DFN-CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

81. Betriebstagung | 08.10.2024

Jürgen Brauckmann

Kurz ein Werbeblock.... .

Veranstaltungen

- Weiterbildung zum Informationssicherheitsbeauftragten: November/Dez. 2024 als Webinar (05.11.-07.11.+03.12.-05.12.2024)
- DFN-Konferenz Datenschutz: 26./27.11.2024, Hamburg
- DFN-Konferenz „Sicherheit in vernetzten Systemen“: 11./12.02.2025, Hamburg

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

DFN

GÉANT TCS

GÉANT TCS

Zahlen:

- 542 Einrichtungen
- Serverzertifikate: ca. 155.000, davon ca. 46% per ACME (**zu wenig!**)
- Clientzertifikate: ca. 149.000
- Codesigning-Zertifikate: 64

Positiv:

- Revalidierung von Organisationen läuft weitestgehend **reibungslos**
- Technische Weiterentwicklung von APIs

Negativ:

- Ende September Ausfälle nach Update von Sectigo (auch: undokumentierte API-Änderungen)
- Kurzfristige **Sperrung** von Client-Zertifikaten!
  - Januar 2024: Sperrung von **1649** Zertifikate aus 5 Einrichtungen
    Ursache: Fehler bei der Validierung von Organisationen
  - September 2024: Sperrung von **399** Zertifikaten einer Einrichtung.
    Ursache: **Falscher** „Fehlerreport" bei Mozilla. Sperrung „out of an abundance of caution".

Hintergrund der Sperrungen:

- S/MIME-Zertifikate mit O= benötigen seit 09/2023 einen **organizationIdentifier**
- Herleitung in S/MIME BR nicht ganz eindeutig:
  - Nach Kap 3.2.3.1 ein **Unique identifier**
  - Weitere Beschreibung in 7.1.4.2.2 geht nicht weiter auf **unique** ein
  - Zulässige Schemata alle problematisch, u.a. VAT, NTR, LEI, GOV

Problemfelder:

- VAT (Umsatzsteuer-Id):
  - Breit verfügbar, z.B. `VATDE-232129737`
  - **Kein** öffentliches Register in DE/EU => Für Sectigo **nicht validierbar**
- NTR (Handelsregister):
  - Register in D **lokal**, nicht auf Bundes- oder Landesebene
  - S/MIME-BR beschreiben NTR-Syntax nur für Bundes/Landesebene, z.B. `NTRUS+CA-12345678`
  - Daher bisherige Praxis: lokale Nummern, z.B. `NTRDE-HRB 88805`
  - Problem: **Nicht eindeutig**

Problemfelder:

- LEI (global Legal Entity Identifier gleif.org):
  - Globale eindeutige ID, ausgestellt nach Registrierung
  - Verschiedene Verifikationslevel (`ENTITY_SUPPLIED_ONLY, FULLY_CORROBORATED`)
  - In D **keine** Möglichkeit für staatliche Einrichtungen, `FULLY_CORROBORATED` zu erlangen
- GOV (Government):
  - Registrierungsschema für Government Entities
  - Eintrag ohne weitere Registernummer, darum eben auch nicht **unique**

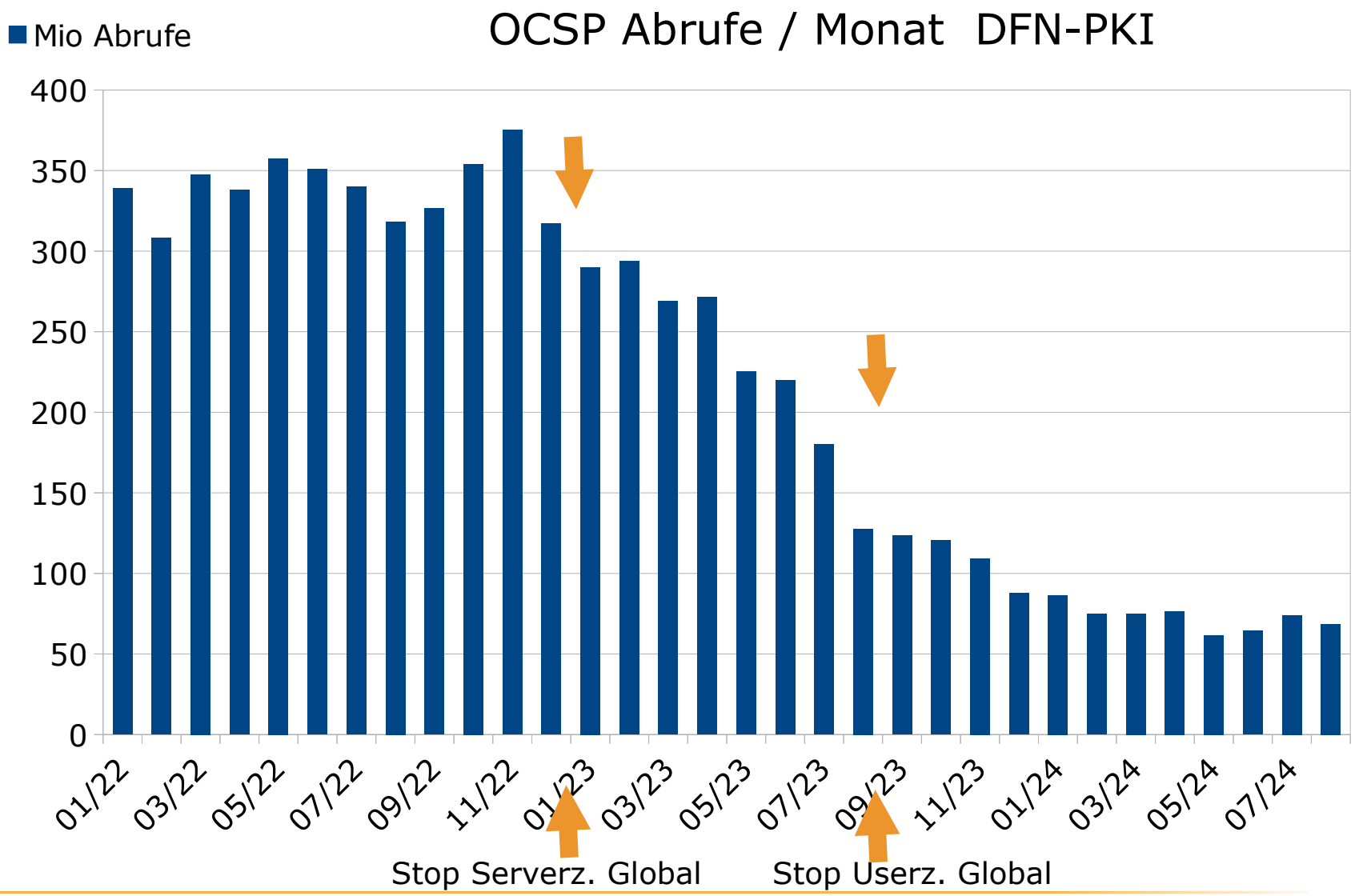
DFN-Verein Community PKI

DFN-Verein Community PKI

Zahlen:

- 221 Einrichtungen
- Serverzertifikate: 2000
- User-Zertifikate: ca. 46.000
- DFN-PKI Global: Noch 225.000 gültige User-Zertifikate

Aktuelle Zahlen



Neu:

- Zertifikate mit **ECC**-Schlüssel möglich
- Anwendungsfall: User-Zertifikate auf Token
- Einschränkungen:
  - „Mix-PKI“: Weiterhin CA-Zertifikat mit RSA => RSA-Signatur unter Zertifikate mit ECC-Key
  - Nur per API. Beantragung per Web-Anwendung folgt.

PKI-Agilität

PKI-Agilität

Zustand der Browser-PKI 2024

- 05/2024: Google Chrome wirft ecommerce monitoring GmbH raus
- 06/2024: Google wirft Entrust zu 11/2024 raus
- 06-07/2024: Harte Diskussionen auf Bugzilla bzgl. Telekom
- 07/2024: Bug in den DCV-Prozeduren von Digicert
  - 80.000 Zertifikate betroffen (=gesperrt)
  - CISO tritt zurück
- 01/2024 und 09/2024: Sperrung von 2000 Zertifikaten in TCS durch Sectigo
  - Unsicherheiten bei der Interpretation der S/MIME-BRs

PKI-Agilität

Vorbereiten auf:

- kurzfristige **Sperrungen**
- Wechsel von **Root-Zertifikaten**
- Verkürzung von **Zertifikatlaufzeiten**
- Änderung von **Prozessen**
- **(Dienstleisterwechsel)**

Es wird nie mehr so stabil wie 2010-2020...

PKI-Agilität

Vorbereiten durch:

- **Automatisierung** für Serverzertifikate
- Verzicht auf **CA-Pinning**
- Aufbau von **einfachen** Prozessen für User-Zertifikate (z.B. idp/clientgeant)
- Verzicht auf **ClientAuth** mit Browser-PKIs
- Wenn passend, **Non-Browser-PKIs** verwenden

Fazit

Fazit

- GÉANT TCS:
  - Läuft im Rahmen der Möglichkeiten der PKI-Industrie
- Community-PKI:
  - ECC-Schlüssel
- PKI-Agilität!

Haben Sie noch Fragen?

- Kontakt:

  DFN-PCA

  dfnpca@dfn-cert.de

  https://www.pki.dfn.de

  https://blog.pki.dfn.de