Trans open trac issues

Eran Messeri, eranm@google.com

Components

- rfc6962-bis
- client-behaviour
- client-privacy

RFC6962-bis - all tickets

- #4: Should we sign TBS for Certificates?
- #10: Permit Precertificate SCTs to be delivered via OCSP Stapling and the TLS Extension.
- #41: missing threat model and security analysis.

RFC6962-bis - all tickets (cont’d)

- #53: Clarify log entry ordering requirements
- #55: Security Considerations: Describe the implications of clients *not* doing certain optional checks
- #58: Maximise number of STH's published per time unit

Ticket 4: Signing TBS for Certs

Should the signature and signature algorithm identifier be excluded from the SCT?

- Will be consistent with Precertificates.
- Will avoid incorrect encoding of signature parameters.

Seems like a good idea overall.

Ticket 10: Delivery of Precert SCTs

- In RFC6962 the origin of the SCT implies Cert/Precert.
- Ticket suggests allowing delivery if Precert SCTs over TLS extension / stapled OCSP.
- Can define backwards-compatible structure that will contain new SCTs.

Ticket 41: Threat model

Steven Kent is writing a threat model and security analysis.

Ticket 53: Log entry ordering req

- (Almost) all RFC6962 logs incorporate entries in chronological order.
- This is not a requirement and clients must not expect this behaviour.

Ticket 55: Security Considerations

- Suggested as a middle ground between mandating client behaviour and not.
- Likely redundant given the client-behaviour comments.

Ticket 58: STH's per time unit

- Ticket calls for maximising the number of STH's published per time unit.
- Would avoid client fingerprinting.
- Enforcement is non-trivial.

Client behaviour

- ~20 tickets.
- Has a dedicated section in the agenda.

Client privacy - ticket #8

- Suggests a way to preserve client privacy batch-fetching inclusion proofs.
- Significant change.
- Does it preserve privacy well enough?
- Postponed not to block RFC6962-bis.