DFN CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

77. Betriebstagung | 18.10.2022

Jürgen Brauckmann

Agenda

1. GÉANT TCS
2. CA/Browserforum S/MIME Baseline Requirements

DFN

GÉANT TCS

GÉANT TCS

Aktueller Zustand des Rollouts:

- >450 Einrichtungen mit funktionsfähigem Zugang
  - ~35k Server-Zertifikate ausgestellt, davon ~1/2 per ACME
  - ~12k Client-Zertifikate
- (Von 50 Einrichtungen noch keine Rückmeldung auf unsere Einladungsmail eingegangen. Bitte gerne bei dfnpca@dfn-cert.de melden.)

  Mail: „DFN-PKI: Teilnahme am GÉANT Trusted Certificate Service“

GÉANT TCS

Umsteigen!

- Serverzertifikate ab 30.12.**2022** nicht mehr aus DFN-PKI Global!
- **VORBEHALT S/MIME-Baseline Requirements:**

  *Nutzerzertifikate ab Ende **2023** nicht mehr aus DFN-PKI Global!*

GÉANT TCS

Umstieg:

- TCS Zugang nutzen
- Workflows in TCS anschauen
  - Web-Formular
  - AAI-geschütztes Web-Formular
  - ACME
  - REST-API (siehe auch Posting auf https://blog.pki.dfn.de)
- Für Workflows entscheiden und in der Einrichtung bekannt machen
- Browserverankerte Serverzertifikate ab **30.12.2022** nur noch aus GÉANT TCS!

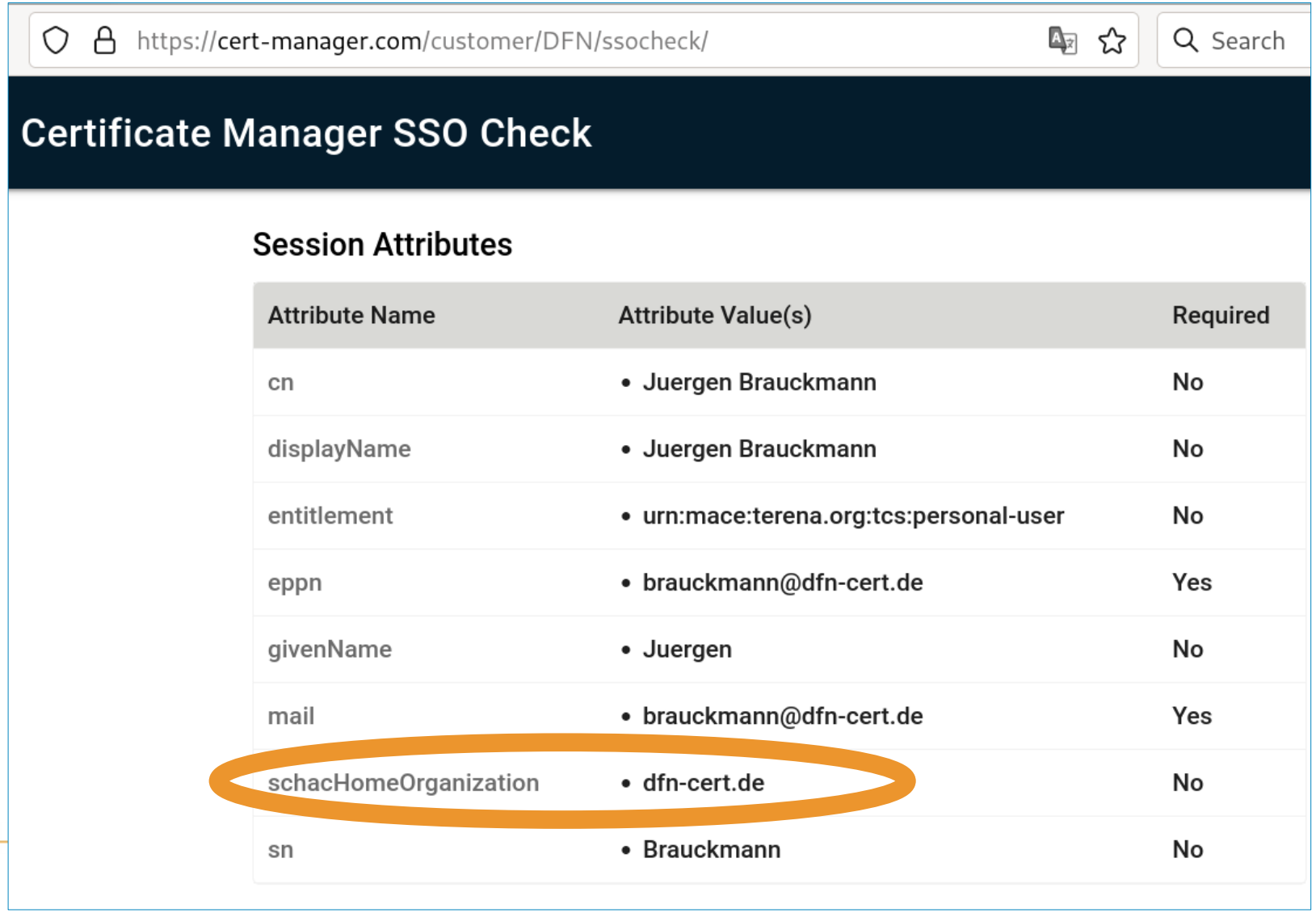
GÉANT TCS

Zugriff per AAI:

- Ihr IdP muss bestimmte Attribute freigeben => Sprechen Sie mit Ihren AAI-Kolleginnen und Kollegen!
  - schacHomeOrganization
  - mail
  - displayName
  - (Weitere Attribute für client certificates)

GÉANT TCS

- Prüfen über: https://cert-manager.com/customer/DFN/ssocheck



GÉANT TCS

Termin:

- Wiederholung GÉANT TCS Workshop am 07.11.2022, 10:00-12:00 Uhr
- Inhalte:
  - Verwaltung von Domains im cert-manager
  - Antragswege für Serverzertifikate (u.a. ACME, Enrollment Forms)
- Keine Anmeldung erforderlich, Zugangslink ca. 1 Woche vorab über dfnpki-d@listserv.dfn.de

CA/Browserforum S/MIME Baseline Requirements

S/MIME BRs

- Neues Regelwerk des CA/Browserforums zu S/MIME-Zertifikaten
- Ca. 95 Seiten
- Auswirkungen auf
  - Prozesse
  - Zertifikatprofile
  - Distinguished Names
  - Validierungsschritte / Identifizierung
- Wirksam: Frühester Termin ab Mitte August 2023

  (Erfolg bei der Abstimmung im CA/Browserforum vorausgesetzt)

S/MIME BRs

Mögliche Konsequenzen

- Bereits jetzt absehbar: **Großer** Anpassungsbedarf
  - Plattform DFN-PKI
  - Ihre Prozesse, Ihre Zertifikate, Ihre Software
  - Migrationsprojekt auch bei Ihnen! **Zusätzlich** zu Migration nach TCS!
- Darum: **Vorzeitige Einstellung** DFN-PKI Global S/MIME-Zertifikate mit Inkrafttreten S/MIME BRs absehbar (frühestens Mitte 08/23)

S/MIME BRs

Konsequenzen in GÉANT TCS:

- Änderungen bei Prozessvorgaben zu Identifizierung und Dokumentation sehr wahrscheinlich
- Wiederholung von Identifizierungen nach 825 Tagen
- Zusätzliche Schritte bei Organisationsvalidierung durch Sectigo
- Distinguished Name werden sich ändern
- **Klärung** über GÉANT läuft

Fazit

Fazit

- GÉANT TCS:
  - Migration Global->TCS: Serverzertifikate zum **30.12.2022**
  - Workshop 07.11., 10:00 Uhr: Infos über dfnpki-d@listserv.dfn.de
- CA/B-Forum S/MIME Baseline Requirements:
  - **Große** Auswirkungen ab Mitte 2023
  - **Vorzeitige Einstellung** DFN-PKI Global S/MIME-Zertifikate mit Inkrafttreten S/MIME BRs absehbar

Haben Sie noch Fragen?

- Kontakt:

  DFN-PCA

  dfnpca@dfn-cert.de

  https://www.pki.dfn.de

  https://blog.pki.dfn.de