RFC 6962-bis update

Ben Laurie

Overall Status

- See https://www.ietf.org/rfcdiff?url1=draft-ietf-trans-rfc6962-bis-05&difftype=--html&submit=Go%21&url2=draft-ietf-trans-rfc6962-bis-07.

- Most historical tickets now resolved.

- Aim to try to resolve outstanding tickets by next IETF.

Server Skew

- A server farm will always have some variance between front ends.
- The existing API did not deal well with this: it was possible to end up in an infinite loop, for example:
  - Get most recent STH from server A
  - Try to audit a recent cert against STH using server B, which only has previous STH. Audit fails.
  - Update STH - from server A again.
  - Rinse, wash, repeat.
- APIs all updated to allow clients to converge on a result despite server skew, by ensuring the response contains necessary server state.

Error Codes

- Added machine readable error codes to responses.

API Efficiency

- In RFC 6962 an inclusion proof took up to three calls: Get STH, Get Consistency Proof from previous STH, Get Inclusion Proof.
- Added a new API to get all three in one call.

Metadata

- Added description of metadata needed to interact with a log.
  - Base URL
  - Hash Algorithm
  - Signing Algorithm
  - Public Key
  - Maximum Merge Delay
  - Final STH (for logs that have ceased operations)

Algorithm Agility

- By far the simplest way to change algorithms is to simply freeze existing logs and start new ones.
- If algorithms are sufficiently broken that the integrity of frozen logs can no longer be guaranteed, then the new logs will have to include a copy of all (relevant) data in the old logs.