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

the certified version:
Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3
of the

nShield F3 500 for netHSM
cryptographic hardware device

produced and sold by **nCipher Corporation Ltd.**

as an electronic signature product

with terms stated in Annex 1

passes the requirements

for the application as a „Type 3 secure signature creation device"

for creating qualified electronic signatures
according to the Act XXXV of 2001.

This certificate has been issued on the basis of the certification report No. HUNG-TJ-062-2013.
Produced on commission of Agricultural and Rural Development Agency.
Certificate registration number: **HUNG-T-062-2013.**
Date of certificate: 23.09.2013.
Validity period of the certificate with yearly certificate review process: 23.09.2016.
Annexes: conditions, requirements, documents on seven pages.

PH.

Endrődi Zsolt
Certification director

Lengyel Csaba
Managing director

Annex 1

Validity terms of the certificate

In the paragraphs below those terms are summarised that must be fulfilled **jointly** in order to maintain the validity of this Certificate.

Terms for the preparation phase

1. During initialisation the following steps shall be performed:
   a) Setting factory defaults (Initialise)
   b) Checking of firmware version (New Enquiry, expected version number: 2.33.60)
   c) Generating long term key (Generate KLF).
   d) Export of the public value of the long term key (GetLongTermKey)

2. When creating Security World the following options must be set:

• Cipher suite: AES	encrypting key blobs with AES
• Key recovery: No	no key recovery
• ACS (K and N): (N=K=2)	secret sharing between 2 NSO (administrator)
• pass phrases: YES	pass phrase needed for administrator authentication
• FIPS 140-2 level 3 compliance: YES	FIPS 140-2 level 3 mode
• FTO: NO	only nCipher card is allowed to be used
• Remote Operator: YES	the signer must access the netHSM remotely as well
• OCS replacement: NO	NSO is not allowed to save, clone and delegate private keys
• Pass phrase replacement: NO	NSO is not allowed to recover pass phrases
• Nonvolatile memory (NVRAM) options: NO	key-blobs can be stored outside the cryptographic hardware device
• Security World SEE options: NO	excluding the usage of SEE (nCipher Secure Execution Engine)
• Real-time clock (RTC) options: NO	excluding the usage of RTC (Real-time clock)
• Security World replacement options: NO	NSO is not allowed to clone Security World

3. Creation of the Operator Card Sets (OCSs) must be done in the presence of the card holders (operators, signers) with the following options:

• OCS (K and N): (N=K=1)	no secret sharing for the signer
• pass phrases: YES	pass phrase is needed for authentication
• formal FIPS 140-2 level 3 compliance: YES	FIPS 140-2 level 3 mode
• OCS persistent: YES	card must be inserted while initiating signing
• remotely-readable: YES or NO	card can be read remotely when YES is set
• Time-outs: no condition	no condition for time-outs
• pass phrase replacement: NO	NSO is not allowed to replace the pass phrase of the signer
• delegation for key-pair generation	giving authorisation with NSO certificate

4. If the creation of the OCS is done with the remote card reading option (remotely-readable: YES), then a miniHSM must be used at the signer's endpoint. The miniHSM applied must have the following features:

- it must have a valid FIPS 140-2 level 3 certificate,
- it must be provided with a software/firmware version that is compatible in client mode with the HSM version that is the object of this certificate (nShield F3 500 for netHSM, hardware version: nC4033P-500N, firmware version: 2.33.60-3).

5. Key-pair generation for created operators (signers) must be performed via these steps:

a) Key-pair generation /purpose: signing, activator: exclusively the signer him/herself, algorithm: RSA, key size: minimum 2048, key recovery: NO/,
b) Export of the public key,
c) Transfer to a QCA /either the signer takes his public key personally, either an RO supervises personally the public key export/,
d) QCA verifies the authenticity of the public key /which means that the public key is intact, the signer possesses the proper private key belonging to the public key, and the key pair has been generated by an SSCD/,
e) The QCA generates a qualified certificate /which contains the signer's name, the public key and the advanced electronic signature of the QCA among other data/,
f) Returning the generated qualified public key certificate back to the signing software.

6. Enforcing the ACS secret sharing (see condition 2 above: ACS (K and N): N=K=2) must be done according to the following:

- card and pass phrase of one of the NSOs remains at the system operators,
- card and pass phrase (the latter is written and put in a closed envelope) of the other NSO are taken to a notary immediately after creating and generating the necessary OCSs in the presence of an auditor.

7. Should a new signing endpoint (miniHSM) installation be needed in the future, the enforcing the secret sharing must be done according to the following:

- the second NSO card and the corresponding pass phrase in the envelope are withdrawn from the notary in the presence of the auditor,
- the signing endpoint is created in the presence of the auditor with involvement of the two NSO,
- the card and the written pass phrase in a closed envelope of the second NSO are taken back without delay to the notary in the presence of the auditor.

8. In the nShield F3 500 for netHSM device and in the applied miniHSM, the auditor (see condition 19) shall place a uniquely identified „tamper-detecting" sign, which clearly can prove the opening of the device.

Terms for the signing software

9. The signing software (belonging to the IT environment) that calls the nShield F3 500 for netHSM must handle the unsuccessful authentication attempts indicated by the nShield F3 500 for netHSM and must enforce the following:

- after the first unsuccessful attempt the software must insert a *t* delay (*t* can be configured or can be a fix value and at least 1 second) delay until the next attempt,
- after each subsequent unsuccessful attempt the software must double this delay,
- the default *t* value has to be set after successful authentication.

10. The signing software (belonging to the environment) must enforce that the pass phrase should contain at least 8 characters and should include letters as well as digits.

11. The signing software (belonging to the environment)

- must verify that it communicates with the PKCS#11 or other (Microsoft CSP, Java) driver provided by the vendor,
- must prepare the DTBS-representation of the data to be signed (at least SHA256 or SHA512 hash) in a format suitable for signing by the netHSM,
- must transfer the DTBS-representation to the netHSM,
- must attach the signature provided by the netHSM to the data.

12. The signing software (being part of the environment)

- must request for the OCS pass phrase before starting each document package (containing several documents) to be signed, and must authenticate the OCS (and via this the signer as well), and in the absence of the OCS it must not start (meaning that before each package start-up a new session must be established compulsorily),
- after the generation of the signatures the software must cancel the session immediately with the netHSM.

Terms for the operational phase:

13. The environment of the nShield F3 500 for netHSM must be provided with a physical protection that prevents the physical tampering of the turned-on nShield F3 500 for netHSM under operation.
If the netHSM is taken away from this protected environment (because of a malicious action), all signing certificate corresponding to private keys generated in the system must be revoked, and the netHSM must be re-initialized.

14. The intactness of the „tamper-detecting" sign placed by the auditor on the netHSM or on the miniHSM must be checked regularly. If the sign is damaged, the certificates corresponding to the signing keys handled by the system must be revoked, and the device must be re- initialized.

15. The signer must take care of the device used for authentication (nCipher smart card), it must be used exclusively for the access to the miniHSM or nShield F3 500 for netHSM in the protected environment. The signer must remove it immediately after the approval and the start-up of the signing process, and must keep it under personal control. If the authentication device gets out from the control of the signer, then the certificate corresponding to the private key generated by the signer must be revoked without delay.

16. The signer must take care for his/her pass phrase needed for the authentication, the value of the pass phrase must not be disclosed to anyone, and the OCS must be held in a secure place.

17. The signing private keys are stored in key blobs, encrypted with AES256, outside the nShield F3 500 for netHSM. When such a key blob is destroyed unrecoverably, a new private key must be generated and the certificate corresponding to the destroyed key must be revoked.

18. Private key used for the generation of qualified signatures must be applied exclusively for qualified electronic signatures.

19. The nShield F3 500 for netHSM device must be used for creating qualified electronic signatures only in such a system that is –regarding its conformance to the terms 1-12 of this certificate– evaluated

- by an accredited evaluation laboratory in the proper accredited procedure, and
- based on this evaluation an accredited certification organisation has certified in the proper accredited procedure

according to technology evaluation criteria, which is fixed by law by a competent IT security authority or which is based on international standard.

Annex 2
PRODUCT CONFORMANCE REQUIREMENTS
Documents containing the requirements

Act XXXV of 2001 of the Republic of Hungary on electronic signature

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

CWA 14169, Secure signature-creation devices “EAL 4+”, March 2004

CWA 14355, Guidelines for the implementation of Secure Signature-Creation Devices, March 2004

Protection Profile — Secure Signature-Creation Device - Type 3, March 2004 (Prepared By: ESIGN Workshop - Expert Group F)

Annex 3
Further documents considered during certification

Request for certification

nShield F3 500 for netHSM secure signature creation device /Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3/ EVALUATION REPORT v1.0 /netHSM_SSCD_ETR_v1.0.doc/

FIPS 140-2 Validation Certificate –nShield F3 500, nShield F3 500 for NetHSM and nShield F3 10 PCI by nCipher Corporation Ltd. (When operated in FIPS mode) 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 Version: 2.2.3 3 June 2008

nCipher Security Officer's Guide

Technical Reference Manual

nCipher netHSM Technical Architecture – White Paper

nShield – User Guide for Windows Version: 7.1