Neues aus der DFN-PKI

Jürgen Brauckmann
dfnpca@dfn-cert.de

Überblick

- Aktuelles
- Nachfolge Deutsche Telekom Root CA 2
- Änderungen zum 1.10.2016
- Veröffentlichung von Zertifikaten
- Behandlung von HTTP in Browsern

Aktuelles

- Audit 2016 in Vorbereitung
- SHA-2-Migration abgeschlossen
  - Beginn: Mitte 2013
  - Umzustellen waren: Zertifikatprofile, DFN-PCA-Zertifikat, Sub-CA-Zertifikate, Zeitstempel, OCSP-Signaturen, CRLs

DFN Deutsches Forschungsnetz

Veranstaltungen:

- **Tutorium „ENISA Kurs: Digital Forensics“**
  6. Oktober 2016, Hamburg
- **Tutorium „Linux Firewalling mit nftables“**
  20. Oktober 2016, Hamburg
- **5. DFN-Konferenz Datenschutz**
  29.-30. November 2016, Hamburg

Bei Interesse: https://www.dfn-cert.de

Nachfolge
Deutsche Telekom Root CA 2

Nachfolge DT Root CA 2

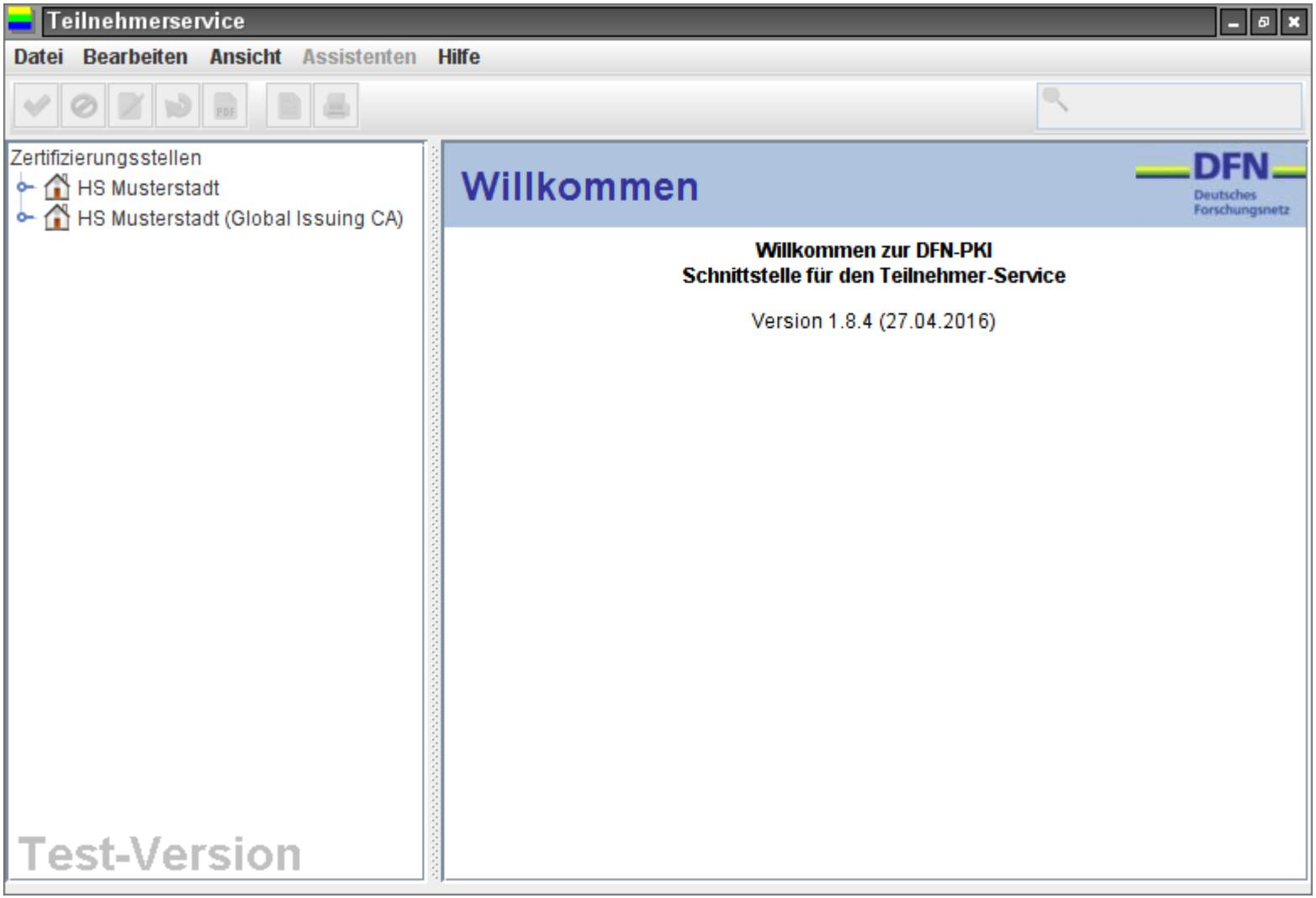
T-TeleSec GlobalRoot Class 2

- DFN-PCA hat begonnen, ersten Anwendern Zugänge zur Verfügung zu stellen
- Separate Antragsseiten für neue Hierarchie

  https://pki.pca.dfn.de/uni-xy-ca-**g2**/pub

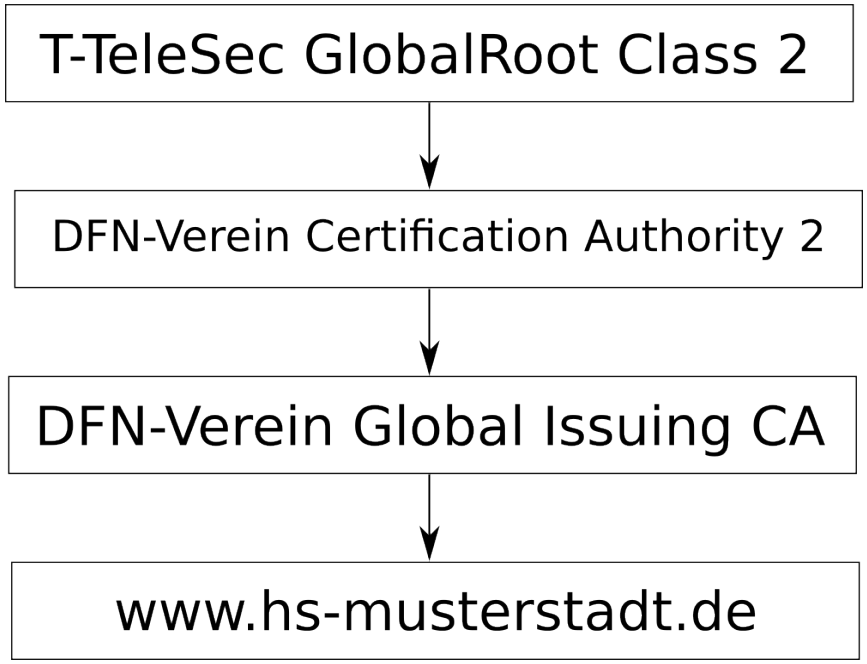
Nachfolge DT Root CA 2

- Separate Zugänge für Teilnehmerservice:



Nachfolge DT Root CA 2

- CA-Kette:



Ausführliche Beschreibung:

https://blog.pki.dfn.de/2016/07/einfuehrung-der-neuen-generation-der-dfn-pki/

Änderungen zum 1.10.2016

Änderungen 1.10.2016

Stichtag für mehrere kleinere Änderungen (Anforderung vom CA/Browserforum)

- Sperrung von noch gültigen Zertifikaten mit internen Domains oder reservierten IP-Adressen: ca. 200 Stück betroffen
- Längere Seriennummern: Mehr Zufallszahlen gegen Hash-Kollisionen

Veröffentlichung von Zertifikaten

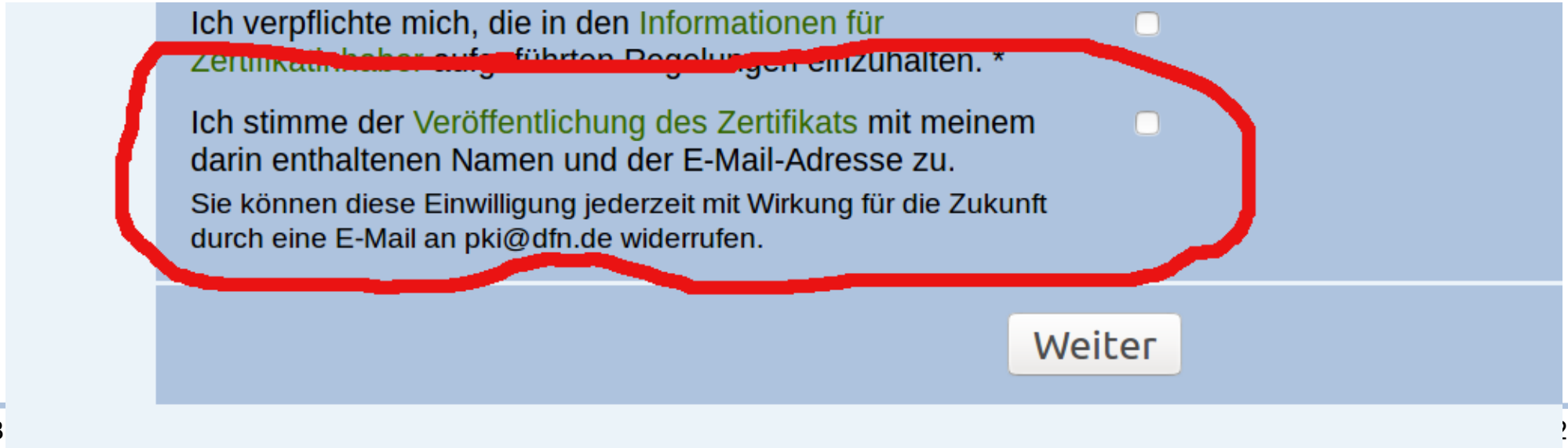
Veröffentlichung

Nutzerzertifikate:

- Veröffentlichung nützlich für verschlüsselte Mail

Serverzertifikate:

- Kein technischer Sinn der Veröffentlichung
- Bisher eingeschränkte Veröffentlichung (kein LDAP)



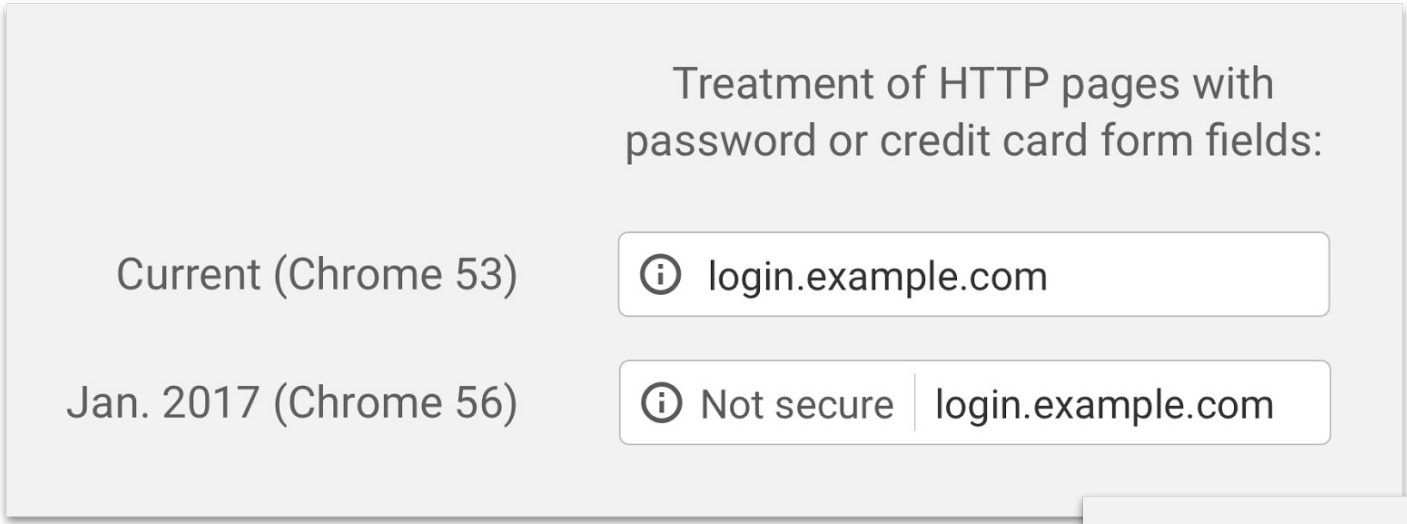
Veröffentlichung

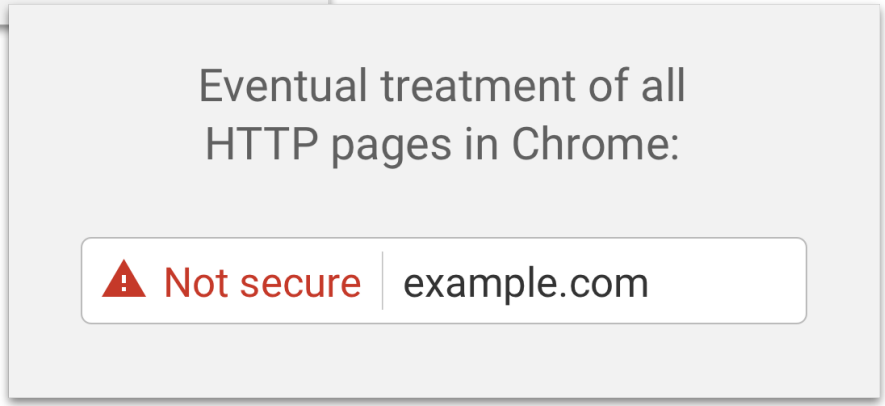
„Certificate Transparency“:

- Jedes Serverzertifikat wird weltweit abrufbar geloggt
- Zweck: Transparenz für die Web-PKI
- DFN-PKI wird mittelfristig teilnehmen (müssen)
- Was bedeutet das für Zertifikate für interne Zwecke?
  exchange.vserv1.intern.hs-musterstadt.de

Unverschlüsseltes HTTP in Browsern

Zukunft in Chrome: Plain HTTP als unsicher markieren





Quelle: https://security.googleblog.com

Zusammenfassung

Zusammenfassung

- Deutsche Telekom Root CA 2
  => T-Telesec GlobalRoot Class 2
- Veröffentlichung von Serverzertifikaten?
- Unverschlüsseltes HTTP wird von Browsern zurückgedrängt

https://blog.pki.dfn.de
dfnpca@dfn-cert.de