User manual for the ECSigner qualified electronic seal

Wersja 1.0 z dnia 29.01.2026

Table of contents

Information

The ECSigner qualified cloud seal is a service that enables you to create a qualified seal using a certificate and keys stored in the cloud, without the need for a physical device.

The service consists of several components:

- **ECSigner mobile application** – for smartphones
- **ECSigner Desktop application** – for computers
- **SecureDoc 2.0 signing application** – for computers

The listed applications are available for devices with Windows and macOS operating systems, or in the case of the mobile application: Android and iOS. In each application you can choose one of the available languages: PL and EN.

STEP 1: Activating your account on the EuroCert Portal

Activate your account on the EuroCert Portal using the activation link that was sent to your email address provided during registration. Click the link and set the access password for your Portal account.

Note! Important security information:

- If the link is no longer active, go to the website: portal.eurocert.pl and use the "forgot password" function, then follow the instructions displayed on the screen.

- Under no circumstances should you share your login password to the EuroCert Portal with anyone. The account is assigned to an individual.
  Anyone who gains access to your password may gain access to your certificate.

- If you suspect unauthorised access to your account, change your password immediately.

STEP 2: Installing the Software

Install the software necessary to handle the ECSigner. You can download it here https://portal.eurocert.pl/ - tab „Software":
1) **ECSigner mobile application** – which is used to generate a one-time OTP code – this code is required to be provided when submitting the seal.
   - Download and install the ECSigner mobile app from the store:
     - **Google Play** (Android)
     - **App Store** (iOS)
     - **AppGallery** (Huawei)
   - When you first launch the app, you'll be asked to set a 4-digit PIN. Enter it twice to save it – it will be required each time you launch the app.
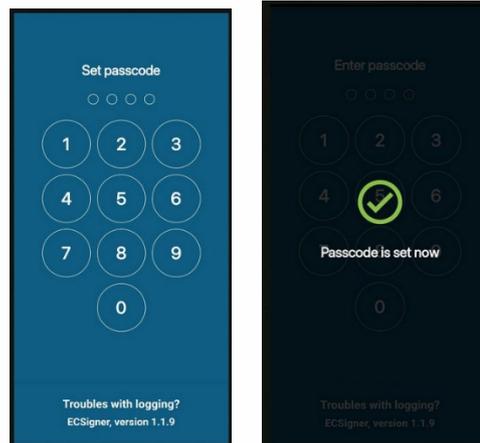
- If you have successfully installed the application on your smartphone, now go to your computer and complete the next steps from there.

2) **ECSigner desktop application –** which is used for communication between the cloud seal and the signing application installed on your computer.
3) **SecureDoc 2.0 application** – which is used to submit and verify the qualified seal.

STEP 3: Activate the ECSigner seal

Once EuroCert has completed the ECSigner seal issuance process, activate the seal yourself. Activation is required to begin using the ECSigner qualified seal. Follow the instructions below:

1) Log in to your account at **portal.eurocert.pl**
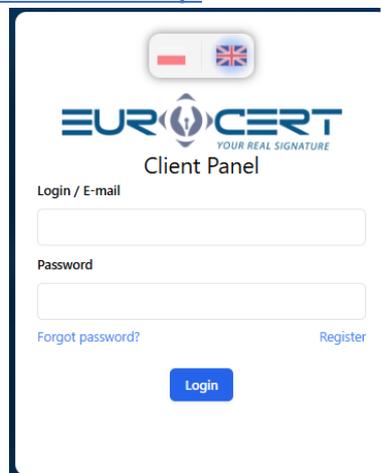
2) Go to the "Certificates" tab, then "Qualified Seal" and click on the "QR Code" icon.

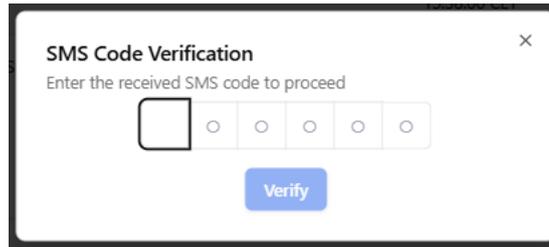| ID	Product	QR Code	Organization name	Organization Identifier	Validity Period	Valid Until	Status	Email	First Name	Last Name	Role
153801	EC Signer Seal		EuroCert Sp. z o.o.	9512352379	2 Years	2028-01-16 12:35:14 CET	Active				Administrat

3) Enter the received SMS code and confirm.

Attention! It typically takes no longer than 3 minutes for the SMS code to be delivered. If you haven't received the message, please try again. After three unsuccessful attempts, contact EuroCert technical support.

After entering the SMS code correctly, a "Secret" will appear in the form of a QR code - do not close this window.
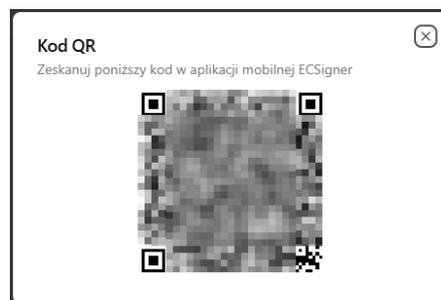

4) Run the previously downloaded ECSigner mobile app on your smartphone and click the "Add Key +" button, then scan the "Secret" QR code - after reading correctly, the OTP code should appear in the ECSigner mobile app.

5) Download and install the ECSigner desktop application - you can find it at portal.eurocert.pl, in the "Software" tab.

6) Download and install the SecureDoc 2.0 seal submission and verification application, which can be found at portal.eurocert.pl, in the "Software" tab, Step 3.

At this point, your ECSigner qualified cloud seal is activated and you have the necessary software installed. You can start using the seal.
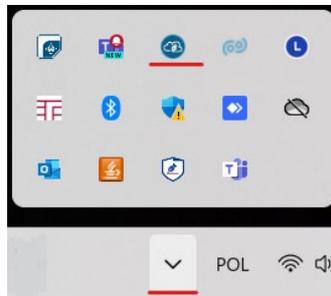
STEP 4: Using the ECSigner Seal

1) Run the ECSigner Desktop certificate software on your computer.

2) Sign in with the same login and password that were created for the account at https://portal.eurocert.pl/
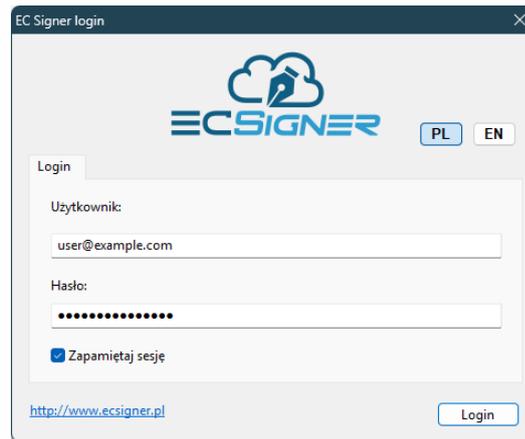
3) After you sign in correctly, the ECSigner application will run in the backgrounduntil the computer is turned off or the application is manually closed.


4) Launch the SecureDoc 2.0 qualified seal application and start the seal creation process.

5) Add the file you want to stamp and then use the "Sign Files" button.
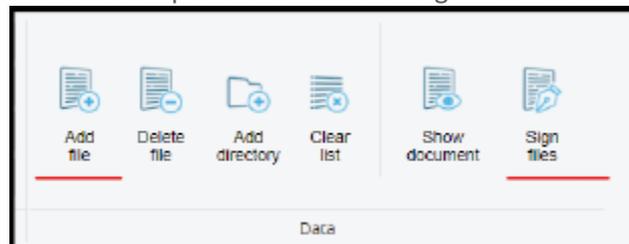
6) Select the "Cryptographic Devices" tab. The list will show cloud certificates the user has access to. Find and select the seal certificate with the organization's data and press "OK."
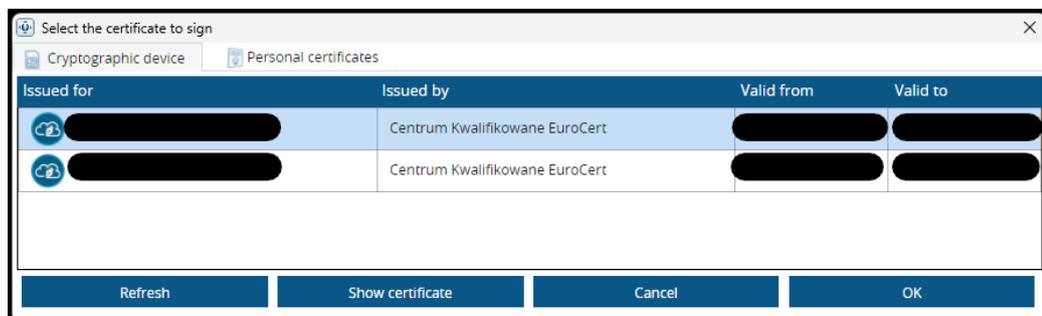
7) The application will then ask you to enter the authorization code, i.e. the OTP code.
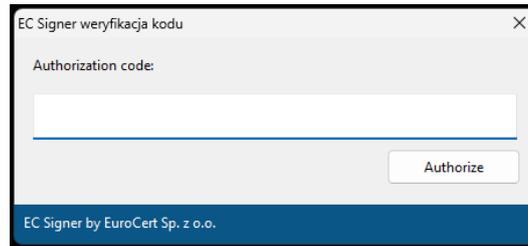
8) Access the ECSigner mobile app, enter your PIN, and enter the OTP code it generates. Each OTP code is valid for only 30 seconds, after which a new code is generated.
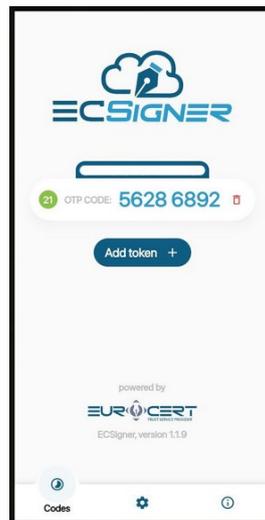
9) After entering the OTP code correctly, the signing application will start the sealing process.

Issuing and managing access for other users

ECSigner Seal Management:

- The ECSigner seal can be managed via the EuroCert Portal: https://portal.eurocert.pl/
- Access to the seal can be granted to multiple users – each using their own login credentials.
- Permissions can be granted to one of two roles: Administrator or User.
- Only users with the "Administrator" role have access to the seal's administrative functions.
- Only one user can use the seal at a time.

Below is the range of opportunities available for each role.

ECSigner Seal "Administrator" role

**"Administrator"** - a user with access to functions related to seal management, such as:

- granting and revoking access to other users,
- requesting certificate renewal,
- using the seal.

Only one person/account can be assigned the Administrator role for a single qualified seal. This permission cannot be transferred to another person or account.

Adding a new user

To add a new user, a user with the "Administrator" role should visit https://portal.eurocert.pl/ and go to the Certificates -> Qualified Seal tab. Select the qualified seal for which you want to grant access from the list and in the "Actions" column. To do this, go to the list of qualified seals and click in the "Actions" column, click the icon
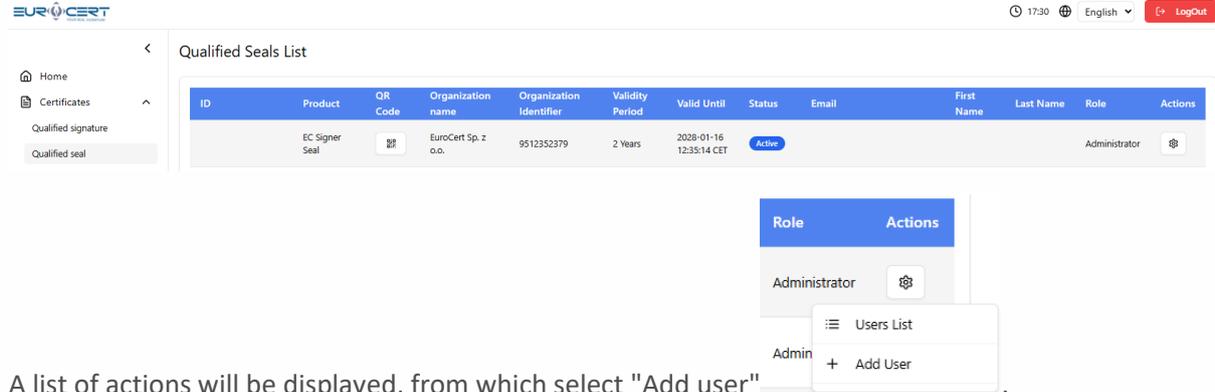
A list of actions will be displayed, from which select "Add user"

Then the message "Issuing access to a qualified seal for a new user" will appear

Enter the email address and mobile phone number of the user you wish to grant access to. Then click "Send" to receive an email invitation to activate access to the seal and their account on the EuroCert

Portal. The provided phone number will be used as an additional security measure: during activation, the user will receive a one-time SMS code.

In the next step, the new user must "Activate Access." Until activation is completed, they will appear on the user list with the status "Pending."

 Additional information:

- If the Administrator makes a mistake in the user's e-mail address or telephone number, the granted access should be removed (function available in the "User List") and then access should be granted again with the correct data.

User list

To view the list of ECSigner seal users, a user with the "Administrator" role should go to the following
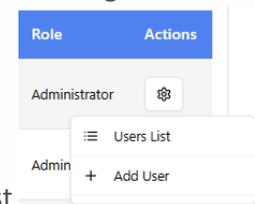
path: EuroCert Portal -> Certificates -> Qualified Seal -> Actions -> User List .

The user list shows both current and historical (deleted) users.

Information available for reading from the list:

- User data: date of entitlement, email address, phone number, first name, last name, role.
- User statuses:
  - Pending - an invitation has been sent, but the user has not yet activated their access.
  - Active - the user has activated their access and can use the seal.
  - Deleted - access to the seal has been revoked and the user cannot use it.

Revoking user access

To revoke access to an ECSigner seal user, a user with the "Administrator" role should go to the following path: EuroCert Portal -> Certificates -> Qualified Seal -> Actions -> User List
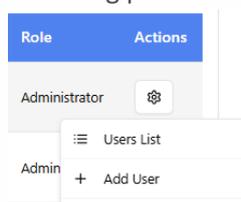
. Then, find the user whose access is to be revoked and click the "Remove"

button in the "Actions" column . In the next step, confirm the operation in the dialog
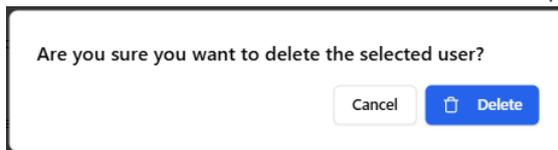
box that appears . Access will be revoked immediately and the system will record the date access was revoked.

ECSigner Seal "User" role

"**User**" – a person authorized solely to use the seal.

- To use the seal, you must have a registered account at https://portal.eurocert.pl/ and be granted permissions by the ECSigner Seal Administrator for the given organization.
- You must complete the ECSigner seal access activation process, described below.
- You can use the seal using your own access details (login and password) and the ECSigner mobile app, which generates an "OTP" code.

Activation of access by user

To activate access to the ECSigner seal, a person with the "User" role should:

1) Receive email notification
   - Check your mailbox and look for a message with the subject: "EuroCert - Activation of access to the seal", which will contain the information "Confirmation of issuing access to the qualified seal". This message means that the Administrator has granted you access to the seal.

2) Log in or register on the EuroCert Portal
   - Use the email redirect or visit https://portal.eurocert.pl/
   - Log in or register a new account
   - The account must be registered with the same email address that the Administrator granted access to. Otherwise, activation will not be possible.

3) Go to the tab: Certificates -> Qualified Seal and select the seal from the list and click "Activate access"
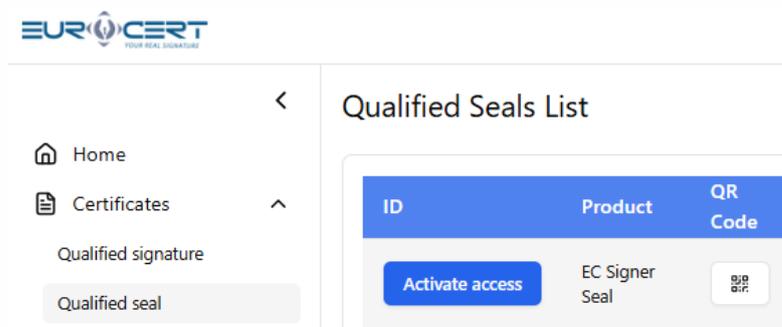
4) Enter the SMS code
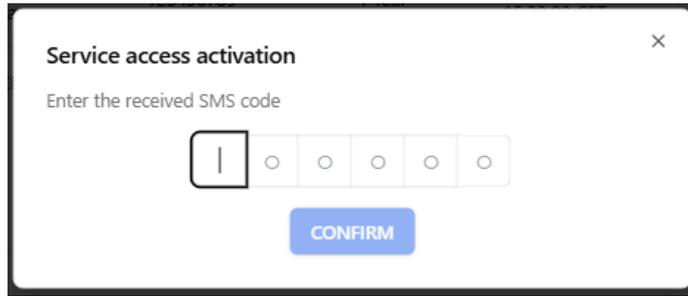
- After clicking "Activate access", an SMS code will be sent, which must be entered in the window that appears.
- Attention!
  o An SMS code will be sent to the phone number provided by the Administrator when granting permissions.
  o This number may be different than the number associated with your account during registration.
  o If the SMS does not arrive, contact the ECSigner seal Administrator and confirm the number is correct.

5) Access activated
- After entering the SMS code correctly, access to the seal will be activated.

6) Follow the next steps of the instructions:
- STEP 2: Installing the Software
- STEP 3: Activating the ECSigner Seal
- STEP 4: Using the ECSigner Seal

How to use the ECSigner mobile application

a) ECSigner mobile application functionalities:
- Storage of the "secret" necessary to generate the OTP code
- OTP code generation - the code consists of 8 digits and it is valid for 30 seconds

b) Settings:
- Changing the language to EN/PL
- Changing the method of signing in to the application with a PIN or a fingerprint
- PIN reset

c) Additional information :

- **How to change the PIN to the application?**
  Sign in to the application, select "Settings" and then "Reset passcode to the app".
  Introduce the currently valid PIN and enter the new PIN twice.

- **What if I forgot my PIN code?**
  Uninstall the application from your smartphone, then redownload and reinstall it. Repeat the signature activation procedure following the instruction - STEP 3.

- **Where should I enter the OTP code to sign?**
  The window to which the OTP code should be entered is displayed by the Secure Doc 2.0 Signature Application. Let us remind you that this window looks as below:
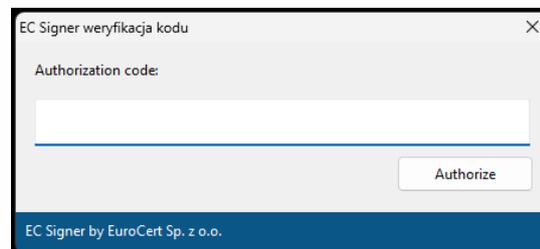
- **Why does the ECSigner application prompt for re-login?**
  The certificate access session remains active throughout the use of the ECSigner application. After each login, the user has approximately 3 minutes to complete the signature. If this time is exceeded, the signing session will expire, and the ECSigner program will prompt for re-login.

- **How to sign in the SecureDoc application using a single OTP code?**
  By activating the 'Remember session' option during the ECSigner application login, the user is prompted to enter only one OTP code for the entire session, regardless of the number of files being signed.

How to use ECSigner Desktop application

a) ECsigner Desktop Application functionalities:
- Signing in and the certificate registration
  - o Once you are signed in to the ECSigner Desktop application, the certificate is automatically registered in the certificates storage and will be visible to the signing application.
  - o Only one person can be signed within one application session.
- Access to the certificate "in the cloud" after correct login (or several certificates if the user has more than one certificate).
- Verification of the certificate data and the validity date:
  - o After launching the application, we can read all the data contained in the certificate.
  - o The application also provides information about the certificate's validity period.
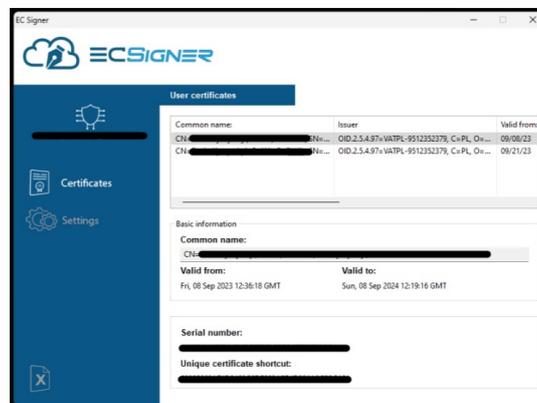
b) Additional information:
- **How to properly sign in to the ECSigner Desktop application?**
  To sign in to the ECSigner application, you must have an activated account at https://portal.eurocert.pl/ . Open the application and enter the login and the password you use for authentication while signing in at https://portal.eurocert.pl/ .

- **How to change the access password to the ECSigner Desktop application?**
  You can do it after log in to your account - https://portal.eurocert.pl/ . After logging in, select the "My data" and "Change password" tab. Then enter the current password and enter the new one twice.
  The second option is to change the password using the "Forgot password" function, which allows you to reset the access password. In this situation, make sure that you know and have access to the email which you use for login.

- **How to check if I am properly logged in to the ECSigner Desktop application?**
  After logging in, click in the application bar on the bottom of the screen "Show hidden icons", select the ECSigner icon, use the right mouse button and click "Settings". If your certificate is displayed, it means that you correctly signed in. If you want to keep the login session, remember when you exit the application, do not close it with "x" but use "-" instead to minimize, so the application continues to run in the background.

EuroCert technical support

Should you have any inquiries or technical problems

- Find the answer in our FAQ section – [Help Center]
- Write us an email support@eurocert.pl