DFN-CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

82. Betriebstagung | 25.03.2025

Jürgen Brauckmann

DFN

GÉANT TCS

PKI-Agilität

Vorbereiten auf:

- kurzfristige **Sperrungen**
- Wechsel von **Root-Zertifikaten**
- Verkürzung von **Zertifikatlaufzeiten**
- Änderung von **Prozessen**
- **(Dienstleisterwechsel)**

Es wird nie mehr so stabil wie 2010-2020...

Betriebstagung 2024-10

GÉANT TCS

- November 2024:
  - TCS-Anbieter **kündigt** den Vertrag mit GÉANT
- Dezember 2024:
  - DFN sichert **Übergangsvertrag** mit neuem Anbieter
  - Zum 20.12.2024 alle Einrichtungen in neuem Anbieter angelegt
- 10.01.2025:
  - Alter Anbieter stellt Zertifikaterstellung für GÉANT ein
  - Sperrungen nicht mehr über SCM möglich, nur per Mail an den Support
- April 2025:
  - Vertragsübergang zu GÉANT ohne technische Auswirkungen

GÉANT TCS

Neuer Anbieter HARICA:

- Teil des griechischen Universitätsnetzes GUnet
- Seit Jahren **Vertrauensdiensteanbieter** nach eIDAS
- Im CA/Browser-Forum sehr aktiv
- Sehr technisch orientiert
- Zugänglicher als der alte Anbieter

GÉANT TCS

Zur Verfügung stehende Arbeitsabläufe *Serverzertifikate*:

- Beantragung per CSR oder Schlüsselerzeugung im Browser
  - Login per AAI oder selbst-erzeugtem Account
  - (Manuelle) Genehmigung durch Rolle Enterprise Approver
  - Zertifikatstyp DV oder OV möglich
- Verwaltung von ACME EAB wird zur Zeit entwickelt
  - Derzeitige Zeitplanung **Ende April**

GÉANT TCS

Zur Verfügung stehende Arbeitsabläufe *S/MIME-Zertifikate*:

- Self-Service:
  - Login per AAI oder selbst-erzeugtem Account
  - CSR oder Schlüsselerzeugung im Browser
  - Zertifikattypen:
    - Email-only: Mail-Challenge, kein weiterer Genehmigungsschritt
    - IV+OV: Identitätsprüfung, Genehmigung
- Administrative Erzeugung:
  - per CSV-Upload
  - Optional auch als IV+OV. Achtung: **Identitätsprüfung**

Automatisierung:

- HARICA API kann auch für eigene Tools verwendet werden
- Aber: Viele Funktionen **nicht** auf Automatisierung zugeschnitten, sondern Web-UI
- Autorisierung **"gewöhnungsbedürftig"**
- Viele Beispiele verlinkt
  https://doku.tid.dfn.de/de:dfnpki:harica2025

GÉANT TCS

Abläufe in Entwicklung:

- ACME EAB inkl. Verwaltung der Keys
- Reduziertes Self-Service-Portal für AAI und S/MIME mit Vorname/Nachname

Nachteile, offene Punkte, Kritik:

- Unvollständige Ankündigung von Updates
- API eher schräg
- Kein Prozess "Erneuerung auf Knopfdruck"
- Andere Begrenzungen als bei Sectigo/DFN-PKI (z.B. nur 100 SaN)
- Keine S/MIME-Zertifikate mit Org-Namen und Mail-Adresse
  - Ersatz: email-only
- Produkte zur digitalen Signatur sichtbar, aber nicht verfügbar

Zeitpläne Laufzeit Serverzertifikate

Zeitpläne

Laufzeit von Serverzertifikaten:

- Starke Motivation auf Browserseite für kürzere Zertifikatlaufzeiten
  - "bessere Qualität"
- März 2023: Erster informeller Vorstoß von Google
  - Ziel **90 Tage** lang gültige Serverzertifikate
- Oktober 2024: Formaler Vorschlag von Apple
  - Direkt als Änderung der Baseline Requirements formuliert
  - Ziel **45 Tage** lang gültige Serverzertifikate plus **drastische Verkürzung** von Revalidierungszeiten

Zeitpläne

Vorschlag von Apple für **Serverzertifikate**:

- Zertifikat-Laufzeit:
  - 2026-03: 200 Tage
  - 2027-03: 100 Tage
  - 2029-03: 47 Tage
- Wiederverwendung von Domainvalidierungen:
  - 2026-03: 200 Tage
  - 2027-03: 100 Tage
  - 2028-03: 10 Tage
- Wiederverwendung von Subject Identity Information:
  - 2026-03: 200 Tage

Draft Draft Draft Draft DFN

Zeitpläne

Derzeitiger Zustand:

- **Entwurf** als Änderung

  Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates

- Ausführliche Diskussion hat stattgefunden

- Weitere Diskussionen? Abstimmung?

Zeitpläne

Bei Annahme des Vorschlags:

- Alles nur für **Serverzertifikate!**
- Zertifikatausstellung und -erneuerung muss **automatisiert** werden
  - Nur 47 Tage Laufzeit ab 2029
- Domainvalidierung muss **automatisiert** werden
  - Revalidierung alle 10 Tage ab 2028
  - Mails an hostmaster@ nicht mehr praktikabel
- Zertifikate mit Organisationsinformationen (OV) werden **aufwändiger**
  - Daten müssen alle 200 Tage revalidiert werden

Draft Draft Draft DFN

Fazit

Fazit

- GÉANT TCS:
  - Migration zu HARICA
- Laufzeitverkürzung Serverzertifikate:
  - Drastisch verkürzte Laufzeiten in der Diskussion
  - Automatisieren!

Haben Sie noch Fragen?

- Kontakt:

  DFN-PCA

  dfnpca@dfn-cert.de

  https://www.pki.dfn.de

  https://blog.pki.dfn.de