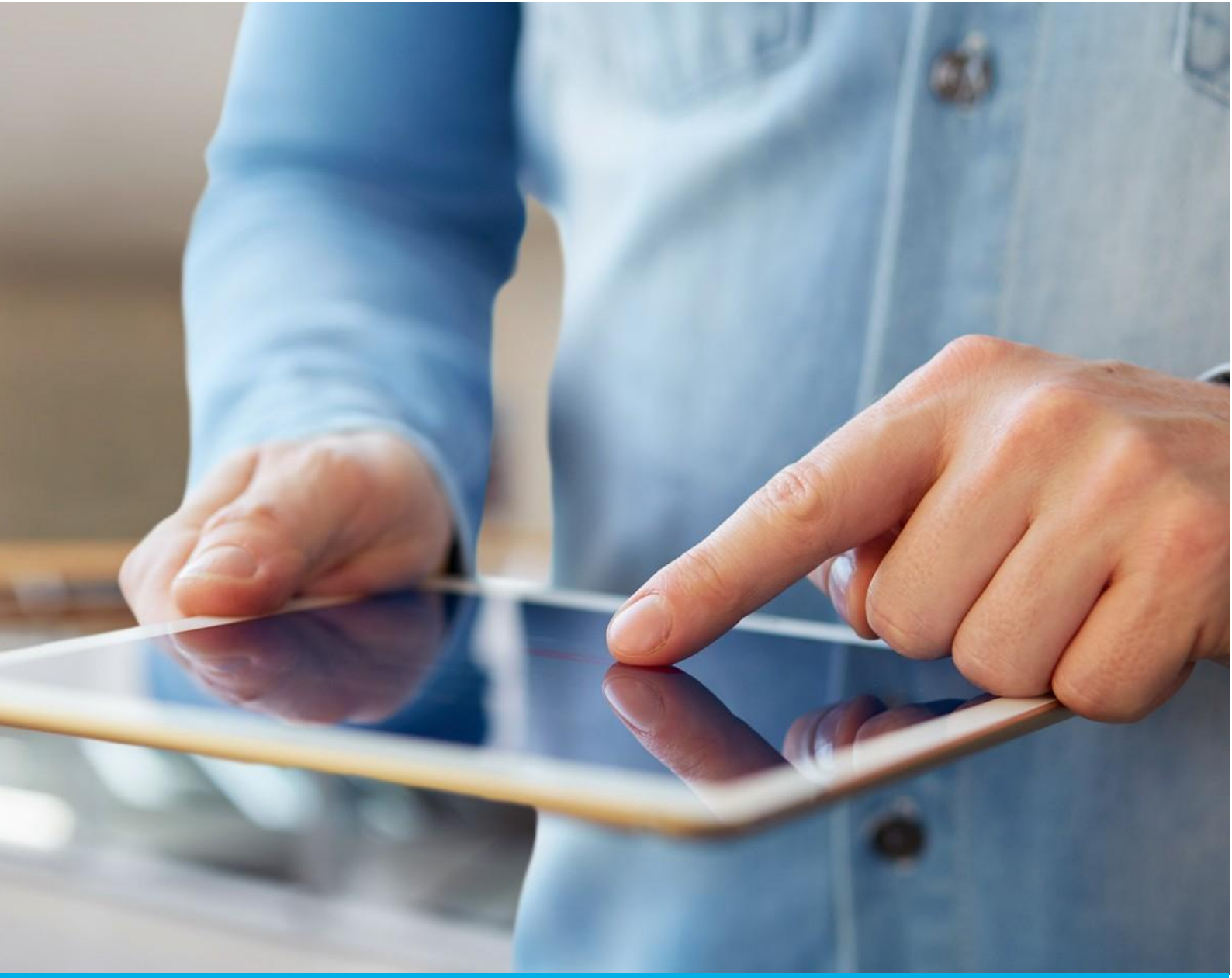


Certum S/MIME Individual certificate activation

Ver. 1.8

asseco

Certum by asseco

Table of Contents

1. Product description

Certum S/MIME certificates are security certificates used in e-mails to secure electronic communication. They enable the encryption of message content, ensuring privacy and confidentiality of e-mail correspondence. Additionally, S/MIME certificates allow for the addition of digital signatures, to confirm the sender's identity and guarantee the integrity of the transmitted content. With Certum S/MIME certificates, it is possible to enhance the security of e-mail communication by verifying the e-mail address/identity of the sender, encrypting messages and ensuring integrity.

2. Certificate activation

As the Certum **customer**, you will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab.

As the **partner**, you start the process through partner panel from the **Dashboard** by choosing the product you want to order.

The process of issuing the certificate consists of several steps:

- **Data verification** – providing the subscriber data and the verification
- **E-mail verification** – providing an e-mail and the verification
- **Certificate activation** – key pair generation, choosing the fields to include in the certificate and submit to issue.

As the activation process goes, each step will go through the next statuses:

Step is awaiting for the data

Data is saved and waiting for verification

Verification was successful

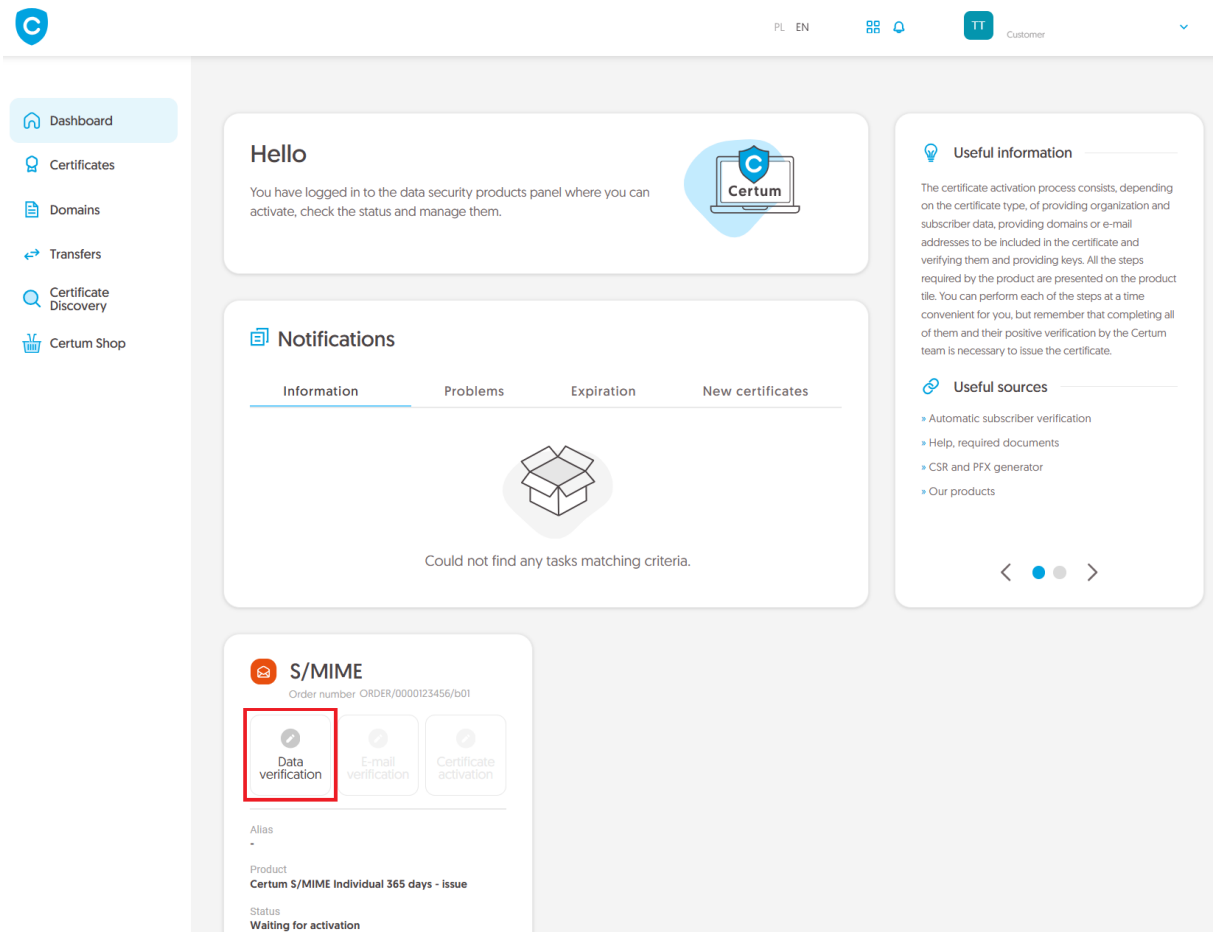
Providing the data is not available yet

Data verification step

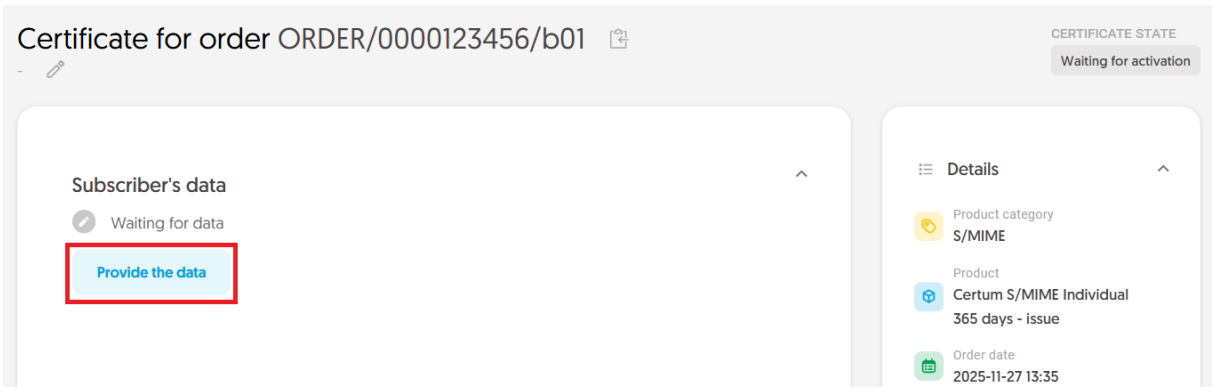
Providing data to be verified is the step in which you provide the data of the subscriber (the person who will be the owner of the certificate). From the data provided here, it will be possible to select data for the certificate in the last step of certificate activation.

The list of supported verification documents you can check at Information about required documents.

As the Certum **customer**, you will be able to start the data verification step from **Dashboard**, using **Data verification** option:

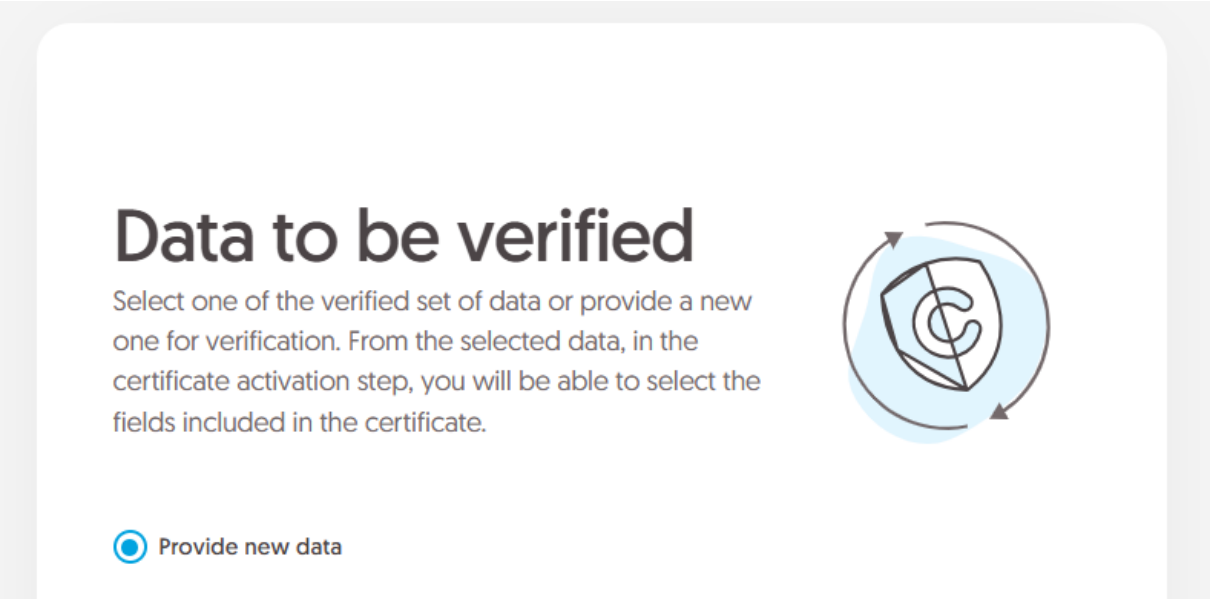


or from the **Certificates** list – choose the certificate you want to activate and use **Provide the data** option in the subscriber's data section:



As the **partner**, you will be able to start the data verification step from **Dashboard**, using new order option. After choosing the product type and providing the order details, you will be able to provide the data used in the first step of issuing the certificate.

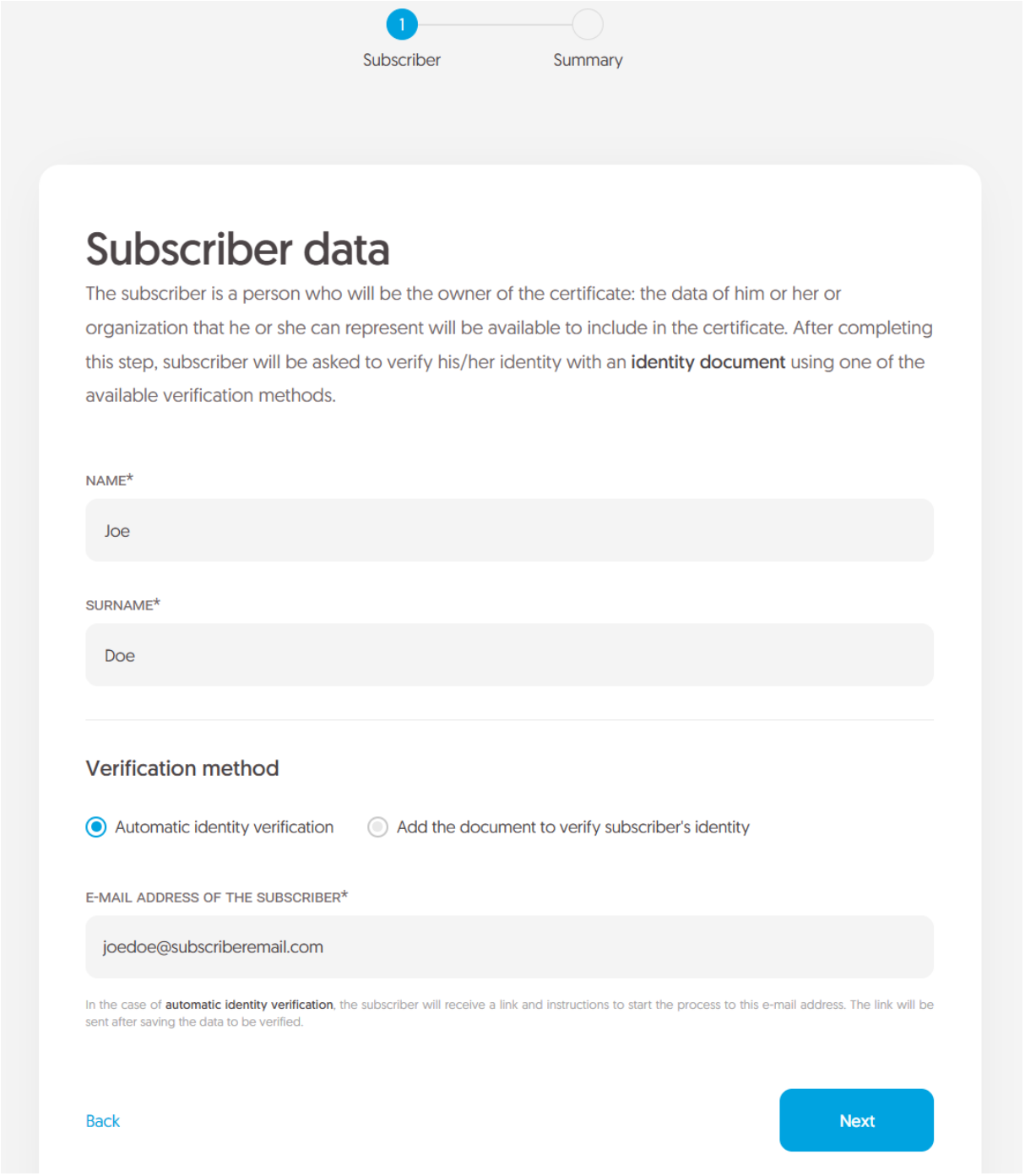
The wizard will guide you through the process of providing the data. In the first stage, choose to **Provide new data**. In the future, it will be possible to use them to issue another certificate.



In the next stage, provide the details of the subscriber, which means the person who will be the owner of the certificate. Please write the names and surnames in the form as they appear on the subscriber's identity document.

Also choose a method for verifying the subscriber's identity from the available ones:

- **Automatic identity verification** – the subscriber will receive an e-mail with a link to the identity verification service to use with a computer or phone camera and an ID document
- **Attaching a document** – you will add a scan of the subscriber's identity document or an identity confirmation.



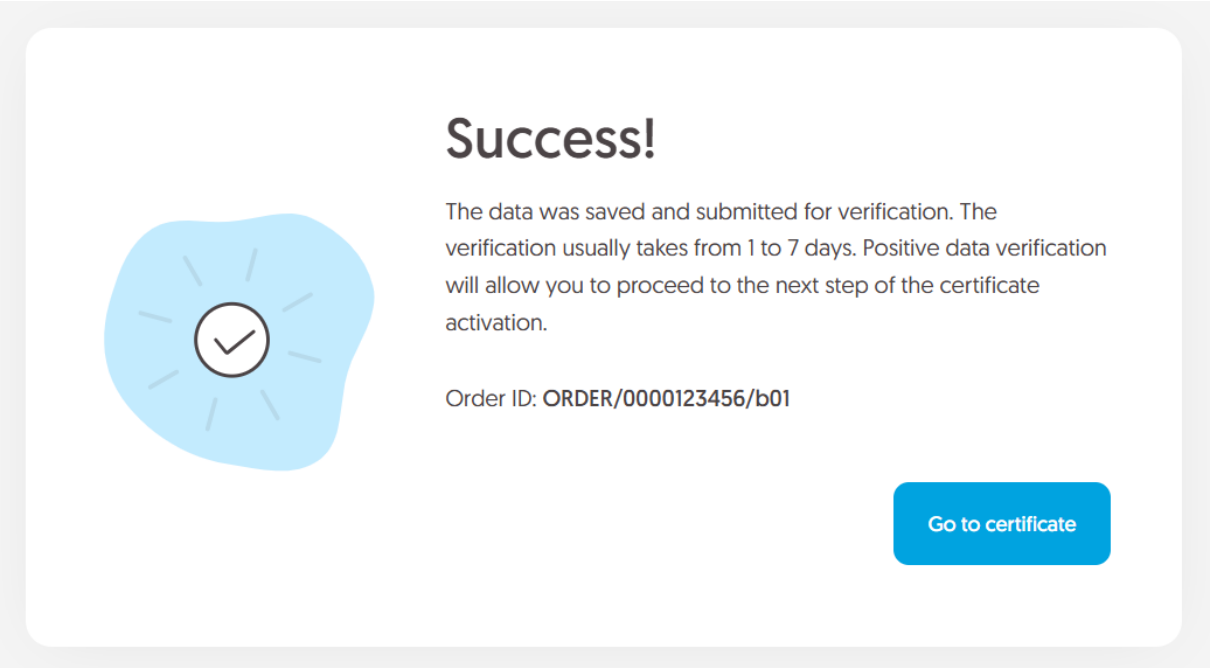
After selecting the verification method go next.

Data verification step summary

Check provided information on the summary screen. If the data is correct, mark the statements if required and complete the step of providing data to be verified.

The success screen will inform you that the data have been saved for verification. Certum will verify it. During this time, if you want to add another document confirming the provided data, you can add

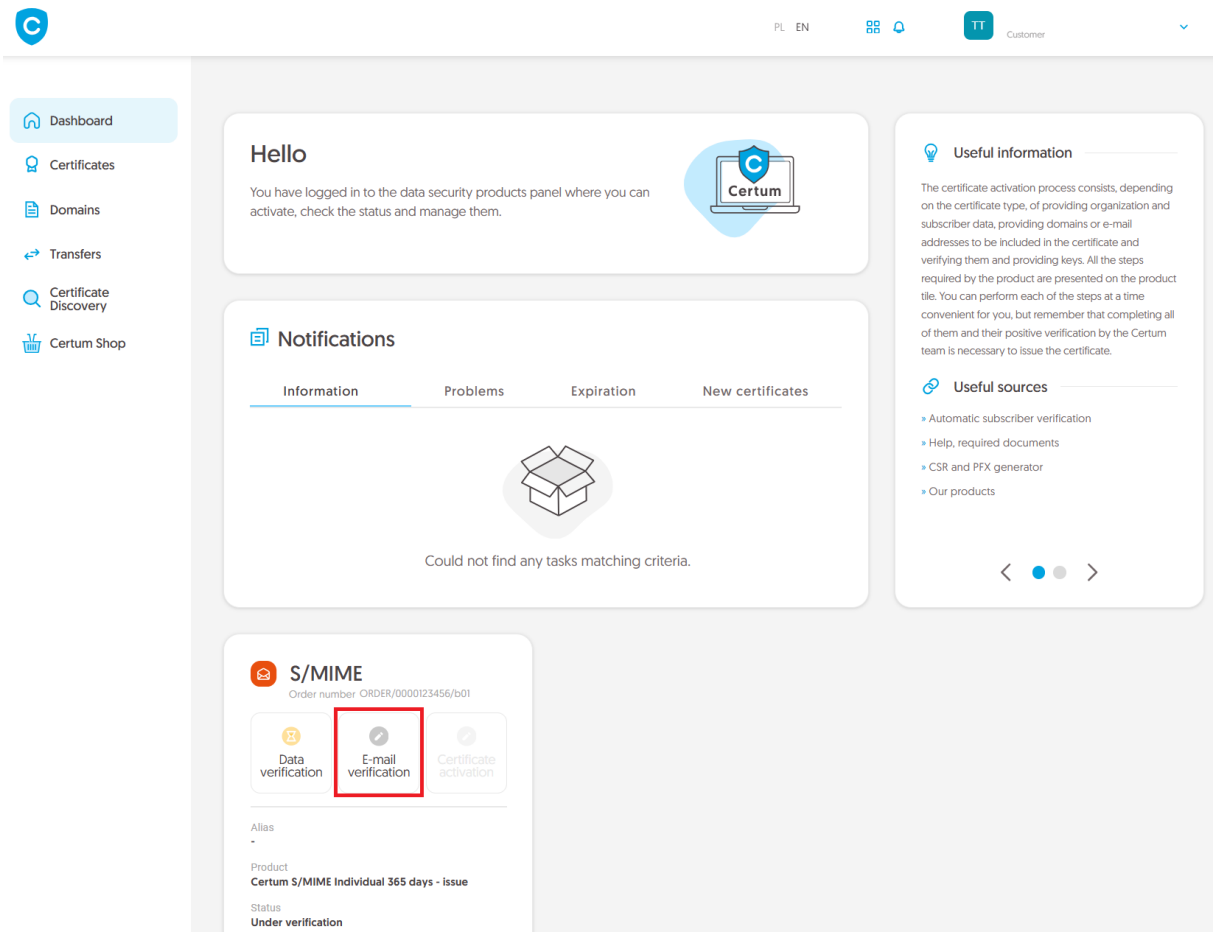
it in the certificate details. This is also the time to perform automatic verification of the subscriber's identity, if such verification method has been chosen. You may check the instruction for automatic identity verification.



When the data to be verified is saved, you can proceed to the next step which is providing an e-mail.

E-mail verification step

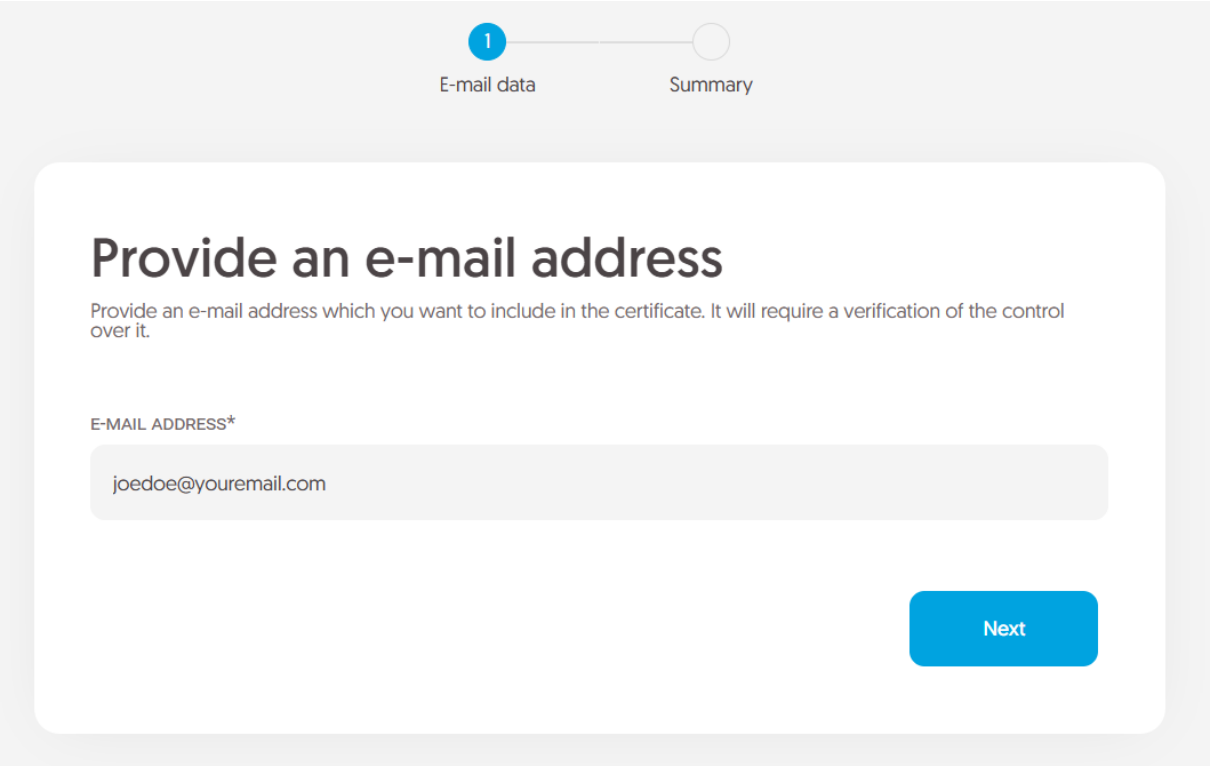
You will be able to start the e-mail verification step from **Dashboard**, using **E-mail verification** option:



or similar to the **Data verification** step: from the **Certificates** list – choose the certificate you want to activate and use **Provide e-mail address** option.

In this step, you will provide the e-mail to be included in the certificate.

Provide the e-mail address to include in the certificate and proceed.



Check provided data on the summary screen. If the data is correct, complete the e-mail verification step.

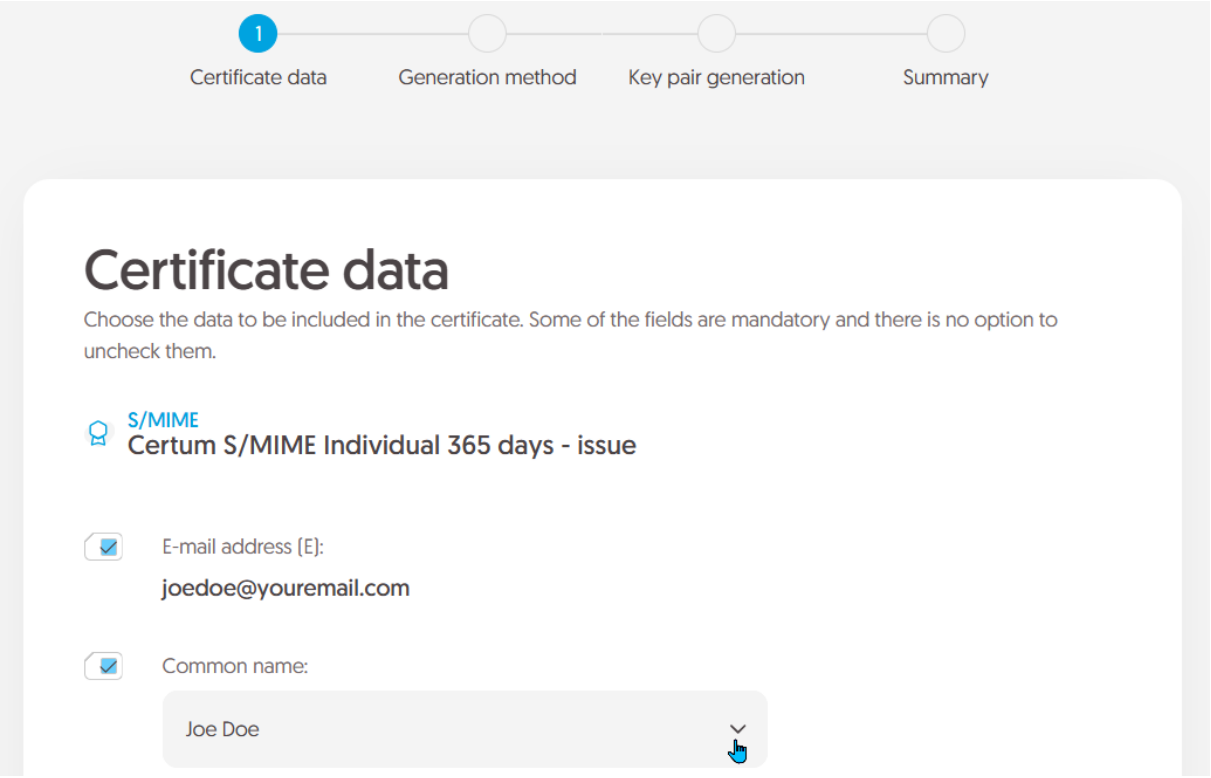
The success screen will inform you that the e-mail address has been saved. Verify the access to it or if the data to be verified and the e-mail address are both verified, proceed to the last step, which is **Certificate activation**.

Certificate activation step

You will be able to start certificate activation step from **Dashboard**, using **Certificate activation** option or similar to the previous step: from the **Certificates** list – choose the certificate you want to activate and use **Activate certificate** option.

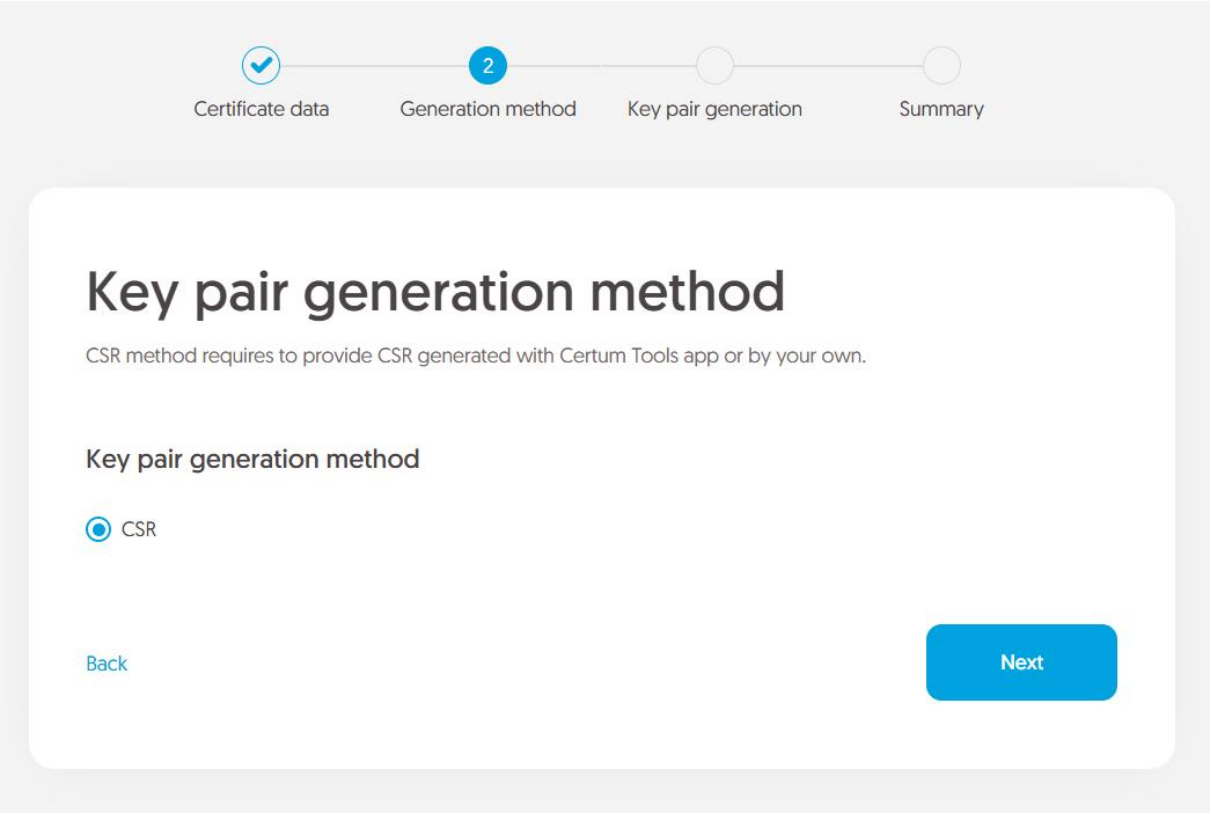
In this step, you will choose the Common name of the certificate and generate key pair.

Choose the Common name of certificate.



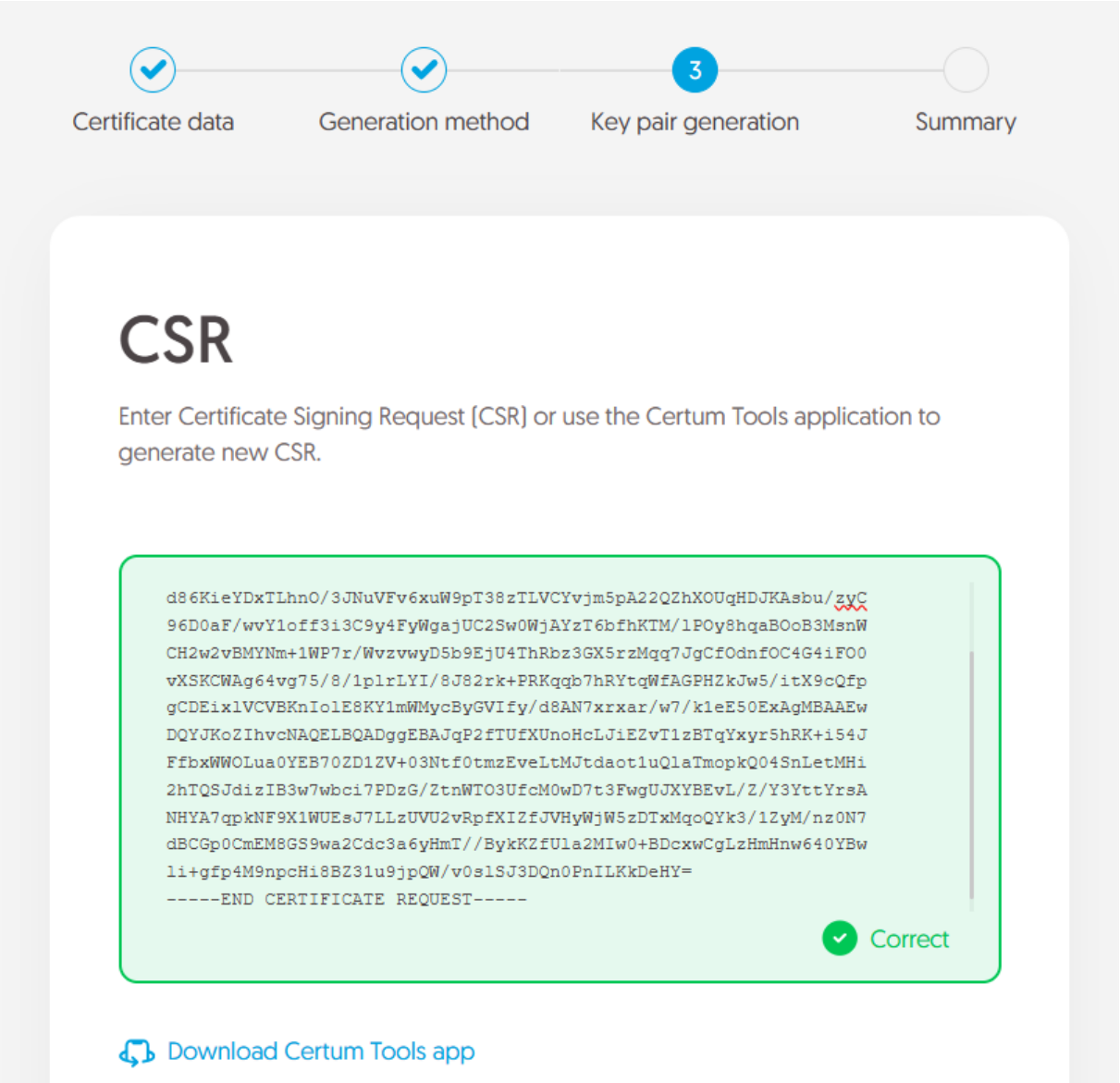
Once you have chosen the Common name of the certificate, go to the key pair generation.

For this type of certificates, the available key generation method is CSR which means providing a certificate signing request generated by a generator, e.g. Certum Tools, or by the application/server where the certificate will be installed.



CSR method

After proceeding, paste your CSR. After pasting the CSR, it will be verified whether it is correct. If a CSR error occurs, it will be indicated in the error message.



Remember to save the private key if you generated a CSR using the generator (e.g. Certum Tools app). You will need it to install the certificate once it is issued.

Providing the correct CSR and proceeding will display the summary screen. Check all of provided data. Mark the required statements if needed and complete certificate activation.

Summary

Go to the summary screen and check all of provided data. Mark the required statements if needed and complete certificate activation.

The success screen will inform you that the certificate has been submitted for issuance. The issued

certificate can be downloaded from the certificate creation e-mail or from the certificate details view: in a convenient **PEM** or **DER** encoding.

From the certificate details view you can also download subordinate certificates for the certificate.

If you need a PFX file, you can use the Certum Tools generator.