RWTH-CA (G2)

Alles wird neu, oder nicht?

IT Center | RWTH AACHEN UNIVERSITY

Allg. Informationen

- Wurzelzertifikat "Deutsche Telekom Root CA 2" der bestehenden DFN-PKI läuft am 9. Juli 2019 ab
  - alle auch neu ausgestellte Zertifikate bleiben gültig (Gültigkeitsdauer!)

- Neues Wurzelzertifikat "T-Telesec GlobalRoot Class 2„ seit Ende 2016 nutzbar
  - Übersichtsseite zu den Zertifikaten
  - Gültig bis 2033

- Jede CA entscheidet autonom, wann auf die neue Generation der DFN-PKI gewechselt wird

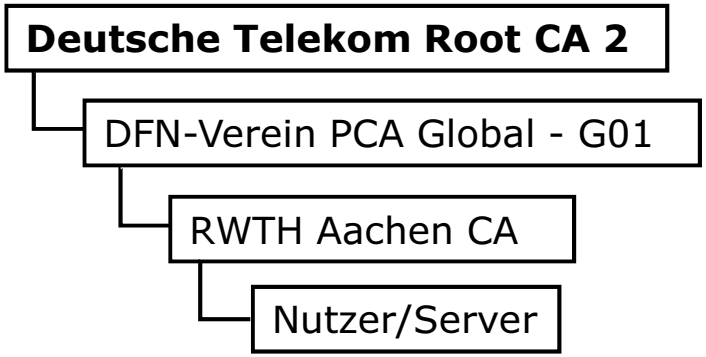
- Zeitplan der RWTH-CA
  - Infos an Administratoren 21.03.2017
  - Infos an Nutzer 25.03.2017
  - Publikation auf doc.itc.rwth-aachen.de 25.03.2017
  - Ablehnung von Anträgen für alte DFN-PKI 10.07.2018

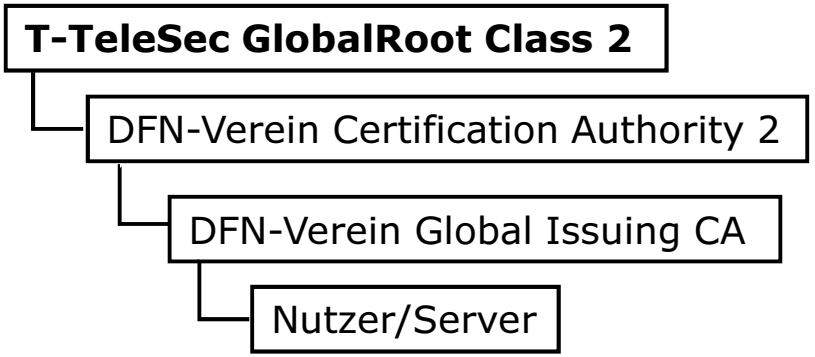
Allg. Informationen → Handlungsbedarf

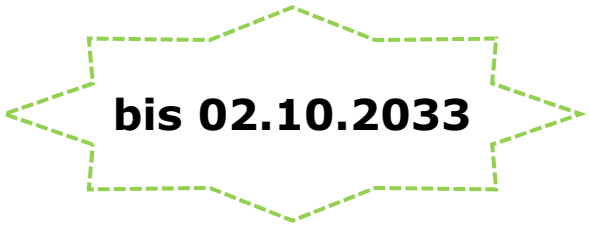
- Die Zertifikate liegen in einer anderen PKI-Hierarchie
  - also muss eine neue CA-Zertifikatkette installiert werden
    - Kann unabhängig von der bisherigen sofort gemacht werden
    - Überall dort wo die neuen Zertifikate eingesetzt werden (bspw. Web-, E-Mail-, Exchange-, LDAP- oder AD-Server, E-Mail-Client oder Browser)
  - Wer ist betroffen: - Administratoren von Servern
    - Endnutzer von eduroam (wg. CA-Pinning)
    - E-Mail-Clients

- Den Zertifikaten wird unter Android <= 4.4 nicht vertraut (Wurzel-CA-Zertifikat "T-TeleSec GlobalRoot Class 2" ist nicht vorinstalliert)
  - Work-Around wäre Cross-Zertifikat – aktuell jedoch Probleme mit Spezial-Software wie Cross-Zertifikat aussieht:
    echo QUIT | openssl s_client -connect info.pca.dfn.de:443 -showcerts
  - Statistik zur Verwendung einzelner Android Versionen

Zertifizierungskette für Server- und Nutzerzertifikate in alter DFN-PKI







Wie erkennt man Antrag für neue DFN-PKI

DFN-PKI

Zertifikatantrag für ein Nutzerzertifikat

- an: DFN-CA Global G2 -

Antragsnummer	1610016
Antragssteller	
Vorname Nachname	Erika Mustermann
E-Mail	erika.mustermann@rwth-aachen.de
Abteilung	
Zertifikatdaten	
Eindeutiger Name	CN=Erika Mustermann, O=RWTH Aachen, C=DE email:erika.mustermann@rwth-aachen.de
Public Key Fingerprint	FC:6A:76:19:6B:4F:7C:3D:03:29:15:87:F0:DA:43:90:EE:46:31:30
Veröffentlichen	Ja
Zertifikatprofil	User

Seite 1/1 (Antragsnummer 1610016)

dfn-ca-global-g2, RA-ID: 3550

Gut zu wissen für Nutzer/Administrator

- Neue Schnittstelle für Nutzer und Administratoren zur neuen DFN-PKI
  https://pki.pca.dfn.de/rwth-ca-g2/pub

- Der Prozess innerhalb der RWTH-CA ändert sich nicht
  - Abgabe von Unterschriebenen Zertifikatsanträgen für Nutzer-/Serverzertifikaten beim IT-ServiceDesk
  - Übermittlung von Zertifikatsanträgen für Serverzertifikaten (!) durch Ansprechpartner via signierter und gerne auch verschlüsselter E-Mail an ra@rwth-aachen.de

- Weitere Informationen:
  - DFN-Blog
  - FAQ Generation 2