Instruction for using Signtool and Jarsigner

Certum Code Signing

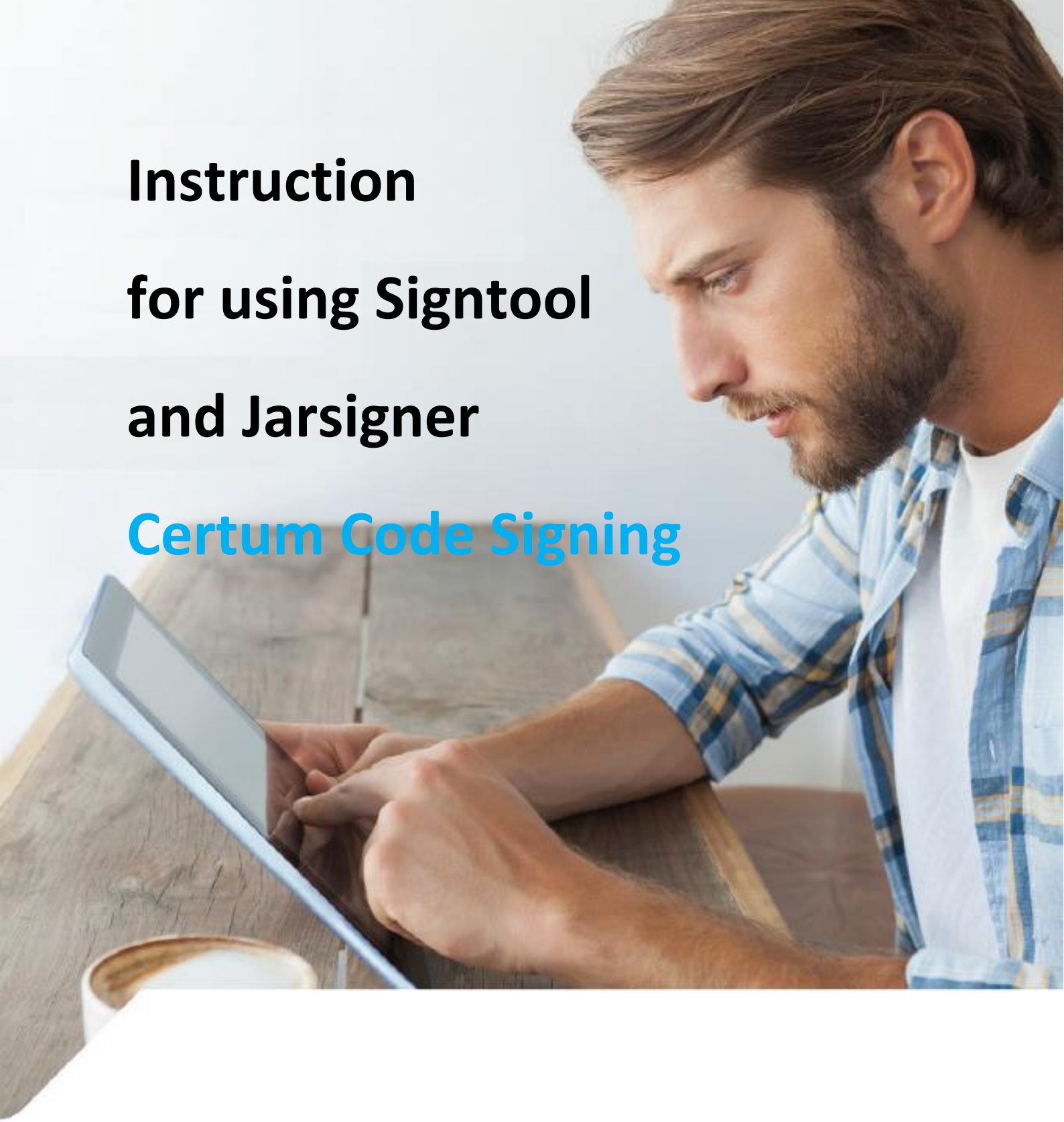


Table of content

1 Product description

The **Code Signing** certificate is used for digital signing of code as well as already developed and installed applications. The certificate is stored on a cryptographic card so both the code as well as already developed applications can be signed using common tools, such as ***signtool.exe*** and ***jarsigner***.

The instruction provides description of the path for using Signtool and Jarsigner.

2 Signtool

The **Code Signing** certificate is used for digital signing of code as well as already developed and installed applications. The certificate is stored on a cryptographic card so both the code as well as already developed applications can be signed using common tools, such as ***signtool.exe*** and ***jarsigner***.

The instruction provides description of the path for using Signtool and Jarsigner.

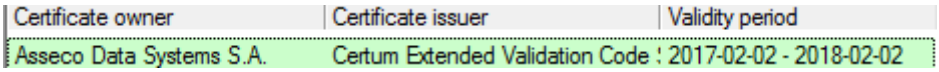
2.1. Tool description

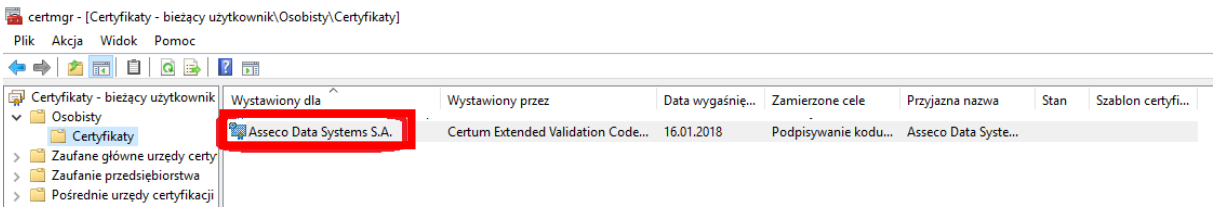
Signtool is a command-line tool for **code signing of files, signature verification in files and date stamping of files.** The tool is available in Windows development kit (Windows SDK[Software Development Kit]). All operations with Code Signing require a reader connected with the card on which the Code Signing certificate is stored. Find out more about the tool here: https://msdn.microsoft.com/pl-pl/library/8s9b9yaz(v=vs.110).aspx

2.2. Signing

To sign a file use the following command in the command line (cmd.exe):
signtool sign /n "[1] " / t [2] /fd [3] /v [4]

[1] – Name of certificate owner, which can be verified in the proCertum CardManager application or system tool certmgr.msc





[2] – Time stamp address. For Certum http://time.certum.pl,
[3] – Name of signature algorithm. Available are sha1 and sha256,
[4] – Path for the file being signed.

Here is an example of a correct command:

> **signtool sign /n "Asseco Data Systems S.A." / t http://time.certum.pl/ /fd sha1 /v file.exe**

2.3. Verification

To verify the file, use the following command in the command line (cmd.exe):
signtool verify /pa [1]

[1] – Name the file being signed

Here is an example of a correct command:

> **signtool verify /pa file.exe**

3. Jarsigner

3.1. Tool description

Jarsigner is a command-line tool for **digital signing of files and signature verification.** The tool is available in Oracle development kit (JDK [Java Development Kit]). All operations with Code Signing require a reader connected with the card on which the Code Signing certificate is stored. Find out more about the tool here:
http://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html

3.2. Configuration

An additional configuration is necessary before *jarsigner* can be used. Provider configuration file must be created for PKCS#11. To do this, create new file in *.cfg format (such as for example: provider.cfg). The content of the file is as follows:

> **name=[1]**
> **library=[2]**
> **slot=[3]**

[1] – Provider's name. Recommended: Crypto3PKCS.
[2] – Path to PKCS library. If the proCertum CardManager application is already installed, the default path is: *C:\Windows\System32\crypto3PKCS.dll*
[3] – Number of the slot with the card in. The default value is -1 which will automatically detect the first available slot.

Here is an example of configuration:

> **name=Crypto3CSP**
> **library=C:\Windows\System32\crypto3PKCS.dll**
> **slot=-1**

3.3. Signing

To sign a file use the following command in the command line (cmd.exe):

jarsigner -keystore NONE -tsa "[1]" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "[2] " -storepass "[3]" "[4]" "[5]"

[1] – Time stamp address. For Certum http://time.certum.pl,
[2] – Path to provider configuration file (“Configuration” section),
[3] – Password for the card,
[4] – Path for the file being signed.
[5] – Name of certificate owner, which can be verified in the proCertum CardManager application.

Here is an example of a correct command:

> **jarsigner -keystore NONE -tsa "http://time.certum.pl" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "provider.cfg" -storepass "123456" "[signed]proCertumJavaApi.jar" "Asseco Data Systems S.A."**

3.4. Verification

To verify the file, use the following command in the command line (cmd.exe):

jarsigner -verify -verbose -keystore NONE -tsa "[1]" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "[2] " -storepass "[3]" "[4]" "[5]"

[1] – Time stamp address. For Certum http://time.certum.pl,
[2] – Path to provider configuration file (“Configuration” section),
[3] – Password for the card,
[4] – Path for the file being signed.
[5] – Name of certificate owner, which can be verified in the proCertum CardManager application.

Here is an example of a correct command:

> **jarsigner -verify -verbose -keystore NONE -tsa "http://time.certum.pl" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "provider.cfg" -storepass "123456" "[signed]proCertumJavaApi.jar" "Asseco Data Systems S.A."**