DFN-CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

84. Betriebstagung | 17.03.2026

Jürgen Brauckmann

Automatisierung

Automatisierung

- Laufzeitverkürzung Serverzertifikate auf **199 Tage** wurde in KW11/2026 umgesetzt
- Nächster Schritt: **100 Tage** ab März 2027

  => Automatisieren!
- Wie? Z.B. mit ACME!
  - Foliensatz aus Webinaren 22.01. und 03.02. verfügbar: https://doku.tid.dfn.de/_media/de:dfnpki:harica:2026-01-22-automatisierung.pdf

Zertifikatprofile

ClientAuth in Serverzertifikaten

- Anwendungsfall: Gegenseitige AuthN zwischen Systemen.

  Z.B. Datenbankanbindung, SMTP, …

- Google Chrome Root Programm fordert jetzt von CAs:
  - **Keine** ClientAuth mehr in normalen Serverzertifikaten!
  - Nur möglich in separaten oder Private Trust PKIs wie DFN-Verein Community PKI

Zertifikatprofile

ClientAuth in Serverzertifikaten

- Ursprünglicher Zeitplan von Google: Abschaltung bis 15.6.2026
  - HARICA: Umsetzung geplant zunächst ab 14.03., dann ab 02.03.06
- Spontane Änderung: Google hat sich umentschieden, Frist wird auf März 2027 verschoben
  - HARICA verschiebt jetzt auf irgendwann gegen Jahresende 2026

=> Durcheinander

ClientAuth in Serverzertifikaten

- Was müssen Sie tun?
  - **Prüfen** Sie, welche Ihrer derzeitigen Serverzertifikate in einem ClientAuth-Kontext verwendet werden.
  - **Planen** Sie deren Umstellung auf andere PKIs (z.B. DFN-Verein Community-PKI).

Zertifikatprofile

OCSP

- OCSP in Serverzertifikaten **verschwindet** aus der WebPKI
- Seit August 2023 in den Baseline Requirements als „optional“ markiert
- Viele CAs entfernen OCSP aus den Serverzertifikaten
  - Let's Encrypt hat ihre OCSP-Responder schon Mitte 2025 abgeschaltet
- HARICA nimmt seit **02.03.2026** auch keine OCSP-URL mehr in Serverzertifikate auf
- HARICA hatte noch nie OCSP in S/MIME-Zertifikaten

OCSP

- Was müssen Sie tun?
  - **Prüfen** Sie, ob Sie in einem Webserver **OCSP Stapling** einsetzen, und schalten Sie es ab.

Zeitstempeldienst

Zeitstempeldienst

- Bestandteil der DFN-PKI

  https://doku.tid.dfn.de/de:dfnpki:zeitstempeldienst

- Ziel: Bestätigung der Existenz eines Dokuments zu einem bestimmten Zeitpunkt durch Trusted Third Party (hier: DFN)

- Technisch: RFC3161

  1. Client sendet Hash des Dokumentes zum Server
  2. Server erstellt signierten Zeitstempel mit Hash+Uhrzeit
  3. Client speichert diesen Zeitstempel neben oder in dem Dokument

- Verwendung z.B. beim Signieren von PDFs

Zeitstempeldienst

Zwei Änderungen stehen an:

- Austausch Signaturzertifikat auf dem Server
- Änderung Erreichbarkeit

Zeitstempeldienst

Austausch Signaturzertifikat

- Derzeitiges Signaturzertifikat aus der DFN-PKI Global **läuft bald ab**
- Verlängerung in DFN-PKI Global **nicht möglich** (ist ja abgeschaltet...)
- Keine Public-Trust Alternativen verfügbar
  - Auch DFN-PKI Global kein Default-Trust in Adobe
  - Musste immer speziell in Anwendungen konfiguriert werden
- Darum: Umstellung auf DFN-Verein Community-PKI am **23.06.2026**

Zeitstempeldienst

Änderung Erreichbarkeit

- DFN-Verein Community-PKI wird nur innerhalb DFN-Anwenderschaft vertraut
- Darum: Ab **23.06.2026** wird der Zugriff nur noch von IP-Adressen aus dem X-WiN **erreichbar** sein

Zeitstempeldienst

- Datum für die Änderungen: **23.06.2026**
- Was müssen Sie tun?
  - Hinterlegen Sie die DFN-Verein Community-PKI in Ihren Systemen, um die ausgestellten Zeitstempel weiterhin prüfen zu können.
  - Prüfen Sie nach der Umstellung, ob Ihre Systeme den Dienst noch erreichen können.

Fazit

Fazit

- Automatisierung: Folien Webinare verfügbar
- Ab Ende 2026: Keine ClientAuth mehr in Serverzertifikaten
- Seit 02.03.2026: Kein OCSP mehr in HARICA-Zertifikaten
- 23.06.2026: Zwei Umstellungen am Zeitstempeldienst:
  - Neues Signaturzertifikat aus DFN-Verein Community-PKI
  - Erreichbarkeit nur mit X-WiN IP-Adresse

Haben Sie noch Fragen?

- Kontakt:

  DFN-PCA

  dfnpca@dfn-cert.de

  https://www.pki.dfn.de

  https://blog.pki.dfn.de