STI Certificate Transparency

draft-wendt-stir-certificate-transparency-01

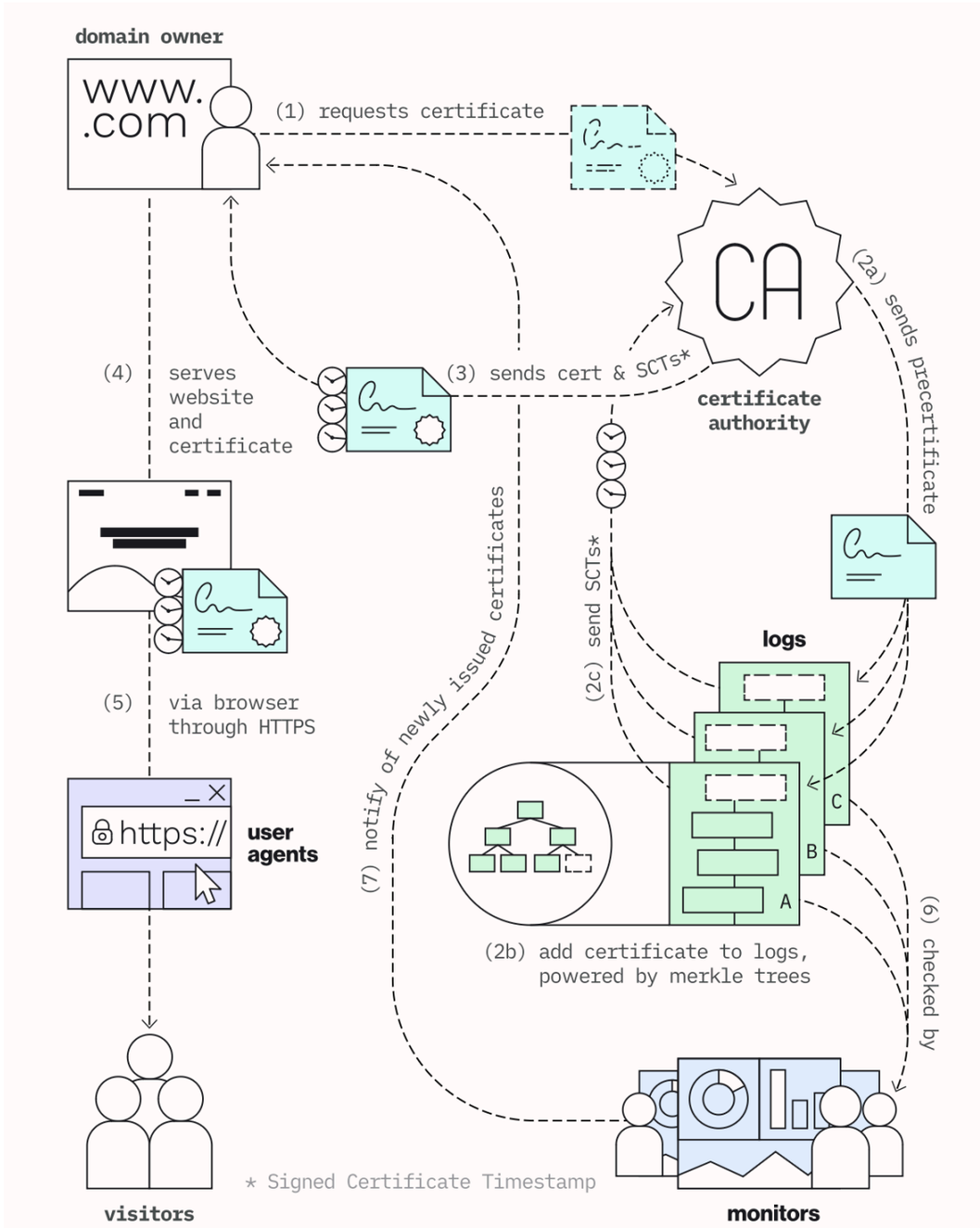
Chris Wendt, Somos
Rob Sliwa, Somos
Alec Fenichel, TransNexus
Vinit Anil Gaikwad, Twilio

STIR Working Group
IETF 118 - 03/18/2024

SOMOS®

Certificate Transparency Overview

- Widely used in web/TLS for protecting against domain certificate misissuance (e.g. bad CA spoofing google.com)
- RFC9162 is Certificate Transparency v2
- Consists of a set of logs and a set of monitors that are available in the ecosystem
- Monitors monitor logs for misissuance
- Uses merkle trees for append only and efficient verification characteristics of log
- Logs provide “receipts” signed certificate timestamps (SCT) that are attached to certificates and can be verified by recipient



SOMOS®

STI Certificate Transparency Overview

- Certificate Transparency (CT) is meant to be an extensible mechanism to be used to establish a level of trust about information, transactions, or events that can be cross verified by interested parties in a particular eco-system serving as a public auditing mechanism.
- This document is intended to extend CT to stir certs (RFC8226) and delegate certs (RFC9060) and could also be extended support other related trusted stir information via public auditing
- Telephone numbers (TNs) and their management and assignment by telephone service providers and Responsible Organizations (RespOrgs) for toll-free numbers share similarities to domains and the Domain Name System (DNS)
- There is a global uniqueness and established association of telephone numbers to jurisdiction and regulatory associations often based on country codes defined in ITU-T e.164 and related documents
- Note: The current version of this document is prescriptive of using one of the flavors of CT that embeds Transparency Information into the certificate itself.

SOMOS®

STI Certificate Transparency - Roles

- Submitters: Submission of certificates to logs for public auditing
  - If the log is accepted an Signed Certificate Timestamp (SCT) is provided as a “receipt” that should be embedded in the certificate
- Logs: A log is a single, append-only Merkle Tree of submitted certificate entries.
  - Logs are able to be queried by Monitors to check for any certificate misissuance that may occur for the scope interested by the Monitor (e.g. telephone number or SPC)
- Monitor: Monitors watch logs to check for correct behavior, for certificates of interest, or for both
  - They act on behalf of those that have interest in validating there is no misissuance or issuance of certificates from unexpected issuers
  - Any misissuance can be dealt with by the eco-system authorities and the CAs responsible.

SOMOS®

STI Certificate Transparency - Verification Service Role

- The goal of STI Certificate Transparency is that a verification service can receive a signed PASSporT using a certificate that contains a Transparency Information extension with the corresponding SCT
- If CT is supported consistently in the eco-system and with logging and monitoring being performed, the verification service can confidently trust that the telephone number or SPC being represented in the stir certificate given the signed SCT receipt.
- No additional queries or network transactions are required.
- TLS CT also support OSCP and other ways of delivering transparency information that could be considered but this was for pragmatic established eco-system reasons. To the extent possible delivery in the certificate is likely preferred simple path forward.

SOMOS®

STI Certificate Transparency

- Note there is many author notes in the current draft asking questions on how prescriptive we want to be for CT for STIR.
- This can be determined once we have a better handle on CT for STIR.
- Questions?

SOMOS®