Time Stamp Option Pack

TSOP v8.1.0 Release Notes

18 October 2024

Table of Contents

1. Introduction

These release notes apply to version v8.1.0 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 2019 x64
- Microsoft Windows Server 2022 x64

With the following nShield Hardware Security Modules (HSMs):

- nShield Solo 500+ F3 for TSOP
  - Supporting v12.72.0 (FIPS certified) or v13.3.1 firmware with v13.6.3 Security World Software.
- nShield Solo XC Base F3 for TSOP
  - Supporting v12.72.1 (FIPS certified), v12.72.3 (FIPS certified) or v13.5.3 firmware with v13.6.3 Security World Software.

New installations 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 or attempt to replace your existing HSM.

This release of TSOP has only been tested with the above firmware and Security World Software versions.

If using an early access release of v12.72.0 or v12.72.1 firmware, please consult the *Security World 12.72 Early Access Release Notes*.

The release notes may be updated with issues that have become known after this release has been made available. For the latest version, see https://nshieldsupport.entrust.com/hc/en-us/sections/360001115837-Release-Notes.

Access to the Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

1.1. Purpose of this release

Time Stamp Option Pack™ version v8.1.0 addresses a number of known issues and introduces a number of enhancements over the previous release, including:

- Updated platform support.
- Updated Security World Software and firmware support.
- StrictSP80056Ar3 Security World support.
- Improved certificate support.
- TSOP ATV file and `ncversions`.

1.2. Versions of these release notes

Revision	Date	Description
1.1	2024-10-18	Documentation tooling update: fixed the website navigation of TSOP SDK v8.1.0 docs. No content changes.
1.0	2024-09-26	TSOP v8.1.0 GA release notes.

2. Changes in this release

The TSOP v8.1.0 release introduces a number of enhancements. These are discussed in the following sections.

2.1. Updated platform support

The following operating system is now supported:

- Microsoft Windows Server 2022 x64

Support for the following operating systems has been deprecated:

- Microsoft Windows Server 2012 x64
- Microsoft Windows Server 2016 x64

See Introduction for the complete list of supported platforms.

2.2. Updated Security World Software and firmware support

v13.6.3 Security World Software is now supported by TSOP, with the following HSM and firmware versions:

- nShield Solo 500+ F3 for TSOP: v12.72.0 (FIPS certified) or v13.3.1 firmware.
- nShield Solo XC Base F3 for TSOP: v12.72.1 (FIPS certified), v12.72.3 (FIPS certified) or v13.5.3 firmware.

See Introduction for the complete list of supported Security World Software and firmware versions.

2.3. StrictSP80056Ar3 Security World support

Security Worlds generated with `StrictSP80056Ar3` set are now supported by TSOP.

2.4. Improved certificate support

Several improvements have been made to how certificates are supported and handled by TSOP, including:

- Adding support for certificates expiring after 2038.
- Improving the interpretation and handling of a certificate's validity period.
- Increasing the duration of newly generated `localaudit` certificates to avoid their early expiration.

2.5. TSOP ATV file and ncversions

An ATV file is now generated for TSOP and will be displayed in the version information returned by `ncversions`.

2.6. Other changes

Other changes include:

- The TSOP installer no longer prompts the user to confirm the **Destination Folder** as this is automatically determined by the installed location of the Security World Software.
- Several third-party dependencies have been updated.

3. 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 *Creating and managing Security Worlds* in the *TSOP v8.1.0 Install and User Guide*.
- 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 *Configuring the TSS* in the *TSOP v8.1.0 Install and User Guide*.
- When performing a firmware upgrade on an existing TSOP deployment, or attempting to replace the HSM, 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 *Administering and using the TSS* in the *TSOP v8.1.0 Install and User Guide*).
  - 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 or replace your HSM.
- This release of TSOP has been tested with the firmware versions detailed in Introduction only.
- If a TSA reports **TAC_Invalid**, and the clock status for that TSA shows as being **Disabled**, it might be necessary to re-set the module clock. This can be confirmed by consulting the board log and looking for entries such as **exceeded 4 seconds per day**. See the *Enabling or disabling the clock* section of the *TSOP Install and User Guide* for further information.
- Support for the Time Source Master Clock (TSMC), and upper clocks, will be removed in a future release.
- If the **Board Log** shows **DSNTP signature was invalid**, it might be necessary to remove the `localaudit` file. This can be confirmed by checking the expiry of the appropriate

localaudit certificate within `%NFAST_KMDATA%\local`. If the certificate has expired, it will be necessary to remove `%NFAST_KMDATA%\local\localaudit` and restart the DSE200 service. This will generate a new `localaudit` file and corresponding certificate.

4. 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 v12.70.2 or v12.80.2 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.do?bug_id=8191040 for more information.