DFN CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

78. Betriebstagung | 28.03.2023

Jürgen Brauckmann

Agenda

1. GÉANT TCS Nutzerzertifikate
2. CA/Browserforum S/MIME Baseline Requirements
3. Perspektive: 90 Tage Laufzeit von Serverzertifikaten

Schnell noch ein Werbeblock.... .

Veranstaltungen

- Weiterbildung zum Informationssicherheitsbeauftragten
  18.-20.04.+20.-21.06., Hamburg
  12.-14.09.+10.-11.10.2023

Anmeldung/Weitere Informationen: https://www.dfn-cert.de

DFN

GÉANT TCS

GÉANT TCS

Aktuell:

- >490 Einrichtungen mit funktionsfähigem Zugang
  - ~67k Server-Zertifikate ausgestellt, davon ca. 50% per ACME

    (bereits mehr als derzeit in DFN-PKI Global noch gültig sind: 56k)

  - ~28k Client-Zertifikate
- Umstieg Serverzertifikate 12/2022 lief hervorragend, danke!

GÉANT TCS

Umsteigen!

Nutzerzertifikate ab **30.08.2023** nicht mehr aus DFN-PKI Global!

GÉANT TCS

Umstieg:

- TCS Zugang nutzen
- Workflows für Client-Zertifikate in TCS anschauen
  - E-Mail Einladung
  - AAI: `idp/clientgeant`
  - REST-API (siehe auch Posting auf `https://blog.pki.dfn.de`)
- Für Workflows entscheiden und in der Einrichtung bekannt machen
- Neue Browserverankerte Nutzerzertifikate ab **30.08.2023** nur noch aus GÉANT TCS!

GÉANT TCS

Termin:

- Wiederholung GÉANT TCS Workshop am 04.04.2023, 10:00-12:00 Uhr
- Inhalte:
  - Anbindung AAI für User-Zertifikate
  - Zertifikate per E-Mail-Einladung
- Keine Anmeldung erforderlich, Zugangslink ca. 1 Woche vorab über dfnpki-d@listserv.dfn.de

CA/Browserforum S/MIME Baseline Requirements

S/MIME BRs

- Erstes **universelles** Regelwerk zu S/MIME-Zertifikaten
- Wirksam: **1. September 2023**
- Auswirkungen auf
  - Betrieb der CA
  - Alle Zertifikatinhalte (insb. Distinguished Names)
  - Prozesse
- Verschiedene Zertifikattypen und Profile

S/MIME BRs

Zertifikattypen und Profile:

Typ	*Inhalte*
Mailbox	E-Mail
Organization	E-Mail, Organisation
Sponsored	E-Mail, Organisation, Angehörige
Individual	E-Mail, Person

Profil	*Eigenschaften*
Strict	Nur S/MIME, 825 Tage Laufzeit
Multi-purpose	S/MIME und andere Zwecke, 825 Tage Laufzeit
Legacy	Laxere Vorgaben, 1185 Tage Laufzeit, in Perspektive abgeschafft

S/MIME BRs

7.1.4.2.5 Subject DN attributes for sponsor-validated profile

Attribute	Legacy (See Note 1)	Multipurpose (See Note 2)	Strict (See Note 2)
commonName	MAY	MAY	MAY
organizationName	SHALL	SHALL	SHALL
organizationalUnitName	MAY	MAY	MAY
organizationIdentifier	SHALL	SHALL	SHALL
givenName	MAY	MAY	MAY
surname	MAY	MAY	MAY
pseudonym	MAY	MAY	MAY
serialNumber	MAY	MAY	MAY
emailAddress	MAY	MAY	MAY
title	MAY	MAY	MAY
streetAddress	MAY	MAY	SHALL NOT
localityName	MAY	MAY	MAY
stateOrProvinceName	MAY	MAY	MAY
postalCode	MAY	MAY	SHALL NOT
countryName	MAY	MAY	MAY
Other	MAY	SHALL NOT	SHALL NOT

S/MIME BRs

Anforderungen an die **CA** an die Identifizierung von Personen:

- Attribute Collection
  - Physical ID document, EU eID, ...
  - **Enterprise RA Records**
- Validierung der gesammelten Attribute
  - Konkrete Prüfungsanforderungen an Physical ID, EU eID, ...
  - **Keine Anforderungen** an Prüfung von Daten aus Enterprise RA Records erkennbar

Aber: Komplexes Dokument, kann **fehlinterpretiert** werden. Umsetzung durch Sectigo abwarten!

S/MIME BRs

Konsequenzen in GÉANT TCS:

- Sectigo wird CP/CPS-Aktualisierung vornehmen müssen
  - Welche Zertifikattypen werden angeboten?
  - UI-Änderungen?
  - Enterprise RA anwendbar?

    => Noch keine Aussage von Sectigo

- Vermutung: Sponsor-Validated, Legacy-Profil
- **Klärung** über GÉANT läuft

Laufzeit von Serverzertifikaten

Laufzeit Serverzertifikate

Hintergrund:

- Stetige Reduktion der erlaubten Zertifikatlaufzeiten für TLS Server Auth (Serverzertifikate) in den letzten Jahren
- Derzeit: Max. 398 Tage
- Reduktion getrieben von den Root-Programmen (Google, Apple, Microsoft, Mozilla)
- Argument: Sicherheit wird durch regelmäßigen schnellen Austausch und Automatisierung erhöht

Laufzeit Serverzertifikate

Ankündigung von **Google**:

- Weitere Reduktion auf **90 Tage** wird kommen!
- Über das CA/B-Forum, oder aber auch **einseitig** durch Google
- Noch kein konkretes Datum. Schätzung: Q4 2024/Q1 2025

Laufzeit Serverzertifikate

Konsequenzen:

- **Automatisieren** Sie die Ausstellung von Serverzertifikaten!
  - ACME
  - REST-API
- **Prüfen** Sie Ihre Zertifikat-Use-Cases!
  - Migration zu Spezial-PKI, wo sinnvoll (Shibboleth, ...)
  - DFN-Verein Community PKI, eigene interne PKI, ...

Fazit

Fazit

- GÉANT TCS:
  - Migration Userzertifikate Global->TCS zum **30.08.2023**
  - Workshop 04.04., 10:00 Uhr: Infos über dfnpki-d@listserv.dfn.de
- CA/B-Forum S/MIME Baseline Requirements:
  - DN für User-Zertifikate wird sich ändern
  - Prozessänderungen?
- Absehbar 90 Tage Laufzeit von Serverzertifikaten:
  - **Jetzt um Automatisierung kümmern!**
  - Use-Cases für Non-Browser-PKIs identifizieren!
    (z.B. DFN-Verein Community-PKI)

Haben Sie noch Fragen?

- Kontakt:

  DFN-PCA

  dfnpca@dfn-cert.de

  https://www.pki.dfn.de

  https://blog.pki.dfn.de