Server-Zertifikate

Warum benötige ich Server-Zertifikate?

- Das Zertifikat dient als Grundlage für verschlüsselte, authentifizierte und manipulationsfreie Datenübertragung bei Nutzung von Netzdiensten (beispielsweise per https) oder auch für die Signierung und Verschlüsselung von E-Mails.
- Nach dem Import der CA-Zertifikate in die Client-Anwendung (Mozilla Firefox, Mozilla Thunderbird etc.) werden die von der TU Clausthal CA ausgestellten Zertifikate automatisch von den Nutzerprogrammen akzeptiert. Aufforderungen zur manuellen Überprüfung von Zertifikaten werden nicht mehr angezeigt.

Beantragung eines Server-Zertifikats

Zur Beantragung eines Server-Zertifikats sind die Beachtungen einiger Formalia unumgänglich:

- Basisinformationen über den Rechner, für den ein Zertifkat beantragt wird
- Ein Zertifikatsantrag, „certificate request“ muss erstellt werden
- Beantragung durch eine akkreditierte Person
- Installation des Zertifikates und Konfiguration des Dienstes für die Verwendung des Zertifikates

Während die eigentliche CA, die Zertifizierungsinstanz, beim DFN-Verein angesiedelt ist, ist im Rechenzentrum die Registrierungs-Instanz (RA) untergebracht, die sich um die Einhaltung der Zertifizierungsrichtlinien kümmert und die entspr. Anträge bearbeitet.

Basisinfos

Laut CA-Policy sind etliche Zertifikatsattribute vorgegeben, die den Rechner bzw. Server identifizieren sollen:

CN-Attribut

Das CN-Attribut ist der FQDN, der „fully qualified domain name“, des Rechners, der mit den Kommandos nslookup bzw. host per DNS abgefragt werden kann. Es muss der Name gesetzt werden, unter dem der Dienst im Netz erreichbar sein soll.

Das Email-Attribut benennt eine administrative Email-Adresse, an welche Anfragen zu richten sind, falls es Probleme mit dem angebotenen Dienst des Servers gibt. Diese Email-Adresse muß auf tu-

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.

clausthal.de enden! und einen gültigen Empfänger besitzen.

OU-Attribut

Laut Policy sind mehrere OU-Attribute (organisational unit) erlaubt.

- Es dürfen nur etablierte Namen und Kurzformen verwendet werden.
- Umlaute sind nicht erlaubt.
- Die OU-Attribute dürfen sich nicht widersprechen.

Beantragung und Installation von Server-Zertifikaten

- Zertifikatsbeantragung
- Zertifikatsinstallation unter Linux/Unix
- Zertifikatsinstallation unter Windows

Direkt-Link:
https://doku.tu-clausthal.de/doku.php?id=sonstige_dienste:ssl-zertifikate:server-zertifikate&rev=1666164292

Letzte Aktualisierung: **07:24 19. October 2022**

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.