Web Services Option Pack

WSOP v3.2.0 Release Notes

10 April 2024

Table of Contents

1. Introduction

These release notes apply to version 3.2.0 of the nShield Web Services Option pack for Security World. They contain information specific to this release such as new features, defect fixes, and known issues.

2. Features of nShield Web Service Option Pack 3.2.0

2.1. New configuration option

- New Security world configuration:

  WSOP now accesses the Security world files, like the module and world files, from the database instead of the kmdata directory. There is a new `HKNSO` configuration option for the hash value which must be set before starting WSOP.

  See *Configure the Web Services Option Pack* in the *User Guide* for more information.

2.2. New Algorithm support

Support for following encryption and decryption algorithms has been added:

- `RSA-OAEP-384`
- `RSA-OAEP-512`

2.3. RSA-OAEP Label support added

As defined in RFC 8017, support has been added for a label L input for encryption and decryption operations with RSA-OAEP.

Please refer to the REST API section of the User Documentation for more information.

2.4. New PKCS #11 migration support

PKCS #11 object migration support for the following key types has been added to the DBMT:

- `CKK_SHA256_HMAC`
- `CKK_SHA384_HMAC`
- `CKK_SHA512_HMAC`

- CKK_RSA

2.5. New PKCS #11 functionality

- Support for message digesting and random number generation functions:
  - C_DigestInit
  - C_Digest
  - C_DigestUpdate
  - C_DigestFinal
  - C_GenerateRandom
- New mechanisms for message digest:
  - CKM_SHA_1
  - CKM_SHA224
  - CKM_SHA256
  - CKM_SHA384
  - CKM_SHA512
  - CKM_SHA3_224
  - CKM_SHA3_256
  - CKM_SHA3_384
  - CKM_SHA3_512
- Generation of RSA keys with C_GenerateKeyPair:
  - CKK_RSA key types generated using CKM_RSA_PKCS_KEY_PAIR_GEN
- New RSA mechanisms for encrypt and decrypt:
  - CKM_RSA_PKCS
  - CKM_RSA_PKCS_OAEP which is supported when used with a CK_RSA_PKCS_MGF_TYPE value that is one of the following:
    - CKG_MGF1_SHA1
    - CKG_MGF1_SHA256
    - CKG_MGF1_SHA384
    - CKG_MGF1_SHA512
- New RSA mechanisms for sign and verify:
  - CKM_SHA256_RSA_PKCS
  - CKM_SHA384_RSA_PKCS

    - CKM_SHA512_RSA_PKCS
    - CKM_SHA256_RSA_PKCS_PSS
    - CKM_SHA384_RSA_PKCS_PSS
    - CKM_SHA512_RSA_PKCS_PSS
- New AES mechanism for encrypt and decrypt:
    - CKM_AES_GCM (not supported with Security Worlds conforming to FIPS 140 Level 3)

3. PKCS #11 v3.0 compliance.

This release is compliant with PKCS #11 Version 3.0 (https://docs.oasis-open.org/pkcs11/pkcs11-base/v3.0/os/pkcs11-base-v3.0-os.html). Support for the following has been added:

- `CKO_PROFILE` objects.
- `CKP_BASELINE_PROVIDER` conforming to the *Baseline Provider Clause* defined in section 3.3 of *PKCS #11 Cryptographic Token Interface Profiles Version 3.0* (https://docs.oasis-open.org/pkcs11/pkcs11-profiles/v3.0/pkcs11-profiles-v3.0.html).
- Cancellation of active operations by calling `C_EncryptInit`, `C_DecryptInit`, `C_SignInit`, `C_VerifyInit`, or `C_DigestInit` with `pMechanism` set to `NULL_PTR`.
- `CKA_UNIQUE_ID`. This attribute can also be used for objects created in earlier versions of the WSOP PKCS #11 library.
- `C_GetInterface` and `C_GetInterfaceList`. Interface versions 2.40 and 3.0 are supported.

4. Compatibility

4.1. Supported MongoDB versions

This release has been tested against MongoDB version 5.0.18.

4.2. Supported hardware

This release is targeted at deployments with any of the following nShield HSMs:

- nShield Solo PCI Express (500+, and 6000+)
- nShield Solo XC (Base, Mid, High)
- nShield nShield 5S (Base, Mid, High)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield nShield 5C (Base, Mid, High, Serial Console)

4.3. Supported operating systems

This release has been tested for compatibility with the following operating systems:

- Red Hat Enterprise Linux Server 7 x64
- Red Hat Enterprise Linux Server 8 x64
- Red Hat Enterprise Linux Server 9 x64
- SUSE Enterprise Linux 12 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 7.6 x64
- Oracle Enterprise Linux 8 x64

Additionally the PKCS #11 library has been tested for compatibility with the following operating systems:

- Windows Server 2019 x64
- Windows Server 2022 x64
- Windows 10 x64
- Windows 11 x64

4.4. Supported Security World versions

This release can be used with the following nShield Security World Software installations:

- Security World v12.80
- Security World v13.3+ and v13.4+

Security World v12.8x is required in order to migrate kmdata files using the Database Management Tool.

Firmware versions supported by the 12.60 release are also supported by WSOP. See the nShield 12.80 Security World Software release notes for further details.

4.5. API version

The nShield Web Service Option Pack REST API version has been increased to v1.4.0.

5. Defect Fixes

Reference	Description in v3.1	Fix in v3.2
NSE-52845	When operating close to the active Protection Domain capacity limit, attempts to activate further domains can sometimes be blocked and available capacity in the cache lost.	Cache behaviour for Protection Domain activations has been improved.
NSE-54972	N/A	Fixed an issue in the Web Services PKCS#11 library where setting CKA_WRAP or CKA_UNWRAP in a key generation template could override values of CKA_SIGN and CKA_VERIFY.
NSE-54829	N/A	It is now possible to create a CKO_CERTIFICATE object with CKA_TRUSTED = CK_FALSE using the Web Services PKCS#11 library.
NSE-53998	N/A	Fixed an issue where corecrypto error messages could be truncated when recorded in the Web Services PKCS#11 library log file.
NSE-52902	N/A	Improved accuracy of log messages for ulCount in C_GenerateKey and C_CreateObject in the Web Services PKCS#11 library log file.
NSE-54419	N/A	The correct version information is now reported back by the DBMT.
NSE-54535	N/A	The branding of the release notes documentation has been corrected.
NSE-54495	N/A	Fixed the issue where the DBMT required a combined certificate and key file for the TLS connection instead of individual files as specified in the configuration file.
NSE-55660	N/A	The command line interface of the DBMT has been improved for usability regarding migrating an individual key via the appname and keyident values.

Reference	Description in v3.1	Fix in v3.2
NSE-56545	N/A	Fixed an issue in the PKCS#11 library where conflicting entries for the same attribute in the template supplied to C_FindObjects could result in invalid search results.
NSE-56423	N/A	Fixed an issue in the PKCS#11 library where C_FindObjects can fail to return matching objects when the template includes a value for CKA_OBJECT_ID that contains NUL bytes.
NSE-56737	N/A	Fixed an issue in the PKCS#11 library where parallel calls to C_Logout on the same session could result in function failure.
NSE-56124	N/A	Fixed an issue which prevented the WSOP server from using an HSM protected private key for TLS.
NSE-56353	N/A	Improvements have been made to key record data for future compatibility.
NSE-54687	N/A	Fixed a DBMT issue which could cause an error when attempting to upgrade a very large quantity of keys.
NSE-57049	N/A	Fixed an issue in the Web Services PKCS#11 library that would cause C_GetSlotList to return 0 slots if the library had to retry the web request.

6. Known Issues

Reference	Description
NSE-48648	The Web Services PKCS#11 library has a dependency on a third party called `cpprestsdk` which has an internal threadpool limit of 40. There is a potential issue in the PKCS#11 library which means that if an application is running more than 40 threads and encounters a large number of persistent errors from the WSOP `corecrypto` service then the threads can become blocked and an application restart would be necessary. This issue can be mitigated by using fewer threads, and by making use of the config file options `MAXRETRIES` and `RETRYDELAY`. Increasing the value of `RETRYDELAY` introduces a delay between retries of failed WSOP requests.
NSE-53106	String fields such as CKA_LABEL and CKA_APPLICATION should not contain any HTML character for example `<`, `>` or `&` as this can result in those values becoming corrupted when they are retrieved later.
NSE-54022	The WSOP server can temporarily become unresponsive if a large number of time intensive requests are sent concurrently. This will cease when the requests are completed.
NSE-56651	An incorrect HTTP response status code of 422 is returned (instead of 400) when a key generation request is rejected because the key ident parameter contains non-alphanumeric characters.
NSE-56623	Key records from previous releases may be incompatible with future releases of WSOP and be limited in future functionality. It is recommended that a new database is used for this release to ensure maximum future compatibility.
NSE-56871	The `offset` filter option is not supported by the `protectiondomains` endpoint. If needed, `offset` can be used with the `groups` endpoint in order to identify and retrieve the desired protection domain.
NSE-56921	WSOP will not self recover if the connection to the MongoDB server is interrupted enough for the periodic health check to fail. If this happens, the WSOP service will need to be restarted before the system can resume operation.
NSE-57190	When a CRL is processed, invalid certificates can be ignored silently. However, a successfully revoked certificate is reported correctly in the logs.