

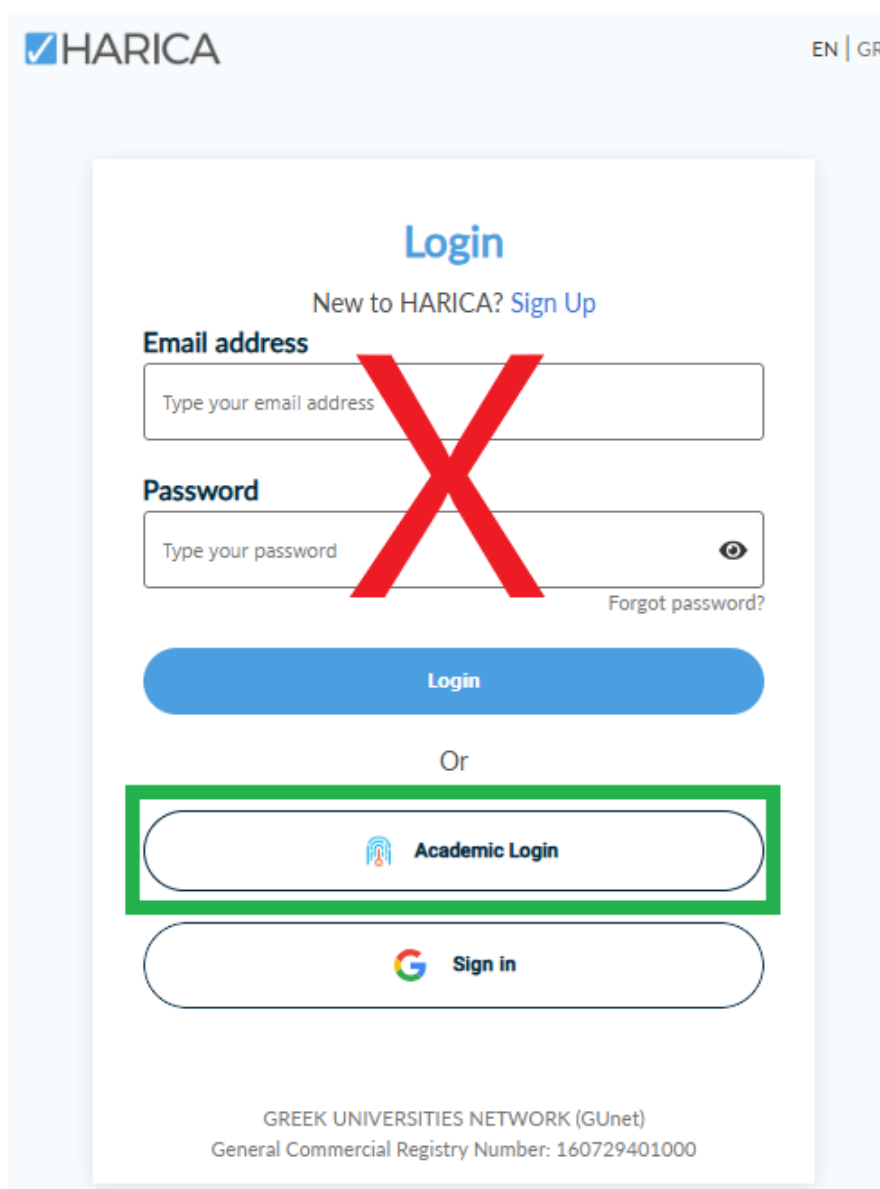
Inhalt

- I. Aufrufen des HARICA-Portals zur Zertifikatsbeantragung.....1
- II. Anleitung zur Betragung von SSL-Serverzertifikaten.....3

I. Aufrufen des HARICA-Portals zur Zertifikatsbeantragung

1. Rufen Sie folgenden Link auf und klicken Sie dort auf Academic Login

<https://cm.harica.gr/>



✓ HARICA EN | GR

Login

New to HARICA? [Sign Up](#)

Email address

Type your email address

Password

Type your password

[Forgot password?](#)

Login

Or

 **Academic Login**

 **Sign in**

GREEK UNIVERSITIES NETWORK (GUnet)
General Commercial Registry Number: 160729401000

Sie werden dann zu einer Webseite zur Authentifizierung geleitet. Suchen Sie dort nach Ihrer Hochschule (HTW oder Uds) und wählen sie entsprechend aus. Auf der folgenden Seite geben Sie Ihre Benutzerkennung ein und bestätigen sie.


Zugriff auf **HARICA**
Unable to verify returning website

Finden Sie Ihre Institution

Ihre Universität, Organisation oder Firma



Beispiele: Technische Universität, jane.doe@example.edu, TU

☒ Diese Auswahl merken [Mehr erfahren](#)

Hochschule für Technik und Wirtsc...
htw-saarland.de

Universität des Saarlandes
uni-saarland.de

2. Sie gelangen dann auf die Startseite des HARICA-Portals


HARICA
Hochschule fuer Technik und ...

 My Dashboard
  eSign Documents

Certificate Requests
  eSignatures
  eSeals
  Server
  Code Signing
  Email
  Client Authentication

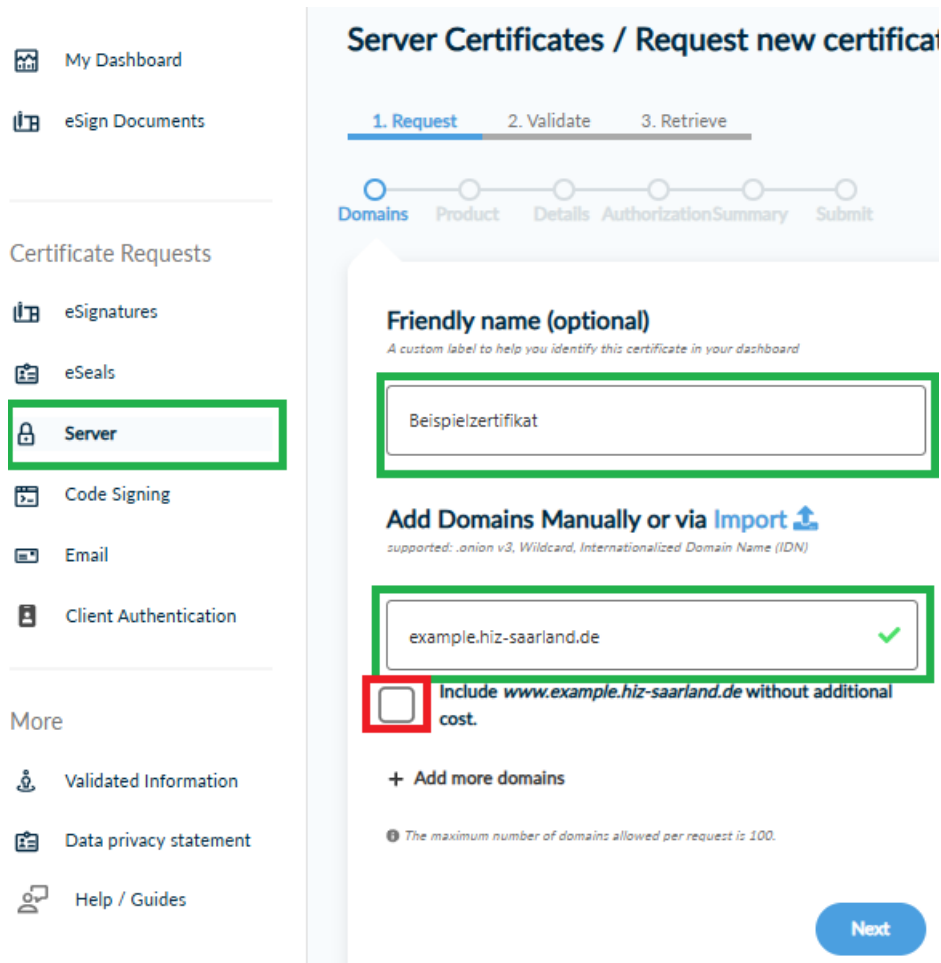
More
  Validated Information
  Data privacy statement
  Help / Guides

My Dashboard

SSL
 eSignature
 Token
 eSeal
 S/MIME
 Remote
 Code Signing
 Client Authentication

II. Anleitung zur Beantragung von SSL-Serverzertifikaten

1. Wählen Sie im Portal auf der linken Seite „**Server**“ aus. Geben Sie dann einen selbstgewählten Anzeigenamen des Antrags (nur sichtbar im Portal) und alle im Zertifikat benötigten Domainnamen ein. Entfernen Sie das Häkchen bei „Include www....“ wenn Sie nicht wirklich diese Namen im Zertifikat benötigen.



My Dashboard

eSign Documents

Certificate Requests

eSignatures

eSeals

Server

Code Signing

Email

Client Authentication

More

Validated Information

Data privacy statement

Help / Guides

Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details AuthorizationSummary Submit

Friendly name (optional)
A custom label to help you identify this certificate in your dashboard

Beispielzertifikat

Add Domains Manually or via Import 
supported: .onion v3, Wildcard, Internationalized Domain Name (IDN)

example.hiz-saarland.de ✓

☐ Include **www.example.hiz-saarland.de** without additional cost.

+ Add more domains

The maximum number of domains allowed per request is 100.

Next

2. Wählen Sie im nächsten Schritt „For enterprises or organisations (OV) aus“

My Dashboard

eSign Documents

Certificate Requests

eSignatures

eSeals

Server

Code Signing

Email

Client Authentication

More

Validated Information

Data privacy statement

Help / Guides

Server Certificates / Request new certificate

1. Request

2. Validate

3. Retrieve

Domains

Product

Details

Authorization

Summary

Submit

Select the type of your certificate

Domain-only (DV)
 SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:
 • One or more domains

Select

Free

For enterprises or organizations (OV)
 SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:
 • One or more domains
 • Information of your organization that owns/controls the domains

Select

Free

For enterprises or organizations (EV)
 SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:
 • One or more domains
 • Information of your organization that owns/controls the domains
 • Official registry information of your organization

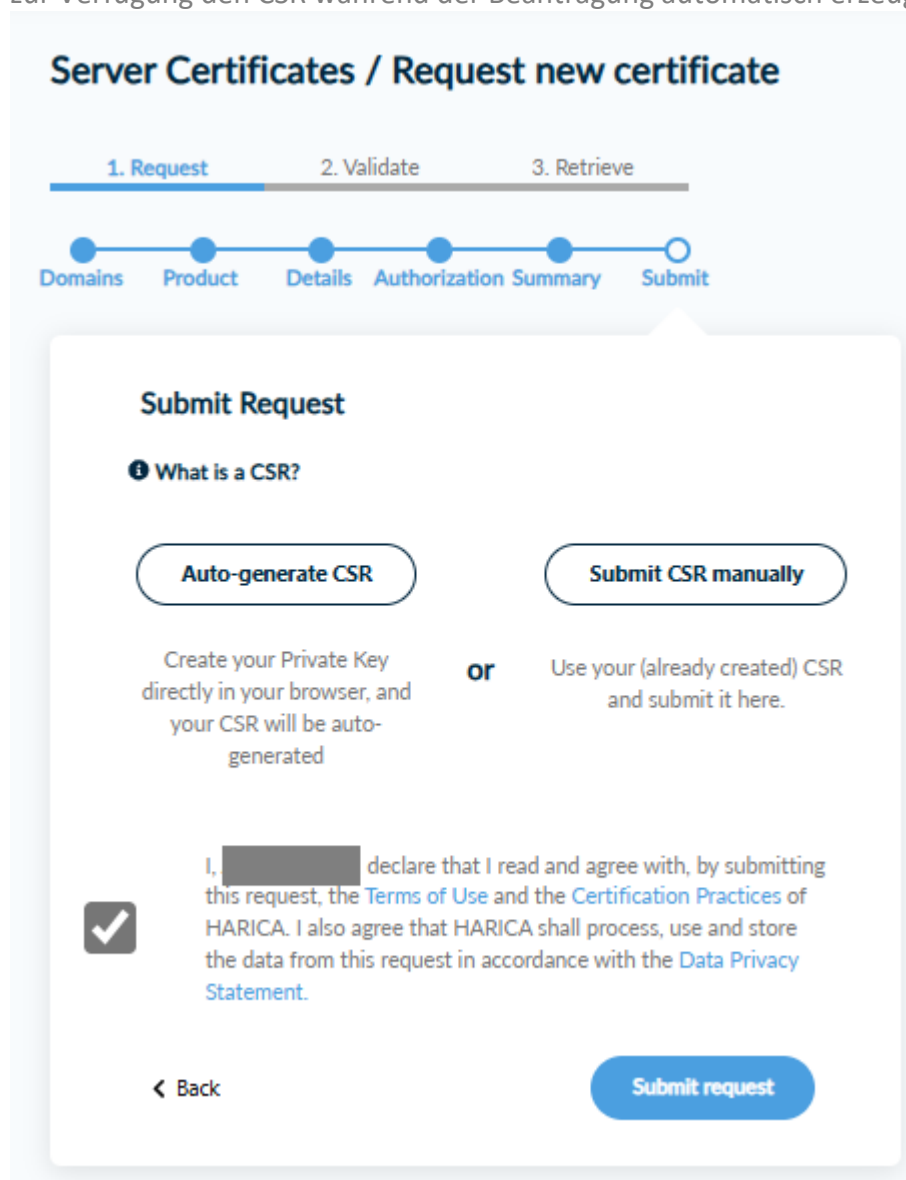
Select

from 275€ year

3. Anschließend erhalten Sie die Auswahl zwischen zwei Möglichkeiten, die sogenannten Zertifikatsignierungsanforderung (Certificate Signing Request (CSR)), hochzuladen.

Technischer Hintergrund

Die standardisierte und obligatorische CSR-Datei enthält neben den Domainnamen selbst auch die kryptografischen Informationen, damit das später ausgestellte Zertifikat überhaupt zu dem privaten Schlüssel (key) passt, der vertraulich und abgesichert zusätzlich zum Zertifikat selbst in Ihrer Anwendung hinterlegt sein muss. Die CSR-Datei kann (meist bei kommerziellen Anwendungen) direkt generiert werden, oder Sie können Sie mit dem openssl-Toolkit über die Kommandozeile selbst erzeugen. Bei Harica steht Ihnen nun auch eine komfortable dritte Möglichkeit zur Verfügung den CSR während der Beantragung automatisch erzeugen zu lassen.



Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Submit Request

i What is a CSR?

Auto-generate CSR **Submit CSR manually**

Create your Private Key directly in your browser, and your CSR will be auto-generated **or** Use your (already created) CSR and submit it here.

☒ 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](#).

[< Back](#) [Submit request](#)

4. Wenn Sie sich für Auto-generate CSR entschieden haben wählen Sie eine Schlüssellänge von 4096 bit, wenn Sie den verbreitetsten Algorithmus RSA verwenden möchten. Der moderne ECDSA-Algorithmus steht aber auch zur Verfügung.
Zuletzt müssen Sie noch ein Passwort setzen, mit dem die Key-Datei geschützt ist.
ACHTUNG: DIESES PASSWORT BENÖTIGEN SIE SPÄTER UNBEDINGT, SONST IST DER KOMPLETTE BEANTRAGUNGS-PROZESS HINFÄLLIG.

Submit Request

i What is a CSR?

Auto-generate CSR

or

Submit CSR manually

You will create a Private Key in your browser and your CSR will be auto-generated.

i Algorithm

i Key size

RSA (default) ▾

4096 ▾

Set a passphrase

.....

👁

Repeat passphrase

.....

👁

☒

I understand that this passphrase is under my sole knowledge and HARICA does not have access to it.

☒

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

Generate Private Key, CSR, and submit order

5. Das Generieren des Schlüsselpaares dauert einige Sekunden im Browser. Bitte brechen Sie den Vorgang nicht ab. Anschließend erscheint die finale Seite der Beantragung.

ACHTUNG: LADEN SIE UNBEDINGT DEN KEY AUF DIESER SEITE HERRUNTER. DER VORGANG KANN SPÄTER NICHT WIEDERHOLT WERDEN UND IST NUR AN DIESER STELLE UND EINMALIG MÖGLICH.

Request submitted successfully

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

You must :

!!! [- Download](#) your Private Key. !!!

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.



I have downloaded my private Key

[Go back to dashboard](#)

6. Nur müssen Sie etwas warten, bis der Antrag genehmigt ist. Die ist ein manueller Prozess. Sie erhalten nach Abschluss eine E-Mail.