Neues aus der DFN-PKI

Jürgen Brauckmann
dfnpca@dfn-cert.de

Überblick

- Aktuelles
- CAA
- Mozilla/crt.sh/DFN-PKI
- Certificate Transparency

Aktuelles

- G2-Einführung problemlos
- Verhältnis gültige Zertifikate:

G1	G2
445.000 :	120.000

- Laufzeit Serverzertifikate:
  Ab März 2018 Begrenzung auf 825 Tage

Aktuelles

- Empfehlungen für SMTP-Transportverschlüsselung:

  https://www.dfn-cert.de/aktuell.html

  - Konzepte
  - DANE/TLSA
  - Postfix/Exim-Konfig-Hinweise

Aktuelles

Veranstaltungen:

- **Tutorium "EU-Datenschutz Grundverordnung - Änderungen und Auswirkungen auf die Praxis"**
  18. Oktober, Hamburg
- **Ausbildung zum Informationssicherheitsbeauftragten**
  Block 1: 14.-16.11., Hamburg
  Block 2 (mit Prüfung): 17.-19.01.2018, Hamburg

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

Aktuelles

Veranstaltungen:

- **6. DFN-Konferenz Datenschutz**
  28.-29. November, Hamburg
- **25. DFN-Konferenz „Sicherheit in vernetzten Systemen“**
  27.-28.02.2018, Hamburg

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

CAA

CAA

RFC6844, „Certification Authority Authorization“

- CAA Resource Records im DNS
- Welche CA darf Zertifikate für die Domain ausstellen?
- Prüfung nur von CAs!

```
$ORIGIN hs-musterstadt.de
.  CAA 0 issue "pki.dfn.de"
.  CAA 0 iodef "mailto:certadmin@hs-musterstadt.de"
```

Auf welche Ebene im DNS können CAA RRs stehen?
=> Überall, Auswertung durch CA von links nach rechts.

Beispiel:

```
hs-musterstadt.de.          IN CAA 0 issue "pki.dfn.de"
sub.hs-musterstadt.de.      IN CAA 0 issue "example-pki.org"
```

Abfragen durch CA:

```
www.institut.sub.hs-musterstadt.de
    institut.sub.hs-musterstadt.de
            sub.hs-musterstadt.de
```

=> example-pki.org darf ausstellen

DFN Deutsches Forschungsnetz

CNAMEs:

- CAs folgen CNAMEs bis zur TLD (RFC6844)
- oder auch nicht (Errata 5065)

```
hs-musterstadt.de.          IN CAA 0 issue "pki.dfn.de"
cname.hs-musterstadt.de.    IN CNAME sub.uni-musterstadt.de.

uni-musterstadt.de.         IN CAA 0 issue "example-pki.org"
```

Abfragen durch die CA (RFC6844):

```
cname.hs-musterstadt.de  => CNAME sub.uni-musterstadt.de
 sub.uni-musterstadt.de
     uni-musterstadt.de  => example-pki.org darf ausstellen
```

Mozilla/crt.sh/DFN-PKI

Mozilla

- crt.sh ermöglicht Prüfung von ausgestellten Zertifikaten durch Dritte
- Dabei fallen Fehler auf
- Alle PKIs betroffen, auch DFN-PKI

Mozilla

- Juli/August: misissued.com
- > 30 PKIs betroffen
- Fehler z.B.:
  - Metadata in OU („.“, „-“)
  - Double-dots in FQDN (www**..**uni-xyz.de)
  - DNSName is not in preferred syntax (www.uni-xyz.de**.**)
  - uvm.

Mozilla

- Reaktion DFN-PKI: Volldurchlauf von Prüftool cablint durchgeführt.
- Ergebnis:
  - 66 Zertifikate mit Metadata-OU
  - 5 Zertifikate mit „DNSName is not in preferred syntax“ (www.uni-xyz.de.)
  - 130 Zertifikate mit doppeltem Servernamen (case-insensitiv, z.B. www.uni-xyz.de und www.Uni-XYZ.de)
  - 12045 Serverzertifikate enthalten E-Mail-Adresse (in der DFN-PKI fälschlicherweise möglich bis 12/2014)

Mozilla

- „Selbstanzeige“ bei Mozilla
- Größte Anzahl: Serverzertifikate mit E-Mail-Adressen
  - 12.045 von ca. 90.000 gültigen Serverzert. in der DFN-PKI
  - Ca. 3/4 dieser Zertifikate (damals erlaubterweise) mit SHA-1 signiert
    => sowieso inzwischen unbenutzbar

Certificate Transparency

Certificate Transparency

- Jedes Serverzertifikat weltweit abrufbar geloggt

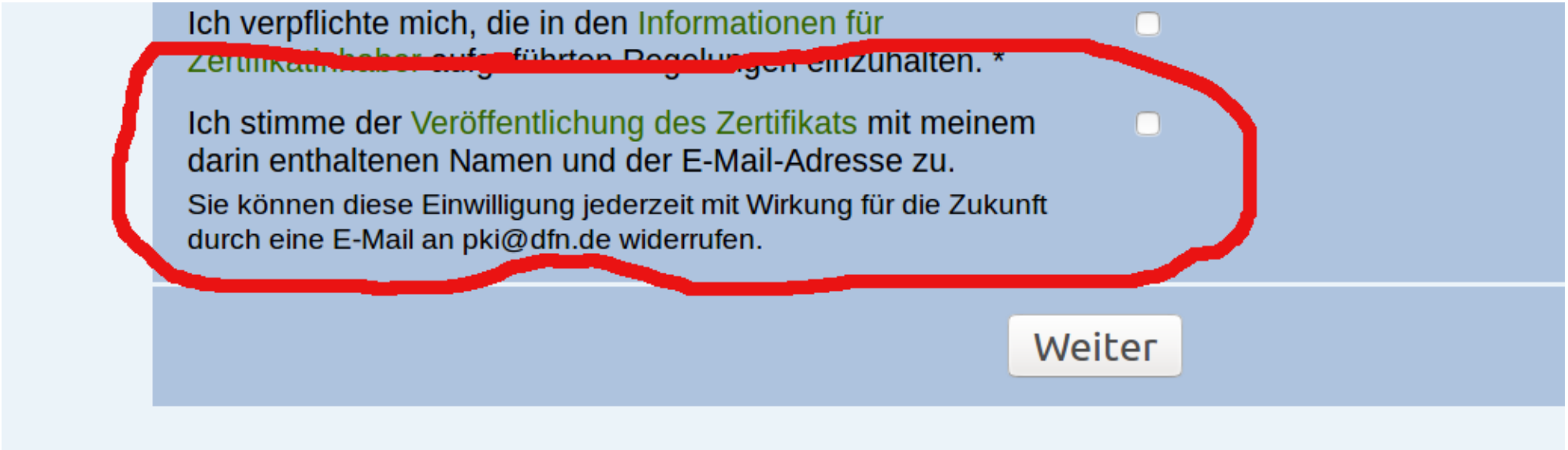
- Google Chrome fordert, dass ab 03/2018 Serverzertifikate in CT geloggt sind.

  => DFN-PKI bereitet CT vor

Certificate Transparency

Veröffentlichen/CT-Loggen als Pflicht!

exchange.vserv1.intern.hs-musterstadt.de



Zusammenfassung

Zusammenfassung

- Empfehlungen SMTP-Transportverschlüsselung
- Veranstaltungen: ITSIBE-Lehrgang
- CAA
- Mozilla/crt.sh/DFN-PKI
- Certificate Transparency

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