-0103

Firmware versions: 6.2.1

electronic signature product
developed by
SafeNet Inc.

is suitable for

the secure operation of the following activities of a qualified certification service provider
in case of fulfilment of criteria listed in Annex 1:

Within the scope of electronic signature certification service:
Generating and storing (qualified) certificate signing keys, signing, saving and recovering (qualified) certificates;

Within the scope of time stamping service:
Generating and storing timestamp signing keys, signing timestamps;

Within the scope of placement of signature creation data in a signature creation device service:
Generating subscriber's (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 has been issued on the basis of the evaluation report HUNG-TJ-070-2015.
Produced on commission of NETLOCK Informatics and Network Privacy Services Ltd.
Certificate registration number: **HUNG-T-070-2015**
Validity start date of the certificate: 27 April 2015
Validity end date of the certificate: 27 April 2018
Annexes: conditions, requirements, documents in six pages.
Budapest, 27 April 2015

LS

Szabó Bálint
Quality assurance director

Csik Balázs
Managing director

Annex 1

Validity conditions of the certificate

The Luna® PCI-e cryptographic module is a set of complex cryptographic devices that were designed for general usage and to satisfy a wide range of user needs. Accordingly, many security attributes can be configured on/off in the devices.

Operation in FIPS 140-2 mode (which focuses on security even 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 an element of the Luna® PCI-e cryptographic module will be used by a qualified certification service provider for its security-critical activities (to sign the issued certificates and timestamp responses) then further requirements have to be fulfilled 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 modes (the whole general utilization scope designed by the manufacturer) for reliable and secure operation.

1. Individuals assigned to different roles (Security Officer, Crypto Officer, Crypto User) using Luna® PCI-e cryptographic module services
   - competent, well-trained and reliable, and
   - follow the mandatory activities defined in different guides.

2. The module must be placed only to such a computer that runs suitably secured operating system and application programs and has proper interface for the module.

3. Physical access to the cryptographic module and the communication connections must be kept under control.

II. Validity conditions due to FIPS 140-2 conformance

The following conditions are essential for the Luna® PCI-e cryptographic module to meet FIPS 140-2 Level 3 requirements.

4. To operate in FIPS-approved mode, the following policy settings are required:
   - "Non-FIPS Algorithms Available" must be disabled.
   - "Trusted path authentication" must be enabled and the module must be initialised with PED to enter the SO authentication data.
   - "Trusted Path operation without a challenge" must be disabled if activation or auto-activation is enabled.
   - "Count failed challenge – response validations" must be enabled if activation or auto-activation is enabled.
   - Raw RSA operations must only be used for key transport in FIPS mode

III. Supplementary conditions for qualified certification service provision

For a qualified certification service provider the following supplementary conditions must be met during Luna® PCI-e cryptographic module usage:

5. Minimal modulus length (`MinModLen`) must be at least 2048-bit in case of RSA signing algorithm.

6. Minimal p prime length (`pMinLen`) must be 2048-bit, minimal q prime length must be 224-bit in case of DSA signature algorithm.

7. In case of ECDSA signing algorithm the following parameter requirements must be fulfilled.: in case of SHA256 `qMinLEN=256` SHA256, and `r0Min` is greater than 10^4 and `MinClass` is at least 200, where parameter notation complies with ETSI TS 102 176-1 v2.1.1.

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

9. Only hash algorithms listed as approved in the current version of ETSI TS 102 167-1 must be applied.

10. The key used to sign a qualified certificate should only be used for signing QCs and, optionally, the related Revocation Status Data including the certificate applied to check their validity.

11. 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 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 Triple-DES or AES 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 for recovering the private key.

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

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

14. In the placement of signature creation data in the signature creation device service -if the generation of the subscriber's signing key pair occurs outside the signature creation device (inside the HSM module)- a secure path between the module and the signature creation device must be assured. This path must provide for confidentiality, integrity and source authentication by proper cryptographic mechanisms.

15. This certificate is only valid for the hardware and firmware versions specified on the first sheet. Upgrade of a new firmware version is only applicable if the following requirements are realized:
    - the new firmware version is authenticated by the digital signature of the developer/manufacturer,
    - the new firmware version has been evaluated by an FIPS 140 accredited laboratory and a new FIPS certificate has been released about it,
    - 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 National Media and Infocommunications Authority.

IV. Other aspects that influence validity

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

17. 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 CONFORMANCE REQUIREMENTS
Requirements document

Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

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

FIPS 140-2: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-2

ETSI TS 102 176-1 V2.1.1 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

Further documents considered during certification

Request for certification

FIPS 140-2 Consolidated Validation Certificate No. 0015, Certificate number:1694

LEVEL 3 NON-PROPRIETARY SECURITY POLICY FOR Luna® PCI-e Cryptographic Module /DOCUMENT NUMBER: CR-3397 Revision 8 April 27, 2012/