

SETCCE

**User Manual
SETCCE proXSign® component v2.0.11 for MAC OS X**

[New generation of SETCCE proXSign® component]



Document identification: N/A
Document version: 8
Document authors: Helena Ostanek, Anja Rožac
Document status: Confidential
Document last change date: 17.11.2016

CONTENT AND COPYRIGHT

proXSign® is a product developed by **SETCCE**. Possession or distribution of **proXSign®** product 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.

The content of this document is copyrighted entirely by SETCCE. No distribution or copying is allowed without permission of SETCCE. SETCCE, SETCCE logos and SETCCE product names are registered trademarks by SETCCE. Copying and usage of logos and product names are not allowed prior to SETCCE approval.

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.si

INDEX

1. New generation of SETCCE proXSign® component	3
2. Supported environment.....	4
2.1. Supported environment	4
3. Prerequisites.....	5
3.1. Communication port.....	5
3.2. Import a personal digital certificate	5
3.3. »SETCCE services root CA« and »SETCCE proXSign intermediate CA« digital certificates	5
3.3.1. How to install SETCCE digital certificates	5
4. Installation and upgrade.....	9
4.1. Install SETCCE proXSign® component.....	9
4.1.1. Installation steps	9
4.2. Autoapdate of SETCCE proXSign® component	10
4.3. Check for updates	10
5. Quit and RESTART SETCCE proXSign® component.....	11
5.1. Start SETCCE proXSign® component.....	11
5.2. Autostart SETCCE proXSign® component.....	12
5.3. Quit (Stop) SETCCE proXSign® component	12
6. Removing SETCCE proXSign® component	14
7. Installing a digital certificate	15
7.1. Is your personal digital certificate installed on your computer?	15
7.1.1. Installation steps	15
7.2. Is your root certificate installed on your computer?.....	16
7.2.1. Installation steps	16
7.2.2. Trust properties settings	17

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® v 2.0.0 has been developed as a response to the limited plug-in support by the majority of browsers.

SETCCE proXSign v 2.0.0 innovative concept provides solution, which is browser independent as it works in all popular browsers.

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

The advantages of the SETCCE proXSign v 2.0.0 are:

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

For assistance with installation or use of SETCCE proXSign v 2.0.0 please first contact the service provider (i.e. on-line banking, governmental services etc.), and then the SETCCE support.

2. SUPPORTED ENVIRONMENT

2.1. Supported environment

Operating system (OS)	Browser
MAC OS X - Yosemite 10.10 - El Capitan 10.11	 Safari 9.0.1 in 9.0.3
macOS Sierra 10.12	 Safari 10.0.1

3. PREREQUIREMENTS

3.1. Communication port

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

- 14972
- 41472
- 57214
- 61427

In order to run SETCCE proXSign® component in your environment you have to ensure that one of the listed ports are unused.

3.2. Import a personal digital certificate

Your personal digital certificate has to be installed in personal certificate store (login keychain). See chapter 7.

3.3. »SETCCE services root CA« and »SETCCE proXSign intermediate CA« digital certificates

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

Therefore two digital certificates issued by SETCCE d.o.o. has to be installed on your computer as a trustworthy certificate:

- **SETCCE services root CA** and
- **SETCCE proXSign intermediate CA**,

hereinafter referred to as **SETCCE digital certificates**.

3.3.1. How to install SETCCE digital certificates

Both digital certificates are automatically installed into system certificate store (System keychain) when the SETCCE proXSign® component is launched for the first time.

Both SETCCE digital certificates are installed in **Keychains/System** and **Category/Certificates** as shown on figure 1.

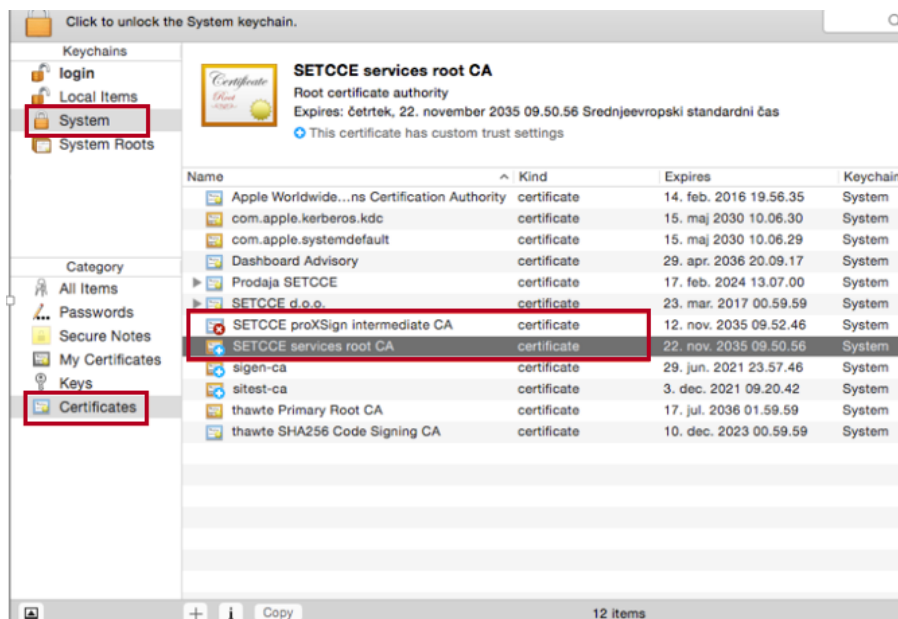


Figure 1: SETCCE digital certificates in System Keychain

You can check thumbprints of »**SETCCE services root CA**« and »**SETCCE proXSign intermediate CA**« digital certificates in digital certificate details view. Thumbprint of »**SETCCE services root CA**« must match Thumbprint on Figure 2 and thumbprint of »**SETCCE proXSign intermediate CA**« must match Thumbprint on Figure 3.

SETCCE services root CA	
Organization	SETCCE d.o.o.
Common Name	SETCCE services root CA
Issuer Name	
Country	SI
State/Province	Slovenia
Organization	SETCCE d.o.o.
Common Name	SETCCE services root CA
Serial Number	00 96 94 B6 D3 A3 54 3E 58
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Tuesday 17 November 2015 09 h 50 min 56 s Central European Standard Time
Not Valid After	Thursday 22 November 2035 09 h 50 min 56 s Central European Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	512 bytes : EE 15 43 5B 7D 6F 9C D4 ...
Exponent	65537
Key Size	4096 bits
Key Usage	Verify
Signature	512 bytes : 61 F3 47 3A E5 1F 4D D1 ...
Extension Key Usage (2.5.29.15)	
Critical	YES
Usage	Digital Signature, Key Cert Sign, CRL Sign
Extension Basic Constraints (2.5.29.19)	
Critical	YES
Certificate Authority	YES
Extension Subject Key Identifier (2.5.29.14)	
Critical	NO
Key ID	11 3F A4 67 11 AC D1 1F D3 6A 5B 7B CF 5E B0 7A BA 60 E8 41
Extension Authority Key Identifier (2.5.29.35)	
Critical	NO
Key ID	11 3F A4 67 11 AC D1 1F D3 6A 5B 7B CF 5E B0 7A BA 60 E8 41
Fingerprints	
SHA1	D0 64 E2 3F 30 2C CE BD 50 39 FF 51 31 25 BB AC 85 39 B7 84
MD5	46 7D D1 BD E2 64 F9 8B 86 42 C1 C6 67 B7 AA 20

Figure 2: thumbprint of »SETCCE services root CA« digital certificate

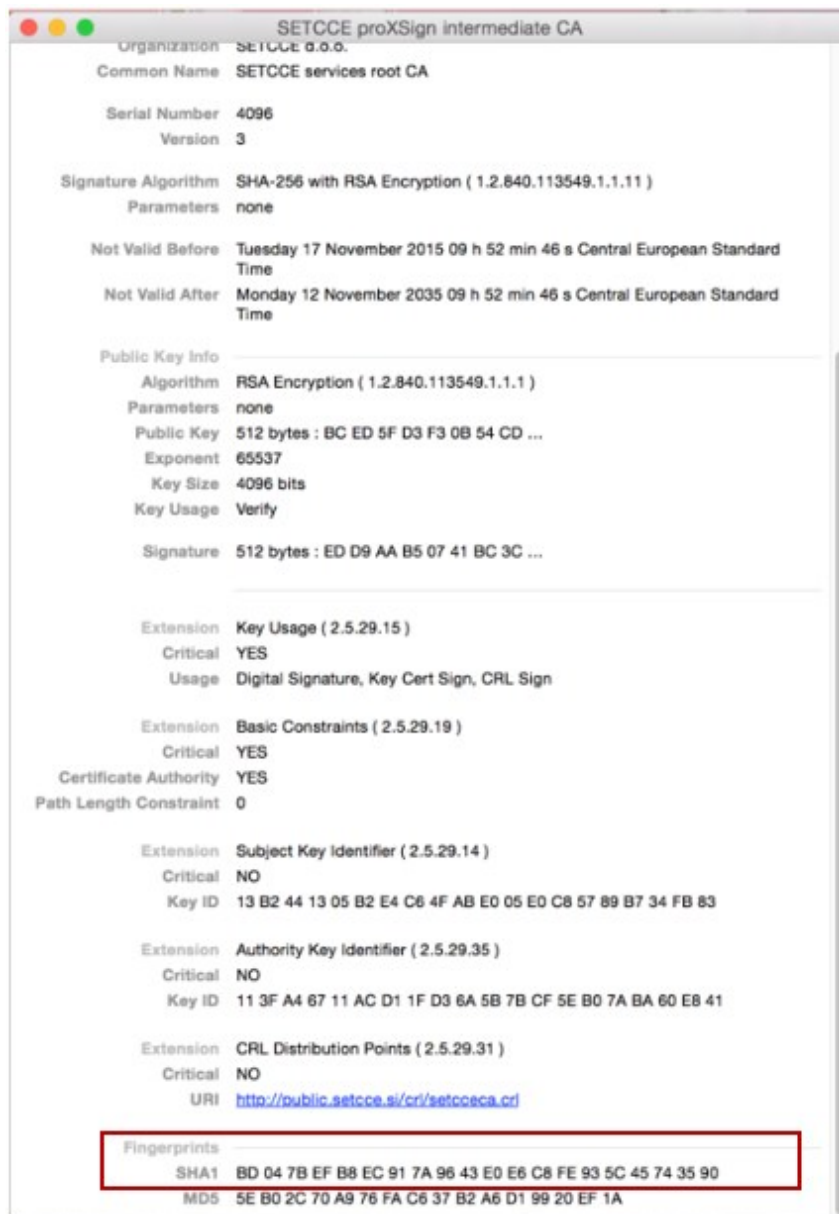


Figure 3: thumbprint of »SETCCE proXSign intermediate CA« digital certificate

4. INSTALLATION AND UPGRADE

SETCCE proXSign® component is installed as a desktop application which 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.

4.1. Install SETCCE proXSign® component

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

Go to »System Preferences«, »Security & Privacy« and choose option »Mac App Store and identified developers« as shown on Figure 4.

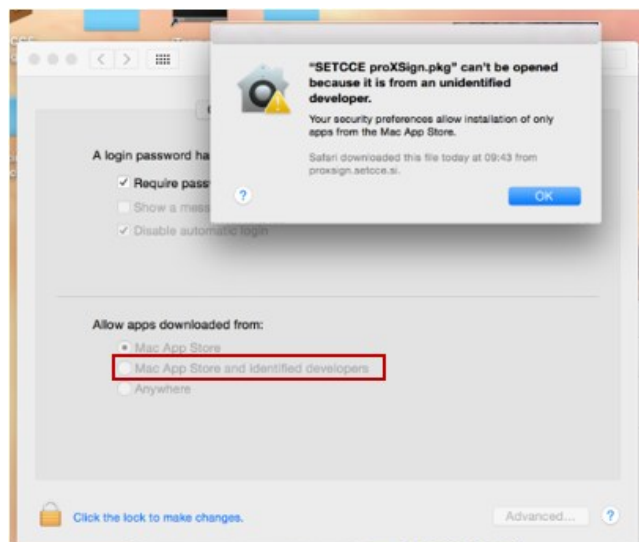


Figure 4: security settings in »System Preferences« / »Security & Privacy«

Only user with administrative privileges can install SETCCE proXSign® component.

4.1.1. Installation steps

To install the component perform the steps as follows:

1. Log in as user with administrative privileges.
2. Download the setup package »SETCCE_proXSign.pkg«.
3. Double click on »SETCCE_proXSign.pkg« and follow the setup instructions. The component will be installed into »Applications« folder by default. You can choose any other folder during the installation process.

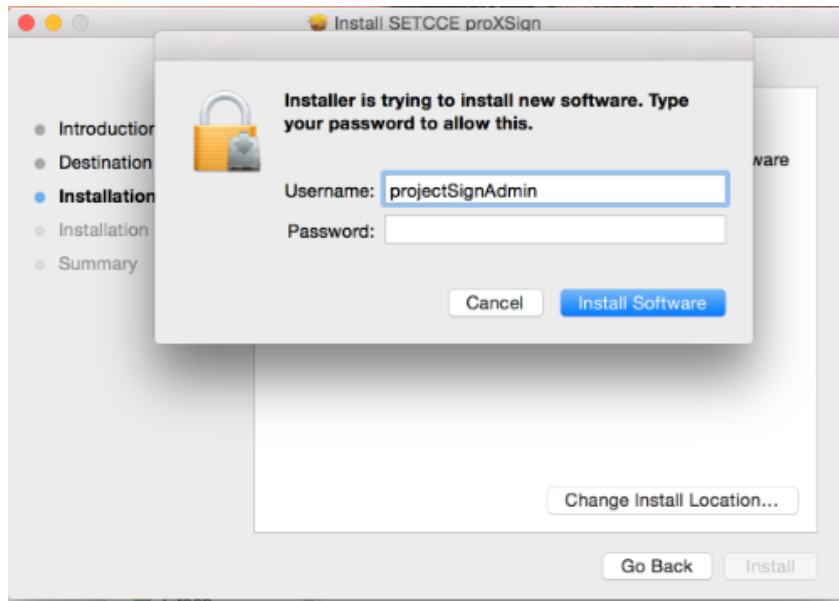


Figure 5: installation process

4. After successful installation you have to run the SETCCE proXSign® component. See chapter 5.1.

Important:

1. Before you upgrade/reinstall the component, you have to stop the component first (»Quit«). See chapter 5.3.

4.2. Autoapdate of SETCCE proXSign® component

Feature called »Autoupdate« is not supported yet.

4.3. Check for updates

Feature called »Check for updates« is not supported yet.

5. QUIT AND RESTART SETCCE PROXSIGN® COMPONENT

5.1. Start SETCCE proXSign® component

The component can be run as follows:

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

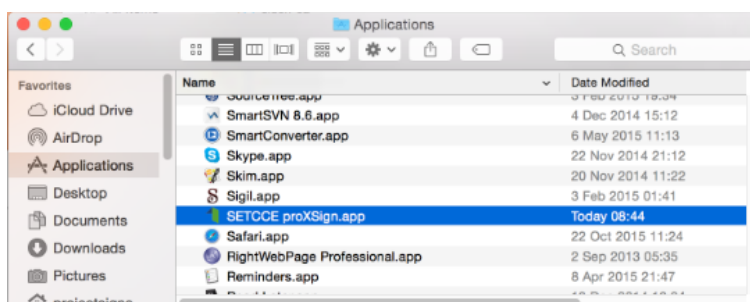


Figure 6: Run SETCCE proXSign.app from »Applications«

2. Double click on »**SETCCE proXSign.app**« and the component will run.

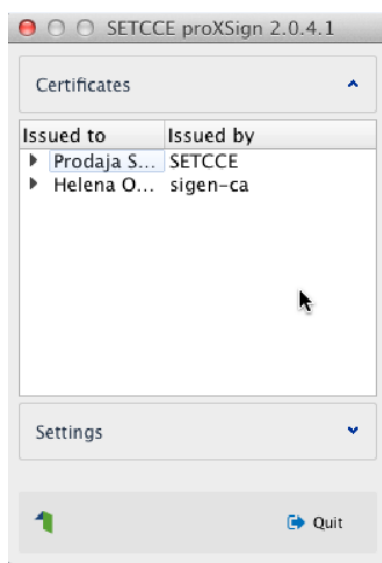


Figure 7: SETCCE proXSign® component main window

3. Run »**Launchpad**« and find the **SETCCE proXSign icon**. Double click on icon and the component will run.



Figure 8: SETCCE proXSign icon in »Launchpad«

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

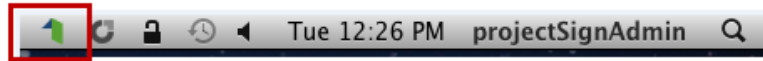


Figure 9: SETCCE proXSign icon in Status menu

5.2. Autostart SETCCE proXSign® component

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

»Autostart« can be configured as follows:

1. In the **Status menu**, click on proXSign icon and choose »Autostart«
2. Click on »Settings« in the main **proXSign** window than choose option »Autostart«.

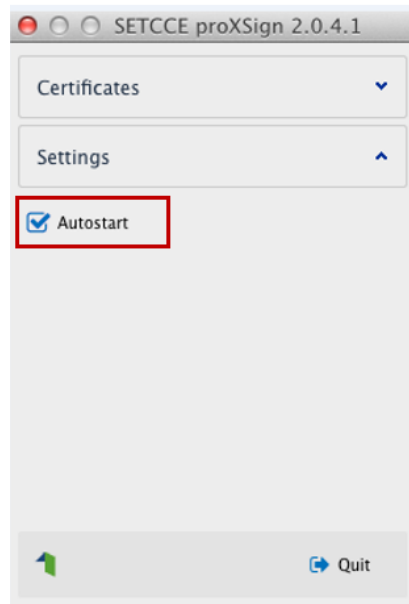


Figure 10: Option »Autostart«

Option »Autostart« is disabled by default.

5.3. Quit (Stop) SETCCE proXSign® component

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

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

1. Click on »Quit«  button in SETCCE proXSign® component main window.
See Chapter 5.1 for restart.

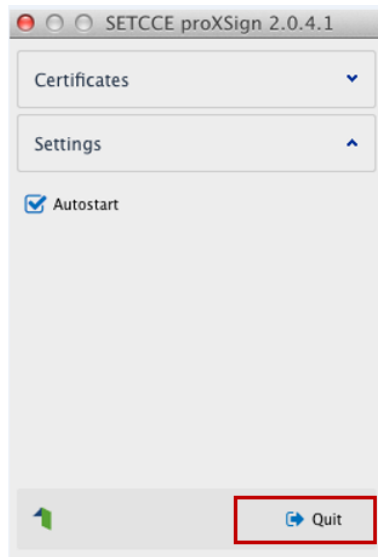


Figure 11: Option »Quit«

2. Click on **proXSign icon** in **Status** menu and choose »Quit«.

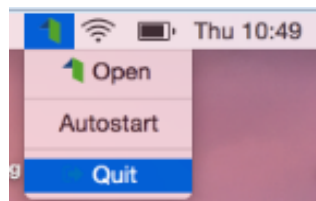


Figure 12: Quit on Status menu

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.

6. REMOVING SETCCE PROXSIGN® COMPONENT

To be able to remove SETCCE proXSign® component from your computer you have to log in to your user account as an administrator.

Then find and remove proXSign.app and »SETCCE_proXSign.pkg« files and remove both digital certificates from system digital store (use Keychain Access):

- »SETCCE services root CA« and
- »SETCCE proXSign intermediate CA«.

7. INSTALLING A DIGITAL CERTIFICATE

7.1. Is your personal digital certificate installed on your computer?

In order to use SETCCE proXSign® component on your computer, your personal digital certificate has to be installed in digital certificate store (Keychain) or on smart card.

7.1.1. Installation steps

To install your personal 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 on Figure 13. Your personal digital certificate is installed in your (User) Keychain. Along with your personal digital certificate, the root 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 certificates see chapter 7.2.

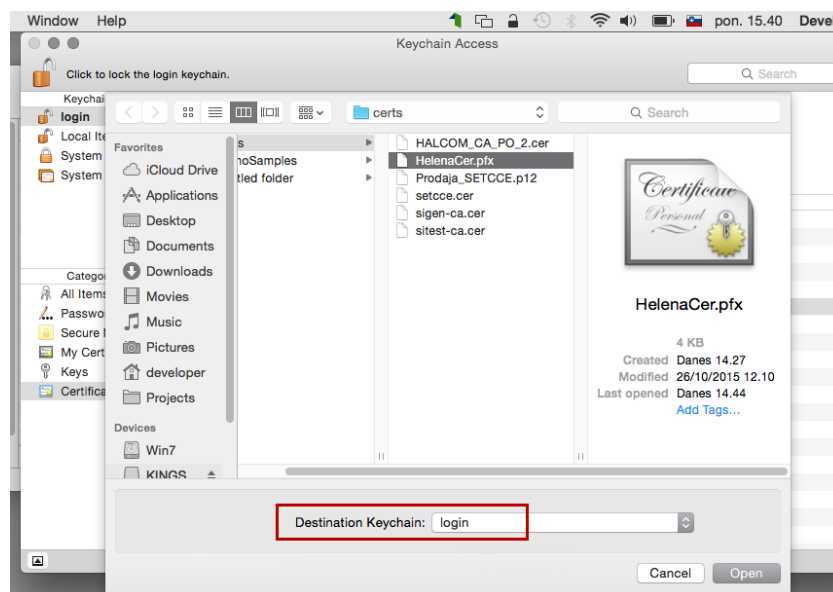


Figure 13: Installing personal digital certificate

With this procedure both digital certificates will be installed in **Keychains/Login** and in **Category/Certificates**. Your personal digital certificate will also be installed in **Category/My Certificates**, as shown on Figure 14.

Important:

1. The root digital certificate is not installed as trustworthy by default, therefore you have to set "Trust" properties as described in chapter 7.2.2.
2. Described installation steps stands for Yosemite and personal digital certificates which can be saved on hard drive.

3. Gemalto smart USB key, which holds your personal digital certificate, is shown as an additional keychain in Keychain Access application as shown on figure 15. For detailed instructions please turn to the CA authority who issued your personal digital certificate.

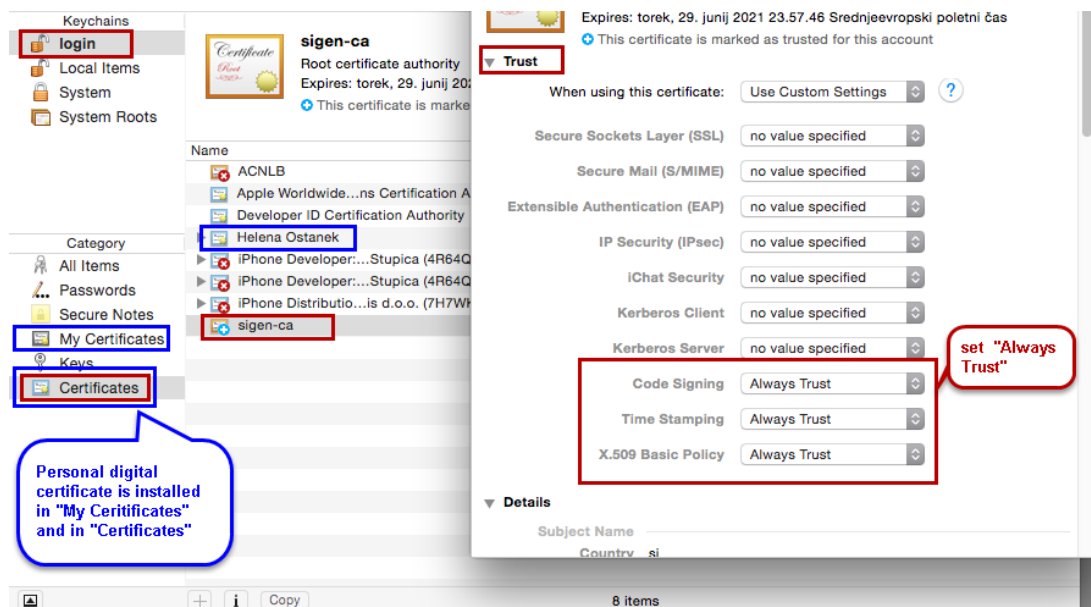


Figure 14: Personal digital certificate in Login (user) Keychain along with root digital certificate

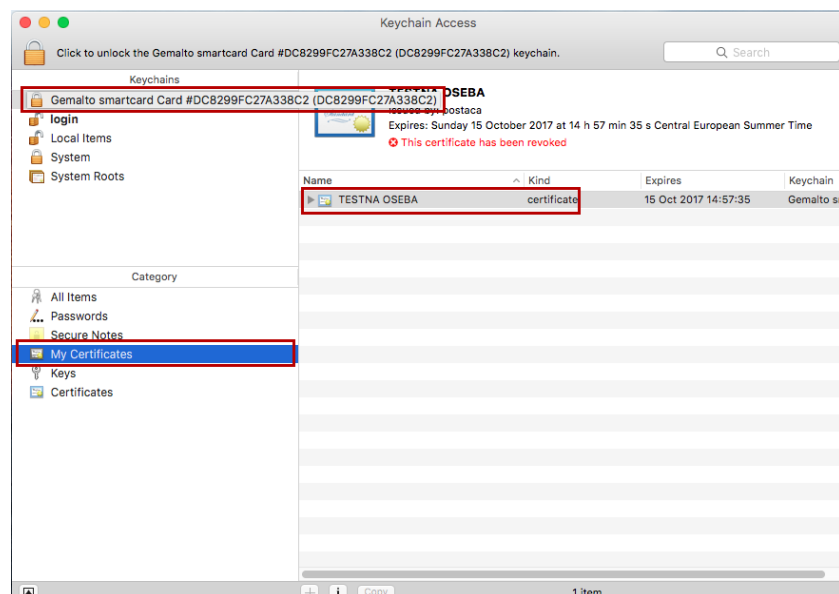


Figure 15: Personal digital certificate on Gemalto smart USB key in Keychain Access

7.2. Is your root certificate installed on your computer?

In order to use SETCCE proXSign® component, you have to install root certificate of Certification Authority which has issued your personal digital certificate.

7.2.1. Installation steps

Root digital certificates can be installed (at least) on two ways:

1. **Automatically**, along with your personal digital certificate (See 7.1). 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 to install it into system keychain. In this case all users on your computer can use/access root certificate for digital signing.

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

1. Log in as 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 root digital certificate from file system on your computer. From 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 7.2.2).

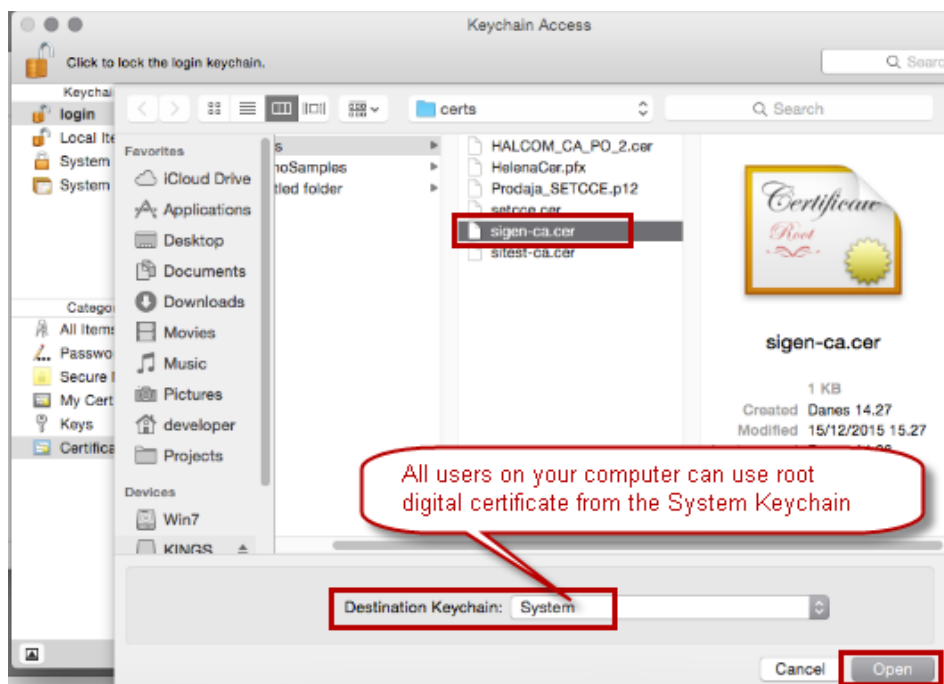


Figure 16: Installing root digital certificate in the System Keychain

7.2.2. Trust properties settings

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

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

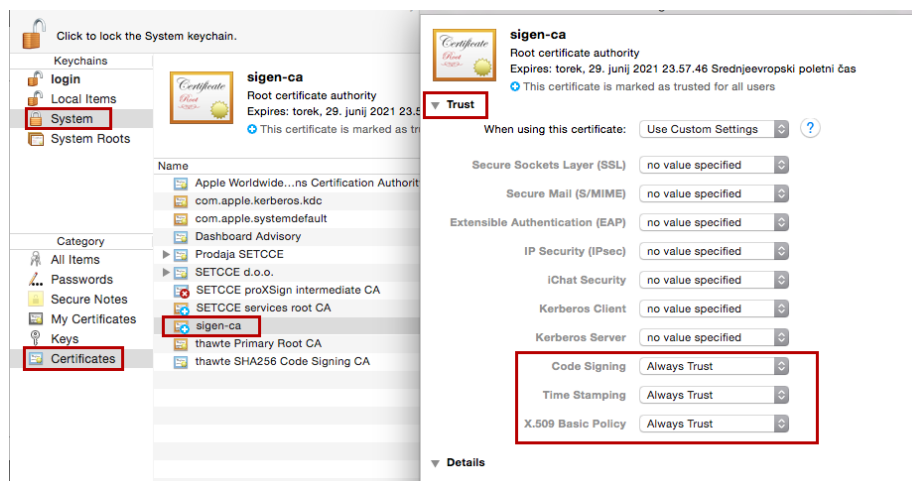


Figure 17: Installing root digital certificate in the System Keychain and setting up "Trust" properties