



Web Signer 1.0.7



User Guide

© **Disig[®], a.s.**

Záhradnícka 151, 821 08 Bratislava

Phone: +421-2-2850150, E-mail: disig@disig.sk

IČO: 35 975 946, VAT ID: SK2022116976

Registered in the Commercial Register of the District Court Bratislava I, Section Sa, File 3794/B

All rights reserved.

Published in Bratislava, Slovak republic.

The information in this document cannot be modified without written permission of Disig, a.s.
This document has not passed formal language review process.

Trademarks

The names mentioned in this document may be the trademarks of their respective owners.

Table of contents

1.	Introduction	5
1.1.	Abbreviations	5
2.	Product description	6
2.1.	System requirements	6
2.1.1.	Microsoft Internet Explorer	6
2.1.2.	Microsoft Edge	6
2.1.3.	Mozilla Firefox 51 or older	7
2.1.4.	Mozilla Firefox 52 or newer	7
2.1.5.	Safari	7
2.1.6.	Google Chrome	7
3.	Description of graphical user interface	8
3.1.	Main application window	8
3.2.	Certificate selection window	10
4.	Application installation	12
4.1.	Microsoft Windows	12
4.2.	Linux	13
4.3.	Mac OS X	14
5.	Microsoft Internet Explorer	18
5.1.	Application installation	18
5.2.	Document signing	18
5.3.	Collecting the diagnostic information	20
6.	Microsoft Edge	21
6.1.	Application installation	21
6.2.	Installation of browser extension	21
6.3.	Document signing	23
6.4.	Collecting the diagnostic information	23
7.	Mozilla Firefox 51 or older and Safari	24
7.1.	Application installation	24
7.2.	Document signing	24
7.3.	Collecting the diagnostic information	25
8.	Mozilla Firefox 52 or newer	26
8.1.	Application installation	26
8.2.	Installation of browser extension	26
8.3.	Document signing	27

8.4.	Collecting the diagnostic information	27
9.	Google Chrome	28
9.1.	Application installation	28
9.2.	Extension installation to browser	28
9.3.	Document signing	29
9.4.	Collecting the diagnostic information	29
10.	Collecting the diagnostic information	30
10.1.	Web Signer application	30
10.2.	ActiveX version of Web Signer	30
10.3.	JAVA applet Web Signer	31
11.	Known issues	33
11.1.	Application does not start in Safari 12	33
11.2.	Extension gets disabled in Microsoft Edge	33
11.3.	Error when selecting signing certificate in Safari	33
12.	Technical support	37

1. Introduction

This document is a user manual for Web Signer 1.0.7 (Web Signer), which enables end user to create a qualified electronic signature in the web browser in accordance with valid legislation of Slovak Republic.

1.1. Abbreviations

API	-	Application Programming Interface
OS	-	Operating system
PKCS	-	Public Key Cryptography Standard
QSCD	-	Qualified Signature Creation Device

2. Product description

Web Signer allows end users to sign electronic documents with a qualified electronic signature in web browser. It is available in multiple technology variants designed specifically for the most popular web browsers.

2.1. System requirements

The basic precondition for successful use of the application is to use a supported operating system along with a supported web browser.

On the Microsoft Windows platform, application has been tested in Windows 7, Windows 8.1 and Windows 10 with Microsoft Internet Explorer 11, Microsoft Edge 42, Mozilla Firefox 63 and Google Chrome 70 browsers.

On Linux platforms, application has been tested in Debian 8 and 9, Ubuntu 16.04 and 18.04, Mint 18 and 19 with Mozilla Firefox 52 - 63 and Google Chrome 70 browsers.

On Mac OS X, application functionality has been tested in Mac OS X 10.13 with Mozilla Firefox 63 and Google Chrome 70, and in Mac OS X 10.10 with Safari 8.

The application may also work with unlisted versions of operating systems and browsers.

2.1.1. Microsoft Internet Explorer

In Microsoft Internet Explorer, on the Microsoft Windows operating system, Web Signer is typically used in the form of ActiveX component that needs to be installed before the first use.

The .NET Framework 2.0 or higher is required to run the Web Signer ActiveX component.

The component is compatible with QSCD devices that communicate via Microsoft CryptoAPI or PKCS#11 API.

2.1.2. Microsoft Edge

A standalone Web Signer application along with a dedicated browser extension is required for Microsoft Edge on Microsoft Windows 10. Both application and extension needs to be installed before the first use.

Browser extension requires Microsoft Edge 40 or newer that is available in Windows 10 since version 1703 also known as Creators Update.

Application requires .NET Framework that is the standard part of Microsoft Windows 10.

Application is compatible with QSCD devices that communicate via Microsoft CryptoAPI or PKCS#11 API.

2.1.3. Mozilla Firefox 51 or older

JAVA applet version of the signing application is used in Mozilla Firefox 51 or older on Microsoft Windows, Linux and Mac OS X platforms.

Applet does not need to be installed but JAVA Runtime Environment 1.6 (JAVA 6) or newer (JAVA 7 or JAVA 8) needs to be present on your computer.

Applet is compatible with QSCD devices that communicate via PKCS#11 API.

2.1.4. Mozilla Firefox 52 or newer

A standalone Web Signer application along with a dedicated browser extension is required for Mozilla Firefox 52 or newer on Microsoft Windows, Linux and Mac OS X. Both application and extension needs to be installed before the first use.

The .NET Framework 2.0 or higher is required on the Microsoft Windows platform.

On Microsoft Windows platform, application is compatible with QSCD devices that communicate via Microsoft CryptoAPI or PKCS#11 API. On other platforms, application is compatible with QSCD devices that communicate via PKCS#11 API.

2.1.5. Safari

JAVA applet version of the signing application is used in Safari on Mac OS X.

See chapter 11.1 for detailed information on supported versions of Safari.

Applet does not need to be installed but JAVA Runtime Environment 1.6 (JAVA 6) or newer (JAVA 7 or JAVA 8) needs to be present on your computer.

Applet is compatible with QSCD devices that communicate via PKCS#11 API.

2.1.6. Google Chrome

A standalone Web Signer application along with a dedicated browser extension is required for Google Chrome on Microsoft Windows, Linux and Mac OS X. Application along with the extension needs to be installed before the first use. Extension for Chrome (without Web Signer signing application) is also available in Chrome Web Store.

The .NET Framework 2.0 or higher is required on the Microsoft Windows platform.

On Microsoft Windows platform, application is compatible with QSCD devices that communicate via Microsoft CryptoAPI or PKCS#11 API. On other platforms, application is compatible with QSCD devices that communicate via PKCS#11 API.

3. Description of graphical user interface

Graphical user interface of the application consists of main window and the certificate selection window.

3.1. Main application window

Graphical user interface of the main application window contains one toolbar at its top and one toolbar at its bottom. The application can operate in signing or viewing mode.



Figure 3-1 Main application window in signing mode



Figure 3-2 Main application window in the viewing mode

The following table describes individual controls available in the main window:

Control number	Control description
1	"Previous Page" button Click the button to view the previous page of the document.
2	„Next page“ button Click the button to view the next page of the document.
3	"Current Page" field This field contains the number of currently displayed page of the document. In this field, you can also manually enter the page you want to view and confirm the entry by pressing the "Enter" key.
4	„Total number of pages“ field This field contains a number representing the total number of pages of the document.
5	„Zoom in“ button Click on the button to zoom in the displayed page.
6	„Zoom out“ button Click on the button to zoom out the displayed page.
7	„Current zoom“ field This field contains current zoom value for displayed page and allows you to change it by selecting one of the predefined values.
8	„View page width“ button Click the button to adjust zoom level so that whole page width is displayed.
9	„View whole page“ button Click the button to adjust zoom level so that the entire page is displayed.
10	„View original size“ button Click the button to adjust zoom level so that page is displayed in its real size (100%).
11	„About“ button

	Click the button to view application version information.
12	<p>„Server name“ field Main window title always shows the name of the server the application is communicating with. User is required to verify that application communicates with the correct server.</p>
13	<p>„Certificate selection“ button Button is only available in signing mode. Click the button to select signing certificate. Button title “Click to choose signing certificate” indicates that signing certificate has not been selected yet and it is not possible to sign the document yet. After the signing certificate has been selected the button title changes to the text describing the selected certificate and “Sign” button becomes active.</p>
14	<p>„Sign“ button Button is only available in signing mode. Click the button to sign currently displayed document.</p>
15	<p>„Close“ button Button is only available in viewing mode. Click the button to close the application.</p>

3.2. Certificate selection window

Graphical user interface of the certificate selection window clearly presents available certificate stores and their contents. The user can choose one specific certificate that will be used for document signing.

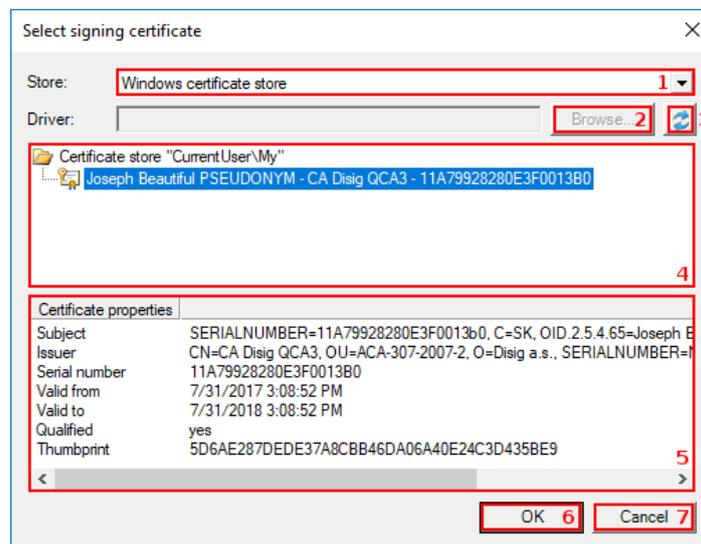


Figure 3-3 Signature Certificate Selection Window

The following table describes individual controls available in the certificate selection window:

Control number	Control description
1	<p>„Store“ field This field contains the list of currently available signing certificate stores that were predefined by the service provider. Certificates located in the selected</p>

	store will be show in the field no. 4 when a particular store is selected. Depending on the type of selected store, application may request user to enter the PIN code needed to access the store.
2	„Browse“ button Click the button to select an arbitrary PKCS#11 library that will provide access to an alternative signing certificate store. Note: This feature may not be available on all web sites.
3	„Refresh“ button Click the button to reload list of signing certificates from selected store.
4	„List of certificates“ field This field contains a list of certificates available in the selected store.
5	„Certificate properties“ field This field contains details about the certificate selected in a filed no. 4.
6	„OK“ button Click the button to confirm that you want to use certificate that is selected in the field no. 4 as a signing certificate.
7	„Cancel“ button Click the button to close the application the window without changing current signing certificate.

4. Application installation

4.1. Microsoft Windows

Start the installation by executing the installation package named „Disig_Web_Signer_1.0.7_*.msi“.



Figure 4-1 First step of installation

Continue by clicking „Next >“.

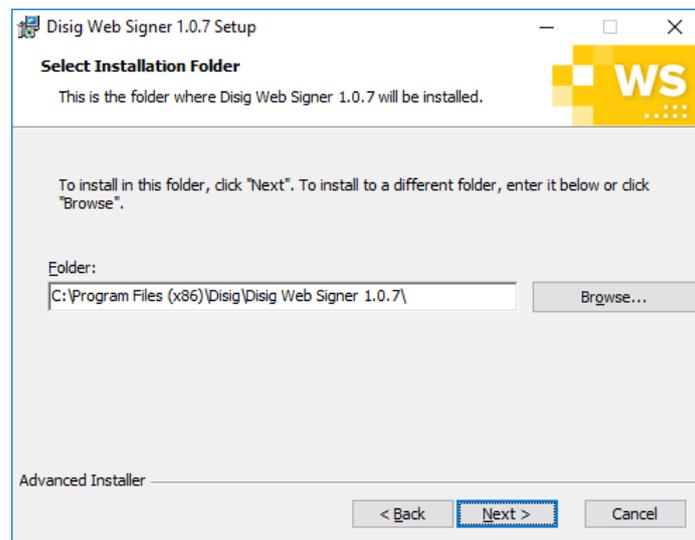


Figure 4-2 Second step of installation

Select destination directory where the application will be installed and click „Next >“ to continue.

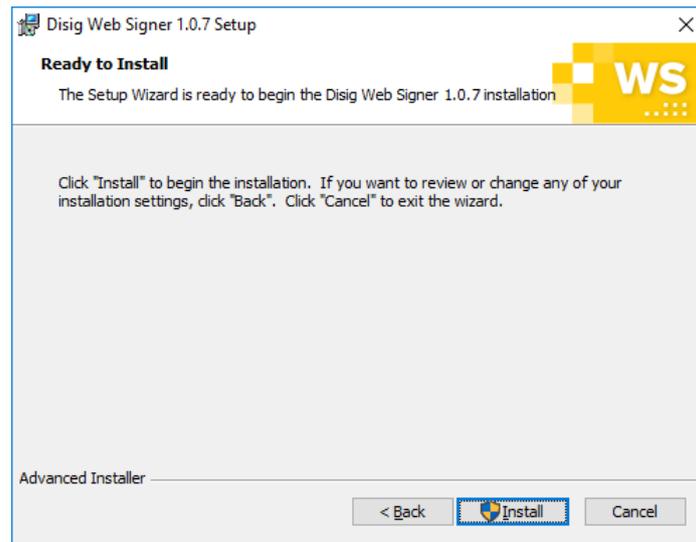


Figure 4-3 Third step of installation

Click „Install” to continue.

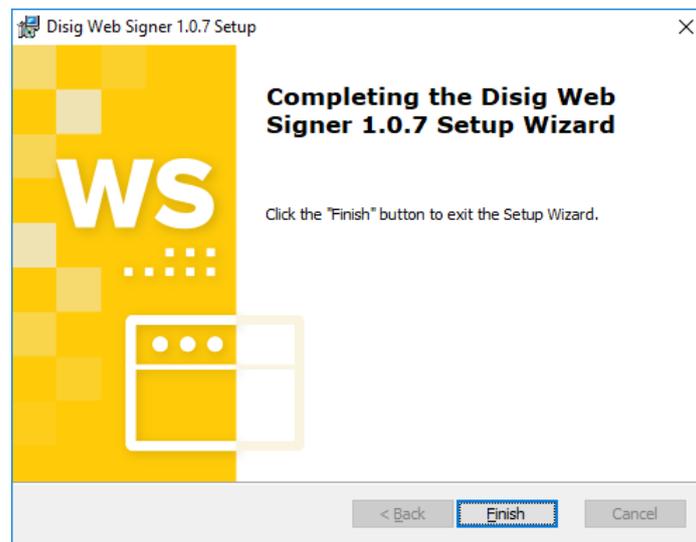


Figure 4-4 Fourth step of installation

Click „Finish” to finish the installation.

4.2. Linux

This chapter describes the installation on Ubuntu 18.04. The procedure may be different for other versions or other distributions.

Start the installation by double clicking the installation package named “disig-web-signer-1-0-7_*.deb” in the graphical user interface

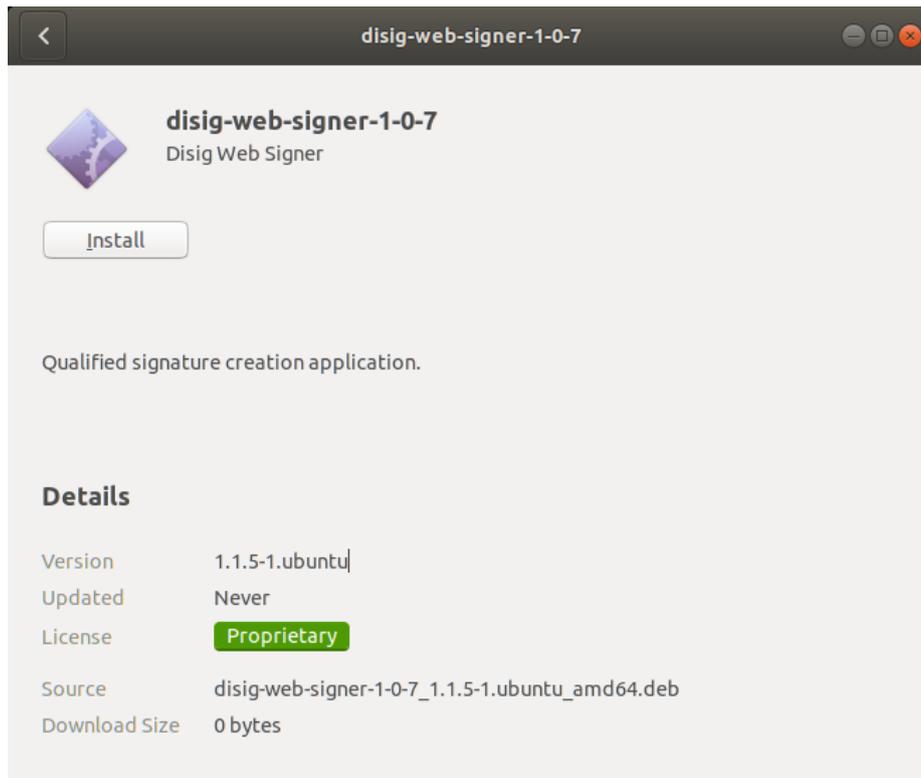


Figure 4-5 Installing package with Ubuntu Software application

In “Ubuntu Software” application, continue by clicking “Install” button. Application may ask you to enter your user password and by doing so grant a permission to install the software.

Once the package is installed successfully, “Ubuntu Software” application can be closed.

4.3. Mac OS X

This chapter describes the installation on Mac OS X 10.13. The procedure may be different for other operating system versions.

Start the installation by double clicking the archive named “Disig_Web_Signer_1.0.7_*.dmg” in the graphical user interface.



Figure 4-6 Contents of the installation archive

Continue by clicking on the installation package " Disig_Web_Signer.pkg ".

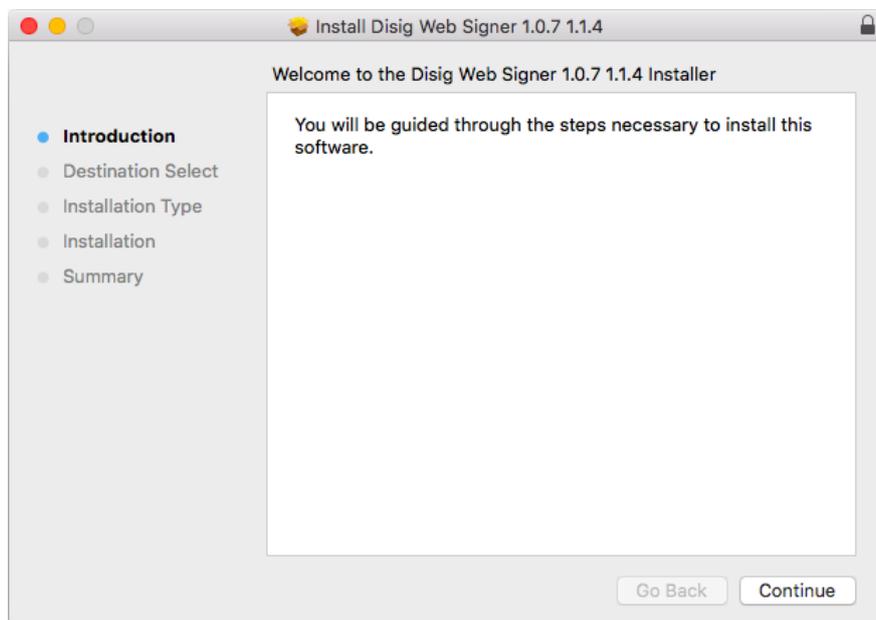


Figure 4-7 First step of installation

Continue by clicking “Continue”.

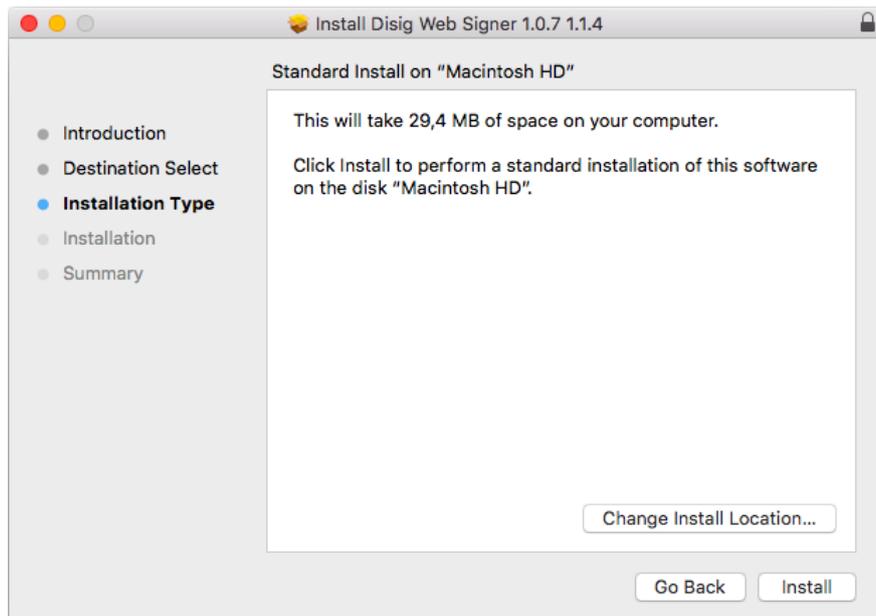


Figure 4-8 Second installation step

Click „Install” to continue.

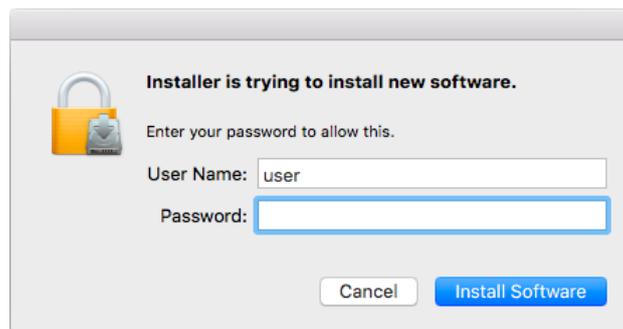


Figure 4-9 Third Installation Step

The operating system may ask you to enter your user password and by doing so grant a permission to install the software. Enter your password and click "Install Software" button to proceed

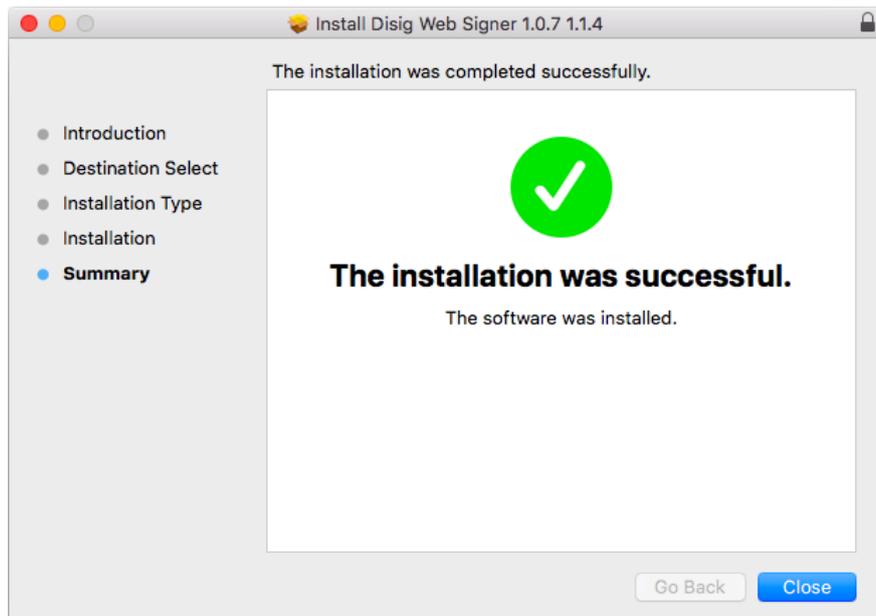


Figure 4-10 Fourth step of installation

Click „Close” to finish the installation.

5. Microsoft Internet Explorer

In Microsoft Internet Explorer, on the Microsoft Windows operating system, Web Signer is typically used in the form of ActiveX component that needs to be installed before the first use.

5.1. Application installation

The application needs to be installed by following the procedure described in chapter 4.

5.2. Document signing

Right after the start, application displays first page of the selected document.



Figure 5-1 Main application window right after the start

Signing certificate can be selected by clicking “Click to choose signing certificate” button at the bottom of the window. Certificate selection window will be displayed and will present certificates available in Microsoft Windows certificate store or in store accessible via PKCS#11 library. User can choose from signing certificate stores that were predefined by the service provider or can select an arbitrary PKCS#11 library that will provide access to an alternative signing certificate store. Application may request user to enter the PIN code needed to access selected certificate store.

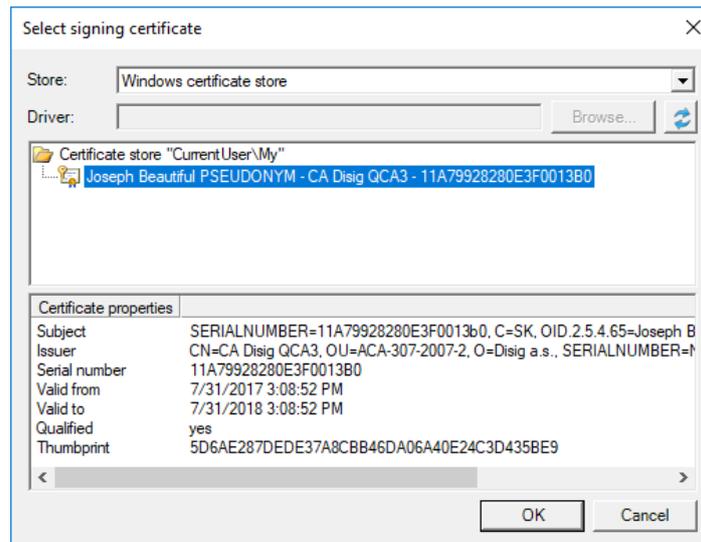


Figure 5-2 Selection of the signing certificate

Signing certificate must be selected and the selection confirmed by clicking “OK” button. After the signing certificate has been selected the button title in the main window changes to the text describing the selected certificate. Signing certificate can be changed at any time by clicking the same button.

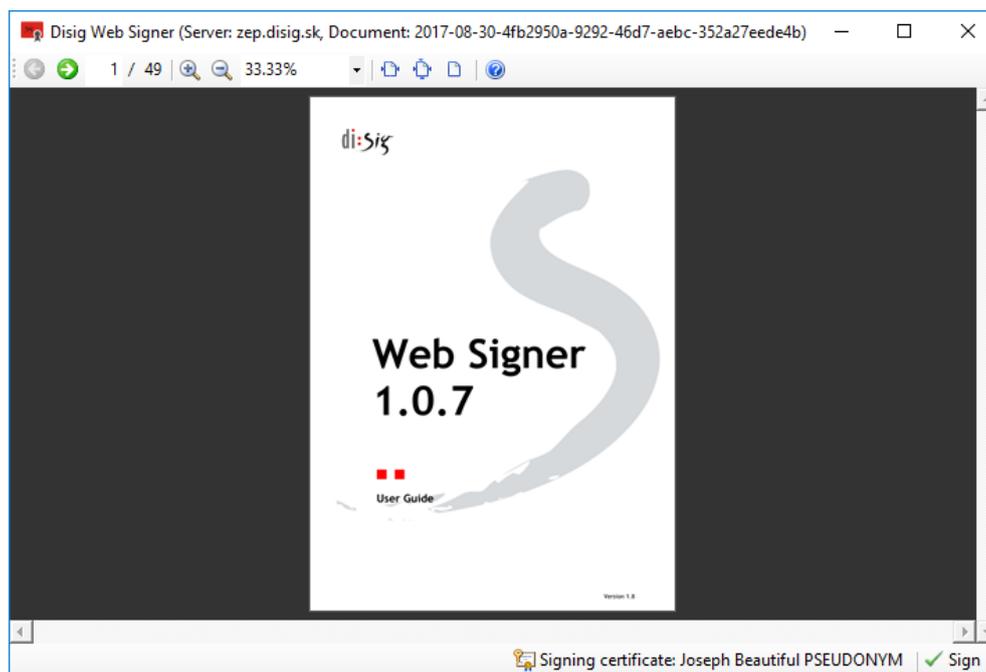


Figure 5-3 Main application window after the selection of signing certificate

After you review content of the document and click the „Sign“ button, a dialog window requesting PIN code for QSCD device will appear.

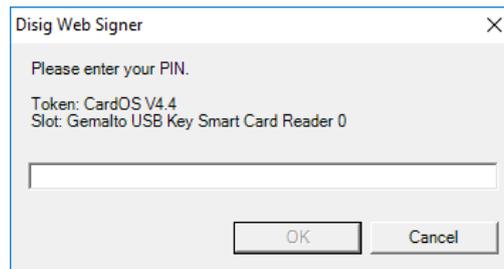


Figure 5-4 Entering the PIN code

Signing process continues once the valid PIN code is entered. Depending on the QSCD device type, you may also need to enter a secondary authentication PIN code to access the private key.

Dialog window informing about the successful signing will appear once the document is signed. After it is confirmed by clicking on “OK” button, Web Signer will be automatically closed and signed document will be made available to the web site.

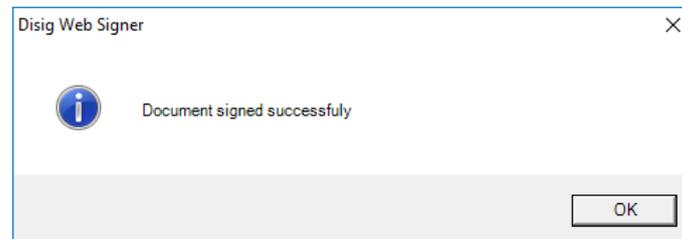


Figure 5-5 Dialog window informing about the successful document signing

5.3. Collecting the diagnostic information

The procedure for collecting the diagnostic information is the same as the procedure described in the chapter 10.2.

6. Microsoft Edge

A standalone Web Signer application along with a dedicated browser extension is required for Microsoft Edge on Microsoft Windows 10. Both application and extension needs to be installed before the first use.

6.1. Application installation

The application needs to be installed by following the procedure described in chapter 4.

6.2. Installation of browser extension

After the successful installation of standalone Web Signer application, you need to install browser extension for Microsoft Edge. This chapter describes the installation on Windows 10 version 1803. The procedure may be different for other versions.

During the installation of browser extension, your operating system must allow installation of applications from trusted sources other than just Windows Store. If you are unable to enable this option for any reason, your only option is to use Web Signer in another browser.

Open “Settings” application from the start menu.

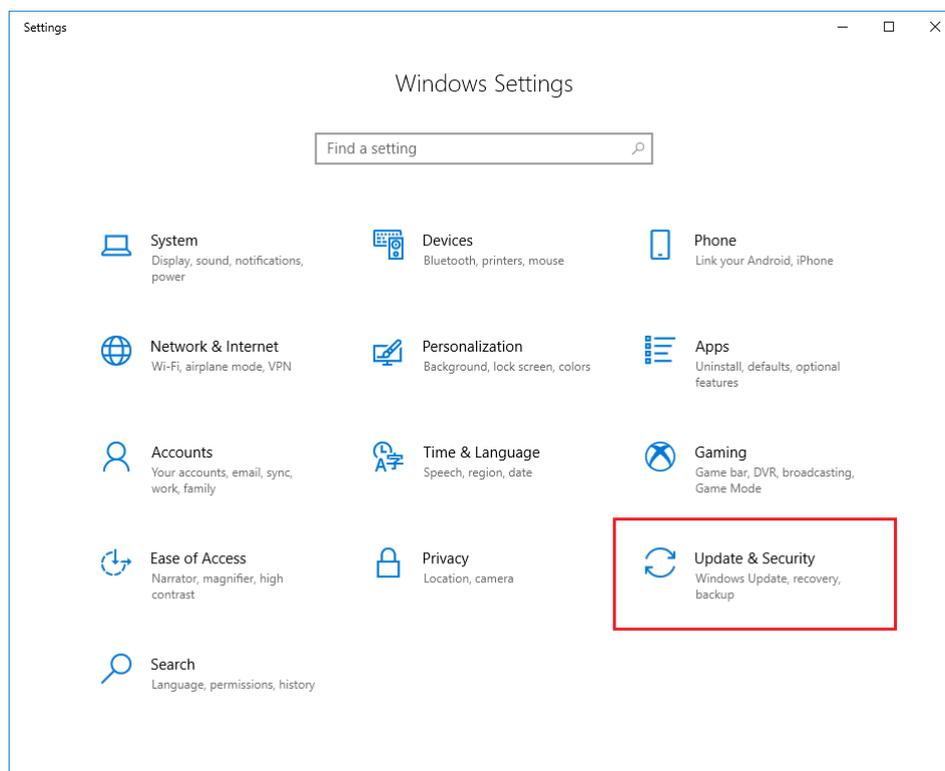


Figure 6-1 Opening “Settings” application

Select “Update & security” option.

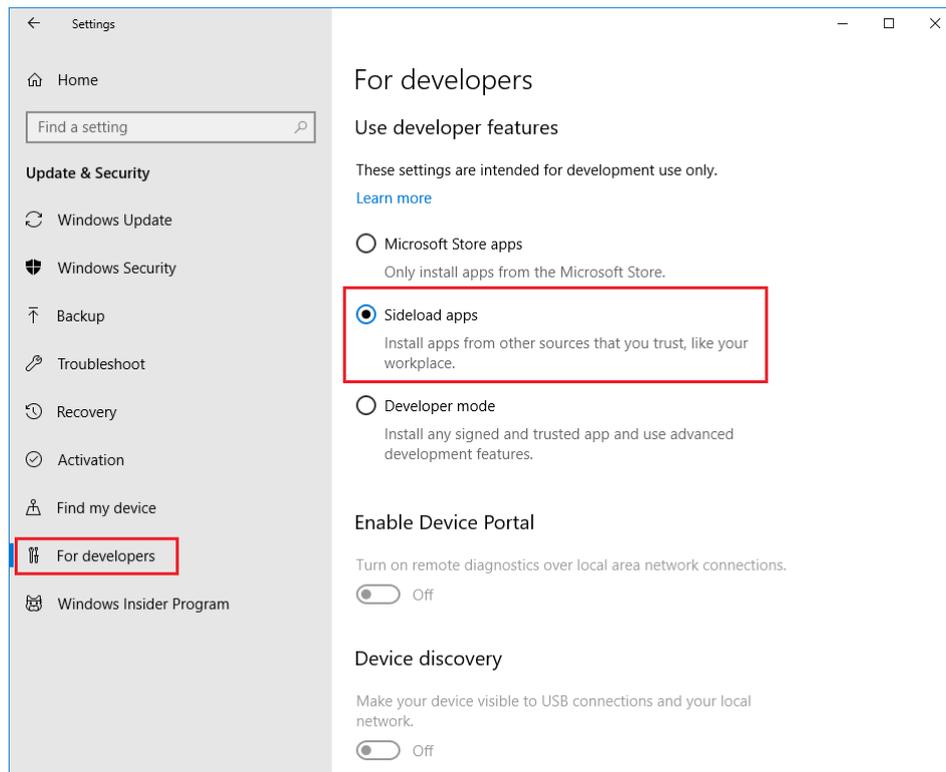


Figure 6-2 Changing the settings in “Settings” application

Select “For developers” option from the left menu and then “Sideload apps” option from the center part of the window.

Start the installation by executing the installation package named “Edge extension 1.0.0.0 for Disig Web Signer 1.0.7.appxbundle” located in “C:\Program Files (x86)\Disig\Disig Web Signer 1.0.7\Extension\Edge” directory.

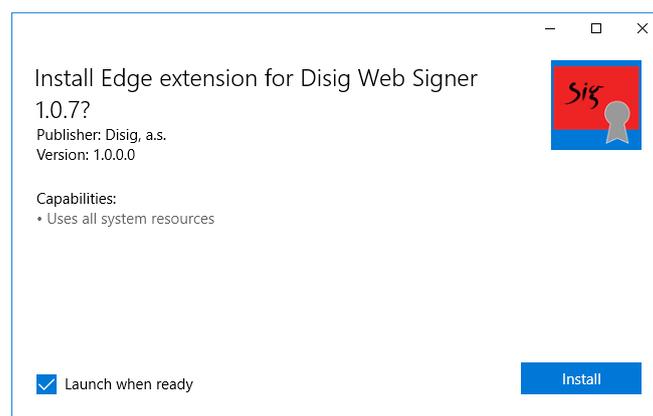


Figure 6-3 First step of installation

Click „Install” to continue.

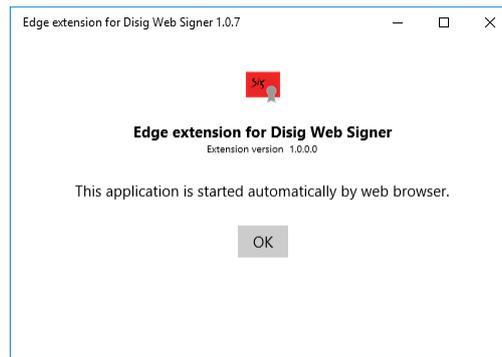


Figure 6-4 Second step of installation

Close the window or click “OK” to finish the installation.

Operating system setting related to installation of applications from other trusted sources then just Windows Store needs to be set back to its original state after the successful installation of extension.

6.3. Document signing

The procedure for document signing in Microsoft Edge is the same as the procedure described in the chapter 5.2.

In case the signing application does not start, follow the procedure described in the chapter 11.2 and verify that browser extension “Disig Web Signer 1.0.7” is not just installed but it is also enabled.

6.4. Collecting the diagnostic information

The procedure for collection of diagnostic information is the same as the procedure described in the chapter 10.2.

7. Mozilla Firefox 51 or older and Safari

Mozilla Firefox 51 or older on Microsoft Windows, Linux and Mac OS X platforms and Safari older than 12 on Mac OS X both use JAVA applet form of Web Signer.

7.1. Application installation

JAVA applet does not need to be installed.

In order to verify the ability of a web browser to use JAVA applets visit:

<http://java.com/en/download/testjava.jsp>

7.2. Document signing

During the initialization of JAVA applet, a dialog window may be displayed informing you that the trusted publisher has signed the applet.



Figure 7-1 Confirming that JAVA applet is trusted

After you enable execution of the applet by clicking "Run" button, second dialog window will be displayed requesting you to allow communication between the applet and web site.

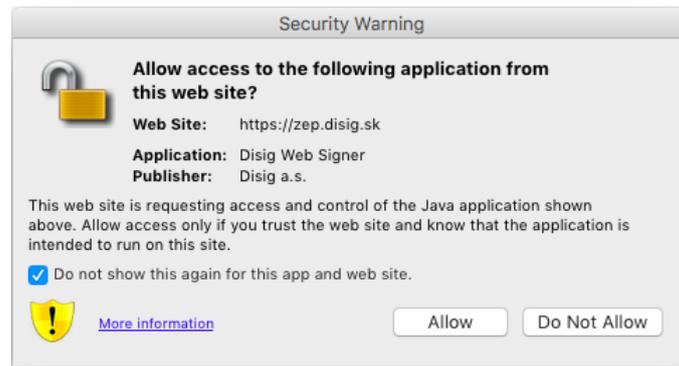


Figure 7-2 Enabling communication between application and web site

After you enable the communication by clicking “Allow” button, the content of the selected document will be displayed.

From this point, the procedure for document signing continues the same way as described in the chapter 5.2.

7.3. Collecting the diagnostic information

The procedure for collection of diagnostic information is the same as the procedure described in the chapter 10.3.

8. Mozilla Firefox 52 or newer

A standalone Web Signer application along with a dedicated browser extension is required for Mozilla Firefox 52 or newer on Microsoft Windows, Linux and Mac OS X. Both application and extension needs to be installed before the first use.

8.1. Application installation

The application needs to be installed by following the procedure described in chapter 4.

8.2. Installation of browser extension

After the successful installation of Web Signer application, browser extension needs to be installed using the file “*websigner.1.0.7.selfdist@disig.sk.xpi*” located:

- on Microsoft Windows platform in directory
C:\Program Files (x86)\Disig\Disig Web Signer 1.0.7\Extension\Firefox
- on Linux platform in directory
/opt/disig/websigner/firefox
- on Mac OS X platform in directory
/Applications/Disig Web Signer.app/Contents/SharedSupport/Firefox/

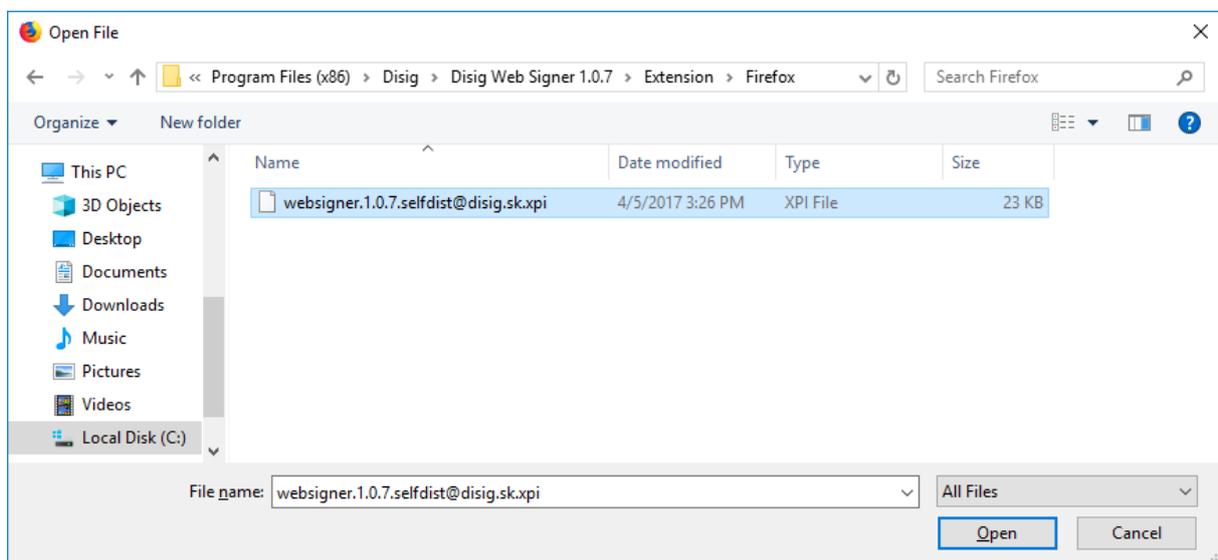


Figure 8-1 First step of extension installation

In the browser press “Ctrl + O” or “Cmd + O” key combination and select specified XPI file.

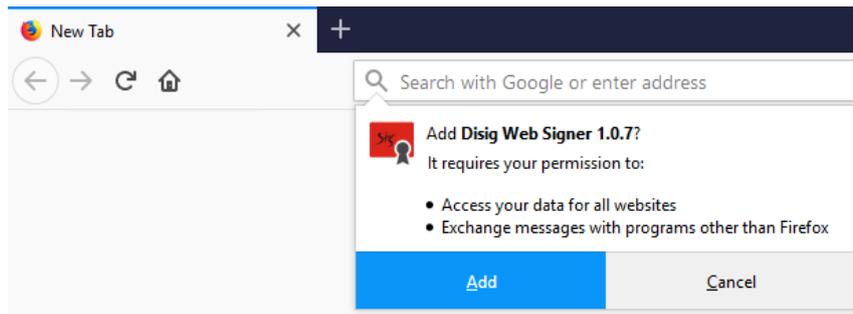


Figure 8-2 Second step of extension installation

Extension installation needs to be confirmed by clicking “Install” button.

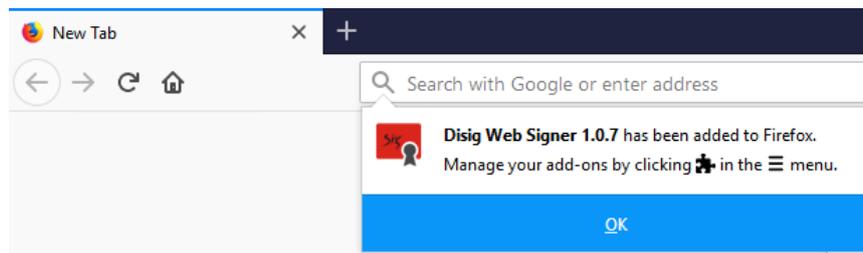


Figure 8-3 Third step of extension installation

Information about the successful installation of the extension needs to be confirmed by clicking “OK” button.

8.3. Document signing

The procedure for document signing in Mozilla Firefox is the same as the procedure described in the chapter 5.2.

8.4. Collecting the diagnostic information

The procedure for collection of diagnostic information on Microsoft Windows platform is the same as the procedure described in the chapter 10.2.

The procedure for collection of diagnostic information on Linux and Mac OS X platforms is the same as the procedure described in the chapter 10.1.

9. Google Chrome

A standalone Web Signer application along with a dedicated browser extension is required for Google Chrome on Microsoft Windows, Linux and Mac OS X. Application along with the extension needs to be installed before the first use. Extension for Chrome (without Web Signer signing application) is also available in Chrome Web Store.

9.1. Application installation

The application needs to be installed by following the procedure described in chapter 4.

9.2. Extension installation to browser

After the successful installation of standalone Web Signer application, availability of “Disig Web Signer 1.0.7” extension should be announced during the next startup of Google Chrome browser.

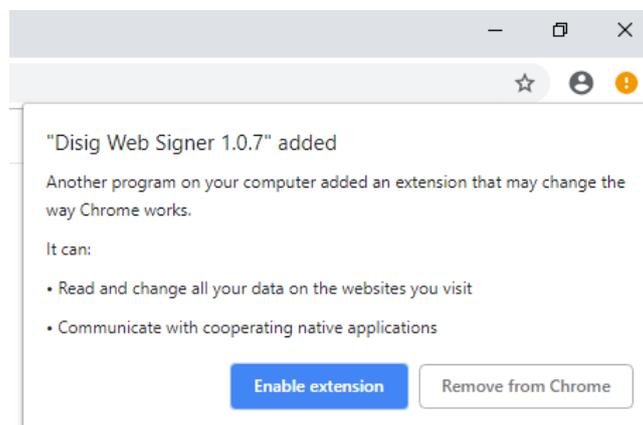


Figure 9-1 Chrome extension installation

Extension needs to be enabled by clicking "Enable extension" button.

If needed, the extension can also be manually installed from the Chrome Web Store where it is available at the following address:

<https://chrome.google.com/webstore/detail/disig-web-signer-107/odbdbcaekkgabdfaabepfjgiooilmaoe>

9.3. Document signing

The procedure for document signing in Google Chrome is the same as the procedure described in the chapter 5.2.

9.4. Collecting the diagnostic information

The procedure for collection of diagnostic information on Microsoft Windows platform is the same as the procedure described in the chapter 10.2.

The procedure for collection of diagnostic information on Linux and Mac OS X platforms is the same as the procedure described in the chapter 10.1.

10. Collecting the diagnostic information

10.1. Web Signer application

In case of any problems with Web Signer application, it is possible to enable the capturing of diagnostic information (enable logging).

Logging can be enable by right-clicking the Web Signer application icon displayed in system tray and selecting “Diagnostics > Turn logging on” option.

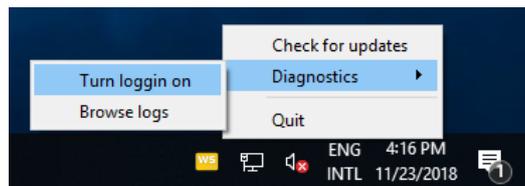


Figure 10-1 Enabling application logging

Logs are recorded into a several files located in “WebSignerLogs” directory that is automatically created in the documents directory of currently logged-on user.

Content of “WebSignerLogs” directory can be displayed by selecting “Diagnostics > Browse logs” option from the context menu.

Logging can be disabled by selecting “Diagnostics > Turn logging off” option from context menu.

10.2. ActiveX version of Web Signer

In case of any problems with ActiveX version of Web Signer, it is possible to capture diagnostic information with freely available application called “Sysinternals DebugView” that can be downloaded from the following address:

<https://docs.microsoft.com/en-us/sysinternals/downloads/debugview>

DebugView needs to be started before the main window of Web Signer is displayed. Diagnostic information will be displayed in DebugView without the need for any further configuration.

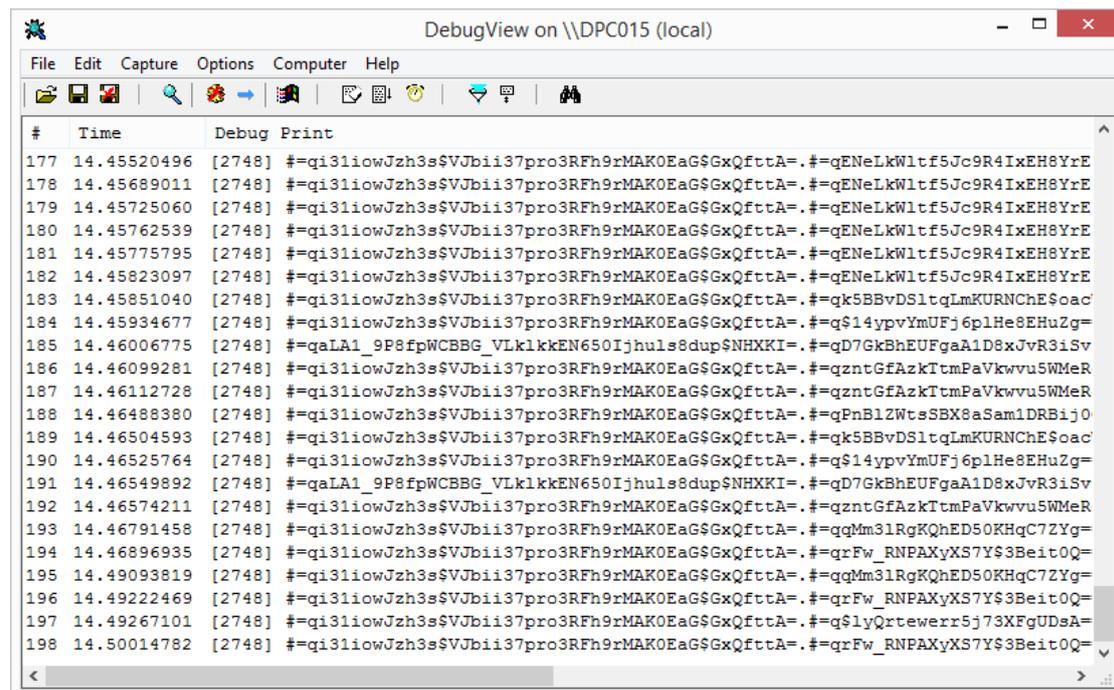


Figure 10-2 Diagnostic information displayed in DebugView

10.3. JAVA applet Web Signer

In case of any problems with JAVA applet version of Web Signer, it is possible to capture diagnostic information with standard logging subsystem of JAVA platform. Rest of the text in this chapter assumes the logging will be directed into “C:\logs\WebSigner.log” file.

As a first step, you need to create a “C:\logs\logging.properties” file with the following content:

```
handlers=java.util.logging.ConsoleHandler, java.util.logging.FileHandler
sk.disig.level=ALL
java.util.logging.ConsoleHandler.level=ALL
java.util.logging.FileHandler.level=ALL
java.util.logging.FileHandler.formatter=java.util.logging.SimpleFormatter
java.util.logging.FileHandler.pattern=C:\\logs\\WebSigner.log
java.util.logging.FileHandler.append=true
```

Next, you need to run “Java Control Panel” application from the “Start > Settings > Control Panel > Java” menu.

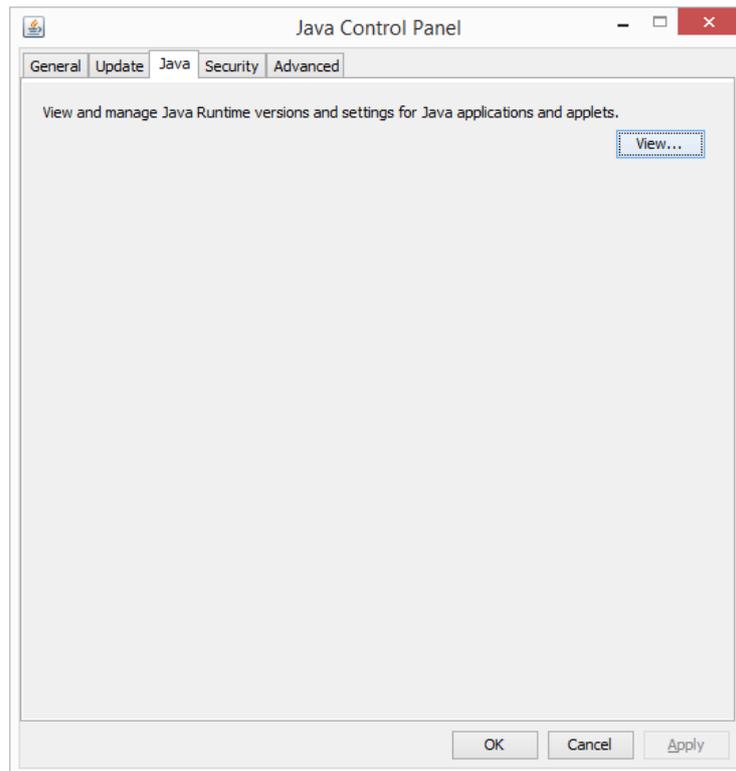


Figure 10-3 Java Control Panel

Click “View” on the “Java” tab to view “Java Runtime Environment Settings” settings.

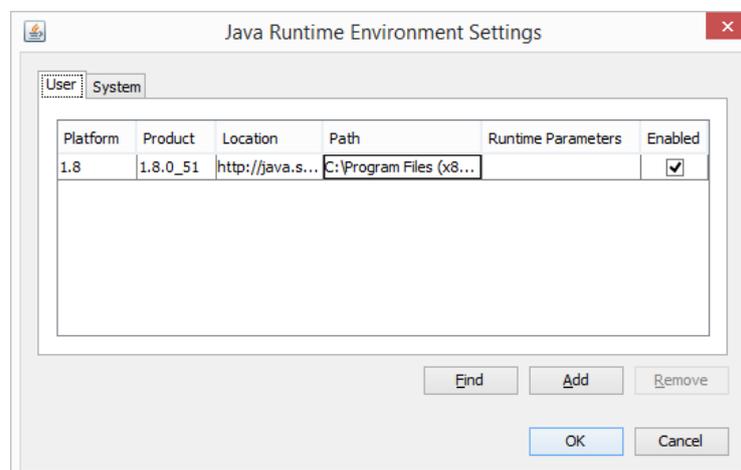


Figure 10-4 Java Runtime Environment Settings

Enter the following text in the "Runtime Parameters" section:

```
-Djava.util.logging.config.file=C:\\logs\\logging.properties
```

You need to confirm the changes in all windows by clicking “OK” button.

The next time JAVA applet version of Web Signer is executed, the diagnostic information should be collected into the “C:\logs\WebSigner.log” file.

11. Known issues

11.1. Application does not start in Safari 12

Beginning with Safari version 12, support has ended for all NPAPI plugins including JAVA plugin required to run Web Signer. Because of that, Web Signer application currently cannot be used in Safari 12 and affected Mac OS X users are advised to use Web Signer application in Mozilla Firefox or Google Chrome browser until the issue is resolved.

11.2. Extension gets disabled in Microsoft Edge

Depending on the exact version of Windows 10 operating system, Microsoft Edge browser may automatically disable “Disig Web Signer 1.0.7” extension. It usually informs the user about this activity on its next startup by displaying information panel in the bottom part of its window.

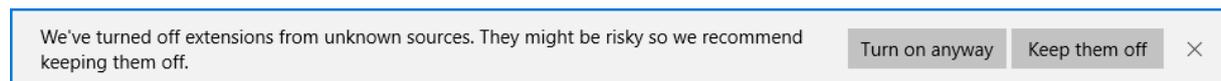


Figure 11-1 Edge disables the extension

Extension can be manually enabled before the signature creation using the browser menu “... > Extensions”.

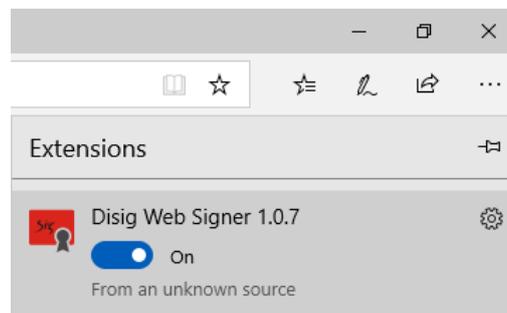


Figure 11-2 Enabling the extension in browser settings

11.3. Error when selecting signing certificate in Safari

Error dialog with phrases “dlopen” and “no suitable image found” present on the first line of the message in the details pane may be displayed during the selection of signing certificate in Safari browser on Mac OS X platform.

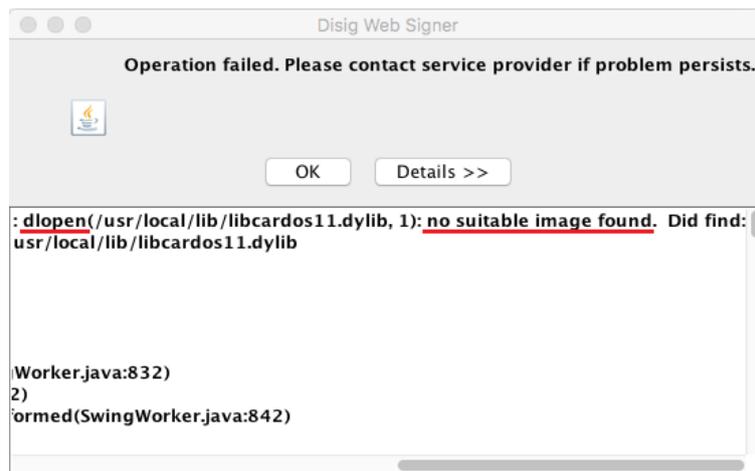


Figure 11-3 Error during the selection of signing certificate

This error usually indicates that additional permissions need to be manually granted to Web Signer so it can access PKCS#11 libraries stored on local disk. This action needs to be performed in the settings of Safari browser which are accessible via “Safari > Preferences” menu.

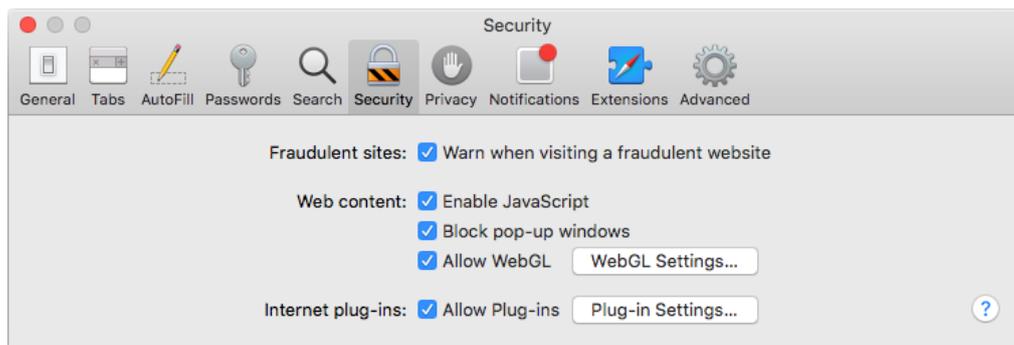


Figure 11-4 Safari Settings

On “Security” tab click “Plug-in Settings...” button.

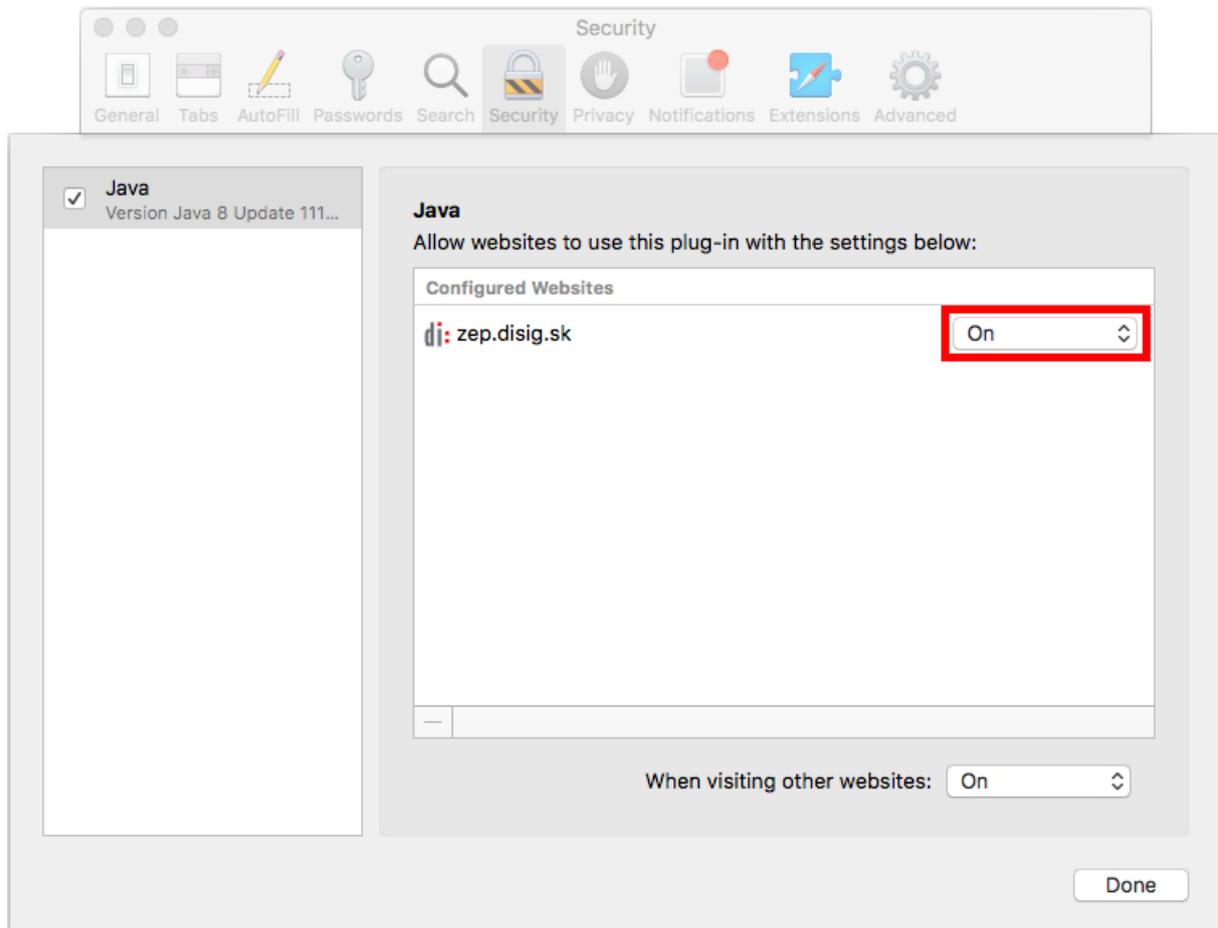


Figure 11-5 Granting permissions

Select “Java” plugin from the list in left pane and then web site working with Web Signer (e.g. zep.disig.sk) from the list in right pane and continue by clicking “On” button with the ALT key pressed.

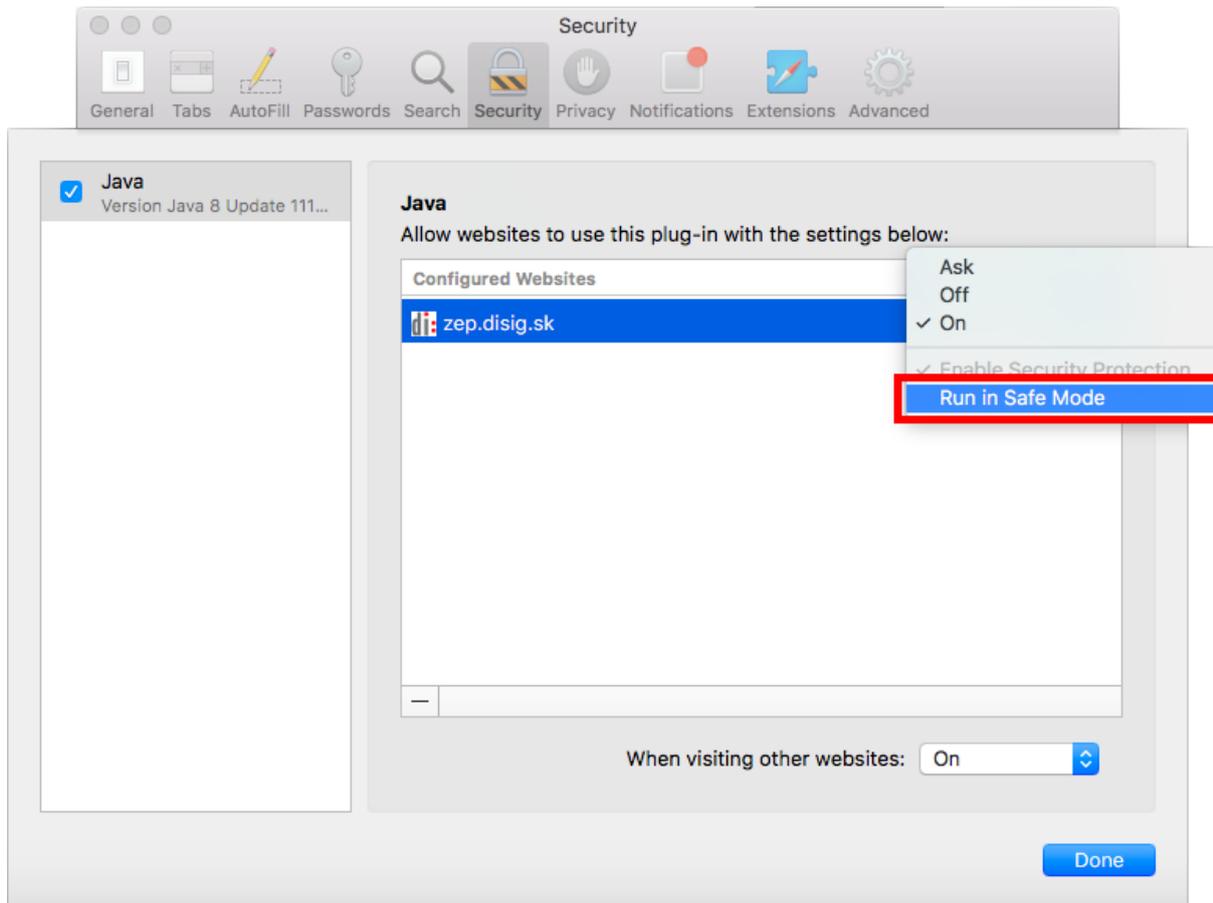


Figure 11-6 Granting permissions to specific website

Uncheck "Run in Safe Mode" option in the displayed menu.

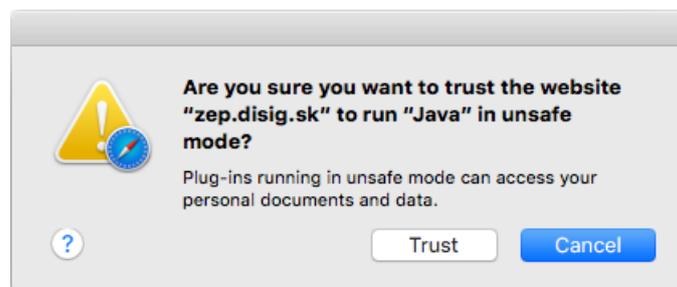


Figure 11-7 Granting permissions to specific website

Confirm the selection by clicking the "Trust" button and save the changes by clicking "Done" button.

12. Technical support

The general terms and conditions for technical support apply to Web Signer application. Additional limitations and/or extensions may be defined in a separate service contract concluded between the application producer and the user.

Recommended procedure for contacting technical support:

- contact technical support via e-mail: **support@disig.sk**
- include the exact description of the problem
- attach screenshot of application and/or error
- include your contact details