6962-bis Status

Ben Laurie (benl@google.com)

Precertificate Format

- Using X509v3 as a format for precerts causes too many difficulties.
- Instead wrap a tbsCertificate in CMS signed-data (RFC 5652 s5).

Precertificate Format

- Signer is the issuing CA's private key.
- Issuing CA certificate is the **only thing** in SignedData.certificates.
- Other required certs to chain to a known root supplied in the "chain" parameter, as in 6962 (because SignedData.certificates is a SET not a SEQUENCE).

Precertificate Format

- Content will require a new OID for tbsCertificate Content Type.
  - Could use Data Content Type (1.2.840.113549.1.7.1, RFC 5652 s4), but a specific data type seems more sensible (also reduces concerns CAs might have about signing general data).
  - Which arc? (Happy to use Google's).

Precertificate Format - proposed text

TBD

Signed Certificate Timestamps

- Trac ticket #34
- SCTs are used in two contexts:
  a. TLS extensions (existing RFC 6962 extension and possibly in gossip).
  b. DER structures (certificates and OCSP)
- So there is no natural format for them - they should either be ASN.1 or TLS structures.

Signed Certificate Timestamps

- We believe TLS is the “natural” home, OCSP/Certificate inclusion is a stop-gap.
- Having different structures for different contexts seems like an unnecessary complication.
- Therefore, we propose to leave SCTs as a TLS structure.

Client Behaviour

- Should 6962-bis specify client behaviour?
- TLS client behaviour is a fast evolving area and the active subject of research
  - e.g. Adrienne Porter Felt et al. “Experimenting At Scale With Google Chrome’s SSL Warning”
- We don’t currently know what the right thing to do is for almost all SSL/TLS error conditions.

Client Behaviour

- Therefore, it does not seem appropriate to attempt to specify it at this stage, particularly for a new component of the TLS protocol suite.
- We believe this reflects WG consensus.

Name Redaction

- Should 6962-bis talk about name redaction?
- Name redaction does not change log behaviour, only client behaviour.
- Therefore 6962-bis should not specify when it is used, or what clients do in response.
- However, the mechanism should be defined so there is a standard way to do it, if needed.

Name Redaction

- We will also include discussion of the compatibility of name redaction with EV, DV and OV certificates, and the BRs.

Progress of the I-D

- Essentially none since the last IETF :-(
- WG debates have taken all our available time (and then some).
- Emerging consensus plus splitting some stuff to other I-Ds means we can now move forward.
- Aim to produce a major update by next IETF, ideally ready for last call.

Remaining Work

- Assuming the WG agrees with our resolution of the issues above, we just need to work our way through the remaining issue list, which we believe should be uncontroversial.
- If there are outstanding issues **not** in Trac, please add them.

Thanks!