CT for Code Signing

Tim Hollebeek, 2023-08-10

Why CT for Code Signing?

- Allow independent evaluation of quality / compliance of issued certificates
- Helps drive uniform minimum compliance across all CAs
- Supports information sharing between CAs
- Enables more advanced revocation and compression technologies
- Allow organizations to monitor for misuse under their subject info / domains / etc

Challenges:

Some people believe the information in their certificates is “private”, despite the fact that it is included in every signature.

Some CAs might not want everyone to know what they’re up to.

Where to log to?

- Setting up a new CT log is easy; open source packages are available
- DigiCert is willing to set up logs to support CABF here
- Microsoft interested in standing one up as well.

- Operational considerations need to be taken into account, though they are likely significantly less than TLS
- Do we need an operational policy for CT?
- Ian would like a quorum of 3 logs, minimum.

What to log?

- All revoked code signing certificates?
- All issued code signing certificates?
- All signings?
  - Microsoft scale ~ 300M signings / day

- How does this interact with short-term / single-use signing certificates?