THALES

www.thales-esecurity.com

Thales e-Security

# Release Notes for the Time Stamp Server™ Software 6.00.00

Applicable to:

- DSE200 Time Stamp Server
- OP3162T Time Stamp Option Pack

Date: 19 August 2016

Doc. no.: 1.0

# Contents

# Chapter 1: Introduction

These release notes contain important information about the Time Stamp Server™ Support Software (TSS) 6.00.00 release.

This release supports the following operating systems:

- Microsoft Windows Server 2008 R2 64-bit
- Microsoft Windows Server 2012 R2 64-bit

With the following Thales nShield Hardware Security Modules (HSMs):

- nShield 500 Solo
- nShield 500 Solo+

Both running 2.61.4 firmware.

**Note:** if you do not wish to reconfigure your TSS, or if your TSA keys were not generated with the **Operator Card-Set** backup option, you should not upgrade your firmware, but be aware that this release of TSS has been tested with 2.61.4 firmware only.

## Purpose of this release

The TSS 6.00.00 release introduces a number of enhancements to the 5.10.01 release. These are detailed within Chapter 2; however, the primary changes include adding support for:

- The Microsoft Windows Server 2012 R2 64-bit operating system
- The nShield 500 Solo+ HSM
- ESSCertIDv2 (RFC5816)

# Chapter 2: Changes in this release

The TSS 6.00.00 release introduces the following enhancements:

- Support for Microsoft's Windows Server 2012 R2 64-bit operating system.
- Support for nShield 500 Solo+ hardware security modules.
- Support for ESSCertIDv2 (RFC5816).
- Security worlds based on an SP800-131 compliant cipher suite are now supported.
  **Note:** this allows a cipher suite to be used that offers 128-bit security.
- The ability to select the DES3 cipher suite has been removed from the TSS web UI when initialising a security world, however, security worlds utilising this cipher suite can still be used with the TSS. This is achieved by using the `new-world` command line utility.
  **Note:** when using `new-world`, ensure that the security world feature `dseeall` is specified. On completion of world generation, it will be necessary to perform SEE delegation - see the *TSS Administrator Guide* for details.
- DSA key support has been expanded to include 2048-bit keys and SHA-256 support.
- The ability to generate 512-bit RSA or DSA keys via the TSS web UI has been removed, however, support for such keys has been retained.
- 2048-bit RSA is now used in TSS SSL communication.
- Apache Tomcat 5 has been updated to Apache Tomcat 7.
  **Note:** if upgrading from TSS 5.10.01 any Apache Tomcat 5 specific configuration will not be inherited by the Apache Tomcat 7 installation.
- Fixed an issue (NSE-4461) where if a Security Officer installs a certificate provided by an attacker, the attacker could potentially execute arbitrary JavaScript in the Security Officer's browser.
- The **Time Stamps Issued** page no longer updates automatically (only when the **Refresh** button is pressed).
- The four default upper clocks which were listed have been removed.

# Chapter 3: Important information

Before deploying the TSS, the following should be considered:

- The TSS 6.00.00 release only supports the Windows Server 2008 R2 and Windows Server 2012 R2 64-bit operating systems and is not designed to be used for upgrades of TSS versions prior to 5.10.01.
- If you require the ability to backup and restore a TSA key you must use OCS protection - see the *TSS Administrator Guide* for details.
- This release contains new firmware. If performing a firmware upgrade on an existing TSS deployment, much of the TSS configuration will be lost, and will have to be set-up again through the TSS web UI. Specifically, please note that:
    - User accounts and the SSL certificate will be retained.
    - TSA keys will be lost, unless they were generated with the **Operator Card-Set** backup option (see the *TSS Administrator Guide* for more information about restoring the TSA key).
    - TSA configuration will also be lost.

  If you do not wish to reconfigure your TSS, or if your TSA keys were not generated with the **Operator Card-Set** backup option, you should not upgrade your firmware, but beware that this release of TSS has been tested with 2.61.4 firmware only.
- If continuing to use the firmware shipped with the 5.10.01 release (2.38.7), it will not be possible to generate an AES (SP800-131 compliant) security world. Attempting to do so will result in "Operation failed: writeNextCard, error (st=UnknownCommand) : NFKM_initworld_begin."
- If 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 the *TSS Administrator Guide* for details.
- The TSS installer no longer includes a Java runtime. You must install a Windows 32-bit Standard Edition Java Runtime Environment (JRE) version 1.8 before installing the TSS software.
- Once installation of the TSS software option pack is complete you must then install the feature certificate for **restricted SEE** before attempting to create a security world, otherwise the keys will not be created correctly for the SEE machine.
- The option is now available to include **ESSCertIDv2** with a SHA-256 hash in the TST, using the **Include ESSCertIDv2 (RFC5816)** checkbox in the TSS web UI, in addition to **ESSCertID** (which uses SHA-1). Please note that:
    - This is not enabled by default as older applications will not understand it.
    - By default the SDK will check the SHA-1 hash in **ESSCertID**, which will verify regardless of whether **ESSCertIDv2** is enabled.

    - By setting the environment variable **TTI_VERIFY_ESSCERTIDV2** to **1** in the environment of the application using the SDK, the SDK will verify **ESSCertIDv2** only (and verification will fail if it is not present or if it uses a hash weaker than SHA-256).

- SOAP Web Service configuration has been changed to set the parameters **sendXsiTypes** and **sendMultiRefs** to false to provide responses compatible with Microsoft .NET. To restore the old configuration, change **%NFAST_HOME%\dse200\Tomcat7\webapps\TSS\WEB-INF\serverconfig.wsdd** to set the **sendXsiTypes** and **sendMultiRefs** parameters to true, i.e.:

```
<parameter name="sendXsiTypes" value="true"/>
<parameter name="sendMultiRefs" value="true"/>
```

# Chapter 4: Bug fixes

The following table lists the host-side bugs fixed in TSS 6.00.00:

| Bug reference | Description |
|---|---|
| 21581 | The TSA response includes a NULL terminator from a C character string |
| 29948 | A malformed timestamp request can terminate the DSE200 service |
| 30784 | TSS admin web interface displays wrong date for server start time and current local time |
| 30805 | [SDK] TimeStampServer class cannot process timestamp responses larger than 4k |
| NSE-4461 | TSS cannot handle certificates with an apostrophe in the subject |
| NSE-5532 | TSS installer can hang when installing registry entries |

# Chapter 5: Known issues

This release includes the following known issues:

- If upgrading from TSS 5.10.01, and you wish to retain previous configuration information, `tss.xml` and `tssUsers.xml` (from within `C:\Program Files (x86)\nCipher\nfast\dse200\UserFiles`) should be manually backed up prior to uninstalling the previous release and then reinstated before installing this release.
- When installing the TSS you may see a message indicating that the DSE200 service was unable to be started: "Unable to detect if the `DSE200' service has started (-1) - start it manually if necessary." It should be confirmed that the DSE200 service is running. **Note:** this can be achieved with `sc query DSE200` or via Microsoft's Windows **Services**.
- The error message **NVMem_LoadDESKey: GenerateDES3Key failed VerifyFailed** is displayed one time after creating a new security world. After the **SEE Delegation** step (an automatic step in the TSS security world creation wizard) is complete, this error should not be reported again.
- When an invalid / unsupported certificate is added to the **SSL Key Store**, the error message in the admin log ends with **SubjectDN:** without a SubjectDN. This is because the certificate could not be parsed.
- 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**, **RTCSet failure**, or **Key Generation failure**, these are likely to have been caused by a **DSEDelegation** error.
- 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.
- When the user enters a DSNTP port for a TSA, the TSS does not verify if that port is already in use by another process.
- The **SSL Certificate > Fulfill** option does not check the key-purpose extensions on the certificate and, if you fulfill this with a certificate that is not usable as an SSL certificate, you cannot then establish an HTTPS connection to the TSS (effectively locking you out of the management interface). If this problem occurs, contact Support at Thales.
- In a strict FIPS security world, certificates with an MD5 signature algorithm cannot be added either to the **TSA Cert Store** or the **Upper Clock Cert Store**. An error is logged in the board log when importing this type of unsupported certificate.

# Internet addresses

| | |
|---|---|
| Web site: | http://www.thales-esecurity.com/ |
| Support: | http://www.thales-esecurity.com/support-landing-page |
| Online documentation: | http://www.thales-esecurity.com/knowledge-base |
| International sales offices: | http://www.thales-esecurity.com/contact |

Addresses and contact information for the main Thales e-Security sales offices are provided at the bottom of the following page.

THALES

www.thales-ecurity.com

## About Thales e-Security

Thales e-Security is a leading global provider of trusted cryptographic solutions with a 40-year track record of protecting the world's most sensitive applications and information. Thales solutions enhance privacy, trusted identities, and secure payments with certified, high performance encryption and digital signature technology for customers in a wide range of markets including financial services, high technology, manufacturing, and government. Thales e-Security has a worldwide support capability, with regional headquarters in the United States, the United Kingdom, and Hong Kong. www.thales-esecurity.com

**Follow us on:**

**Americas –** Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
**Asia Pacific –** Unit 4101 41/F 248, Queen's Road East, Wanchai, Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
**Europe, Middle East, Africa –** Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com