DFN CERT

deutsches forschungsnetz

Neues aus der DFN-PKI

68. Betriebstagung | 14.03.2017

Jürgen Brauckmann

Agenda

1. Aktuelles
   - Änderungen zum 26.02.
   - Policy-Versionen
   - Java >=9
   - DSGVO
2. Validierung von Domains
3. Fazit und Ausblick

Aktuelles

Änderungen zum 26.02.2018

- Certificate Transparency
  - Serverzertifikate werden nun stets in CT-Logs veröffentlicht
  - Serverzertifikate enthalten „Embedded SCT“ => Funktionieren weiterhin in Chrome ohne Konfigurationsänderung vom Webserver
  - Aktuell benutzte Logs: Google, Comodo, NORDUnet
- Laufzeit Serverzertifikate begrenzt auf 825 Tage (ca. 27.5 Monate)
  - Tendenz/Wunsch von Browserherstellern nach weiterer Verkürzung... .

Policy-Versionen

DFN-PKI Sicherheitsniveau „Global“:

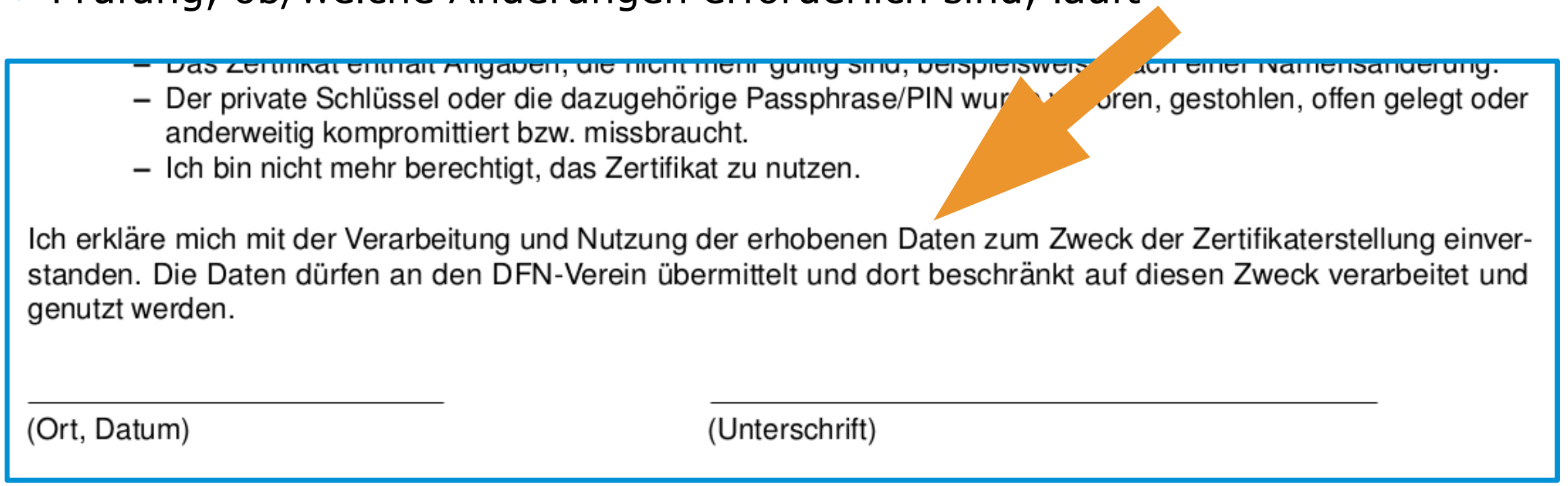
- Version 3.7 (15.02.2018)
  - Änderungen: Formalia für das Audit
  - Anforderung von TÜViT
- Version 3.8 (19.03.2018)
  - Änderungen: Domain-Validierungsverfahren
  - Anforderung vom CA/Browser-Forum

Java >= 9

- Java 8: Updates von Oracle für nicht-private Nutzung bis Januar 2019
- RA-Oberfläche noch nicht 100%ig Java-9-bereit
  - Hauptproblem: Inkompatible API-Änderungen bei Token/PKCS#11
- DFN-PCA arbeitet daran

DSGVO

- Besonders betroffen: Einverständniserklärung auf dem Antragsformular
- Prüfung, ob/welche Änderungen erforderlich sind, läuft



– Das Zertifikat enthält Angaben, die nicht mehr gültig sind, beispielsweise nach einer Namensänderung.
– Der private Schlüssel oder die dazugehörige Passphrase/PIN wurden verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
– Ich bin nicht mehr berechtigt, das Zertifikat zu nutzen.

Ich erkläre mich mit der Verarbeitung und Nutzung der erhobenen Daten zum Zweck der Zertifikaterstellung einverstanden. Die Daten dürfen an den DFN-Verein übermittelt und dort beschränkt auf diesen Zweck verarbeitet und genutzt werden.

(Ort, Datum) (Unterschrift)

Veranstaltungen

- Ausbildung zum Informations-Sicherheitsbeauftragten

  10. - 12. April 2018 (Block I)

  28./29. Mai 2018 (Block II)

  30. Mai 2018 (Prüfung)

  Hamburg

- 7. DFN-Konferenz Datenschutz

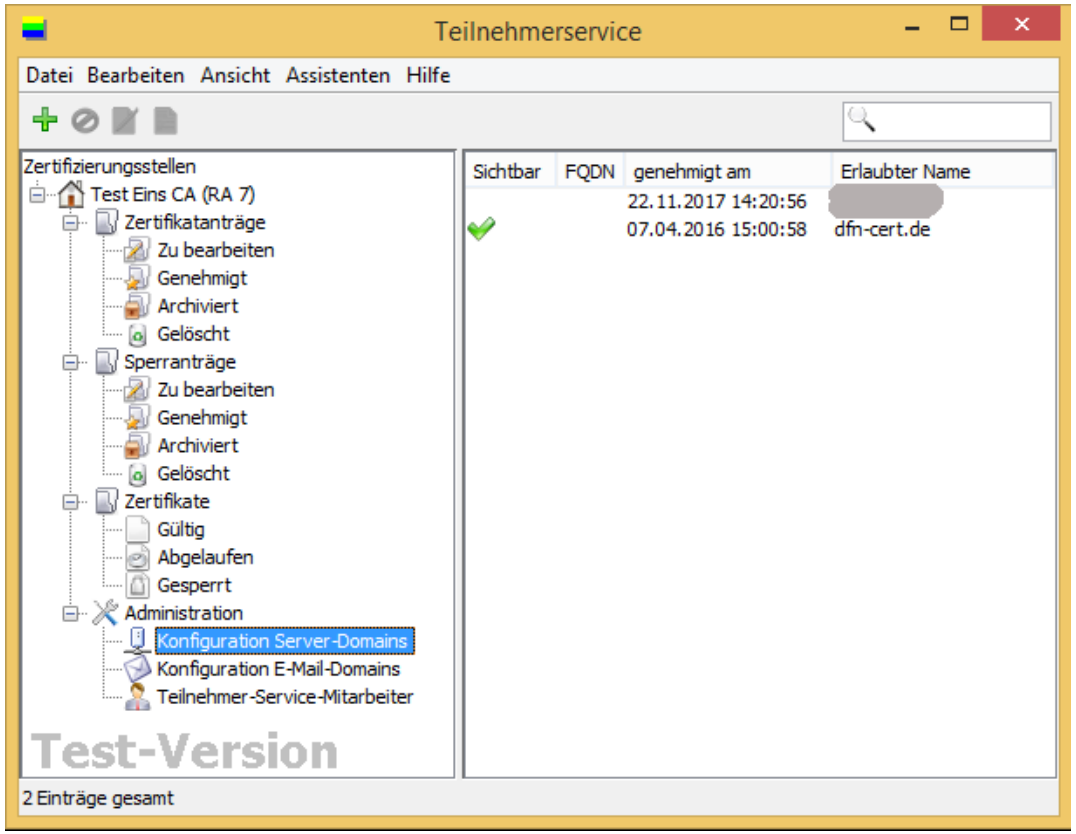
  20./21. November 2018, Hamburg

Validierung von Domains

Validierung von Domains

Bisher:

- Teilnehmerservice trägt gewünschte Domain in der Java RA-Oberfläche ein
- DFN-PCA prüft gegen WHOIS
  - Wenn Einrichtung Domaininhaber, Admin-C, Tech-C: Direkt Freischaltung
  - Sonst: Domainauthorisierungschreiben
- Nach Freischaltung 825 Tage lang gültig
- DFN-PCA kümmert sich um erneute Prüfung vor Ablauf von 825 Tagen



Validierung von Domains

Entwicklung CA/Browserforum:

- Diskussion seit 19. Dezember, angestoßen von Digicert:
  - Kritik: Daten im WHOIS prinzipiell unzuverlässig
- 3. Januar: Plötzlicher Entwurf, die bisherigen Validierungen zum 1. März als ungültig anzusehen => DFN-PKI wäre lahmgelegt
- 6. Februar: Beschluss mit veränderter Deadline 1. August
- Zusätzliche Komplikation: WHOIS vs. DSGVO

Validierung von Domains

Konsequenz:

- DFN-PCA arbeitet mit Hochdruck an alternativen Verfahren
- Erstes Alternativ-Verfahren: E-Mail-Challenge
- Ebenfalls denkbar: Challenge im DNS, Challenge auf einem Webserver
- Nachteil aller Alternativ-Verfahren:
  - Teilnehmer müssen selbst mehr tun!
  - Werkzeugunterstützung notwendig
- Umstellung direkt auf ACME/Let's Encrypt-Protokoll keine kurzfristige Alternative. (Organisationsvalidierung nicht direkt vorgesehen)

Validierung von Domains

Zukünftiger Ablauf mit Verfahren „E-Mail-Challenge“:

- Teilnehmerservice trägt gewünschte Domain in der Java RA-Oberfläche ein
- Teilnehmer wählt Challenge-E-Mail-Adresse aus

  (Im Ausnahmefall auch E-Mail-Adresse aus WHOIS möglich)
- DFN-PCA sendet signierte Challenge-E-Mail
- Empfänger muss Link aufrufen, danach ist die Domain freigeschaltet
- Vor Ablauf von 825 Tagen muss der Teilnehmer selbst tätig werden (Warn-E-Mails werden verschickt werden)

Validierung von Domains

From: dfnpki-mailsender-noreply@dfn-cert.de

To: webmaster@uni-xyz.de

Subject: DFN-PKI: Validierung des Domainnamens uni-xyz.de

Sehr geehrte Damen und Herren,

Sie bekommen diese E-Mail, weil Sie für die Domain uni-xyz.de Serverzertifikate in der CA dfn-ca-global-g2, RA 5200 beziehen wollen. Öffnen Sie zum Bestätigen bitte folgende Seite:

https://pki.pca.dfn.de/Eva/domain/ca-xyz/74c98445p7f73q11c5-b6a0q9ba437e

Weitere Informationen erhalten Sie unter https://www.pki.dfn.de/faqpki/domains

Für Rückfragen können Sie sich gerne an dfnpca@dfn-cert.de wenden.

Mit freundlichen Grüßen

Ihr DFN-PKI-Team

Validierung von Domains

Mögliche Challenge-E-Mail-Adressen:

- local-part: admin@, administrator@,
  webmaster@, postmaster@, hostmaster@
- domain-part: Jede Variante bis zur Base-Domain.
  Beispiel: Bei gewünschter Domain inst1.inf.uni-xyz.de sind möglich:
  @inst1.inf.uni-xyz.de
  @inf.uni-xyz.de
  @uni-xyz.de
- Alternative für den Notfall: E-Mail-Adressen aus WHOIS (Schwierigkeiten absehbar wg. DSGVO)

Validierung von Domains

Vor- und Nachteile „E-Mail-Challenge“:

- Vorteil: Sollte in allen Betriebssituationen machbar sein
- Nachteil: MX und vordefinierte E-Mail-Adresse müssen vorhanden sein
- Andere Verfahren brauchen noch mehr Werkzeugunterstützung...

Validierung von Domains

Zeitplan:

- Juni: Technische Voraussetzungen für neues Verfahren „E-Mail-Challenges“ fertig
- Juni/Juli: DFN-PCA fordert Teilnehmer auf, alle benötigten Domains neu mit „E-Mail-Challenge“ zu validieren
- 1. August: Domains, die nicht erneut mit neuem Verfahren validiert wurden, können nicht mehr in neuen Serverzertifikaten genutzt werden.
  (bestehende Zertifikate bleiben gültig)

Fazit und Ausblick

Fazit und Ausblick

- Java >= 9, DSVGO: Ist in Arbeit
- Domain-Validierung:
  - Es wird für Sie aufwändiger
  - Potentiell schnellere Domain-Validierungen, keine Brief-Post mehr
  - Sie müssen vor dem Stichtag 1. August Ihre Domains mit neuen Methoden validieren lassen
  - ...Aber erst muss die DFN-PCA die Werkzeuge fertigstellen...

Haben Sie noch Fragen?

- Kontakt:

  DFN-PCA

  dfnpca@dfn-cert.de

  https://www.pki.dfn.de

  https://blog.pki.dfn.de