6962-bis update

Eran Messeri, eranm@google.com

Overview

Significant feedback from Mozilla post WGLC, in (roughly) 4 categories:

- Architecture
- Data structures
- Editorial
- HTTP API

All issues captured in the issue tracker.

Almost all were triaged.

Editorial

All of these seems sensible to us:

- State the log parameters in the section that defines a log (#166)
- Single Extension types for SCTs & STHs (#173)
- Remove use of `digitally-signed` (#174)
    - Better consistency with TLS 1.3
    - But not removing the bytes indicating signature, hash algorithms (simplify impl)
- Better explanations:
    - Instructions for constructing leaf hash from cert + SCT (#177)
    - Add description of how to validate an SCT (#178)

Editorial (cont’d)

- Consolidate all Merkle tree data formats (#180)
  - Yes, it’s spread all over.
- Clarify notation in the Merkle tree section (#182)
  - Notation for specifying “a tree of size N”, “entry at index K”, etc.
  - Suggestions welcome!
- Error codes (#186):
  - Clarify which are common; no reuse beyond that.
- Define "incorporate" (#167)
  - Making it clear that a submission is incorporated when a corresponding LogEntry exists.

Data structures

- Get rid of the SCTWithProofDataV2 and similar data structures (#172).
  - Should do; SCTWithProofDataV2 isn’t that useful without redaction.
- Remove `timestamp` from STH? (#175)
  - Re-cast for discussing STHs for liveliness.
- Remove `X509ChainEntry` and `PrecertChainEntryV2` (#176)
  - Making get-entries output consistent with the add-chain input.
- Indicate certificate / precertificate in Entry and SCT (#179)
  - Intent: Move the Precert/X.509 cert indication into the SCT rather than the TransItem.

HTTP / API

- Remove STH from `get-entries` response (#168)
  - We may overdid front-end skew.
- Don't guess at STHs (#169)
  - Don’t return STH in get-sth-consistency; get-all-by-hash. Related to #168.
- Consolidate "Add Chain" and "Add PreCertChain" endpoints (#181)
  - Already implied by the parameter.
- Don't violate BCP 190 (URIs advertised in a directory) (#185)
  - Clients need a bunch of metadata on the log; service discovery is of limited use in that case.
  - Document why 6962-bis doesn’t adhere to that.

Architecture

- Allow for separate SCT and STH keys? (#170)
  - Right now no clear benefit to allowing that.
  - Suggestion: Note in security considerations. (can be done if necessary)
- Remove unnecessary operational restrictions on logs (#165)
  - "Log operators MUST NOT impost any conditions on retrieving or sharing data from the log"
    - Suggestion: change MUST to SHOULD, require in policy.
  - "the log MUST veirfy that [a submitted cert] has a valid signature chain to an accepted trust anchor"
    - Spam mitigation; leave as-is, better explanation why it’s essential (in light of TBSCert)
- Incorporate new protocol mechanisms into TLS Client section (#164)
  - Explain that inclusion proofs, if delivered in-band, should be validated.

Architecture (cont’d)

- The entire STH history of the log must be accessible (#163)
  - Add API (get-sths) for getting historic STHs.
  - Add sequence number to STHs.
- Bound the set of artifacts a log is expected to produce (#162)
  - TBD

Undecided - no (internal) consensus

- Log IDs: OID or INT32? (#171)
- OIDs from an IANA-managed registry (#187)

Way forward

- Write up clarifications / suggestion conclusions in filed tickets.
- Pull Requests for issues we believe there’s consensus.
- Post each change to the trans list (individually) to confirm consensus.
- Hash out the few remaining disagreements.
- Separate document to describe the variant of CT with stronger guarantees for clients.