SECDISPATCH
@IETF123

Merkle Tree Certificates

draft-davidben-tls-merkle-tree-certs

David Benjamin (Google), Devon O'Brien, Bas Westerbaan (Cloudflare),
Luke Valenta (Cloudflare), Filippo Valsorda (Geomys)

Motivation

Problem: Certificate-Transparency-based PKIs are getting larger

Post-quantum signature algorithms are *big*

- 64 byte ⇒ 1,312 byte pubkey and 64 byte ⇒ 2,420 byte sig (P-256 ⇒ ML-DSA-44)
- Certificate Transparency log entries get larger
- TLS handshake gets larger (sigs from CA *and* logs)
- ML-KEM transition was just the *start* of post-quantum

Certificate lifetimes getting shorter

- Issuance volume goes up
- Certificate Transparency logs have more entries

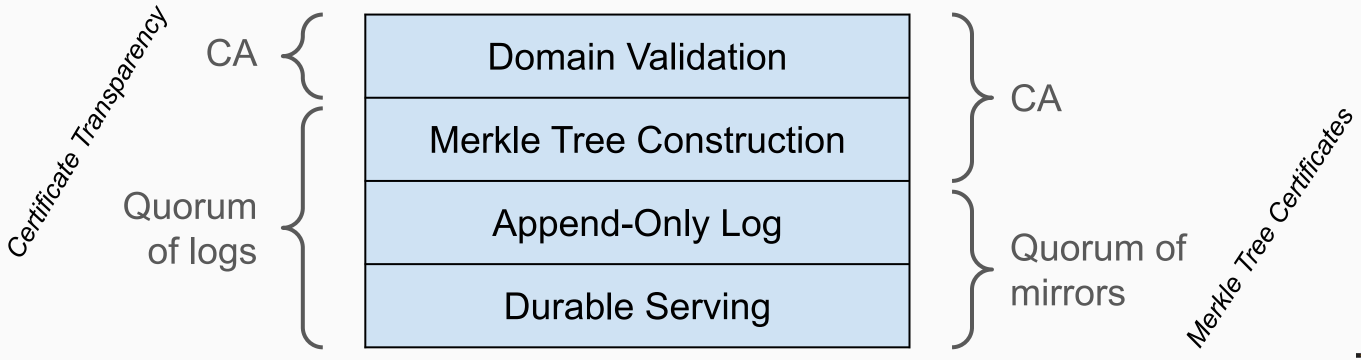
Opportunity: We have to do a transition for post-quantum anyway

Merkle Tree Certificates

A.k.a. “Photosynthesis” — turn sunlight* into certificates

https://datatracker.ietf.org/doc/draft-davidben-tls-merkle-tree-certs/
https://github.com/davidben/merkle-tree-certs

Integrate transparency instead afterthought: move tree construction to CA



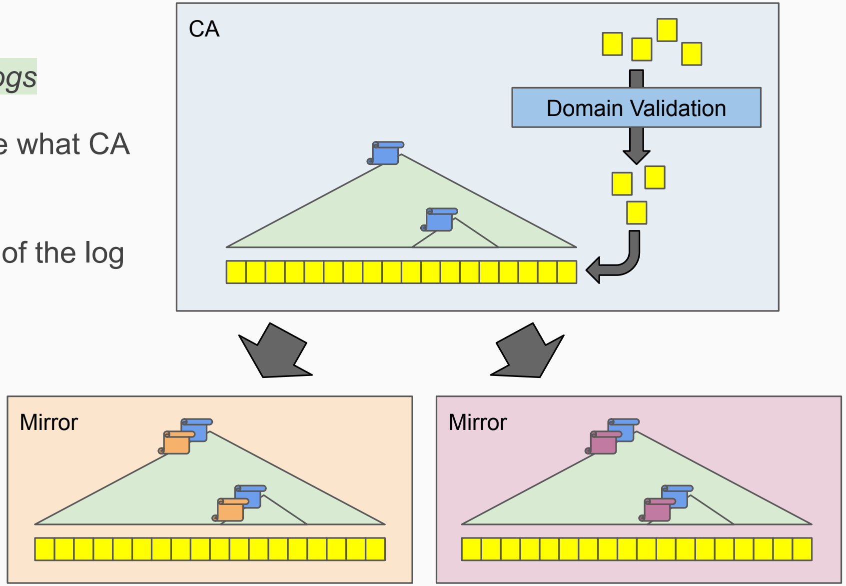
* RFC 6962 was once draft-laurie-pki-sunlight, more recently https://sunlight.dev/

Overview

CAs run *issuance logs*

Log entries describe what CA has issued

CAs (co)sign views of the log



Mirrors mirror contents and cosign views

Size Savings

Log entries have no signatures, can hash public keys down

Mirror contents are identical ⇒ monitors don't download duplicates

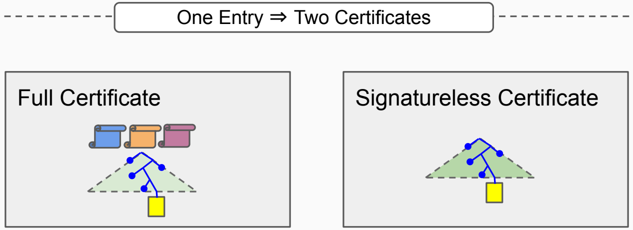
Tree pruning (see draft)

Signatureless certificates available as optional certificate size optimization

Package up as X.509 certificate:

TBSCertificate ⇔ entry

Signature ⇔ inclusion proof + cosignatures

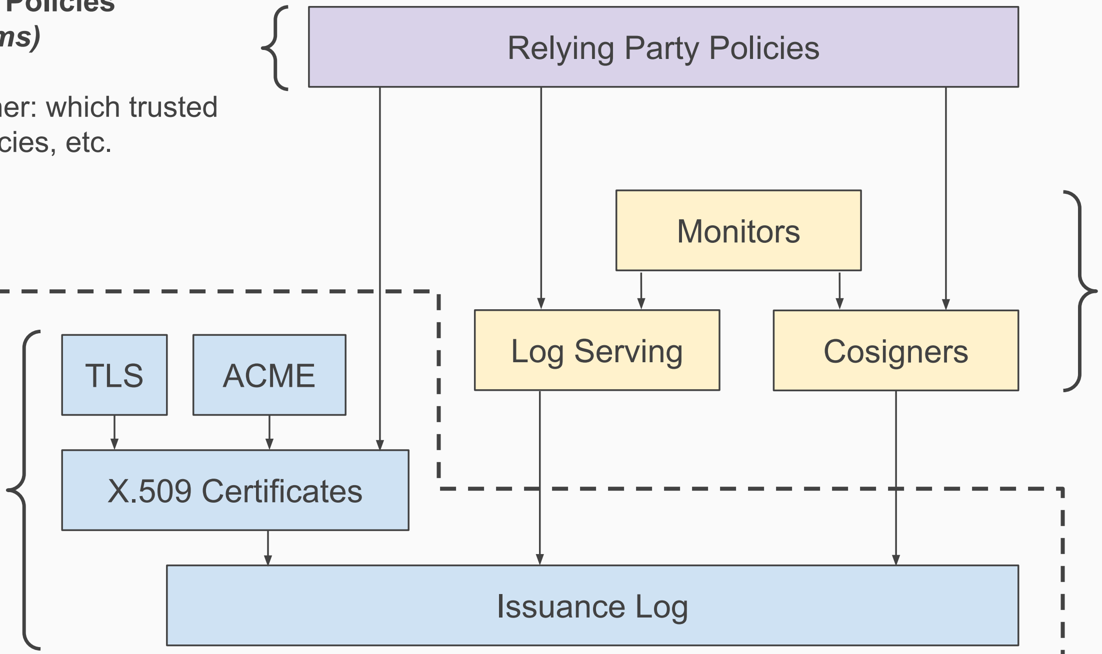


Cosignatures can be omitted with up-to-date relying parties

Components and Scope

Relying Party Policies
(Root Programs)

Put it all together: which trusted cosigners, policies, etc.



Certificate Construction
(This Draft)

X.509 certificate profile

Issuance log structure

TLS, ACME integration

Transparency Ecosystem
(C2SP, etc.)

Log serving protocols

Cosigner roles and protocols

Running code: Static CT and Tiled Transparency Logs

Dispatching

Center of *this draft* is the X.509 encoding ⇒ LAMPS?

Center of overall system is the issuance log ⇒ broader scope?

Experience from CT: Transparency ecosystem details *do not impact interop* for X.509, TLS clients, TLS servers ⇒ prescribing this currently not in scope for draft

Feedback welcome on lists or at https://github.com/davidben/merkle-tree-certs