IETF89 Trans

Discussion points & notes

- Issues in trac
  - [trac#1] Options for avoiding logging private subdomains
    - [trac#2] Require log submitters to verify SCTs
    - [trac#3] TLS clients should audit
    - [trac#4] Should we sign TBH for certs
    - [trac#5] Add extensions to STH
    - [trac#6] Should we flatten the MerkleTreeLeaf structure ?
    - [trac#7] Clarify error messages from logs
    - [trac#8] Need a way to obtain Merkle proofs for a batch of certs around SCT timestamp
- Gossip
- Embedding Inclusion Proof in TLS/OCSP
- Timelines: WG Final Call vs Chrome Deadlines
- Privacy preserving inclusion proof lookups

[trac#1] Options for avoiding logging private subdomains

Rob Stradling's proposal:

1. Allow name-constrained intermediate cert logged in place of EE:
   a. NC must include 1+ permitted domain names (no TLDs or public suffix)
   b. Intermediate has flag explicitly permitting it to be logged in place of EE

2. Allow masking of private subdomains in PreCert:
   a. Precert has `SAN:dNSName="<PRIVATE>".customer.com`
   b. EE has:
      i. `SAN:dNSName=top.secret.customer.com`
      ii. an INT for each CN & SAN which specifies how many left-most domain components are masked

[trac#1] Options for avoiding logging private subdomains

- Bonus: Allows CT TLS clients to perform the same checks for "overly-broad" EE wildcard certs to the NC of issuing certs.
  - e.g `NC=<PRIVATE>.co.uk` issues `top.secret.blah.co.uk` may be rejected by clients.
- Though the log probably shouldn't enforce client policy.

EE SAN	CT Log sees	TLS client w/o CT sees	TLS client w CT sees
*.co.uk	*.co.uk	*.co.uk (rej)	*.co.uk (rej)
top.secret.co.uk	<PRIVATE>.co.uk	top.secret.co.uk (accept)	<PRIVATE>.co.uk (rej)

Gossip

Goal: Detect forked/split-world logs
Mechanism:

- Gossip STHs between CT aware parties to detect inconsistency
  - Between TLS Client & Server
  - With Logs (about other logs)
- TLS Servers could maintain a pool of STHs sent by clients and pass a fraction of them out at random during responses

Embedding Inclusion Proof in TLS/OCSP

- Transforms potentially privacy-eroding inclusion proof query into a simple tree consistency proof request.
- Optional - has page-load-latency/size impact & 10 year roll out.

Google

Timelines: WG Final Call vs Chrome Deadlines

Privacy preserving inclusion proof lookups

- DNS query mechanism
- Batch queries around SCT Timestamp
  - Risks when log is/was not accepting many certs at the time