

deutsches forschungsnetz

Automatisierung mit ACME

September 2026

Automatisierung mit ACME

Zu diesem Webinar:

- ▶ Folien werden zur Verfügung gestellt
- ▶ Rückfragen per Zoom-Q&A
- ▶ Kontakt: `dfnpca@dfn-cert.de`
- ▶ Dokumentation auf
<https://doku.tid.dfn.de/de:dfnpki:tcs:2025:acme>
- ▶ Community auf dfnpki-d-Mailingliste
<https://www.listserv.dfn.de/sympa/info/dfnpki-d>

Automatisierung mit ACME

- ▶ Motivation
- ▶ Basisbegriffe
- ▶ Werkzeuge
- ▶ Praxis mit HARICA
- ▶ Ausblick

DFN

Motivation

Motivation

- ▶ „Früher“:
 - ▷ 5 Jahre lang gültige Serverzertifikate
 - ▷ ...über Webseiten bei der CA beantragt
 - ▷ ...nach manuellem Prozess ausgestellt
 - ▷ ...per Hand installiert

Motivation

- ▶ Jetzt:
 - ▷ TLS auf jedem Server => Viel mehr Zertifikate
 - ▷ Protokolle für Automatisierung existieren
 - ▷ Massensperrungen
 - ▷ Drastische Reduzierung der Gültigkeit von Serverzertifikaten und von Domainvalidierungen

Roadmap Gültigkeit von Serverzertifikaten:

Ab Datum	Maximale Gültigkeit
15.03.2026	200 Tage
15.03.2027	100 Tage
15.03.2029	47 Tage

Roadmap Gültigkeit von Domainvalidierungen:

Ab Datum	Maximale Gültigkeit
15.03.2026	200 Tage
15.03.2027	100 Tage
15.03.2029	10 Tage

- ▶ Konsequenz: Ohne Automatisierung geht nichts mehr
- ▶ Positiv: Automatisierung und Monitoring kann höhere Qualität bringen
- ▶ Zwei verschiedene Probleme zu lösen:
 - ▷ Problem 1: Gültigkeit von Serverzertifikaten 47 Tage ab 2029
Lösung: Automatisierung per ACME => Dieses Webinar
 - ▷ Problem 2: Gültigkeit von Domainvalidierungen 10 Tage ab 2029
Lösung: Teilweise ACME, teilweise *TODO* => *später*

Basisbegriffe

- ▶ RFC8555 Automatic Certificate Management Environment (ACME)
 - ▷ Entwicklung von 2015-2019 durch Mozilla, EFF, University of Michigan
 - ▷ Eng gekoppelt mit der Entwicklung von Let's Encrypt
- ▶ Starke Anreize für PKI-Anbieter, ACME zur Verfügung zu stellen („SHOULD“ durch Google Chrome Root Programm)
- ▶ Vielfalt an Werkzeugen auf Client-Seite
- ▶ Darum: ACME als empfehlenswerte Lösung

Basisbegriffe

ACME Server

- ▶ ACME Schnittstelle eines PKI-Anbieters
- ▶ Definiert durch eine URL. Diese kann auch für jeden User individuell sein.

ACME Client

- ▶ Software, die mit dem ACME Server kommuniziert
- ▶ Muss nicht das System sein, auf dem die Zertifikate eingesetzt werden.

Account

- ▶ Beim ersten Kontakt erstellt jeder Client einen Account mit dem Server
 - ▷ Technisch: Schlüsselpaar. Public Key ist beim Server registriert.

Basisbegriffe

External Account Binding (EAB)

- ▶ Zweck:
 - ▷ Bindung eines ACME-Accounts eines Clients an ein Konto in einer Kundenverwaltung der CA separat von ACME
 - ▷ Zur Verwendung von vorvalidierten Werten, z.B. O=DFN-CERT oder vorvalidierte Domains
- ▶ HMAC Key und Key Identifier
 - ▷ Ausgegeben von der CA
 - ▷ Geheim zu halten!

Basisbegriffe

Challenge

- ▶ Mehrere Verfahren, mit denen der Client dem Server demonstrieren kann, dass er die Kontrolle über einen FQDN hat
- ▶ Challenges sind notwendig
 - ▷ wenn der FQDN nicht anderweitig validiert wurde
 - ▷ oder die CA eigene Gründe hat
- ▶ Client kann sich vom Server ein Verfahren wünschen
 - ▷ z.B. per Parameter `--preferred-challenges http` o.ä.

Basisbegriffe

Challenge http-01

- ▶ Server gibt dem Client ein Token (eine Zufallszahl)
- ▶ Client erzeugt aus dem Token eine "Key Authorization" und legt diese ab unter `http://<FQDN>/.well-known/acme-challenge/<token>`
- ▶ Server prüft die an dieser URL hinterlegte Key Authorization
 - ▷ Webserver auf Port 80, HTTP
 - ▷ Server SOLLTE Redirects folgen
 - ▷ Wenn der FQDN auf mehrere IPs auflöst, kann der Server sich eine aussuchen.
- ▶ Nicht für Wildcard-Zertifikate

Basisbegriffe

Challenge dns-01

- ▶ Server gibt dem Client ein Token (eine Zufallszahl)
- ▶ Client erzeugt aus dem Token eine "Key Authorization" und davon den SHA256-Hash, und legt diesen im DNS als TXT-Record ab:

```
_acme-challenge.www.example.org. 300 IN TXT "gfj9Xq...Rg85nM"
```

- ▶ Server prüft den Hash der Key Authorization in diesem TXT-Record
- ▶ Server darf CNAMEs folgen
 - ▷ Damit können „ACME-Challenge“-Zonen gebaut werden mit anderem Access als die Haupt-Zonen
- ▶ Für Wildcard-Zertifikate

Basisbegriffe

Challenge **tls-alpn-01**

- ▶ Verfahren auf Ebene TLS mit Application Layer Protocol Negotiation
- ▶ Wenige Implementierungen verfügbar
- ▶ Für Spezialfälle

Basisbegriffe

ACME Renewal Information (ARI)

- ▶ RFC 9773 - ACME Renewal Information (ARI) Extension- Juni 2025
- ▶ Erweiterung, mit dem der Client den optimalen Erneuerungszeitpunkt für ein Zertifikat vom Server abfragen kann
- ▶ Wichtiges Werkzeug, um Ausfallrisiko durch CA-seitige Sperrungen von Zertifikaten zu minimieren
- ▶ ARI muss sowohl vom Server als auch vom Client implementiert werden. Z.B. derzeit:
 - ▷ Certbot ja, mod_md ja, acme.sh seit Juli 2026,
 - ▷ Let's Encrypt ja, HARICA seit Juli 2026

DFN

Werkzeuge

Werkzeuge

Betriebsweise von ACME Clients:

1. Zertifikat initial ausstellen lassen und installieren
2. Regelmäßiger Check, ob Erneuerung notwendig
 - ▶ cron
 - ▶ Windows Aufgabenplanung
 - ▶ Integrierte Tasks vom ACME Client in der Anwendung

Werkzeuge

- ▶ Zu Beachten bei der Auswahl des ACME Clients:
Individueller Funktionsumfang!
- ▶ Insbesondere zu Prüfen:
 - ▷ Kompatibilität Zertifikatinstallation?
 - ▷ Support für ACME Renewal Information?
 - ▷ Wenn Nutzung von dns-01 geplant: Plugins für schreibenden Zugriff auf DNS-Server vorhanden?

Werkzeuge

certbot

- ▶ In vielen (allen?) Linux-Distributionen enthalten
- ▶ Referenzimplementierung eines ACME Clients der EFF
- ▶ Zertifikatinstallation in Apache, nginx
- ▶ Plugins für viele DNS-Server/Anbieter
- ▶ Unterstützt ARI
- ▶ Benötigt externe `cron`-Konfig

Werkzeuge

`simple-acme`

- ▶ Standard-Lösung für Windows
- ▶ Nachfolger von `win-acme`
- ▶ Zertifikatinstallation in IIS
- ▶ Plugins für viele DNS-Server/Anbieter
- ▶ Unterstützt ARI
- ▶ Besonders nützlich: `--setuptaskscheduler`

Werkzeuge

ACME Clients direkt in der Infrastruktur:

- ▶ Apache Modul `mod_md`
- ▶ Caddy, Traefik
- ▶ Certmanager (Kubernetes/OpenShift)

Viele weitere Werkzeuge:

- ▶ `acme.sh`, `dehydrated`, `getssl`, `CertSage`, `lego`, `Posh-ACME`,...

Praxis mit HARICA

Praxis mit HARICA

- ▶ ACME bei HARICA ausschließlich per External Account Binding
 - 1) EAB Account mit HMAC Key/Key Identifier im certmanager erzeugen
 - 2) ACME Client mit HMAC Key/Key Identifier konfigurieren
- ▶ Verschiedene Ausprägungen:
 - ▷ Enterprise EAB Accounts
 - SSL OV
 - SSL DV
 - ▷ Personal EAB Accounts

Praxis mit HARICA

Wann ist eine ACME Challenge erforderlich?

Account Typ	Variante	Domain	Challenge?
Enterprise	SSL DV	vorvalidiert	nein
		nicht validiert	ja
Enterprise	SSL OV	vorvalidiert	nein
		nicht validiert	nicht möglich, Fehler
Personal		vorvalidiert	ja
		nicht validiert	ja

Praxis mit HARICA

Enterprise EAB Accounts:

- ▶ Können nur vom Enterprise Admin angelegt werden
- ▶ Verfügbare Domains müssen dem EAB Account zugewiesen werden
- ▶ Kontrollierte Weitergabe von HMAC Key/Key Identifier an Systemverantwortliche möglich

Praxis mit HARICA

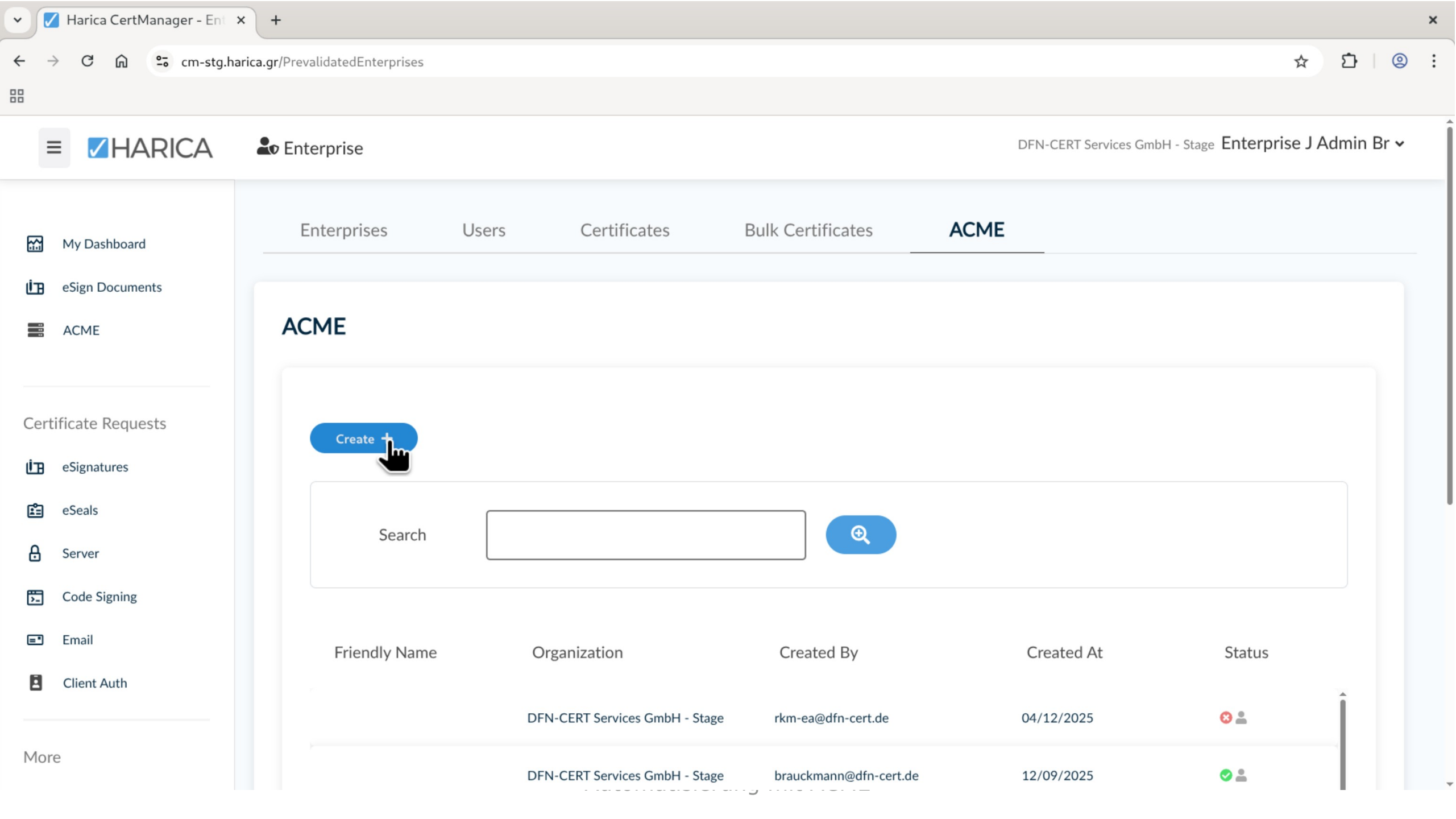
Enterprise EAB Accounts in zwei Varianten:

SSL DV	SSL OV
Ohne Organisationsinfo	Mit Organisationsinfo (O=DFN-CERT)
Domain muss im certmanager eingetragen sein	Domain muss im certmanager eingetragen und vorvalidiert sein
Für Domains mit und ohne Vorvalidierung. Ohne Vorvalidierung: ACME Challenge	Nur vorvalidierte Domains möglich

Praxis mit HARICA

Tour durch das HARICA-Interface:

- ▶ Enterprise Admin: Erzeugen von Enterprise EAB Accounts



Create ACME EAB Account ✕

1 Choose Organization

DFN-CERT Services GmbH - Stage

Country: DE
State: Hamburg
Locality:
Name: DFN-CERT Services GmbH - Stage
Domains:

uni-pellworm.de
dfn-cert.de

Please note: You can define specific rules for each domain that will be included in this ACME EAB account later.

2 Choose Certificate Type

SSL OV

3 Add Friendly Name

A custom label to help you identify this account

jbr-acme-demo



I, Enterprise J Admin Br , 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](#).

Create

Close

Harica CertManager - Ent

cm-stg.harica.gr/PrevalidatedEnterprises

DFN-CERT Services GmbH - Stage Enterprise J Admin Br

My Dashboard

eSign Documents

ACME

Certificate Requests

eSignatures

eSeals

Server

Code Signing

Email

Client Auth

More

EnterprisesUsersCertificatesBulk CertificatesACME

ACME

Create +

Search

Friendly Name	Organization	Created By	Created At	Status
r-acme-demo	DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	09/01/2026	
	DFN-CERT Services GmbH - Stage	rkm-ea@dfn-cert.de	04/12/2025	

Harica CertManager - Ent

cm-stg.harica.gr/PrevalidatedEnterprises

☆🏠👤⋮

Email

Client Auth

More

Validated Information

Data privacy statement

Help / Guides

GREEK UNIVERSITIES

NETWORK (GUnet)

General Commercial Registry

Number: 160729401000

Friendly Name	Organization	Created By	Created At	Status
jbr-acme-demo	DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	09/01/2026	🟢🏠

DetailsCertificatesDomains

Organization	DFN-CERT Services GmbH - Stage
Created At	Friday, January 9, 2026
Created By	jbr-ea@dfn-cert.de
Key ID	📄LYDFFaxyTP68yoD4tlhE
HMAC Key	📄ZOkQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSlxH4
Server URL	📄https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory
Certificate Type	SSL OV
Status	🟢
Notes	
Tags	🏠
Actions	Disable

Harica CertManager - Ent

cm-stg.harica.gr/PrevalidatedEnterprises

Email

Client Auth

More

Validated Information

Data privacy statement

Help / Guides

GREEK UNIVERSITIES NETWORK (GUnet)

General Commercial Registry

Number: 160729401000

Friendly Name	Organization	Created By	Created At	Status
jbr-acme-demo	DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	09/01/2026	

DetailsCertificatesDomains

Allow All Domains

Available Domains

Domain	Validity
+ uni-pellworm.de	09/02/2027
+ dfn-cert.de	09/02/2027

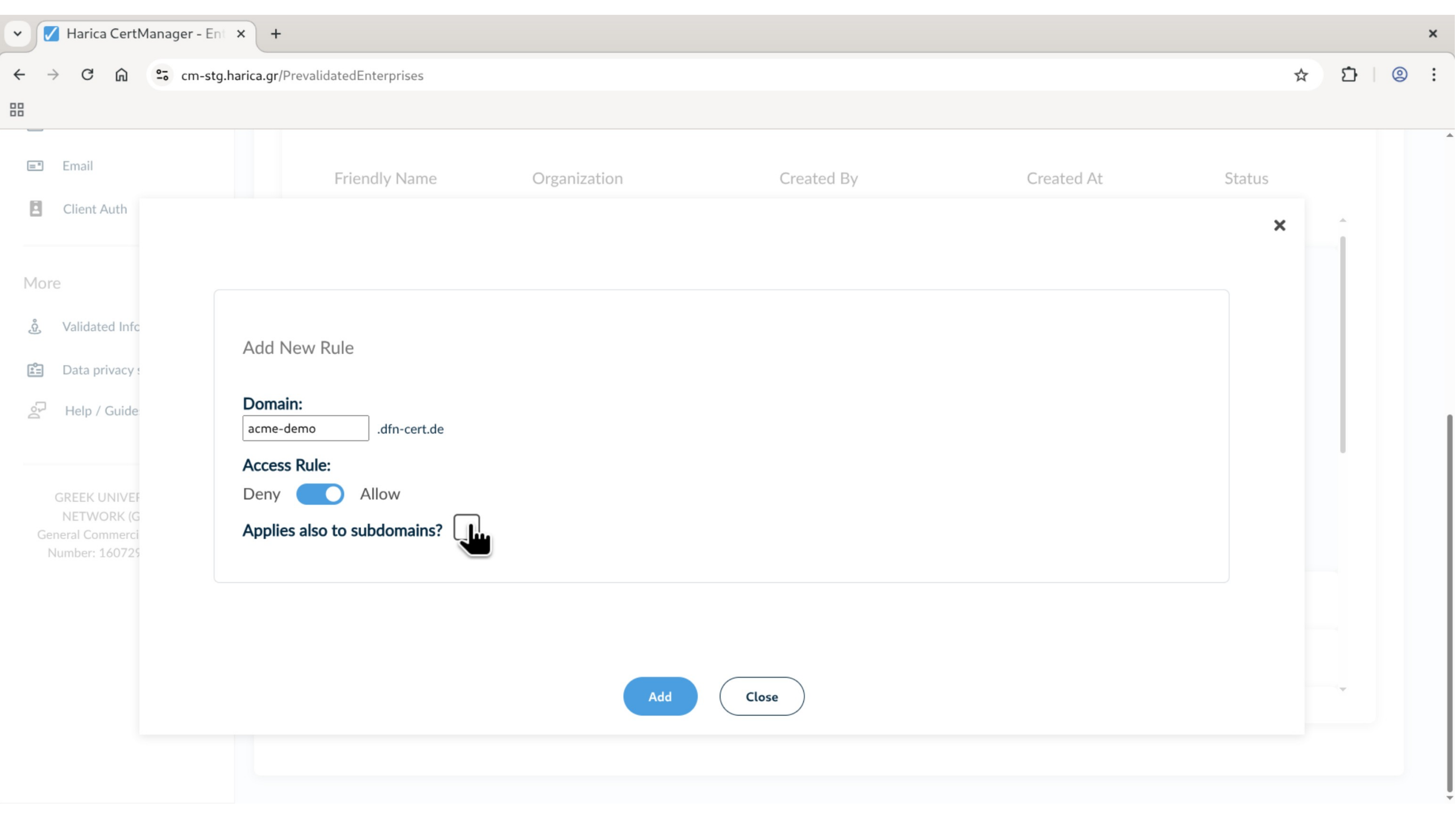
Active Rules (Explicit denial takes precedence over allowance)

Domain	Allowed	Rule applies to Subdomains
--------	---------	----------------------------

Inactive Rules

Domain	Allowed	Rule applies to Subdomains
--------	---------	----------------------------

DFN-CERT Services GmbH - Stage	rkm-ea@dfn-cert.de	04/12/2025	
DFN-CERT Services GmbH - Stage	brauckmann@dfn-cert.de	12/09/2025	



Email

Client Auth

More

Validated Info

Data privacy s

Help / Guide

Friendly Name

Organization

Created By

Created At

Status

Add New Rule

Domain:

acme-demo

.dfn-cert.de

Access Rule:

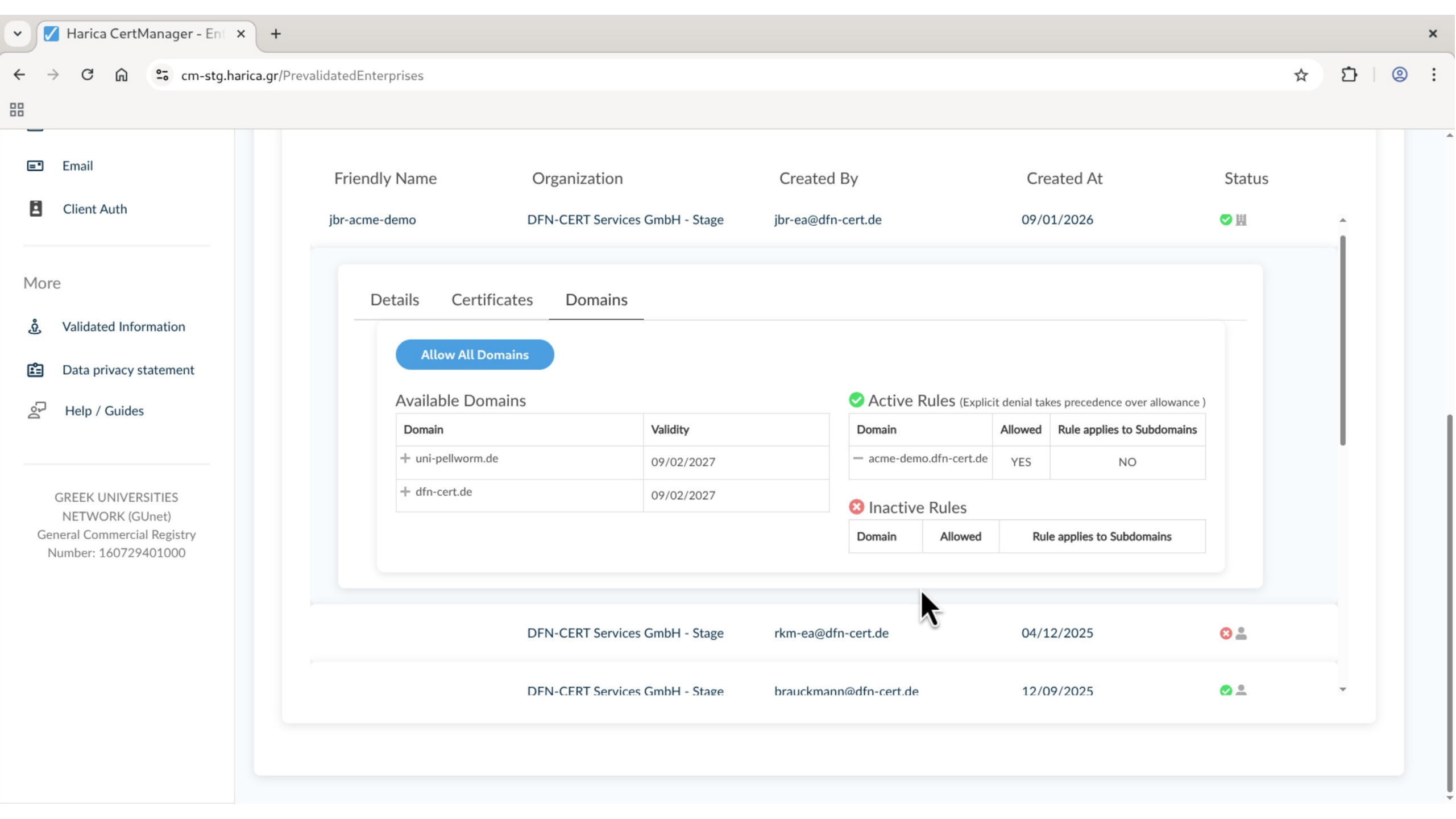
Deny ☒ Allow

Applies also to subdomains?



Add

Close



Harica CertManager - Ent

cm-stg.harica.gr/PrevalidatedEnterprises

Code Signing

Email

Client Auth

PSD2

Validated Information

Data privacy statement

Help / Guides

GREEK UNIVERSITIES NETWORK (GUnet)

General Commercial Registry Number: 160729401000

Friendly Name	Organization	Created By	Created At	Status
jbr-acme-demo	DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	09/01/2026	

Details

Certificates

Domains

Settings

Credits

Unlimited

Leave empty for unlimited. Used: 5

Expiration Date

mm/dd/yyyy

Leave empty for no expiration.

Status

Active

Paused

Comments

Optional comments...

Up to 500 characters. 0 / 500

Save

Praxis mit HARICA

Tour: Nutzung der EAB Accounts mit `certbot`

Harica CertManager - Ent

cm-stg.harica.gr/PrevalidatedEnterprises

Email

Client Auth

More

Validated Information

Data privacy statement

Help / Guides

GREEK UNIVERSITIES NETWORK (GUnet)

General Commercial Registry Number: 160729401000

Friendly Name	Organization	Created By	Created At	Status
jbr-acme-demo	DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	09/01/2026	

Details

Certificates

Domains

Organization

DFN-CERT Services GmbH - Stage

Created At

Friday, January 9, 2026

Created By

jbr-ea@dfn-cert.de

Key ID

LYDFFaxyTP68yoD4tlhE

HMAC Key

ZOkQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSlxH4

Server URL

https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory

Certificate Type

SSL OV

Status

Notes

Tags

Actions

Disable



```
matt.dfn-cert.de:~ # certbot --apache --agree-tos --email brauckmann@dfn-cert.de \  
--eab-kid LYDFFaxyTP68yoD4tlhE \  
--eab-hmac-key Z0kQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSIxH4 \  
--server https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory \  
--domain acme-demo.dfn-cert.de
```

```
brauckma@jitterbug: ~  
matt.dfn-cert.de:~ # certbot --apache --agree-tos --email brauckmann@dfn-cert.de \  
--eab-kid LYDFFaxyTP68yoD4tlhE \  
--eab-hmac-key Z0kQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSIxH4 \  
--server https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory \  
--domain acme-demo.dfn-cert.de  
Saving debug log to /var/log/letsencrypt/letsencrypt.log  
  
-----  
Would you be willing, once your first certificate is successfully issued, to  
share your email address with the Electronic Frontier Foundation, a founding  
partner of the Let's Encrypt project and the non-profit organization that  
develops Certbot? We'd like to send you email about our work encrypting the web,  
EFF news, campaigns, and ways to support digital freedom.  
-----  
(Y)es/(N)o: N  
Account registered.  
Requesting a certificate for acme-demo.dfn-cert.de  
  
Successfully received certificate.  
Certificate is saved at: /etc/letsencrypt/live/acme-demo.dfn-cert.de/fullchain.pem  
Key is saved at: /etc/letsencrypt/live/acme-demo.dfn-cert.de/privkey.pem  
This certificate expires on 2027-01-19.  
These files will be updated when the certificate renews.  
  
Deploying certificate  
Successfully deployed certificate for acme-demo.dfn-cert.de to /etc/apache2/sites-enabled/default-ssl.conf  
Congratulations! You have successfully enabled HTTPS on https://acme-demo.dfn-cert.de  
  
NEXT STEPS:  
- The certificate will need to be renewed before it expires. Certbot can automatically renew the certificate in the backgr  
ound, but you may need to take steps to enable that functionality. See https://certbot.org/renewal-setup for instructions.  
  
-----  
If you like Certbot, please consider supporting our work by:  
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate  
* Donating to EFF: https://eff.org/donate-le  
-----  
matt.dfn-cert.de:~ #
```

```
brauckma@jitterbug: ~  
matt.dfn-cert.de:~ # certbot --apache --agree-tos --email brauckmann@dfn-cert.de \  
--eab-kid LYDFFaxyTP68yoD4tlhE \  
--eab-hmac-key Z0kQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSIxH4 \  
--server https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory \  
--domain acme-demo.dfn-cert.de  
Saving debug log to /var/log/letsencrypt/letsencrypt.log  
  
-----  
Would you be willing, once your first certificate is successfully issued, to  
share your email address with the Electronic Frontier Foundation, a founding  
partner of the Let's Encrypt project and the non-profit organization that  
develops Certbot? We'd like to send you email about our work encrypting the web,  
EFF news, campaigns, and ways to support digital freedom.  
-----  
(Y)es/(N)o: N  
Account registered.  
Requesting a certificate for acme-demo.dfn-cert.de  
  
Successfully received certificate.  
Certificate is saved at: /etc/letsencrypt/live/acme-demo.dfn-cert.de/fullchain.pem  
Key is saved at: /etc/letsencrypt/live/acme-demo.dfn-cert.de/privkey.pem  
This certificate expires on 2027-01-19.  
These files will be updated when the certificate renews.  
  
Deploying certificate  
Successfully deployed certificate for acme-demo.dfn-cert.de to /etc/apache2/sites-enabled/default-ssl.conf  
Congratulations! You have successfully enabled HTTPS on https://acme-demo.dfn-cert.de  
  
NEXT STEPS:  
- The certificate will need to be renewed before it expires. Certbot can automatically renew the certificate in the backgr  
ound, but you may need to take steps to enable that functionality. See https://certbot.org/renewal-setup for instructions.  
  
If you like Certbot, please consider supporting our work by:  
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate  
* Donating to EFF: https://eff.org/donate-le  
-----  
matt.dfn-cert.de:~ #
```

Praxis mit HARICA

Tour: Fehlerfälle bei Enterprise EAB Accounts

- ▶ Domain nicht im Enterprise EAP Account hinterlegt, aber prinzipiell im Enterprise verfügbar:

`The following domains are not whitelisted: <fqdn>`

- ▶ Domain nicht im Enterprise verfügbar:

`Identifiers could not be parsed from ACME Server`

- ▶ Timeouts im Staging System:

`requests.exceptions.ReadTimeout: ...`



```
matt.dfn-cert.de:~ # certbot certonly --standalone --agree-tos --email brauckmann@dfn-cert.de --eab-kid LYDFFaxyTP68y  
oD4tlhE --eab-hmac-key Z0kQ4-ywLr_NzE8QaFbq2V95TEDJHXc --server https://acme-stg-v02.harica.gr/acme/  
0af10805-2e71-45cc-b051-8d61bd5afe51/directory --domain acme-demo1.dfn-cert.de  
Saving debug log to /var/log/letsencrypt/letsencrypt.log  
Requesting a certificate for acme-demo1.dfn-cert.de  
An unexpected error occurred:  
The following domains are not whitelisted: acme-demo1.dfn-cert.de.  
Ask for help or search for solutions at https://community.letsencrypt.org. See the logfile /var/log/letsencrypt/letsencryp  
t.log or re-run Certbot with -v for more details.  
matt.dfn-cert.de:~ #
```

Domain nicht im Enterprise EAB Account
hinterlegt, aber prinzipiell im Enterprise
verfügbar

```
brauckma@jitterbug: ~  
matt.dfn-cert.de:~ # certbot certonly --standalone --agree-tos --email brauckmann@dfn-cert.de --eab-kid LYDFFaxyTP68y  
oD4tlhE --eab-hmac-key Z0kQ4-ywLr_NzE8QaFbq2V95TEDJHgeQSPnFuS1xH4 --server https://acme-stg-v02.charica.gr/acme/  
0af10805-2e71-45cc-b051-8d61bd5afe51/directory --domain acme-demo.akjjdlgjdsldgjdlgjfdgjfdgdfg.de  
Saving debug log to /var/log/letsencrypt/letsencrypt.log  
Requesting a certificate for acme-demo.akjjdlgjdsldgjdlgjfdgjfdgdfg.de  
An unexpected error occurred:  
Identifiers could not be parsed from ACME Server  
Ask for help or search for solutions at https://community.letsencrypt.org. See the logfile /var/log/letsencrypt/letsencryp  
t.log or re-run Certbot with -v for more details.  
matt.dfn-cert.de:~ #
```

Domain nicht im Enterprise verfügbar



```
matt.dfn-cert.de:/etc/apache2/sites-enabled # certbot certonly --standalone --agree-tos --email brauckmann@dfn-cert.de
--eab-kid LYDFFaxyTP68yoD4tlhE --eab-hmac-key Z0kQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSIxH4 --server https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory --domain acme-demo.dfn-cert.de
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Renewing an existing certificate for acme-demo.dfn-cert.de
An unexpected error occurred:
requests.exceptions.ReadTimeout: HTTPConnectionPool(host='acme-stg-v02.harica.gr', port=443): Read timed out. (read timeout=45)
Ask for help or search for solutions at https://community.letsencrypt.org. See the logfile /var/log/letsencrypt/letsencrypt.log or re-run Certbot with -v for more details.
matt.dfn-cert.de:/etc/apache2/sites-enabled #
```

Timeouts im Staging-System

Praxis mit HARICA

Tour: Nutzung der EAB Accounts mit Apache `mod_md`

Harica CertManager - Ent

cm-stg.harica.gr/PrevalidatedEnterprises

Email

Client Auth

More

Validated Information

Data privacy statement

Help / Guides

GREEK UNIVERSITIES NETWORK (GUnet)

General Commercial Registry

Number: 160729401000

Friendly Name	Organization	Created By	Created At	Status
jbr-acme-demo	DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	09/01/2026	

Details

Certificates

Domains

Organization

DFN-CERT Services GmbH - Stage

Created At

Friday, January 9, 2026

Created By

jbr-ea@dfn-cert.de

Key ID

LYDFFaxyTP68yoD4tlhE

HMAC Key

ZOkQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSlxH4

Server URL

https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory

Certificate Type

SSL OV

Status

Notes

Tags

Actions

Disable



```
matt.dfn-cert.de:/etc/apache2 # a2enmod md ssl
```

```
Module md already enabled
```

```
Considering dependency mime for ssl:
```

```
Module mime already enabled
```

```
Considering dependency socache_shmcb for ssl:
```

```
Module socache_shmcb already enabled
```

```
Module ssl already enabled
```

```
matt.dfn-cert.de:/etc/apache2 #
```



```
matt.dfn-cert.de:/etc/apache2 # a2enmod md ssl
```

```
Module md already enabled
```

```
Considering dependency mime for ssl:
```

```
Module mime already enabled
```

```
Considering dependency socache_shmcb for ssl:
```

```
Module socache_shmcb already enabled
```

```
Module ssl already enabled
```

```
matt.dfn-cert.de:/etc/apache2 # head sites-enabled/default-ssl.conf
```

```
MDomain acme-demo.dfn-cert.de
```

```
MContactEmail dfnpca@dfn-cert.de
```

```
MCertificateAuthority https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory
```

```
MCertificateAgreement accepted
```

```
MExternalAccountBinding /etc/apache2/secret/harica-eab-file
```

```
<VirtualHost *:443>
```

```
    ServerName acme-demo.dfn-cert.de
```

```
    DocumentRoot /var/www/html
```

```
matt.dfn-cert.de:/etc/apache2 #
```



```
matt.dfn-cert.de:/etc/apache2 # a2enmod md ssl
```

```
Module md already enabled
```

```
Considering dependency mime for ssl:
```

```
Module mime already enabled
```

```
Considering dependency socache_shmcb for ssl:
```

```
Module socache_shmcb already enabled
```

```
Module ssl already enabled
```

```
matt.dfn-cert.de:/etc/apache2 # head sites-enabled/default-ssl.conf
```

```
MDomain acme-demo.dfn-cert.de
```

```
MDContactEmail dfnpca@dfn-cert.de
```

```
MDCertificateAuthority https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory
```

```
MDCertificateAgreement accepted
```

```
MDExternalAccountBinding /etc/apache2/secret/harica-eab-file
```

```
<VirtualHost *:443>
```

```
    ServerName acme-demo.dfn-cert.de
```

```
    DocumentRoot /var/www/html
```

```
matt.dfn-cert.de:/etc/apache2 # cat secret/harica-eab-file
```

```
{"kid": "LYDFFaxyTP68yoD4tlhE", "hmac": "Z0kQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSIxH4"}
```

```
matt.dfn-cert.de:/etc/apache2 #
```



```
matt.dfn-cert.de:/etc/apache2 # a2enmod md ssl
```

```
Module md already enabled
```

```
Considering dependency mime for ssl:
```

```
Module mime already enabled
```

```
Considering dependency socache_shmcb for ssl:
```

```
Module socache_shmcb already enabled
```

```
Module ssl already enabled
```

```
matt.dfn-cert.de:/etc/apache2 # head sites-enabled/default-ssl.conf
```

```
MDomain acme-demo.dfn-cert.de
```

```
MDEmail dfnpca@dfn-cert.de
```

```
MDCertificateAuthority https://acme-stg-v02.harica.gr/acme/0af10805-2e71-45cc-b051-8d61bd5afe51/directory
```

```
MDCertificateAgreement accepted
```

```
MDExternalAccountBinding /etc/apache2/secret/harica-eab-file
```

```
<VirtualHost *:443>
```

```
    ServerName acme-demo.dfn-cert.de
```

```
    DocumentRoot /var/www/html
```

```
matt.dfn-cert.de:/etc/apache2 # cat secret/harica-eab-file
```

```
{"kid": "LYDFFaxyTP68yoD4tlhE", "hmac": "Z0kQ4-ywLr_NzE8QaFbq2V95TEDJHXqeQsPnFuSIxH4"}
```

```
matt.dfn-cert.de:/etc/apache2 # apache2ctl restart
```

```
matt.dfn-cert.de:/etc/apache2 # apache2ctl restart
```

Praxis mit HARICA

Personal EAB Accounts:

- ▶ Für alle User, die im certmanager dem Enterprise zugeordnet sind
- ▶ Generelle Funktion nur nach Freischaltung Enterprise Admin
- ▶ SSL DV (ohne Organisationsinformation)
- ▶ Alle Domains aus dem Enterprise, dem der User zugeordnet ist, verfügbar (auch nicht vorvalidierte)
- ▶ Immer mit ACME Challenge zur Berechtigungsprüfung

Praxis mit HARICA

Tour durch das HARICA-Interface:

- ▶ Enterprise Admin: Freischalten von Personal ACME für alle User

📊

My Dashboard

📄

eSign Documents

☰

ACME

Certificate Requests

📄

eSignatures

📄

eSeals

🔒

Server

📺

Code Signing

✉️

Email

👤

Client Auth

More

Enterprises

Users

Certificates

Bulk Certificates

ACME

Enterprises

Search

▼

🔍

Alias	Email	Domains
DFN-CERT - Stage	dfnpca@dfn-cert.de	uni-pellworm.de, dfn-cert.de

Enterprises

Domains

Legal Name	Country Locality	Domain
DFN-CERT Services GmbH - ...	DE , Hamburg	uni-pellworm.de, dfn-cert.de

Harica CertManager - Ent

cm-stg.harica.gr/PrevalidatedEnterprises

☆🔖👤⋮

☰

HA

My Dashboard

eSign Documents

ACME

Certificate Request

eSignatures

eSeals

Server

Code Signing

Email

Client Auth

More

FQDN

uni-pellworm.de, dfn-cert.de

DN

O=DFN-CERT Services GmbH - Stage, ST=Hamburg, C=DE

Validity

OV: 14/04/2027
EV: 08/01/2025

(EN)

Organization official name

DFN-CERT Services GmbH - Stage

(local language)

ASCII-fied Name

Organizational Unit

State or province

Hamburg

Locality name

ISO 3166-1 Alpha-2

(EN)

Country

DE

Germany

Organization Identifier

NTRDE-DEK1101R.HRB88805

Group

Product list

History

Jurisdiction Country

Remote eSignature

DSA

Max

🔑🌐➡️

Tags

J Admin Br

Harica CertManager - Ent

cm-stg.harica.gr/PrevalidatedEnterprises

☆ | 🏠 | 👤 | ⋮

☰

HA

My Dashboard

eSign Documents

ACME

Certificate Request

eSignatures

eSeals

Server

Code Signing

Email

Client Auth

More

Admin Br

FQDN

uni-pellworm.de, dfn-cert.de

DN

O=DFN-CERT Services GmbH - Stage, ST=Hamburg, C=DE

Validity

OV: 14/04/2027
EV: 08/01/2025

Organization official name

ASCII-fied Name

Organizational Unit

State or province

Locality name

Country

DE

Germany

Organization Identifier

NTRDE-DEK1101R.HRB88805

Group

Product list

History

Remote eSignature

DSA

Max

Update Enterprise tags

#IGTF-Organization

#ACME-Personal

Save

Praxis mit HARICA

Tour durch das HARICA-Interface:

- ▶ User: Erzeugen eines Personal EAB Accounts

- 📊

My Dashboard
- 📁

eSign Documents
- 📋

ACME

Certificate Requests

- 📁

eSignatures
- 📁

eSeals
- 🔒

Server
- 📅

Code Signing
- ✉

Email
- 👤

Client Auth

More

My Dashboard

- SSL
- eSignature
- Token
- eSeal
- S/MIME
- Remote
- Code Signing

Cancelled Requests

Product	Details	Information	Actions
SSL DV	Pending Transactions Expiration	testserver	⋮
S/MIME	Pending Transactions Expiration		⋮
SSL DV	Pending Transactions Expiration	jitterbug	⋮
S/MIME	Pending Transactions Expiration		⋮

 My Dashboard

 eSign Documents

 ACME

Certificate Requests

 eSignatures

 eSeals

 Server

 Code Signing

 Email

 Client Auth

More

Manage ACME EAB Accounts

To issue SSL/TLS server certificates using the ACME protocol, you must first create an ACME External Account Binding (EAB) account. This account currently allows you to obtain Domain Validated (DV) certificates by demonstrating control over your domain using the supported ACME challenge types: HTTP-01 and DNS-01.

Please note: You may have up to three (3) active EAB accounts at any given time.

Create +


Organization	Created By	Created At	Status
DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	24/06/2025	
DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	19/06/2025	
DFN-CERT Services GmbH - Stage	jbr-ea@dfn-cert.de	19/06/2025	

DFN

Ausblick

Ausblick

Fortgeschrittene Themen:

- ▶ Systeme, die nicht outbound zum ACME Server kommunizieren können
 - ▷ Lösung: Zentrales System in der Infrastruktur, dass als ACME Client Zertifikate bezieht und intern weiterverteilt
- ▶ dns-01 challenges

Jetzt ist der richtige Zeitpunkt,
mit der Automatisierung zu beginnen.

- ▶ Kontakt: dfnpca@dfn-cert.de
- ▶ Dokumentation auf
<https://doku.tid.dfn.de/de:dfnpki:tcs:2025:acme>
- ▶ Community auf dfnpki-d-Mailingliste
<https://www.listserv.dfn.de/sympa/info/dfnpki-d>

