DFN-CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

85. Betriebstagung | 06.10.2026

Reimer Karlsen-Masur

DFN

DFN-PKI Global

Letztes TÜV-Audit der DFN-PKI Global Infrastruktur

Erhaltungsbetrieb:

- Keine neuen Zertifikate mehr ab September 2023
- Neue Zertifikatsperrungen möglich
- Restzertifikate (ca. 20.000 Smartcard User) gültig bis Ende März 2027
- Erfolgreiches Audit Ende September 2026 - TÜVIT-Zertifikat kommt
- Ausblick: Abschaltung & Archivierung
  - Abschaltung **OCSP** für Global-PKI ab 01.04.**2027**
  - Abschaltung **CDP/CRLs** für Global-PKI ab 01.04.**2034**

DFN-PKI Grid

DFN-PKI Grid

Modernisierung:

- Neue Grid-CA-Zertifikate
  - Hierarchisch (Root-CA / Issuing-CA)
  - 4096 Bit RSA Schlüssel
  - SHA256 signiert
- Überarbeitung der Grid-Policy (CP / CPS)
- Migration von alter in neue Grid-Issuing-CA
- Abschaltung der alten Grid-CA nach Ablauf ausgestellter Zertifikate

Zeitstempeldienst

Zeitstempeldienst (Folie von 84. BT)

- 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 waren geplant:

- Austausch Signaturzertifikat auf dem Server am 23.06.2026 
  - Hinterlegen Sie die DFN-Verein Community-PKI in Ihren Systemen, um die ausgestellten Zeitstempel weiterhin prüfen zu können.
- ~~Änderung Erreichbarkeit: Ab 23.06.2026 wird der Zugriff nur noch von IP-Adressen aus dem X-WiN erreichbar sein~~ 
  - keine technischen Zugriffseinschränkungen mehr vorgesehen

DFN

GÉANT TCS von HARICA

Neue Features

Neue Features I

ACME, IPv4/6 Adressen in Serverzertifikaten, Web-UI

- ACME
  - ACME Renewal Information (ARI) Unterstützung seit 07/2026 eingeführt
  - Detaillierteres EAB-Credential-Management im Web-UI:
    Ablaufdatum,
    temporäres Pausieren,
    Kommentarfeld,
    CSV-Liste der ausgestellten Serverzertifikate
- Serverzertifikate mit IPv4/6-Adressen via ACME seit 09/2026
  - einzige DCV-Methode: http-01, also Inbound-Zugriff auf Port 80 auf die IP# nötig
- Kleinere Anpassungen im Web-UI von HARICAs Certificate Manager

Neue Features II

HARICA Monitoring, Statistiken, Domain-Onboarding, DCV-API

- Neue HARICA Monitoring-Web-Seiten
  - aktuelle Status-Info https://status.harica.gr/
  - Verfügbarkeits-Info https://availability.harica.gr/
- ab Mitte Oktober
  - Zertifikatsstatistiken für Enterprise-Admins im Web-UI
  - Selfservice für Domain-Onboarding und -Entfernung im Web-UI
  - API-Funktionen mit API-Keys für Enterprise-Admins zur Domain Control Validierung (DCV)

Neue Features III

Domain Control Validation (DCV)

- DCV mittels „DNS TXT Record with Persistent Value“
  - andere Namen: DNS-PERSIST-01, 3.2.2.4.22
  - Support durch HARICA schon länger angekündigt - jetzt für 11/2026
  - inkl. API für Enterprise-Admins im HARICA-System
- technisch realisiert mittels TXT Record im DNS der Form
  - `_validation-persist.<domain> IN TXT "harica.gr; accounturi=<url>; persistUntil=<unix-time>"`
- für Q2/2027: Variante für Validierung von IP-Adressen im Reverse-Namespace
- Vorteil & Nachteil: Persistent => Dekommissionierung mitplanen

TCS-Zertifikatprofile

Anpassung der Zertifikatprofile

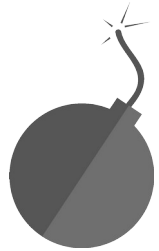
Planänderung bei Wegfall von EKU ClientAuth in Serverzertifikaten

- Anwendungsfall: Gegenseitige AuthN zwischen Systemen.
  Z.B. Datenbankanbindung, SMTP, …
- Google Chrome Root Programm fordert ab 03/2027 von CAs der WebPKI:
  - **Keine** EKU ClientAuth mehr in normalen Serverzertifikaten!
- Prüfen Sie, welche Ihrer derzeitigen Serverzertifikate in einem ClientAuth-Kontext verwendet werden.
- Planen Sie deren Umstellung auf andere separate oder Private Trust PKIs (z.B. DFN-Verein Community-PKI).

Zertifikatprofile

Wegfall der EKU ClientAuth in Serverzertifikaten

- Ursprünglicher Zeitplan von Google: Abschaltung bis 15.06.2026
  - HARICA: Technische Umsetzung geplant zunächst ab 14.03., dann ab 02.03.2026
- Kurzfristige Änderung: Google hat sich umentschieden, Frist wird auf März 2027 verschoben
  - HARICA verschiebt den technischen Termin zunächst auf Nov/Dez 2026
  - vergisst aber, die Rücknahme in den eigenen Richtlinien nachzupflegen
  - stellt somit für ein paar Wochen regelwidrige Serverzertifikate mit EKU ClientAuth aus



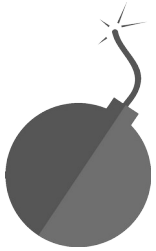
=> Richtlinien-Durcheinander bei HARICA führt in der Folge zunächst zu Incident 1 und Massensperrungen am 20. Juli 2026

- **Aktueller technischer Termin nun Mitte Januar 2027 vorgesehen**

Zertifikatprofile

Wegfall Online Certificate Status Protocol (OCSP) URL in Serverzertifikaten

- OCSP in Serverzertifikaten verschwindet aus der WebPKI
- HARICA nimmt bereits seit 02.03.2026 keine OCSP-URL mehr in Serverzertifikate auf, allerdings
  - HARICAs Richtlinien so komplex & umständlich formuliert, dass monatelang nicht auffällt, dass die OCSP-URL in Serverzertifikaten vorhanden sein muss
  - für ein paar Monate werden regelwidrige Serverzertifikate ohne OCSP-URL ausgestellt (auch die eben erneuerten Serverzertifikate aus Incident 1)



=> Richtlinien-Durcheinander bei HARICA führt in der Folge zu Incident 2 und weiteren Massensperrungen am 25. Juli 2026

Incidents

HARICAs Incidents

Massensperrung von Serverzertifikaten

- Zwei **nicht-sicherheitskritische** Incidents in der TCS/HARICA-PKI
  - Bekanntmachung durch HARICA am 16. bzw. 20. Juli 2026
  - Diskrepanz zwischen HARICAs Zertifizierungsrichtlinie und ausgestellten Serverzertifikaten bzgl. Zertifikatsprofil (EKU ClientAuth & OCSP-URL)
- Individuelle Hilfe der Teilnehmer durch unsere Support-Kanäle läuft an
- Massensperrung und Austausch von insg. ca. **90.000 Serverzertifikaten** alleine bei DFN-Teilnehmern jeweils nach maximal 5 Tagen

HARICAs Incidents

Massensperrung von Serverzertifikaten

- erste Sperrungen von 12.000 Zertifikaten dann am 20.07. (Incident 1)
- in Folge des Erneuerungsansturms kommt es bei HARICA über Tage zu zeitweisen Überlastsituationen
  - Timeouts, verzögerte Zertifikatsausstellungen, Zeitdruck, Frust
- HARICA informiert am 23.07. zur Überlastsituation und deren Mitigationen
- DFN-Info-Webinar zur Lage der TCS/HARICA-PKI am 24.07.
  - ca. 500 Teilnehmende
- weitere Sperrungen von 78.000 Zertifikaten dann am 25.07. (Incident 2)
- mind. 5 weitere CAs der WebPKI ebenfalls von dieser Problem-Klasse betroffen

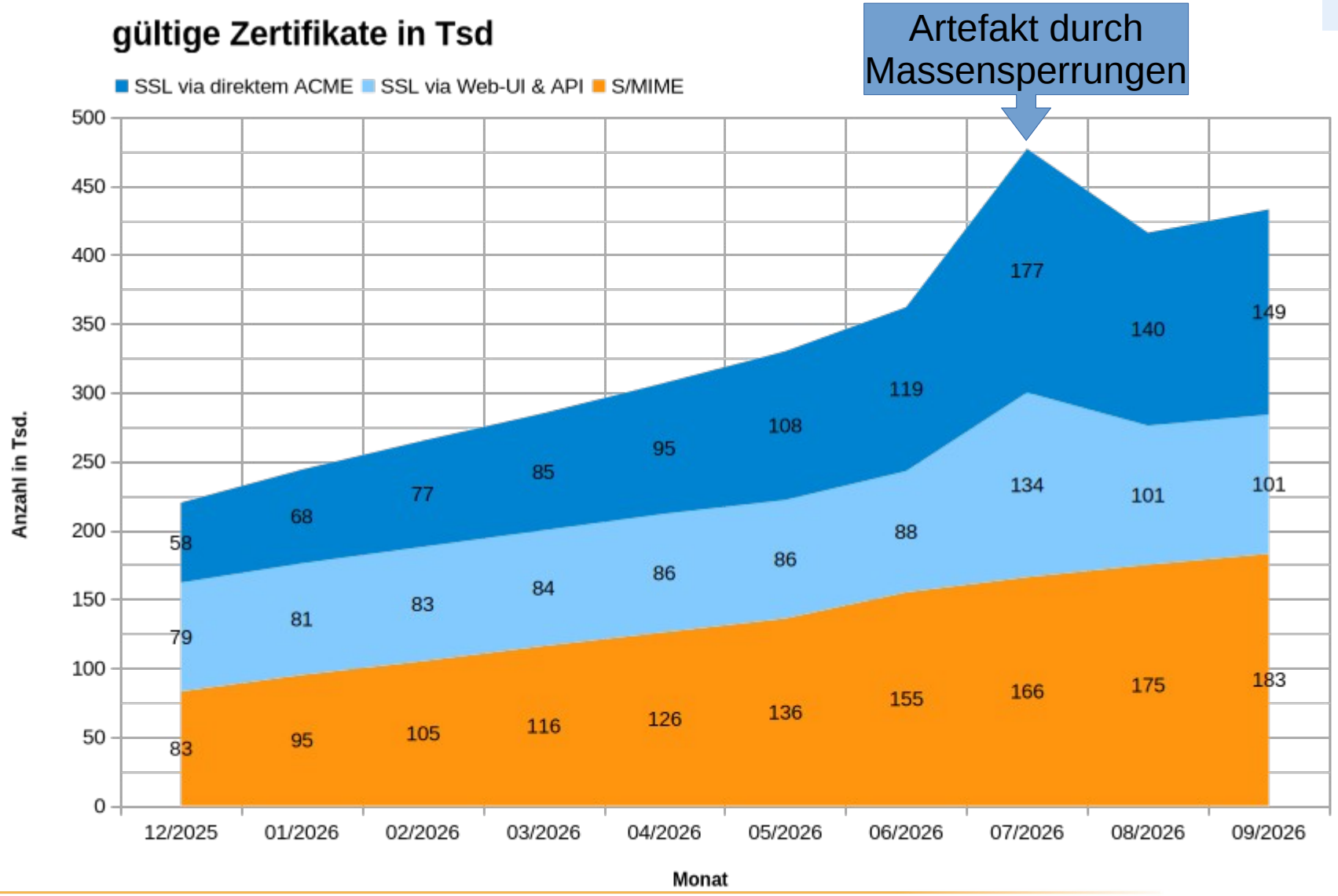
HARICAs Incidents

Lessons learned @ HARICA

- kurzfristige Einführung von ACME Renewal Information (ARI) Unterstützung
- Kommunikation verbessern
  - automatische Zertifikatserneuerung durch HARICA vs Eigeninitiative bei Teilnehmern führte zu eigentlich unnötigen Doppelausstellungen
- Technische Verbesserungen der Architektur, Software und Datenbanken zur allgemeinen Beschleunigung
- Ausbau der Kapazitäten
- Verbesserungen & Automatisierungen von Richtlinien-Compliance-Prüfungen

Details siehe E-Mail „Statement von HARICA“ über Mailing-Liste dfnpki-announce am 23.7.

DFN-weite Zahlen - GÉANT TCS von HARICA



HARICAs Incidents

Aktuelle Nutzung von ACME im Detail

- **380 Einrichtungen** von ca. 550 nutzen aktuell ACME mit **mindestens einem ACME-Account** direkt bei HARICA
- Diese 380 Einrichtungen haben insgesamt ca. 8.500 **ACME-Accounts** angelegt.
- ca. 150.000 gültige Serverzertifikate über ACME automatisiert ausgestellt
  - seit April 2026 > 50% aller Serverzertifikate
- Dunkelziffer: alternative Automatisierung bei den Teilnehmern durch Verwendung von HARICAs API anstatt von ACME

Automatisierung

Automatisierung

- aktuelle Laufzeit von Serverzertifikaten und DCV-Info:

  199 Tage

- Nächste Eskalationsstufen via CA/Browser-Forum Baseline Requirements:
  - **100 Tage** ab März 2027; **47 Tage** (10 Tage für DCV-Info) ab März 2029
  - Wegfall von DCV-Methoden mittels Challenge-E-Mails ab 03/2028

  => weiter automatisieren!

- Z.B. mit ACME! Inkl. ARI & DCV mit DNS TXT Record with Persistent Value

  und mit Integration für automatisiertes DNS-Update
  - aktualisierter Foliensatz aus Webinar verfügbar: https://doku.tid.dfn.de/_media/de:dfnpki:harica:2026-09-28-automatisierung.pdf

Zukunft

Zukunft

Was wird kommen?

- Das TCS-Vergabeverfahren von GÉANT ist noch nicht abgeschlossen
  - sonst hätten wir natürlich schon berichtet :-)
- Nach dem, was wir so hören, halten wir es derzeit für sehr unwahrscheinlich, dass im Rahmen des Übergangs Aufwände wegen eines Plattformwechsels anfallen werden.



Fazit

Fazit

- TCS bleibt
- Automatisierung Serverzertifikatausstellung: Weitermachen!
- Ab Mitte Januar 2027: Keine EKU ClientAuth mehr in Serverzertifikaten
- Zeitstempeldienst: Neues Signaturzertifikat aus DFN-Verein Community-PKI im Einsatz, keine Zugriffbeschränkung auf den Dienst
- DFN-PKI Grid wird modernisiert
- Abbau DFN-PKI Global läuft

Haben Sie noch Fragen?

- Kontakt:
  - DFN-PCA / Trust & Identity-Team
  - dfnpca@dfn-cert.de
  - https://www.pki.dfn.de
  - https://blog.pki.dfn.de

