

# HARICA-Serverzertifikate

## Anmeldung im Harica CertManager

Um ein Serverzertifikat über Harica zu erstellen, melden Sie sich zuerst im Browser unter <https://cm.harica.gr/login> an.

Auf der Anmelde-Seite wählen Sie dafür „Academic Login“ aus.


**Login**

New to HARICA? [Sign Up](#)

**Email address**

Type your email address


**Password**

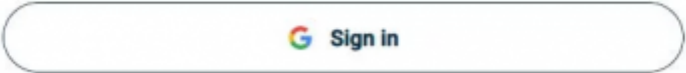
Type your password 

[Forgot password?](#)

**Login**

Or

 **Academic Login**

 **Sign in**

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

Wählen Sie in der Liste die Universität Freiburg aus. Falls diese nicht sofort angezeigt wird, können Sie über die Suchleiste danach suchen.

## Choose Your Institution

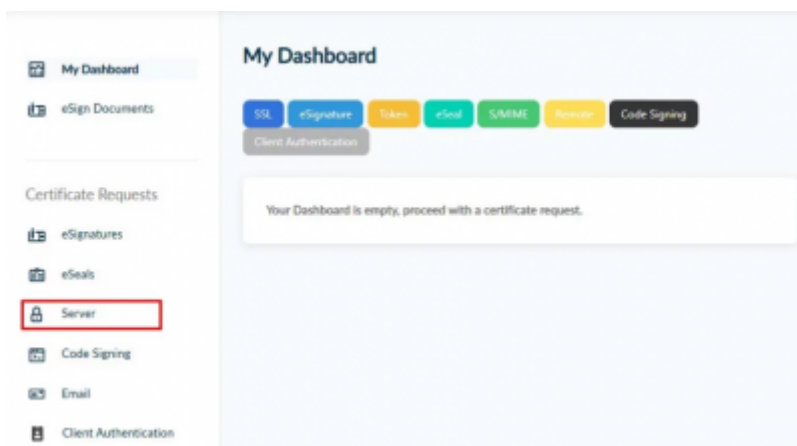
Recent institutions

**UNI FREIBURG** **Albert-Ludwigs-Universität Freiburg** uni-freiburg.de

[+ Add another institution](#) [Edit](#)

Sie werden nun weitergeleitet, um sich über Shibboleth mit Ihrem UniAccount und dem zugehörigen Passwort anzumelden. Nach diesem Schritt sind Sie angemeldet und können auf der Website ein Serverzertifikat beantragen.

Sobald Sie die Anmeldung abgeschlossen haben, können Sie links auf dem Dashboard unter dem Reiter „Certificate Request“ die Schaltfläche „Server“ auswählen.



In dem Fenster, das sich nun öffnet, geben Sie in den nächsten Schritten die Informationen zu dem gewünschten Serverzertifikat an. Der „Friendly Name“ ist hierbei optional (hier beispielsweise „Webserver Universität Freiburg“). Unter „Add domains“ geben Sie den Namen des Servers an (in diesem Fall „webserver.uni-freiburg.de“). Falls es Alternativnamen des Servers gibt, können Sie diese mit einem Klick auf „+ Add more domains“ hinzufügen (hier „meinwebserver.uni-freiburg.de“). Der Haken vor Include [www.webserver.uni-freiburg.de](http://www.webserver.uni-freiburg.de) without additional cost sollte deaktiviert werden, wenn diese Domain nicht benötigt wird (Standardfall). Klicken Sie anschließend auf „Next“.

### Server Certificates / Request new certificate

1. Request      2. Validate      3. Retrieve

Domains    Product    Details    Authorization    Summary    Submit

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

Webserver Universität Freiburg

**Add Domains Manually or via Import** [↑](#)  
supported: .onion v3, Wildcard, Internationalized Domain Name (IDN)

webserver.uni-freiburg.de ✓ ✕

Include **www.webserver.uni-freiburg.de** without additional cost.

meinwebserver.uni-freiburg.de ✓ ✕

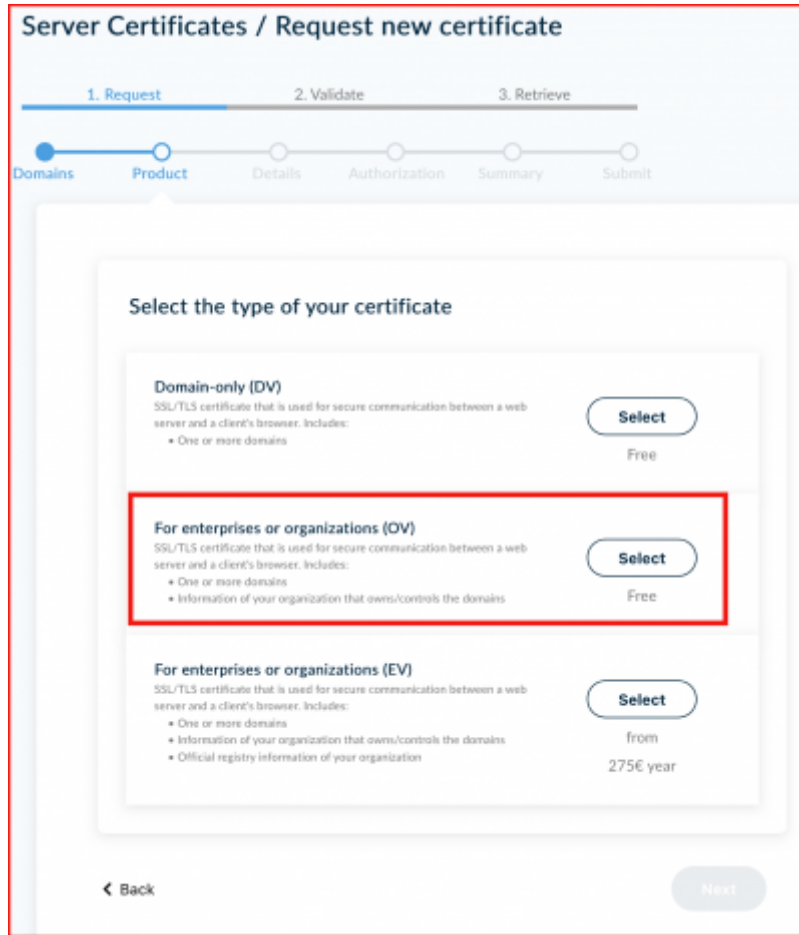
Include **www.meinwebserver.uni-freiburg.de** without additional cost.

+ Add more domains

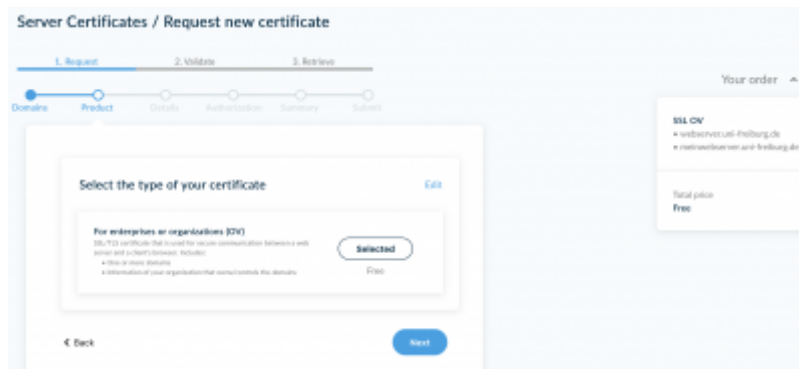
📌 The maximum number of domains allowed per request is 20.

Next

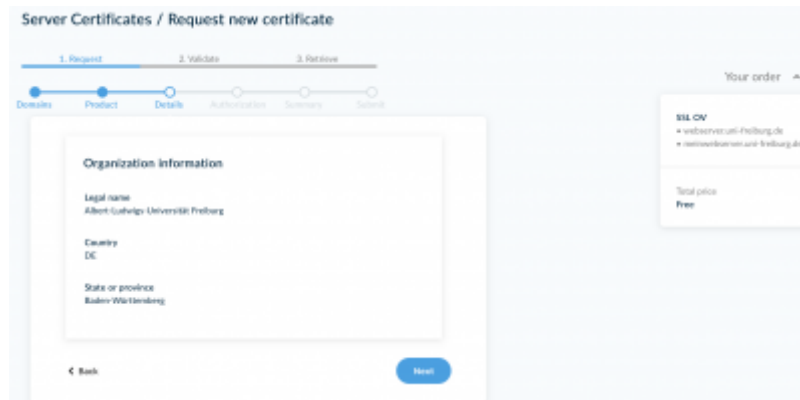
Im nächsten Schritt wählen Sie bitte bei „type of your certificate“ die Option „For enterprises or organisations (OV)“ aus (achten sie auf den korrekten Zusatz in Klammern!) und klicken auf „Next“.



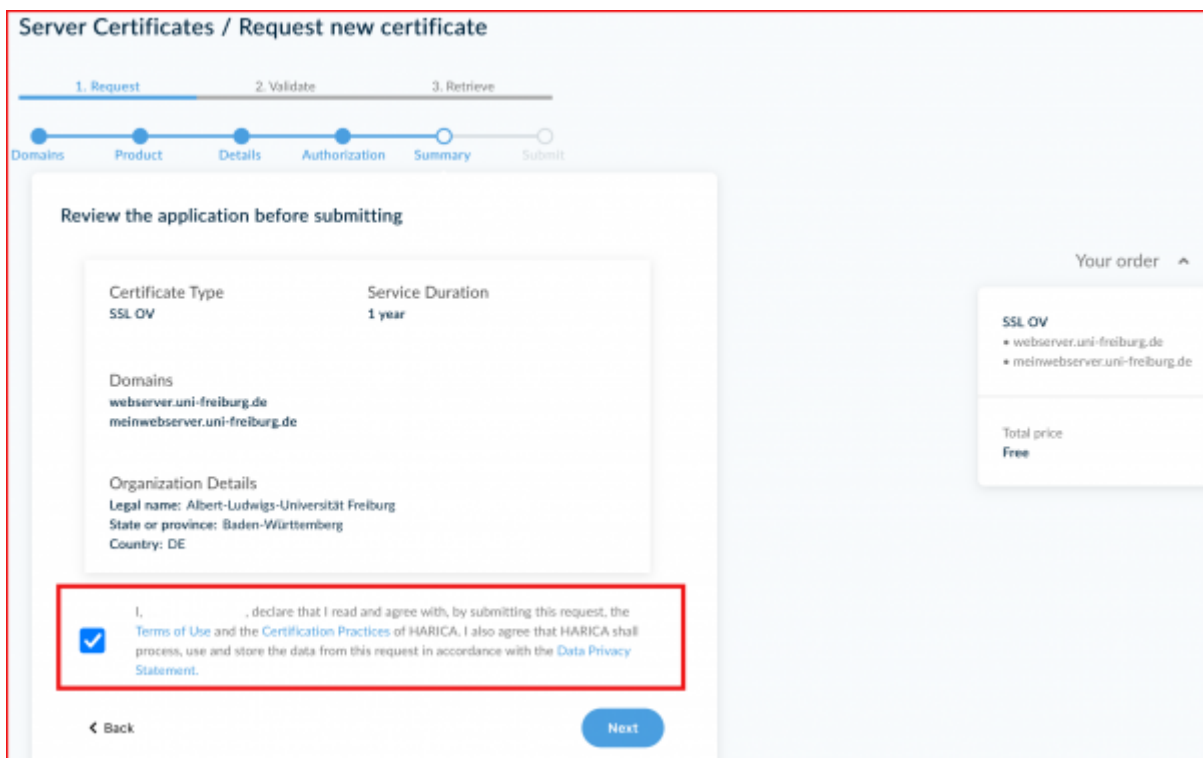
Nun bestätigen Sie Ihre Auswahl mit einem weiteren Klick auf „Next“.



Die Informationen zur Organisation können Sie ebenso mit einem Klick auf „Next“ bestätigen, da diese durch die Anmeldung mit Shibboleth gegeben sind.



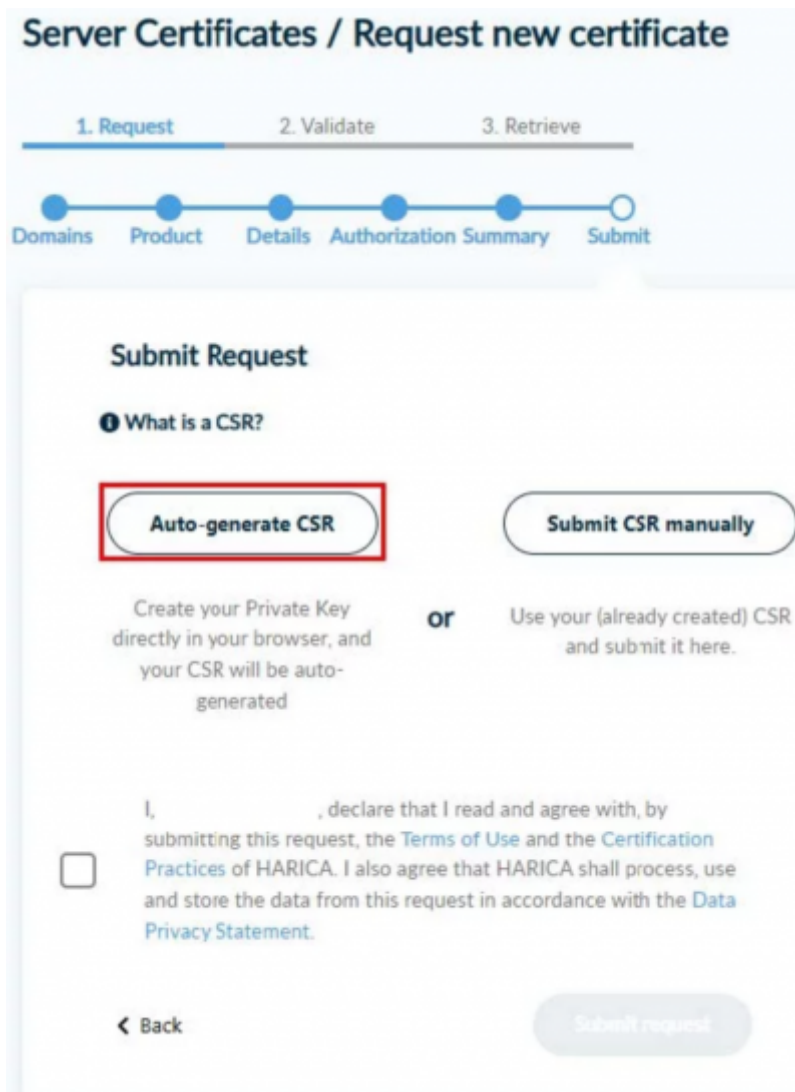
Unter der Übersicht für die Beantragung setzen Sie nun den Haken zur Zustimmung, bevor Sie auf „Next“ klicken.



Ihr nächster Schritt ist abhängig davon, ob Sie sich einen CSR (Certificate Signing Request) automatisch generieren lassen wollen, oder einen über OpenSSL erzeugten CSR selbst hochladen wollen.

## CSR automatisch generieren

Falls Sie sich einen CSR automatisch generieren lassen wollen, klicken Sie zuerst auf „Auto-generate CSR“.



Nun werden mehrere Angaben von Ihnen gefordert:

- Den Verschlüsselungs-Algorithmus und die dazugehörige Key size (Die Länge des privaten Schlüssels sollte 4096 Bit betragen.)
- Ein Passwort festlegen und wiederholen
- Beide Häkchen setzen

Dann können Sie „Generate Private Key, CSR, and submit order“ anklicken, um den Vorgang abzuschließen.

### Submit Request

[What is a CSR?](#)

or

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

**Algorithm**

RSA (default)

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](#)

Um Ihre Zertifikatsdatei nun herunter zu laden, klicken Sie bitte auf „Download“.

Der Private Key wird nun im Download-Ordner Ihres PCs als privateKey.pem gespeichert.

1. Request      2. Validate      3. Retrieve

---

### 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.

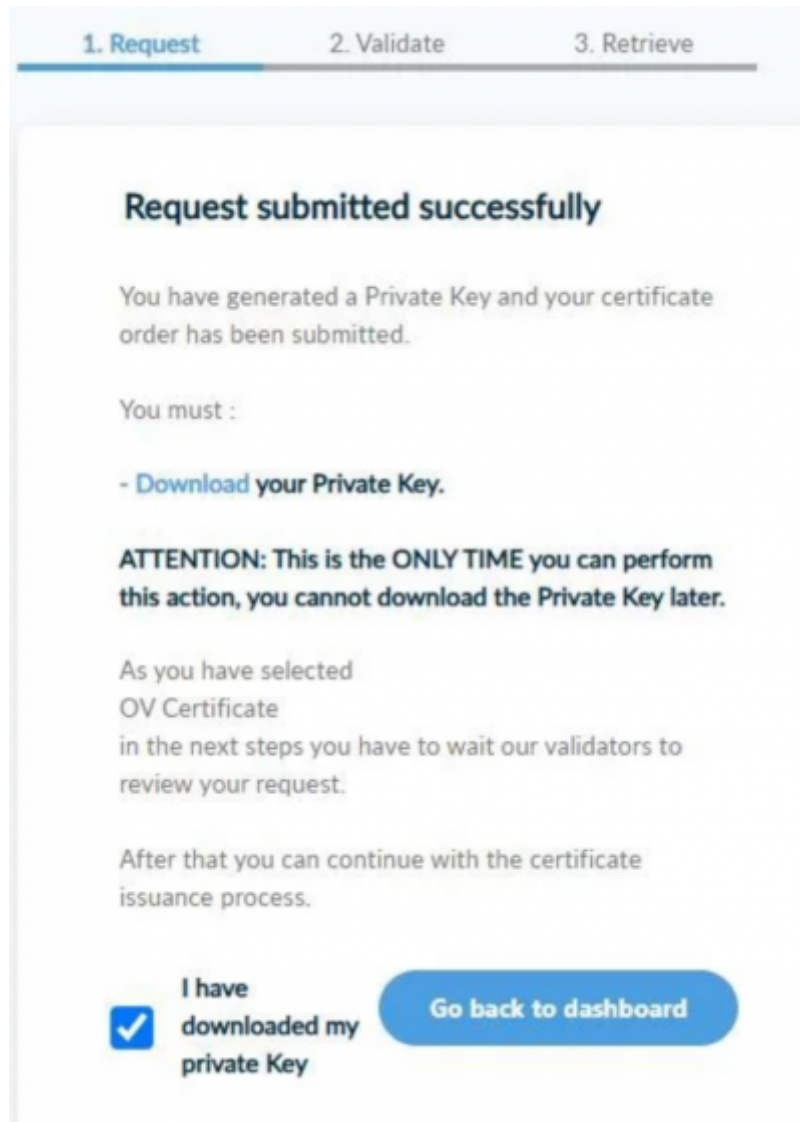
After that you can continue with the certificate issuance process.

**I have downloaded my private Key**

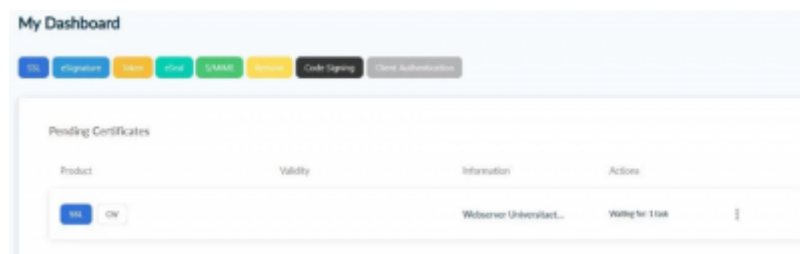
[Go back to dashboard](#)

Wenn der Download des Private Key fehlerfrei beendet wurde, können die den Haken setzen und den Download bestätigen, und mit einem Klick auf „Go back to dashboard“ zur Übersicht zurückkehren.



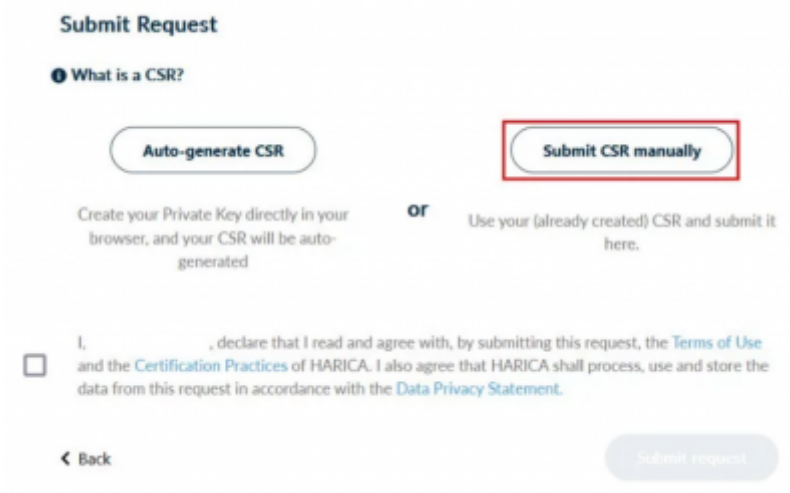


Zurück im Dashboard sehen Sie jetzt den Zertifikatsrequest, welcher nun von einer der berechtigten Personen im ITS genehmigt werden muss.

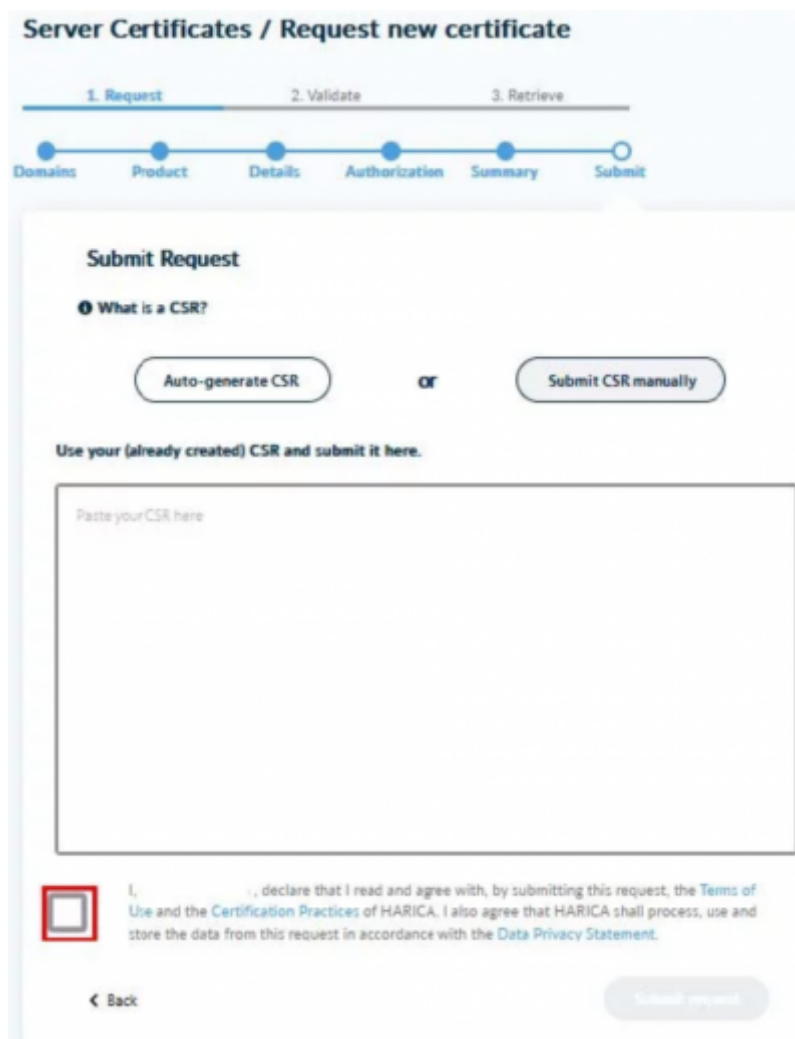


## CSR manuell hochladen

Falls Sie einen selbst-erzeugten CSR hochladen wollen, klicken Sie zuerst auf „Submit CSR manually“.

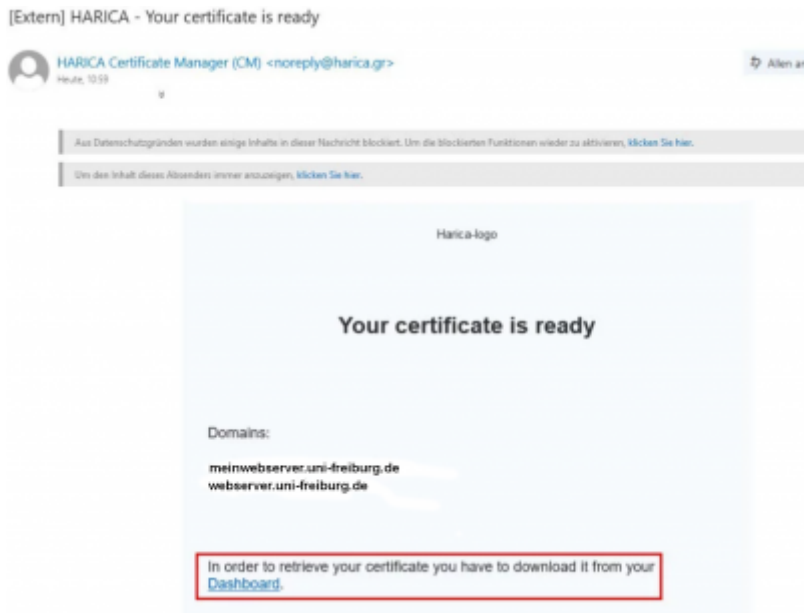


Nun kopieren Sie den Inhalt Ihres CSR und fügen diesen in das geöffnete Dialogfeld ein. Anschließend setzen Sie den Haken und schließen den Vorgang mit „Submit request“ ab.



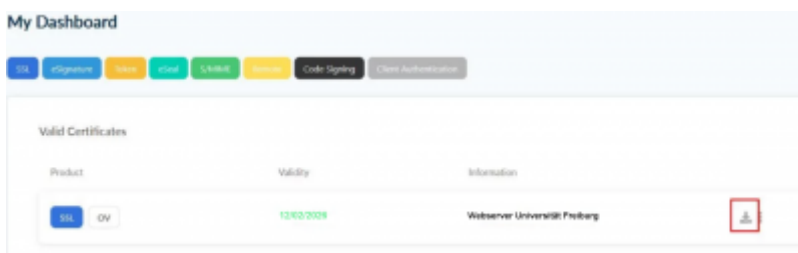
### Zertifikat herunterladen

Nachdem das Zertifikat genehmigt wurde, erhalten Sie eine E-Mail von Harica. Klicken Sie auf den in der Mail enthaltenen Link zum „Dashboard“ und melden Sie sich erneut auf der Website an.

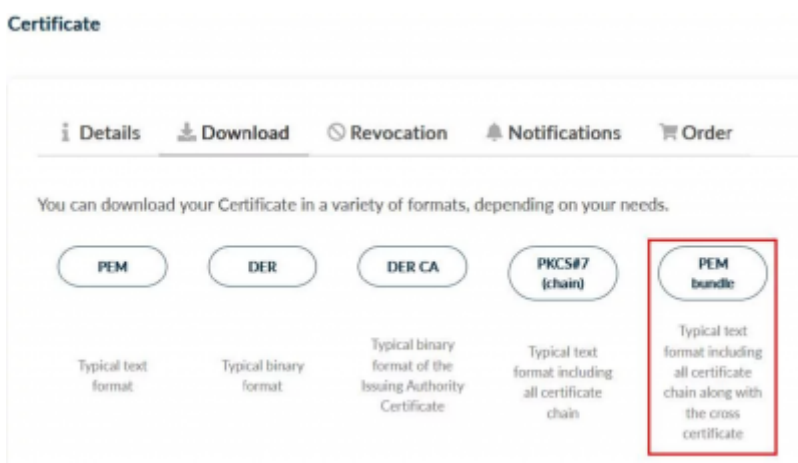


Im Dashboard sehen Sie nun Ihr genehmigtes Zertifikat.

Klicken Sie auf das Download-Symbol, um das Zertifikat herunterzuladen



Das Zertifikat kann man in den verschiedenen Dateiformaten herunterladen. Wir empfehlen „PEM-bundle“ zu wählen. Darin ist das eigentliche Zertifikat sowie die Zertifikatskette enthalten



Beim Download des Zertifikates kann es sein, dass der Browser meldet, die Seite würde nicht reagieren. Klicken Sie den Fehler so lange mithilfe der Schaltfläche „Warten“ weg, bis der Download abgeschlossen ist.

**Seite reagiert nicht**

Du kannst warten, bis die Seite wieder reagiert, oder sie schließen.

Harica CertManager - Server Certificate Request

**Warten** Seite verlassen

[server-zerts](#), [Sicherheit - Artikelübersicht](#), [-](#), [Artikelübersicht](#), [Zertifikate - Artikelübersicht](#), [Sicherheit - Artikelübersicht](#)

From:

<https://wiki.uni-freiburg.de/rz/> - RZ

Permanent link:

<https://wiki.uni-freiburg.de/rz/doku.php?id=harica-serverzertifikate>

Last update: **2025/02/14 15:19**

