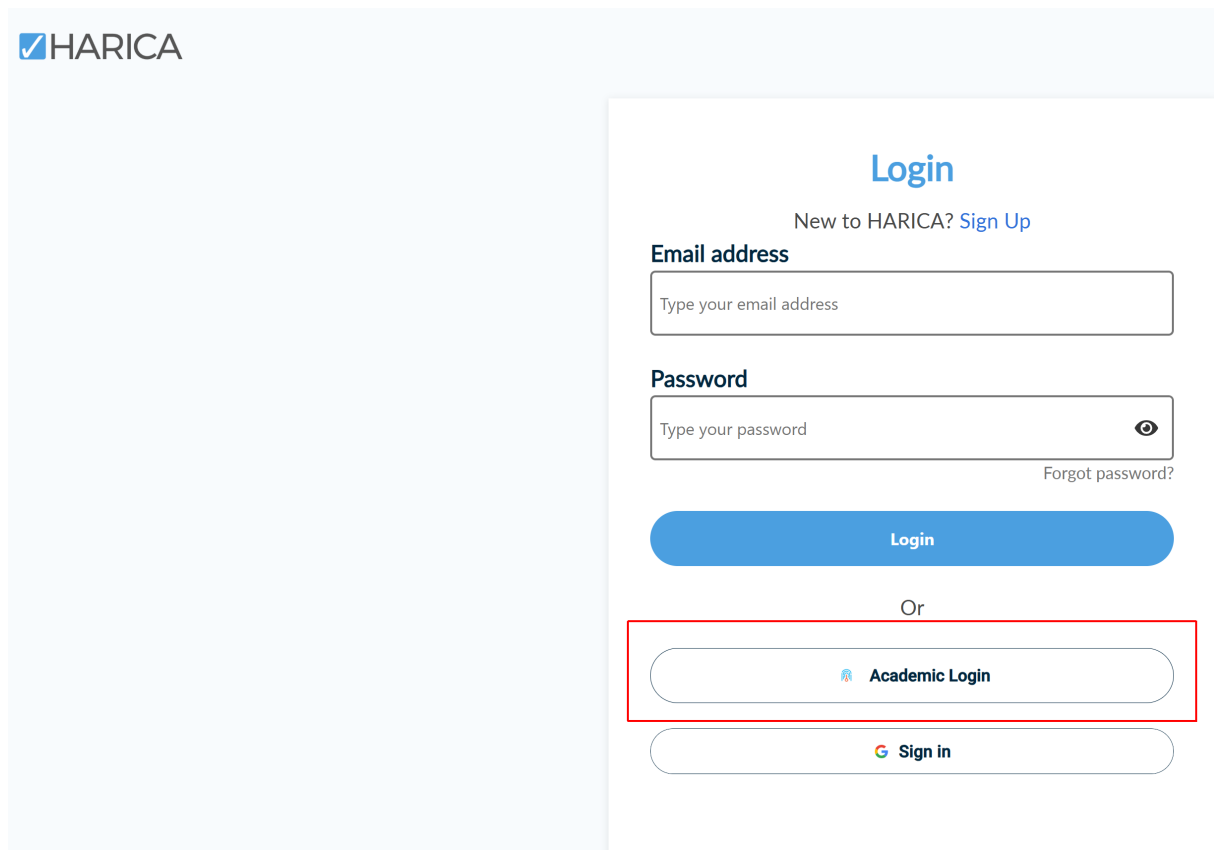


## SSL-Zertifikat beantragen

Anmelden mittels „Academic Login“ über SSO, verwenden Sie folgenden Link

<https://cm.harica.gr>




**HARICA**

### Login

New to HARICA? [Sign Up](#)


**Email address**  
Type your email address


**Password**  
Type your password 

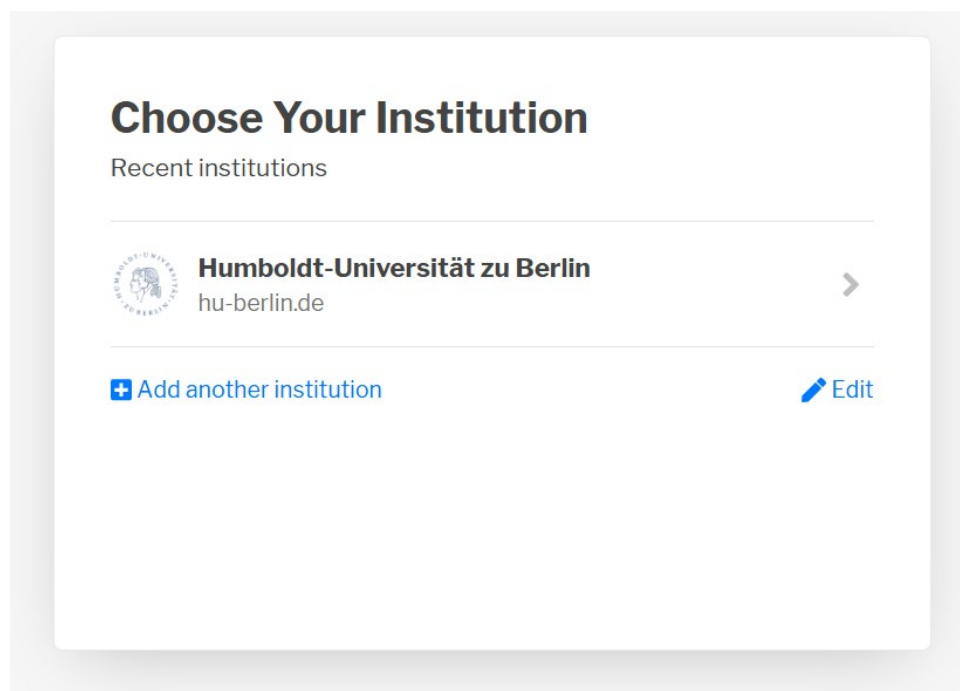
[Forgot password?](#)

**Login**

Or



 **Academic Login**

 **Sign in**



## Choose Your Institution

Recent institutions

 **Humboldt-Universität zu Berlin**   
hu-berlin.de

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

Falls **hu-berlin.de** nicht voreingetragen ist, suchen Sie über das Suchfeld danach und klicken darauf.



### Zentraler Login

HU-Account	<input type="text" value="cmsgridp"/>	
HU-Passwort	<input type="password" value="....."/>	<a href="#">Passwort vergessen?</a>
<input type="checkbox"/> Zustimmungserklärung für die Übertragung persönlicher Daten an diesen Service zurücksetzen		

Ihr HU-Login wird für die Anmeldung bei diesem Dienst verwendet:

	<b>HARICA</b>
Hellenic Academic and Research Institutions Certification Authority	
<a href="#">Datenschutzinformationen dieses Dienstes</a>	
<a href="#">Zusätzliche Informationen über diesen Dienst</a>	

Diese Login-Seite operiert im Rahmen der DFN-AAI Föderation und HU-interner Shibboleth-Seiten. Für die Authentifizierung benötigen Sie einen gültigen *HU-Account*. Nach erfolgreicher Anmeldung können Sie alle weiteren am Shibboleth Single Sign-On teilnehmenden Webseiten ohne nochmalige Angabe von HU-Account und HU-Passwort nutzen.

#### Weitere Informationen

[Mehr über Shibboleth](#)

#### Kontakt

[CMS Benutzerberatung](#)

Sie gelangen dann zum zentralen Login der HU, melden Sie sich dort mit dem gültigen HU-Account an für den Sie ein Nutzerzertifikat beantragen wollen.

### Zentraler Login

Ihr HU-Login wird für die Anmeldung bei diesem Dienst verwendet:

	<b>HARICA</b>
Hellenic Academic and Research Institutions Certification Authority	
<a href="#">Datenschutzinformationen dieses Dienstes</a>	
<a href="#">Zusätzliche Informationen über diesen Dienst</a>	
<b>Information zur Übertragung an den Service</b> <input checked="" type="checkbox"/> <b>Alle</b>	
E-Mail	<input type="text" value="grid-pki@cms.hu-berlin.de"/> <b>notwendig</b>
Heimatinrichtung (Domain Name)	<input type="text" value="hu-berlin.de"/> <input checked="" type="checkbox"/>
Nachname	<input type="text" value="Platzer"/> <b>notwendig</b>
Organisationsname	<input type="text" value="Humboldt-Universität zu Berlin"/> <input checked="" type="checkbox"/>
Pairwise ID	<input type="text" value="TLE4DQI4KWR72TWJ4YQOWF6TPJVKSTJ@hu-berlin.de"/> <input checked="" type="checkbox"/>
Personliche ID für den Dienst (pseudonyme Kennung)	<input type="text" value="TLE4DQI4KWR72TWJ4YQOWF6TPJVKSTJ"/> <b>notwendig</b>
Vertrauensprofil	<input type="text" value="https://refeds.org/assurance\nhttps://refeds.org/assurance/ATP/ePA-1m\nhttps://refeds.org/assurance/ATP/ePA-1d\nhttps://refeds.org/assurance/ID/unique\nhttps://refeds.org/assurance/IAP/low"/> <input checked="" type="checkbox"/>
Vorname	<input type="text" value="Steffen"/> <b>notwendig</b>

Die angezeigten Informationen werden an den Dienst übertragen, wenn Sie zustimmen.

Wählen Sie eine Gültigkeitsdauer für Ihre Zustimmung:

Einmal übertragen, beim nächsten Anmelden wieder nachfragen.

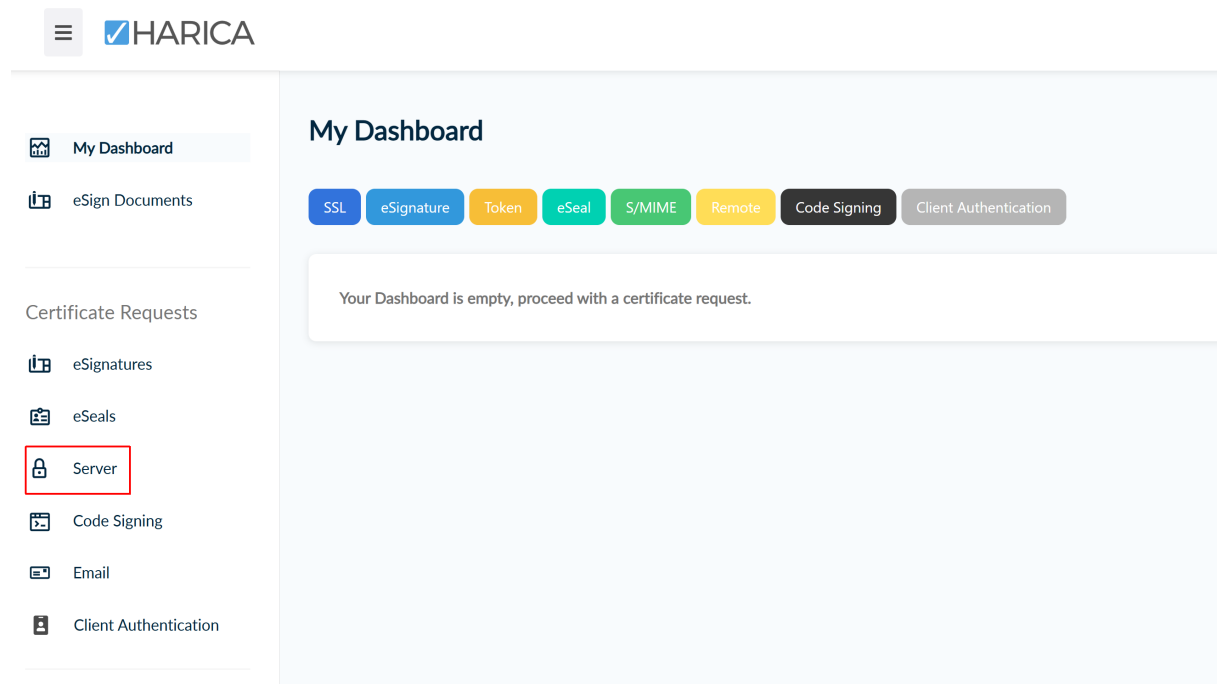
An diesen Dienst übertragen und wieder nachfragen, falls sich Informationen ändern.

Nicht wieder nachfragen und immer **alle** Informationen an **beliebige** Dienste übertragen.

Diese Einstellungen können jederzeit durch Markieren der Checkbox auf der Loginseite widerrufen werden.

Stimmen Sie der Datenübermittlung an den Dienst HARICA zu.

Sie befinden sich dann in der Übersicht „My Dashboard“



Die nachfolgende Anleitung beschreibt das Verfahren einen selbst erzeugten CSR (CertificateSigningRequest) bei der HARICA einzureichen um ein Organisationsvalidiertes SSL-Zertifikat zu erhalten.

Tragen Sie hier den gewünschten FQDN, sowie evtl. zusätzliche FQDN's als SubjectAlternativeNames ein. Die Anzahl der SubjectAlternativeNames ist derzeit auf **20** begrenzt.

My Dashboard

eSign Documents

---

Certificate Requests

eSignatures

eSeals

**Server**

Code Signing

Email

Client Authentication

---

More

Validated Information

Data privacy statement

Help / Guides

---

GREEK UNIVERSITIES NETWORK (GUnet4)  
General Commercial Registry Number: 160729401000

## Server Certificates / Request new certificate

1. Request 2. Validate 3. Re

Domains Product Details Authorization Summary

**Friendly name (optional)**

icard-Webserver

**Add domains**  
supported: .onion v3, Wildcard, Internationalized Domain Name (IDN)

icard.cms.hu-berlin.de ✓

Include **www.icard.cms.hu-berlin.de** without additional cost.

icardtest.cms.hu-berlin.de ✓

Include **www.icardtest.cms.hu-berlin.de** without additional cost.

icard.hu-berlin.de ✓

Include **www.icard.hu-berlin.de** without additional cost.

icardtest.hu-berlin.de ✓

Include **www.icardtest.hu-berlin.de** without additional cost.

+ Add more domains

< Back **Next**

# Server Certificates / Request new certificate

1. Request

2. Validate

3. Retrieve

Domains

Product

Details

Authorization

Summary

Su

## 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  
250€ year

← Back

Next

## Select the type of your certificate

Edit

### 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

Selected

Free

← Back

Next

## Organization information

**Legal name**

Humboldt-Universitaet zu Berlin

**Country**

DE

**State or province**

Berlin

← Back

Next

## Review the application before submitting

**Certificate Type**

SSL OV

**Service Duration**

1 year

**Domains**

icard.cms.hu-berlin.de

icardtest.cms.hu-berlin.de

icard.hu-berlin.de

icardtest.hu-berlin.de

**Organization Details**

**Legal name:** Humboldt-Universitaet zu Berlin

**State or province:** Berlin

**Country:** DE



I, Steffen Platzer, 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

Next

Wählen Sie die Option „Submit CSR manually“, kopieren ihren CSR in das Textfeld und bestätigen Sie ihr Einverständnis mit den angeführten Regularien.

### Submit Request

What is a CSR?

Auto-generate CSR

OR

Submit CSR manually

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC+TCCAECAQAwg6MxMzA1BgNVBAYTAkRFRMw8wDQYDVQQIEwZCZXJsaW4xZDZAN
BgNVBAcTBkllcmxpbiEoMUYGA1UEChMfSHVtYm9sZHQtdVW5pdmVyc2l0YWV0IHp1
IEJlcmxpbiEMMAoGA1UECjMDQ01TMSMwIQYDVQQDEExpY2FyZHRlc3QuY21zLmhh
LWJlcmxpbi5kZTElMCMGCSqGSIb3DQEJARYWc21hcnRjYXJkQW5kZG91LWJlcmxpbi5k
ZTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANftnA8vUfa8Vo2z3tU
u0iTDz/zf50qEaaq+mb9ewVMm7T8dsZX8htlqMR32JaIMi4dY8zOvYwNouSmb6Q0
b9oiCrXg6Cnc6VeRrHPcD2RsQE6qMNATHXyDPld7J73mZXpf2dihYfa8B1xoj/h
3DiZbZ1RmHguGvMOScxX9WWQLy6zqDkDN4M801j4C5ZvKnlouhXzZdtOJQANylr
wnf+P1p8nW2xlpvea5v3cne4mN6dVirhqVbDLttfFmq4D5L96K1ECLGmp1WbjaM
7ieZgcl6j1h0Mo/VmdSxdvNelYqeQn1tuSA2Lu8XOkz7alOTK7QpY/a1xK1mgNbU
JZsCAwEAaAAAMA0GCsGSIb3DQEBAUAA4IBAQAHLVKKOsRn/ESl6gYc9xOwigy
TNPZt5DLkXHEpsoveEIU7YFujD6fK+KOceDb0Q5kYtsG7fAkNksCQRF873Q2Dx+O
V8KphwbwZJxGtvNdMgJShi9gg22oNAYvDQxiR509i7+eD3vd2wixDFHE8PqhBqGE
PRUBteiORp0Y5rJfYH+UPbiu7OuRI4uqba3nx+it0Szyfx8T1dk2UitjW8y2fOMN
00CzKqgsyyi9N5cUyEMJ9iWfezrOAS5NbhH66TB5hFEPRQIXy8G7x9ce+KrcV5Pqw
Tlxqf55opJHnuktPng845MQk/W3sKsf4vTbTNc5KlWjhnJfnt6iYdSq1+a6
-----END CERTIFICATE REQUEST-----
```

I, Steffen Platzer, 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

Mit „Submit request“ übermitteln Sie ihren Request an die CA.

Danach befinden Sie sich wieder in ihrer Übersicht „My Dashboard“

### My Dashboard

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


#### Pending Certificates

Product	Validity	Information	Actions
SSL OV		icard-Webserver	Waiting for: 1 task <a href="#">Order details</a> <a href="#">Cancel request</a>

Hier sehen Sie eine Übersicht der eingereichten Requests, oder bereits ausgestellter Zertifikate.

Nach Ausstellung des SSL-Zertifikates erhalten Sie eine Bestätigungs-E-Mail von HARICA Certificate Manager (CM) noreply@harica.gr mit dem Betreff:“ HARICA - Your certificate is ready“.

Von: HARICA Certificate Manager (CM) <noreply@harica.gr>  
An: grid-pki@cms.hu-berlin.de  
Betreff: HARICA - Your certificate is ready



## Your certificate is ready

Domains:

- icardtest.hu-berlin.de
- icard.hu-berlin.de
- icardtest.cms.hu-berlin.de
- icard.cms.hu-berlin.de

In order to retrieve your certificate you have to download it from your [Dashboard](#).

In ihrem „My Dashboard“ finden Sie das ausgestellte SSL-Zertifikat zum Download.

### My Dashboard

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

Valid Certificates

Product	Validity	Information
SSL OV	16/01/2026	icard-Webserver

Download

Hierzu muss das Download-Icon neben dem Zertifikat angewählt werden. Mit dem Button „PEM bundle“ im anschließenden Dialog erhält man eine Datei, die für Webserver wie Apache oder nginx direkt verwendbar ist.

### Certificate

Details Download Revocation Notifications Order

You can download your Certificate in a variety of formats, depending on your needs.

PEM	DER	DER CA	PKCS#7 (chain)	PEM bundle
Typical text format	Typical binary format	Typical binary format of the Issuing Authority Certificate	Typical text format including all certificate chain	Typical text format including all certificate chain along with the cross certificate