[en] Certificate -SSL Certificate Request - server certificates with ACME (in DFN-PKI / SECTIGO)

09/17/2024 18:50:06

FAQ Article Print

Category:	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	en	**Last update:**	13:55:03 - 01/08/2024

Keywords

ACME TLS certificate PKI Webserver ssl Zertifikatsbeantragung ACME CSR

Solution (public)

The PKI (public key infrastructur) of the DFN (currently operated by SECTIGO) supports the ACME protocol to request and issue server certificates. To use ACME, an ACME account must be created and assigned permissions to request certificates for specific domains [1]. We strongly recommend to use a separate ACME account for each server.

Requesting an ACME account

the server admins request an ACME account for the server's official tu-dresden.de hostname and optionally further domain names hosted on the server by sending an email to the service desk.

the service desk verify that the admin is responsible for the requested domains

the service desk creates an ACME account and assigns permission for the requested domains. The ACME credentials are sent to the admin

the server admin configures the ACME client software on the server. The software must support "External Account Bindung" (EAB) (e.g. certbot, acme.sh or win-acme).

the ACME client requests (and installs) a certificate

if one of the domains [3] in the certificate requests has not been validated by SECTIGO before, or the previous validation was more than 1 year ago, SECTIGO initiiates a domain validation via ACME challenge (like it would happen with Letsencrypt)

For more information about certbot, e.g. on how to set-up auto-renewal of certificates, please see the official certbot docs:
[1]https://certbot.eff.org/docs

Preconditions

SECTIGO can only issue certificates for domains associated to TU Dresden. This means the domain should comply with the rules described in TUD's IT regulations (sudomains to tu-dresden.de or project domain registered through TU Dresden).

[1] In contrast to ACME as deployed by Letsencrypt, SECTIGO validates organization membership. This means, a domain is always associated to an organisation and certificates may only be requested by ACME accounts in the same organization.

[2] We strongly object against using the same ACME account on multiple servers to limit the impact of a potential compromise. An exception to this would be a scheme where certificates are generated/requested on a central management system and deployed to individual servers via a configuration mangement tool.

[3] Applies to "registrable domains" only, ie. an entry from the public suffix list plus one additional label. E.g. tu-dresden.de, bbb.co.uk, google.de, but not zih.tu-dresden.de

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