DigiCert® PKI Platform

Key Export Tool User's Guide

digicert®

Legal Notice

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
https://www.digicert.com/

Table of Contents

1 PKI Platform 7.x Key Export Tool Usage

The PKI Platform 7.x Key Export tool lets you export your PKI certificates from PKI Platform 7.x solution (typically via your locally hosted Key Management Server) and import them into PKI Platform 8.x Cloud or Local Key Escrow solution. This tool lets you export your user's escrowed certificates, in bulk, to a zip archive file.

This document assumes you have a valid Administrator certificate to access the Platform 7.x Control Center admin web console.

Important: DigiCert recommends running this export tool in a secured environment as the exported certificates contains private keys which has highly confidential and sensitive data. It is your responsibility to securely delete all the exported files after the certificates have been imported into your PKI Platform 8.x account.

NOTE: DigiCert recommends running this export tool during maintenance window and when there are no new enrollments to avoid losing the new data during migration. You can also run your Key Management Server in EXCLUSIVE mode to avoid new enrollments during migration.

1.1 Pre-requisites

- Install and configure PKI Web Services 1.0.3. It should also use the same key recovery data source that was used for Platform 7.x. For more information, refer to DigiCert™ Managed PKI Web Services Key Management Server Installation and Configuration Guide available for download from the Managed PKI Control Center, or contact your DigiCert representative.

- The Registration Authority (RA) certificate that is stored on a software-based Java keystore is used and not Hardware Security Module (HSM).

- The Key Management Server must be configured on http:// rather than https:// Communications between enterprise clients and the Key Management Server are secured using basic authentication.

1.2 Qualified Platform

Table 1-1 Supported platform

PKI Platform 7.x	Key recovery data source	Account Type	Key Management Server
Windows Server 2008 R2 SP2	Oracle 11g Dual control for key recovery	Private Managed PKI account RA certificate and key generation in software	Windows Server 2008 R2 SP2

1.3 Using the PKI Key Export Tool

Task 1. Obtain the key export tool package

Obtain the configuration files from the link provided by your DigiCert representative. Extract the `mpkiexport-utility.tar` file into a temporary folder. This writes the files `mpki-export-utility.jar` and `config.properties`

Task 2. Configure the Key Export Tool

Open config.properties in a standard text editor. Configure the values from Table 1-2.

Table 1-2 Configuration file

Variable	Description
`localhost.ws.endpoint`	Endpoint for the KMS PKI Web Services. For example: `localhost.ws.endpoint = http://localhost:8081`
`kms.authenticate.username`	Username used for securing the communication between your enterprise client and KMS. For example: `kms.authenticate.username = pkiadmin`

`kms.authenticate.password`	Password used for securing the communication between your enterprise client and KMS. For example: `kms.authenticate.password = pki@dmin123`
`dual.key.recovery.enabled`	Value to indicate if multiple admin control for key recovery is enabled (true or false).
`admin.certificate.location.2`	Same as admin.certificate.location.1 This value is required only if dual.key.recovery.enabled is set to True.
`ca.issuer.dn`	Navigate to MPKI Control Center: https://onsite-admin.pki.digicert.com/OnSiteHome.htm 1. Click Configuration -> Download Policy File 2. Open the downloaded policy file in any text editor 3. Search for certIssuerDN 4. Copy and paste the value for the certIssuerDN parameter For example: `ca.issuer.dn = CN = QA V3, OU = For test purposes only, O = PrivateEye, C = US`
`max.zip.file.size`	The maximum size of the zip file is 20 MB
`filter.search.common.name`	Filter for the search certificate API. Use this filter to export certificates that match the provided substring. If this value is empty, then all escrowed certificates will be exported.

Task 3. Using the tool

Copy the mpki-export-utility.jar and config.properties to the temporary folder and run the following command. Use Java 1.7 and make sure that Java path is defined.

```
java -jar mpki-export-utility.jar -config config.properties
```

The status of the export process is displayed in the console in real time.

1.3.1 Output Files

The output folder `mpki-export-utility-tmp/final` contains a zip file with all the exported certificates. Each zip file contains the following:

- `*.pfx` end-user certificates
- `*.p7b` issuer certificates of CA certificate chain
- `certinfo.xml` containing the details of the certificates in the zip including *.p7b, *.pfx, and associated password

The zip file size cannot exceed 20MB and can hold up to 6094 end-user certificates of 2048-bit key size. If the file size exceeds 20 MB, a new zip file is created.

You can import these certificates into PKI Platform 8.x or your Local Key Management Service. Do not change the folder structure or update the zip file during the import operation. Importing a 20MB file approximately takes 20 minutes.

Important: DigiCert strongly recommends you securely delete the zip file after the certificates in the zip file is successfully uploaded, since it has confidential and sensitive data.

1.3.2 Log Files

The log file has a summary of the certificates exported. A **`mpki-export-utility.log`** file is created in the temporary directory where the export tool was run.

This is a sample output of a log file:

```
**********************************************************************
TIME ELAPSED - 45:59:00
TOTAL CERTIFICATE COUNT - 60245
TOTAL SUCCESS IN THIS RUN - 60225
TOTAL FAILURES IN THIS RUN - 20
**********************************************************************
```

NOTE: If there are any failed exported records, you have to re-run the tool. The log file will show a message failure against every exported serial number.

1.4 Filtering Search Results

To filter certificates, do the following:

- For exporting all the escrowed certificates in PKI Platform 7.x account, do not use any value for the filter.

  ```
  filter.search.common.name =
  ```

- For exporting certificates based on a specific common name, use the below filter. All the certificates that match this value will be exported.

  ```
  filter.search.common.name = TEST
  ```

All the certificates in PKI Platform 7.x account that has TEST in its common name will be exported.

1.5 Troubleshooting the Export Tool

- You may experience the following issues while running the export tool:
  - If there are network issues, the tool will not export all the certificates. You must re-run the tool when the network issue is resolved.
  - If data is corrupted in the datastore, the export fails for that particular record. You have to manually re-run the record.
- When you run the tool, a temporary database file is created to keep track of failed records. When you rerun the tool, it processes the failed records. For example, if there are failures in the initial run, when the tool is re-run, it processes all the records and ignores the already imported certificates and imports the ones that failed in the previous run.

  If you want to re-create the zip files again, delete the folder from the mpki-export-util-tmp location and run the tool again. All certificates will be exported based on your filter criteria.
- The key recovery may fail for PKI Platform 7.x single key pairs setup, where key recovery data source is LDAP. You must modify the kmsconfig.properties file and replace `kms.keyrecovery.ldap.iv=uid` to `kms.keyrecovery.ldap.iv=l`