



DVS DCI Signing Certificate Tool

User Guide

User Guide Version 1.0 for the DVS DCI Signing Certificate Tool Version 1.0

Copyright © 2008 by DVS Digital Video Systems AG, Hanover. All rights reserved.

The manuals as well as the soft- and/or hardware described here and all their constituent parts are protected by copyright. Without the express permission of DVS Digital Video Systems AG any form of use which goes beyond the narrow bounds prescribed by copyright legislation is prohibited and liable to prosecution.

This particularly applies to duplication, copying, translation, processing, evaluation, publishing, and storing and/or processing in an electronic system.

Specifications and data may change without notice. We offer no guarantee that this documentation is correct and/or complete. In no event shall DVS Digital Video Systems AG 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 DVS Digital Video Systems AG.

CLIPSTER and DVS are registered trademarks of DVS Digital Video Systems AG.

Any other product names mentioned in this documentation may be trademarks or registered trademarks of their respective owners and as such are subject to the usual statutory provisions.

DVS DCI Signing Certificate Tool

This document describes the DVS DCI Signing Certificate Tool.

The DVS DCI Signing Certificate Tool is included in the delivery of the CLIPSTER DCI Mastering feature. It enables you to create your own key pair (a personal information exchange file and a certificate file) to digitally sign files.



The most appropriate way to receive a signing key is to order it from a certificate authority (CA).

The signing key that can be created with this program is an X.509 certificate as specified by the DCI. It can be used in a DCI Mastering with CLIPSTER but may not be limited to this purpose.



Do not create your own signing key lightly. With it you should define and install a certificate hierarchy to enable others to verify your identity. You are the one responsible for certificates issued within your certificate chain.

This document contains the following information:

- Basics
 - What's a Key
 - What's a Certificate
 - What's a Certificate Chain
- Installation
- Usage
 - Starting the Program
 - Exiting the Program
- The User Interface

Basics

The following explains some basics that you may find helpful when using the DVS DCI Signing Certificate Tool.

What's a Key

A key is a piece of information (normally a string) that determines the output of a cryptographic algorithm. The key is used during encryption by the cryptographic algorithm to transform a certain piece of information (e.g. plaintext) to ciphertext, i.e. encrypted information. Vice versa, during decryption the key is used by the algorithm to decode the ciphertext back to the original information.

There are two types of keys available:

symmetric	If the algorithm uses the same key during en- and decryption, it is known as a symmetric key algorithm.
asymmetric	Algorithms that require two different keys, one for encryption and one for decryption, are called asymmetric key algorithms. The concept behind them is that it is almost impossible to compute one key from the other. With this you can make one key public (the public key) while keeping the other in secret (the private key), thus providing others with the means, for example, to send encrypted pieces of information to the private key holder that only he can decode.

What's a Certificate

A certificate is a file that usually contains a key. Additionally it includes a digital signature to ensure the validity of the key/certificate. With this the purpose of a certificate is, on the one hand, to provide you with a key and, on the other, to confirm that this certificate and key belong to a certain identity (e.g. a person, institute or company).

Ideally the signature comes from a certificate authority (CA) employed with the task to check identities before issuing certificates that refer to this identity. However, the most commonly used certificates are those that users make for themselves (self-signed certificates). Also common are certificates that users make for others so that these can certify validities on behalf of the user (certificate chain, see section "What's a Certificate Chain").

In the DCI Mastering a certificate normally contains a public key (*.cer or *.pem files). A private key is usually provided in a personal information exchange file (*.pfx) which is typically encrypted and re-

quires a password to be opened. Mostly this file will contain the public-key certificate (or more than one if a certificate chain is involved) for authentication as well.

What's a Certificate Chain

Certificates (see section "What's a Certificate") can be distributed in a chain, where the last certificate (the leaf certificate that cannot create other certificates) certifies that it comes from another certificate (the intermediate certificate), this certifying that it comes from a further certificate (another intermediate), and so on until the last certificate in the chain is reached (the root certificate that confirms the validity of the whole chain as well as the identity of its issuer).

The whole structure of a certificate chain implies a hierarchy where the highest rank is held by the root and the lowest by the leaves.

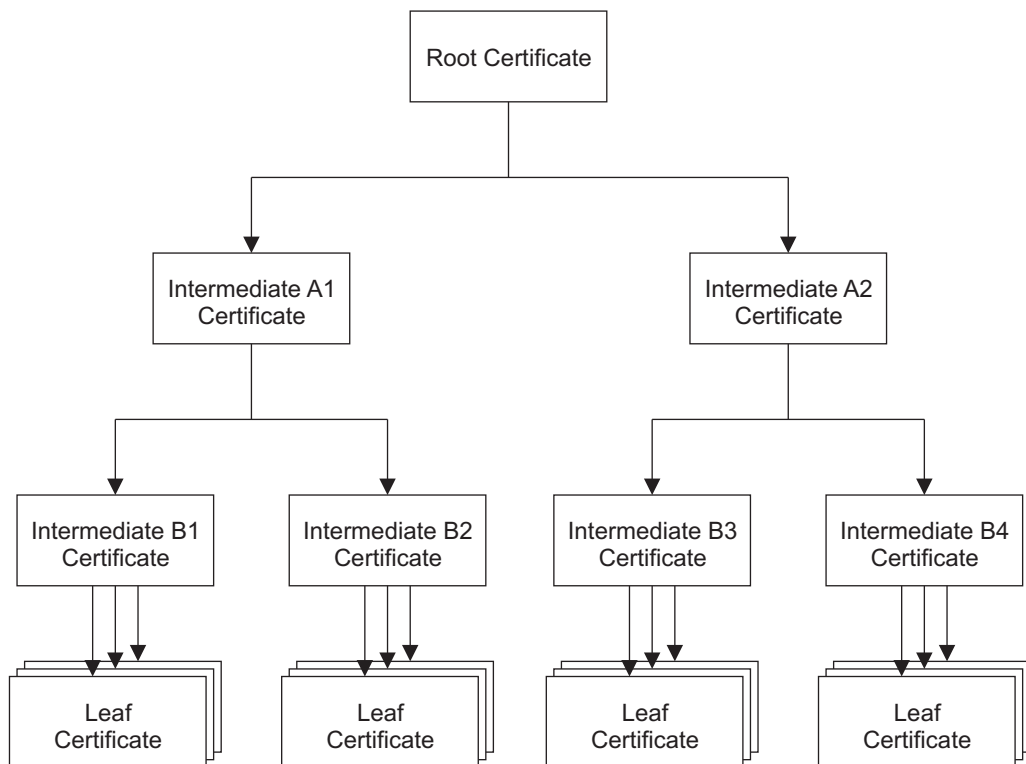


Figure 1: Certificate hierarchy

The root certificate is either a CA-issued certificate or a self-signed one, i.e. it is signed by its own private key. From this root certificate other certificates can be created (intermediates), that enable other users to digitally sign items in the name of the root via their private keys. Additionally, from intermediate certificates further certificates can be created (either other intermediates or leaf certificates). The last link in the

chain is the leaf certificate that can only be used for signing, meaning other certificates cannot be created from a leaf.

All certificates in a certificate chain refer back to the identity that is bound to the root certificate and thus inherit the trustworthiness of the root.

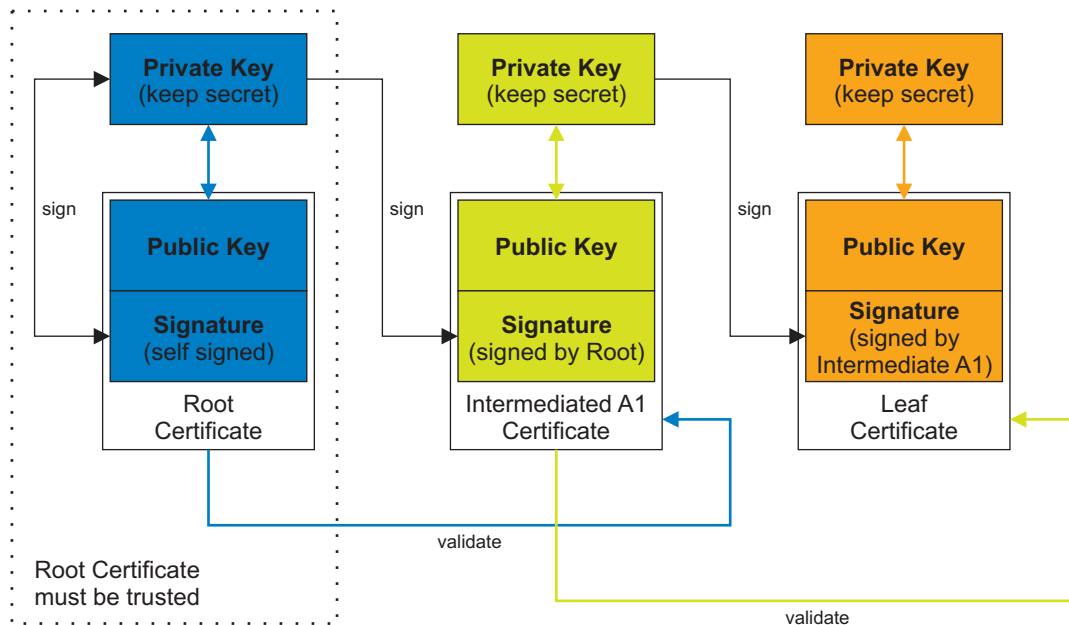


Figure 2: Certificate chain validation

In a public-key certificate no certificate chain is stored. So, in order to validate a leaf certificate at the end of a certificate chain, the complete chain up to the root certificate has to be available.

The maximum path depth from root to leaf that is allowed in a certificate hierarchy is a property of the root certificate. During the creation of the root it has to be set and it will be inherited correspondingly to the lower ranks. Within this path depth certificates can be created from root and intermediate certificates.

When setting up a certificate hierarchy take care that only trusted users receive certificates (i.e. the private key of these certificates). This applies especially to intermediate certificates that can be used to create other certificates.

Installation

The program will be delivered on a CD-ROM with the CLIPSTER DCI Mastering feature. To start the installation perform the following:



The DVS DCI Signing Certificate Tool has to be installed and can be run on a CLIPSTER DCI Mastering system only.

- Open a file manager (e.g. Windows Explorer) on the computer system where the DVS DCI Signing Certificate Tool should be installed and browse to the installation file (*Install_DCISigning-CertificateTool_<version no.>.exe*).
- Execute the installation file, for example, with a double-click of the mouse.

This starts the installation routine which will guide you through the installation.

- Follow the instructions given on the screen.

During the installation procedure the necessary files will be installed on the computer system. Most files will be installed in the installation path of the CLIPSTER software (usually *C:\Program Files\DVS\Clipster*). The installation is finished as soon as a message reports this.



The tool can be deinstalled easily via the provided uninstallation file stored in the same directory.

Usage

This section describes the basic usage of the DVS DCI Signing Certificate Tool, i.e. it is explained how to start the program and how to exit it.

Starting the Program


This section provides you with a description about how to start the DVS DCI Signing Certificate Tool:

- Select from the **START** button menu of Windows in the submenu **DVS** the entry **Maintenance**.
- From the opening submenu select the entry for the DVS DCI Signing Certificate Tool (for example, **All Programs » DVS » Maintenance » DVS DCISigningCertificateTool**).

This will start the DVS DCI Signing Certificate Tool by DVS and its user interface will be displayed on the screen (see section “The User Interface” on page 7).

Exiting the Program

To end the DVS DCI Signing Certificate Tool and exit it perform the following:

- Use the exit button  provided by the window of the DVS DCI Signing Certificate Tool or press the keyboard combination [Alt + F4].

After this the program will be closed.

The User Interface

After starting the DVS DCI Signing Certificate Tool (see section “Starting the Program” on page 6) its user interface will be displayed on the screen:

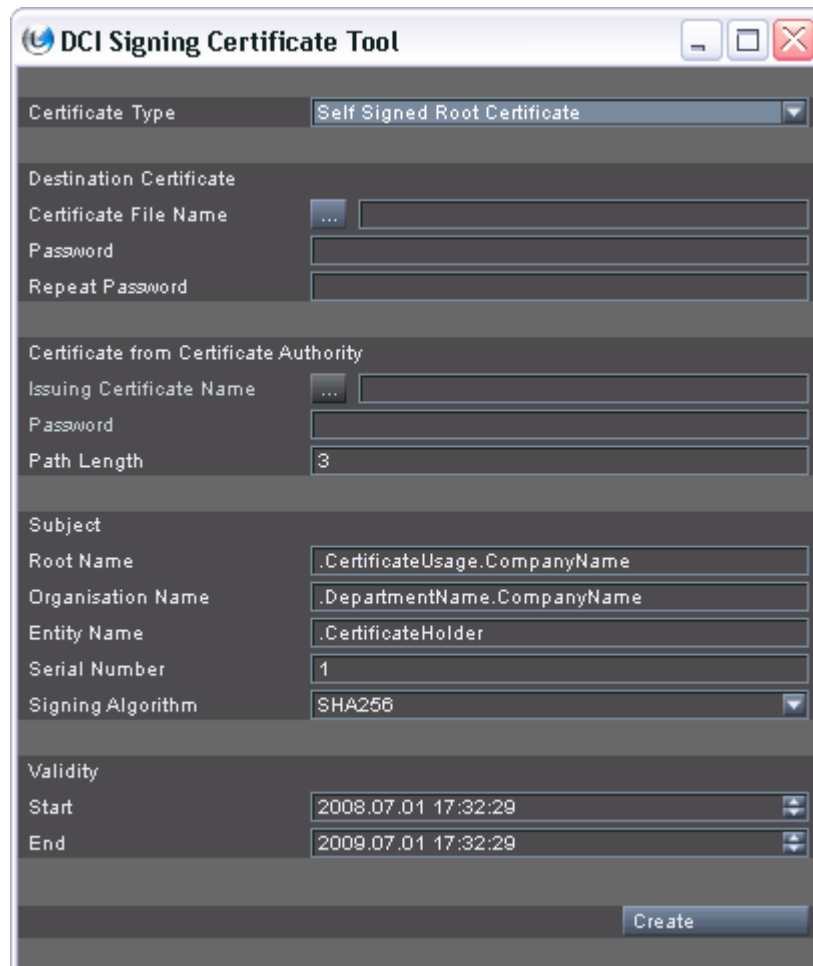






Figure 3: User interface of the DVS DCI Signing Certificate Tool

The items provided by the user interface enable you to create signing keys. The following items are available:

- | | |
|------------------------------|---|
| Certificate Type | Use this combo box to select the type of the certificate, i.e. root, intermediate or leaf. |
| Certificate File Name | Either enter a path and file name in the entry field or use the button  to browse to a directory and select a file (or enter a file name). You may leave out the file extension. |

Password	The content of the private key file will be encrypted and requires an authentication to be used. In this entry field type in the password that should be used to authenticate the usage of the private key file. It has to be entered case sensitive.
Repeat Password	To be sure that the password has been typed in correctly repeat the password in this field.
Issuing Certificate Name	Not required for a root. When creating an intermediate or leaf, you have to specify here the private key file (PKCS12 file) that the certificate to be created should be derived from (parent signing key). Either enter a path and file name in the entry field or use the button  to browse to the file.
Password	Not required for a root. When creating an intermediate or leaf, type in in this field the password for the private key file entered in Issuing Certificate Name .
Path Length	In this field enter the path length that should be allowed in your certificate chain. For a root it can be set freely. For an intermediate or leaf it is a property of the private key file entered in Issuing Certificate Name . Then the maximum allowed value is <code><path length of private key file> - 1</code> , but can be set to a lesser value if wanted.
Root Name	Not required for an intermediate or leaf, i.e. the one of the private key file entered in Issuing Certificate Name will be used. Enter in this field a unique name for the organization that is in possession of the root. Example: CA.<domain name>.<company name>
Organization Name	Enter in this field a unique name for the organization that issues the certificate to be created. In case of a company this can be the name of the department.  The entries in the fields Root Name and Organization Name should be different. Example: <company name>.<department name>

Entity Name	<p>Enter in this field the name of the certificate holder (e.g. name of a person or department).</p> <p><i>Leaf certificates only:</i> When a leaf certificate for a D-Cinema environment (DCI) is created, the entity name should also carry the name's role in this environment as a prefix. For a CLIPSTER DCI Mastering system this will usually be 'CS' for content signer. It will be automatically added to the name entered here when a leaf is created, resulting in the name CS.<name>.</p> <p>Example: <department name>.<holder/entity name>.</p>
Serial Number	<p>This field is available for convenience reasons because issued certificates should be disambiguous. The entries in the fields Root Name, Organization Name, Entity Name and Serial Number are taken to form such an ID (fields 'Subject' and 'Serial number' of the certificate). To facilitate this, the serial number of the program will increase by one with every certificate created. Although it starts by one, you can enter any serial number you want.</p> <p> The latest used serial number is written to a file saved at the same location as the DVS DCI Signing Certificate Tool.</p>
Signing Algorithm	<p>Specify in this field the signing algorithm that should be used for the certificate. The following signing algorithms are available:</p> <p>SHA1 Use this setting to create a certificate for D-Cinema players based on the JPEG Interop standard.</p> <p>SHA256 Use this setting to create a certificate for D-Cinema players based on the SMPTE standard.</p>
Start End	<p>Enter the start and end validity for the certificate to be created in these fields. For a root it can be set freely. For an intermediate or leaf it is a property of the private key file entered in Issuing Certificate Name. Then the validity must lie within the validity of the parent signing key.</p>
CREATE	<p>Use this button to create the certificate. If entries are wrong you will then be informed about them and the respective fields will be adjusted automatically to the maximum/minimum allowed value.</p>

Once all settings are made a click on the button **CREATE** will create the signing key (i.e. one *.pem and one *.pfx file) at the specified location.



Figure 4: Certificates were successfully created

The latest used serial number is written to a file saved at the same location as the DVS DCI Signing Certificate Tool.

If entries are wrong, for example, because they are outside the boundaries set by the parent signing key, you will be informed about them and the respective fields will be adjusted automatically to the maximum/minimum allowed value.