Web Services Option Pack

nShield Web Services CNG Provider v3.3.1 User Guide

21 October 2024

© Entrust Corporation. All rights reserved.

Table of Contents

1. nShield Web Services Key Storage Provider . . . 1
2. Installing the provider . . . 2
3. Configuring the provider . . . 3
    3.1. Default provider configuration . . . 3
    3.2. Mandatory configuration parameters . . . 3
        3.2.1. Web Services server hostname . . . 3
        3.2.2. Web Services server port number . . . 3
        3.2.3. Client certificate . . . 3
        3.2.4. Client library . . . 4
        3.2.5. Protection domain UUID . . . 4
        3.2.6. Protection domain passphrase . . . 4
    3.3. Optional configuration parameters . . . 4
        3.3.1. Logging communication with the Web Services server . . . 4
        3.3.2. Key group UUID . . . 4
        3.3.3. Number of times to retry an operation . . . 5
        3.3.4. Base delay for request retry . . . 5
        3.3.5. Maximum delay between retries . . . 5
    3.4. Additional logging . . . 5
    3.5. Multiple provider configurations . . . 6
4. Server/client mutual authentication . . . 7
    4.1. Overview . . . 7
    4.2. Installing certificates . . . 7
5. Utilities . . . 9

1. nShield Web Services Key Storage Provider

The nShield Web Services Key Storage Provider, a web services-based Cryptography API: Next Generation (CNG) provider, can be used to generate and use keys for creating and ver ifying signatures.

The client machine where the provider is installed does not require any existing Web Services or Security World Software to be present.

The following set of algorithms are supported for signing operations:

- RSA
- ECDSA_P256
- ECDSA_P384
- ECDSA_P521

The nShield Web Services Key Storage Provider can be used to integrate with the following applications:

- Microsoft Authenticode
- Microsoft Internet Information Services (IIS)
- Microsoft Active Directory Certificate Services (AD CS)

2. Installing the provider

To install the nShield Web Services Key Storage Provider:

1. Ensure that `Microsoft Visual C++ 2015-2022 Redistributable (x64)` has been installed. A supported version is included in the installation media or can be downloaded from https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170.
2. Sign in as Administrator or as a user with local administrator rights.
3. Using the provided installation media, launch `setup.msi` manually (silent installations are also supported using `msiexec`).
4. Follow the onscreen instructions.
5. Accept the license terms and select **Next** to continue.
6. Specify the installation directory and select **Next** to continue.
7. Choose which features are required and select **Install** to continue.
8. Select **Finish** to complete the installation.
9. If you are installing nShield Web Services Key Storage Provider for the first time, go to the `C:\ProgramData\nCipher\WebServices\CNG\conf` folder and copy the `example_cngwebservices.cfg` file to `cngwebservices.cfg`.

   If you are reinstalling or updating - and do not want to overwrite your existing `cngwebservices.cfg` file - you can skip this step.

10. By default, the provider will log information and error level output to Event Viewer (source: `nShield Web Services Key Storage Provider`).

    Additional logging can be obtained by setting the following environment variables: `WSCNG_LOGFILE` and `WSCNG_LOG_STDERR`. See Configuring the provider for additional information.

3. Configuring the provider

The `cngwebservices.cfg` file contains an example provider configuration. Before being able to use the provider, it is necessary to ensure that all mandatory entries in `cngwebservices.cfg` are correctly specified.

3.1. Default provider configuration

The provider is installed with a default configuration. Entrust recommends reviewing and updating the initial configuration before the provider is used to ensure that all configuration settings are appropriate for the deployment environment.

Ensure that the configuration file and certificates have restrictive access control, so that only the application using the provider has access to these.

3.2. Mandatory configuration parameters

The following configuration parameters must be set before using the provider.

3.2.1. Web Services server hostname

```
hostname=ADDR
```

Set `ADDR` to the Web Services server hostname.

3.2.2. Web Services server port number

```
port=18001
```

Specify the Web Services server port number (`port` is set to `18001` by default).

3.2.3. Client certificate

```
client_cert_thumbprint=THUMBPRINT
```

Set `THUMBPRINT` to the client certificate thumbprint. This should be specified in the following format: `<system_store>\<certificate_store>\<certificate_thumbprint>`. For example:

```
client_cert_thumbprint=LocalMachine\My\6d1ee99b3795338613354751daa351635f8f3fe0
```

See Server/client mutual authentication for further information on client certificates.

3.2.4. Client library

```
clientlibrary=C:\Program Files\nCipher\WebServices\CNG\clientlibrary\COpenApiClient.dll
```

Specify the full path of the Web Services client library (`clientlibrary` is set to `C:\Program Files\nCipher\WebServices\CNG\clientlibrary\COpenApiClient.dll` by default).

3.2.5. Protection domain UUID

```
protection_domain_uuid=DOMAIN_UUID
```

Set `DOMAIN_UUID` to the UUID of the protection domain.

3.2.6. Protection domain passphrase

```
protection_domain_passphrase=PASS
```

Set `PASS` to the passphrase of the protection domain.

3.3. Optional configuration parameters

The following configuration parameters are optional.

3.3.1. Logging communication with the Web Services server

```
log_ws_client=0
```

Set `log_ws_client` to `1` to enable logging of communication with the Web Services server to a logfile (`log_ws_client` is set to `0` by default). See Additional logging for information on how to configure logging to a file.

3.3.2. Key group UUID

```
key_group_uuid=GROUP_UUID
```

Set `GROUP_UUID` to the UUID of the desired key group (if unset, the protection domain's default key group is used).

3.3.3. Number of times to retry an operation

```
request_retry_max=10
```

Specify the maximum number of times an operation should be retried should the Web Services server report errors (if unset, `request_retry_max` is set to `10` by default).

3.3.4. Base delay for request retry

```
request_retry_delay_base=1000
```

Specify the base delay for request retry in milliseconds (if unset, `request_retry_delay_base` is set to `1000` by default).

3.3.5. Maximum delay between retries

```
request_retry_delay_cap=32000
```

Specify the maximum delay between retrying operations in milliseconds (if unset, `request_retry_delay_cap` is set to `32000` by default).

3.4. Additional logging

The following environment variables can be used to configure, and acquire, additional logging from the provider:

`WSCNG_LOGFILE` — If set, and specifying a full path and filename, the provider will log - including additional debug level output - to the specified file. Ensure that appropriate permissions have been applied to the file specified by `WSCNG_LOGFILE`. Information and error level output will continue to be sent to Event Viewer.

`WSCNG_LOG_STDERR`	If set to 1, log output - including debug level output - will be sent to stderr. Information and error level output will continue to be sent to Event Viewer.

3.5. Multiple provider configurations

It is possible, on a single client machine, to have multiple provider configuration files in use. This is achieved by setting the following environment variable:

`WSCNG_CONFIGFILE`	If set, and specifying a full path and filename, the provider configuration specified will be used.

4. Server/client mutual authentication

4.1. Overview

The nShield Web Services Key Storage Provider can only communicate securely with a Web Services server if the following certificates are installed:

- The Web Services server's CA certificate.
- An appropriate client certificate (with each client using its own client certificate).
- Any intermediate CA certificates that are to be used to form a complete chain to verify the client certificate on the Web Services server.

See the *nShield Web Services Option Pack User Guide* for further information concerning server/client authentication, as well as for important security guidance.

4.2. Installing certificates

The following guidance should be followed when installing certificates:

1. Install the Web Services server's CA certificate into the `Root` store.
   Below is an example of how you can do this using `certutil.exe`.
   a. Add a CA certificate to the `Root` store

   ```
   certutil.exe -addstore Root <ca_certificate.pem>
   ```

   b. Check that the certificate has been installed:

   ```
   certutil.exe -store Root
   ```

2. Install any intermediate CA certificates for the client certificate.
   Below is an example of how you can do this by using `certutil.exe` to load the client certificate's intermediate certificates into the `CA` certificate store:

   ```
   certutil.exe -addstore CA <intermediate_ca_certificate.pem>
   ```

3. Install the client certificate and its private key. This should be a PFX file that contains a single certificate and the associated private key.

   The PFX must not contain the full certificate chain.

For example, to install the PFX file in the Local Machine's certificate store

```
certutil.exe -p <password> -importPFX [certificatestorename] <client-cert.pfx>
```

or to install the PFX file into the Current User's certificate store

```
certutil.exe -p <password> -importPFX -user [certificatestorename] <client-cert.pfx>
```

To find the thumbprint of a certificate, use `certutil.exe` to view the certificate's properties, then select the `Details` tab and scroll down to the `Thumbprint` field. For example, to view thumbprints in `My` store.

```
certutil.exe -viewstore My
```

PowerShell can also be used to see the thumbprint on a list. In this example store is `My` and store type is `LocalMachine`.

```
Get-ChildItem -Path Cert:LocalMachine\My
```

If necessary, update `client_cert_thumbprint` within `cngwebservices.cfg` with the changed thumbprint (see Configuring the provider for further information).

5. Utilities

The following utilities are provided:

`wscnglist`	Lists information about the installed CNG providers.
`wscngregister`	Used to register or unregister the nShield Web Services Key Storage Provider (`wscngregister` is automatically called when nShield Web Services CNG is installed or uninstalled).
`wscngsoak`	A performance test tool for the installed CNG providers.

For more information about these utilities, see their associated help, for example:

```
C:\Program Files\nCipher\WebServices\CNG\bin\wscnglist.exe --help
```