[de] Zertifikate - Beantragung SSL Zertifikate - Server Zertifikate per ACME (mit DFN-PKI / SECTIGO)

29.04.2024 04:29:35

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	**Bewertungen:**	1
Status:	öffentlich (Alle)	**Ergebnis:**	100.00 %
Sprache:	de	**Letzte Aktualisierung:**	13:54:37 - 08.01.2024

Schlüsselwörter

Zertifikatsbeantragung ACME Certificate PKI TLS Webserver Zertifikat ssl ACME CSR

Lösung (öffentlich)

Die PKI des DFN (aktuell betrieben durch SECTIGO) unterstützt das ACME-Protokoll zum Beantragen und Ausstellen von Serverzertifikaten. Um ACME zu nutzen, muss ein ACME-Account erstellt und zum Ausstellen von Zertifikaten für bestimmte Domains legitimiert werden [1]. Für jeden Server sollte unbedingt ein separater ACME-Account benutzt werden [2]. Eine Validierung der Domain beim Ausstellen der Zertifikate ist nicht immer notwendig, siehe unten.

Beantragungsprozess

die Serveradmins beantragen beim Service Desk einen ACME-Account für den offiziellen tu-dresden.de Hostnamen des Servers und ggf. weitere Domains, die auf dem Server betrieben werden.

der Service Desk prüft, dass die Admin für die beantragten Domains zuständig ist.

der Service Desk erstellt einen ACME-Account, vergibt Berechtigungen für die Domains und schickt die Zugangsdaten an die Admin

die Admins richten den ACME Client auf dem Server ein. Der ACME Client muss "External Account Bindung" (EAB) unterstützen (z. B.certbot, acme.sh oder win-acme).

der ACME Client beantragt ein Zertifikat. Falls eine Domain [3] nicht durch SECTIGO validiert wurde bzw. die letzte Domainvalidierung länger als 12 Monate zurückliegt, wird analog zu Letsencrypt eine Domain Validierung per ACME Challenge durchgeführt.

Weitere Informationen zu certbot, z. B. zum automatischen Erneuern von Zertifikaten, finden Sie in der offiziellen certbot Doku:
[1]https://certbot.eff.org/docs

Voraussetzungen

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).

[1] Im Gegensatz zu ACME bei Letsencrypt wird bei SECTIGO die Organisationszugehörigkeit überprüft. Das bedeutet, Domains sind immer einer Organisation zugeordnet und Zertifikate dürfen nur von ACME-Accounts beantragt werden, die der gleichen Organisation zugeordnet sind.

[2] Wir raten dringend davon ab, den gleichen ACME-Account auf mehreren Systemen zu nutzen, u. a. um die Auswirkungen bei einer Kompromittierung zu beschränken. Eine Ausnahme könnte sein, wenn Serverzertifikate auf einem zentralen Managementsystem erstellt/beantragt werden und über ein Konfigurationsmanagement-Tool auf die Server verteilt werden.

[3] Genauer eine sogenannte Second-Level bzw. registrierbare Domain, d. h. eine Domain aus der öffentlichen Suffix-Liste plus dem Domainteil davor. z. B.: tu-dresden.de, bbc.co.uk, google.de

[1] https://certbot.eff.org/docs