Information on activating a certificate for a.sign RK HSM

1 Requirements

- a.sign RK HSM is reachable in your network and the IP address is known.
- Access to A-Trust webshop (https://www.a-trust.at/shop)

The HSM is delivered with a large number of pre-generated keys (open key labels), these keys cannot be used without a certificate. To issue a certificate for a classification key (VAT-ID, GLN, …) , the following steps must be taken:

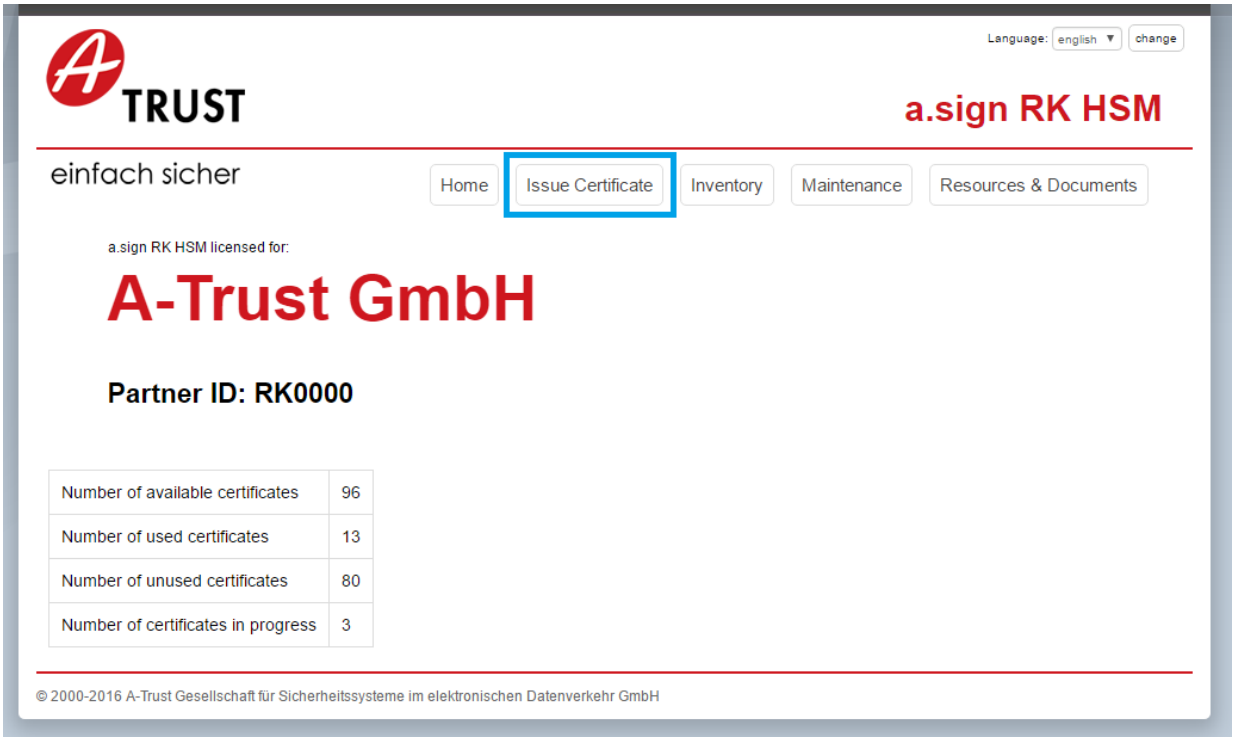
Certificate issuance is a two-step process: first, you have to generate a certificate request (certificate signing request) on the HSM. Next, you have to upload the request file into the A-Trust web shop. Finally, you have to import the result file from the web shop into the HSM.

2 Create a new certificate (manually)

2.1 Creating a certificate request

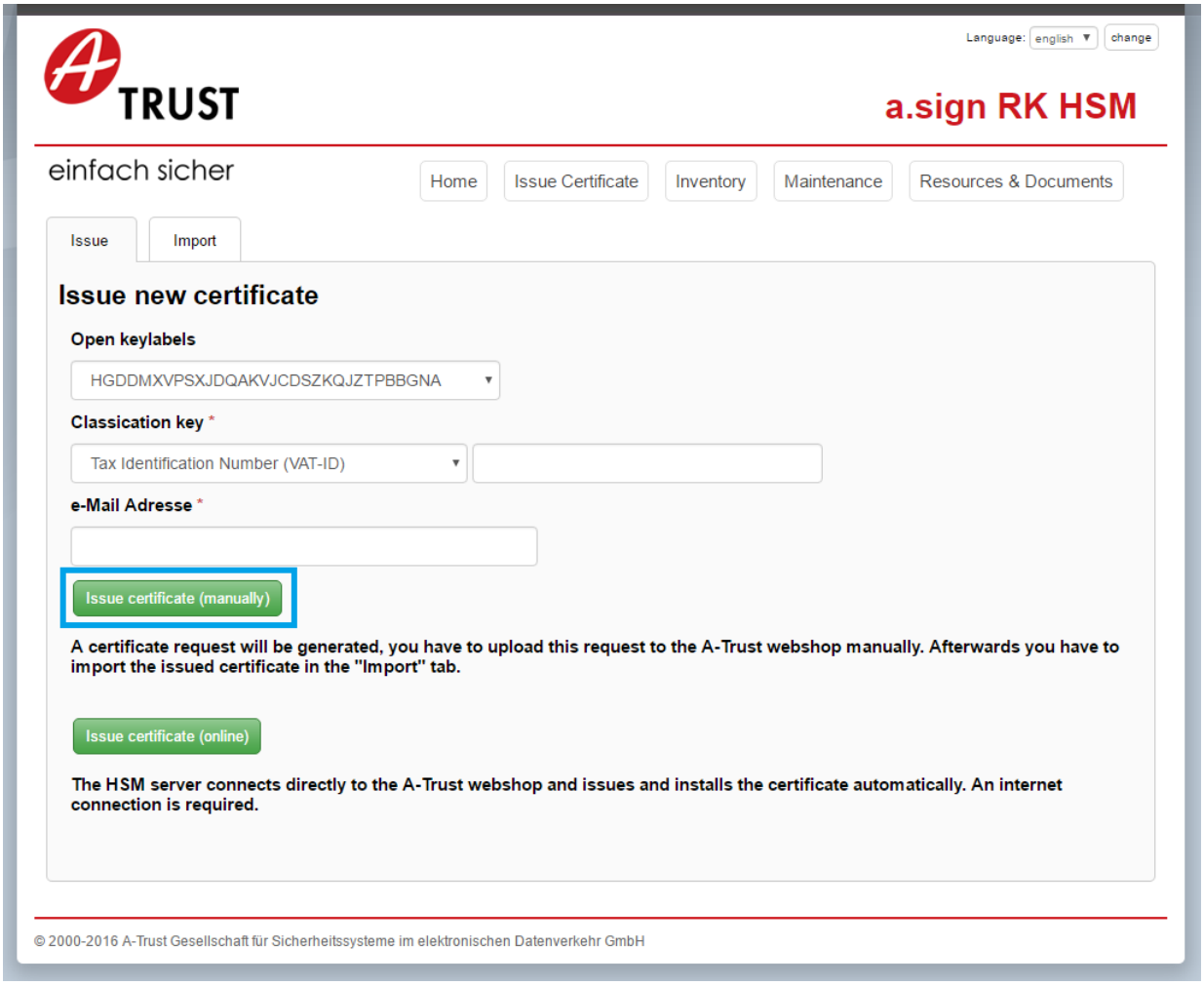
Open the a.sign RK HSM website by entering its IP address in the web browser.

Select the menu item Issue Certificates. The figure below shows this function highlighted in blue.



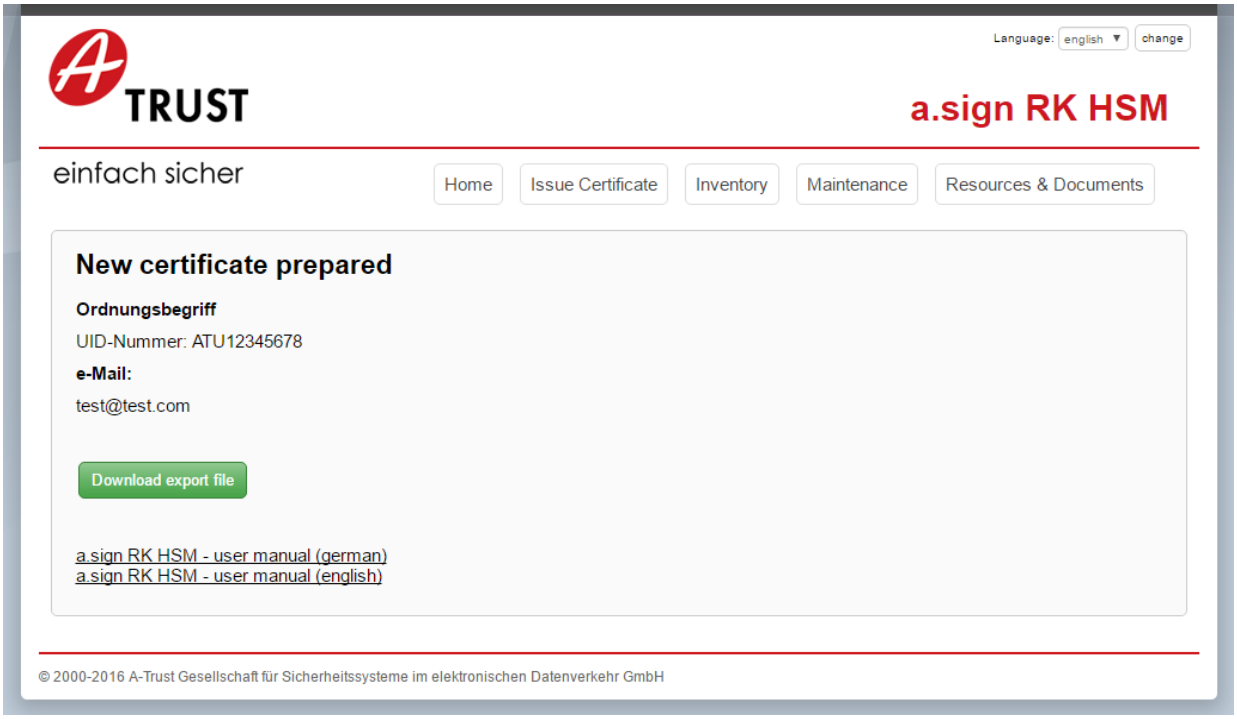
On the following page the data which will appear in the a.sign RK HSM certificate is entered. The certificate type is selected from the dropdown menu **Classification Key**. The choices available are: Value-Added Tax Identification Number (VAT-ID), Global Location Number (GLN), and Tax Number. Additionally, the adjacent text field must be filled with the value corresponding to the type. This field simple validation checks to ensure that the format is correct.

After entering the E-Mail address the certificate request can be generated via the button **Issue Certificate (manually)**.



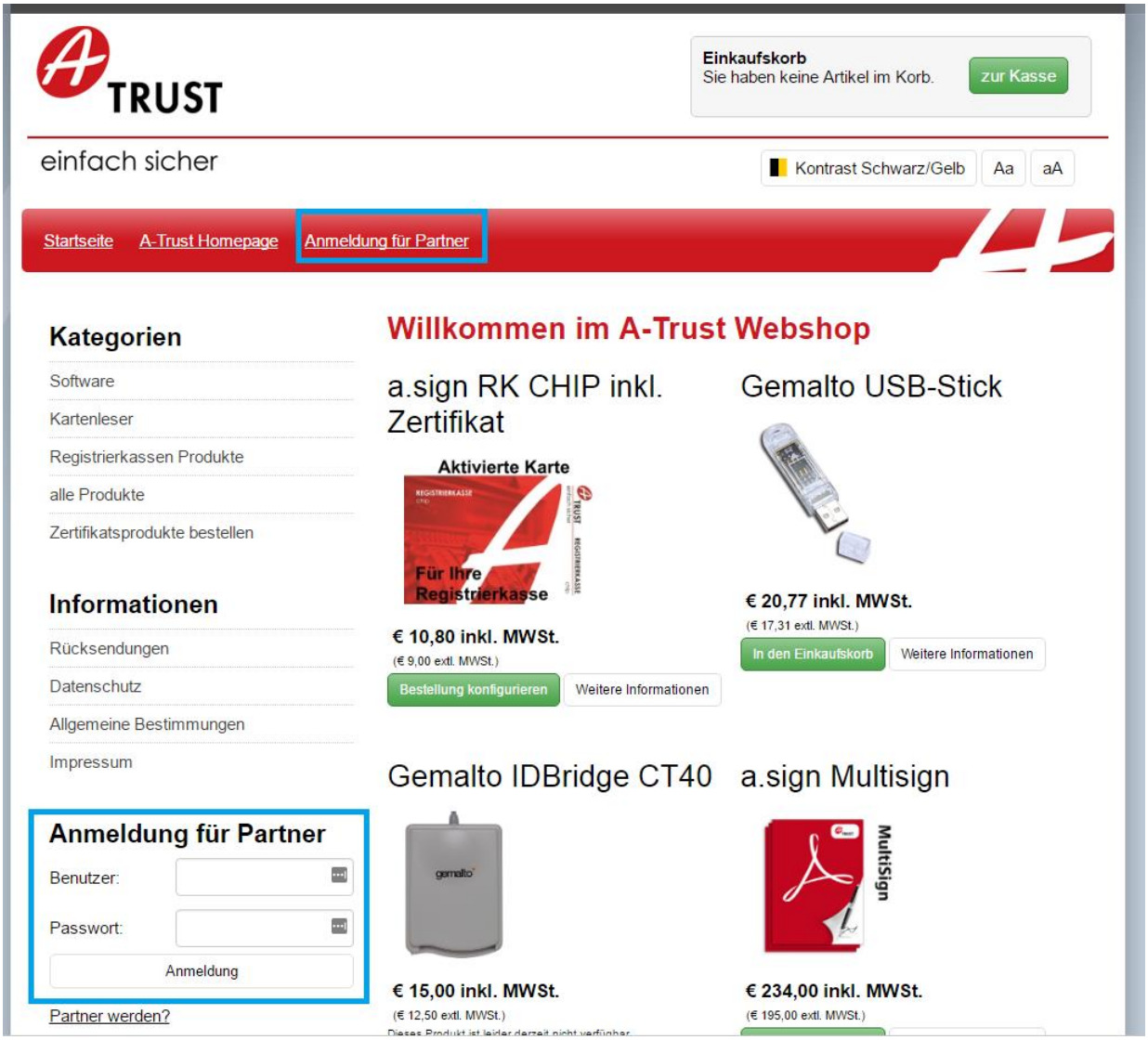
The value in the field keylabel (here HGDDMX…BGNA) is used to select the key to sign with over the REST interface.

On the next page you see a summary of the certificate request and can download it. Click on **Donwload export file** to download the certificate request.

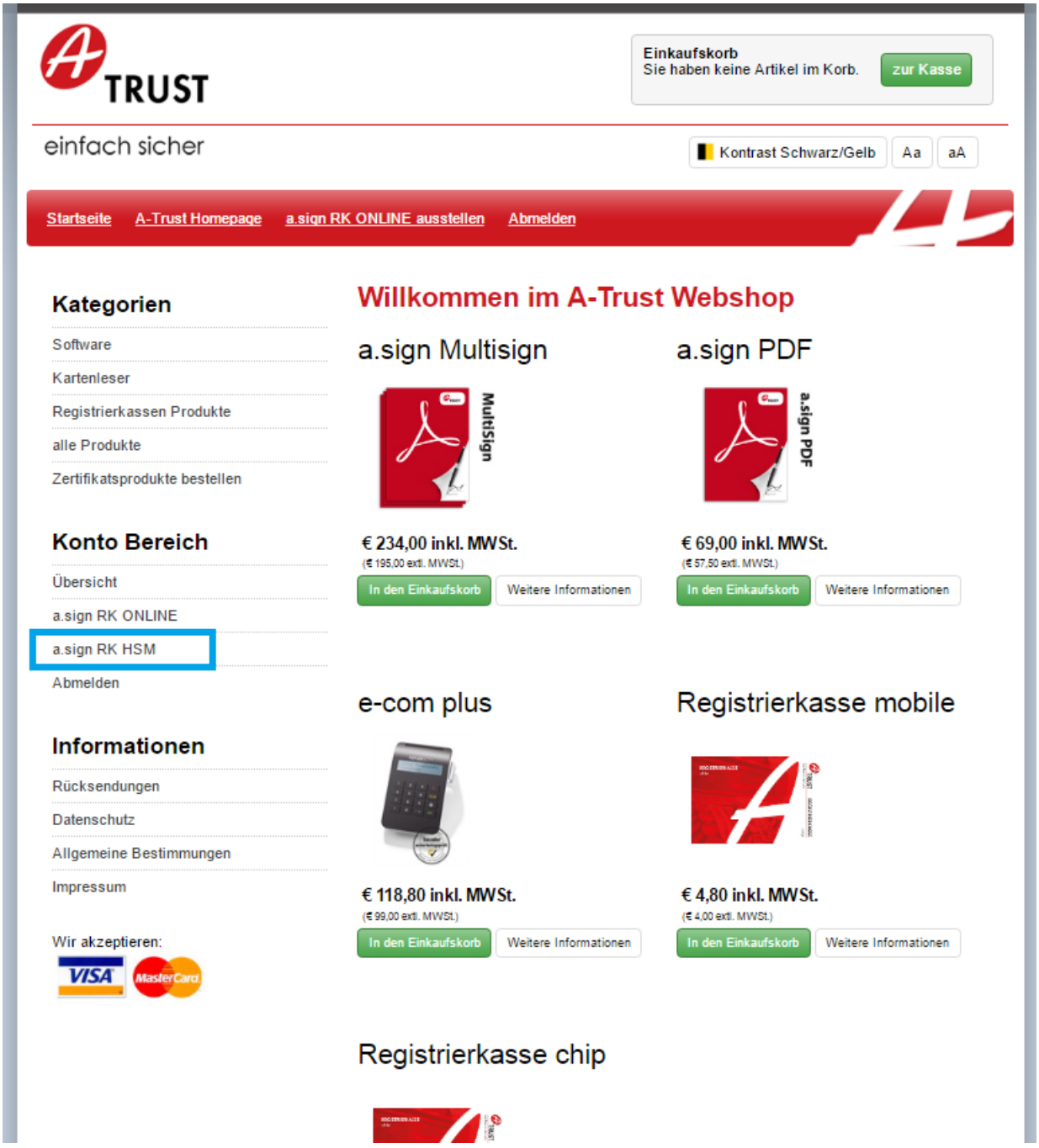


2.2 Issuing a certificate in the A-Trust Webshop

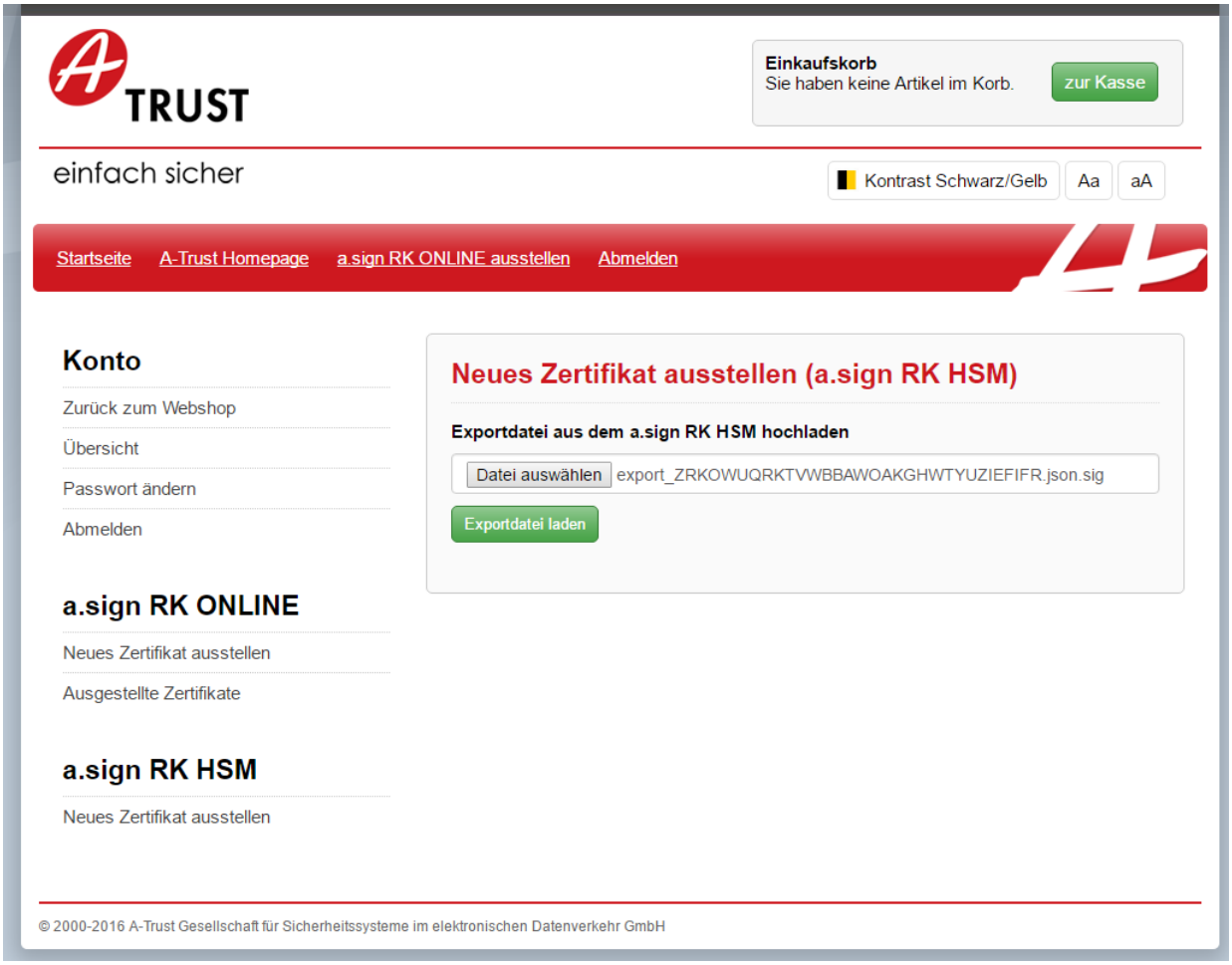
Use your login credentials to sign in to the A-Trust Webshop (https://www.a-trust.at/shop). In the following screenshot the sign-in functions are marked in blue. You can use either of these to login.



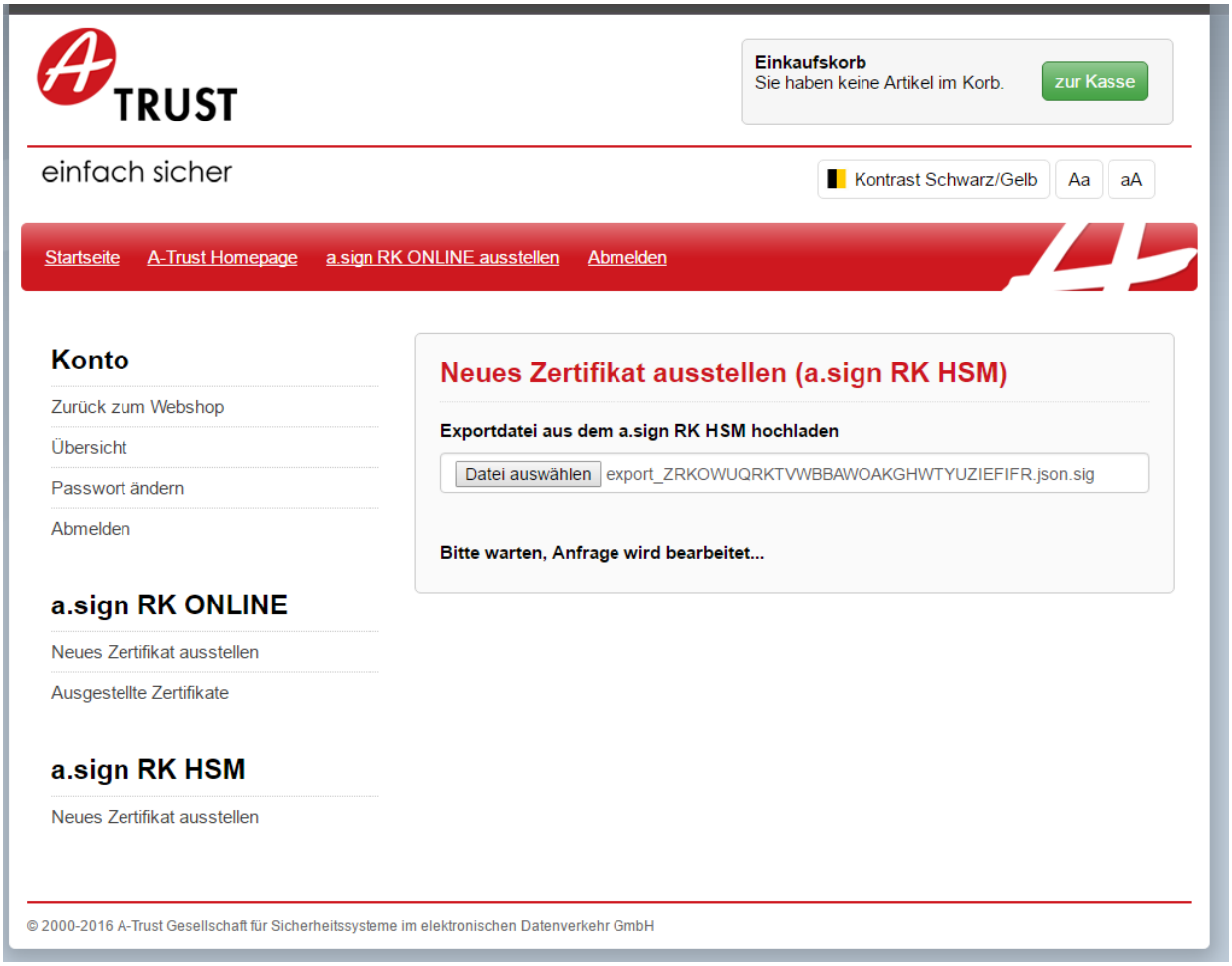
After successful login, the menu item **a.sign RK HSM** becomes visible (marked in blue in the screenshot) on the left-hand side under **Konto Bereich**. Select this menu item to start issuing a certificate.



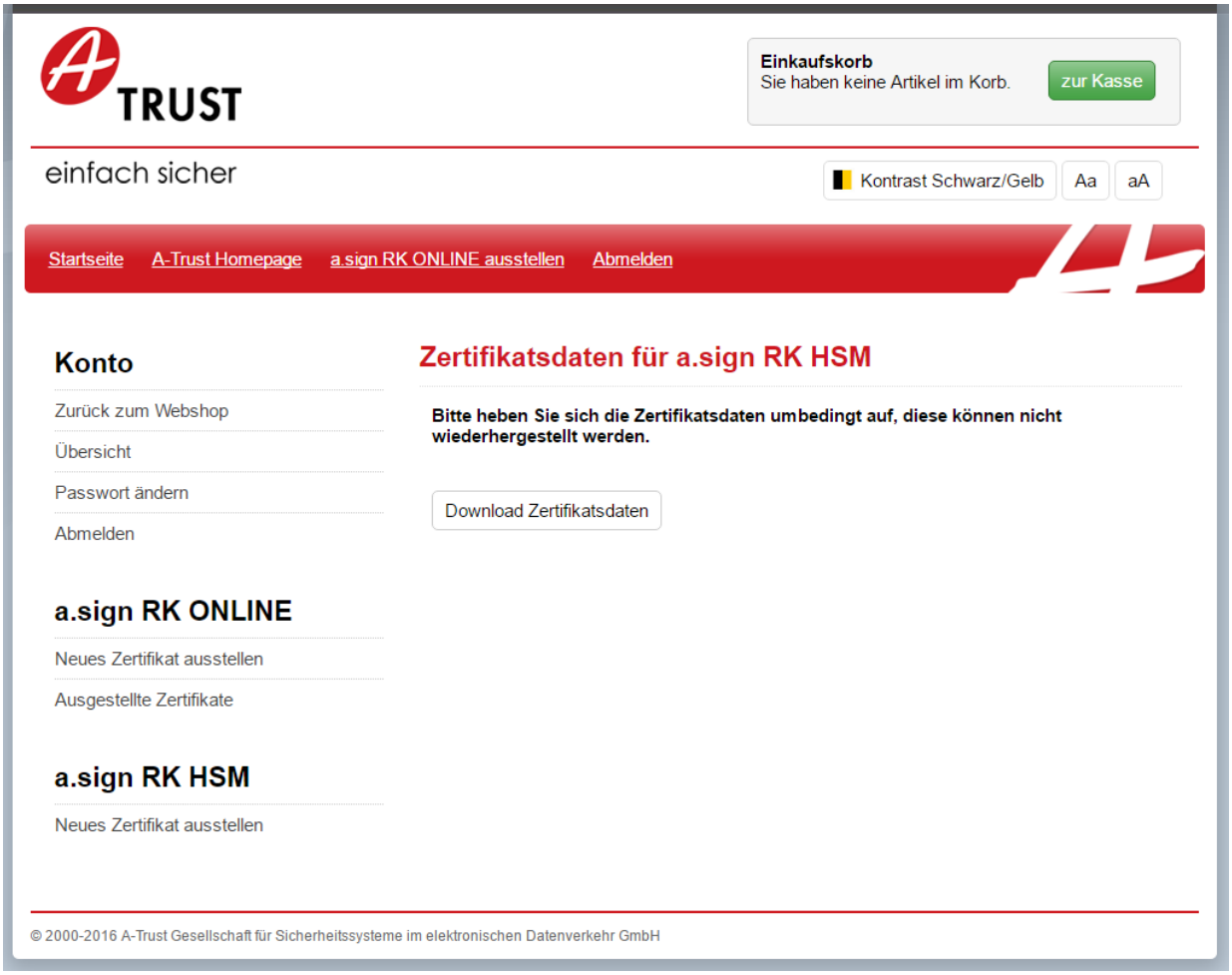
On the following page, choose the certificate request you created earlier and then click on the button **Exportdatei laden**.



In place of the button, the text **Bitte warten, Anfrage wird bearbeitet** appears. A certificate is now generated. This can take a few seconds. After successful processing you are redirected to the next page automatically.

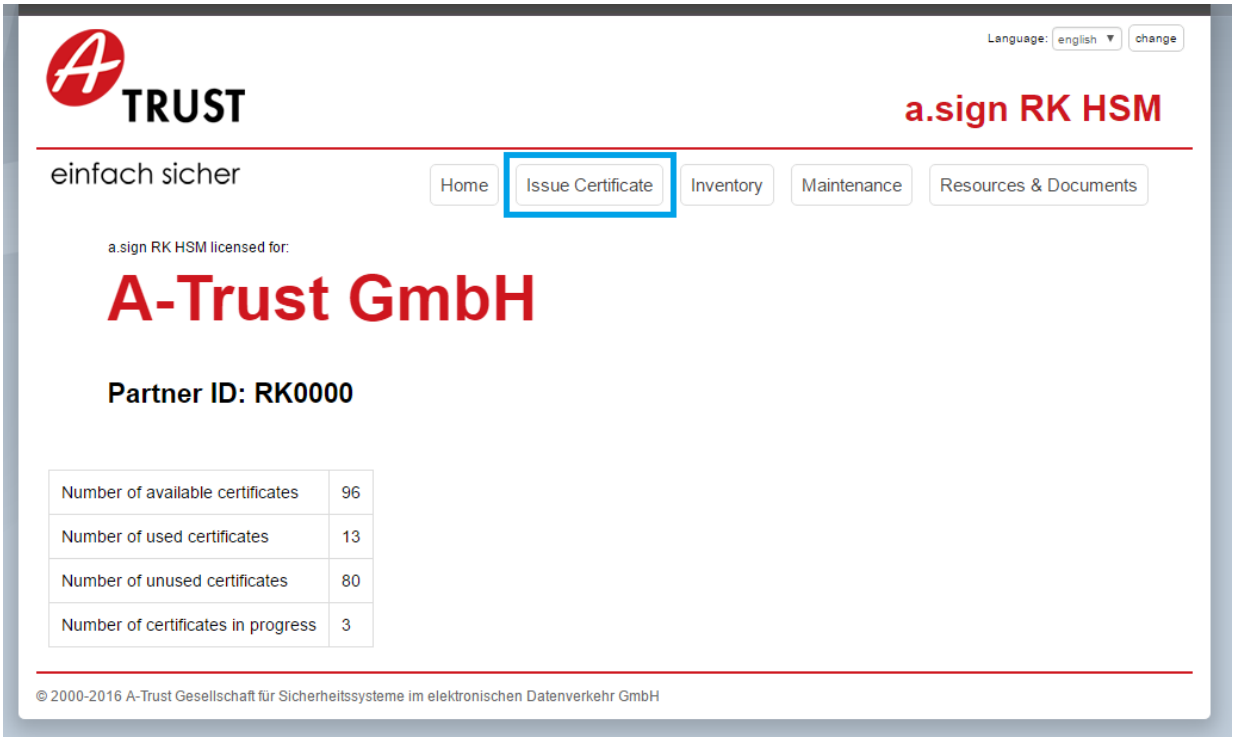


On the following page load the certificate data using the button **Download Zertifikatsdaten**. This data will be required in the next step where you load it into your HSM.

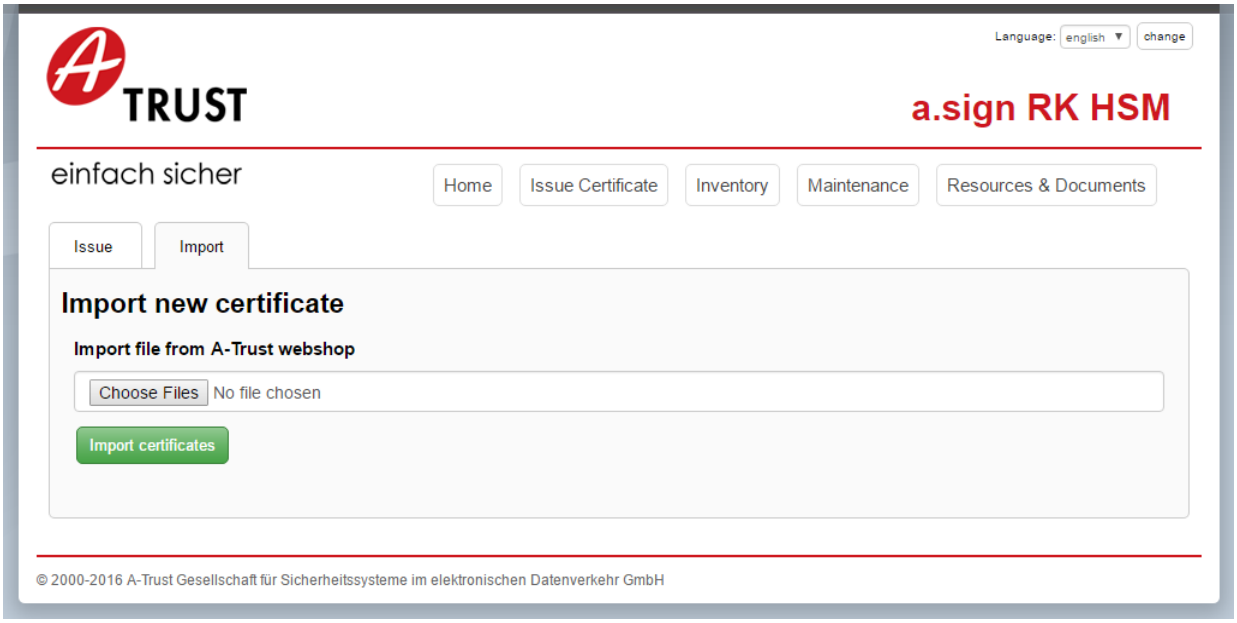


2.3 Import Certificate Data into a.sign RK HSM

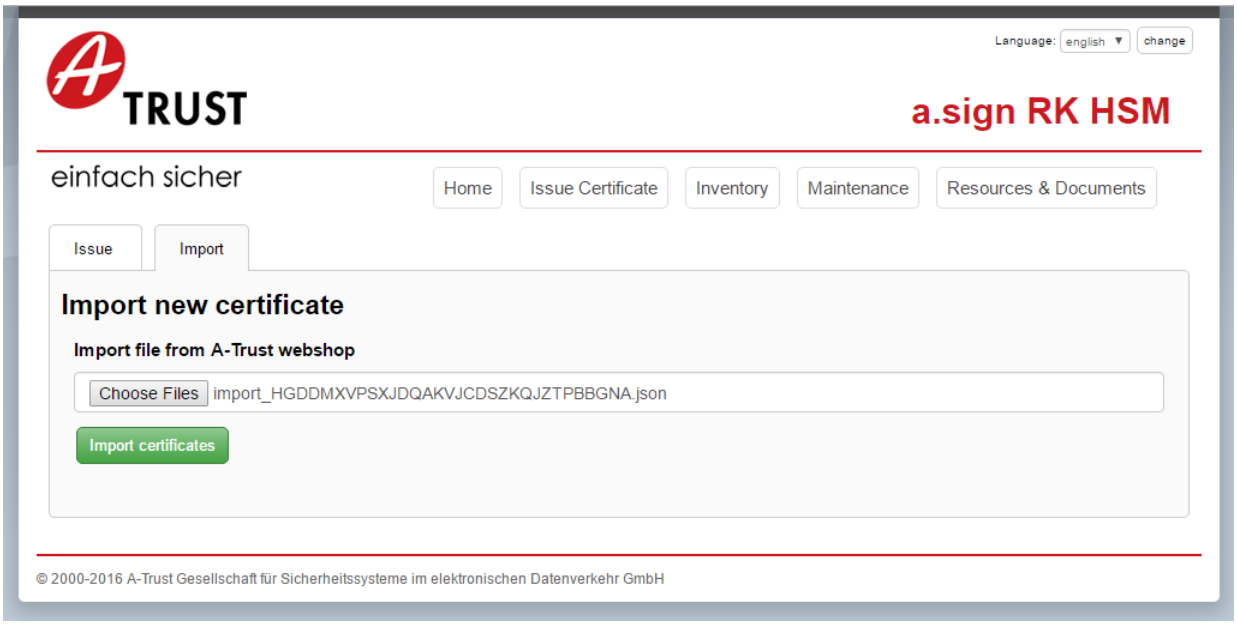
Navigate to the a.sign RK HSM page and select the menu item Issue Certificate. This is shown marked in blue in the following screenshot.



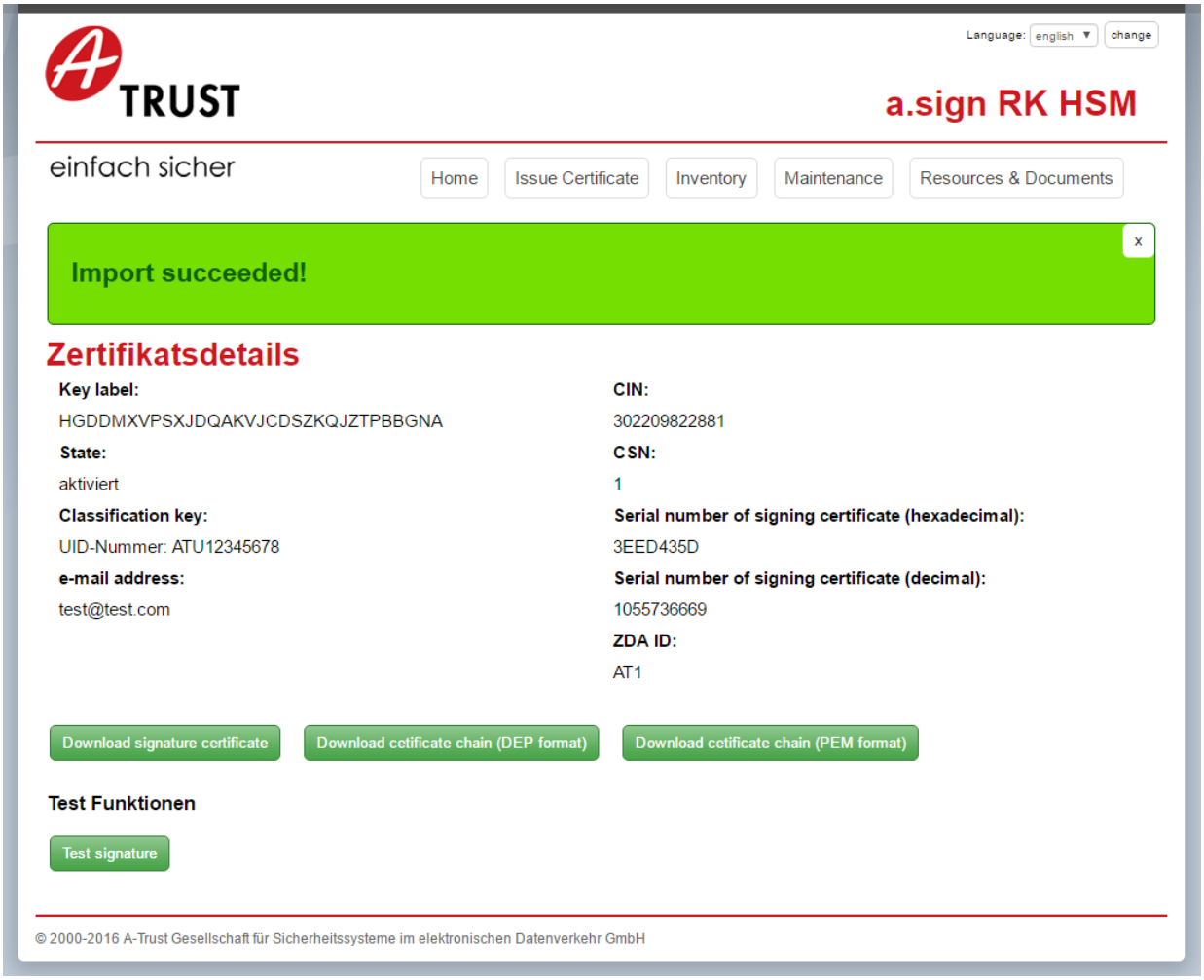
On the next page choose the menu item Import. This is shown marked in blue in the following screenshot.



On the next page choose the certificate file you generated in section 2.2 and then click on the button **Import certificates**.



If the import is successful you will see the following screen. The certificate with the given keylabel is now operational.

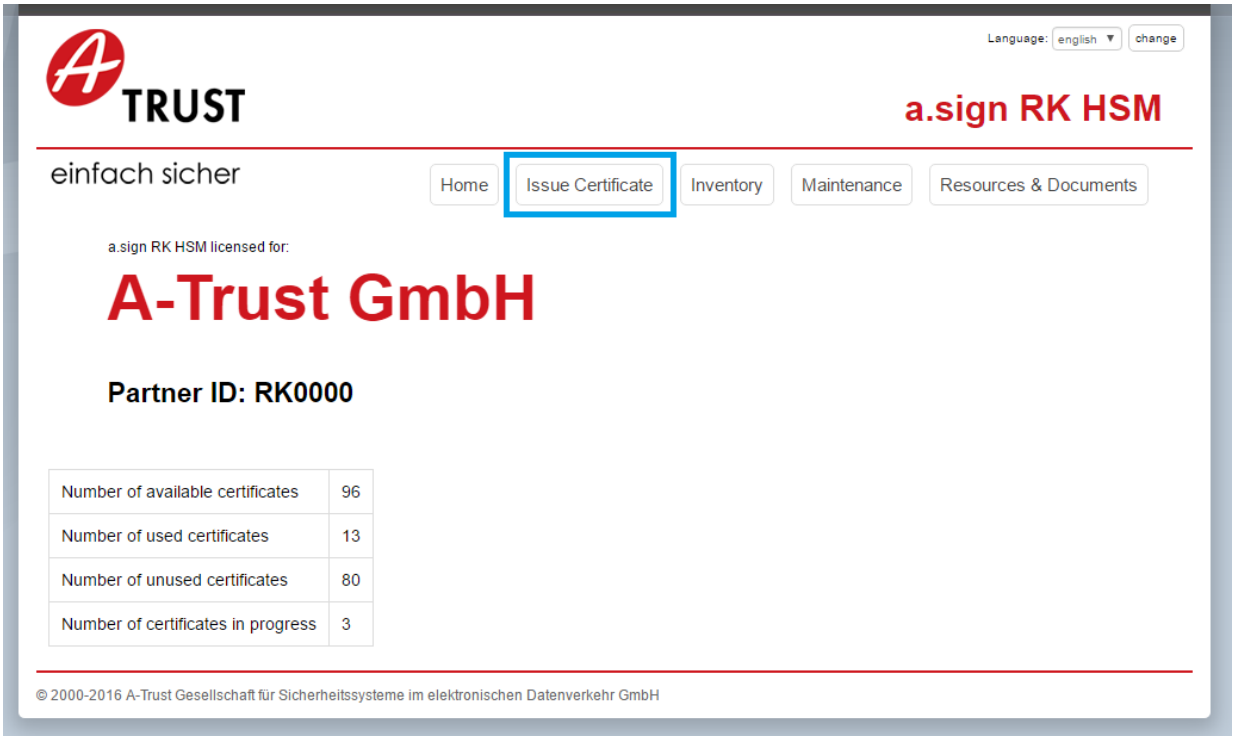


3 Create a new account (automatically)

If your a.sign RK HSM has internet access, certificates can be issued using the following simplified process.

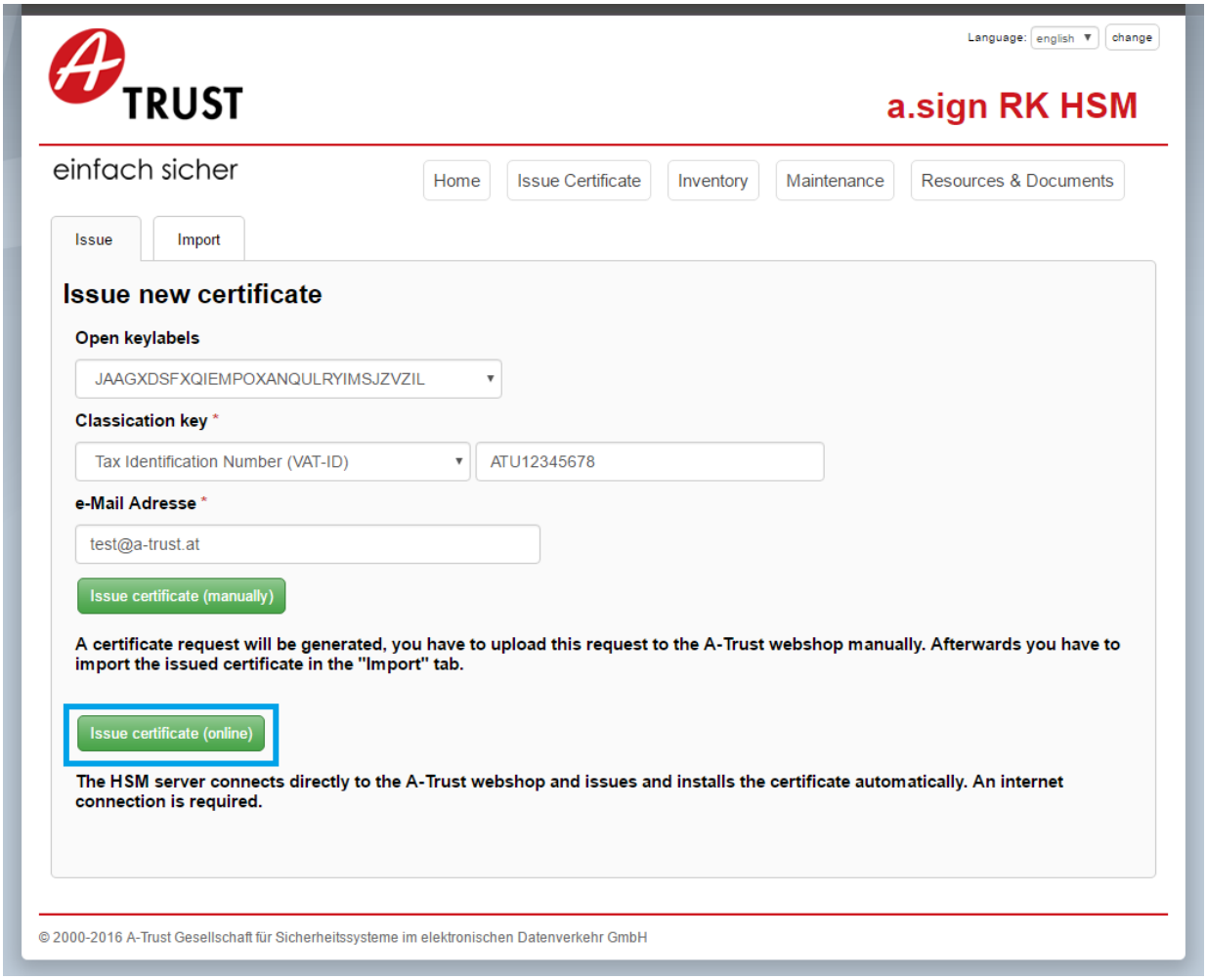
Navigate to the a.sign RK HSM website by entering the IP address of your HSM in your web browser – this may have the form http://192.168.1.1/ – where of course you must enter the IP address of your HSM.

Select the menu item Issue Certificate. This is marked in blue in the following screenshot.

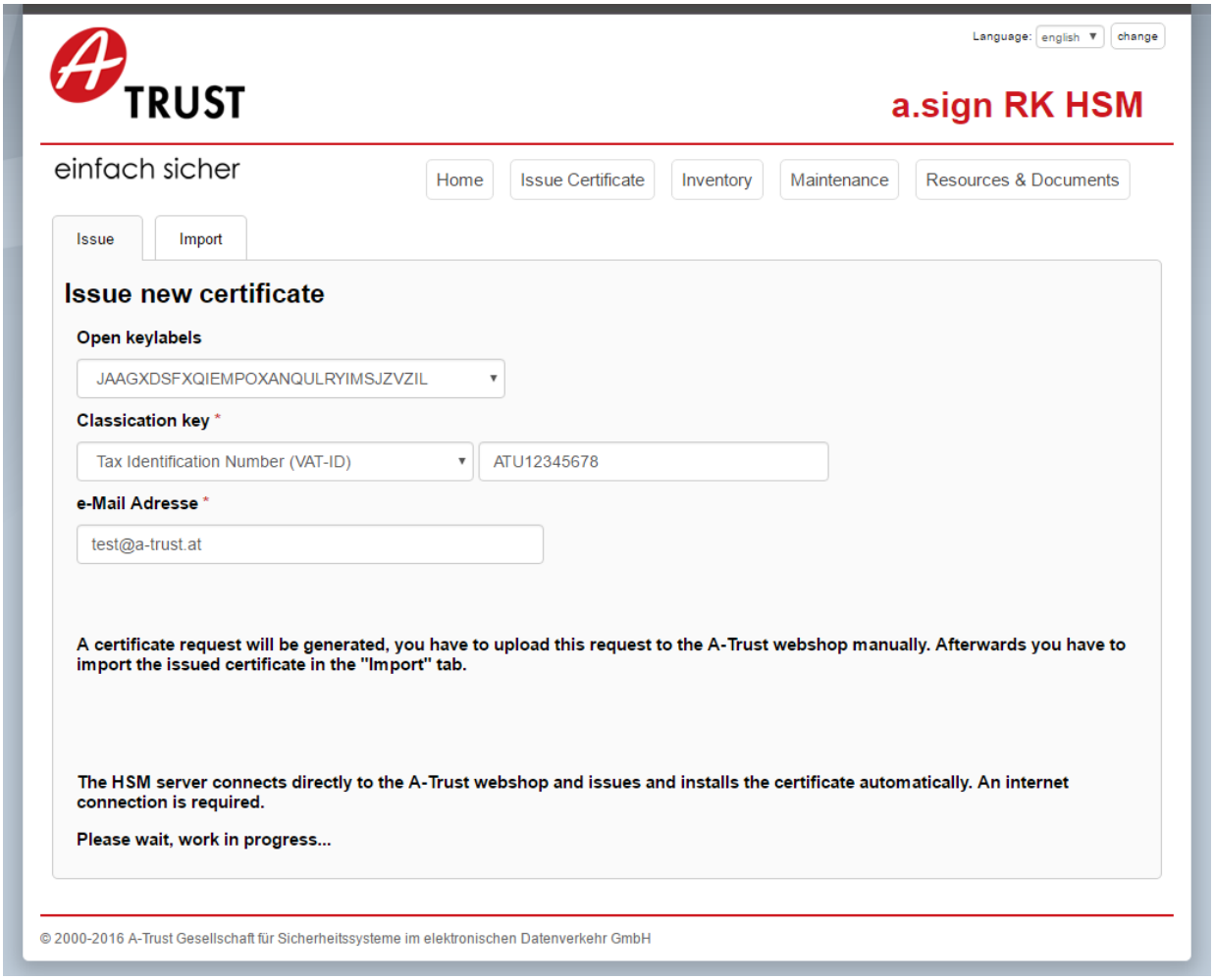


On the following page the data which will appear in the a.sign RK HSM certificate is entered. The certificate type is selected from the dropdown menu **Classification Key**. The choices available are: Value-Added Tax Identification Number (VAT-ID), Global Location Number (GLN), and Tax Number. Additionally, the adjacent text field must be filled with the value corresponding to the type. This field simple validation checks to ensure that the format is correct.

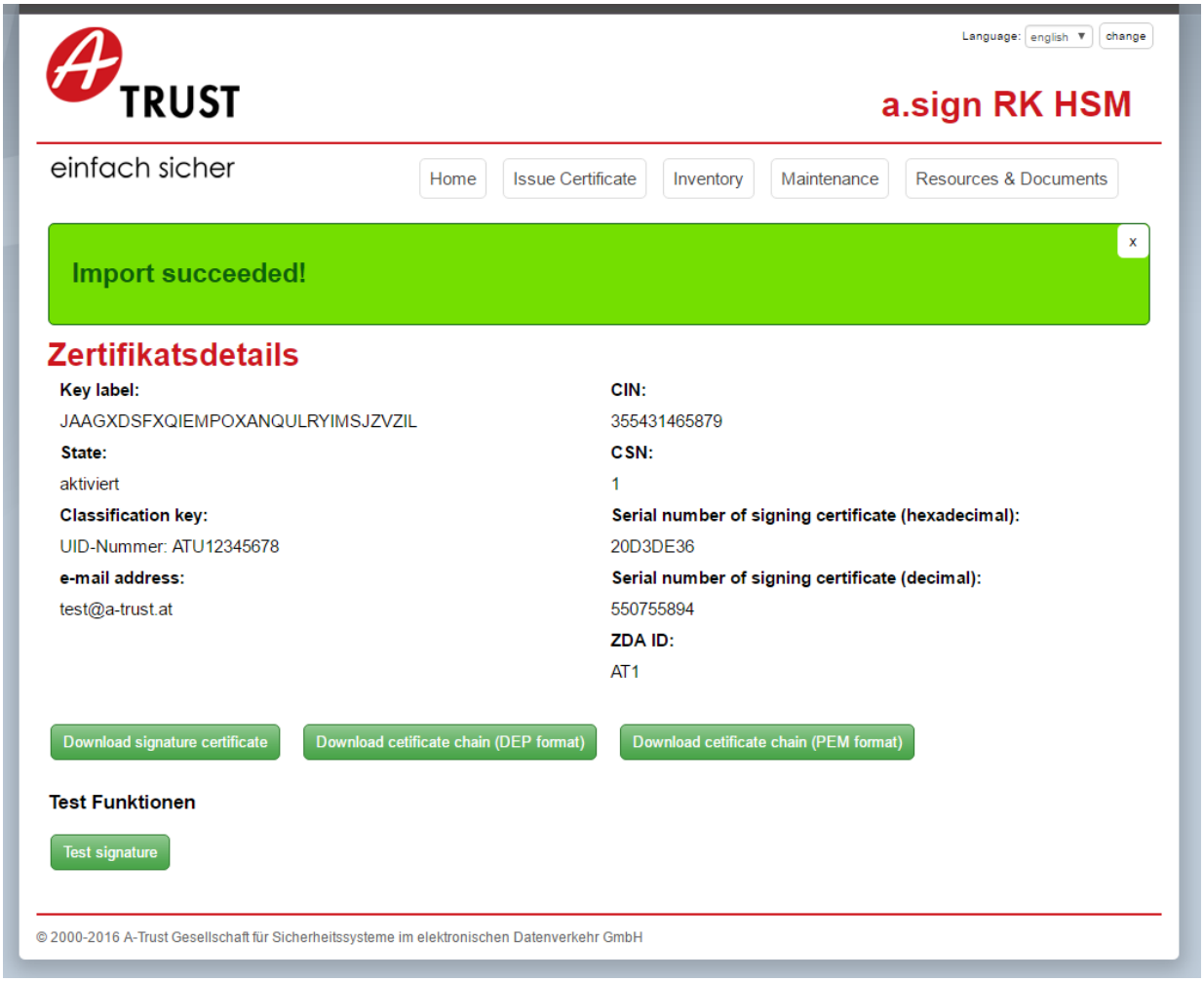
After entering the E-Mail address the certificate request can be generated via the button **Issue certificate (online)**.



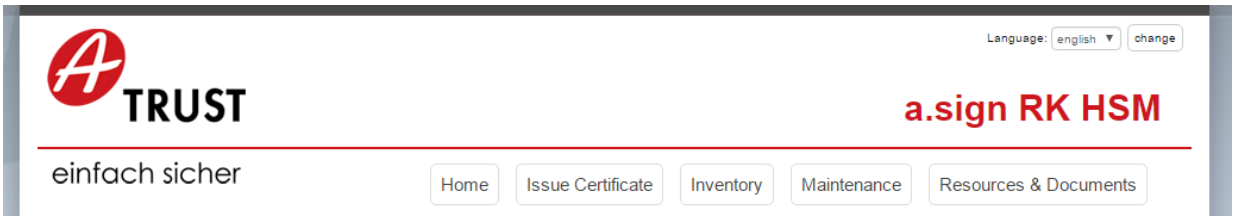
The screen now shows the message **Please wait, work in progress…** The processing can take a number of seconds.



Finally the certificate details screen is shown. The certificate has now been issued and the account can be used.



4 Inventory



The taskbar item Inventory provides an overview of all keys (keylabels). Issued certificates together with their corresponding classification keys (e.g. ATU12345678) can be seen. It is also possible to filter according to predefined search terms, or to see how many keys are still available.