Time Stamp Option Pack

TSOP v7.20.0 Release Notes

10 April 2024

Table of Contents

1. Introduction

These release notes apply to version 7.20.0 of the Time Stamp Option Pack™ (TSOP). They contain information specific to this release such as new features, defect fixes, and known issues.

This release supports the following operating systems:

- Microsoft Windows Server 2012 R2 x64
- Microsoft Windows Server 2016 x64
- Microsoft Windows Server 2019 x64

With the following nShield Hardware Security Modules (HSMs):

- nShield Solo 500+ F3

Running 2.61.4, 12.40.0, 12.50.8 (FIPS certified), 12.60.2 or 12.70.2 firmware.

New installations using an nShield Solo 500+ F3 may need to upgrade their firmware from the version shipped to one listed above.

If you do not wish to reconfigure your Time Stamp Server™ (TSS), or if your Time Stamping Authority (TSA) keys were not protected using an operator cardset, you should not upgrade your firmware.

This release of TSOP has only been tested with the above firmware versions (with v12.40, v12.60 and v12.70 Security World Software).

The Release Notes may from time to time be updated with issues that have come to light after this release has been made available. Please check Entrust nShield Support at https://nshieldsupport.entrust.com for the most up to date version of this document and the TSOP user documentation.

Access to support is available to customers under maintenance. Please contact Entrust nShield Support at nShield.support@entrust.com to request an account.

2. Purpose of this release

Time Stamp Option Pack™ version 7.20.0 addresses a number of known issues and introduces a number of enhancements over the previous 7.10.0 release, including:

- v12.70 software and firmware support.
- Support for all Security World modes.
- Microsoft Windows Server 2019 x64 support.
- Additional branding updates.

3. Changes in this release

The TSOP 7.20.0 release introduces a number of enhancements. These are discussed in the following sections.

3.1. v12.70 software and firmware support

TSOP now supports v12.70-based Security World Software.

If you create a new FIPS 140-2 Level 3 Security World with v12.60 or 12.70 software and firmware, it will not be possible to use a Time Source Master Clock as an upper clock audit source.

3.2. Support for all Security World modes

TSOP now supports all available Security World modes - specifically: FIPS 140-2 level 2, FIPS 140-2 level 3 and Common Criteria CMTS Security World modes.

3.3. Microsoft Windows Server 2019 x64 support

Microsoft Windows Server 2019 x64 is now supported by TSOP.

Support for TSOP on Microsoft Windows Server 2008 R2 x64 has been deprecated.

3.4. Additional branding updates

This release includes a number of additional branding related changes (for example, replacing the included organizational unit (OU) certificate attribute of "nCipher Security TSS ESN" with "nShield TSS ESN" and updating the default test TLS certificate). None of these changes affect product functionality.

3.5. Other changes

Other changes include:

- Fixed an issue where certificates containing large issuer and subject distinguished names could prevent successful audit requests.

- The installer no longer requests a DSNTP_PORT for tsaid_0, nor does the installer add `%NFAST_HOME%\bin` to **PATH**.
- As user documentation is no longer included on the ISO, the *TSOP Administrator Guide* can no longer be requested via the TSOP Web UI. See Introduction for how to obtain the TSOP user documentation.
- Several third-party dependencies have been updated.

4. Important Information

Before deploying the TSOP, the following should be considered:

- This release only supports the operating systems detailed in Introduction.
- Before attempting to create a Security World, it is necessary to install the **SEE Activation (Restricted)** feature certificate, otherwise the keys will not be created correctly for the SEE machine. Similarly, the **Elliptic Curve algorithms** feature certificate should be installed to allow the generation of ECDSA-based TSA keys.
- When using `new-world` to generate a Security World, ensure that the **dseeall** feature is specified. On completion of world generation, it will be necessary to perform SEE delegation - see Security World: SEE delegation.
- Before upgrading an existing TSOP deployment, ensure that the files within `%NFAST_HOME%\dse200\UserFiles` are backed up.
- If you require the ability to back up and restore a TSA key, you must use OCS protection. See Creating Operator Card Sets.
- When performing a firmware upgrade on an existing TSOP deployment, much of the TSOP configuration will be lost and will have to be set-up again through the TSOP web interface. Specifically, please note that:
  - TSA keys will be lost, unless they were generated with the Operator Card-Set backup option (see Restoring a TSA key).
  - TSA configuration will be lost.
- If you do not wish to reconfigure your TSOP deployment, or if your TSA keys are not protected using an operator cardset, you should not upgrade your firmware.
- This release of TSOP has been tested with the firmware versions detailed in Introduction only.
- If continuing to use the firmware shipped with the 5.10.01 and 6.00.00 releases (2.38.7 and 2.61.4 respectively), it will not be possible to generate an ECDSA-based TSA key using the SECP256k1 curve. This curve is only supported from 12.40.0 firmware.

5. Known issues

This release includes the following known issues:

- If the SEE Delegation is not set up correctly, this can result in errors whose cause is not obvious. If you are getting unexplained errors and the board log includes messages about **NVRam failure**, **RTC failure**, or **Key Generation failure**, these are likely to have been caused by a **DSEDelegation** error.
- **Fatal Error: Java Failure, com.ncipher.km.nfkm.SecurityWorld object initialization failure** is displayed if `nonpriv_port` and `priv_port` are not set within the hardserver's config file. These ports can be set by running: `config-serverstartup.exe --port 9000 --privport 9001` or by editing the file (located at `%NFAST_KMDATA%\config\config`) and setting `nonpriv_port=9000` and `priv_port=9001` (substituting the port numbers as appropriate). It is then necessary to restart the hardserver (which, in turn, will restart the DSE200 service).
- If the TSS is very busy responding to time-stamp requests during a DSNTP audit, the DSNTP audit will likely fail with a large communication delay.
- If using 12.70.4 firmware, when in a FIPS 140-2 Level 3 Security World, both DSE200 service start up time and individual audit requests will take longer due to additional key generation checks being performed on clock audit.
- When a DSNTP port is entered for a TSA, the TSS does not verify if that port is already in use by another process.
- If using a version of Java impacted by JDK-8191040, it will be necessary to either move to a different version or to apply the documented workaround, see https://bugs.java.com/bugdatabase/view_bug?bug_id=8191040 for more information.