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

nShield F3 500,
nShield F3 500 for netHSM, and
nShield F3 10 PCI

Hardware versions: nC4033P-500, nC4033P-500N and nC4033P-10, Build Standard N

firmware versions: 2.33.60-3

electronic signature product
manufactured and sold by
nCipher Corporation Ltd.

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-044-2008.
Produced on commission of Microsec Informatics and Development Ltd.
Registration number: **HUNG-T-44-2008.**
Date of the certification: December 22, 2008
Validity of this certificate in case of yearly revision: December 22, 2011
Annexes: conditions, requirements, documents in eigth pages.

LS

Endrődi Zsolt   dr. Szabó István
Certification director   Managing director

Annex 1

Validity conditions of the certificate

The nShiled F3 500 Hardware Security Module are 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 the nShiled F3 500 Hardware Security 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 (nCipher Security Officer, Junior Security Officer, User) using nShield F3 500 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

The following conditions are essential for the nShield F3 500, nShield F3 500 for netHSM, and nShield F3 10 PCI Hardware Security Modules to meet FIPS 140-2 requirements.
The nCipher enabled application must perform the following services:

2. To initialise a module
> 1 Put the mode switch into the initialisation position and restart the module
> 2 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
> 3 The tool prompts you to insert cards and to enter a pass phrase for each card.

4 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

3. To return a module to factory state

This clears the Security Officer's key, the module signing key and any loaded module keys.

1. Fit the initialisation link and restart the module
2. Use the **Initialise** command to enter the Initialisation state.
3. Load a random value to use as the hash of the Security Officer's key.
4. Set Security Officer service to set the Security Officer's key and the operational policy of the module.
5. Remove the initialisation link and restart the module.
6. After this operation the module must be initialized correctly before it can be used in a FIPS approved mode.

nCipher supply a graphical user interface KeySafe and a command line tool new-world that automate these steps.

4. To create a new operator

1. Create a logical token.
2. Write one or more shares of this token onto software tokens.
3. For each key the operator will require, export the key as a key blob under this token.
4. Give the operator any pass phrases used and the key blob.

nCipher supply a graphical user interface KeySafe and a command line tool new-world that automate these steps.

5. To authorize the operator to create keys

1. Create a new key, with an ACL that only permits **UseAsSigningKey**.
2. Export this key as a key blob under the operator's token.
3. Create a certificate signed by the nCipher Security Officer's key that:
4. includes the hash of this key as the certifier
5. authorizes the action **GenerateKey** or GenerateKeyPair depending on the type of key required.
6. if the operator needs to store the keys, enables the action **MakeBlob**, limited to their token.
7. Give the operator the key blob and certificate.

nCipher supply a graphical user interface KeySafe and a command line tool new-world that automate these steps.

6. To authorize an operator to act as a Junior Security Officer

1. Generate a logical token to use to protect the Junior Security Officer's key.
2. Write one or more shares of this token onto software tokens
3. Create a new key pair,
4. Give the private half an ACL that permits **Sign** and **UseAsSigningKey**.
5. Give the public half an ACL that permits **ExportAsPlainText**

6. Export the private half of the Junior Security Officer's key as a key blob under this token.
7. Export the public half of the Junior Security Officer's key as plain text.
8. Create a certificate signed by the nCipher Security officer's key includes the hash of this key as the certifier
9. authorizes the actions **GenerateKey**, **GenerateKeyPair**
10. authorizes the actions **GenerateLogicalToken**, **WriteShare** and **MakeBlob**, these may be limited to a particular module key.
11. Give the Junior Security Officer the software token, any pass phrases used, the key blob and certificate.

nCipher supply a graphical user interface KeySafe and a command line tool new-world that automate these steps.

7. To authenticate an operator to use a stored key
1. Use the **LoadLogicalToken** service to create the space for a logical token.
2. Use the **ReadShare** service to read each share from the software token.
3. Use the **LoadBlob** service to load the key from the key blob.
4. The operator can now perform the services specified in the ACL for this key.
5. To assume Security Officer role load the Security Officer's key using this procedure. The Security Officer's key can then be used in certificates authorising further operations.

nCipher supply a graphical user interface KeySafe and a command line tool new-world that automate these steps.

8. To authenticate an operator to create a new key
1. If you have not already loaded your operator token, load it as above.
2. Use the **LoadBlob** service to load the authorization key from the key blob.
3. Use the **KeyId** returned to build a signing key certificate.
4. Present this certificate with the certificate supplied by the security officer with the **GenerateKey**, **GenerateKeyPair** or **MakeBlob** command.

nCipher supply a graphical user interface KeySafe and a command line tool new-world that automate these steps.

III. Supplementary conditions for qualified certification service provision

For a qualified certification service provider the following supplementary conditions must be met during nShield F3 500 Hardware Security Module usage:

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

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

11. 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.

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

13. 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.

14. 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.

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

16. 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 nShiled F3 500 module)- it must be assured that signing keys for electronic signature are different from other keys, e.g. keys for encryption.

17. 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 nShield F3 500 module)- a secure path between the nShield F3 500 module and the signature creation device must be assured. This path must provide for confidentiality, integrity and source authentication by proper cryptographic mechanisms.

18. 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 Hungarian National Communications Authority.

IV. Other aspects that influence validity

19. 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.

20. 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 101 456 v1.4.3 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

Questionnaire for the 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. 966

nShield security policy nShield F3 500, nShield F3 500 for netHSM and nShield F3 10 PCI in FIPS 140-2 level 3 mode /v2.2.3/

nCipher Security Advisory No. 12

nCipher Security Advisory No. 13

nCipher Security Advisory No. 14