Zertifikate

DNS CAA, Transparency und co

DNS CAA

- Certification Authority Authorization (CAA) Resource Records (RR)
- RFC 6844
- Besitzer einer Domain definiert erwünschte Zertifizierungsstellen (CA‘s) zwecks Erstellung von X.509 Zertifikate
- Ab Sept. 2017 sind Zertifizierungsstellen (CA/Browser Forum) verpflichtet diesen RR zu validieren

DNS CAA

- Regelungen für CAA Records innerhalb der Domains (delegiert an RWTH-Nameservern)
  - DFN-PKI ist für alle Zonen (Domains) per default erlaubt (CAA RRs sind bereits vom RWTH-Hostmaster eingepflegt)
  - DNS-Administratoren können über DNS-Admin weiter CAA RRs setzen/ auswählen
  - Eintrag auch über E-Mail möglich
    - hostmaster@rwth-aachen.de
    - ca@rwth-aachen.de
    - servicedesk@itc.rwth-aachen.de

DNS CAA

- Liste der zur Auswahl stehenden CAs wird von der RWTH CA gepflegt
- Bereits ausgestellte Zertifikate sind nicht betroffen (Prüfung bei Erstellung)
- CAA RRs mit Eigenschaft „issuewild“ sind nur für Hosts erlaubt, Antrag an die RWTH CA (wie Wildcard-Zertifikate ja auch)
- Wegen des hierarchischen Aufbaus: spezifischer Host-Eintrag vor dem Zonen-Eintrag
- weitere Infos: https://blog.pki.dfn.de/2017/03/rfc-6844-certification-authority-authorization-caa/

DNS CAA

- Das bedeutet für den Admin
  - CAA Records für den Hostnamen (FQDN) seines Servers im DNS setzen/prüfen.
  - Zertifikatsantrag (CSR) generieren und an eine im CAA Record definierte CA schicken
  - ggf. vorher RWTH CA um neuen Eintrag einer weiteren CA bitten

Veröffentlichung von Serverzertifikaten mit Certificate Transparency

- ab 26.02.2018 werden Zertifikate aus der DFN-PKI mit Certificate Transparency veröffentlicht
- Infos dazu siehe https://blog.pki.dfn.de/2018/01/certificate-transparency-in-der-dfn-pki/
- Neuerung für Antragsteller: einer Veröffentlichung **muss** zugestimmt werden
- Rücknahme des Wunsches auf Veröffentlichung nicht möglich
- die Modalitäten für Nutzerzertifikate sind nicht betroffen
- Infos siehe https://www.dfn.de/fileadmin/PKI/anleitungen/Pflichten-der-Teilnehmer_V1.3.pdf https://www.dfn.de/fileadmin/PKI/anleitungen/Informationen-fuer-Zertifikatinhaber_V1.2.pdf

Zertifikate

geänderte Laufzeit Serverzertifikate DFN PKI Sicherheitsniveau "G2"

- nun 27,5 Monate (wg. Richtlinie CA/Browser-Forums, ab Anfang März 2018 maximal 825 Tagen)
- ab 26.02.2018 automatisch gesetzt
- bereits ausgestellte Zertifikate werden nicht tangiert
- keine Handlungsbedarf auf Seiten der Nutzer - Benachrichtigung etc. erfolgt angepasst
- Nutzerzertifikate sind nicht betroffen

Ergebnis des letztjährigen Audits der DFN-PKI

- neue Version 3.7 der Zertifizierungsrichtlinie
- Infos hierzu https://www.pki.dfn.de/fileadmin/PKI/Policy-Archiv/DFN-PKI_CP_V3.7.pdf
- wichtigsten Änderungen sind im Einzelnen
  - Neuer Audit-Standard ETSI EN 319 411-1
  - Klarstellungen bzgl. Verbots von E-Mailadressen in Serverzertifikaten

Ergebnis des letztjährigen Audits der DFN-PKI

– Klarstellungen bzgl. der Sperrgründe in Kapitel 4.9.1

- Das Zertifikat enthält Angaben, die nicht gültig sind.
- Der private Schlüssel wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Der Zertifikatinhaber ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Das Zertifikat verletzt Warenzeichen o. ä. nach Abschnitt 3.1.6
- Die Nutzung des Zertifikats verstößt gegen die CP oder das CPS.
- Die ausstellende CA stellt den Zertifizierungsbetrieb ein.
- Der Zertifikatinhaber bzw. Teilnehmer stellt einen Sperrantrag.
- Darüber hinaus alle Gründe, die in Kapitel 4.9.1 der Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [CAB-BR] angegeben sind

Vielen Dank
für Ihre Aufmerksamkeit