Short-lived Certificates and Certificate Transparency

IETF 100, Singapore
TRANS WG
Diego Lopez, Antonio Pastor-Perales, Yaron Sheffer & Thomas Fossati
Problem Statement

• How to cope with the growing number of short-lived certificates?
  • Fast increase in log size that was not expected when CT was originally designed (estimates were for ~1M certificates/year)
  • Rough estimates of two orders of magnitude increase
  • Implications on log structure, implementation, rotation, monitoring, etc.

• Is this a real problem?
  • Al’s message on the TRANS list seems to suggest it might not be\(^1\)

A generic solution?

• Any ideas how to address this in the general case?

• Eran Messeri et al., “Certificate Transparency with Privacy”, PETS’17:
  
  [...] Instead of creating one log entry per certificate for short-lived certificates, a large number of potential short-lived certificates will be allotted one log entry. This log entry will have a special flag set to indicate that it corresponds to a family of short-lived certificates, and the validity period for the log entry will be comparable to that of a regular, long-lived certificate. The special log entry will also include the root of a Merkle tree of all the short-lived certificates affiliated with the entry. When visiting a site that uses short-lived certificates, auditors will receive a proof that the SCT for that site’s certificate is in the Merkle tree whose root appears in the corresponding log entry. [....]

• Any browser vendor and log implementer interested?
The STAR case

• What is STAR?
  • ACME extension to allow a name owner to obtain a string of short-lived certificates that are automatically renewed by the issuing CA
  • For the same key pair, that may be used by other entities than the name owner (delegation use cases)
  • The name owner controls the request of the string of short-lived certs
  • The name owner controls the lifetime of the renewal process, which can continue for as long as initially agreed, or be prematurely cancelled due to, e.g., a key compromise
  • STAR removes the dependency on the revocation infrastructure, while at the same time automating (and minimizing) the required interaction of name owners with their RA/CA
STAR and CT

• What makes STAR different from a generic short-lived certificate?
  • A STAR certificate can be thought of as a single “long-term” certificate that is made of a collection of same short-lived certificates that differ only for their (sliding) validity windows and serial number.
  • Therefore, it seems (at least theoretically) possible to treat all of them as a single entity from a CT log perspective? In the spirit of Eran’s email on the TRANS list
  1
    • Range of serial numbers
    • Dates associated with the whole string lifespan