JÜLICH
FORSCHUNGSZENTRUM

Neues zu Zertifikaten

6. Oktober 2016

Martin Sczimarowsky

Überblick:

- Aktueller Stand
- Neue Generation der DFN-PKI Global
- OCSP Stapling

Zertifikate im FZJ: aktueller Stand

- DFN Public Key Infrastructure (Vertrauenshierarchie)
- FZJ bietet Server- und Benutzerzertifikate in zwei Hierarchien an: **Global** und **Grid**

Gültige Zertifikate	Server	Benutzer
Grid	70	50
Global	800	800

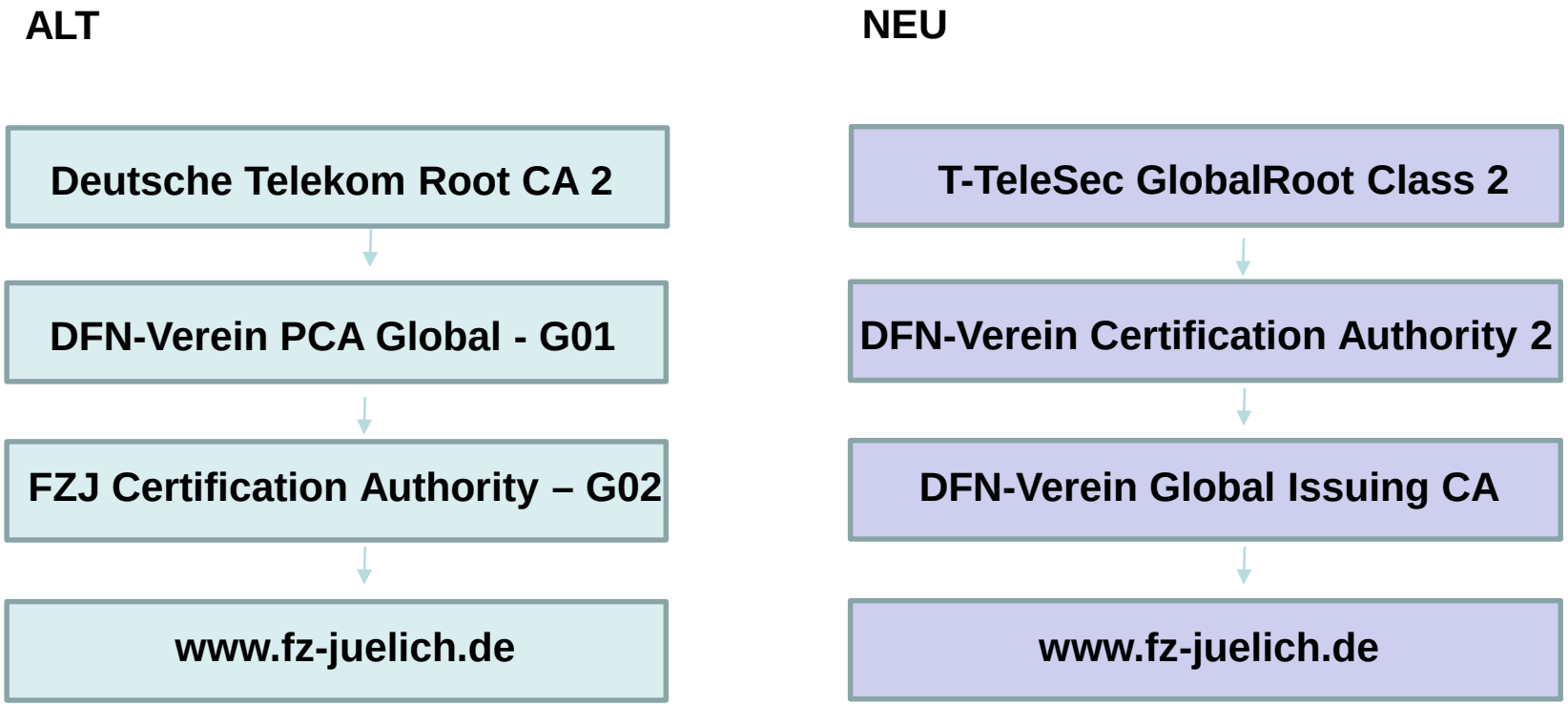
Zertifikate im FZJ: aktueller Stand

- Teilnehmer-Service FZJ (früher RA):
  JSC-Dispatch (Ch.Dohmen, B.Hossfeld)
  M.Sczimarowsky
- Email: ts@fz-juelich.de
- Informationen zum Thema:
  JSC-Online - Zertifikate
  https://www.pki.dfn.de

Neue Generation der DFN-PKI Global

- Die aktuelle PKI Global existiert seit 2007
- Root-Zertifikat:
  Deutsche Telekom Root CA 2,
  gültig bis zum 9. Juli 2019
- Neue Root:
  T-TeleSec GlobalRoot Class 2,
  gültig bis 2033
  (https://www.pki.dfn.de/root/globalroot2/)

Vergleich der beiden Global - Zertifizierungshierarchien



Zertifikate der alten PKI (Deutsche Telekom Root CA 2)

- Die alte PKI kann unverändert weiter genutzt werden
- Zertifikate bleiben gültig bis Ablauf, maximal bis zum 9. Juli 2019
- können grundsätzlich weiterhin bis zum 9. Juli 2019 beantragt und ausgestellt werden. Bei Verfügbarkeit der neuen Hierarchie sollte aber bei neuen Zertifikaten nur noch diese verwendet werden
- https://pki.pca.dfn.de/fzj-ca

Zertifikate der neuen PKI (T-TeleSec GlobalRoot Class 2)

- In den nächsten Monaten wird die Benutzung der neuen PKI für die DFN-Einrichtungen sukzessive aktiviert
- Der Zugang zu den Antragsseiten geschieht über eine neue Web-Seite, die wir bei Verfügbarkeit auf unseren Zertifikatsseiten verlinken werden
- https://pki.pca.dfn.de/fzj-ca-gen2/
- Gültigkeit: max. 39 Monate für Serverzertifikate
  max. 5 Jahre für Benutzer-Zertifikate

Was müssen Nutzer bei den neuen Zertifikaten beachten?

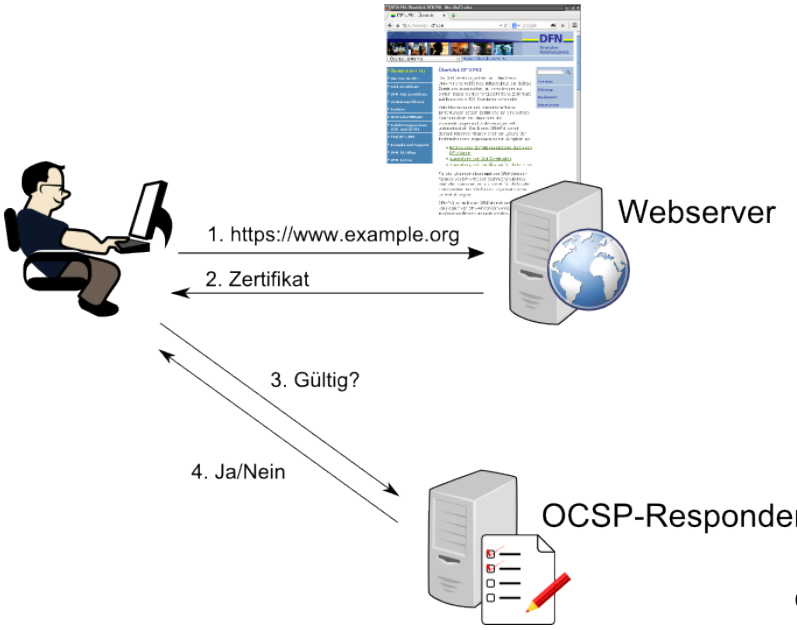
- Nichts. Die neue Root ist in allen gängigen und aktuellen Browsern etc. bereits enthalten.
- Android <=4.4 unterstützt die neue Root nicht.

Was ist bei Servern zu beachten?

- Auf Servern, die Client-Authentisierung mittels Zertifikaten machen, können in der Übergangszeit gültige Client-Zertifikate aus mehreren unterschiedlichen PKIs auftauchen. Solche Server müssen entsprechend konfiguriert werden.
- DFN-PCA hat versprochen, für gängige Server-Software Konfigurationshinweise bereit zu stellen.

Online Certificate Status Protocol (OCSP)

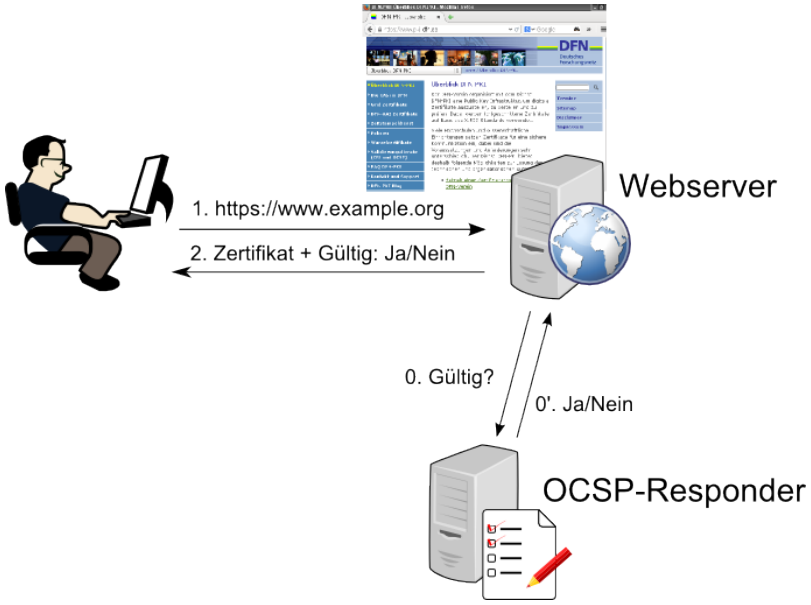
- Moderneres Verfahren ggü. den früher verwendeten CRL (Certificate Revocation List)



Quelle: DFN-PKI-Blog

OCSP Stapling

- Schutz der Privacy, Verringerung der Latenz
- Feature der Webserver-Software



Quelle: DFN-PKI-Blog

Dank für die Aufmerksamkeit