



Handout für die Beantragung eines SSL-Zertifikats (Server)

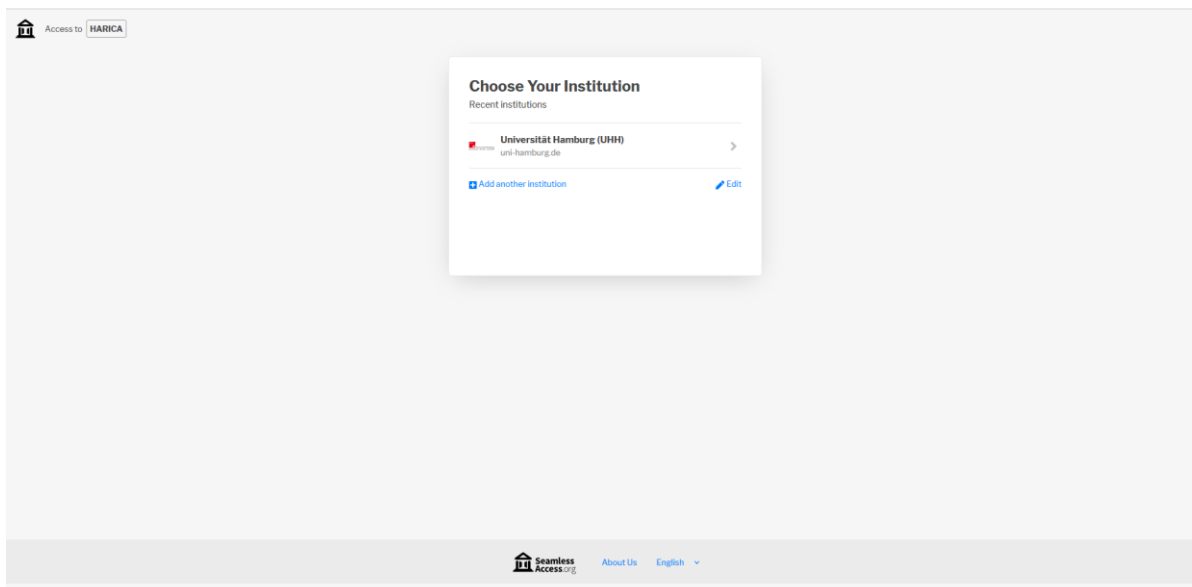
Die Beantragung von SSL Zertifikaten für Server erfolgt eigenständig über die Zertifizierungsstelle Hellenic Academics and Research Institutions Certification Authority (Harica).

1. Anmeldung über „Academic Login“ bei Harica Certificate Manager

Öffnen Sie das Webportal des Zertifikatsmanagers Harica unter <https://cm.harica.gr/> in Ihrem Webbrowser.

Wählen Sie nun die Option „Academic Login“ und im nächsten Bildschirm, unter „Choose Your Institution“, dann „Universität Hamburg (UHH)“ aus.

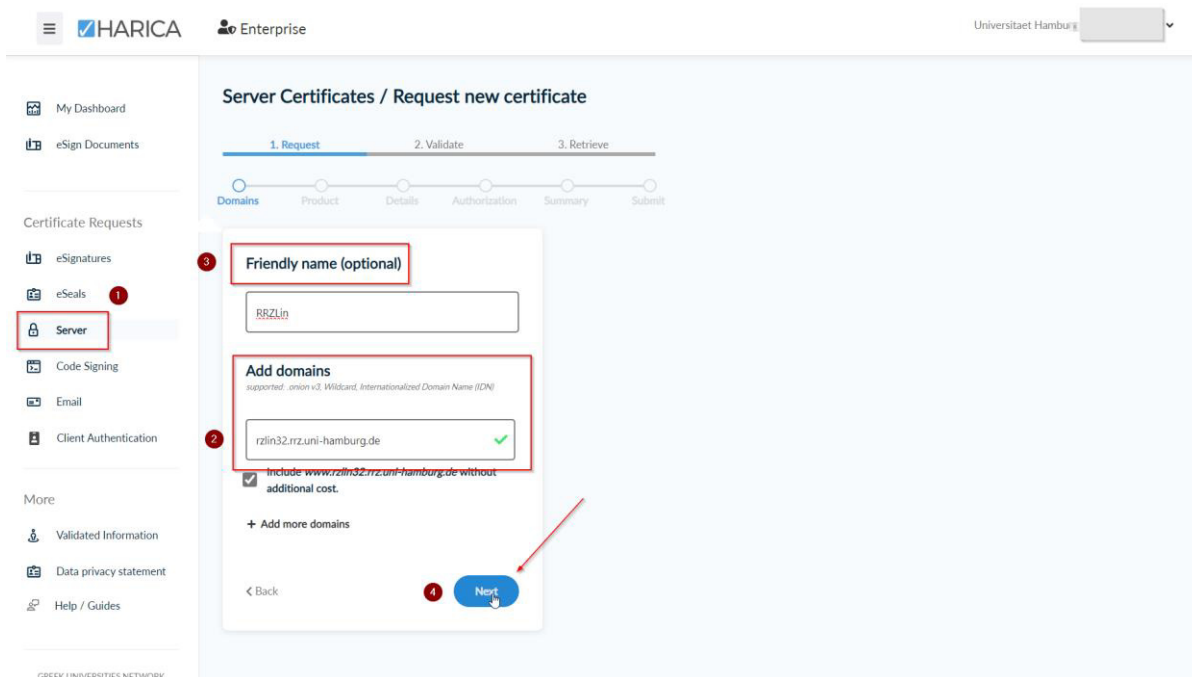
The screenshot shows the HARICA login page. The browser address bar displays <https://cm.harica.gr/login?returnUrl=%2F>. The page header includes the HARICA logo and the text "EN | GR". The main content area features a "Login" section with the text "New to HARICA? Sign Up". Below this are two input fields: "Email address" (with the placeholder "Type your email address") and "Password" (with the placeholder "Type your password" and a toggle icon). A "Forgot password?" link is located below the password field. There are three login buttons: a blue "Login" button, a grey "Academic Login" button (highlighted with a red circle and the number 1), and a white "Sign in" button with a Google logo. The footer contains the text "GREEK UNIVERSITIES NETWORK (GUnet)" and "General Commercial Registry Number: 160729401000".



Sie gelangen nun zu der Seite „My Dashboard“.

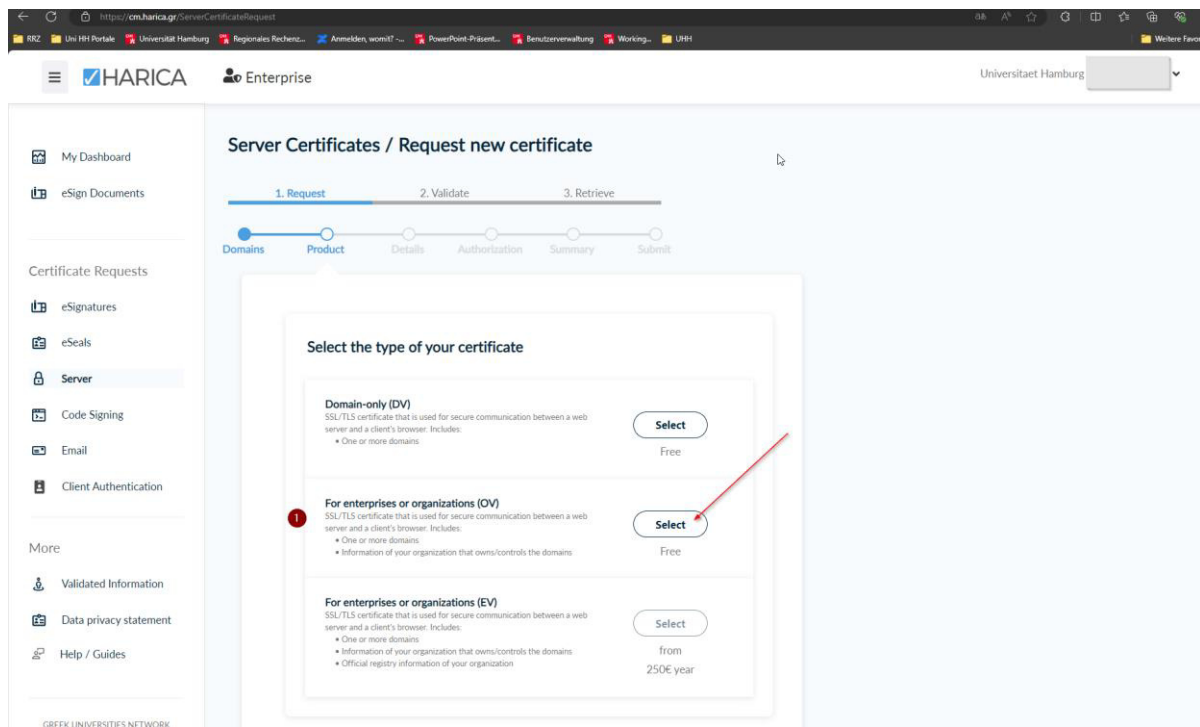
1. Domains:

Navigieren Sie zu „Server“ und tragen dort den vollen Domain Namen ein (stellen Sie sicher, dass Sie den korrekten Domain Namen verwenden – sollte ein nicht der UHH zugehöriger Domainname gewählt werden, wird das Produkt kostenpflichtig), optional können Sie einen „Friendly Name“ als Bezeichnung angeben. Betätigen Sie abschließend die Schaltfläche „Next“.

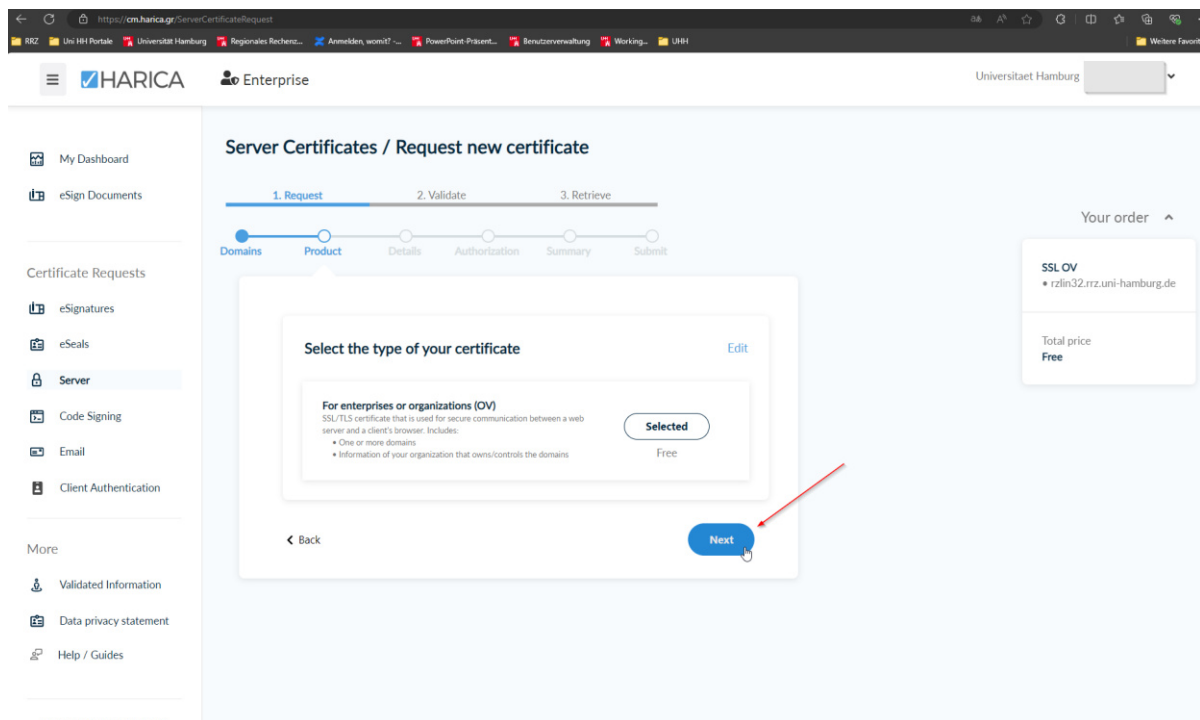


1b. Product:

Wählen Sie das Produkt „For enterprises or organizations (OV)“.

**1b. Product:**

Bestätigen Sie Ihre Produktauswahl durch betätigen der Schaltfläche „Next“.



1c Details:

Bestätigen Sie die „*Organization Information*“ durch betätigen der Schaltfläche „Next“.

The screenshot shows the HARICA 'Request new certificate' page. The progress bar indicates the 'Details' step is active. The 'Organization information' form contains the following details:

- Legal name:** Universitaet Hamburg
- Country:** DE
- State or province:** Hamburg

A red arrow points to the 'Next' button at the bottom right of the form. The 'Your order' summary on the right shows:

- SSL OV** • rzlin32.rzz.uni-hamburg.de
- Total price:** Free

1d. Authorization:

Bestätigen Sie die Nutzungsvereinbarungen und betätigen abschließend die Schaltfläche „Next“.

The screenshot shows the HARICA 'Request new certificate' page at the 'Authorization' step. The 'Review the application before submitting' form displays the following details:

- Certificate Type:** SSL OV
- Service Duration:** 1 year
- Domains:** rzlin32.rzz.uni-hamburg.de
- Organization Details:**
 - Legal name:** Universitaet Hamburg
 - State or province:** Hamburg
 - Country:** DE

Below the details, there is a checkbox and a declaration: "I, [redacted] declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#)." The checkbox is checked. A red arrow points to the 'Next' button at the bottom right of the form.

1e. Summary:

Wählen Sie entweder A) *“Auto-generate CSR”* wählen ein Passwort („*Select a passphrase*“) und wiederholen die Eingabe des Passworts („*Repeat passphrase*“). Bestätigen Sie, a) dass nur Sie das Passwort kennen und b) die Vereinbarung zu Nutzung und Datenschutz. Betätigen Sie abschließend die Schaltfläche *„Generate private key CSR, and submit request“* zum Einreichen Ihres Antrags.

*Hinweis: Bitte beachten Sie, dass **Passwort wieder aus dem Zertifikat zu entfernen**. Andernfalls starten Linux Webserver (z.B.: Apache, nginx) nicht ohne manuelle Eingabe des Passworts. Bei einem reboot würde der Webserver erst nach Passworteingabe starten.*

Mit dem Tool „openssl“ lässt sich die Passphrase auch entfernen, dafür muss ein neuer Key erzeugt werden: `openssl rsa -in cert.key -out cert_new.key`

Es ist daher ratsam, das manuelle Hochladen des CSR „*Submit CSR manually*“ zu verwenden. Ein CSR kann auch über das Webtool <https://csr.rrz.uni-hamburg.de/> erzeugt werden.

The screenshot shows the 'Submit Request' page of the HARICA web interface. The page has a top navigation bar with tabs: Domains, Product, Details, Authorization, Summary, and Submit (which is active). On the left, there is a sidebar with 'Certificate Requests' and a list of services: eSignatures, eSeals, Server (highlighted), Code Signing, Email, and Client Authentication. Below this is a 'More' section with links to Validated Information, Data privacy statement, and Help / Guides. The main content area is titled 'Submit Request' and includes a sub-header 'What is a CSR?'. It offers two options: 'Auto-generate CSR' (selected) and 'Submit CSR manually'. A note states: 'You will create a Private Key in your browser and your CSR will be auto-generated.' Below this, there are dropdowns for 'Algorithm' (RSA (default)) and 'Key size' (2048 (default)). There are two password input fields: 'Set a passphrase' and 'Repeat passphrase', both with red numbered icons (2 and 3) and eye icons. A checkbox (4) is checked, with the text: 'I understand that this passphrase is under my sole knowledge and HARICA does not have access to it.' Below that, another checkbox (5) is checked, with the text: 'I, [redacted], declare that I read and agree with, by submitting this request, the Terms of Use and the Certification Practices of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the Data Privacy Statement.' At the bottom, there is a 'Back' link and a large blue button labeled 'Generate Private Key, CSR, and submit order' with a red numbered icon (6). On the right side, there is a 'Your order' summary box showing 'SSL OV' for 'rzlin32.rrz.uni-hamburg.de' and a 'Total price Free'.

Oder B) *“Submit CSR manually”* und hinterlegen Sie Ihren CSR manuell, bestätigen die Vereinbarung zu Nutzung und Datenschutz und betätigen abschließend die Schaltfläche *„Submit request“*

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Submit Request

What is a CSR?

Auto-generate CSR or **1 Submit CSR manually**

2 Use your (already created) CSR and submit it here.

Paste your CSR here

3 ☒ I declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices of HARICA](#). I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

[Back](#) **4** [Submit request](#)

Your order

SSL OV
• rzln32.rlz.uni-hamburg.de

Total price
Free

1f. Download Private Key:

Laden Sie Ihren „Private Key“ herunter und bestätigen dies.

Abschließend betätigen Sie die Schaltfläche „Go back to MyDashboard“

1. Request 2. Validate 3. Retrieve

Request submitted successfully

You have generated a Private Key and your certificate order has been submitted.

You must :

1 Download your Private Key.

2 ATTENTION: This is the ONLY TIME you can perform this action, you cannot download the Private Key later.

As you have selected OV Certificate in the next steps you have to wait our validators to review your request.

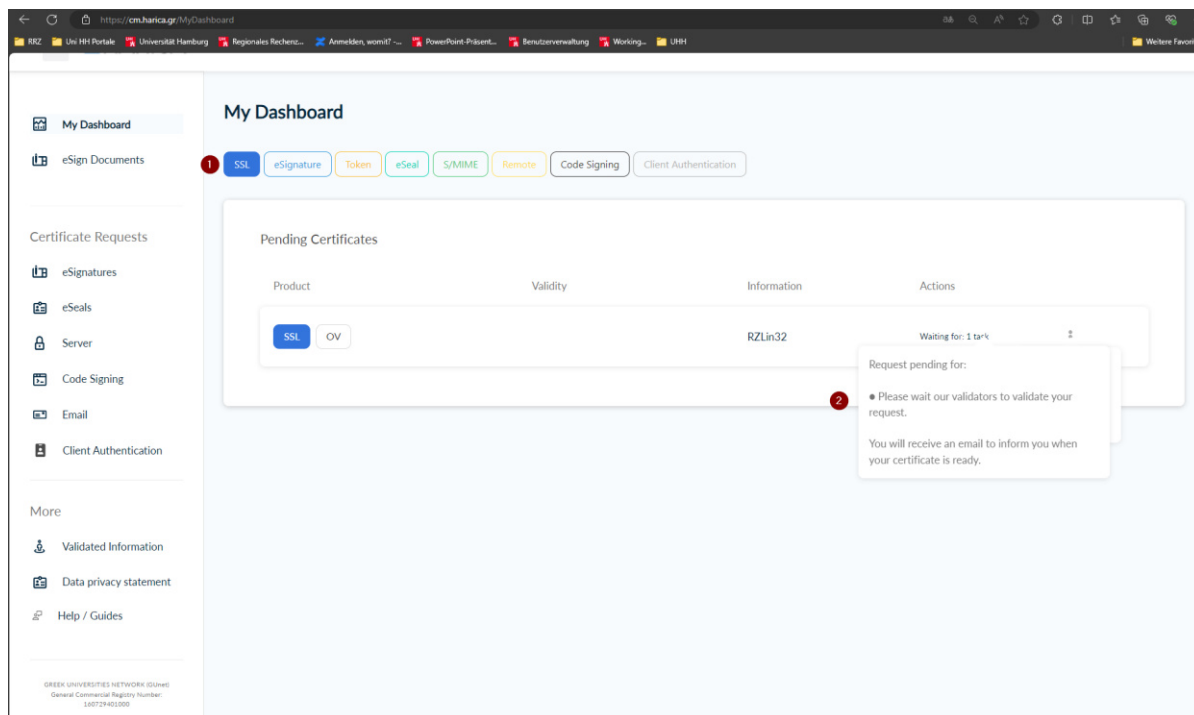
After that you can continue with the certificate issuance process.

3 ☒ I have downloaded my private Key

4 [Go back to dashboard](#)

3. MyDashboard – Status Zertifikat:

Über die Schaltflächen können Sie nach den verschiedenen Zertifikats Typen filtern. Unter „SSL“ sehen Sie den Status Ihrer Beantragung. Der Antrag wird geprüft und Sie werden per E-Mail informiert wenn das Zertifikat fertig ist.



4. Beantragung Freigabe:

Bitte beantragen Sie nun die Freischaltung Ihres beantragten Server-Zertifikats mit dem „Webformular zur Freischaltung des beantragten Serverzertifikats : RRZ : Universität Hamburg“ untere <https://www.rrz.uni-hamburg.de/services/sicherheit/pki/teilnehmerservicestellen/freischaltenserver.html>

Nach erfolgter Freigabe kann das SSL Zertifikat heruntergeladen werden unter „My Dashboard“

The screenshot shows the HARICA 'My Dashboard' for an 'Enterprise' user. The dashboard is titled 'My Dashboard' and features a sidebar with navigation links: My Dashboard, eSign Documents, Certificate Requests, eSignatures, eSeals, Server, Code Signing, Email, Client Authentication, and More. The main content area displays 'Valid Certificates' in a table. The table has columns for Product, Validity, Information, and Actions. One certificate is highlighted with a blue border and a red arrow pointing to the 'Download' button in the Actions column. Below the 'Valid Certificates' section, there is a 'Ready Certificates' section with a table containing one row for an S/MIME certificate and an 'Enroll your Certificate' button.

Product	Validity	Information	Actions
S/MIME	09/01/2027	E=...@uni-ham...	Download
SSL OV	10/01/2026	RZLin32	Download
S/MIME	09/01/2027	E=...@uni-ham...	Download

Product	Validity	Information	Actions
S/MIME			Enroll your Certificate

Und das Zertifikat auf dem Server installiert werden mit Hilfe folgender Anleitung:

<https://www.rrz.uni-hamburg.de/services/sicherheit/pki/hilfe-fuer-administratoren/installieren.html>