“trans” open tickets

Eran Messeri, eranm@google.com

Ticket 4

Should we sign TBS for Certificates (i.e. non-Precerts)?

- Probably makes sense given we're likely to change how Precertificates work

Ticket 8

A way to obtain inclusion proofs for a batch of certificates around a given timestamp (Privacy)

- Proposal: Add two methods to the API:
  - Give me the timestamp between every 10,000 certs, then 1,000 certs, until happy with window size.
  - Fetch inclusion proofs for all certs in the range (incl. proofs must be independent; server may be able to calculate more efficiently).

Ticket 10

Permit Precertificate SCTs delivery through TLS extension / OCSP stapling.

- Proposal: a general TLS Extension for CT-related data: A list of data structures, each identified by IDs (IANA manages the registry).
- Will permit inclusion proof embedding, etc.

Tickets 13, 19

Problem: Separate, subsequent client calls to get STH and inclusion proof can fail.

Proposal: New API

- Combining get-sth and get-proof-by-hash
- Also return STH for get-entries

Ticket 14

Clarify ASN.1 encoding to indicate how an SCTList extension is encoded in Precertificates and OCSP responses.

Just needs doing!

Ticket 16

Naming: Decide between ‘Audit Proof’ / ‘Audit Path’ / ‘Inclusion Proof’

Proposal: ‘Inclusion Proof’, under review.

Ticket 17

Add advice on Common Names, regarding name redaction.

Proposal: The CN entry in the Precertificate will be the redacted domain name, we'll use the first entry in the redaction list if the CN is present.

Ticket 20

Do we want to be tield to the TLS signing algoritm?

Proposal: Yes, close. If TLS is not using a hash/signature algorithm because it’s not strong enough, it won’t be useful for CT’s needs either.

Ticket 21

Clarify the purpose (& mechanism) behind signature checking the log performs.

- Won’t clarify how we deviate from RFC5280
- Instead specify the set of minimal checks that need to be performed.

Ticket 22

Explain why there are three SCT delivery mechanisms.

Just needs doing!

Assigned to Ben, so likely to happen very soon.

Ticket 23

How can TLS clients match SCT to a certificate? (since they can be for non-EE certs)

Rob Stradling had some thoughts, nothing finalized.

Ticket 24

Add a section about Logs metadata.

- Don’t intend to specify *how* clients get the metadata.
- Under review.

Ticket 25

Allow freezing a log (for shutdown, etc).

Proposal:

- Final STH is a part of the log's metadata.
- Specify how a client should be have in this case (likely ignoring STHs past final one).

Ticket 26

Alternative Precertificates format.

- Major concern is that Precertificates look too much like a valid X.509 certificate (and share serial number).
- Any suggestions?

Ticket 15

Specifying TLS client behaviour.

Ben has a slide about it

Ticket 9

Explain why multiple SCTs are useful, how should a TLS client handle multiple SCTS.

Just needs work