draft-linus-trans-gossip-ct

Daniel Kahn Gillmor, ACLU
Linus Nordberg, NORDUnet

IETF93, Prague
why
  ▶ log accountability – verifying the append-only property in space and over time
  ▶ changing entries
  ▶ not keeping the promise of an SCT
  ▶ log exposing multiple views (partitioning)

how
  ▶ getting SCT’s and STH’s to auditors and monitors

changes in -02
  ▶ three browser channels for sharing SCT’s and STH’s
  ▶ STH pollination being the actual news

working group adoption
Certificate Transparency
(detect CA misbehavior)
Certificate Transparency
(detect CA misbehavior)
Certificate Transparency (detect CA misbehavior)

Gossip

detect Log misbehavior
Certificate Transparency (detect CA misbehavior)
Log

Monitor

Auditor

Website

Browser

Gossip

Certificate Transparency

detect CA misbehavior

Detect Log misbehavior

- SCT Feedback
- STH Pollination

CA

cert request

cert chain + SCT

Website

[Cert]

[SCT]

[Cert]

[SCT]

Log

Inclusion Proof

[STH, SCT]

Consistency Proof

SCT, StH

Everything

STH

STH

STH

Browser

HTTPS Traffic

SCT+certs

SCT+certs

Polling?

STHs

STHs

SCTs
Certificate Transparency (detect CA misbehavior)