State of Redaction

Why Redact?

- Secrecy has general consent of being worth discussing and possible to come to agreement on.
    - This addresses concerns of split-horizon DNS, delegation to private name servers, and similar issues.
    - draft-ietf-trans-rfc6962-bis-16, draft-strad-trans-redaction-00, and (more recently) “Precertificate Transformation Extension” focus primarily on this use-case.
- Privacy will be difficult to implement technologically while maintaining the base security principles/goals of the specification.
    - Privacy concerns focus around a potential legal requirement to remove data, such as PII or illegal content, from a log
    - If it’s easy in a given ecosystem to remove trust in a log, then logs can remove/replace nodes willy nilly in compliance with legal requirements and no further technological solution is needed.
    - If the technology is unable to support implementations which utilize easy-ish log rotation and agility, then we would need to discuss further in the WG.
        - We’d likely only find out about technological limitations of current draft(s) as implementers respond to real-world needs to address Privacy arise; none have arisen yet.
    - If discussed further, some have expressed that Privacy considerations would require logging “reason” leafs or implementing other “revocation”-like mechanisms. Yeah…

Redaction Requirements/Assumptions (Peter)

1. For all TLDs which consist of three or more letters, except for “mil”, “gov”, and “int”, and for certain two letter TLDs, the existence of a domain name consisting of the label immediately below plus the label that is the TLD is public information.

2. Logging certificates to a CT log is optional. An unlogged certificate may not be accepted by some clients or relying parties, but is not currently classified technically nor by policy as a mis-issued certificate.

3. Split horizon DNS exists, as does delegation to private name servers. This means that names that are unique in the global namespace might not be resolvable from the public Internet.

4. Given a full certificate, it *must* be possible to deterministically reconstruct the precertificate.

5. Given a precertificate and a full certificate, it should be possible to confirm the full certificate is the only viable/accurate match for the precertificate.

6. Given a precertificate and full certificate, it should not be possible to (re)construct other full certificates given only their precertificates.

7. The only entity that knows if a given certificate was *not* supposed to be issued with the certificate’s included SAN:dNSName values is the entity who was the domain registrant of the included SAN:dNSName values at the time of issuance.

8. The only way to get the content of a full certificate is to have a full certificate.
    a. An alternative or addition would be to have a way of authoritatively reconstructing the full certificate from only the precertificate.

Brief History of Redaction

draft-ietf-trans-rfc6962-bis-01

- Introduces redaction on April 16, 2014
- Includes “Redacting Domain Name Labels in Precertificates” and “Using a Name-Constrained Intermediate CA”

draft-ietf-trans-rfc6962-bis-16

- Various updates to redaction mechanisms; published on May 27, 2016
- Includes “Redacting Labels in Precertificates” and “Using a Name-Constrained Intermediate CA”
- Includes a “Redacted Labels” extension, allowing TLS clients to reconstruct the TBSCertificate component of the precertificate from the full certificate
- Requires a fair bit of work from TLS clients to implement
- Multiple full certificates could be associated to a single precertificate

Active Proposals and Discussions

draft-ietf-trans-rfc6962-bis-17 -> draft-strad-trans-redaction-00

- Further updates redaction mechanisms on July 21, 2016
- Forked into draft-strad-trans-redaction-00/01 on January 17, 2017
- Includes “Using a Name-Constrained Intermediate CA” and “Redacting Labels in Precertificates”
- Moves to using a “redactedSubjectAltName” extension (in full certificate and precertificates)
- Reduces complexity for TLS clients to reconstruct full certificates

Private Subdomains in CT

- Proposal/discussion from Saba Eskandarian, Eran Messeri, Joe Bonneau, and Dan Boneh on March 8, 2017
- Outlines threat model which redaction addresses
- Domain owner supplies input for inclusion in certificate and SCT
- Low-ish complexity for TLS clients to verify proof

Precertificate Transformation Extension

- Proposal/discussion from Tarah Wheeler and Peter Bowen on March 22, 2017
- Somewhat similar to draft-ietf-trans-rfc6962-bis-16, but provides for unique association between precertificate and full certificate
- Uses “precertificateTransformation” extension
- Adds support for SAN:iPAddress in addition to SAN:dNSName values
- Necessitates significant complexity for TLS clients to implement full certificate reconstructions