

DFN-CERT

deutsches forschungsnetz



Neues aus der DFN-PKI

83. Betriebstagung | 07.10.2025

Jürgen Brauckmann

DFN

DFN-PKI Global



Erhaltungsbetrieb:

- ▶ Noch >100.000 gültige User-Zertifikate
 - ▶ Bis 2027-03-22
- ▶ **Sperrungen** selbstverständlich nach wie vor möglich
- ▶ PKI wird weiterhin **auditert**
 - ▶ Anpassungen CP/CPS an aktuelle Vorgaben
 - ▶ Technik-Änderungen wo notwendig

DFN

GÉANT TCS



ACME seit Ende Juni verfügbar

► Wie bei TCS 2024: Mit ACME External Account Binding (EAB)

```
certbot certonly --standalone --non-interactive --agree-tos  
--email <eigene Mailadresse>  
--eab-kid <Key ID> --eab-hmac-key <HMAC Key> --server <Server URL>  
--domain <FQDN des Zertifikats>
```

► Varianten:

- Enterprise ACME SSL OV und SSL DV
- Personal ACME
- Je nach Variante nur für validierte oder auch nicht validierte Domains

ACME Enterprise Accounts

- ▶ Konfiguriert vom Enterprise Admin
- ▶ Exakte **Konfiguration** von möglichen FQDN/Domains
- ▶ Variante **OV** mit Org-Informationen. Nur für bereits validierte Domains
- ▶ Variante **DV**. Auch für konfigurierte, aber nicht validierte Domains
(dann mit ACME Challenge http-01 oder dns-01)
- ▶ **Übernahme** von Validierungen durch ACME-Challenges in cert-manager in Vorbereitung

ACME Personal Accounts

- ▶ Erst nach **Freischaltung** im Enterprise. Dann: Für jeden User in diesem Enterprise zugänglich
- ▶ SSL DV (ohne Org-Informationen)
- ▶ Für alle konfigurierten Domains im Enterprise, auch unvalidierte
- ▶ Immer mit **ACME Challenge** http-01 oder dns-01

ACME Challenges

Account Typ	Variante	Domain	Challenge?
Enterprise	SSL DV	vorvalidiert	nein
		nicht validiert	ja
Enterprise	SSL OV	vorvalidiert	nein
		nicht validiert	nicht möglich, Fehler
Personal		vorvalidiert	ja
		nicht validiert	ja

S/MIME per AAI

- ▶ Kein separates Portal, sondern **Datenübernahme** bei Academic Login
- ▶ Voraussetzung:
 - ▶ eduPersonPrincipleName
 - ▶ eduPersonEntitlement
`urn:mace:terena.org:tcs:smime-sv-autoissue` oder
`urn:mace:terena.org:tcs:personal-user`

(Wichtig: Nur nach **Identifizierung** der User in der Organisation!)
- ▶ Bezug von S/MIME IV+OV mit Übernahme von Vor/Nachname und automatischer Ausstellung

S/MIME

- ▶ HARICA **sperrt** korrekterweise Zertifikate mit offensichtlich falschen Daten
- ▶ Keine Zertifikate "CN=Poststelle" oder "CN=Test Test" erstellen!
 - ▶ Gruppen/Funktionszertifikate per Typ `email-only`
- ▶ Immer valide Identifizierung für IV+OV-Zertifikate vorhalten!

Web-PKI

Web-PKI

Risiken unverändert

- ▶ Microsoft muss xx Millionen Zertifikate **sperren**
 - ▷ Grund: quasi "Tippfehler" im CPS
 - ▷ Zertifikate aus Kundensicht vollkommen OK
- ▶ Diskussionen um Validierungen bei Digicert
 - ▷ Ursache: Definitionen in den Baseline Requirements prinzipbedingt nicht absolut exakt

=> Zertifikatsperrungen aufgrund von unvorhersehbaren Ereignissen können **jederzeit** auftreten

Web-PKI

Änderungen

- ▶ Spätestens ab **15.03.2026:**
Serverzertifikate und Domainvalidierungen nur noch max. **200 Tage** gültig!
- ▶ Spätestens ab **15.06.2026:**
Kein **ClientAuth** mehr in Serverzertifikaten!

Perspektive

- ▶ **ACME Renewal Information** (ARI, RFC 9773) kann das Problem der Sperrungen lösen:
 - ▶ ACME Client ("certbot") kann von der CA regelmäßig abfragen, wann ein Zertifikat zu erneuern ist.
 - ▶ CA signalisiert den Clients bei Sperrungen die vorzeitige Erneuerung
- ▶ **Domainvalidierungsmethoden** entwickeln sich weiter (z.B. "DNS TXT Record with Persistent Value")

DFN

Fazit

Fazit

- ▶ GÉANT TCS:
 - ▷ ACME und S/MIME AAI funktioniert
- ▶ Ab 15.03.2026:
 - ▷ Nur noch 200 Tage Laufzeit für Serverzertifikate und Domainvalidierungen
- ▶ Ab 15.06.2026:
 - ▷ Keine ClientAuth mehr in Serverzertifikate

Haben Sie noch Fragen?

DFN

► Kontakt:

DFN-PCA

dfnpca@dfn-cert.de

<https://www.pki.dfn.de>

<https://blog.pki.dfn.de>

