

Inhalt

I.	Aufrufen des HARICA-Portals zur Zertifikatsbeantragung1
II.	Anleitung zur Betragung von SSL-Serverzertifikaten

I. Aufrufen des HARICA-Portals zur Zertifikatsbeantragung

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



https://cm.harica.gr/



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.

Ì	Zugriff auf HARICA <u>Unable to verify returning website</u>			
Finden Sie Ihre Institution				
	saarland Q			
B	eispiele: Technische Universität, jane.doe@example.edu, TU Diese Auswahl merken Mehr erfahren			
H	lochschule für Technik und Wirtsc tw-saarland.de			
U	Iniversität des Saarlandes ni-saarland.de			

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

≡ Z HARICA	Hochschule fuer Technik und 🗸
없 My Dashboard	My Dashboard
₫Ъ eSign Documents	SSL esignature Token eseal S/MIME Remote Code Signing Client Authentication
Certificate Requests	
eSignatures	
🖆 eSeals	
A Server	
Code Signing	
🖃 Email	
Client Authentication	
More	
బ్రీ Validated Information	
🛱 Data privacy statement	
Help / Guides	



II. Anleitung zur Betragung 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	Server Certificates / Request new certification
Ú3	eSign Documents	1. Request 2. Validate 3. Retrieve
Cert	ificate Requests	OOOO Domains Product Details AuthorizationSummary Submit
ŰB	eSignatures	Friendly name (optional)
Ē	eSeals	A custom label to help you identity this certificate in your dashboard
₿	Server	Beispielzertifikat
>-	Code Signing	Add Domains Manually or via Import 🕹
=	Email	supported: .onion v3, Wildcard, Internationalized Domain Name (IDN)
8	Client Authentication	example.hiz-saarland.de
More		Include <i>www.example.hiz-saarland.de</i> without additional cost.
. දු	Validated Information	+ Add more domains
Ē	Data privacy statement	The maximum number of domains allowed per request is 100.
P ₀	Help / Guides	Next



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





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



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
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.
Algorithm Key size
RSA (default) V 4096 V
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 :



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.