DFN-CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

80. Betriebstagung | 19.03.2024

Jürgen Brauckmann

Kurz ein Werbeblock.... .

Veranstaltungen

- Weiterbildung zum Informationssicherheitsbeauftragten:
  April/Mai 2024 München (16.-18.04.+14.-16.05.2024)
  Sep/Okt 2024 Hamburg (10.-12.09.+15.-17.10.2024)
- 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

Aktuelle Zahlen

- TCS:
  - 530 Einrichtungen
  - ~142k gültige Server-Zertifikate, davon ca. 45% per ACME (Anteil sinkt?!)
  - ~95k gültige Client-Zertifikate
- DFN-Verein Community-PKI:
  - 160 Einrichtungen
  - ~2k gültige Server-Zertifikate
  - ~22k gültige Client-Zertifikate

CA/Browserforum, CAA-Records für S/MIME

- Records im DNS: Welche CAs dürfen Zertifikate ausstellen?
- Seit 2017 relevant für die Ausstellung von **Serverzertifikaten**
- Jetzt neu auch für **S/MIME-Zertifikate**
  - Umsetzung durch CAs: SHOULD ab 15.09.2024, MUST ab 15.03.2025
- **Keine Pflicht** für Einrichtungen oder User!
- Beispiel:

```
uni-pellform.de CAA 0 issuemail "pki.dfn.de"
```

Laufzeit von Serverzertifikaten

- 03/2023: Ankündigung von Google, Maximallaufzeit von **90 Tagen** durchsetzen zu wollen. Kein konkretes Datum benannt.
- **Aktuell:** Immer noch kein konkretes Datum, keine weiteren Ankündigungen oder Äußerungen

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, ...

Digitale Signatur

- Weiterhin viele Nachfragen
- Unterscheidung interne/externe Use-Cases
- Dokumentation zur digitalen Signatur mit der DFN-Verein Community-PKI auf `https://doku.tid.dfn.de`
- GÉANT prüft Etablierung eines Dienstes **eduSign**
  - Anbindung an AAI, Signatur im Web-Browser, Gegensignaturen möglich
  - Zeitachse?

DFN-LDAP

- ldap.pca.dfn.de enthält User-Zertifikate aus DFN-PKI Global
- Für TCS existiert **kein** LDAP
  - Keine Abfrage der Einwilligung zur Veröffentlichung im TCS-Workflow
  - Unterschiedliche Voraussetzungen in den Einrichtungen bzgl. Veröffentlichung
  - => Generelle „TCS-LDAP"-Lösung unwahrscheinlich
- Vertragliche Lösung möglich:

  Einrichtungen veröffentlichen die Daten selbst auf ldap.pca.dfn.de

DFN

GÉANT TCS

GÉANT TCS

Umstellung S/MIME-BR:

- Seit 08.12.2023 alle Einrichtungen wieder validiert
- Dauer: **102** Tage für 523 Organisationen

GÉANT TCS

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

Sperrungen:

- Sectigo **sperrt** von sich aus auch Client-Zertifikate, kurzfristig!
- Aktueller Vorfall:
  - Ende Januar Sperrung von **1649** Zertifikate aus 5 Einrichtungen
  - Ursache: Fehler bei der Validierung von Organisationen durch Sectigo

Ablauf der Sperrung:

- **22.1., 16:14 Uhr**: Mail von Sectigo an zwei pers. Adressen im DFN-CERT: Sperrung von 1649 Zertifikaten am **26.1., 23:15 UTC**
  - 1649 Zert.-Seriennummern und Organisationsnamen geliefert, aber keine Namen/Mailadressen
- **22.1., ca. 18:30 Uhr**: Wir warnen betroffene Einrichtungen vor
- **23.1., ca. 10:30 Uhr**: Wir informieren über die Mailadressen zu den 1649 Zertifikate
- **26.1., 23:15 UTC**: Sperrung

Auswirkungen der Sperrungen:

- Eine Einrichtung betroffen, die VPN mit ClientAuth mit Sectigo-Client-Zertifikaten macht. Ca. 300 User drohen VPN-Zugriff zu verlieren.

Generell:

- Sorgfältig prüfen, ob ClientAuth-Use-Cases in GÉANT TCS wirklich das Risiko wert sind! **Wir raten ab!** Community-PKI oder andere Nicht-Browser-PKI verwenden!
- Fristverlängerungen nicht möglich. Haben wir auch hier probiert, wurde abgelehnt.

Fazit

Fazit

- Absehbar 90 Tage Laufzeit von Serverzertifikaten:
  - Keine Neuigkeiten, aber trotzdem: **Jetzt um Automatisierung kümmern!**
- Digitale Signatur: DFN-Verein Community-PKI, GÉANT-Aktivitäten
- GÉANT TCS:
  - Migration S/MIME Baseline Requirements (endlich) abgeschlossen
  - Auch Client-Zertifikate können kurzfristig gesperrt werden
- 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