# 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-058-2011,**

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

**nShield F3 6000e /Hw: nC4033E-6K0/,**
**nShield F3 1500e /Hw: nC4033E-1K5/,**
**nShield F3 500e /Hw: nC4033E-500/,**
**nShield F3 10e /Hw: nC4033E-030/,**
**nShield F3 6000e for nShield Connect /Hw: nC4033E-6K0N/,**
**nShield F3 1500e for nShield Connect /Hw: nC4033E-1K5N/ and**
**nShield F3 500e for nShield Connect /Hw: nC4033E-500N/**

**firmware version: 2.38.4-3 and 2.38.7-3**

electronic signature product
developed by
**Thales e-Security Ltd.**

are modified with the following restrictions:

1. Use of SHA-1 or weaker hash algorithm is forbidden after 01 January 2012.

Registration number of this Certificate Review Record: **HUNG-FJ-058/1-2011**
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. 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)

## certifies that

**nShield F3 6000e /Hw: nC4033E-6K0/,**
**nShield F3 1500e /Hw: nC4033E-1K5/,**
**nShield F3 500e /Hw: nC4033E-500/,**
**nShield F3 10e /Hw: nC4033E-030/,**
**nShield F3 6000e for nShield Connect /Hw: nC4033E-6K0N/,**
**nShield F3 1500e for nShield Connect /Hw: nC4033E-1K5N/ and**
**nShield F3 500e for nShield Connect /Hw: nC4033E-500N/**

**firmware versions: 2.38.4-3 and 2.38.7-3**

**electronic signature product**
developed by
**Thales e-Security Ltd.**

## is suitable for

**the secure operation of the following activities of**
**a qualified and non 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, signing revocation status data;

**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 and non 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-058-2011.
Produced on commission of Digitoll Information Technology and Servicing Ltd.
Registration number: **HUNG-T-058-2011.**
Date of the certification: July 07, 2011
Validity of this certificate in case of yearly revision: July 07, 2014
Annexes: conditions, requirements, documents in six pages.

LS

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

# Annex 1

## Validity conditions of the certificate

The nShiled F3 PCIe cryptographic module family 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 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 nShiled F3 PCIe cryptographic module family will be used by a qualified or non-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 (nCipher Security Officer, Junior Security Officer, User) using nShield F3 PCIe cryptographic module family 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. A module of the nShield F3 PCIe cryptographic module family must be initialized as described below in order to comply with FIPS 140-2 Level 3:
   a) Put the mode switch into the initialisation position and restart the module
   b) Use either the graphical user interface KeySafe or the command line tool new-world. Using either tool you must specify the number of cards in the Administrator Card Set and the encryption algorithm to use, Triple-DES or AES. To ensure that the module is in Level 3 mode you must
      - Using Keysafe select the option "Strict FIPS 140 Mode" = Yes.
      - Using new-world specify the -F flag in the command line
   c) The tool prompts you to insert cards and to enter a pass phrase for each card.
   d) When you have created all the cards, reset the mode switch into the operational position and restart the module.

If a module is initialised in level 3 mode

- Keysafe displays Strict FIPS 140-2 Mode" = Yes in the information panel for that module.
- The command line tool Enquiry include StrictFIPS in the list of flags for the module

**III. Supplementary conditions for qualified certification service provision**

For a qualified certification service provider the following supplementary conditions must be met during nShield F3 PCIe cryptographic module family 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 2.0.0.

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

7. 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.

8. 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.

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

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

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

12. 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

13. 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.

14. Currently there is no information in public sources that may influence the secure operation of the module. This examination must be performed 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 V2.0.0 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

FIPS 140-2 Validation Certificate No. 1197

The nShield security policy / v2.5.4/