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 Communications Decree 9/2005. (VII.21)

certifies that,

nShield F3 SCSI,
nShield F3 Ultrasign 32 SCSI,
nShield F3 Ultrasign SCSI,
payShield SCSI and
payShield Ultra SCSI

Hardware versions: nC4032W-150, nC4132W-400, nC4032W-400, nC4232W-150 and nC4232W-400

firmware version: 2.18.15-3

electronic signature product
manufactured and sold by
nChiper Corporation Ltd.

in case of fulfilment of criteria listed in Annex 1:

is suitable for

the secure operation of the following activities of a qualified certification service provider

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-041-2008.
Produced on commission of Microsec Informatics Development Ltd.
Registration number: **HUNG-T-041-2008.**
Date of the certification: February 25, 2008
Validity of this certificate in case of yearly revision: February 25, 2011
Annexes: conditions, requirements, documents in nine pages.

LS

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Validity conditions of the certificate

The nShiled SCSI 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 SCSI cryptographic module family will be 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 SCSI 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

The following conditions are necessary so that the SCSI cryptographic module family shall meet the security level of FIPS 140-2 Level 3.

The nCipher enabled application must perform the following services:

2 To initialise a module

1. Fit the initialisation link and restart the module
2. Use the Initialise command to enter the Initialisation state.
3. Generate a key pair to use a Security Officer's key.
4. Generate a logical token to use to protect the Security Officer's key.
5. Write one or more shares of this token onto software tokens.
6. Export the private half of the Security Officer's key as a key blob under this token.
7. Export the public half of the Security Officer's key as plain text.

8. Use the Set Security Officer service to set the Security Officer's key and the operational policy of the module. In order to comply with FIPS 140-2 level 3 operation you must set at least the following flags:
    - NSOPerms_ops_ReadFile
    - NSOPerms_ops_WriteFile
    - NSOPerms_ops_EraseShare
    - NSOPerms_ops_EraseFile
    - NSOPerms_ops_FormatToken
    - NSOPerms_ops_GenerateLogToken
    - NSOPerms_ops_SetKM
    - NSOPerms_ops_RemoveKM
    - NSOPerms_ops_StrictFIPS140
9. Keep the tokens and key blobs safe.
   You can create extra module keys in order to distinguish groups of users.
   You may want to create working keys and user authorization at this stage.
10. Remove the initialisation link and restart the module.

nCipher supply a graphical user interface KeySafe and a command line tool new-world that automate these steps.
If you use KeySafe, you must set the StrictFIPS 140 flag.
If you use new-world, you must select the -F flag

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 user

1. Create a logical token.
2. Write one or more shares of this token onto software tokens.
3. For each key the user will require, export the key as a key blob under this token.
4. Give the user 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 user to create keys

1. Create a new key, with an ACL that only permits UseAsSigningKey. This action may need to be authenticated.
2. Export this key as a key blob under the users token.
3. Create a certificate signed by the nCipher Security Officer's key that:
   - includes the hash of this key as the certifier
   - authorizes the action GenerateKey or GenerateKeyPair depending on the type of key required.
   - if the user needs to store the keys, enables the action MakeBlob, limited to their token.
4. Give the user 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 a user 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,
   - Give the private half an ACL that permits Sign and UseAsSigningKey.
   - Give the public half an ACL that permits ExportAsPlainText
4. Export the private half of the Junior Security Officer's key as a key blob under this token.
5. Export the public half of the Junior Security Officer's key as plain text.
   - Create a certificate signed by the nCipher Security officer's key includes the hash of this key as the certifier
   - authorizes the actions GenerateKey, GenerateKeyPair
   - authorizes the actions GenerateLogicalToken, WriteShare and MakeBlob, these may be limited to a particular module key.
6. 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 a user 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 user can now perform the services specified in the ACL for this key.

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 a user to create a new key

1. If you have not already loaded your user 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.

9. Operating a level 2 module in FIPS mode

In order to comply with FIPS mode the user must not generate private or secret keys with the EpxportAsPlain ACL entry; nor should they use the Import service to import such keys in plain text.
A user can verify that a key was generated correctly using the `nfkmverify` utility supplied by nCipher. This utility checks the ACL stored in the key-generation certificate.

III. Supplementary conditions for qualified certification service provision

For a qualified certification service provider the following supplementary conditions must be met during nShield cryptographic module family usage:

10. Minimal modulus length (`MinModLen`) must be at least 1020-bit in case of RSA signing algorithm.
11. Minimal p prime length (`pMinLen`) must be 1024-bit, minimal q prime length (`qMinLen`) must be 160-bit in case of DSA signature algorithm.
12. Only blocks with bit length divisible by 8 can be signed digitally.
13. Keys used to sign qualified certificates are only usable for signing qualified certificates and possibly to sign their certificate revocation lists.
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 are 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 SCSI cryptographic 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 SCSI cryptographic module)- a secure path between the nShield SCSI cryptographic 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 certification organization, and the new version is included in the secure signing products registry of the Hungarian National Communications Authority.
19. The module must not be used by certification service providers for generating Diffie-Hellman keys.

20. A certification service provider must use the module services only via the following high level API calls:
    - PKCS#11
    - Microsoft CAPI
    - Crypto Hardware Interface Layer CHIL (hwcrhk)
    - OpenSSL
    - JCE

IV. Other aspects that influence validity

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

22. 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

Directive 2/2002 (IV.26) MeHVM on security requirements of qualified electronic signature services and its service providers

FIPS 140-2: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-2

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 14167-2:2002 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. 525

The nShield and payShield security policy /v1.4.20/

nCipher Security Advisory No. 12

nCipher Security Advisory No. 13

nCipher Security Advisory No. 14