DFN CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

79. Betriebstagung | 17.10.2023

Jürgen Brauckmann

Agenda

1. GÉANT TCS
2. Digitale Signatur
3. Perspektive: 90 Tage Laufzeit von Serverzertifikaten

Schnell noch ein Werbeblock.... .

Veranstaltungen

- 10. DFN-Konferenz Datenschutz: 28./29.11.2023, Hamburg
- DFN-Konferenz „Sicherheit in vernetzten Systemen“: 30./31.01.2024, Hamburg
- Weiterbildung zum Informationssicherheitsbeauftragten:
  Nov/Dez 2023 Webinar (07.-09.11+05.-07.11.)
  April/Mai 2024 München (16.-18.04.+14.-16.05.2024)
  Sep/Okt 2024 Hamburg (10.-12.09.+15.-17.10.2024)

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

DFN

GÉANT TCS

GÉANT TCS

Aktuell:

- 521 Einrichtungen mit Zugang zu TCS
  - ~109k gültige Server-Zertifikate, davon ca. 60% per ACME
  - ~58k gültige Client-Zertifikate
- Umstellung S/MIME-BR: 387 Einrichtungen wieder in der Lage, Client-Zertifikate auszustellen (Stand 12.10.)

Problem:

- Sectigo muss alle 521 Einrichtungen nach neuen Regeln revalidieren
- Sectigo hat
  - zu spät die technischen Voraussetzungen geschaffen
  - zu spät mit der Revalidierung begonnen
  - zu wenig Ressourcen bereitgestellt
- Ergebnis:
  - **Serviceausfälle** für Clientzertifikate
  - Im allg. Chaos auch Probleme bei Serverzertifikaten

CTIGO® Certificate Manager

DFN

Organizations

NAME	STATUS
Fachhochschule Kiel	ACTION REQUIRED
FH Aachen University of Applied Sciences	ACTION REQUIRED
Filmuniversität Babelsberg KONRAD WO...	ACTION REQUIRED
FIZ Karlsruhe - Leibniz-Institut für Inform...	ACTION REQUIRED
Frankfurt School of Finance & Managem...	ACTION REQUIRED
Freie Universität Berlin	ACTION REQUIRED
Friedrich-Alexander-Universität Erlangen...	ACTION REQUIRED
Georg-August-Universität Göttingen	ACTION REQUIRED
Hahn-Schickard-Gesellschaft für angew...	ACTION REQUIRED
Helmholtz-Zentrum für Infektionsforsch...	ACTION REQUIRED
Helmholtz-Zentrum für Ozeanforschung ...	ACTION REQUIRED
Helmholtz-Zentrum für Umweltforschun...	ACTION REQUIRED
Helmut-Schmidt-Universitaet	ACTION REQUIRED

Total: 370

Organization Validation (OV)

ID 1767980589

Sectigo Public CA

Validator: Reimer Karlsen-Masur

Status: VALIDATED

Expires: 27/09/2024

Revalidate | Reset

Secondary Organization Validation (OV)

ID 1854028967

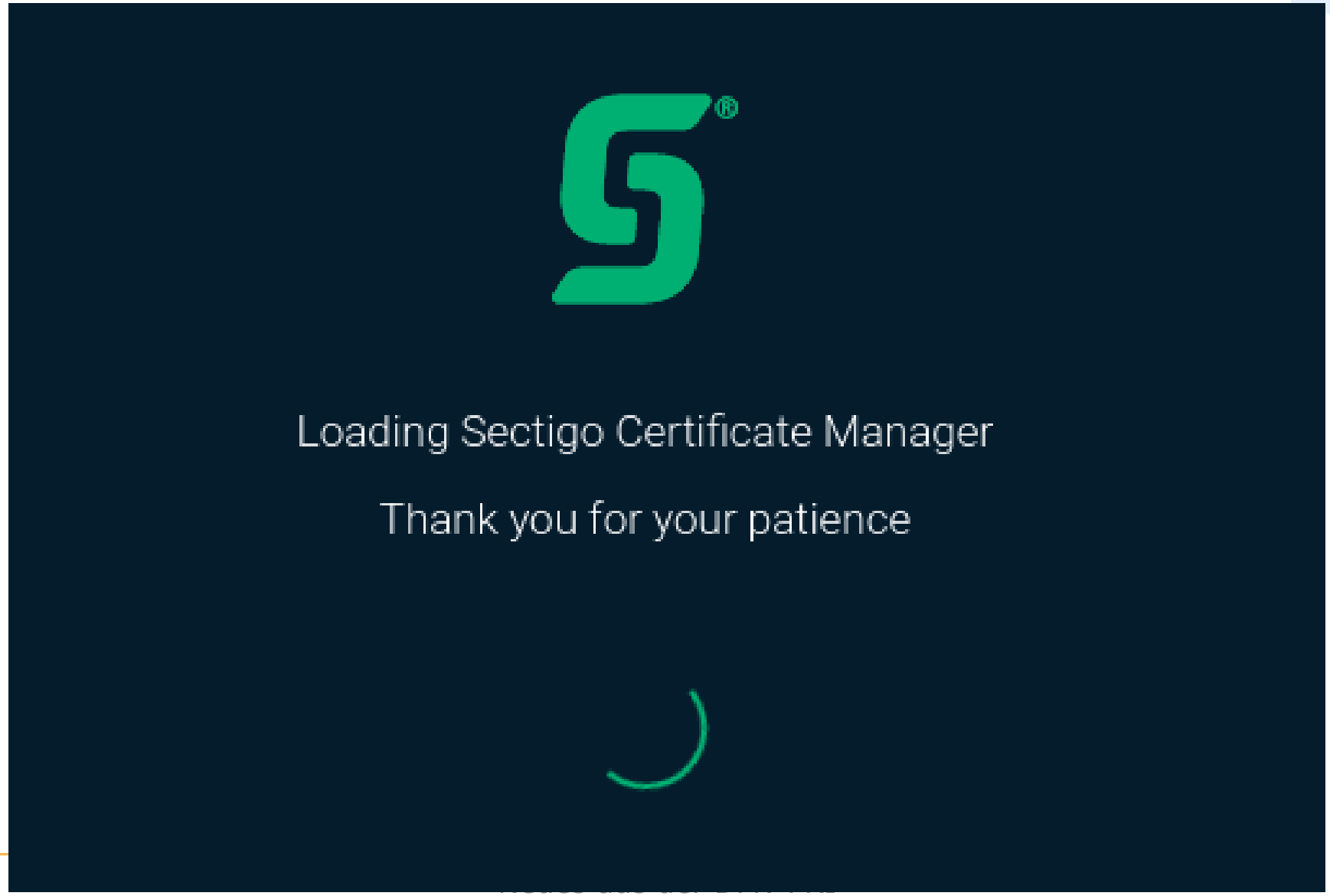
Sectigo Public CA

Validator: Jürgen Brauckmann

Status: PENDING

Expires:

Reset


Loading Sectigo Certificate Manager
Thank you for your patience

GÉANT TCS

Zertifikattypen für S/MIME:

- GÉANT Personal email signing and encryption:
  - Zertifikatinhalt: Vorname/Nachname, E-Mail-Adresse, Organisation
  - Identifizierung (wie bisher auch)
  - **Niemals** „Testuser 1234“!
- GÉANT Organisation email signing
  - auch Verschlüsselung möglich!
  - Zertifikatinhalt: E-Mail-Adresse, Organisation
    => keine Identifizierung notwendig
  - Auch für Gruppen
- Profile für Grid-Computing jetzt nur auf Anfrage

GÉANT TCS

Umstieg auf S/MIME-Baseline Requirements:

- Enrollment Forms:
  - Profile ändern
  - Validation Type von Personen auf HIGH setzen
- AAI über `idp/clientgeant`:
  - surname/givenName übertragen
- REST-API:
  - Profile ändern
  - Validation Type HIGH

Digitale Signatur

Digitale Signatur

Hintergrund:

- Informationsaustausch 26.09. mit eingeladenen Expertinnen und Experten

- Diverse Ausprägungen möglich:
  - Remote / lokale Signatur
  - Siegel
  - Einfache / fortgeschrittene / qualifizierte Signatur
  - Adobe Approved Trust List
- Fazit: Heterogene Anforderungen
- Ggf simpler Websignaturdienst zur Abdeckung geeigneter Use Cases?

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 mit einiger Wahrscheinlichkeit 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 läuft, wenn auch holprig
- Digitale Signatur
- 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