SSL/TLS Serverzertifikate Überblick (mit DFN-PKI / HARICA)

03.07.2025 08:21:56

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	**Bewertungen:**	3
Status:	öffentlich (Alle)	**Ergebnis:**	58.33 %
Sprache:	de	**Letzte Aktualisierung:**	07:43:04 - 03.06.2025

Schlüsselwörter

Zertifikatsbeantragung ACME Certificate PKI TLS ssl CSR Sectigo OpenSSL Server Webserver Zertifikat Harica

Lösung (öffentlich)

Über die PKI des DFN (aktuell betrieben durch HARICA) können Serverzertifikate bezogen werden. Der Bezug von Zertifikaten sollte über das ACME-Protokoll erfolgen. Während des Ausstellungsprozesses der Zertifikate werden die Domains validiert.

Im einfachsten Fall (Debian Server mit Apache Webserver) erhalten Sie mit den folgenden Kommandos ein neues Zertifikat:
- Certbot installieren:

sudo apt install certbot python3-certbot-apache

- Zertifikat ausstellen und im Apache installieren:

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

Weitere Details zu ACME Clients sind im Artikel [1]ACME Clients beschrieben.

Was ist ACME? ACME ist ein Protokoll, über das Server automatisiert Zertifikate von einer Zertifizierungsstelle (CA) beziehen können. Dabei prüft die CA ob der Anfragende die Kontrolle über die Domains hat, die im Zertifikat stehen sollen. Das läuft in etwa wie folgt ab:
- Server fragt per ACME ein Zertifikat für beispiel.tud.de an
- CA nennt dem Server einen zufälligen Wert (z.B. 9182) und fordert ihn auf diesen in der Datei 123.txt abzulegen
- Server schreibt den Wert in eine Datei, die unter http://beispiel.tud.de/.well-known/acme-challenge/123.txt abgerufen werden kann
- CA ruft die Datei ab, wenn der zufällige Wert (9182) drin steht, wird das Zertifikat ausgestellt

Diese Überprüfung wird bei uns von einem internen System (acme.pki.cert.tu-dresden.de) durchgeführt. D.h. die Server müssen zur Zertifikatsausstellung per HTTP (Port 80) aus dem Campus erreichbar sein. Der Servername muss im offiziellen DNS registriert sein.

Was tun, wenn ACME nicht möglich ist? Es gibt verschiedene Szenarien, in denen es nicht möglich ist, einen ACME-Client zu benutzen:
- Interne Server ohne campusweiten DNS Namen oder die nicht per HTTP (Port 80) aus dem Campus erreichbar sind
- Server werden über ein Konfigurationsmanagement verwaltet, Zertifikate werden darüber ausgerollt
- Server/kommerzielle Appliances, die kein ACME unterstützen oder nur bestimmte Anbieter unterstützen
- Cluster-Setups, bei denen nicht garantiert werden kann, dass die ACME-Challenge von dem Server bearbeitet wird, wo der ACME-Client läuft

Hierbei ist die bevorzugte Option, einen ACME-Account für einzelne Domains freizuschalten, der auf einem abgesicherten administrativen Rechner eingrichtet wird und zum Ausstellen von Zertifikaten benutzt wird. Eine Anleitung dazu findet sich in [2]ACME Account Freischaltung

In Ausnahmefällen ist es auch möglich, einen CSR für die Zertifikatserstellung über den Service Desk einzureichen. Allerdings sollte versucht werden, ACME zu nutzen, da dort der Zertifikatsbezug und die Erneuerung automatisiert werden kann. Es gibt Pläne, die Gültigkeit von Serverzertifikaten im Internet grundsätzlich auf 30 Tage zu begrenzen. Wenn das umgesetzt wird, ist der Aufwand zur manuellen Erneuerung von Serverzertifikaten nicht mehr tragbar.
Voraussetzungen und Einschränkungen zum Bezug von Serverzertifikaten
- Es können nur Zertifikate für Domains ausgestellt werden, die der TU Dresden zugeordnet sind, d. h. die Domain sollte den Vorgaben zu Domains aus der IT-Ordnung genügen (Subdomain von tu-dresden.de oder über die TU Dresden registrierte Projekt-Domain)
- es können keine Zertifikate für IP-Adressen ausgestellt werden
- Domains müssen bei der Zertifizierungsstelle (CA) HARICA registriert und validiert sein
- die CA überprüft im DNS ob es einen "CAA" Record für die Domain oder übergeordnete Domains gibt; Falls ja, muss "harica.gr" darin aufgeführt sein. Für Domains die vom ZIH verwaltet werden ist das gegeben
- alle Domains im Zertifikat benötigen einen DNS-Eintrag, der auf eine IP im Campusnetz der TU Dresden zeigt (nicht relevant bei ACME mit Account-Freischaltung)
- alle Domains im Zertifikat benötigen einen DNS-Eintrag, der auf den Server zeigt, auf dem der ACME Client ausgeführt wird (nicht relevant bei ACME mit Account-Freischaltung)
- die Domains im Zertifikat müssen per HTTP (Port 80) vom Server acme.pki.cert.tu-dresden.de erreichbar sein (nicht relevant bei ACME mit Account-Freischaltung)
- es können max. 100 Domains (Subject Alternative Names, SANs) pro Zertifikat

beantragt werden

[1] https://faq.tickets.tu-dresden.de/v/ItemID=1274
[2] http://faq.tickets.tu-dresden.de/v/ItemID=1298