Certificate Transparency Gossip

Daniel Kahn Gillmor <dkg@aclu.org>
Linus Nordberg <linus@nordu.net>

IETF-92, Dallas
March 2015

https://tools.ietf.org/html/draft-linus-trans-gossip-ct-01

Gossip is to keep logs accountable

- Logs keep CAs accountable
- What keeps Logs accountable?
  - They need to prove that they are honoring their MMD
  - They need to not present split views of the tree head to the public
- Auditors do this work

Auditors

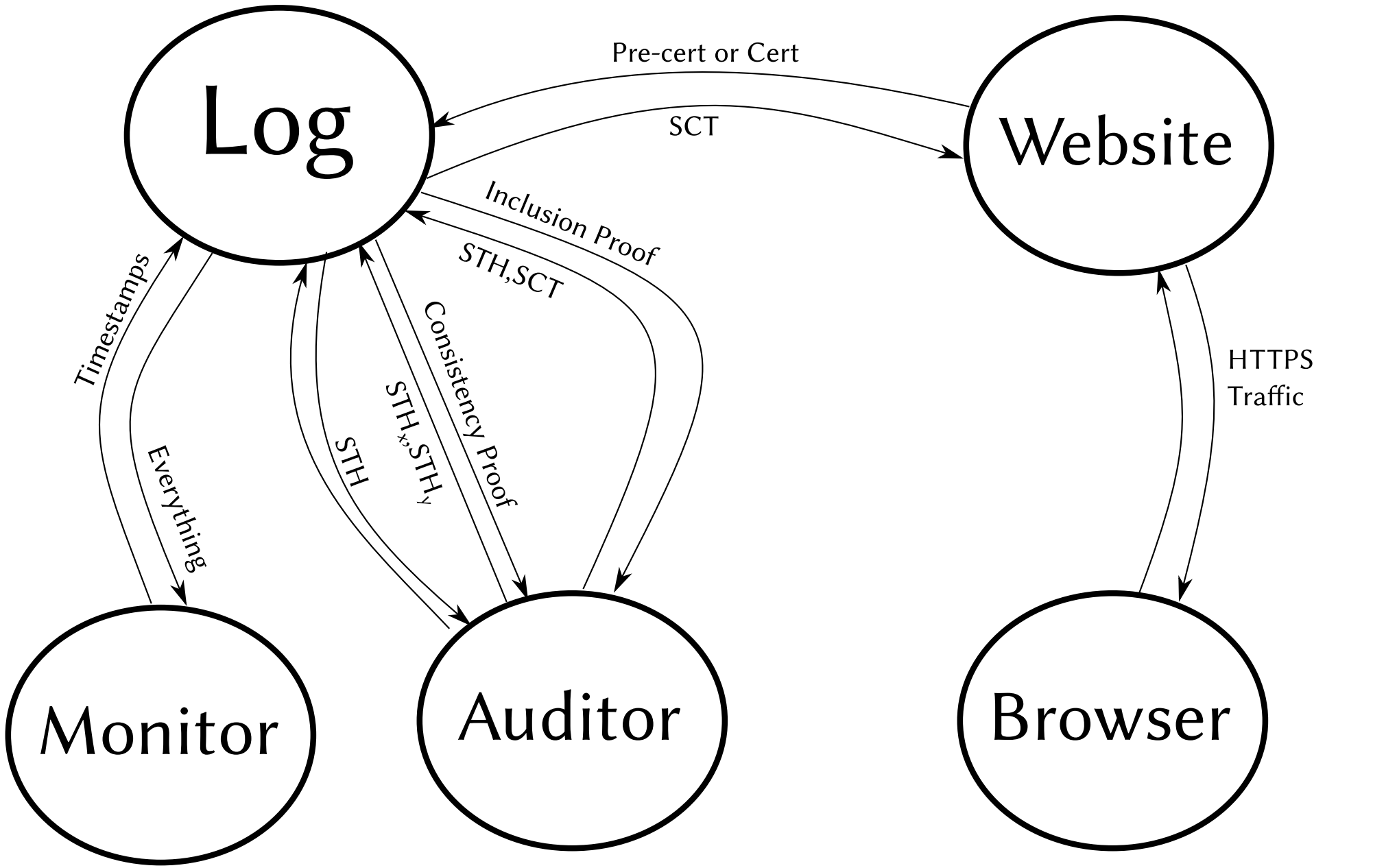
- What is a CT Auditor?
- We believe it is likely that CT Monitors will also be Auditors.
- Not all Auditors are Montiors

Privacy considerations for gossip

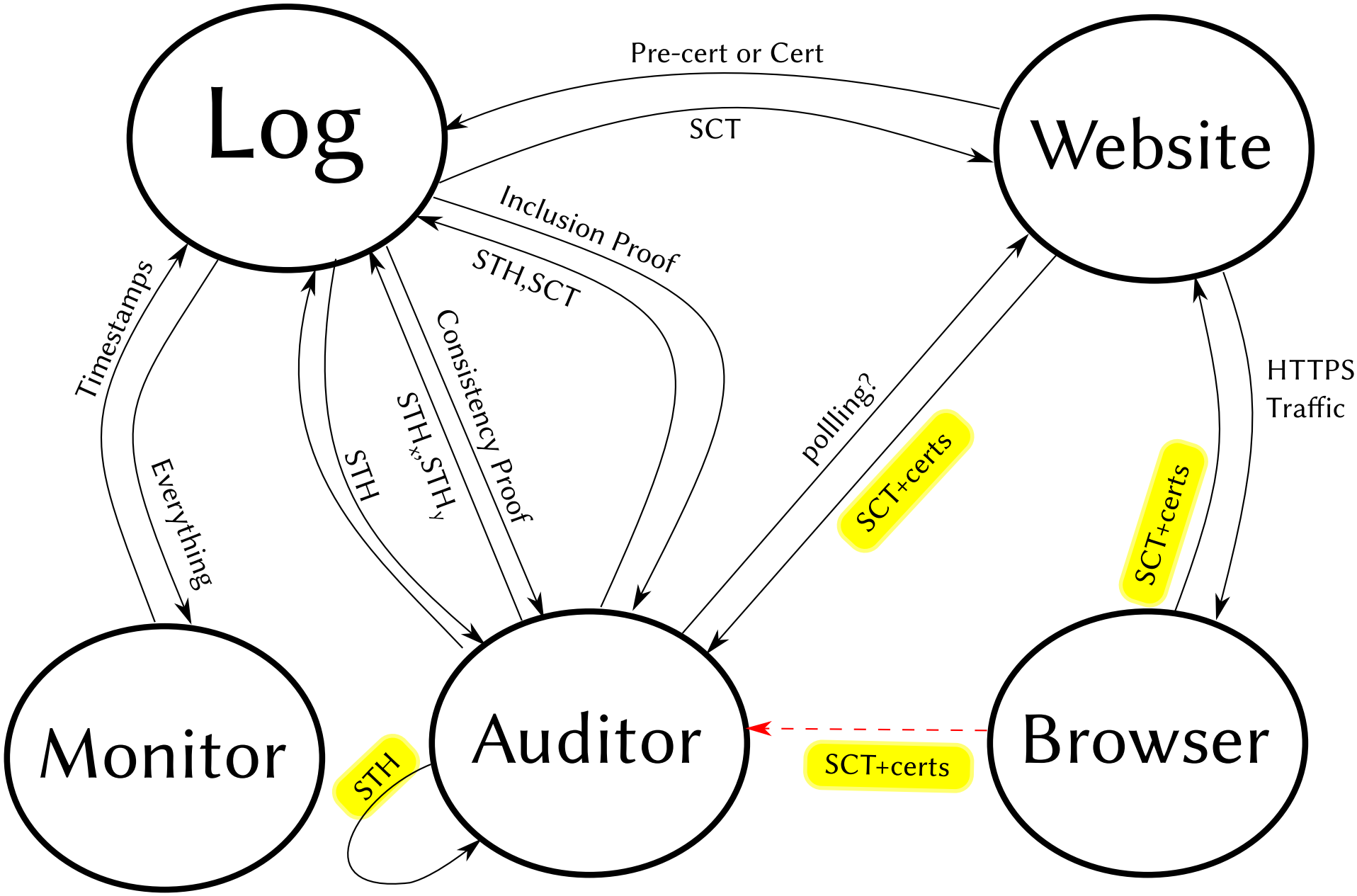
- Relationships between servers and clients are the most sensitive. (e.g. “who visited https://scary.example/ ?”)
- We do not need to protect relationships between auditors and logs, or between servers and logs.

Where does gossip happen?

- Between auditors (STHs)
- Between server operators and auditors about themselves (SCTs and certs)
- Between clients and servers about the server
- (sometimes) Between clients and auditors they explicitly trust with their confidential history



Certificate Transparency Activity



Certificate Transparency Gossip

Questions and concerns?

- HTTPS-only (client-server feedback unspecified for non-HTTP TLS services)
- Using well-known URLs
- Mixing policy for data from trusted Auditors?
- When should Auditors poll Servers vs. Servers send?

Feedback to the list, please!

https://tools.ietf.org/html/draft-linus-trans-gossip-ct-01