Web Services Option Pack

nShield Web Services Key Migration Guide

21 October 2024

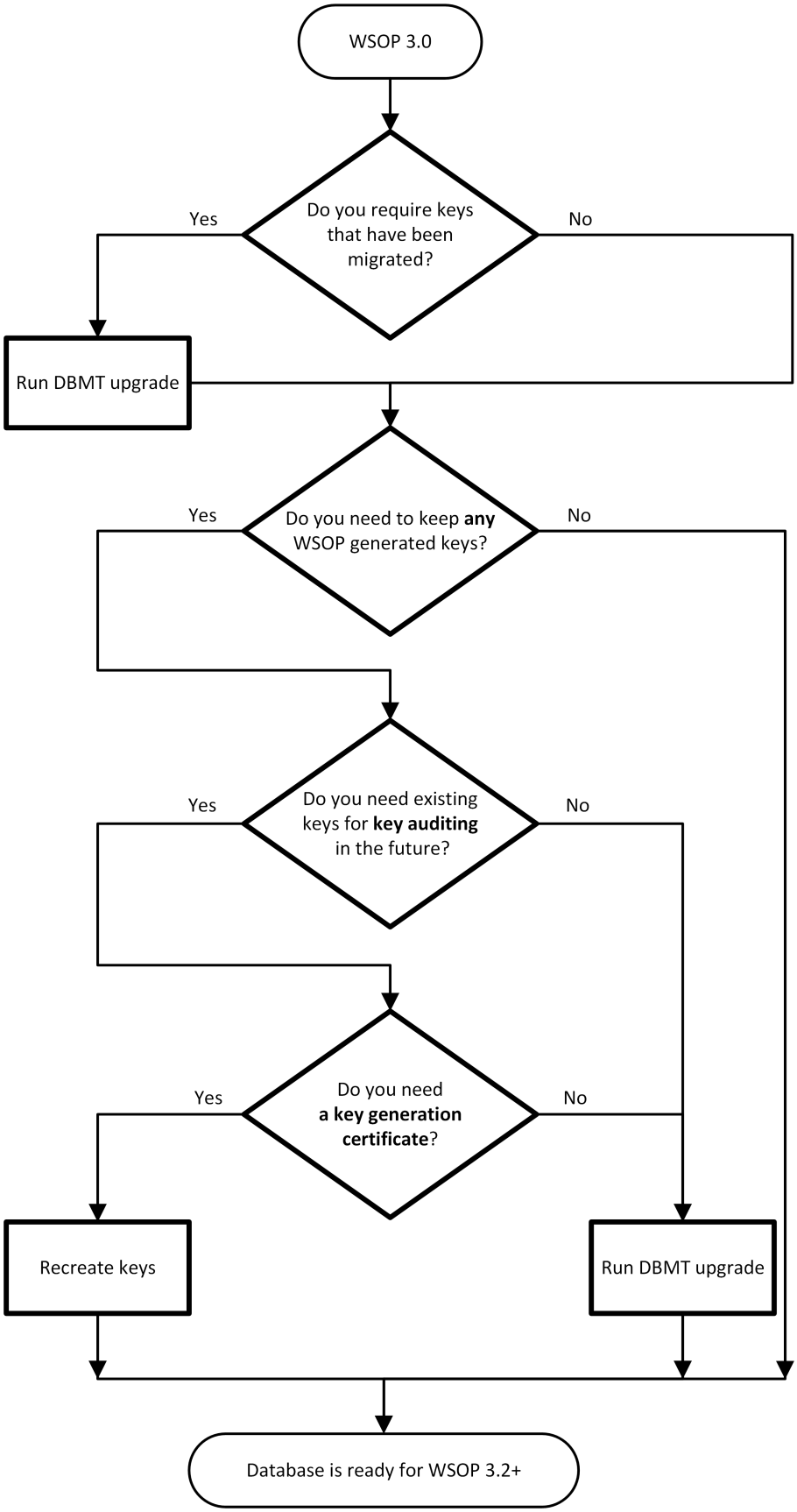
Table of Contents

1. Introduction

This guide is for those upgrading WSOP from v3.0 or v3.1 and would like to continue using their existing keys in WSOP v3.2 and later. The existing keys need to be upgraded to be used in later WSOP versions. There are different upgrade paths to take, depending on the WSOP version you upgrade from, to ensure the keys are compatible with WSOP v3.2 and later.

2. When upgrading WSOP from v3.0

The process described in this section applies to keys that have been migrated using DBMT and also to keys that have been generated with WSOP v3.0. The upgrade paths differ depending on the origin and requirements of the existing keys:



Keys generated with WSOP v3.0 do not have a key generation certificate. If a key generation certificate is required for the WSOP

> generated key, recreate the key using WSOP v3.2 or later with the key generation certificate included. See Recreate keys.

2.1. Run DBMT upgrade

You can run the DBMT upgrade tool to enable the full functionality of the existing keys for use in WSOP v3.2 and later. The commands in this section use DBMT v2.1.0. Later versions of the tool can be used, too.

1. Install DBMT:

```
tar -xf dbmt-2.1.0.tar.gz
cd opt/nfast/webservices/dbmt-2.1.0
./install.sh
```

2. Run DBMT upgrade:

```
dbmt upgrade --config /path/to/config.yaml
```

When all the database records have been upgraded, you can install a new version of WSOP. See section *Upgrading the Web Services Option Pack* in the *WSOP User Guide*.

3. When ugrading WSOP from v3.1

4. Recreate keys

If the flowchart indicated that you have to recreate your keys, you have to recreate these keys with WSOP v3.2 or later. When the replacement keys have been generated, revoke the legacy key. You must use the replacement keys when you re-encrypt and re-sign all data that were previously encrypted or signed with the revoked keys.

Procedure

If you haven't already initialized a new database as part of When upgrading WSOP from v3.0 or Migrate keys when upgrading WSOP from v3.1:

1. Install DBMT:

   The commands in this section use DBMT v2.1.0. Later versions of the tool can be used, too.

   ```
   tar -xf dbmt-2.1.0.tar.gz
   cd opt/nfast/webservices/dbmt-2.1.0
   ./install.sh
   ```

2. Change the database name in the DBMT configuration to the new database.

   For more information on how to install and configure DBMT, see section *WSOP Database Management Tool* in the *WSOP User Guide*.

3. Initialize the new database:

   ```
   dbmt db-init --config  /path/to/new/config.yaml
   ```

4. With the old WSOP version still running, install the WSOP v3.2 or higher on another local system, for example on a Linux server. See section *Upgrading the Web Services Option Pack* in the *WSOP User Guide*.
5. Configure the new WSOP version to use the new database.

4.1. Generate a new key for encryption/decryption

1. Ensure the client terminals for the new and old WSOP instances instances are in a secure environment. This ensure that the confidentiality of the exposed plaintext is protected.
2. With the old WSOP version and the old key, decrypt the relevant ciphertext:

   ```
   curl --cacert server_ca.pem \
   ```

```
    --cert client_crt.pem \
    --key client_key.pem \
    --header 'Content-Type: application/json' \
    --header 'Accept: application/json' \
    --request POST \
    -d '{"alg":"RSA-OAEP", "kid":"/km/v1/groups/2dc4849d-583c-5a9e-9901-dfe3415bc91f/keys/0ff67c26-379c-
52c3-9880-cb8a138a5b66","ciphertext":"<base64url-encoded ciphertext omitted>"}' \
    'https://wsop.server:18001/crypto/v1/decrypt'
Result:
{
  "plaintext": "aGVsbG8gd29ybGQ"
}
```

3. Generate a replacement key with the new WSOP version:

```
curl --cacert server_ca.pem \
    --cert client_crt.pem \
    --key client_key.pem \
    --header 'Content-Type: application/json' \
    --header 'Accept: application/json' \
    --request POST \
    -d '{"keytype": "RSA", "length": 2048, "appname": "simple", "ident": "newrsakey"}' \
    'https://wsop.server:18001/km/v1/groups/2dc4849d-583c-5a9e-9901-dfe3415bc91f/keys'
Result:
{"kid":"/km/v1/groups/2dc4849d-583c-5a9e-9901-dfe3415bc91f/keys/49b26396-88bf-53c9-9ca8-535e0fe9ef2e"}
```

4. Re-encrypt the plaintext with the replacement key:

```
curl --cacert server_ca.pem \
    --cert client_crt.pem \
    --key client_key.pem \
    --header 'Content-Type: application/json' \
    --header 'Accept: application/json' \
    --request POST \
    -d '{"alg":"RSA-OAEP", "kid":"/km/v1/groups/2dc4849d-583c-5a9e-9901-dfe3415bc91f/keys/49b26396-88bf-
53c9-9ca8-535e0fe9ef2e","payload":"aGVsbG8gd29ybGQ"}' \
    'https://wsop.server:18001/crypto/v1/encrypt'
```

4.2. Generate a new key for signing/verifying

1. With the new WSOP version, generate a replacement key:

```
curl --cacert server_ca.pem \
    --cert client_crt.pem \
    --key client_key.pem \
    --header 'Content-Type: application/json' \
    --header 'Accept: application/json' \
    --request POST \
    -d '{"keytype": "RSA", "length": 2048, "appname": "simple", "ident": "newrsakey"}' \
    'https://wsop.server:18001/km/v1/groups/2dc4849d-583c-5a9e-9901-dfe3415bc91f/keys'
Result:
{"kid":"/km/v1/groups/2dc4849d-583c-5a9e-9901-dfe3415bc91f/keys/49b26396-88bf-53c9-9ca8-535e0fe9ef2e"}
```

2. Re-sign the payload with the replacement key:

```
curl --cacert server_ca.pem \
    --cert client_crt.pem \
    --key client_key.pem \
    --header 'Content-Type: application/json' \
    --header 'Accept: application/json' \
    --request POST \
    -d '{"alg":"RS256", "kid":"/km/v1/groups/2dc4849d-583c-5a9e-9901-dfe3415bc91f/keys/49b26396-88bf-53c9-
9ca8-535e0fe9ef2e","payload": "aGVsbG8gd29ybGQ"}' \
    'https://wsop.server:18001/crypto/v1/sign'
```

4.3. Revoke the legacy keys

When you have generated replacement keys for all legacy keys, revoke the legacy keys.

The replacement keys are ready for use in the new WSOP version.