“trans” issues update

Eran Messeri, eranm@google.com

Since IETF 93

- 59 commits to rfc6962-bis.xml
- ~12 tickets closed.

Closed tickets

- #75: Breaking down a long sentence.
- #5, #70: Adding extensions to STHs (SCTs already had them)
  - Also specifying format.
- #77: Left-over client-behaviour issue.
- #96: Metadata: Should it be dynamic?
  - Agreement among authors that metadata distribution is out of scope.
  - Also allowing changing it during log operation adds complexity.

Closed tickets

- #106: Include LogID in the STH (to identify its origin)
- #107: Structify TreeHeadSignature
  - So it can be TLS-encoded and gossiped.
- #110: Reorganize requirements into appropriate sections
  - The Log Format and Operation section describe just that.
  - Requirements for other parties (Submitters, CAs, TLS servers and TLS clients) moved into more appropriate sections.
- #105: Shrink LogID - opted for using OIDs to identify logs.

Open tickets

- #10: Permit Precertificate SCTs to be delivered via OCSP Stapling and the TLS Extension
  - Rob has a concrete plan for addressing this.
- #78: algorithm agility discussion is inadequate
  - Editors feel description is adequate, though should be extended to cover cases other than algorithm agility. Suggested edits welcome.
- #83: CT should mandate the use of deterministic ECDSA
  - Solved for ECDSA, but not RSA.
- #95: Should the response size to get-entries be a part of the log metadata?
  - Seems like there’s a consensus around suggesting a size in the RFC.

Open tickets

Split into 3 categories:

- Missing functionality
- “Better wording required”
  - If not consensus, at least clear direction.
- Technicalities / small issues

Open tickets - missing functionality

- Add SCT Inclusion Proof extension (#104)
  - Ability to staple inclusion proofs in all SCT delivery mechanisms.
- Permit Precertificate SCTs to be delivered via OCSP Stapling and the TLS Extension (#10)
  - Rob Stradling is hard at work on both!
- Log shutdown timeline and behavior (#109)

Open tickets - “careful wording”

- Removing specification of signature and hash algorithm (#64)
  - Agreement that there should be a reference to an external document.
  - Partly done.
- Normative client behaviour specification leftover (#76).
  - Agreement that client behaviour should live in a separate document.
  - Some leftover text that should live somewhere else.
- Satisfactory phrasing of algorithm agility (#78).
  - Agreement that allowing logs to change signature/hashing algorithms would be very complex.
  - Solution: Shutting down one log and turning up another.
  - Need to carefully explain why and how.

Open tickets - “careful wording” (cont’d)

- Inconsistent definition of monitor behaviour (#93)
- Fetching of inclusion proofs: Why and when are clients expected to do this? (#94)
  - I believe the gossip draft does a pretty good job of explaining that.
- Should the response size to get-entries be a part of the log metadata? (#95)
  - Conclusion that the standard should recommend a size.
  - Specifying it in the metadata is too inflexible
  - Clients would have to cope with responses of various sizes anyway.
- Clearer definition of when a certificate is CT-compliant needed (#99)

Open tickets - Technicalities / small issues

- OIDs and IANA considerations (#81)
- Mandating use of deterministic ECDSA (#83)
  - Done for ECDSA, has to account for RSA.
- Adding reference to threat analysis document (#87)
- "root" should be "trust anchor" (#102)
- TLS session resumption: Server MUST NOT send SCTs (#108)
- Clarify log entry ordering requirements (#53)
- Allocate an OID for CMS precertificates (#97)

Implementations

- Martin Smith is working on one.
- So far only thing uncovered is difficulty verifying signature over CMS.
- Feedback, particularly on domain redaction, still sought.