SSL/TLS server certificates overview (DFN-PKI / HARICA)

08.11.2025 11:24:29

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	08:36:03 - 04.11.2025

Schlüsselwörter

Serverzertifikat Zertifikatsbeantragung ACME PKI TLS SSL CSR Sectigo OpenSSL Server Webserver Zertifikat Harica

Lösung (öffentlich)

Server certificates for web servers can be obtained via the PKI of the DFN (currently operated by HARICA). Certificates should be obtained through the ACME protocol. Certificate domains will be validated during the certificate issuing process.

In the most common case (Debian/Ubuntu server with Apache webserver) you can get a certificate with the following commands:

- install certbot:

sudo apt install certbot python3-certbot-apache

- issue a certificate and install it in Apache:

sudo certbot run -m ADMIN-EMAIL@tu-dresden.de --server [1]https://acme.pki.cert.tu-dresden.de/ -d example1.tud.de

More details about ACME clients and their usage can be found in [2]ACME Clients.

What is ACME?

ACME is a network protocol by which a server can obtain tls server certificates from a certificate authority (CA) in an automated way. During this process, the CA will verify that the requesting server controls the domain names that will be addedd to the certificate. This work roughly like this:

- server requests a certificate for example.tud.de through ACME
- the CA tells the servers a random value (e.g. 9182) and asks it to place it in a file 123.txt in the webserver
- The server write the value to a file that can be accessed at [3]http://example.tud.de/.well-known/acme-challenge/123.txt
- the CA fetches the url and if the random value matches, the certificate will be issued

This validation will be carried out by a system on the TUD campus network (acme.pki.cert.tu-dresden.de). Due to this, servers must be accessible via HTTP from the campus network. The servername must be registered in the official DNS system. But the server doesn't have to be accessible from the internet.

What to do if ACME is not possible?

There are various scenarios in which it is not possible to use ACME as described before:

-

internal servers where port 80 is not accessible (and cannot be made accessible) from TUD campus network

-

servers with wildcard DNS entries and wildcard certificates

-

Servers are managed via configuration management, certificates are rolled out through config management

-

Servers/commercial appliances that do not support ACME or only support certain providers

-

Cluster setups where it cannot be guaranteed that the ACME challenge will be processed by the server where the ACME client is running

In such cases, the preferred option is to activate/authorize an ACME accounts for individual domains. This ACME account is to be used on a protected administrative computer to obtain server certificates. Instructions can be found in "ACME account activation".

In exceptional cases, it is also possible to submit a CSR for certificate creation via the Service Desk. However, ACME should be preferred in most cases

because certificate issuance and renewal can be automated. There are plans to cut certificate validity in the internet to 30 days. If this is implemented, the effort required for manual certificate renewal is not sustainable.

Requirements and restrictions for server certificates
-

Certificates can only be issued for domains that are assigned to TU Dresden, i.e. the domain should meet the requirements for domains from the IT regulations (subdomain of tu-dresden.de or project domain registered via TU Dresden)

-

No certificates can be issued for IP addresses

-

The domains must be registered and validated with the certification authority (CA) HARICA

-

the CA mus check for "CAA" DNS records for the requested domains and higher level domains. If such records exist, they must contain "harica.gr". This is already configured for domains managed by ZIH

-

All domains in the certificate require a DNS entry pointing to an IP in the TU Dresden campus network (does not apply to ACME accounts with activation)

-

All domains in the certificate require a DNS entry pointing to the server on which the ACME client is running (does not apply to ACME accounts with activation)

-

The domains in the certificate must be accessible via HTTP (Port 80) from the server acme.pki.cert.tu-dresden.de (does not apply to ACME accounts with activation)

-

at most 100 domains (Subject Alternative Names, SANs) can be used per certificate

[1] https://acme.pki.cert.tu-dresden.de/
[2] https://faq.tickets.tu-dresden.de/v/ItemID=1280
[3] http://example.tud.de/.well-known/acme-challenge/123.txt