RFC6962-bis update

- Some tweaking still needed.
- Last call should wait for our implementation.
    - A member of the Certificate Transparency team at Google is working on it.
- We think all major issues resolved.
- Interoperability:
    - A log cannot support both V1 and V2.
    - Nothing prevents an operator from running both.
    - Clients may have to support both for a while.

“trans” issues update

Eran Messeri, eranm@google.com

Closed tickets

- #4: Should we sign TBS for Certificates?
  - Yes!
- #80: Issuer key hash (re-)introduced to the signed data covered by the SCT.
  - Structure of signed data for Precertificates and X.509 certs is now identical.
  - Includes TBSCertificate and issuer key hash.
- #86: SCTs are returned in final format (from add-chain/add-pre-chain).
- #68, 69: specification of sha-256 for the SCT, STH.
  - Some fields explicitly called out as containing sha-256 hashes. Removed.
  - Also ticket #72, #64 re citing specific algorithms.
- #90: Clarify how to turn a MerkleTreeLeaf into a leaf hash.
  - Added text to make implementers’ lives easier!

Closed tickets

- #82: Add a way to get the SCTs for entries returned by get-entries
  - Needed for mirroring, easier investigation of incorporation time.
- #92: get-entries needs to return the whole X509ChainEntry.
  - Including the actual leaf so the client could verify signature by the right CA key.
  - Note SCT signature no longer covers the entire X.509 cert in case of add-chain submission.
- #89: get-entries: "end" greater than "tree_size" should be allowed
  - To allow dealing with skew.
  - Logs now MUST return partial replies as well as STHs.
- #58: Limit the number of STH's allowed to be published per time unit
  - To prevent client fingerprinting.
  - Related to #83, use of deterministic ECDSA signatures.

Closed tickets

- #84: Clarify that root certs have empty certificate_chain
  - It’s pointless to log, but technically allowed…
- #81: OIDs and IANA Considerations
  - Apparently nobody had a strong opinion about it?
- #73: Section 3 text re log cert validation is ambiguous.
  - Certs that are valid according to RFC5280 MUST be accepted, otherwise MAY be.
  - Also MAY log but not produce an SCT
- #65: remove section 5.4 and reference to "Auditor" in section 3
  - Auditor -> auditing as an operation done by participants who care to.
- #91 (minor): Clarify encoding of fields in the log client messages.
  - It wasn’t clear that some things are base64-encoded, fixed.

Closed tickets

- #40: missing threat model and security analysis
  - Steve Kent’s proposed threat model draft has been adopted by the WG.
  - Related #55: Describe the implications of clients *not* doing certain optional checks
- #85: Precertificate CMS structures MUST be DER.
  - Even though CMS allows BER, for simplicity DER is required.

Tickets related to client behaviour

- What a client MUST do to confirm compliance with the protocol (or comply with the protocol itself). ← This is not “client behaviour”.
- The actions a client takes when it detects non-conformance (of a cert, log) ← This is “client behaviour”

Related tickets:

- #63: remove all normative references to client behavior
- #74: normative statement of TLS client behavior in Section 3
- #76, #77: Normative client behavior specified in Section 3.4.

Pending review

- #70: Spec for STH Top-level extensions syntax.
  - Incorporated text proposed by Steve Kent, pending review.
- #76, #77 - covered in client behaviour.
- #96: Metadata: Should it be dynamic?
  - Was discussed, we could expand on the reasoning behind it.

Open tickets

- #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.
- #96: Metadata: Should it be dynamic?
  - Should evaluate on a per-item basis, in my opinion.
- #95: Should the response size to get-entries be a part of the log metadata?
  - In practice clients would still want to use partial replies, so would have to ignore.

Open issues

- #87: Add reference to threat analysis document
- #64: remove specification of signature and hash lags from section 2
- #93: Monitor description: Inconsistency between intro and section 5.4
  - Bigger issue may be distinction between different flavours of monitors.
- #94: Fetching of inclusion proofs: Why and when are clients expected to do this?
  - May belong in an architecture document describing the entire system.