Certificate Limitation Profile

Application-level trust model

Dmitry Belyavskiy

Technical Centre of Internet

Current state (RFC 5280)

- Binary model of trust
  - Trusted CAs
  - CRL/OCSP
  - CA-driven revocation

- Future of revocation
  - https://cabforum.org/pipermail/public/2017-March/010287.html

Google vs Symantec (2017)

- “Too big to fail” CA
- List of limitations:
  - A reduction in the accepted validity period.
  - An incremental distrust of all currently-trusted Symantec-issued certificates.
  - Removal of recognition of the Extended Validation status of Symantec issued certificates.

Source: https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/eUAKwjihhBs/rpxMXjZHCQAJ

Application-level trust now

- Managing list of trusted CAs
- CRL/OCSP validation
  - What if OCSP is unavailable?
- Hardcode in case of limitations

Solution: CLP

- List distributed with/by application
- CRL-like syntax, crypto-signed format
- Shared codebase instead of app-level hardcode

List of limitation

- **Itself/descendants**

- **maxIssued** – no trust to certs issued after
- **maxValidity** – no trust to certs after
- **validityPeriod** – maximum validity period
- **ignoredX509Extensions**
- **requiredX509Extensions**

Verification process with CLP

- Build chain of trust
- Process from root till the end
- Apply limitations to the matching certs

Application level checks

- CLP in use
- Minimal date of issuance
- Signed by correct trust anchor

Questions?

beldmit@gmail.com