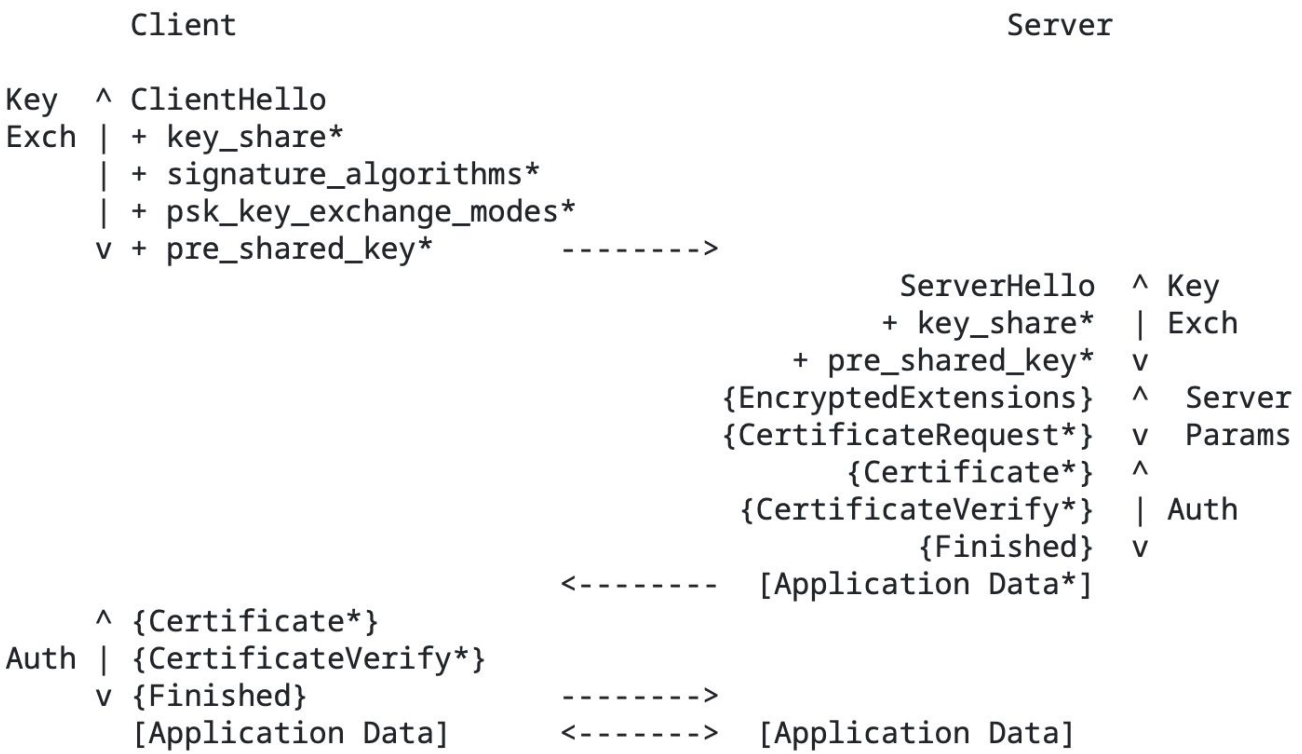
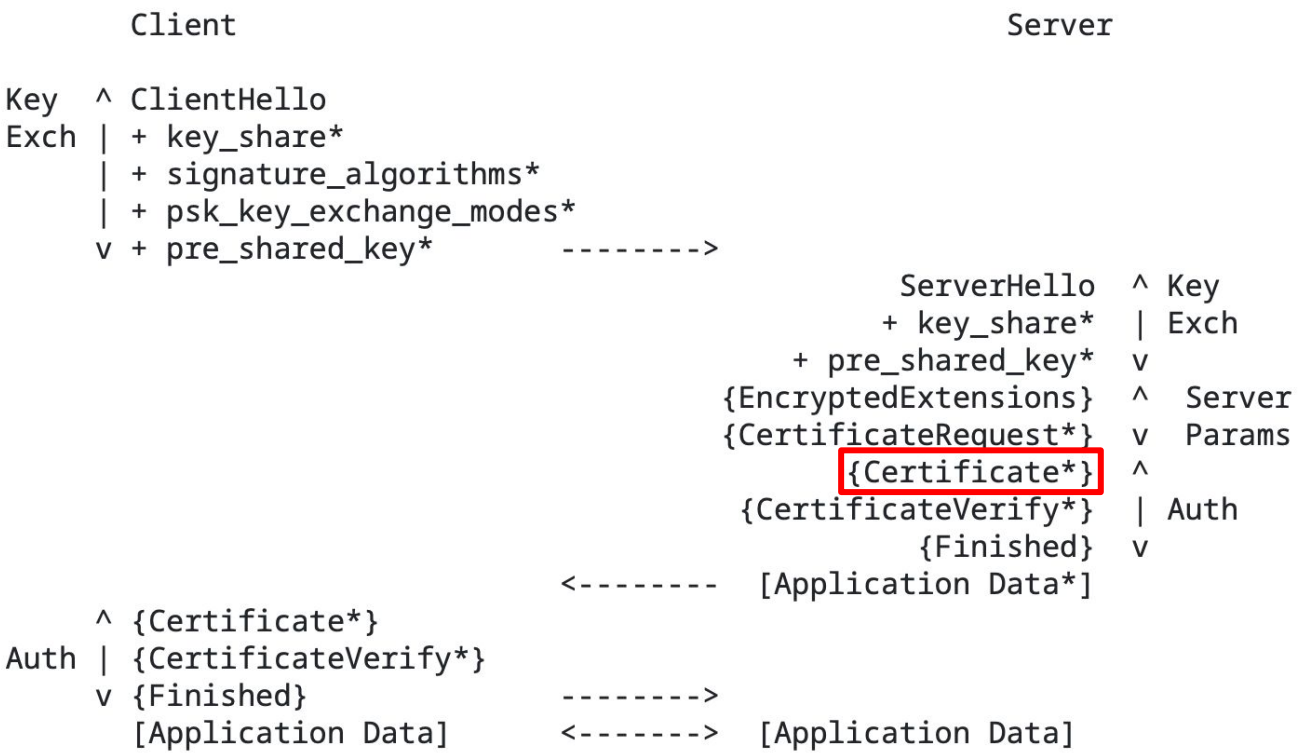
TLS Trust Tussle

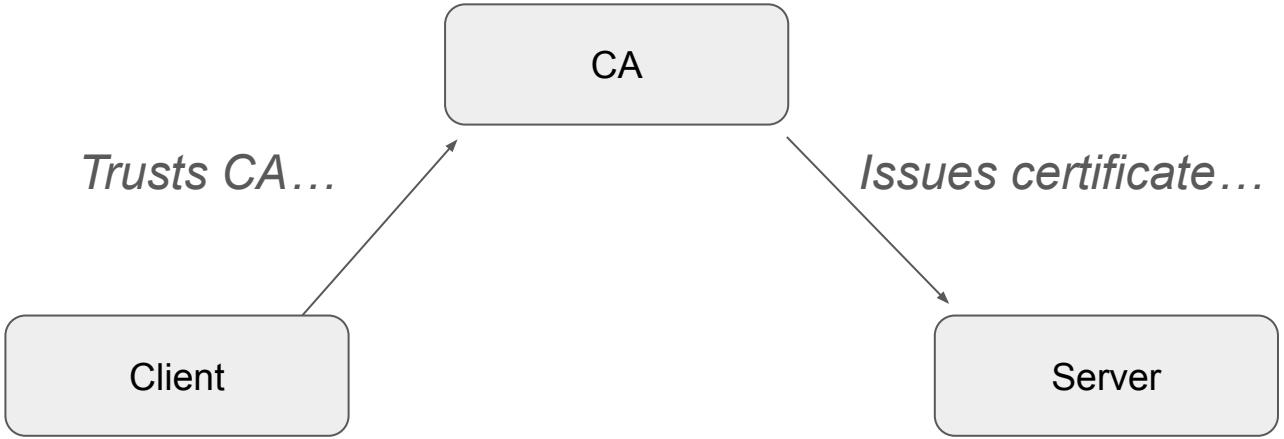
Establishing trust



Establishing trust



Establishing trust



Primary Goals

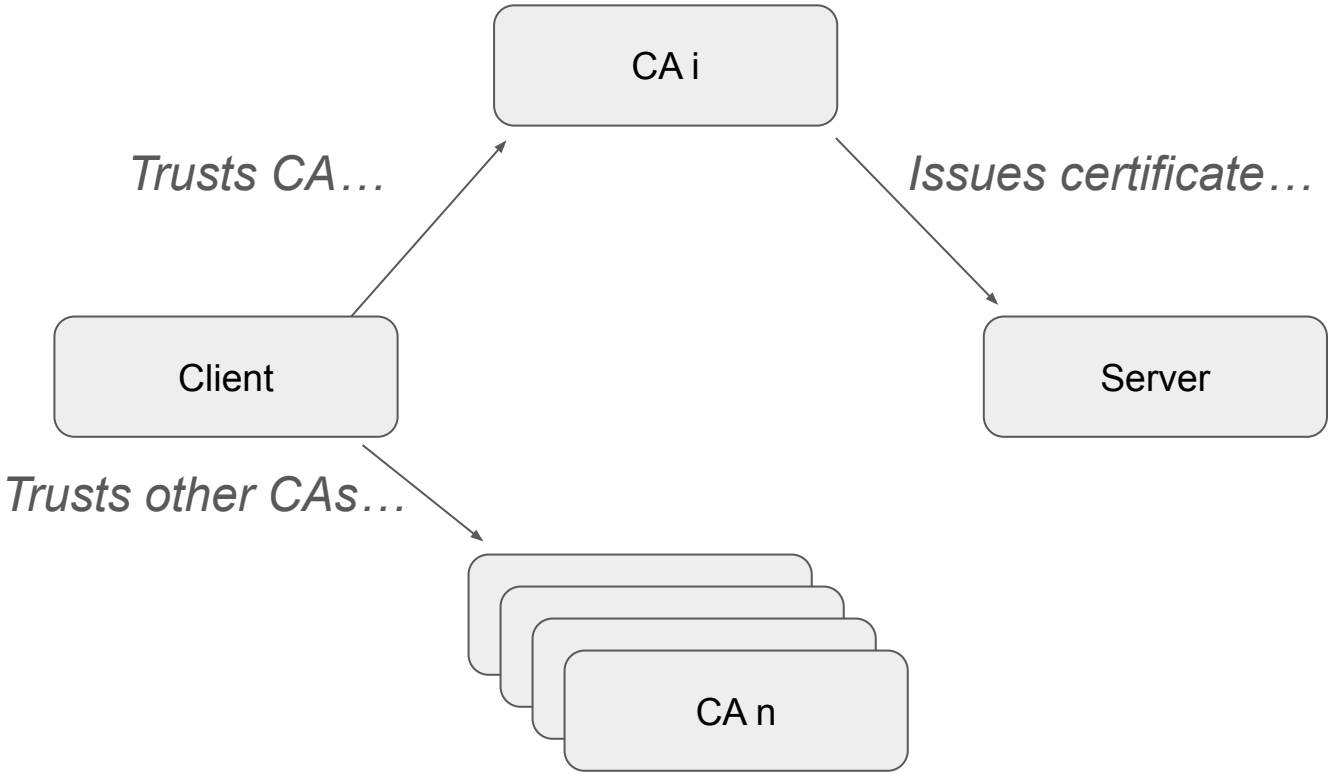
Availability

Servers should be able to provide service for all their clients

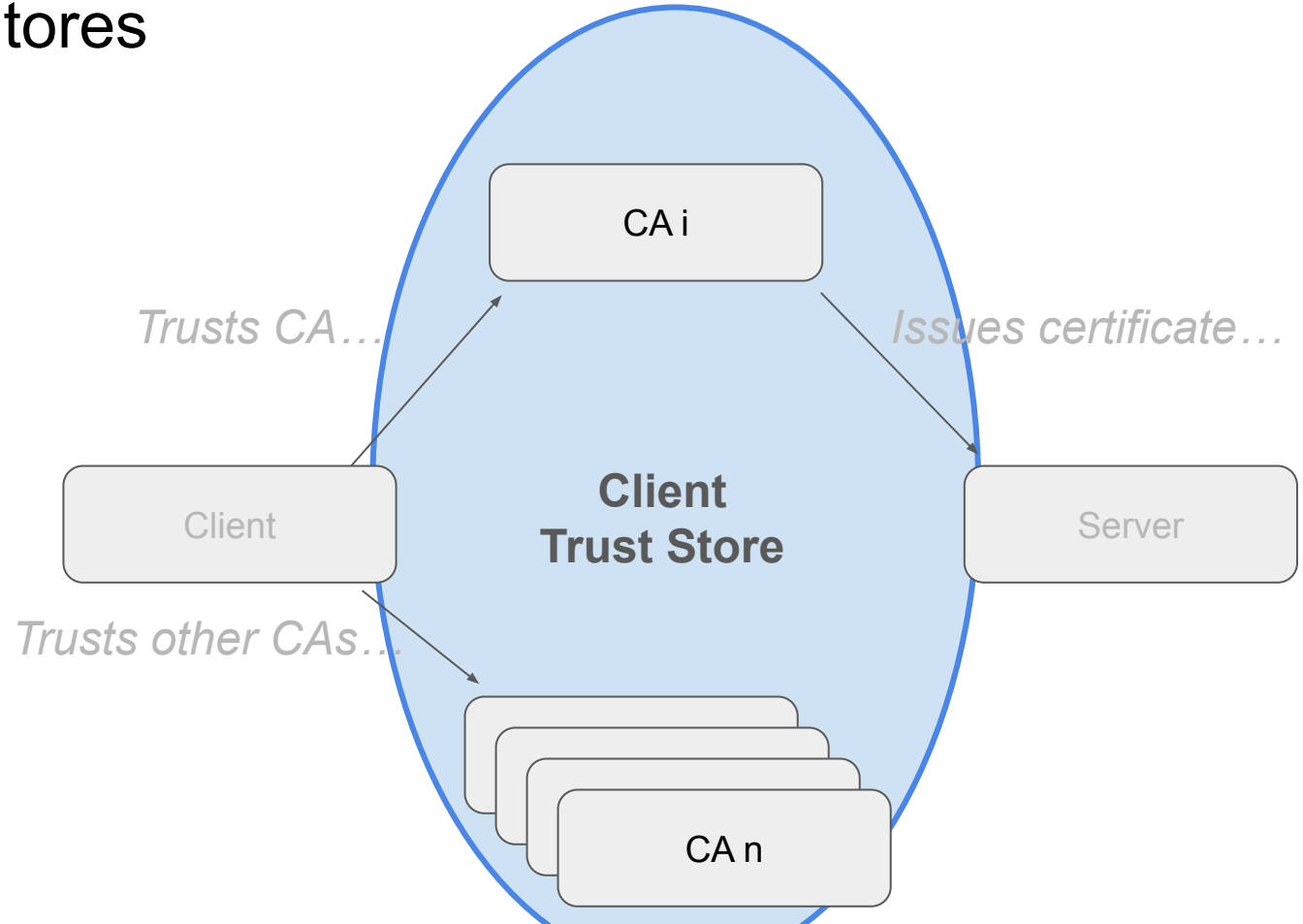
Security

Clients should only trust legitimately issued certificates, not attacker controlled certificates (and keys) → Clients should not trust *untrustworthy* CAs

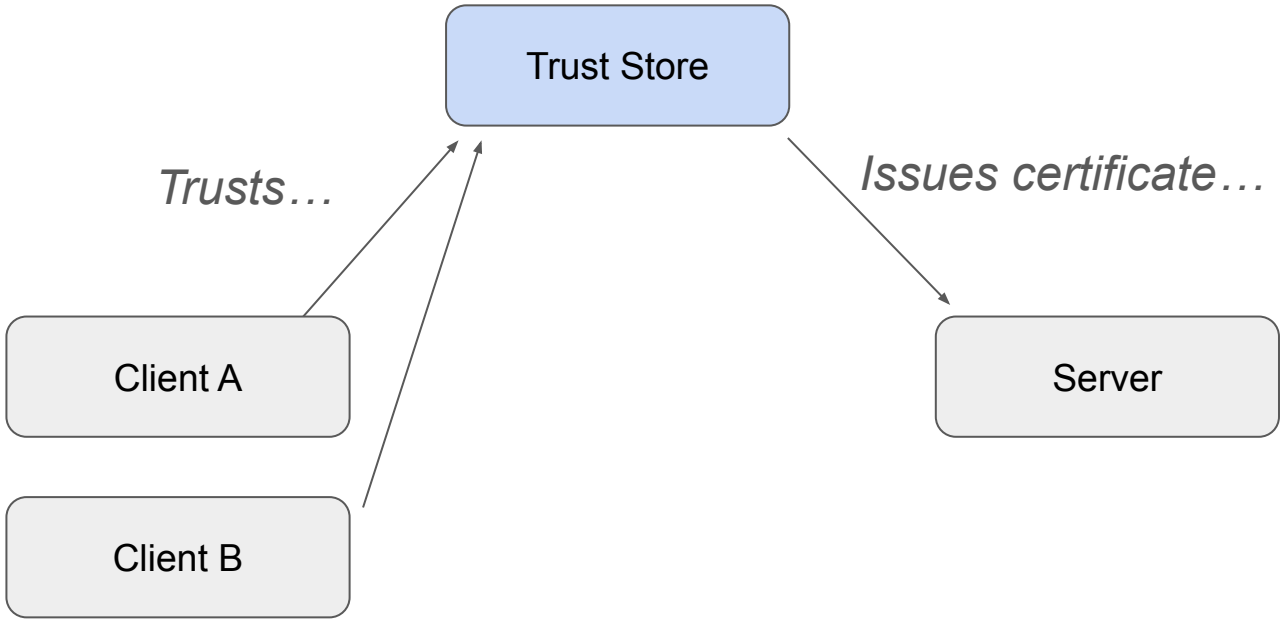
Trust Stores



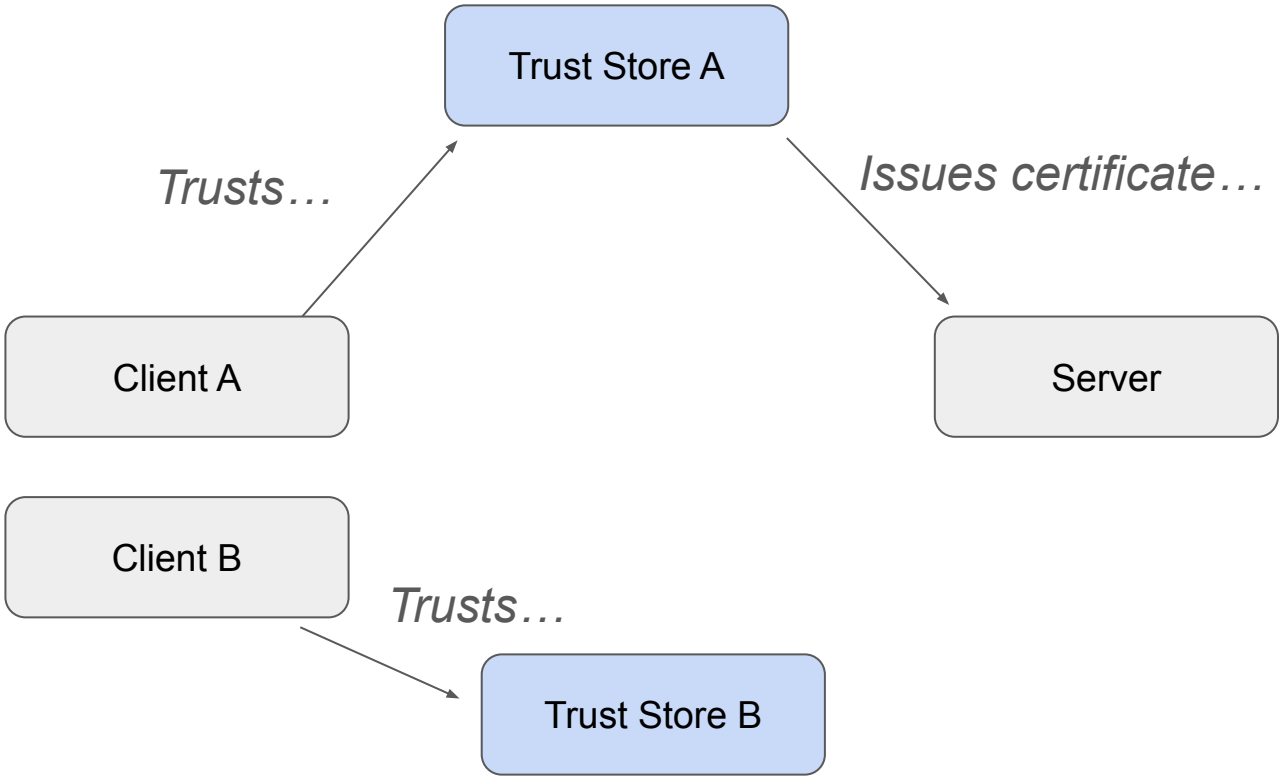
Trust Stores



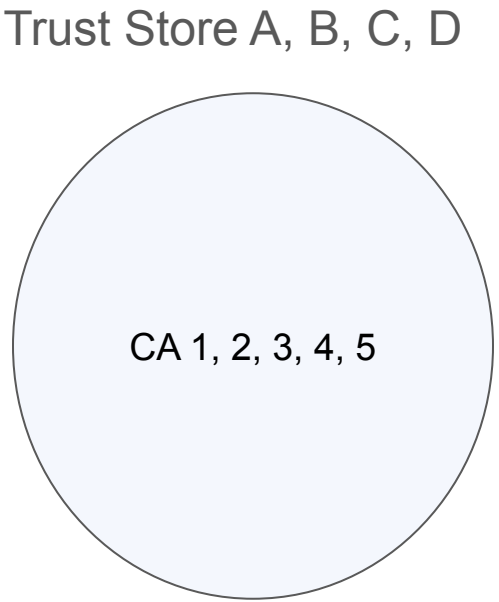
Ideally…


Trust Store
Trusts…
Issues certificate…
Client A
Client B
Server

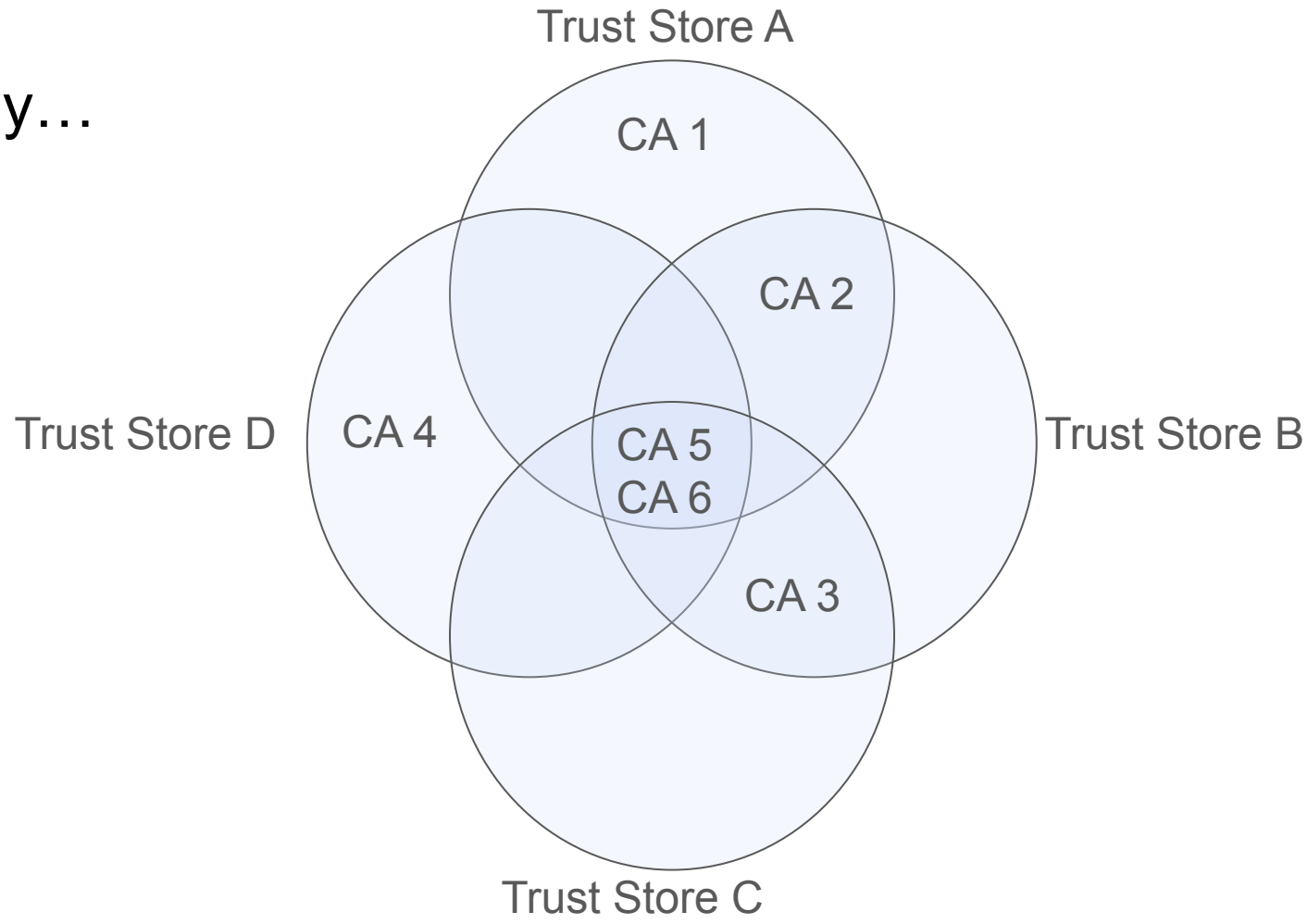
Ideally…


Trust Store A
Trusts…
Issues certificate…
Client A
Server
Client B
Trusts…
Trust Store B

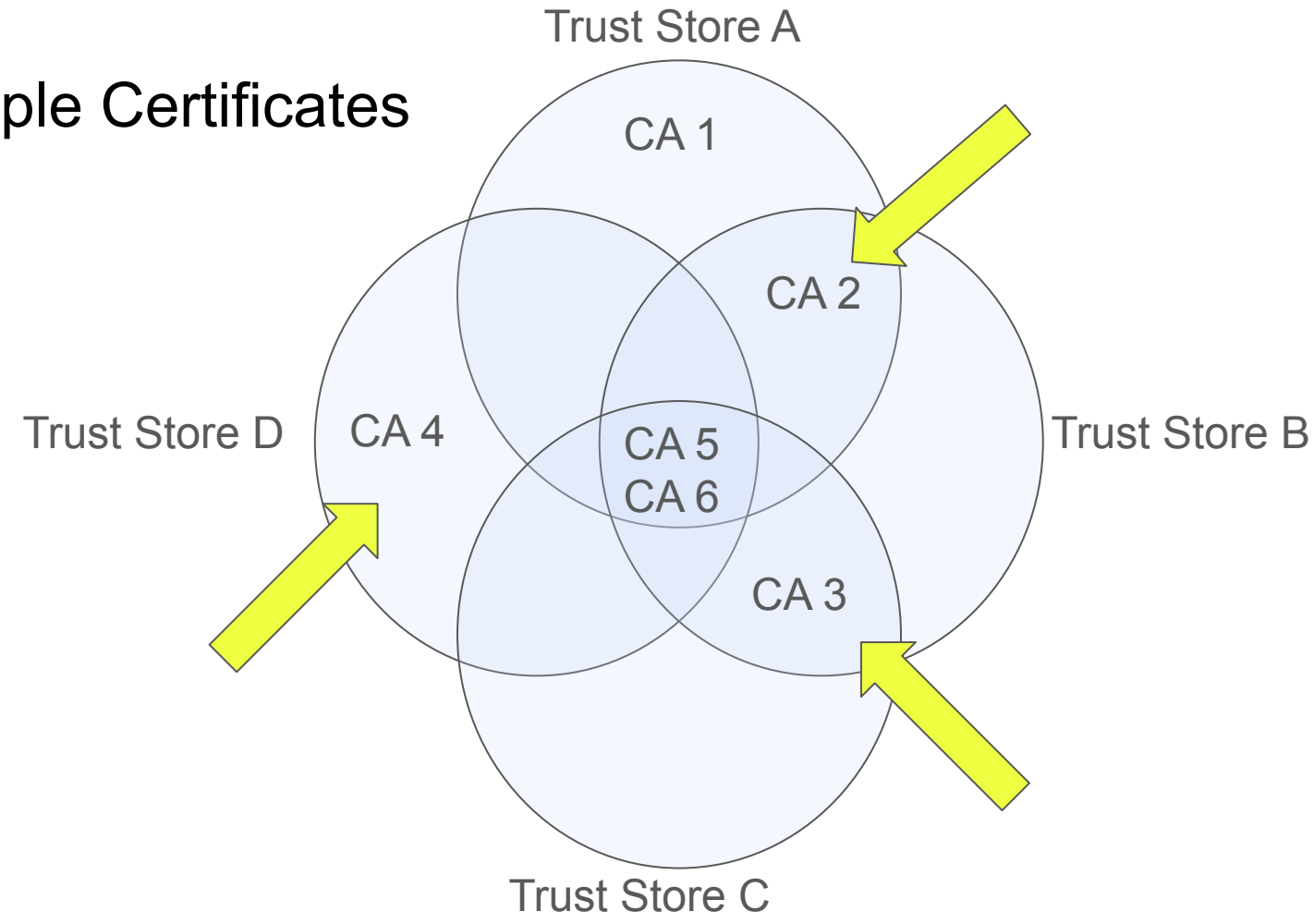
Ideally…



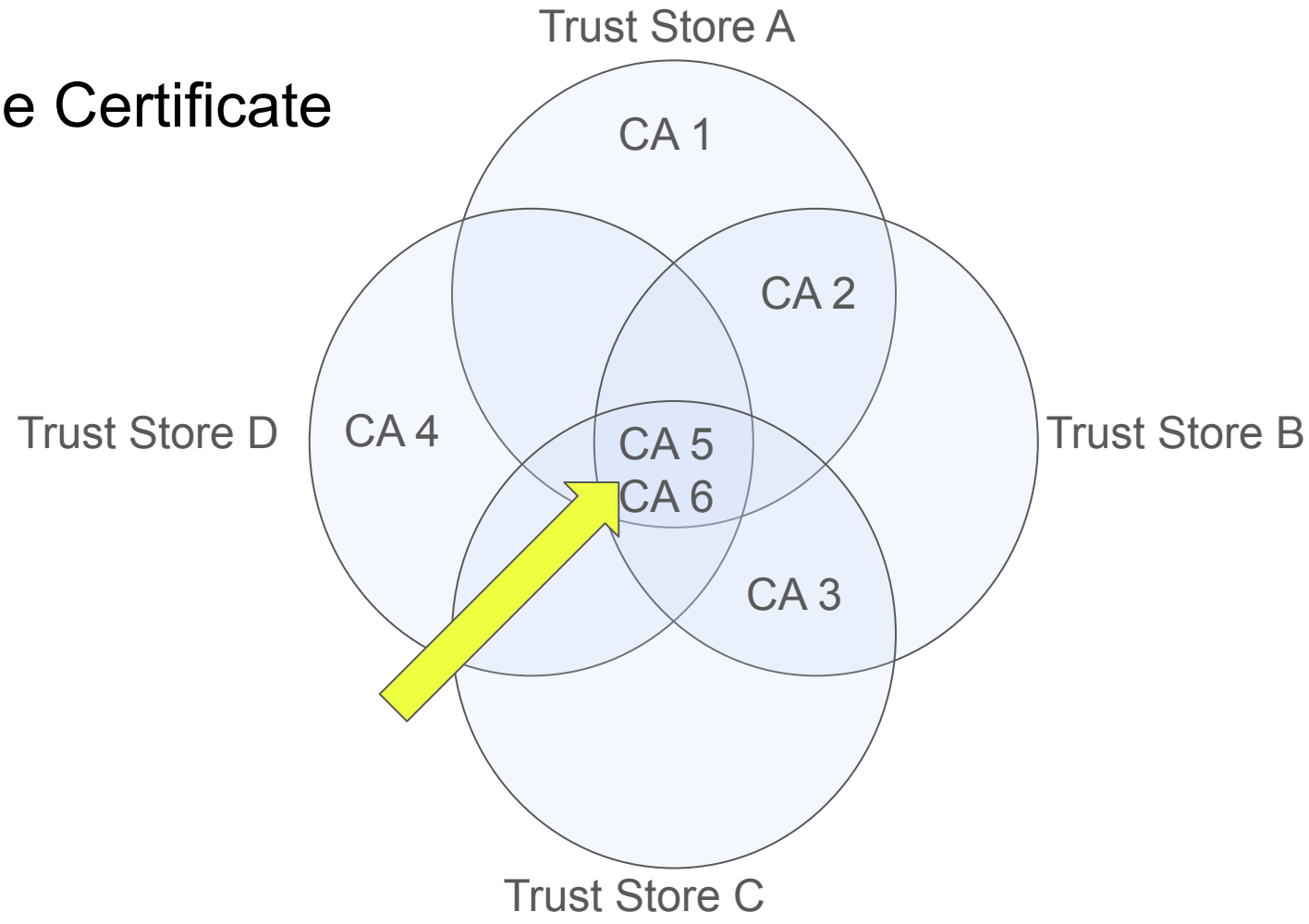
Really…


Trust Store A
CA 1
CA 2
Trust Store D
CA 4
CA 5
CA 6
Trust Store B
CA 3
Trust Store C

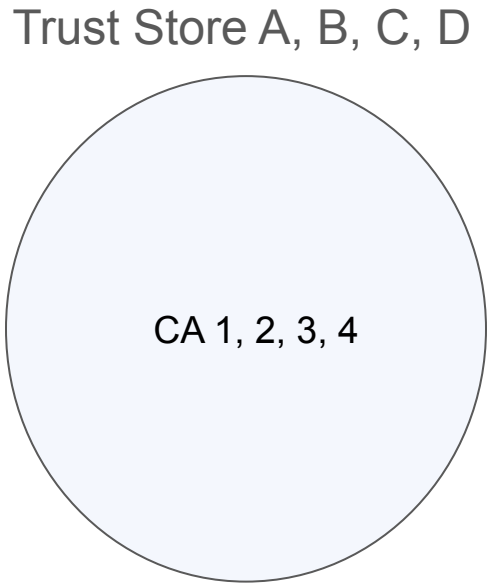
Multiple Certificates



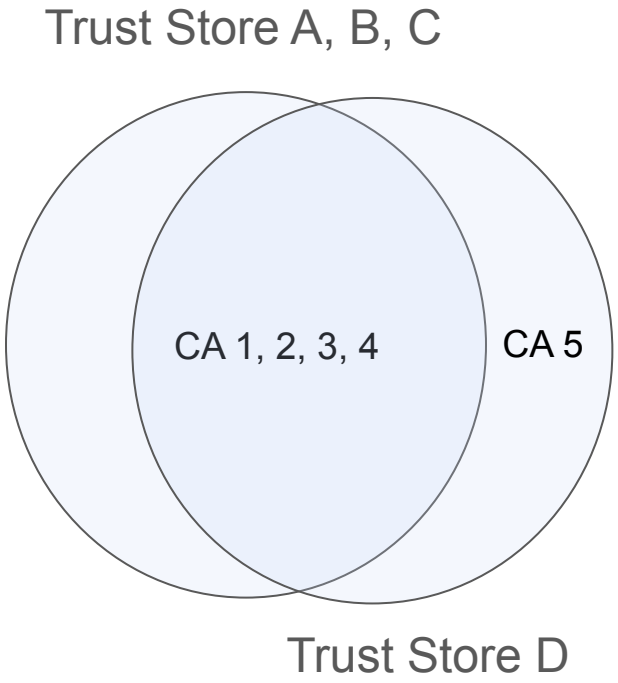
Single Certificate



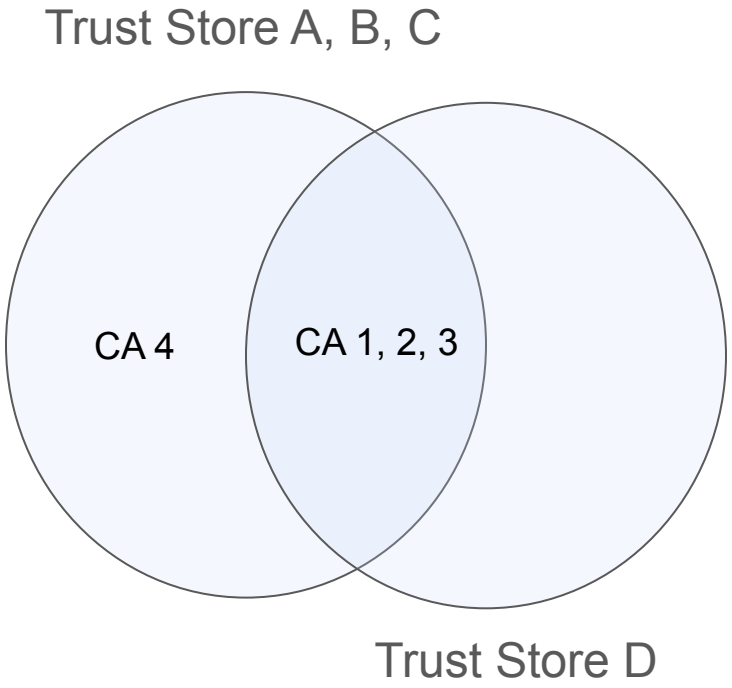
Pressures for Trust Store Divergence



Forces of Trust Store Divergence
CA addition



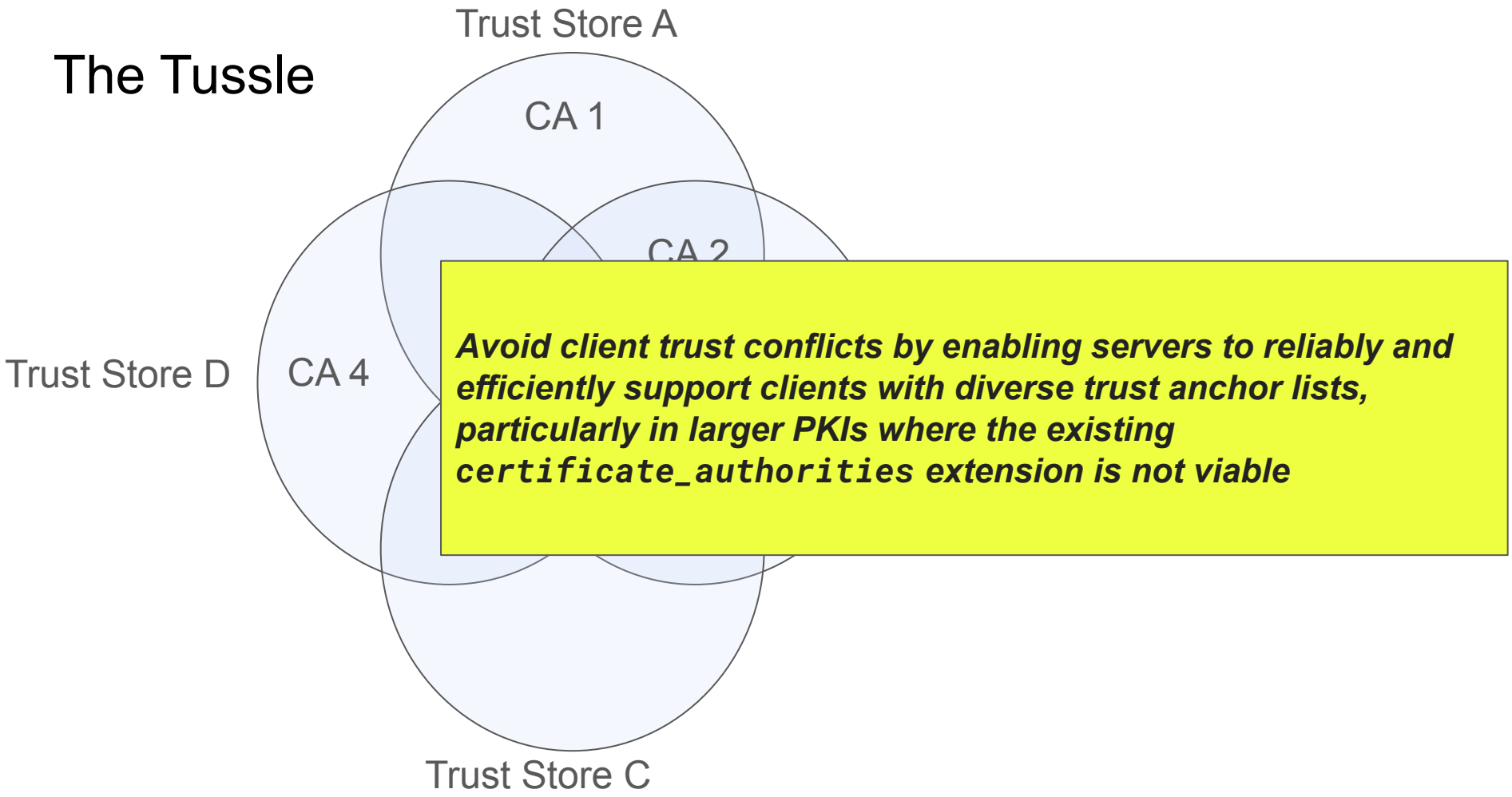
Forces of Trust Store Divergence
CA removal



Diversity Pressures

- Clients are empowered to make update decisions independently
  - Differing requirements, e.g., CT inclusion and deployment constraints
- Clients may make more restrictive trust decisions
  - In practice, this sometimes manifests as pinning
- Client deployments deliver updates at different rates

The Tussle



Avoid client trust conflicts by enabling servers to reliably and efficiently support clients with diverse trust anchor lists, particularly in larger PKIs where the existing `certificate_authorities` extension is not viable

Considerations

- Is the extent and duration of divergence not actually a widely accepted pain in practice?
- Are forces of change (divergence) so few and far between, that the current distribution of operational pain seems like the best outcome?
- Do we really only care about solving the PQ PKI problem, rather than generalizing to address types of change?
- What are the possible downstream effects of solving this tussle?