Karlsruher Institut für Technologie

Stand und Roadmap für (Server-)Zertifikate am KIT

DFN-PKI Global ist End-Of-Life

- Details siehe Vortrag vom September 2021

- Die KIT-CA (bzw. die DFN-PKI Global) stellt
  - nach dem 30.12.2022 keine Serverzertifikate und
  - nach dem 30.12.2023 keine Personenzertifikate mehr aus

- Das sind harte Deadlines, auf die wir keinen Einfluss haben.

- Fokus heute deshalb nur auf **Server**-Zertifikate.

Wo bekommt man ab 2023 Server-Zertifikate?

- Gibt im Wesentlichen vier Optionen

1. Let’s Encrypt
2. GÉANT Trusted Certificate Service (TCS)
3. (Beliebige andere kommerzielle CA)
4. (Eigene CA / Self-Signed / DFN-PKI (Community) CA)

Option Eins: Let’s Encrypt

- Unser Wunsch: in 2023 machen das 99% der KIT-Dienste!
- Mittels DNS-01-ACME-Challenge auch für den großen Teil aller schwierigen Szenarien (Server nicht via Internet erreichbar, hat keinen Webserver, Wildcard-Zertifikate, …) geeignet. kit.edu hat ausreichend Ratelimit bekommen.
- Die fehlende Komponente dafür (acme4netvs) wird gerade fertig. Mehr dazu später…

Option Zwei: GÉANT TCS

- Der offizielle Nachfolger der DFN-PKI. Betrieben durch einen (alle fünf Jahre wechselnden) kommerziellen CA-Anbieter; aktuell Sectigo.
- TCS ist leider 💩😱🤕🤮… Alles voller Fallstricke und Dornen.
- TCS leider (fast) alternativlos für Personen- und Spezialzertifikate (bspw. Code Signing). Problem für die Zukunft…
- Sectigo-Prozesse quasi unbenutzbar. Eigenes Frontend in Arbeit. Wahrscheinlich nicht bis Ende 2022 einsatzfähig.
- Wir bieten potentiell einen händischen Übergangsprozess an.

(Option Drei: Beliebige kommerzielle CA)

- Kostet €€€.
- Eigentlich nicht besser als Let‘s Encrypt oder TCS/Sectigo; unterliegen alle den CAB/BR.
- Potentiell nötig bei expliziten (in der Regel externen) Anforderungen.

(Option Vier:
Eigene CA/Self-Signed/DFN-PKI custom CA)

- kein globaler Trust → muss **a priori** auf **allen** potentiellen Clients installiert werden
- Nur für bestimmte Szenarien sinnvoll

Unser Ziel bis Ende des Jahres

- Genug Unterstützung (Tooling, Dokumentation) bereitstellen, damit jeder eigenständig auf Let‘s Encrypt migrieren kann.

- Ein Plan B für den Rest haben.

Konkreter Plan

- Regelmäßige Treffen/Workshops zu acme4netvs
  - Ankündigung dazu per Infomail an IT-EK-*-Listen / SCC-Alle

- In sinnvollen Intervallen alle aktuellen Zertifikatsinhaber auffordern sich bis spätestens Mitte Dezember nochmal ein neues Zertifikat bei der KIT-CA zu besorgen

acme4netvs

Karlsruher Institut für Technologie

Der “missing link” zwischen ACME-Clients und dem NETVS.

Stand:

- Funktioniert mit certbot (, ,), dehydrated (,) und win-acme (); andere Clients mit Wrapper möglich
- Geschrieben in Golang: single binary ohne Abhängigkeiten, für quasi alle Architekturen und Systeme verfügbar
- Debian-Pakete über Repository (→ Auto-Updates möglich)

Was fehlt:

- (Bessere) Dokumentation
- (Mehr) Beta-Tester

acme4netvs

- Community-Chat auf KIT-Matrix:

  https://matrix.to/#/#acme4netvs-community:kit.edu

- Quellcode: https://git.scc.kit.edu/KIT-CA/acme4netvs
- Releases: https://www.ca.kit.edu/p/software/acme4netvs
- Dokumentation: https://docs.ca.kit.edu/acme4netvs/en/