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

certifies that

ProtectServer Gold

Hardware revision B4 running firmware versions 2.07.00, 2,08.00 and 3.00.03,
Hardware revisions B2 and B3 running firmware version 2.08.00 and
Hardware revision C / PSG-01-0101 running firmware version 2.08.00
electronic signature product
manufactured and sold 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 certification report HUNG-TJ-061-2013.
Produced on commission of NETLOCK Informatics and Network Privacy Services Ltd.
Registration number: **HUNG-T-061-2013.**
Date of the certification: September 02, 2013
Validity of this certificate in case of yearly revision: September 07, 2016
Annexes: conditions, requirements, documents in six pages.

LS

Endrődi Zsolt
Certification director

Lengyel Csaba
Managing director

Annex 1

Validity conditions of the certificate

The ProtectServer Gold (PSG) 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 140-2 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 ProtectServer Gold 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 modes (the whole general utilization scope designed by the manufacturer) for reliable and secure operation.

1. Individuals assigned to different roles (cryptographic user, Administrator) using ProtectServer Gold cryptographic module's services
   - competent, well-trained and reliable, and
   - follow the mandatory activities defined in different guides.

II. Validity conditions due to FIPS 140-2 conformance

2. In order to comply with FIPS operation mode the ProtectServer Gold must be configured securely. This includes the following:
   - Operation with only FIPS-approved algorithms;
   - Not permitting the export of clear keys;
   - Locking the security mode to prevent circumvention of the mode setting,
   - Not permitting PINs to be used in clear,
   - Not permitting changes to the PSG firmware without first clearing all protected Keys and critical security parameters; and
   - Providing authentication and session management security.

An operator may place the ProtectServer Gold in "FIPS mode" by running the `CTCONF -fF` command from the remote management facility. Once this command is executed the PSG will reject all requests for non-FIPS algorithms or configurations.

An operator may view the current PSG mode of operation by running the `CTCONF -v` command. As a result of this command execution the PSG will respond with full details of the adapter configuration. The configuration details include details of the firmware loaded and a listing of the adapter security mode flags one of which indicates that the module is in the FIPS mode of operation.

III. Supplementary conditions for qualified certification service provision

For a qualified certification service provider the following supplementary conditions must be met during ProtectServer Gold usage:

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

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

5. 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 v 2.1.1.

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

7. Use of SHA-1 or weaker hash algorithm for creating electronic signature is forbidden.

8. Signing key used for signing qualified certificates should be applied only to sign qualified certificates, and possibly to sign revocation information linked to these certificates, and to sign certificates needed to issue the revocation information.

9. 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.

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

11. 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 ProtectServer Gold module)- it must be assured that signing keys for electronic signature are different from other keys, e.g. keys for encryption.

12. 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 ProtectServer Gold module)- a secure path between the ProtectServer Gold module and the signature creation device must be assured. This path must provide for confidentiality, integrity and source authentication by proper cryptographic mechanisms.

13. The certificate is valid only for the identified hardware and firmware versions. Upgrade of new firmware version is possible if the following conditions are jointly met.
    - 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

14 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.

15. 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

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

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 Generation Services – Protection Profile (CMCKG-PP, HSM-PP)

FIPS 140-2 Validation Certificate No. 1137 /ProtectServer Gold/

Level3 Security Policy for ProtectServer Gold (PSG) /Revision: 31; Document Number: CR-2505/