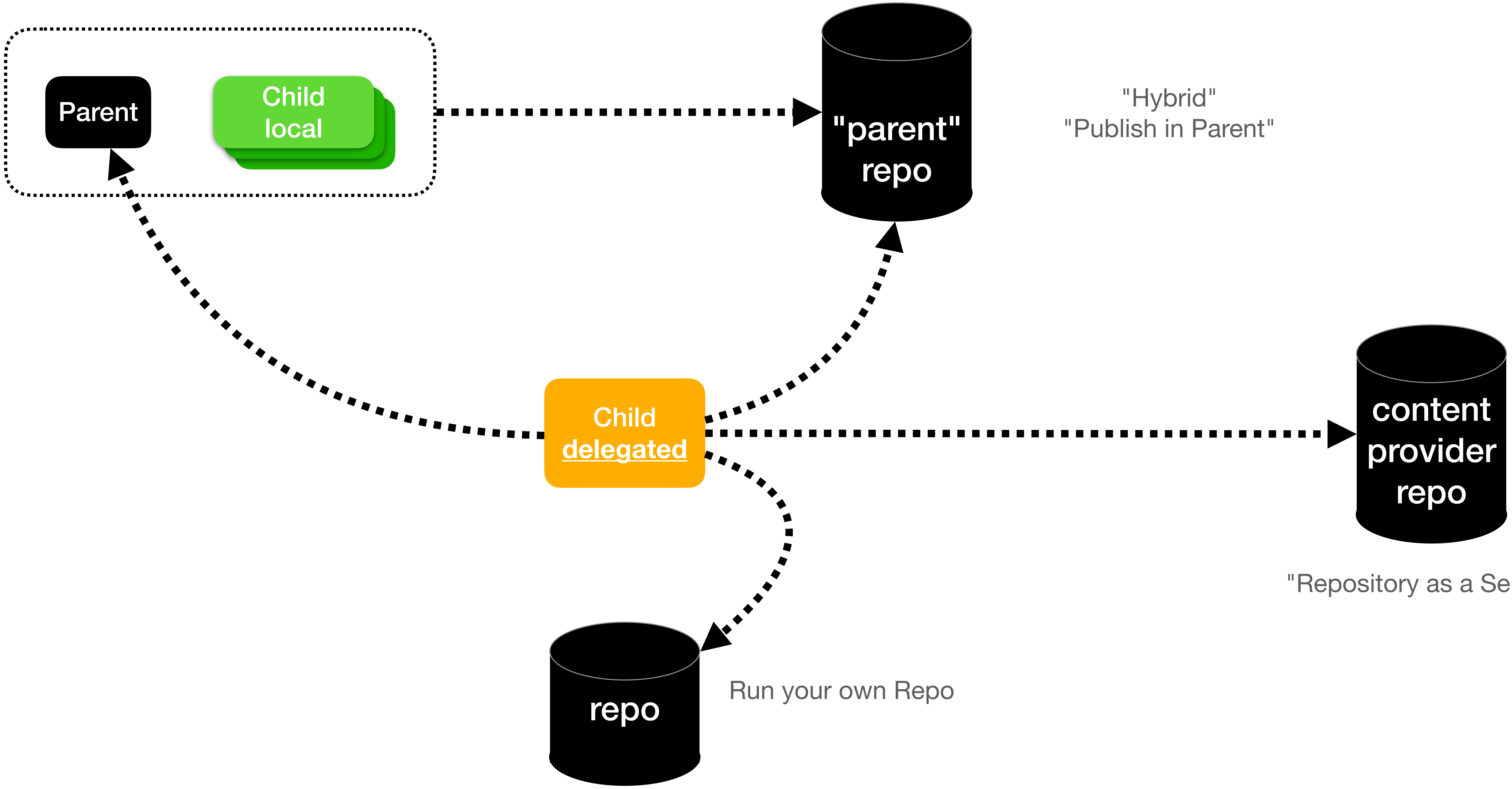
Delegated CAs and Repositories

a short story about migrations

Hosted RPKI Service vs Delegated



Parent

Child local

"parent" repo

"Hybrid"
"Publish in Parent"

Child **delegated**

content provider repo

"Repository as a Service"

repo

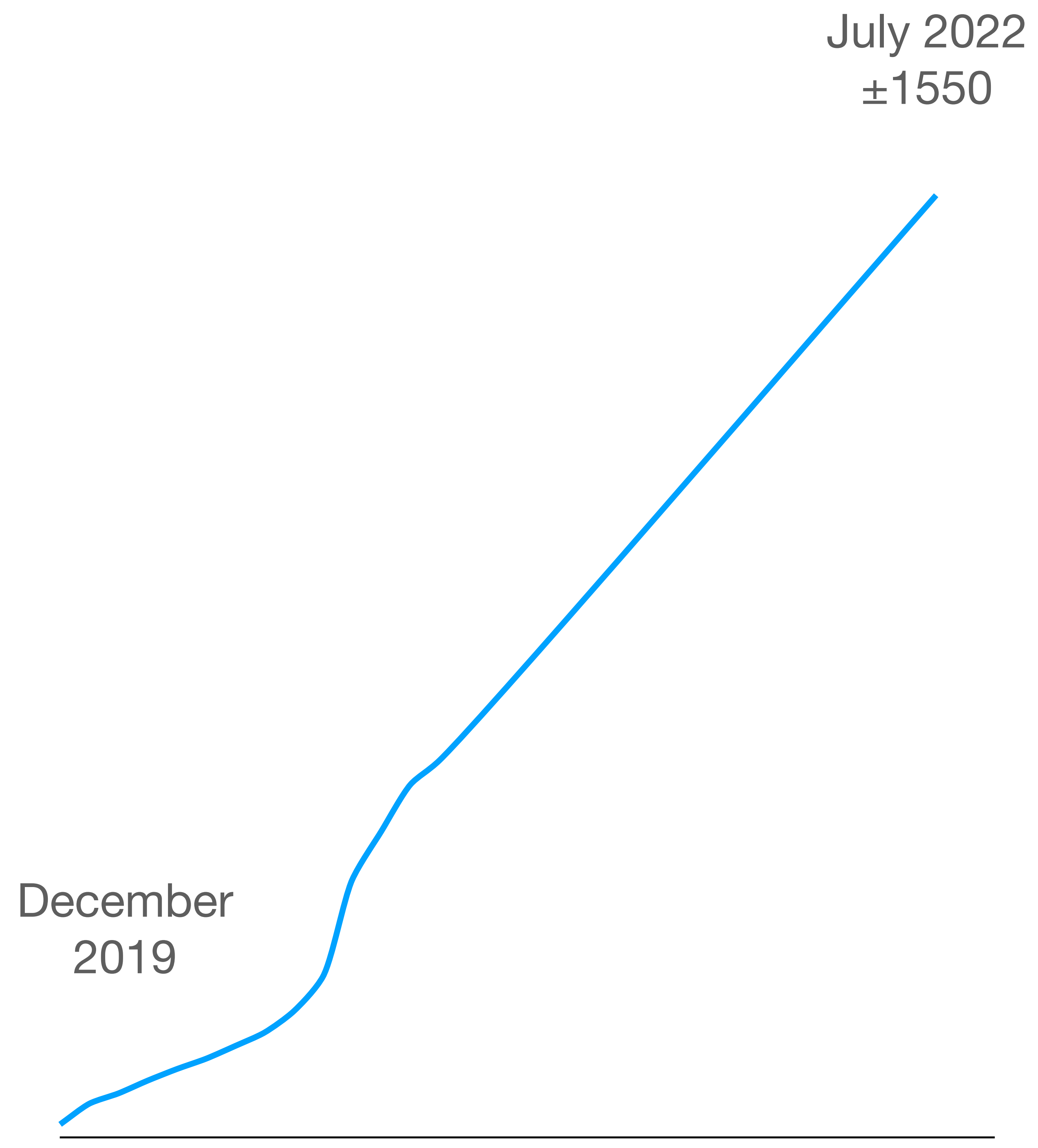
Run your own Repo

Repository as a Service

- Huge enabler for running delegated

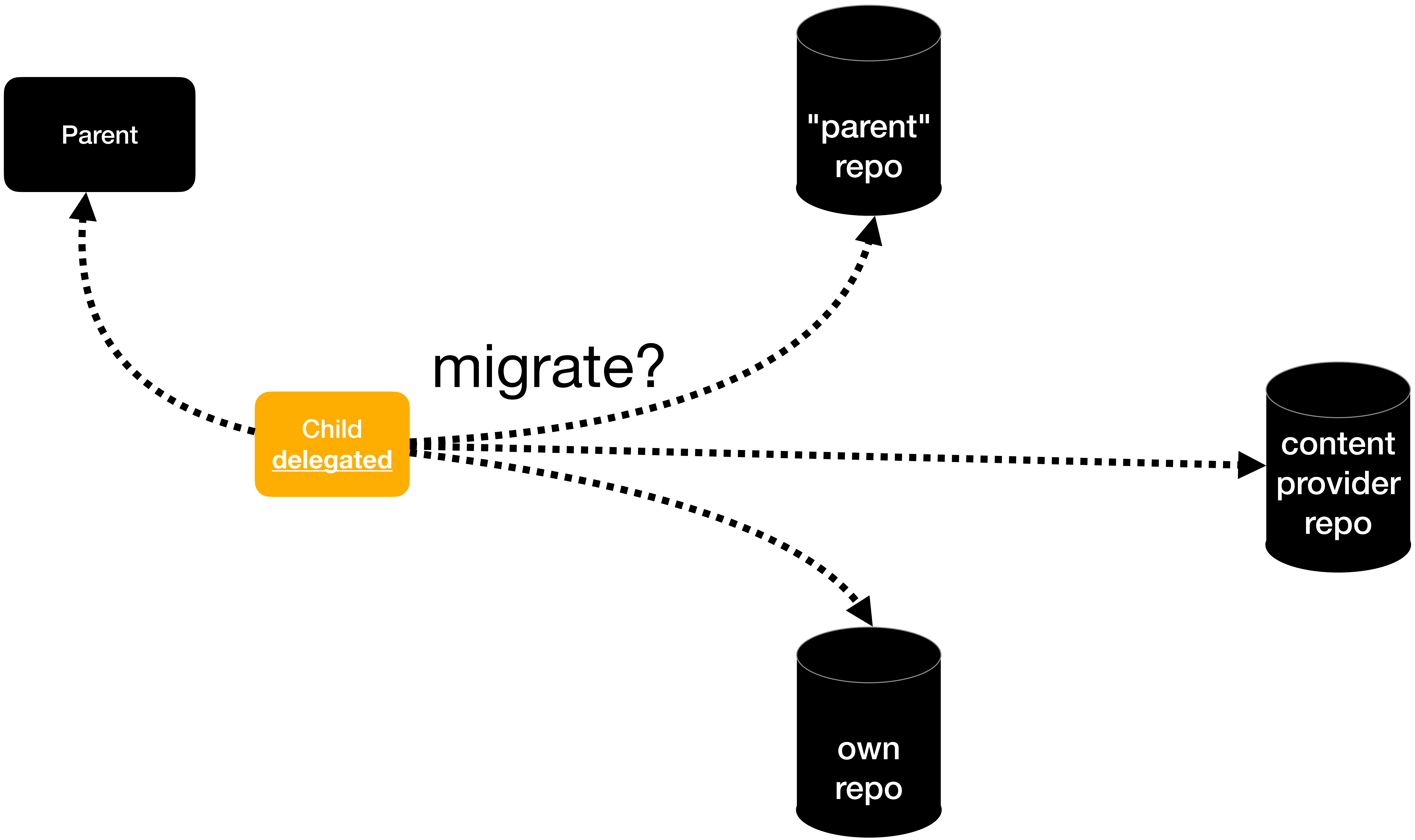
- Can run a simple CA behind firewall
- No need for public facing HTTPs
- No need for public facing rsyncd
- Uptime CA is much more forgiving

  (republish before MFT/CRL expire)

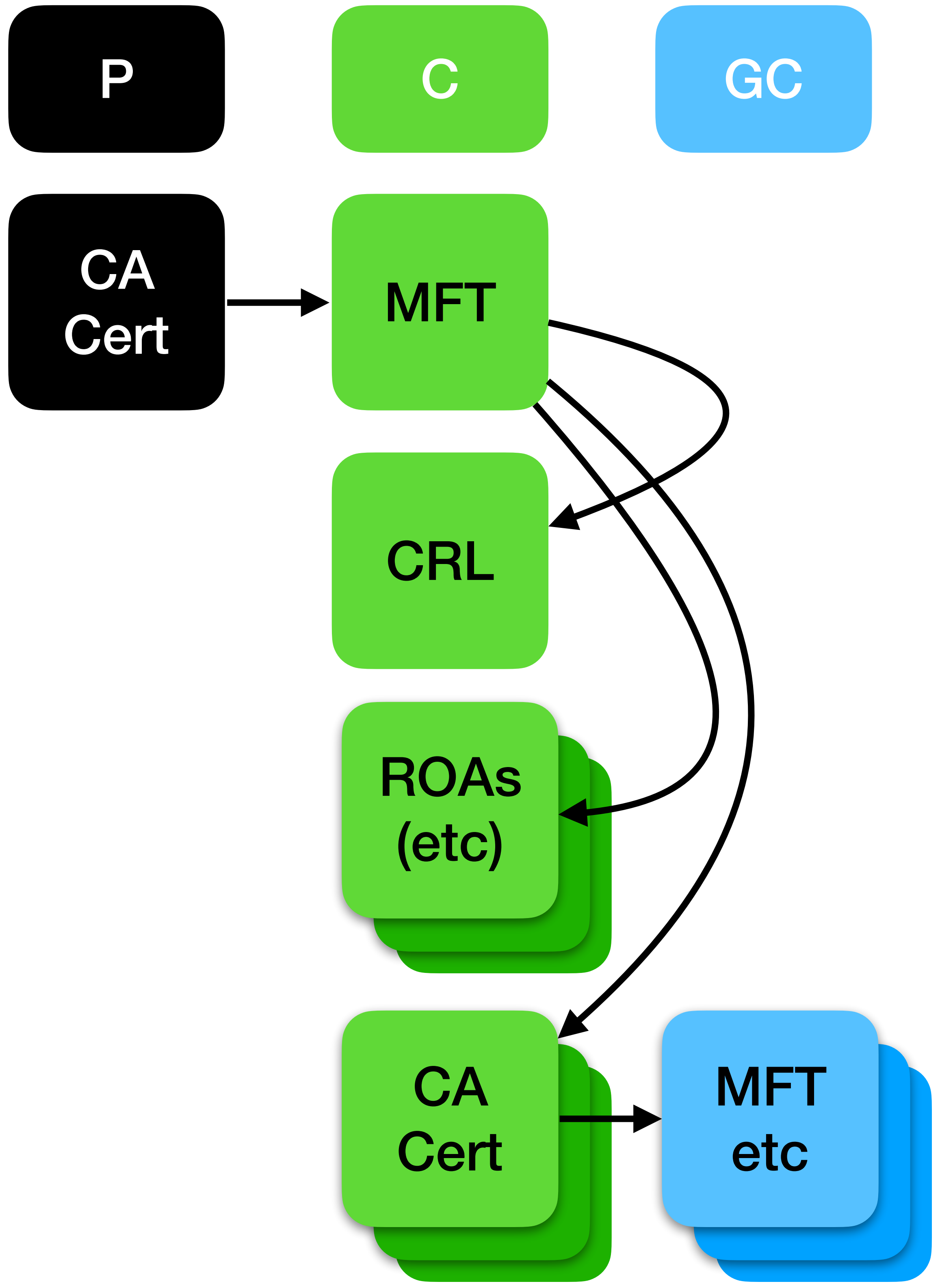


Delegated CAs in Brasil over Time

Migrating Repository



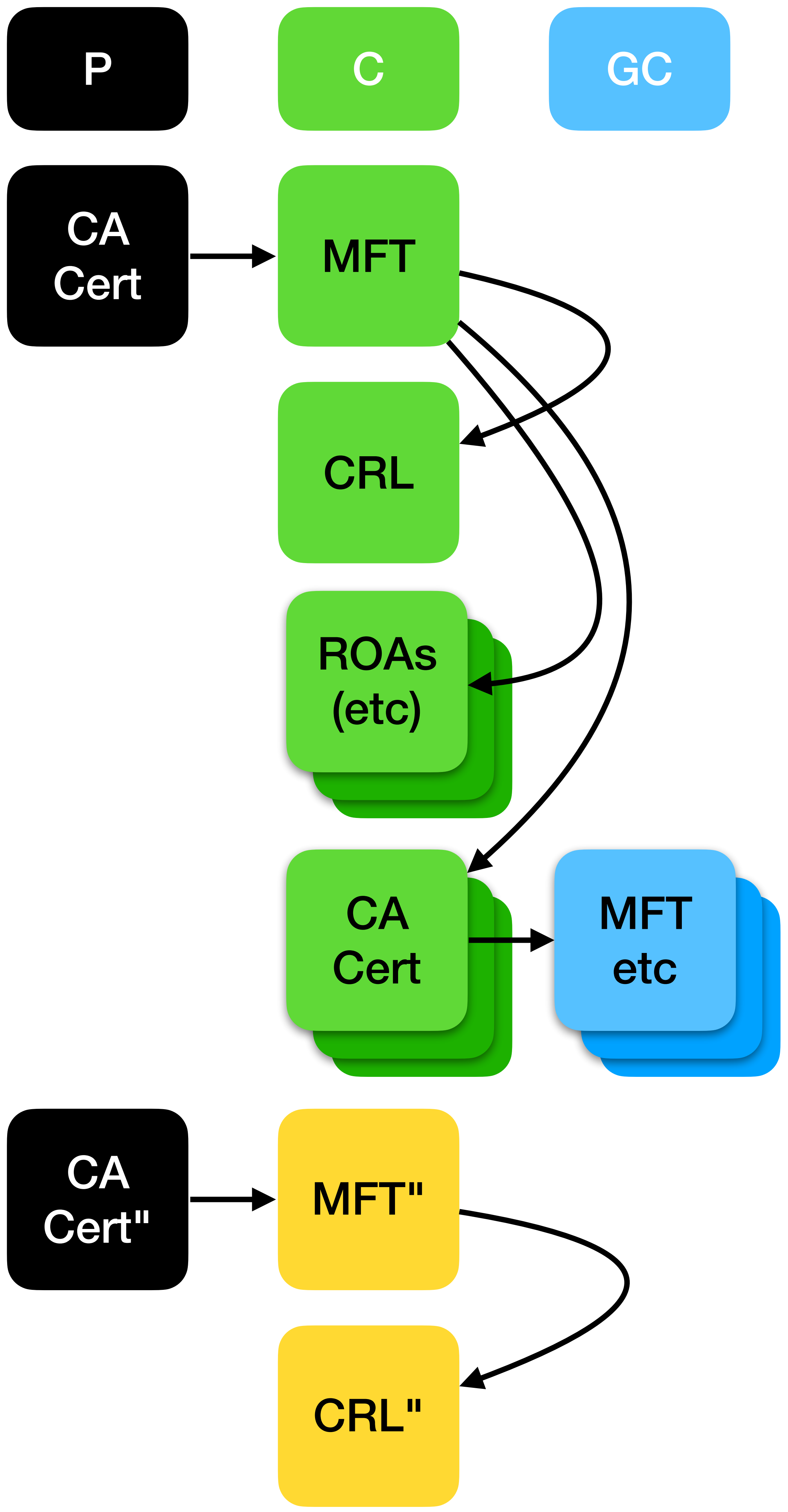
Normal Key Rollover (RFC 6489)



Phase 0: Before key rollover

- Child (C) gets CA certificate from Parent (P)
- Child issues manifest, CRL, signed objects
- Child issued delegated CA certificates to grandchildren (GC)

Normal Key Rollover (RFC 6489)

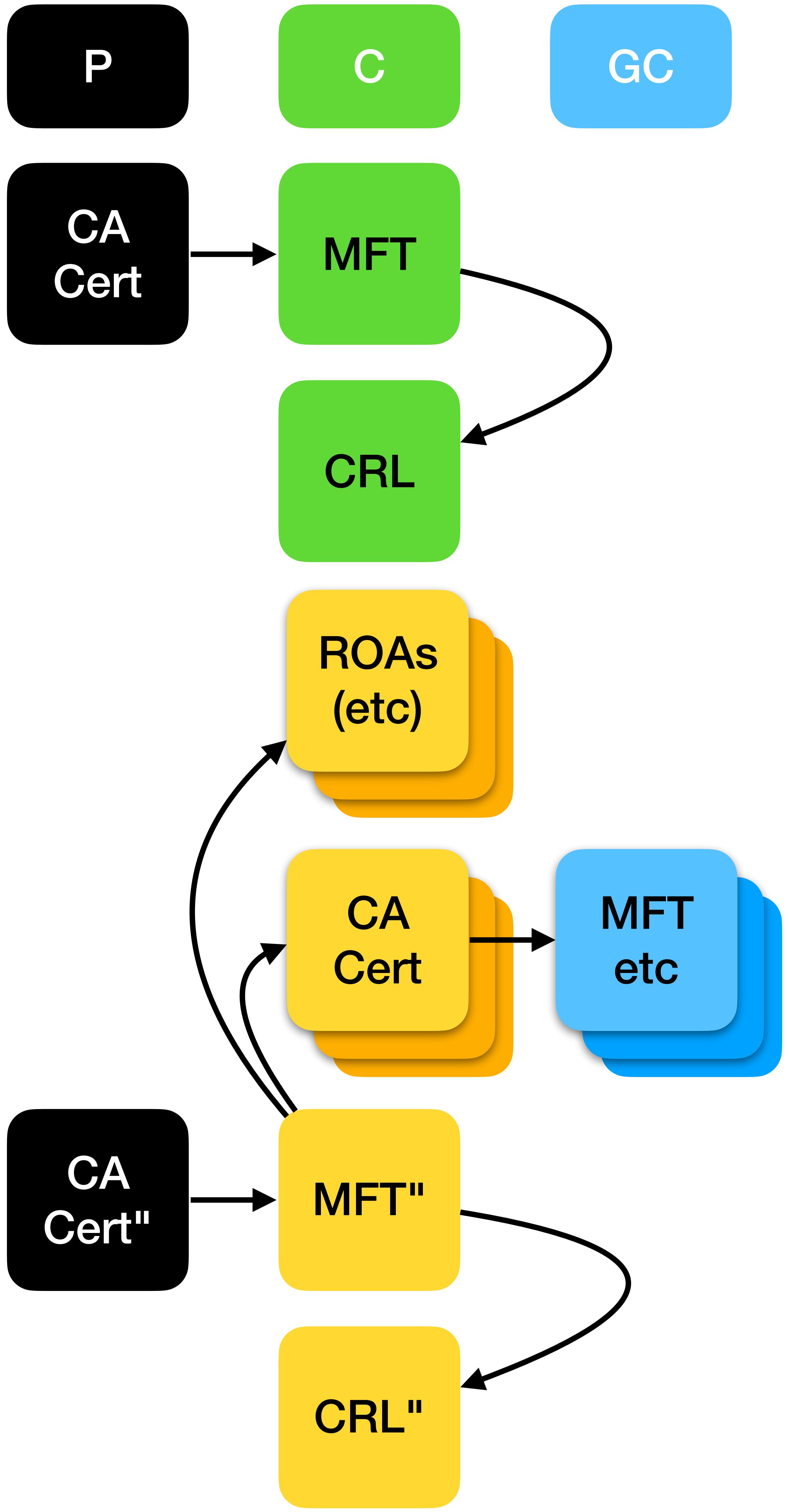


Phase 1: Initiate key rollover

- Child creates new key pair: "
- Child gets CA cert" from parent
- Child issues manifest, CRL only for "
- Child publishes in <u>the same</u> rsync directory

- Start of 24 hour staging period

Normal Key Rollover (RFC 6489)

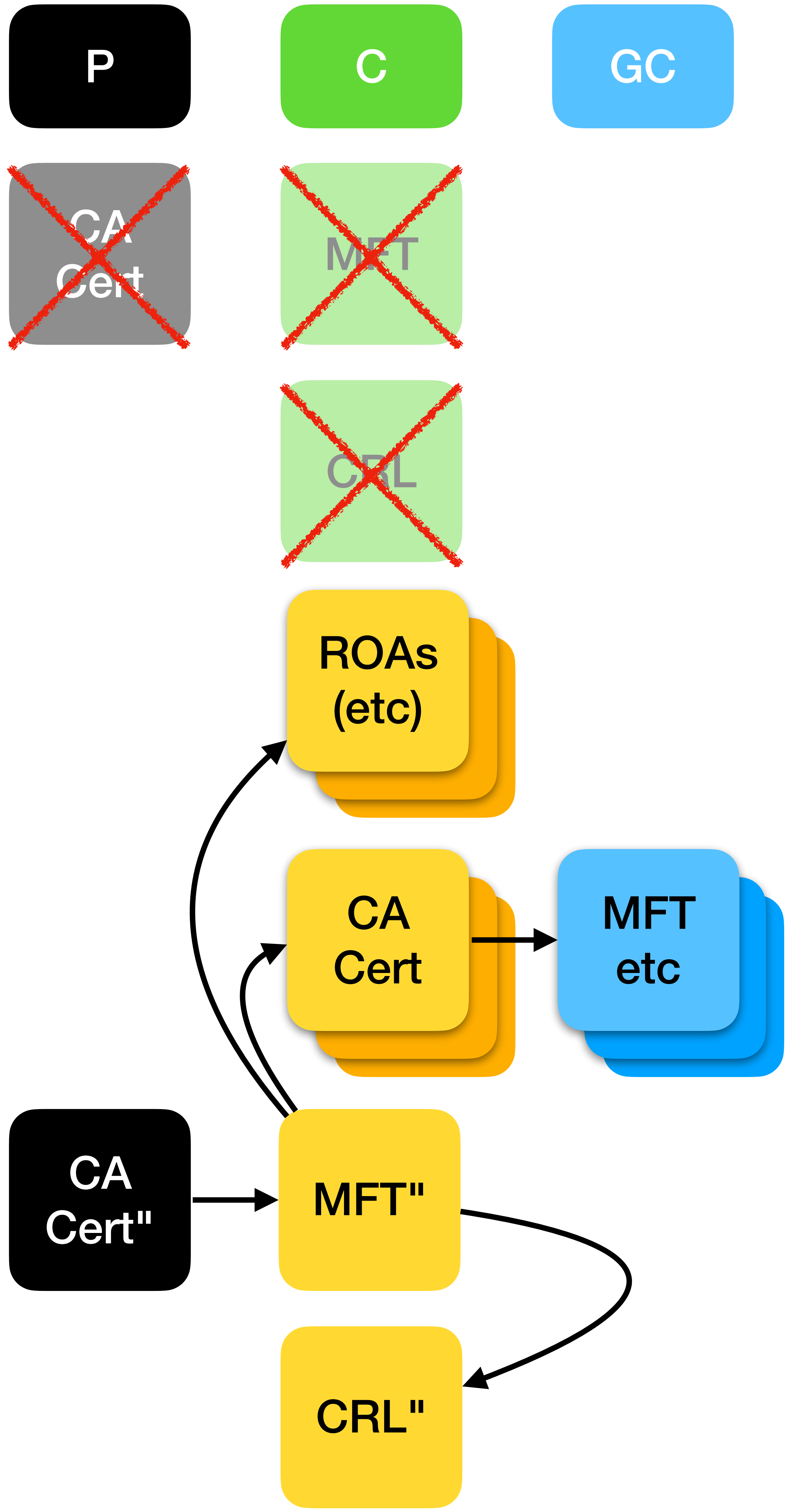


Phase 2a: Activate new key

- Child re-issues all signed objects with key "
- Child re-issues delegated CA certs with key "
- URIs of re-issued objects are <u>unchanged</u>
- Child re-issues manifest and CRL for old key

- ALL done in one go! As one publication delta.
- RPs get this as one delta (both RRDP or rsync)

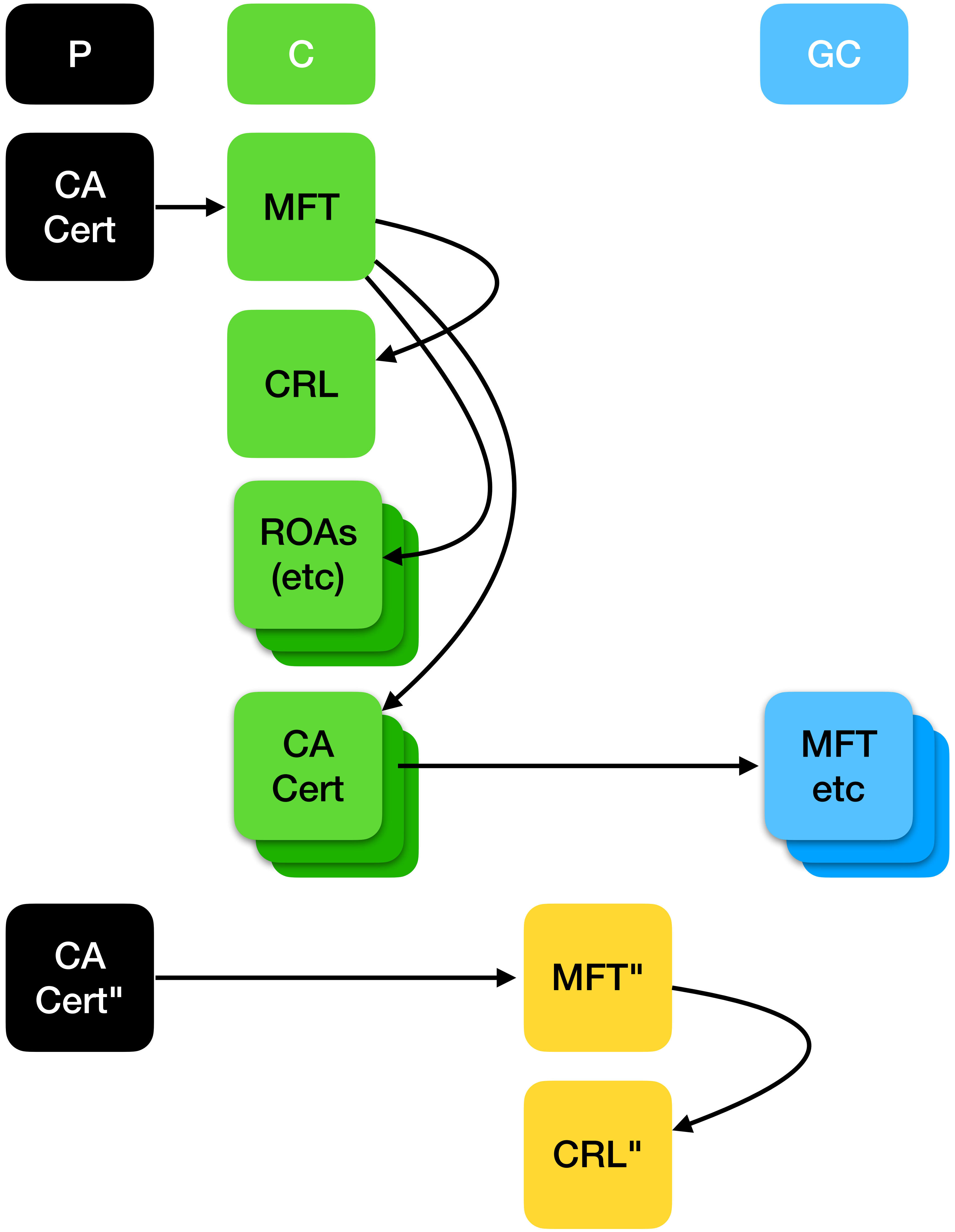
Normal Key Rollover (RFC 6489)



Phase 2b: revoke old

- Immediately following activation of new key
- Child asks parent to revoke old key
- Child removes MFT and CRL for old key

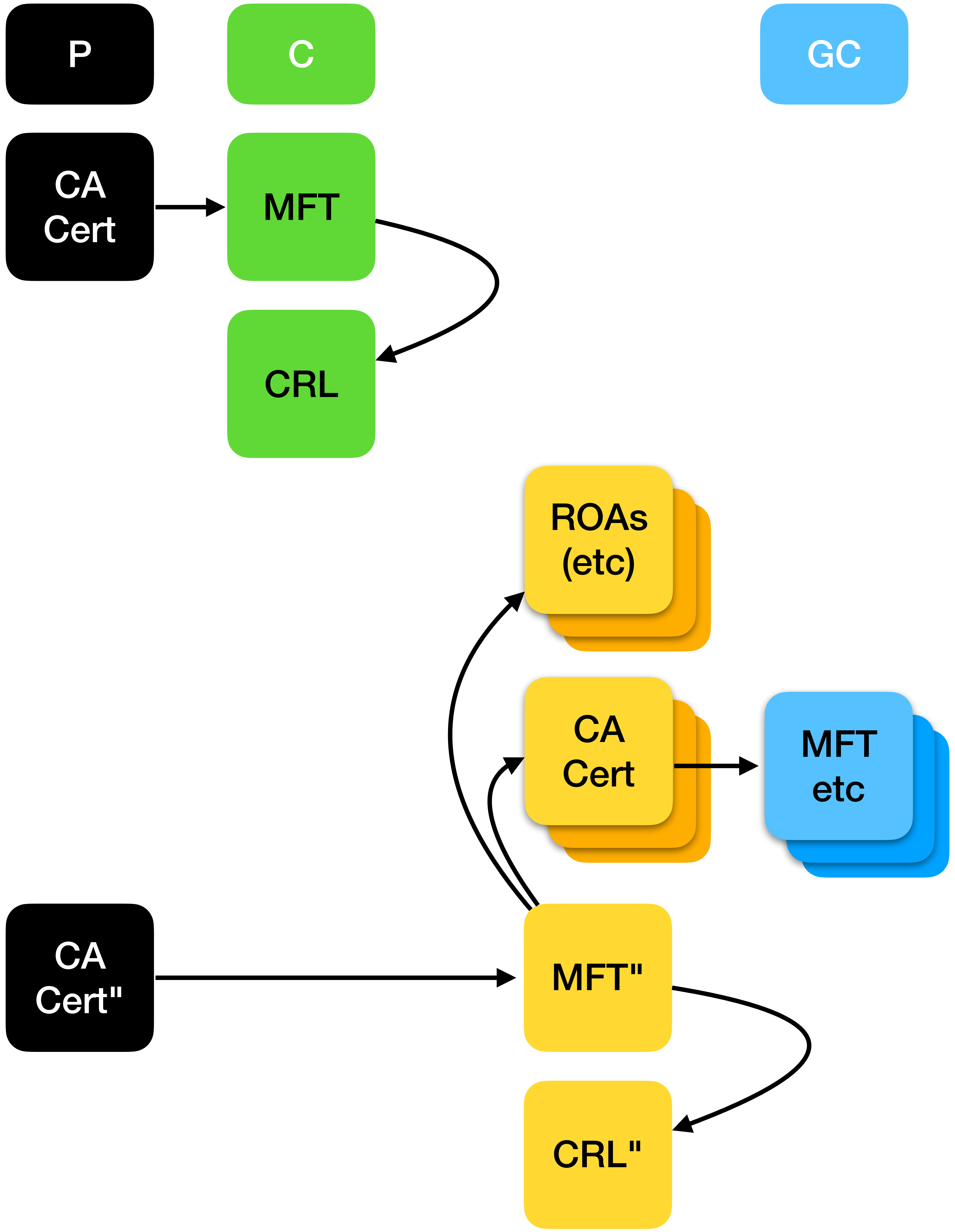
Key Rollover - New Repository



Phase 1: Initiate key rollover

- Child uses new repository for new key
- Enter 24 hour staging period. Is this really needed?

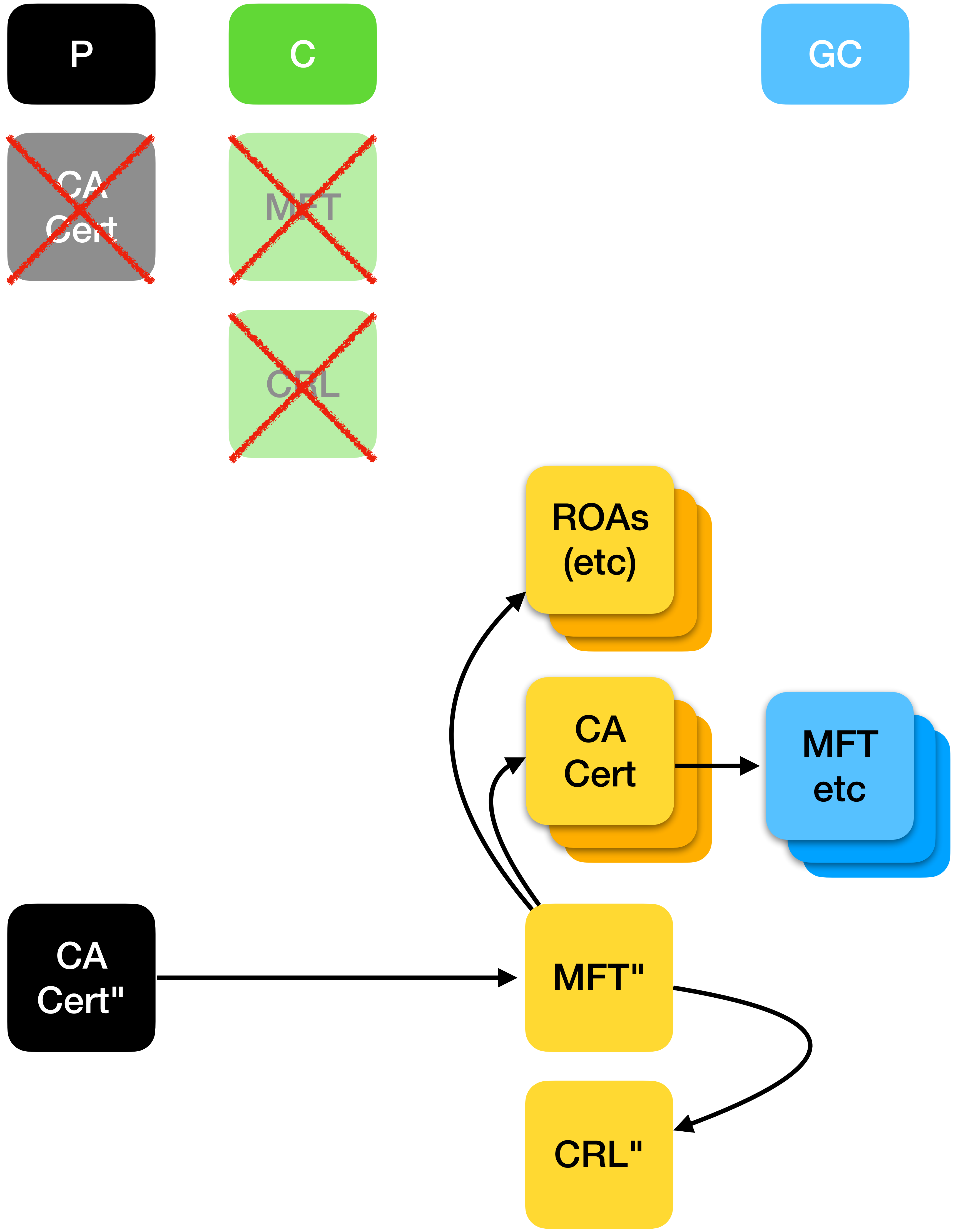
Key Rollover - New Repository



Phase 2a: Activate new key

- Child re-issues signed objects and CA certs under new key, in new repository
- Child removes signed objects and CA certs under old key in old repository
- Currently done as one step with two publication events
- Should probably be changed: keep old a while longer as fetches are out of sync

Key Rollover - New Repository



Phase 2b: Revoke old key

- Immediately following activation of new key
- Child asks parent to revoke old key
- Child removes MFT and CRL for old key

- AIA pointers of GC objects are misaligned. Child may only find out on next RFC 6492 Resource Class List Query sent.
- Treat AIA as purely informational?

Questions

- Standardise Repository Migration?