SWITCHpki News

Thomas Weller
pki@switch.ch
Tr&Id WG Meeting, Berne, 15 May 2019
CAA Resource Record

- CAA - Certification Authority Authorization
- Resource Record in the DNS

- Standard already adopted in 2013

- Since September 8, 2017
  - **mandatory for CAs** (CA/Browser forum)
  - check and follow the CAA content

- **No requirement** in SWITCHpki for domain owners to implement CAA records
Why CAA

- "whitelists" authorities (CA's) issuing x509 certificates for a specific domain
- increase the security of the whole public key infrastructure

Heise Magazine c't 07/2018: “Zertifizierungsstellen mit CAA-Records selbst reglementieren"
CAA - Benefit

More security for your domain(s)...

• certificates only from the CAs I trust

• prevent unauthorized issued certificates
  ➢ it still happens (sloppy CA...!)!
  ➢ attacker request certificate from other CAs
  ➢ Various attack scenarios
    o Man in the middle
    o redirected to manipulated hosts
CAA in SWITCHpki

- Whitelist: Certification Authority QuoVadis
- CAA entries from several CAs allowed

Format:

```
example.com.   CAA 0 issue "quovadisglobal.com"
example.com.   CAA 0 issuewild "quovadisglobal.com"
example.com.   CAA 0 iodef "mailto:cert-admin@example.com"
```

IODEF (Incident Object Description Exchange Format) tag

- report malicious requests for the corresponding domain
CAA – Policy and Security

Policy
• e.g. a set of possible CAs for
  ➢ second level domain (cover all subdomains)
  ➢ subdomain can overwrite policy
  ➢ helpful: Certificate Transparency Logs for issuing CAs
    o Certificate Search: https://crt.sh/

Security
• Use DNSSEC to secure CAA records
• include your iodef contact
Errors

- wrong CAA records
- SERVFAIL
- Timeouts...
- CA QuoVadis not whitelisted
- ...

Subscriber will be informed in SWITCHpki
Useful links

CA/B Baseline Requirements:
https://cabforum.org/baseline-requirements-documents/
(CAA section 3.2.2.8)

QuoVadis CAA documentation:
https://swit.ch/qvcaa

Generate and Proof CAA
https://sslmate.com/labs/caa
https://www.ssllabs.com/ssltest/
**Elliptic Curve Cryptography (ECC)**

- assymetric cryptography
- based on calculation of elliptic curves

**Main benfits**

- ECC requires smaller keys (compared to non-ECC cryptography e.g. RSA)
  - reduces storage and transmission requirements
  - increase the speed in using ECC
  - less computing power

- used in mobile apps, IoT etc.
ECC in SWITCHpki

- ECC certificates available in SWITCHpki
  - Business ECC SSL: ready
  - soon: EV ECC SSLs

- Supported Curves in Trust/Link
  - 256 Bit curve (prime256v1)
  - Standard: ANSI / SECG

QuoVadis ECC documentation:
https://swit.ch/qvecc
Fusion QuoVadis - DigiCert

- Certificates will remain
  - TLS/SSL Zertifikate / Secure E-Mail
  - Order and renewal processes

- same Contact persons
  - for SWITCH: Service / Support QuoVadis
  - SWITCHpki participant: SWITCH – pki@switch.ch