SETCCE

User Manual
SETCCE proXSign® component v2.2 for macOS

[New generation of SETCCE proXSign® component]

Document identification:	N/A
Document version:	16
Document authors:	Helena Ostanek
Document status:	/
Document last change date:	08.06.2023

CONTENT AND COPYRIGHT

ProXSign® is a product developed by **SETCCE**. Possession or distribution of **proXSign®** products without a license is illegal. To obtain your license please contact your service provider who uses **proXSign®** component within the service you are using. If you are interested in buying license for integration into your solution, please contact SETCCE.

About SETCCE

SETCCE is the leading regional provider of specialized solutions and services for business process dematerialization. We have pioneered in local as well as in international markets with technologies that deliver trust in e-business and e-government services, and comply with the most demanding legislative requirements.

Working with industries such as telecom, finance, and the governmental sector, SETCCE delivers a range of products and services covering the fields of:

- Electronic invoicing
- Electronic archiving
- Electronic signing
- PKI and information security

Contacts

SETCCE d.o.o.
Tehnološki park 21
SI-1000 Ljubljana
Slovenia
Europe
Web: www.setcce.com

INDEX

1. NEW GENERATION OF SETCCE PROXSIGN® COMPONENT

The SETCCE proXSign® components provide digital signing, encryption/decryption, and time stamping of your documents.

The new generation of SETCCE proXSign® v2 has been developed as a response to the limited plug-in support by the majority of browsers.

SETCCE proXSign® v2 innovative concept provides a solution, which is browser-independent as it works in all popular browsers.

The new SETCCE proXSign® component is installed as a desktop application that runs as a background process. Features like »Autostart« are configurable in the graphical user interface. You can also always check if the component is running.

The advantages of the SETCCE proXSign® v2 are:

- One component for all functionalities (signing of PDF and XML documents, timestamping)

For assistance with installation or use of SETCCE proXSign® v2 please first contact the service provider (i.e. online banking, governmental services, etc.), and then the SETCCE support.

2. SUPPORTED ENVIRONMENT

2.1. Supported environment

macOS	Browser
• Monterey 12 • Ventura 13	• Safari from v14.0.3 • Mozilla Firefox from v91 • Google Chrome; latest stable channel version
Note: For security reasons, use the latest available version of macOS and browsers.	

3. REQUIREMENTS

3.1. Communication port

Browsers communicate with SETCCE proXSign® component over one of the following unused ports:

- 14972
- 41472
- 57214
- 61427

To run SETCCE proXSign® component in your environment, you have to ensure that one of the listed ports is unused.

3.2. Import a personal digital certificate

Your digital certificate has to be installed in the personal certificate store (login keychain) or Mozzila Firefox. Install also root and intermediate digital certificate for your certificate. In case you need help with your digital certificate, please turn to your CA. See chapter 9.

3.3. »SETCCE proXSign« digital certificate

SETCCE proXSign® component provides a higher level of security to its user by encrypting the communication between the component and the browser.

Therefore digital certificate **»SETCCE proXSign«** issued by SETCCE d.o.o. has to be installed on your computer as a trustworthy certificate:

»SETCCE proXSign« digital certificate is dynamically created for each user on the computer (current user) and it is installed at the first launch of the component. It is installed into Keychain and Mozilla Firefox digital certificate store. It is valid for two years from the day it was created.

3.3.1. How to install »SETCCE proXSign« digital certificate

When the SETCCE proXSign® component is successfully installed, the following security warning dialog windows appear (Figure 1). You need to confirm this action and you need to confirm Trust settings (Figure 2) for the component to work.

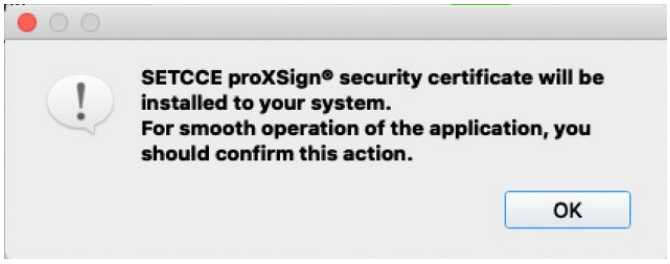

Figure 1: Information window for installing SETCCE proXSign® digital certificate

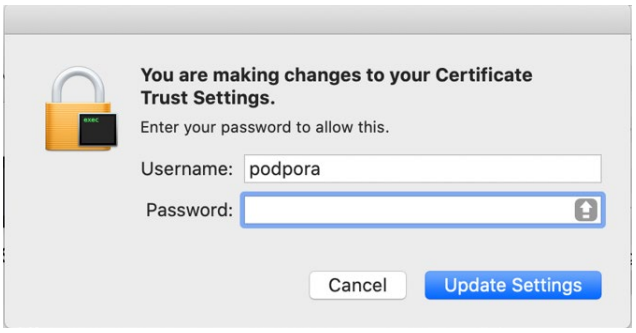

Figure 2: Mac OS dialog window for Trust Settings

»SETCCE proXSign« digital certificate is installed in **Keychains/Login** and **Category/Certificates** as shown in figure 3.

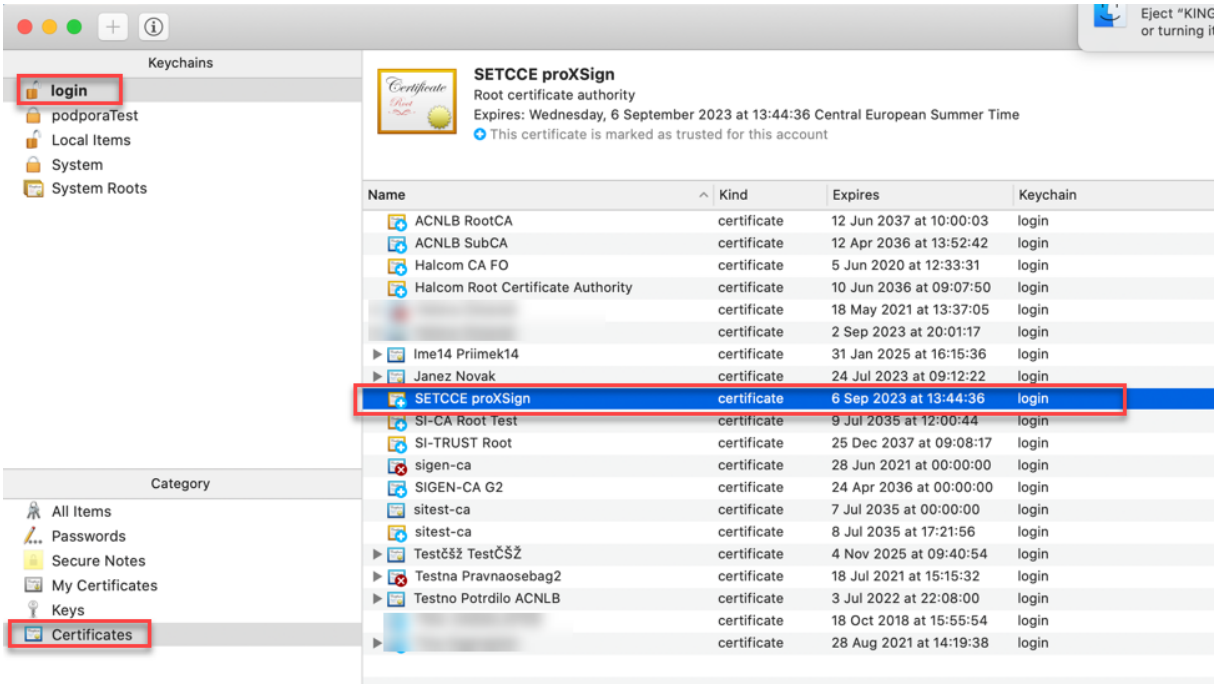

Figure 1: »SETCCE proXSign« digital certificate in Keychains/Login

3.3.2. Auto-renewal of »SETCCE proXSign« digital certificate

Each time the component is started, the SETCCE proXSign® certificate time validity is checked automatically.

Ten days before it expires, or if it is already expired, the warning dialog to delete the old one and install a new one appears; you have to confirm its installation otherwise the component won't work. At the same time, it is installed in the Mozilla Firefox user store (if the browser is installed) but silently, without extra user confirmation.

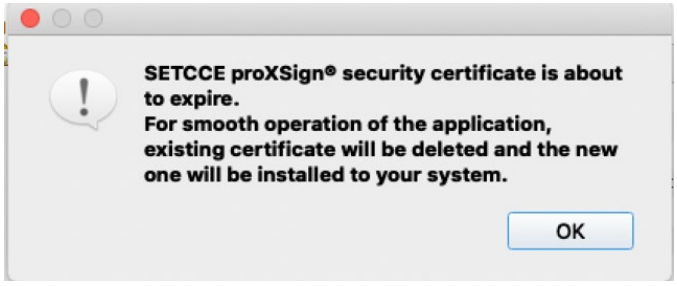

Figure 4: Warning window to install a new digital certificate

3.3.3. How to check if the »SETCCE proXSign« digital certificate is trustworthy

If you are in doubt, that the digital certificate you are installing is not trustworthy and issued by SETCCE, you can check and compare the thumbprint of the **»SETCCE proXSign«** digital certificate from Keychain with one on your file system: `[User]\Library\Application Support\SETCCE\proXSign\PlugoutRoot.crt`. Their thumbprints must match.

Select `Support\SETCCE\proXSign\PlugoutRoot.crt` and press the Space button on your keyboard; the info window with certificate details will pop up.

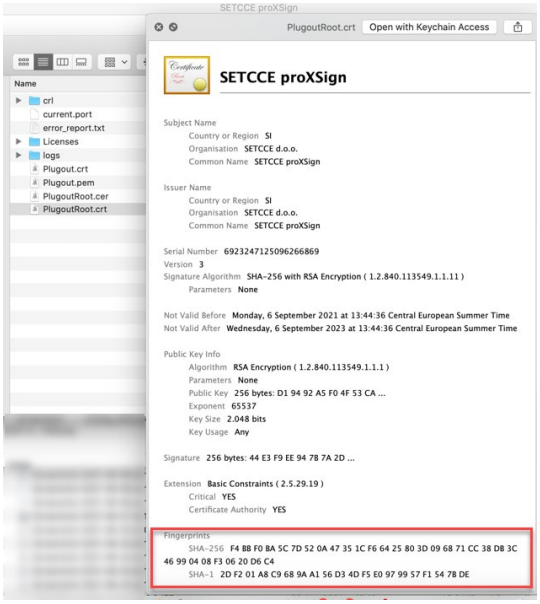

Figure 5: Example of SETCCE proXSign digital certificate on the file system

And compare it with the one, installed into your keychain. Thumbprints must match.

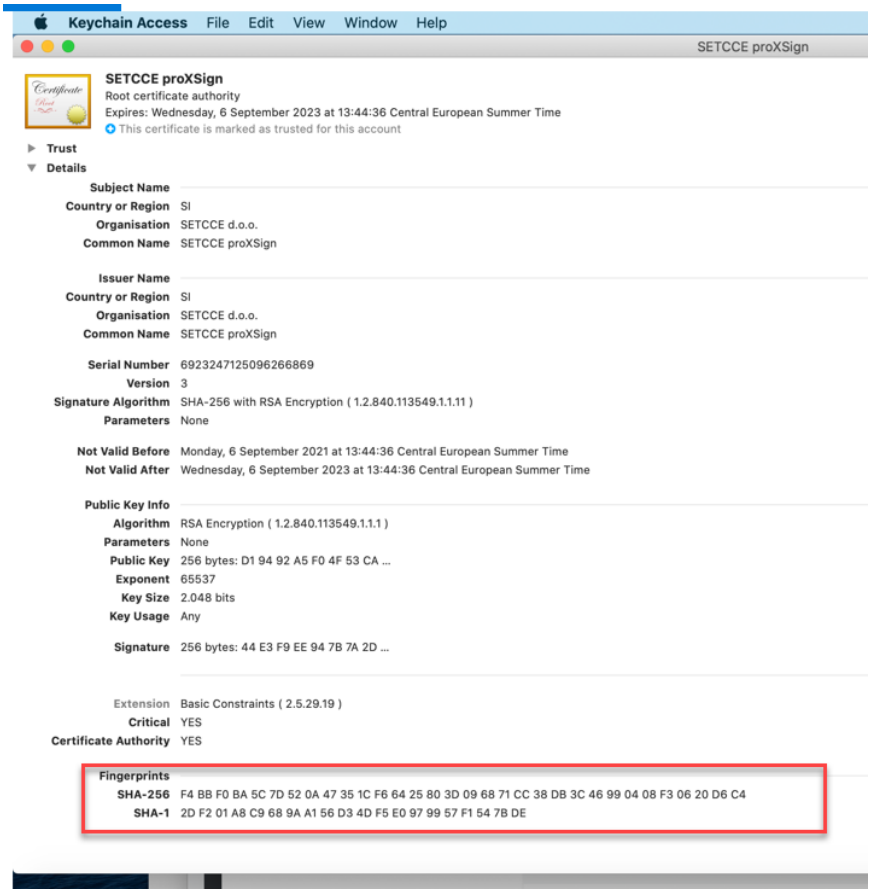

Figure 6: Thumbprint of »SETCCE proXSign« digital certificate

4. INSTALLATION

SETCCE proXSign® component is installed as a desktop application that runs as a background process. The feature »Autostart« is configurable in SETCCE proXSign® graphical user interface. You can also check if the SETCCE proXSign® component is running.

The setup package is called »SETCCE_proXSign_<*version*>.pkg«. Since the setup package is not signed and downloaded from the Mac App Store you have to enable/allow installation in the security settings.

You will need administrative privileges to install the SETCCE proxsign® component.

4.1. Install SETCCE proXSign® component

To install the component, perform the steps as follows:

1. Log in as a user with administrative privileges.
2. Go to »System Preferences«, »Security & Privacy« and choose the option »Mac App Store and identified developers« as shown in Figure 7.

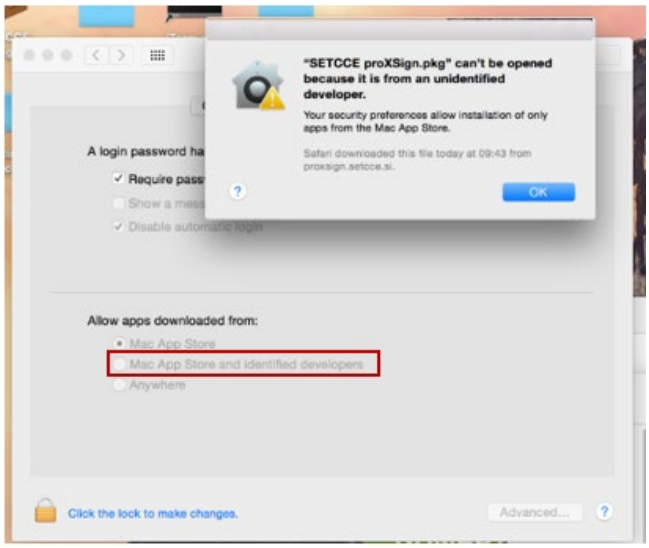

Figure 7: Security settings in »System Preferences« / »Security & Privacy«

3. Download the setup package »SETCCE_proXSign_<*version*>.pkg«.
4. Double click on »SETCCE_proXSign_<*version*>.pkg« and follow the setup instructions. The component will be installed into the »Applications« folder by default. You can choose any other folder during the installation process.

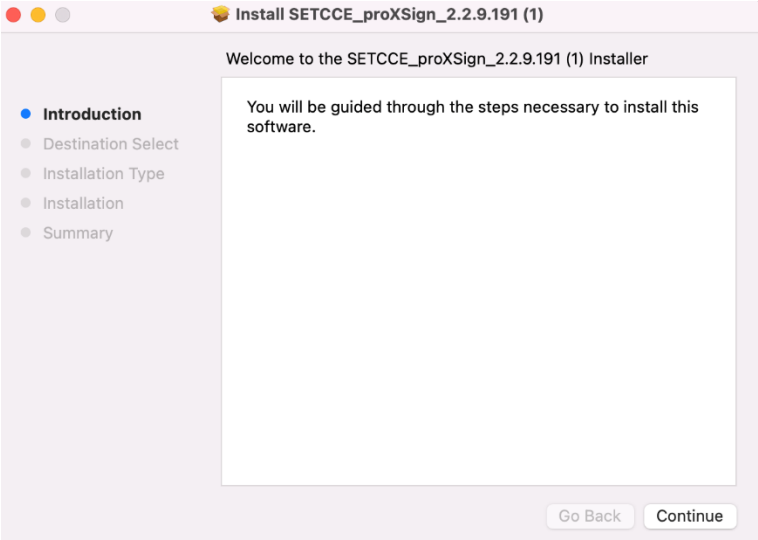

Figure 8: Installation process

Important:
When the installation is finished, the SETCCE digital certificate is installed. You need to confirm all steps during installation, otherwise, the component won't work. See chapter 3.3.

After the successful installation, the SETCCE proXSign® icon appears in the Status menu. By double-clicking on ikon, the main proXSign window opens, with all your digital certificates from Keychain and/or Mozilla Firefox.

Figure 9: SETCCE proXSign icon in the Status menu

5. REMOVING SETCCE PROXSIGN® COMPONENT

To be able to remove SETCCE proXSign® component from your computer you have to:

1. Log in to your user account as an administrator**.**
2. Find and remove SETCCE proXSign.app and remove »SETCCE proXSign« digital certificate from login keychain and Mozilla Firefox certificate store.

proXSign.app is installed into the Applications folders by default.

6. START SETCCE PROXSIGN® COMPONENT

6.1. Start

The component can be launched as follows:

1. Find **SETCCE proXSign.app** in the »**Applications**« or on any other location where you installed it during the installation process.

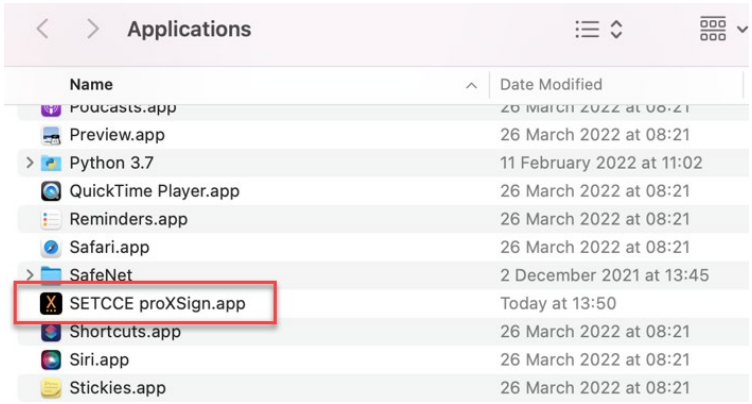

Figure 10: Run SETCCE proXSign.app from »Applications«

2. Double click on »**SETCCE proXSign.app**« and the component will run. The main window "Certificates" will open. See figure 13.
3. Run »**Launchpad**« and find the **SETCCE proXSign icon**. Double click on the icon and the component will run.

Figure 11: SETCCE proXSign icon in »Launchpad«

Check for icon proXSign in the Status menu. If the component SETCCE proXSign® is already running, the icon proXSign is shown in the Status menu.

Figure 12: SETCCE proXSign icon in the status menu

6.2. Autostart

See chapter 7.2.1.

7. SETCCE PROXSING® GRAPHICAL USER INTERFACE OVERVIEW AND SETTINGS

By double-clicking on the proXSign icon in the Status menu (Figure 12), the main proxsign® window will open, with the list of all your digital certificates (Figure 13).

7.1. Main graphical user interface and Certificates section

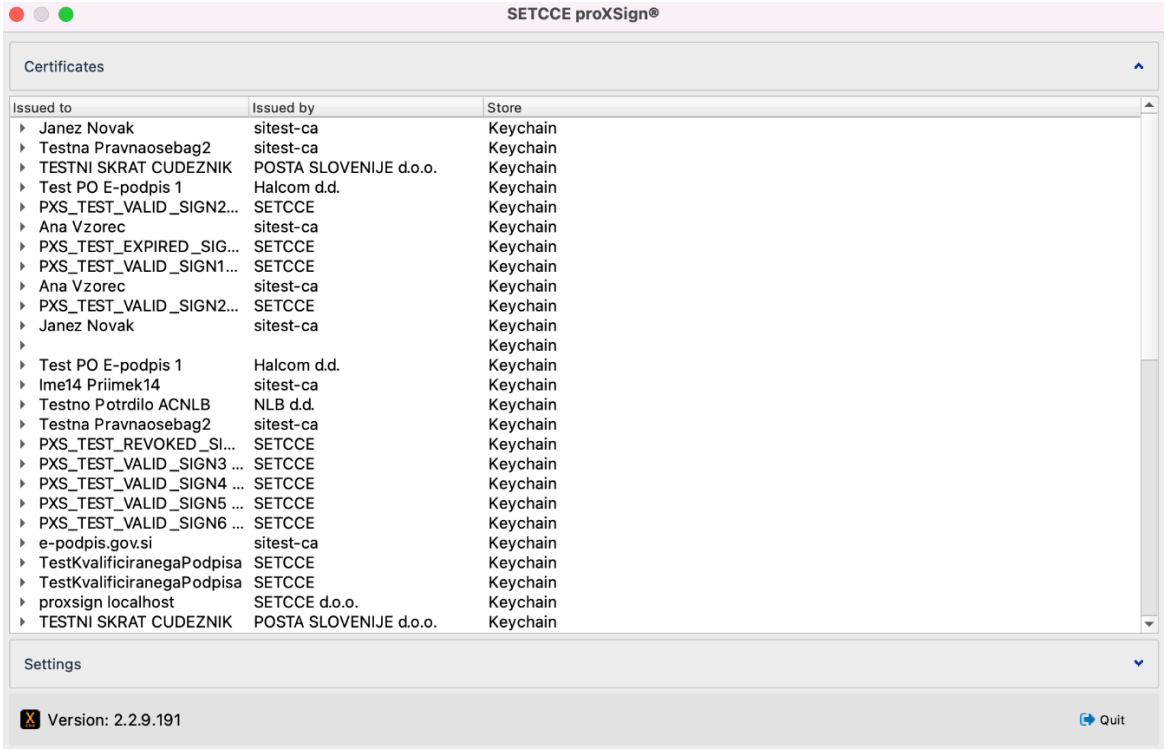

Figure 13: Main proXSign® GUI with a list of Certificates

Columns in proXSign® main GUI represents:

- **Issued to:** Common Name (CN) of your digital certificate
- **Issued by:** Issuer of your digital certificate
- **Store:** certificate store where your certificate is installed (Windows or Firefox)

Optional:

- **Chain Validity:** Chain validity of your digital certificate (the status if the digital certificate is revoked is not checked (CRL check)).

  When Chain Validity status is »Not OK«, the digital signature with such digital certificate won't pass. The reason can lay in the expired digital certificate (or one of them in the chain is not time valid), or the certificate chain is not complete, or if one of the certificates in the chain is not Trusted (In the case of Mozzila Firefox certificate store) ….

This column is visible only if you set the appropriate parameter in the `proxsign.ini` file. You will need administrator privileges.

Steps:

1. Quit form proXSign®
2. Open file `[C:\Program Files (x86)]\SETCCE\proXSign\etc\proxsign.ini`
3. Change value
   `check_all_chains=false`
   on
   `check_all_chains=true`
4. Save changes
5. Start SETCCE proXSign®

Example form proxsign.ini when check validity is enabled:

```
[common]
update_url=http://public.setcce.si/proxsign/update/SETCCE_proXSign_update.exe
version_url=http://public.setcce.si/proxsign/update/version
check_all_chains=true
; use_CNG : no, yes, prefer, only
use_CNG = no
```

Note:
In case the proXSign® is launched very slowly on your computer, you please disable Check Validity.

7.2. Settings

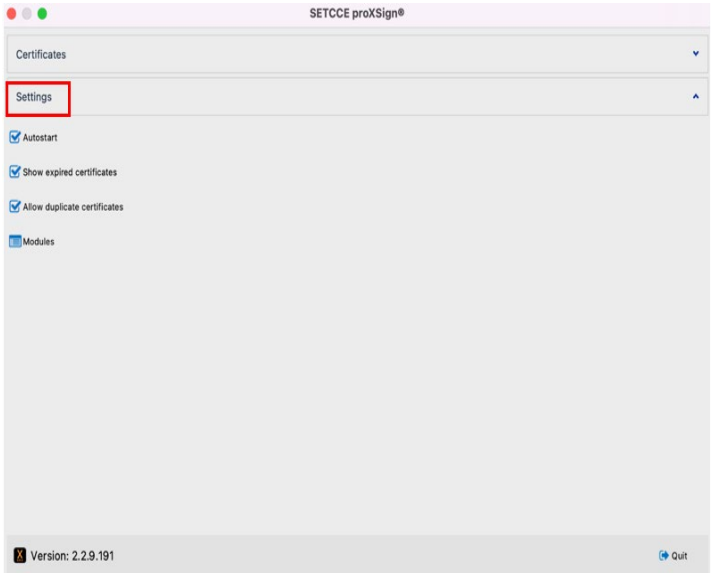

Figure 14: Settings in proXSign® component

7.2.1. Autostart

The SETCCE proXSign® component supports autostart functionality. If the »Autostart« option is configured, the component is launched when you log in.

The SETCCE proXSign® component supports autostart functionality. If the »Autostart« setting is configured, the component runs when you log in.

Setting »Autostart« is enabled by default.

7.2.2. Show expired certificates

Expired digital certificates are displayed only in the main proXSign GUI, but the digital signature with expired certificates is disabled by default.

Setting »Show Expired certificates« is disabled by default.

7.2.3. Allow duplicate certificates

In case your digital certificate is installed into the Windows certificate store and in Mozzila Firefox browser, then proXSign® displays the same certificate from both stores, and digital signature is enabled with both certificates.

The setting »Allow duplicate certificates« is disabled by default.

7.2.4. Modules

Modules setting enables proXSign® to use pkcs#11 modules/libraries for digital signing with digital certificates issued on QSCD (smart cards and smart USB). Currently, only digital certificate posta®CA is tested and supported.

Example:
The location of pkcs#11 in Thales Safenet Authentication Client 10.2 (10.2.97.0):
`/usr/local/lib/`**`libeTPkcs11.dylib`**

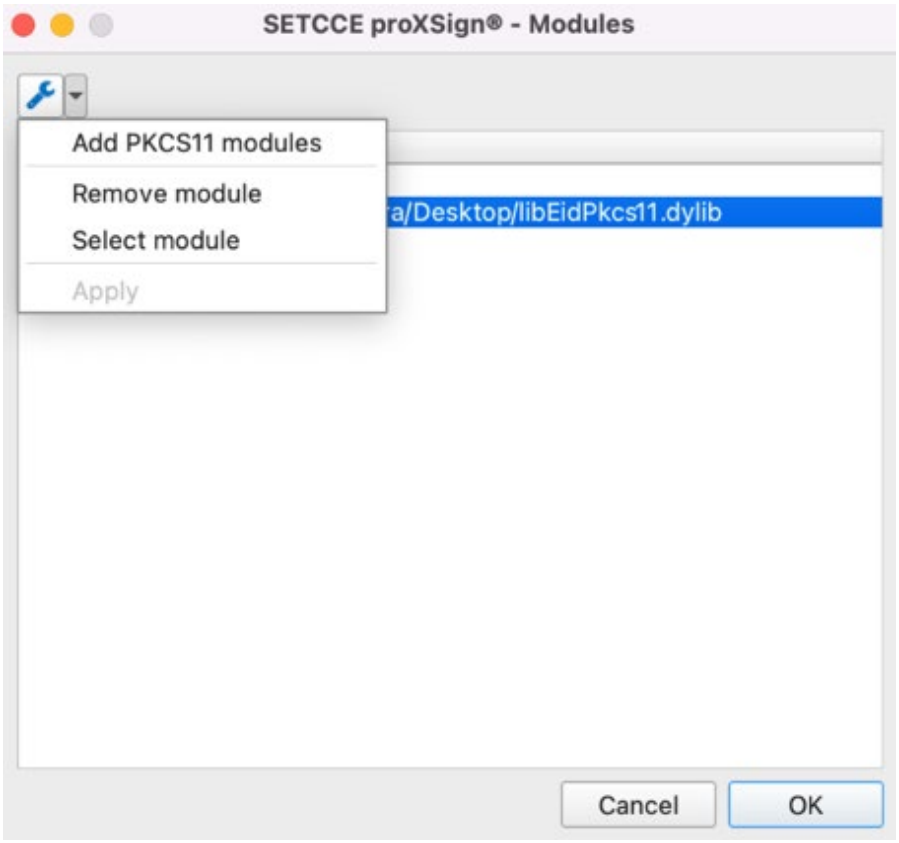

Figure 15: Settings up pkcs#11 module for posta®CA

8. QUIT (STOP) SETCCE PROXSIGN® COMPONENT

We suggest running SETCCE proXSign® component as a background process. In this case, the component itself does not perform any activity.

You can **stop** the SETCCE proXSign® component (kill the process) as follows:

1. Click on the »Quit«  button in SETCCE proXSign® component main window.

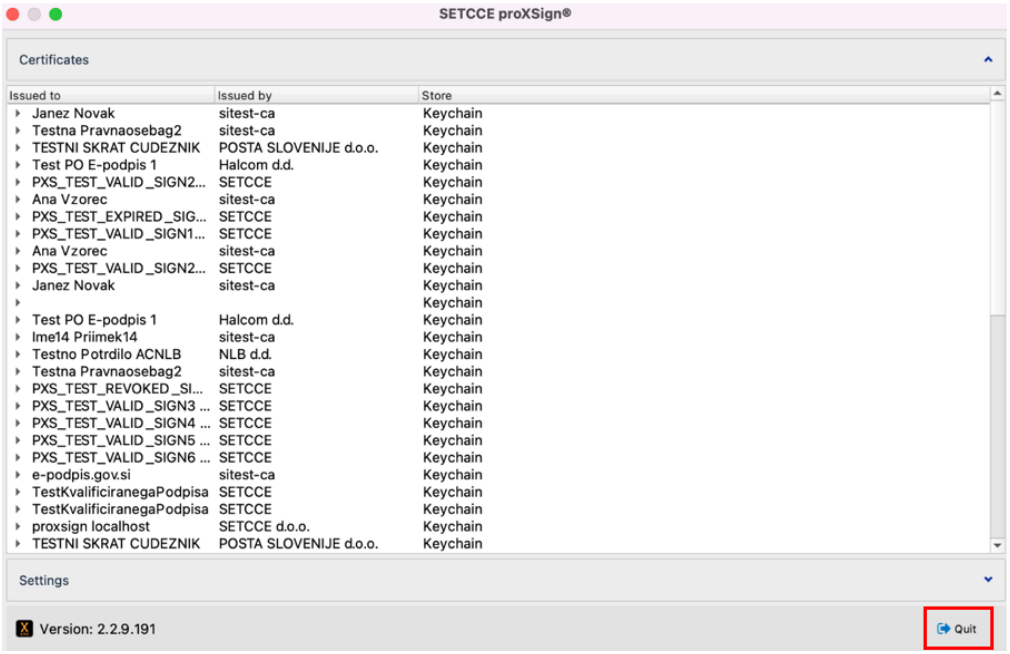

Figure 16: Button »Quit«

2. Click on the **SETCCE proXSign icon** in the **status** menu and choose »**Quit**«.

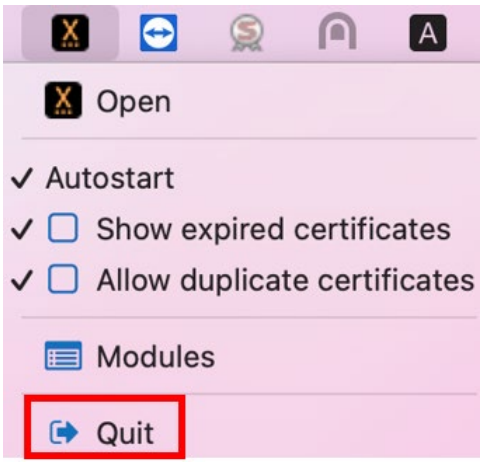

Figure 17: Quit button on the status menu

If you want to hide or minimize the SETCCE proXSign user interface, then click on  in the left corner of the main window of the component. In this case, the SETCCE proXSign® component is still running in the background**.**

9. INSTALLING A PERSONAL DIGITAL CERTIFICATE

9.1. Is your digital certificate installed on your computer?

To use SETCCE proXSign® component on your computer, your digital certificate has to be installed in a digital certificate store (Keychain Login or Mozilla Firefox store).

9.1.1. Installation steps for Keychain

To install your digital certificates perform steps as follows:

1. Run **Keychain Access** application (Spotlight->Keychain Access)
2. Choose **File->Import Items** and select your digital certificate from the file system. In »**Destination Keychain**« choose »**Login**« as shown in Figure 18. Your digital certificate is installed in your (User) Keychain. Along with your personal digital certificate, the root and intermediate digital certificate will be installed automatically, also in your (User) keychain, therefore it can be used only within your user account. For more info about root and intermediate certificates see chapter 20.

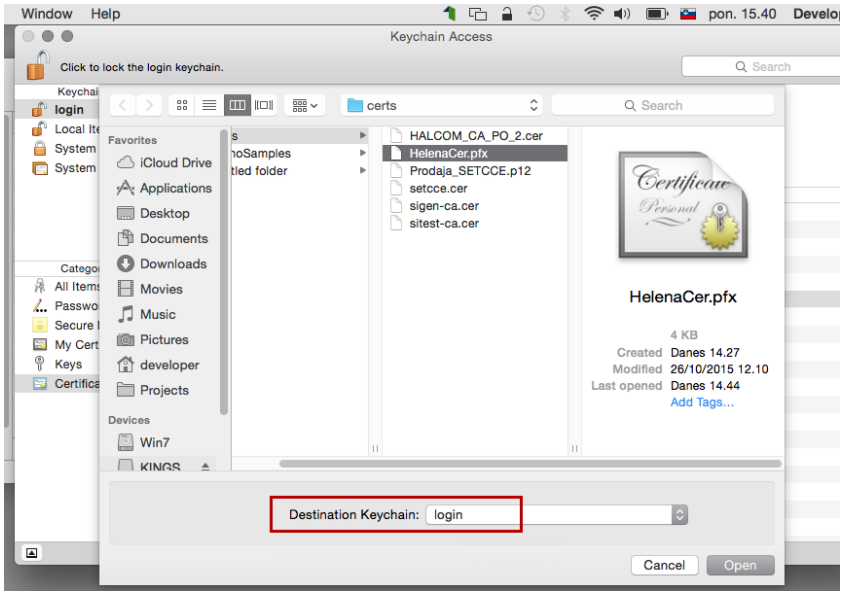

Figure 18: Installing personal digital certificate

With this procedure, both digital certificates will be installed in **Keychains/Login** and **Category/Certificates**. Your personal digital certificate will also be installed in **Category/My Certificates**.

Important:

1. The root digital certificate is not installed as trustworthy by default, therefore you have to set "Trust" properties as described in chapter 9.2.2.
2. Described installation steps stand for Yosemite and personal digital certificates which can be saved on a hard drive.

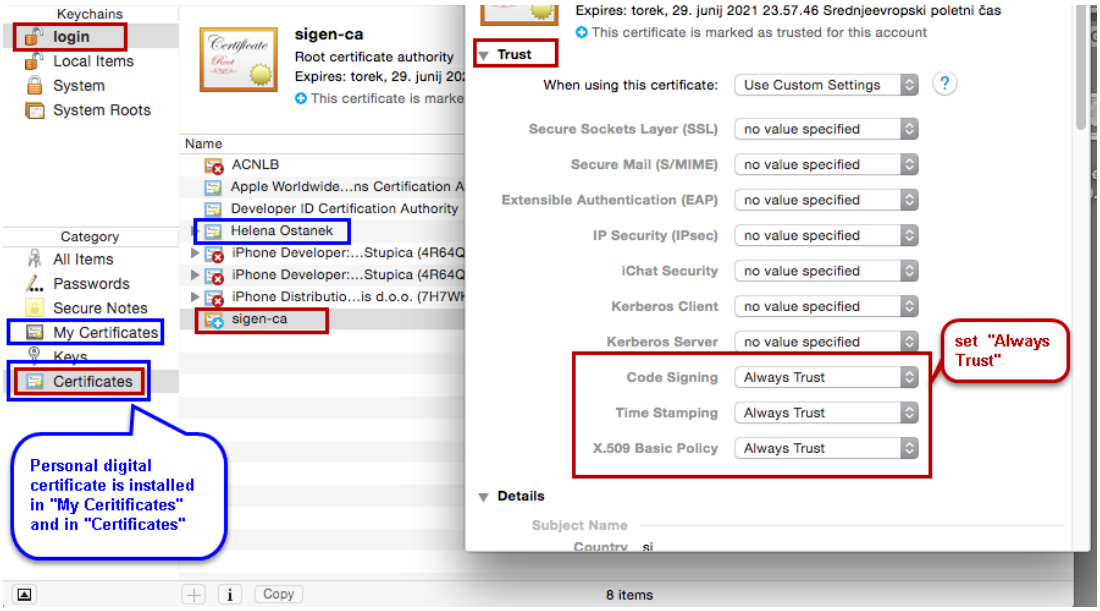

Figure 19: Personal digital certificate in Login (user) Keychain along with root digital certificate

9.2. Are your root and intermediate certificate installed on your computer?

To use SETCCE proXSign® component, you have to install a root and intermediate certificate of Certification Authority which issued your personal digital certificate.

9.2.1. Installation steps

Root and intermediate digital certificates can be installed (at least) in two ways:

1. **Automatically**, along with your personal digital certificate. In this case, it is installed in Keychains/Login and Category/Certificates and it can be used only within your user account.
2. **With standard procedure (use Keychain Access)**. We suggested installing it into the system keychain. In this case, all users on your computer can use/access root certificates for digital signing**.**

Installation steps for the standard procedure (root digital certificate in System Keychain):

1. Log in as a user with administrator privileges.
2. Download your root digital certificate and save it to your computer.
3. Run **Keychain Access** application (Spotlight->Keychain Access).
4. Select **File**->**Import Items** and chose a root digital certificate from the file system on your computer. From the drop-down menu »**Destination Keychain**« choose »**System**«. Your root digital certificate will be installed in the System Keychain, therefore it can be used for signing for all users (user accounts) on your computer.
5. Set up "Trust" properties (see chapter 9.2.2).

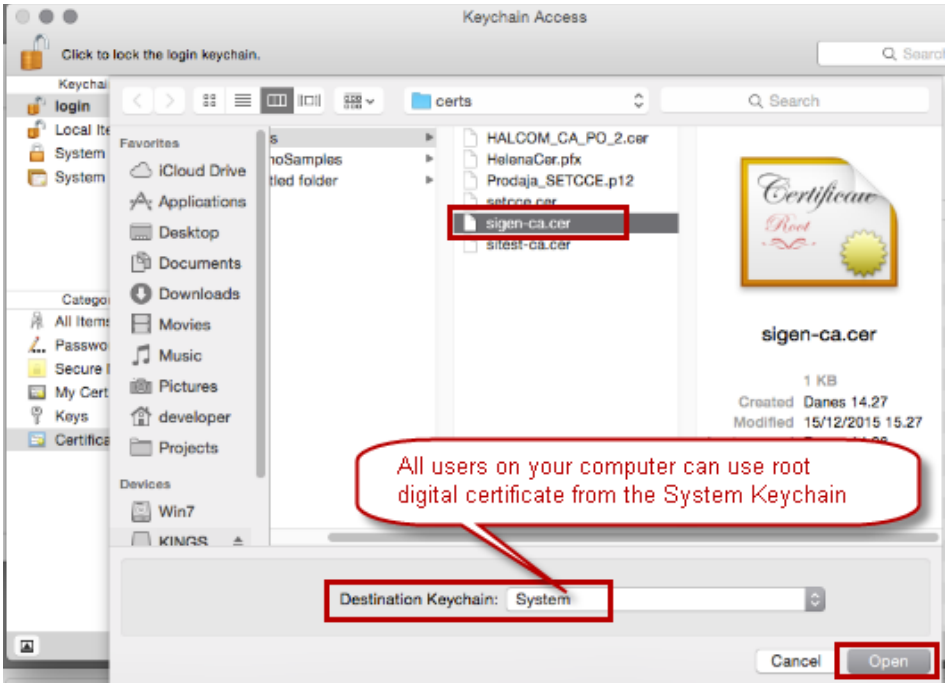

Figure 20: Installing root digital certificate in the System Keychain

9.2.2. Trust properties settings

If the Root and Intermediate digital certificate is not installed as trustworthy, you have to set properties additionally. Follow the steps below:

1. Double click on root and intermediate digital certificate and the window with certificate properties open.
2. Select "Trust" and set at least the last three options as „**Always Trust**".
3. Close window with click on standard x.
4. Confirm the changes with the administrator username and password.

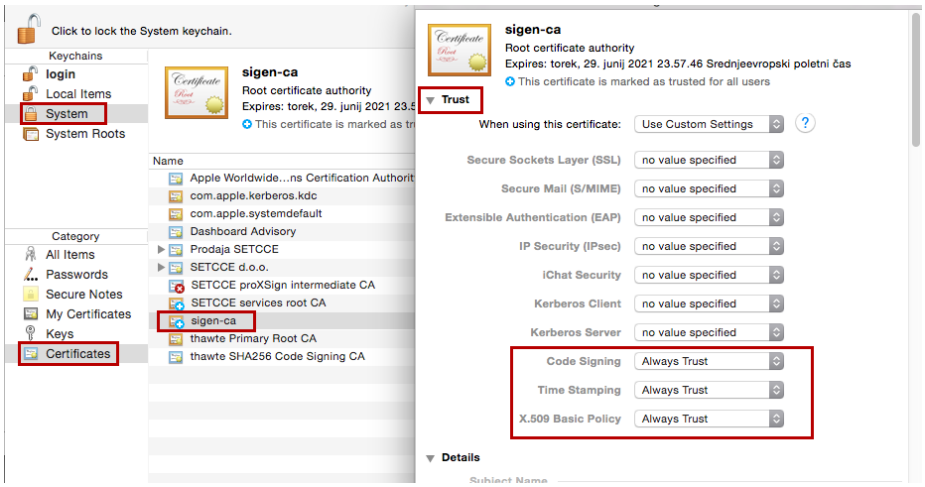

Figure 21: Installing a root digital certificate in the System Keychain and setting up "Trust" properties

9.3. Installation steps for Mozilla Firefox store

Steps to install your personal digital certificate in Mozilla Firefox store by Mozilla Firefox:

1. Save your digital certificate on your computer.
2. Open Mozilla Firefox and go to Options/Advanced/View Certificates/Your Certificates.
3. Then click »Import« and select your certificate. Enter the password in the dialog window and click »**OK**«.
4. Your digital certificate is installed in the Mozilla Firefox certificate store, among Personal certificates, as shown in Figure 22.

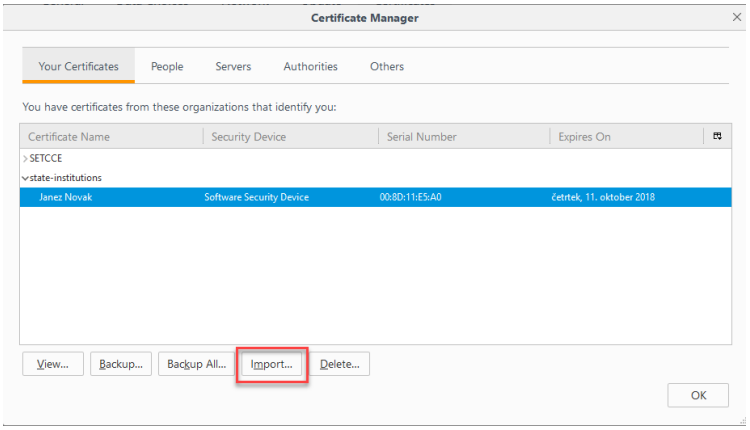

Figure 22: Digital certificate »Janez Novak« among Personal certificates in Mozilla Firefox.

In the Mozilla Firefox certificate store, you have to install the root digital certificate into »Authorities«, as shown in Figure 23.

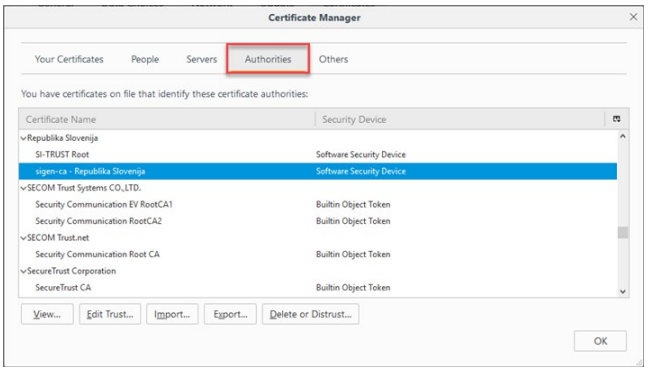

Figure 23: Root certificate »Sigen-ca« in »Authorities« in the Mozilla Firefox store.

Important:

1. If you want to install the **Mozilla Firefox** browser on your computer, after the SETCCE proXSign® component has already been installed and running, **you have to restart the component**. The restart of the SETCCE proXSign® component **installs** the »SETCCE proXSign« certificate into the Firefox certificate store. To refresh digital certificate data in the **Mozilla Firefox** browser, you must restart the browser.
2. If you **install and run the SETCCE proXSign® component using the Mozilla Firefox browser**, you have to **restart the browser** after a successful installation.