CERTIFICATE

REVIEW RECORD

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. (6 Kékgolyó str. Budapest 1123 Hungary) as a certification authority assigned by the assignment document No. IKF/1262-1/2016-NFM of the Ministry of National Development based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

in Certificate Review Process examined
the statements included in the
CERTIFICATE HUNG-T-062-2013
and states the following about the

nShield F3 500 for netHSM

electronic signature product with the following certified components and versions
Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3
manufactured and sold by

nCipher Corporation Ltd.

According to the requirements of legal certainty and available open source information the certification authority extends the validity of the certificate HUNG-T-062-2013 until 23 September, 2019 maintaining the terms regarding the secure usage conditions in Annex 1.

Registration number of this Certificate Review Record: **HUNG-FJ-062/1-2016**
Budapest, 20 June, 2016

LS.

Endrődi Zsolt
Certification director

Szűcs Ákos Balázs
Managing director

Annex 1

Validity terms

1. Validity of existing conditions

The secure usage conditions defined in the first annex of Certificate HUNG-T-062-2013 have to be satisfied.

2. New condition

The multifunctional (electronic signature creation, validation, key generation, key protection) nShield F3 500 for netHSM is allowed to create only 20 RSA2048 key-pairs between 2016.06.20 and 2019.09.23.

The implementation of a (new) certified system is not allowed with nShield F3 500 for netHSM from 2016.06.20.

Rationale

The Certification Report on which the Certificate HUNG-T-062-2013 is based used the FIPS 140-2 certificate (number 996) of the nShield F3 500 for netHSM. This FIPS certificate was moved to the „Historical List[1]" on 2016.01.31 with the term that the random generation does not meet the requirements from 2016. The Security Policy of the document claims that the RNG algorithm conforms to FIPS-186-2. This restricting regulation is in proportion with document SP-800-131A Revision1 (Nov. 2015) (table 3.), which qualifies the said RNG algorithms as outdated and not allowed. There are no vulnerabilities available in open source information.

The introduction of the „Historical List" confides using the device to the organization's risk assessment. According to our own risk assessment the device is suitable for the generation of a few bits of random.

For this reason, the number of the RSA2048 bit keys that can be generated using the device and the applicability of the device in new systems has been restricted.

[1] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-historical.htm