Electronic signature
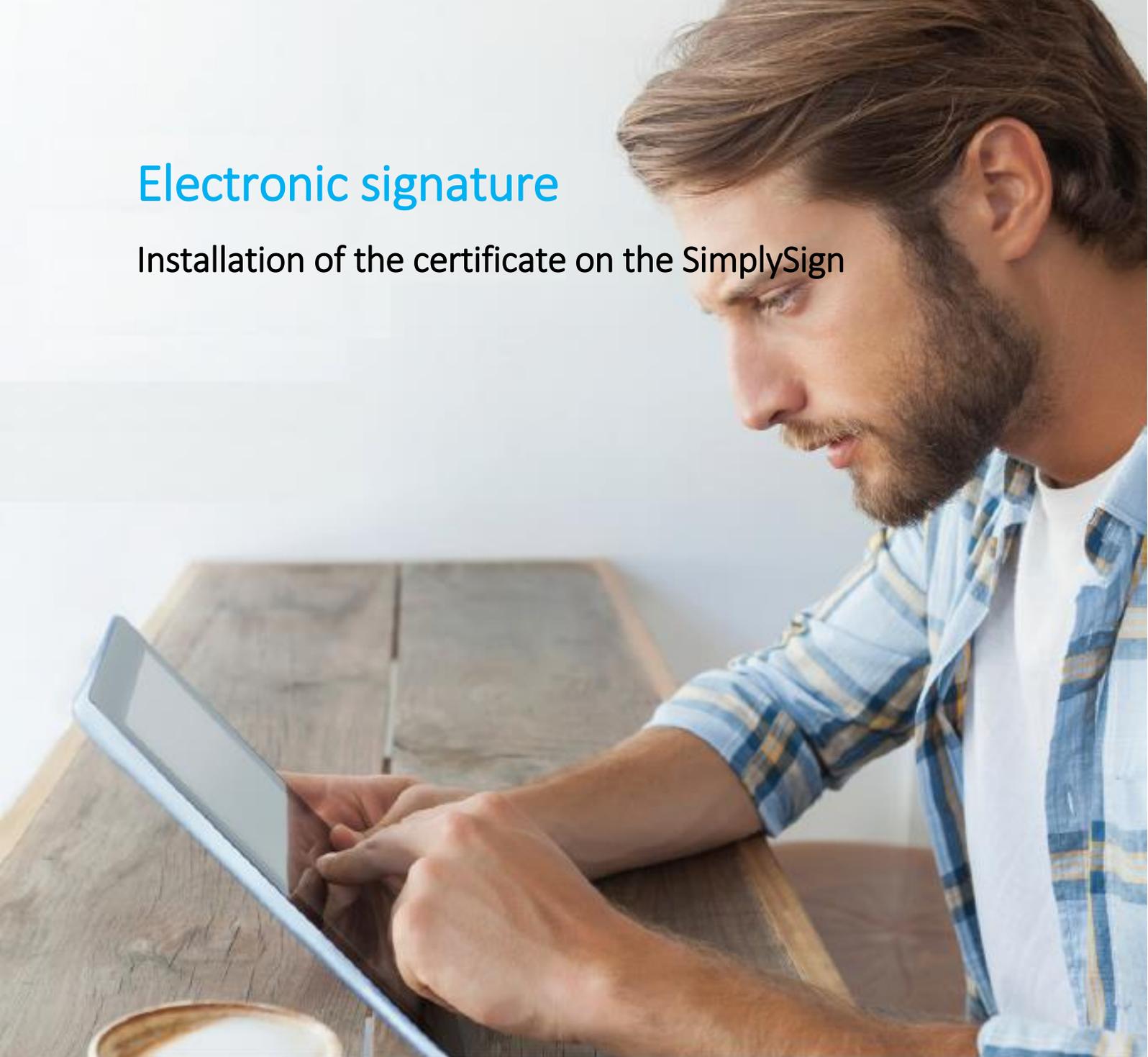
Installation of the certificate on the SimplySign

Instructions for installing the certificate on SimplySign

version 1.1

Certum
by asseco

Table of Contents

1. General information

A qualified certificate is issued by Certum after receiving a set of correctly completed documents. The following instructions contain the next steps in the process of installing the SimplySign qualified certificate.
In the process of installing the certificate, use the buttons that appear on the screen, e.g. "Next", not the navigation arrows in the browser.

## 2. Information about issuing the certificate

The certificate installation procedure begins upon receipt of information confirming the issuance of a qualified certificate by Certum. In the message, you will also receive a link to the **Certum panel** through which you can install the qualified certificate.

3. Certificate installing

After logging in to your account, go to the **Dashboard** tab visible in the menu on the left side of the screen

On the list of certificates you can see a list of your certificates. Certificates that have not yet been installed are displayed in white frames, while certificates that have already been installed are displayed in blue.
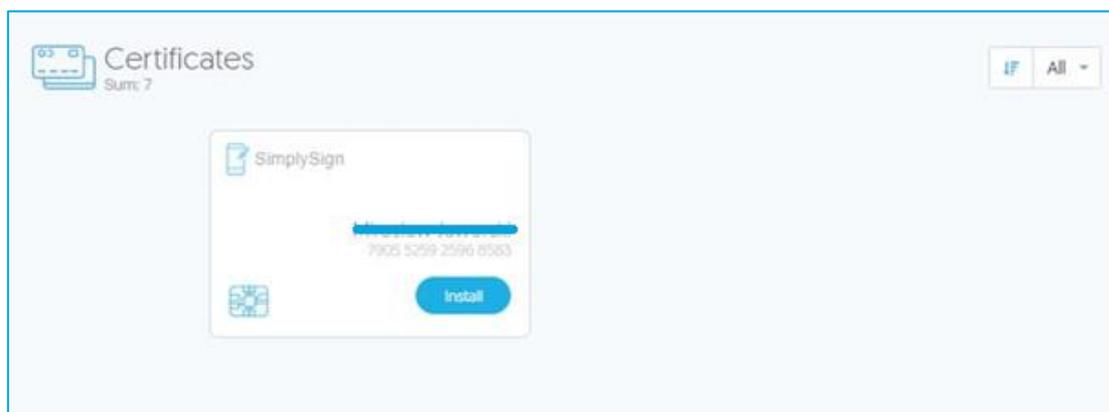
> **!** **If there are no certificates for installation on the list, you should verify that you are logged in to the correct account (on the account from which the activation was performed).**

In the list in the new certificate you want to install, select the **Install** option


In the next step, it will be necessary to prepare your mobile device (Smartphone / Tablet) on which you plan to install the certificate. Make sure you have the SimplySign application installed on it.

In the SimplySign application on the mobile device, select **Authentication Data** as the activation method.

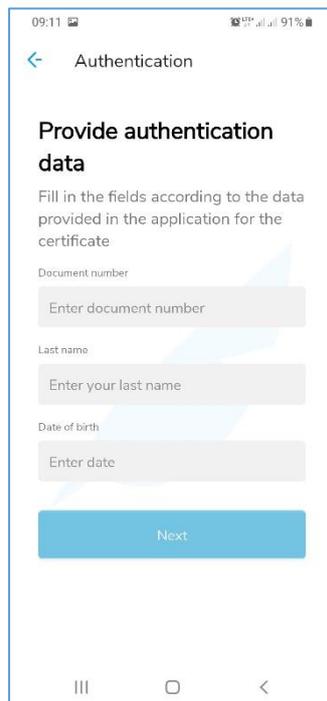Then, in the field **Enter your e-mail address**, you must enter an email, which is the User's ID.
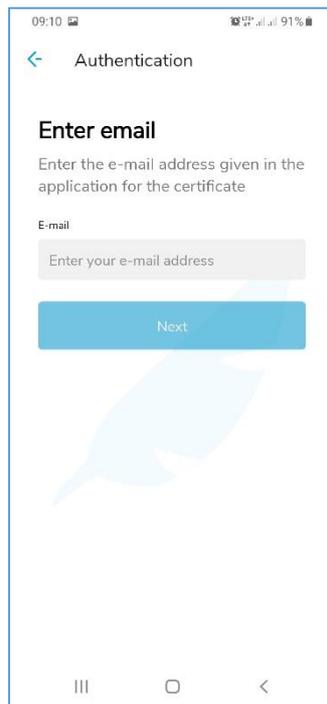
If the ID is correct, the application will ask to enter 3 random personal data of the User, which were previously provided in the certificate application.

After entering the personal data, press the **Next** button. If the personal data is correct, the application will be activated

The application will go to the start screen, in which you must select the application operating mode.

Two modes are available:

- **Sign documents** – it only allows you to sign documents – in such a case the login token will be downloaded from another device;

- **Generate token code** – it only allows you to generate a token – in such a case you will have to place a signature using another device;

The modes can be combined in order to obtain a possibility to generate a token and sign documents on the same device.

After selecting the appropriate modes, press the **Finish Activation** button. A screen indicating that the application is active will be displayed.

After completing the above steps, return to the certificate installation screen and select the **Next** button.

Following this, you will be asked to accept the certificate.

> **!** **Before accepting the certificate, make sure that all the data is correct.**
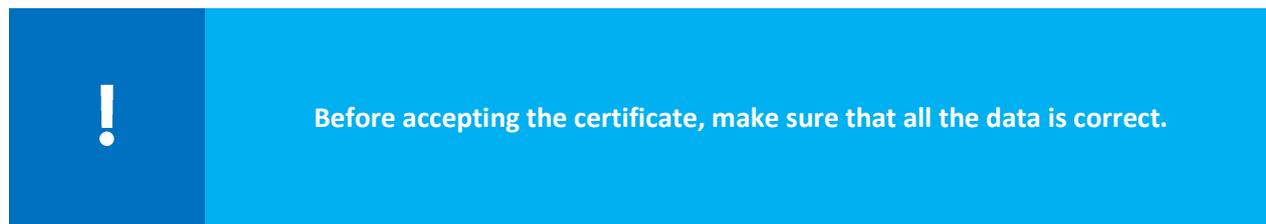
If you notice erroneous data in the certificate, use the **Report an error** option. In the error description field, type a description of the error you noticed, the maximum number of characters in the description is 180. After selecting the Find out more option, you will find out which reports are subject to complaint.
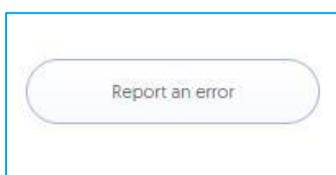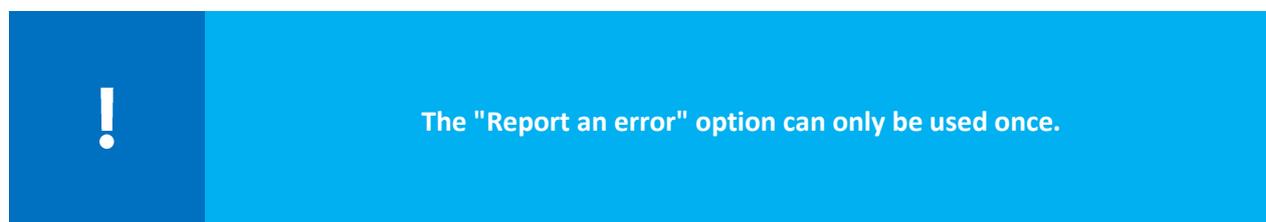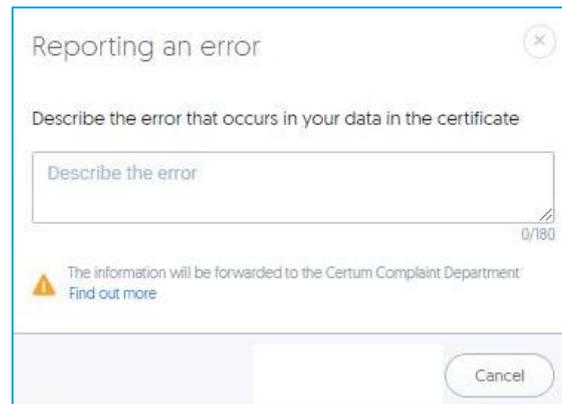
> **!** **The "Report an error" option can only be used once.**

Report an error
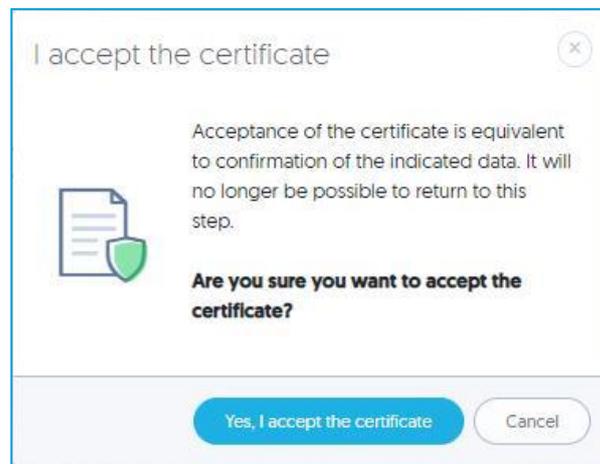
If all the data is correct, select **I accept certificate**.
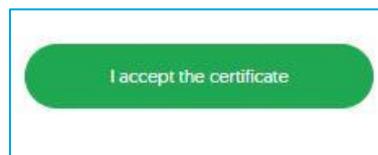
In a new window you will be asked to accept the certificate. Acceptance of the certificate is equivalent to confirming the data in the certificate. You will not be able to return to this step.
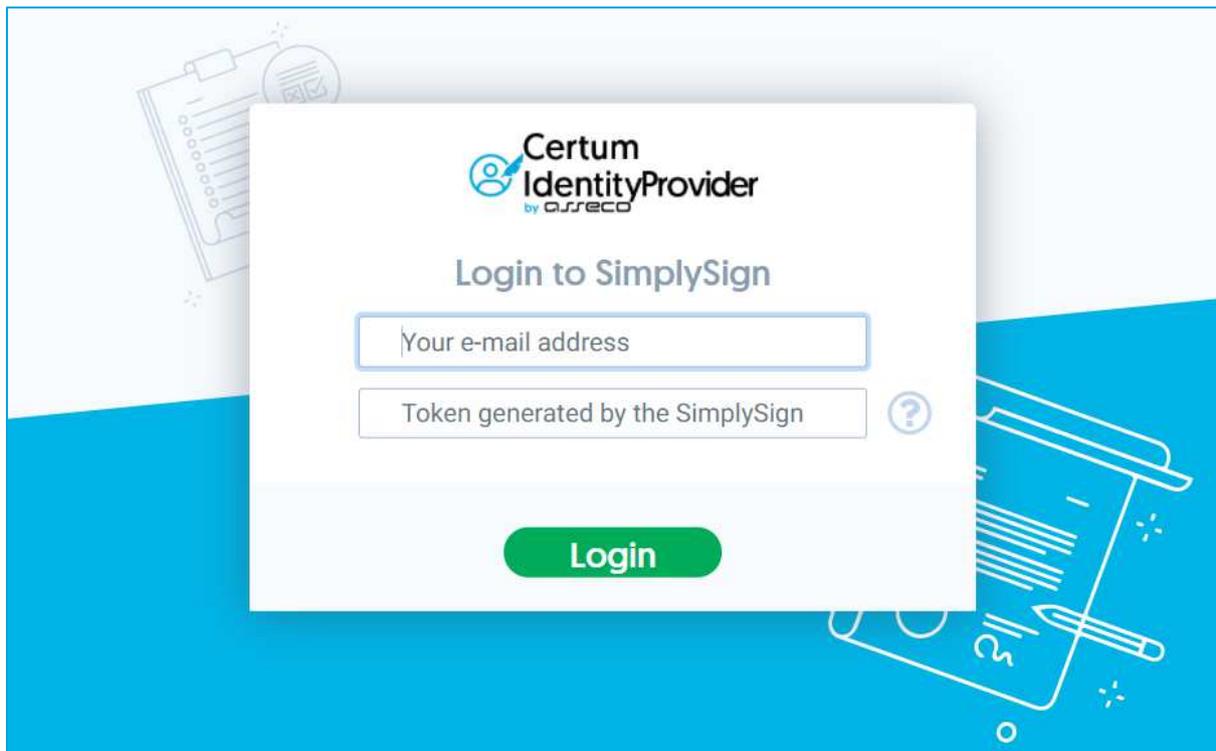

If you accept the certificate select **Yes, I accept the certificate**.
In the next step, you will be asked to log in to SimplySign.

> **!** **In the e-mail address field enter the e-mail address assigned to your SimplySign account; the Token can be generated in the SimplySign app on your mobile device.**

You will then be asked to assign a PUK code and PIN to the service. Your code must be at least 6 characters long.

> **!** **The PIN and PUK code is assigned by the user, if the codes are lost or blocked, access to the service will be impossible.**
>
> **if PIN and PUK have already been assigned to the cloud card, this step is skipped and the certificate is installed immediately after the certificate is accepted. So you do not need to enter the PIN to the cloud card to be able to install the certificate.**

After entering the codes, click **Next**. A **Summary** will be displayed on the final screen. After clicking the **Finish** button, the process will be completed.