DCI Mastering

KeyStore

Supplement

Supplement for the “CLIPSTER/Fuze DCI Mastering” supplement user guide: “DCI Mastering – KeyStore”
Document Version 1.0

Specifications and data may change without notice. We offer no guarantee that this documentation is correct and/or complete. In no event shall Rohde & Schwarz DVS GmbH be liable for any damages whatsoever (including without limitation any special, indirect or consequential damages, and damages resulting from loss of use, data or profits, or business interruption) arising out of the use of or inability to use the hardware, software and/or manual materials.

Those parts of this documentation that describe optional software or hardware features usually contain a corresponding note. Anyway, a lack of this note does not mean any commitment from Rohde & Schwarz DVS GmbH.

DCI Mastering – KeyStore

This document describes the KeyStore feature available for a DCI Mastering with, for example, a CLIPSTER or Fuze system. It makes the handling of encrypted DCPs easier at the creator’s site.

First some general information about the KeyStore feature are provided, followed by some important notes that you have to observe. Afterwards it will be explained how to create a KeyStore network certificate and how to install the certificate on a DCI Mastering system.

Contents of this document:

- Introduction to the KeyStore Feature
- Important Notes
- Creating a KeyStore Network Certificate
- Installing the KeyStore Network Certificate
  - Installing the Private Key on a DCI Mastering System
  - Installing the Public Key on a DCI Mastering System

Introduction to the KeyStore Feature

If you want to view or modify an encrypted DCP, a KDM for the system where to view/modify the DCP on must be created and delivered along with the DCP. DVS offered some ease of this issue via self KDMs. The KeyStore feature now makes the viewing or modification of DCP content at the creator’s site even easier.

General Functionality of the KeyStore Feature

For all DVS DCI Mastering systems the general functionality of the KeyStore feature will be available. Instead of just creating a self KDM to enable you to view or modify DCP content, it will store all necessary information of the self KDM in a database. If the self KDM was intended for the same DCI Mastering system that also created the DCP, you will be able to add single MXF files of an encrypted DCP to the bin and timeline without having to specify the self KDM in an additional step.

The self KDM as a file, however, will still be created the usual way. This ensures that, if the self KDM was intended for another DCI Mastering system (i.e. not the one that created the DCP), it can be used on such a system same as in the past, even without the network-based KeyStore feature (see below).

Network-based KeyStore Feature

An even greater benefit of the KeyStore database is that it can be accessed by other DVS DCI Mastering systems via the Spycer network (SpycerNet). When a special certificate (KeyStore network certificate) is installed, encrypted DCPs or single MXF files can be decrypted on every DCI Mastering system where the certificate is installed as long as the system is in the same domain (optional) and Spycer group (mandatory).

On the DCI Mastering system that creates the DCP, instead of encrypting the AES keys of the MXF files with the hardware related certificate for the self KDM, they are encrypted with the public key of the KeyStore network certificate. The encrypted AES keys are then stored in the database and can afterwards be accessed by requesting systems via the SpycerNet. During transfer over the network the keys will remain encrypted. After receiving, the requesting system will be able to decrypt the information if it has the private key of the KeyStore network certificate installed. Then the decrypted AES keys of the DCP or MXF file will be handed over to the hardware that performs the final AES decryption of the content.

On all systems that should be part of the network-based KeyStore feature the KeyStore network certificate has to be installed.

Usage

The general functionality of the KeyStore feature is enabled and available on all DVS DCI Mastering systems.

The network-based KeyStore feature on the other hand requires the installation of the KeyStore network certificate. Once it is installed, the networking of the KeyStore database can be controlled with the check box **Use KeyStore Certificate** of the group ***DCI*** of the Configuration Tool (see figure 1-6 on page 9). When activated, the database will be available for accesses via the SpycerNet; when deactivated, a networking is prohibited.

Important Notes

Please observe the following important notes:

- To use the network-based KeyStore feature (see section “Network-based KeyStore Feature” on page 2) Windows 7 or higher must be installed on every participating DCI Mastering system. On other versions of the Windows operating system the network-based KeyStore feature will be disabled automatically. The general functionality of the KeyStore feature (see section “General Functionality of the KeyStore Feature” on page 1) is available on all versions of Windows.

- The KeyStore network certificate will allow a DVS DCI Mastering system in a network to decrypt encrypted DCP content if the certificate is installed on this system.
- The KeyStore network certificate is managed by the Windows operating system in a certificate store and not kept in hardware. This does not comply with a DCI-trusted environment.
- The Rohde & Schwarz DVS GmbH cannot be held responsible for security issues resulting from the use of the KeyStore feature or the KeyStore network certificate such as possible data leaks or loss of data.
- The system’s administrator should be aware of how the Windows certificate store works and must keep the certificate password at a safe place protected from unauthorized access.

Creating a KeyStore Network Certificate

The KeyStore feature allows DVS DCI Mastering systems to exchange encrypted DCPs over a network without the need to create system-specific KDMs. This feature requires the installation of a unique and special KeyStore network certificate (RSA public and private key pair) on all systems that should use the network-based KeyStore feature.

This section describes how to generate the KeyStore network certificate using the OpenSSL framework:

It is strongly recommended to hand over the certificate creation to a trusted system administrator familiar with certificates.

- If not already the case, install OpenSSL (www.openssl.org, for the Windows binaries see www.openssl.org/related/binaries.html).
- Download and install e.g. ’Win32 OpenSSL v1.0.1c Light’ or higher. By default the installation path is *C:\OpenSSL-Win32*.
- Open the Windows command prompt and create an empty writeable directory within the *bin* directory of OpenSSL.
- Switch/change into this directory.

Before starting you will have to set an environment for the OpenSSL configuration file.

- In the command line type in
  `set OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg`
  and press [Enter].

Next, you can create an RSA certificate with a public and private key pair:

⚠ Please observe the `–days` parameter. It sets the expiration date of the certificate. After expiration the encrypted information stored in the KeyStore database cannot be decrypted anymore. With the following command the certificate will expire in approx. 100 years.

- Type in
  ```
  ..\openssl.exe req -x509 -nodes -days 36500
  -newkey "rsa:2048" -keyout keystore.pem -out
  keystore.pem
  ```
  and press [Enter].

Afterwards you will be asked for some information.

- Answer the requested information as shown in the following example. In case you want to answer with empty/nothing, enter a dot (`.`).

  ℹ The field 'OU' (organizational unit) provides an additional security feature allowing you to specify a domain name by entering `#KSD=MyDomain`. When specified, the DVS software will use the network-based KeyStore feature only if the system is part of the given domain (in this case 'MyDomain'). If you cannot ensure that all systems using the network-based KeyStore feature are in this domain, leave out the domain name and enter `#KSD=` only.

Country name (2-letter code)	`US`
State or province name (full name)	`MyState`
Locality name (e.g. city)	`MyCity`
Organization name (e.g. company)	`MyCompany`
Organizational unit name (see above)	`#KSD=MyDomain`
Common name	`KeyStore`
E-mail address	`.`

Next, you have to convert the certificate to a PFX file:

⚠ In this step you will be asked to enter a password. Setting a password is mandatory to use the KeyStore feature. This is an important security issue: Select a secure password and make sure that only trusted people be aware of it. You will be asked for this password every time you install the certificate.

- Type in
  ```
  ..\openssl pkcs12 -export -out keystore.pfx -in
  keystore.pem -name "KeyStore"
  ```
  and press [Enter].

Afterwards you have to extract the public key to a CER file by performing the following two steps:

- Type in
  ```
  ..\openssl pkcs12 -in keystore.pfx -out
  keystore.crt -nokeys -clcerts
  ```
  and press [Enter]. During this you have to enter the password specified in the previous step.
- Then enter
  ```
  ..\openssl x509 -inform pem -in keystore.crt
  -outform der -out keystore.cer
  ```
  and press [Enter].

With this you have created the PFX and CER files, i.e. the RSA private and public keys. You now have to finish the certificate creation by performing the following:

- Delete all temporary files created during this process except the *keystore.pfx* and *keystore.cer* files and memorize the password or keep it at a safe place but never together with these files.

After this the creation of the KeyStore network certificate (RSA public and private key pair) is finished. In essence you can find in the CER file the public key, while the password encrypted PFX file contains the private key.

For the step to install the certificate on one or more DVS DCI Mastering systems the two files should be stored in a safe way on a removable media. They are required for each system that should use the KeyStore feature.

Installing the KeyStore Network Certificate

Once the KeyStore network certificate is available, you can install it on DVS DCI Mastering systems. It must be installed on every DCI Mastering system that should use the KeyStore feature, regardless whether they create DCP content or decrypt it. Furthermore, the systems must be in the same domain (optional, depending on the setting of the field 'OU', see section "Creating a KeyStore Network Certificate" on page 3) and they must be in the same SpycerNet group (mandatory). Both keys, the private and the public key, have to be installed.

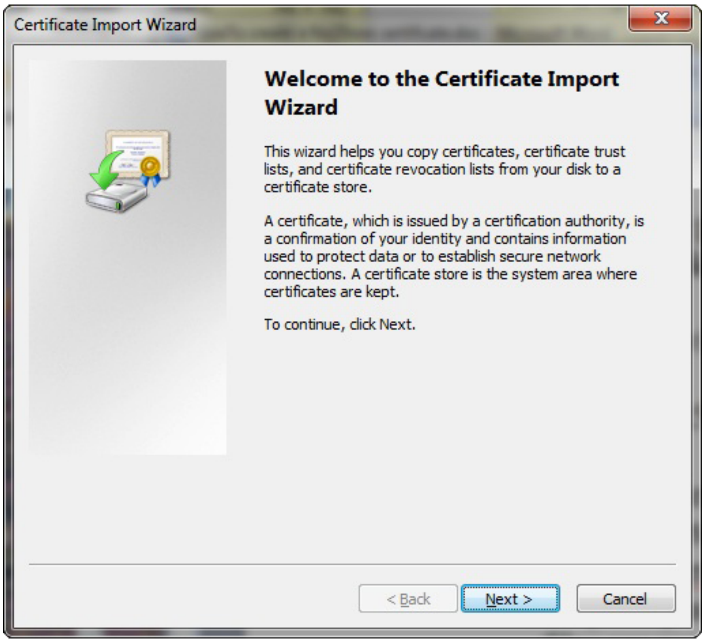
Installing the Private Key on a DCI Mastering System

This section explains how to install the private key on a DCI Mastering system. For this perform the following:

- At the DCI Mastering system that should be able to use the KeyStore feature insert the removable media with the *keystore.pfx* file.

- Open the file explorer, browse to the location of the file and execute the `keystore.pfx` file (e.g. with a double-click of the mouse).

This will automatically start the certificate import wizard. By stepping through the wizard as explained below you will install the KeyStore network certificate in the Windows certificate store:



Certificate Import Wizard

Welcome to the Certificate Import Wizard

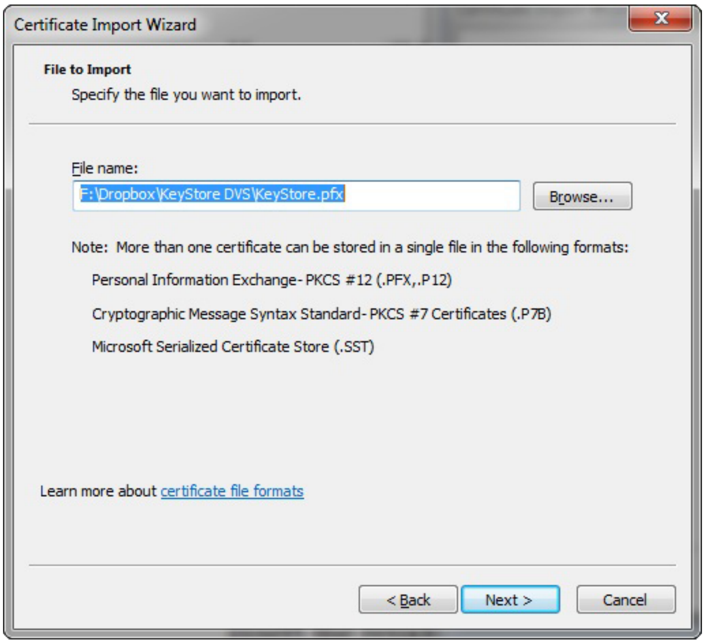
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 1-1: Welcome to the wizard

- Click on the button **Next**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

F:\Dropbox\KeyStore DVS\KeyStore.pfx

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

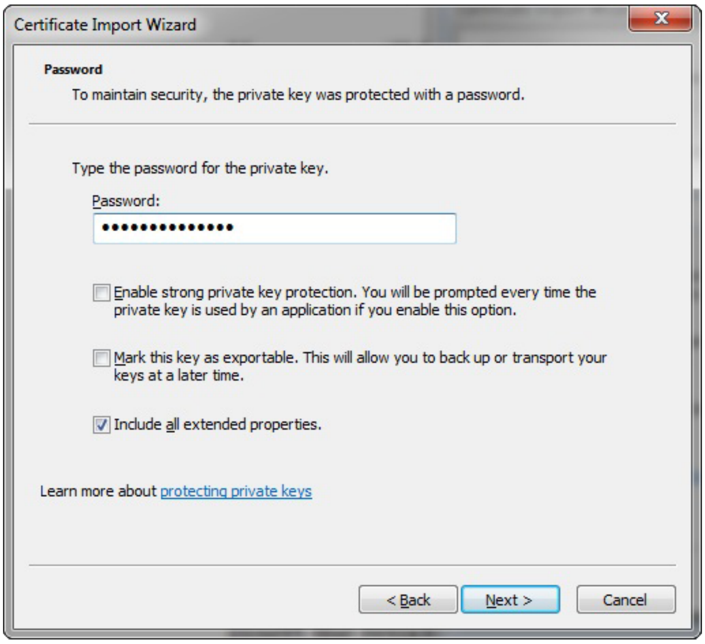
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Figure 1-2: File to import

- Click on the button **Next**.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••••••••

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

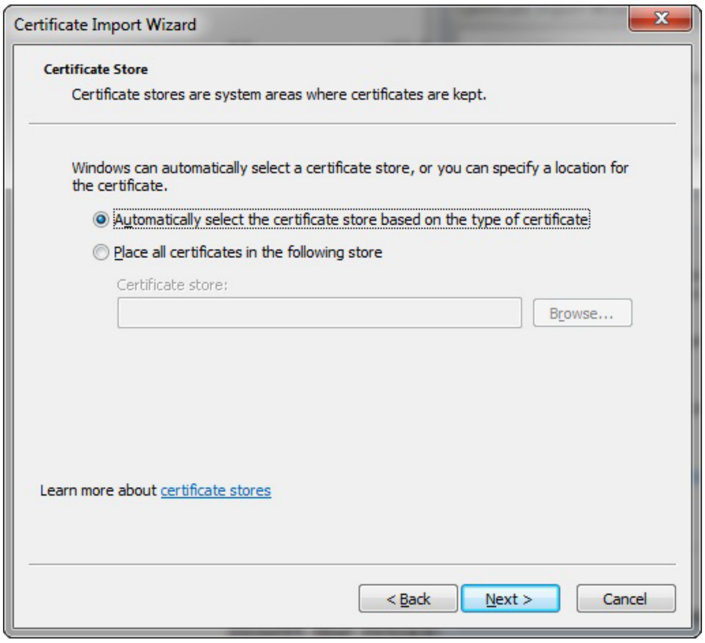
□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

Figure 1-3: Enter the password

- Enter the password for the certificate.
- Deactivate the check boxes **Enable strong private key protection…** and **Mark this key as exportable…** (last check box **Include all extended properties.** should be activated).
- Click on the button **NEXT**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

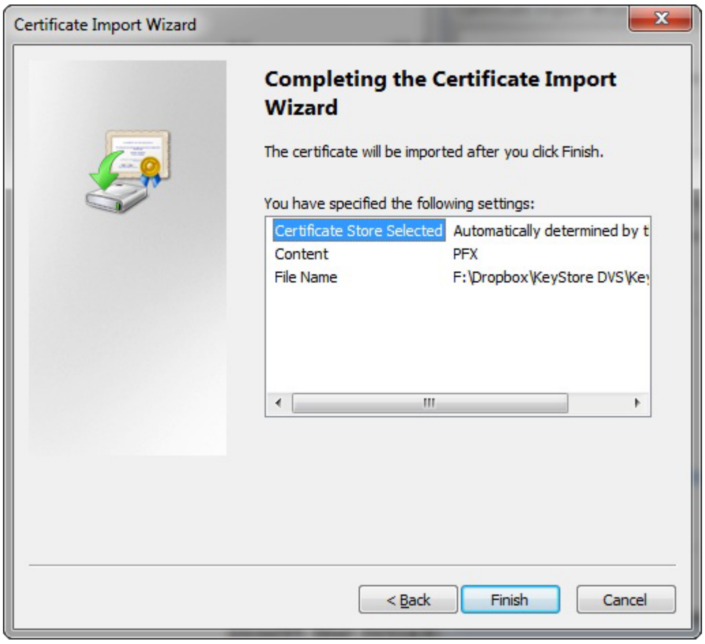
○ Place all certificates in the following store

Certificate store:

Learn more about certificate stores

Figure 1-4: Certificate store

- Click on the button **NEXT**.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	F:\Dropbox\KeyStore DVS\Key

Figure 1-5: Summary of your settings

This screen provides a summary of the certificate import.

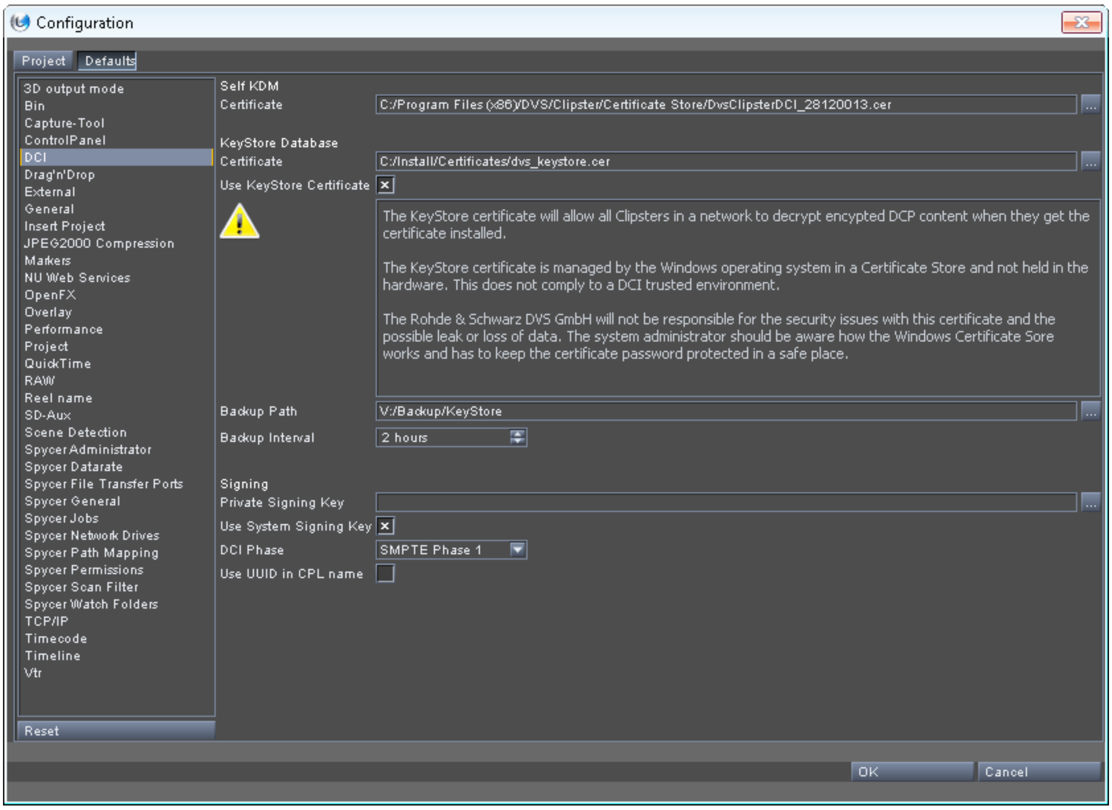
- Click on the button **FINISH**.

The certificate is now installed in the Windows certificate store. You can verify this with the Windows program *certmgr.msc*. The KeyStore network certificate can be found in the folder **Personal**.

Installing the Public Key on a DCI Mastering System

This section explains how to install and set up the certificate containing the public key on a DCI Mastering system. For this perform the following:

- At the DCI Mastering system that should be able to use the KeyStore feature copy the *keystore.cer* file to a location of your choice on the local storage. No security issues have to be regarded here because the file contains the public key of the certificate only.
- Next, start the DVS software and click on the **CONFIG…** button at the bottom to open the Configuration Tool.
- Switch to the tab **Defaults** and select the group ***DCI***.



Self KDM
Certificate: C:/Program Files (x86)/DVS/Clipster/Certificate Store/DvsClipsterDCI_28120013.cer

KeyStore Database
Certificate: C:/Install/Certificates/dvs_keystore.cer
Use KeyStore Certificate ☒

The KeyStore certificate will allow all Clipsters in a network to decrypt encypted DCP content when they get the certificate installed.

The KeyStore certificate is managed by the Windows operating system in a Certificate Store and not held in the hardware. This does not comply to a DCI trusted environment.

The Rohde & Schwarz DVS GmbH will not be responsible for the security issues with this certificate and the possible leak or loss of data. The system administrator should be aware how the Windows Certificate Sore works and has to keep the certificate password protected in a safe place.

Backup Path: V:/Backup/KeyStore
Backup Interval: 2 hours

Signing
Private Signing Key:
Use System Signing Key ☒
DCI Phase: SMPTE Phase 1
Use UUID in CPL name □

Figure 1-6: Settings to activate the KeyStore feature

- Set the path **Certificate** under **KeyStore Database** to the locally stored `keystore.cer` file and activate the check box **Use KeyStore Certificate**.

If everything is fine the check box will remain activated and the KeyStore feature will be ready for usage.

- As a last step, if not already done, configure the SpycerNet groups in the group ***Spycer Administrator*** of the Configuration Tool. All systems exchanging information for the KeyStore feature must be in the same SpycerNet group.

After confirming the settings in the Configuration Tool the procedure to install the private and public key of the KeyStore network certificate is finished. The respective DCI Mastering system should then be ready to create DCP content or decrypt it when coming from another DCI Mastering system within the same domain and/or SpycerNet group.

In case other DVS DCI Mastering systems should also be able to create or decrypt DCPs using the KeyStore feature, you have to repeat the steps to install the KeyStore network certificate on each of them.