Neues aus der IT-Sicherheit im DFN

Ralf Gröper

79. Betriebstagung des DFN-Vereins | 17.10.2023

Rückblick: Neuaufstellung der DFN-PKI

- 2006-2023: Zentrales Element der DFN-PKI war das **Sicherheitsniveau „Global“**
  - Durch DFN **selbstbetriebene browserverankerte PKI**
  - **Letztes Zertifikat** wurde Ende August 2023 ausgestellt
  - seit dem **Erhaltungsbetrieb** für bereits ausgestellte Zertifikate

- GÉANT **TCS** und die **DFN-Verein Community PKI** lösen die bekannte DFN-PKI „Global“ ab

- **Trusted Certificate Service** (TCS)
  - Kommerzieller PKI-Anbieter „Sectigo“ stellt browserverankerte Zertifikate aus
  - PKI-Leistungen werden von GÉANT ausgeschrieben und vom DFN-Verein über GÉANT bezogen
  - besonders geeignet für Anwendungsfälle mit **notwendiger Browserverankerung**

- **DFN-Verein Community PKI**
  - Vom DFN-Verein selbst betrieben, ähnlich zu Sicherheitsniveau „Global“
  - Ohne Browserverankerung
  - besonders geeignet für Anwendungsfälle **ohne notwendige Browserverankerung**

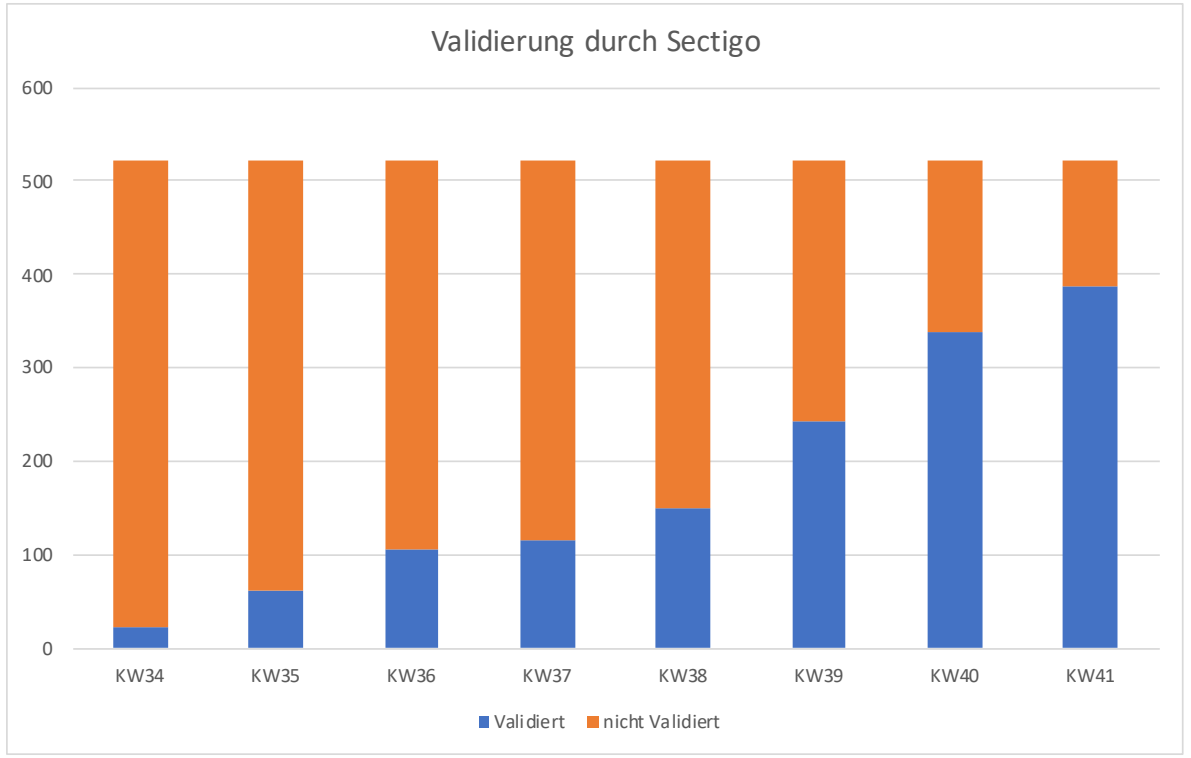
Aktuelle Probleme mit TCS

- Ab 01.09.2023 gab es **massive Probleme** bei Sectigo bei **Validierung von Einrichtungsnamen**
  - Neu: „organization Identifier“, z.B. Handels-/Vereinsregisternummer, USt.-ID,…
  - Sectigo hat erst **Ende August** angefangen, diese Daten zu erheben und zu validieren
    - Sie hätten das lange im Vorfeld bereits starten können
    - Sectigo ist selber Mitglied der S/MIME Working Group des CA/Browser Forums
- Nicht validierte Einrichtungen können **keine S/MIME-Zertifikate** mehr ausstellen
  - Serverzertifikate sind weiterhin verfügbar

Aktuelle Probleme mit TCS: Zeitlicher Verlauf

- Zunächst wurden nur ca. 10 bis 50 Einrichtungen pro Woche revalidiert, inzwischen 50-100

- Aktueller Stand: (12.10.): 387 von 521 Einrichtungen sind revalidiert



Aktuelle Probleme mit TCS: Was hat der DFN getan?

- Intensive **Konsultationen mit Sectigo** auf technischer Ebene
  - Wir (Jürgen Brauckmann und Team) haben **viele Fehler** gefunden und bei Sectigo eskaliert
  - Damit konnten wir den Prozess bei Sectigo im Vergleich zu anderen Ländern **deutlich beschleunigen**
    - Durch Priorisierung bei Sectigo konnten wir Einrichtungen mit großen Problemen häufig helfen
    - Die Wartezeit war und ist trotzdem zu lang!
  - Außerdem haben wir dadurch GÉANT, anderen NRENs (und auch Sectigo…) sehr geholfen
- Intensive begleitende **Konsultationen mit GÉANT**
- **Konsultationen** mit Kunden **anderer Anbieter**
  - Erkenntnis: Durchaus vergleichbare Zustände – kein Problem exklusiv bei Sectigo
- Mehr zu TCS und anderen Themen aus der DFN-PKI von J. Brauckmann im Forum Sicherheit

Rollout DFN.Security: Verträge

- Nach Mitgliederversammlung im Juni **beschränkter Rollout** für letzte Feedbackrunde zu Dienstvereinbarung und Auftragsverarbeitungsvereinbarung (AVV)
  - Ergebnis: Keine inhaltlichen Änderungen mehr erforderlich

- **Unbeschränkter Rollout** der Verträge läuft
  - Neue Teilnehmer bekommen die neuen Verträge
  - Wenn Sie die Logdatenanalyse nutzen möchten und/oder noch einen DoS-Basisschutz benötigen, rufen Sie bitte die Verträge bei uns ab: dfn.security@dfn.de

- Aktuell **17 Dienstvereinbarungen** für DFN.Security unterschrieben
  - Bemerkung: Dazu kommen die Bestandsnutzer aus dem DFN-CERT Dienst

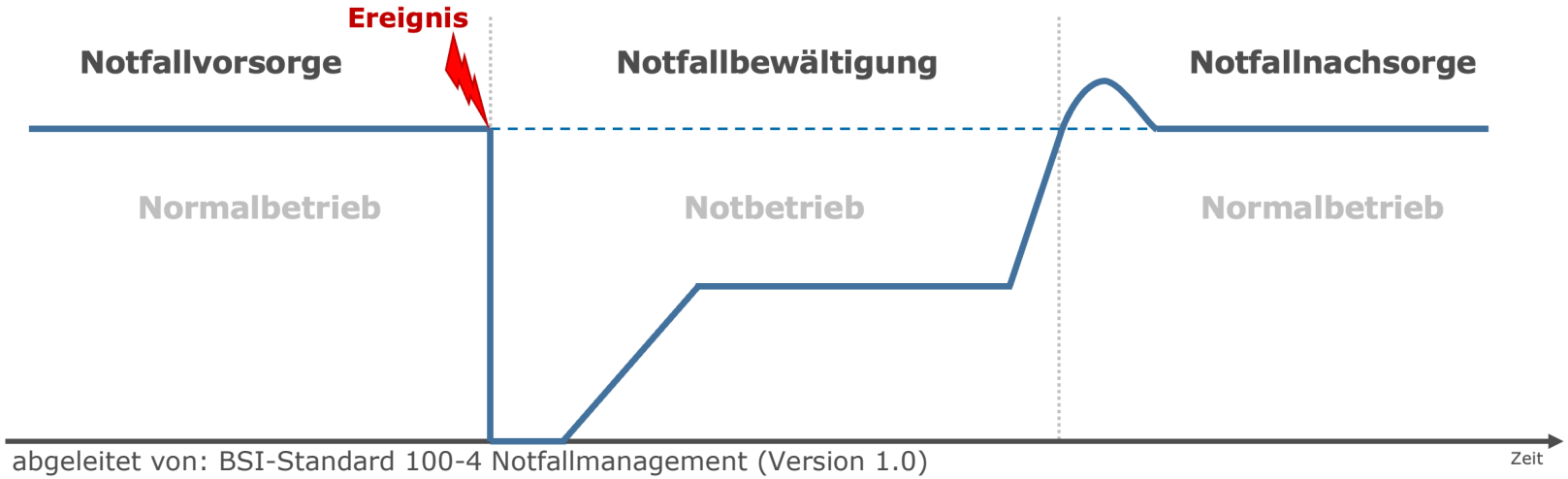
- Davon **zwei** Einrichtungen mit „**erweiterte Leistungen**“

Rollout DFN.Security: Technik

- Alle angekündigten Leistungsmerkmale sind **in Betrieb**
  - Letztes neues Leistungsmerkmal: **Aktives Dienstemonitoring**
- Kommendes Leistungsmerkmal in den Basisleistungen: **„DNS-Firewall“**
  - In Kooperation mit SWITCH
- Aktuelles Thema in den erweiterten Leistungen: Logdatenanalyse für **Windows Active Directory** / **Domaincontroller**
  - Herausforderung: Know-How-Aufbau Windows-Systeme durch Austausch mit Teilnehmern
- Mehr zu DFN.Security von C. Kahl im Forum Sicherheit

…und sonst noch?

- **größere Sicherheitsvorfälle** bei Teilnehmern im DFN im letzten Jahr
  - Mehr dazu im Forum Sicherheit



abgeleitet von: BSI-Standard 100-4 Notfallmanagement (Version 1.0)

- Der DFN und seine Gremien beschäftigen sich intensiv mit diesem Thema
  - **Neue Leistungsmerkmale** der DFN-Dienste werden dies berücksichtigen
  - Stay tuned…

31. DFN-Konferenz „Sicherheit in vernetzten Systemen“

Das DFN-CERT veranstaltet am 30. / 31. Januar 2024 im Auftrag des DFN-Vereins die 31. DFN-Konferenz „Sicherheit in vernetzten Systemen“ im Grand Elysée Hotel Hamburg.

Weitere Informationen unter

https://www.dfn.de/event/31-dfn-konferenz-sicherheit-in-vernetzten-systemen/

Forum Sicherheit

Heute, 17.10. 14:00 - 16:00 Uhr
Forensprecher: Stefan Kelm, DFN-CERT

- Neues aus dem DFN-CERT
  - C. Kahl, DFN-CERT
- Notfallmanagement: Die ersten 24 Stunden nach (und vor!) einer Kompromittierung
  - J. Becker, TU Darmstadt
- Neues aus der DFN-PKI
  - J. Brauckmann, DFN-CERT
- Betrieb eine PKI Middleware für GÉANT TCS
  - F. Ritterhoff, HS München