“trans” open tickets

Eran Messeri, eranm@google.com

Distribution of tickets

- 37 tickets open.
- 19 need work
  - Grouped, comments as I go over them.
- 13 need discussion & resolution
  - Presented in-depth
- 5 belong to separate documents

Need (editing) work

- 8: Obtain Merkle proofs for a batch for certificates around the SCT timestamp.
- 10: Precertificate SCTs delivery via OCSP Stapling and the TLS Extension
- 13: Deal with server farm skew.
- 14: Clarify ASN.1 encoding

Need (editing) work

- 17: Add advice on CNs
- **19: Rejig API for efficiency/correctness**
- 22: Explain why there are three delivery mechanisms for SCTs.
- 24: Add a section about log metadata.
- **25: Freezing a log's state**
- 26: Precertificates: alternative to X.509

Need (editing) work

- 29: what does "immediately" mean?
- 32: algorithm for client checks of SCT
- 45: Incorporate RFC6962 errata
- 48: Enforce the rules for Name-constrained Intermediates
- 49: Explain why OCSP Stapling is acceptable but OCSP Fetching is not

Need (editing) work

- 15: Client behaviour specification needed (for multiple SCTs).
- 46: Log handling of already-logged certificates.
- 35: server SCT transmission restriction is misstated
- 44: Precertificates SHOULD NOT be submitted to add-chain

Pending discussion & resolution

- 38: Client behavior: In Ben’s slides.
- 42: Redacted cert dangers:
  - Pending usability clarification from browser vendors.
- 40: Auditor behavior:
  - No suggested clarifications so far.
- 4: Should we sign TBS for Certificates?
  - There were no objections
- 27: Signature & hash alg specification

Pending discussion & resolution

- 28: Algorithm agility: Partially addressed.
- 33: Cert chain length as log metadata.
- 34: RFC 5246 syntax to define the SCT:
  - In Ben’s slides.
- 36: error indications for log/client exchanges
  - Did not find that useful in past discussions.

Pending discussion & resolution

- 43: Key rollover:
  - Potentially addressed by log freezing.
- 47: Dealing with (minor) DER violations:
  - Some suggestions on how a log should behave.
- 50: Revocation checking and SCT processing order.
- 9: Security Considerations for number and variety of SCTs

TBR in a separate document

- 31: Incremental Deployment.
  - I (Eran) intend to write it up.
- 37: Client gossiping: On the agenda
- 41: Threat model and security analysis
  - Started by Stephen Kent
- 21: Signature checking purpose:
  - Spawned off to a document about log checks.
- 39: Monitor behaviour: Same?