draft-ietf-sidrops-signed-tal-07

●●●

IETF 111 SIDROPS Working Group

Recap

- Signal to relying parties that the TA key or certificate URLs have changed, by way of a **T**rust **A**nchor **K**ey (TAK) signed object
- Main goal is simplifying key rollover
  - If the client supports TAK objects, then the client can get new TAL data automatically - no need to wait for (or depend on) client upgrade, or custom TA update process
  - More confidence around key rollover helps with HSM vendor lock-in
- Secondary goal is the ability to update URLs
  - Gives more flexibility around deployment

Changes since 06

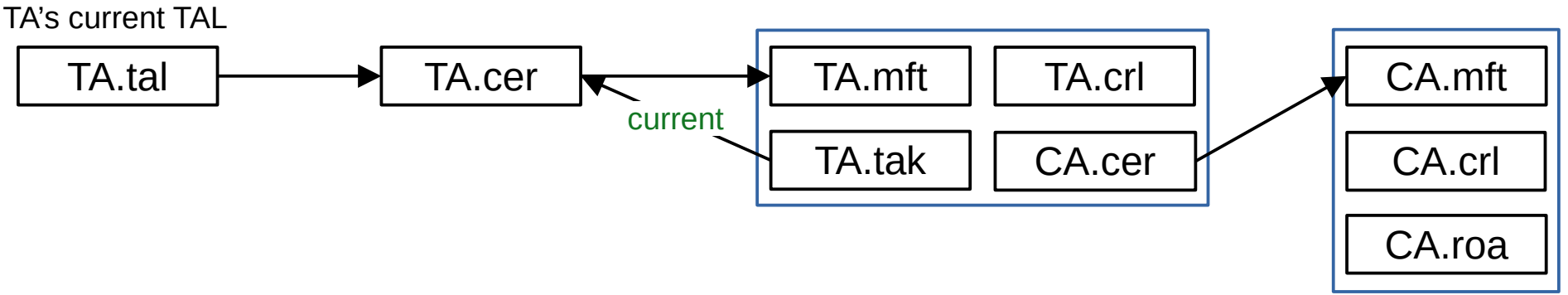
- Limit TAKs to two keys: current and successor

```
TAKey ::= SEQUENCE {
    certificateURIs       SEQUENCE SIZE (1..MAX) OF CertificateURI,
    subjectPublicKeyInfo SubjectPublicKeyInfo
}

TAK ::= SEQUENCE {
    version      INTEGER DEFAULT 0,
    current      TAKey,
    successor    TAKey OPTIONAL,
    revoked      BOOLEAN
}
```

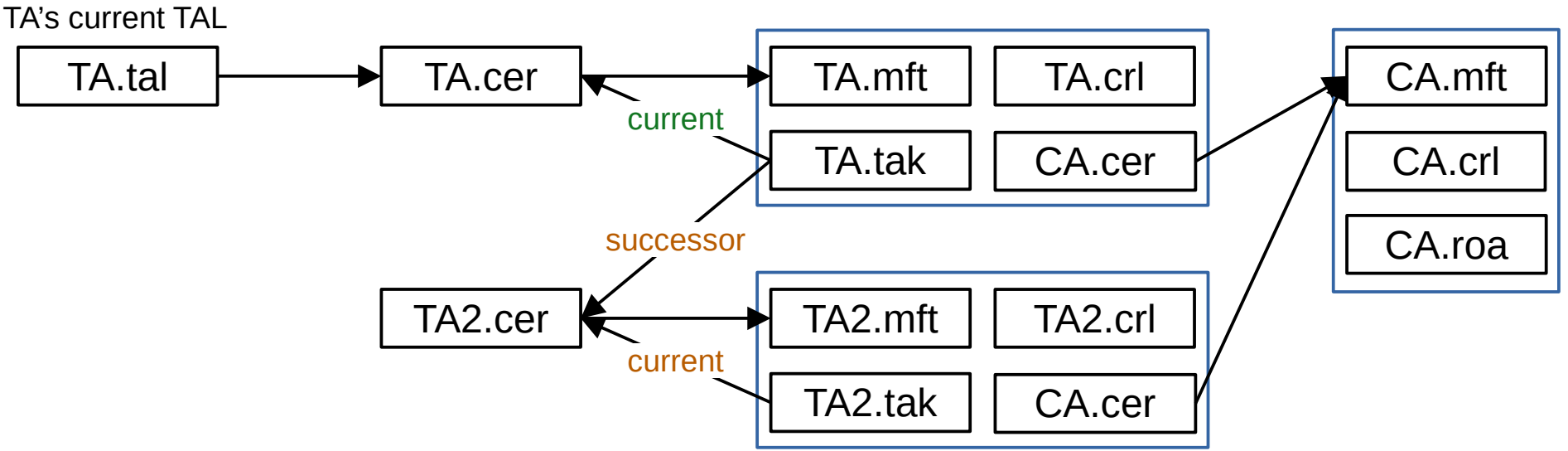
- ASN.1 module fixes (thanks to Russ Housley)

Phase 1



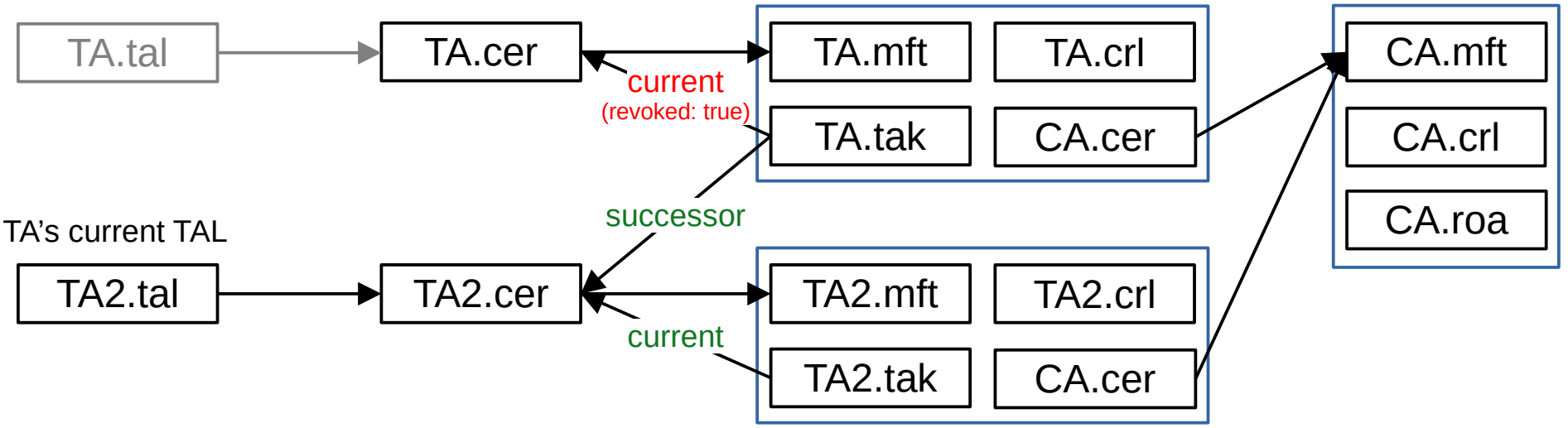
- TA publishes TAK object pointing to TA.cer as current key
- TAK contains updated URL set (compared with what's in the TAL)
- TA can determine which clients are relying on TAKs by observing which clients fetch from the new URLs
- (Same as for 06)

Phase 2



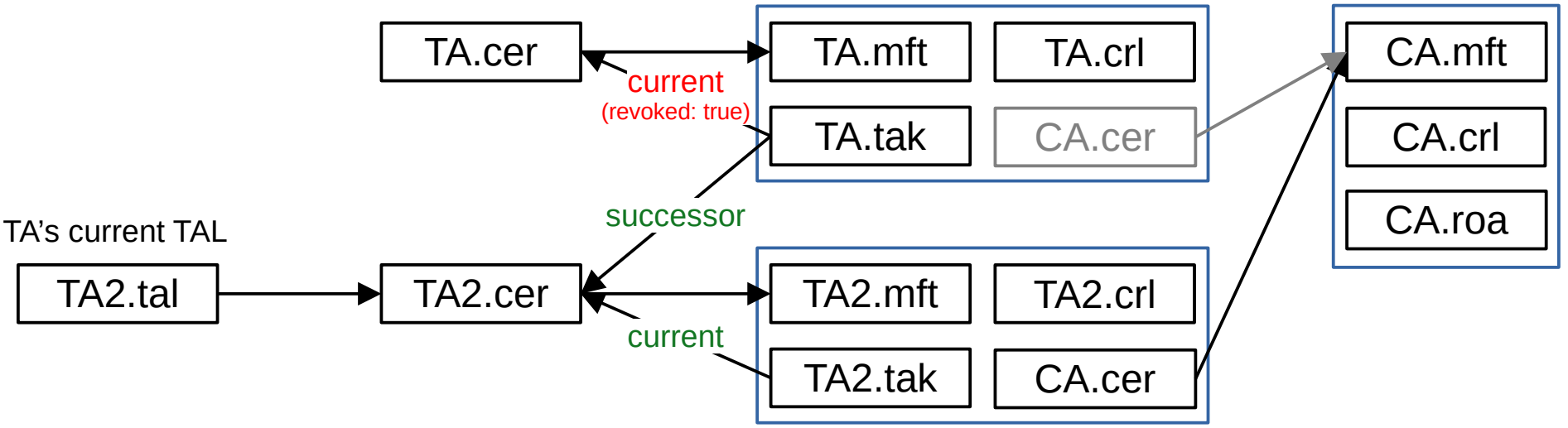
- TA.tak adds pointer to successor key
  - Current key (TA.cer) MUST be used for validation, though
  - No need for client using TA.tal to process TA2.cer, yet (just advisory)
- TA2.tak points only to TA2.cer
  - Unlike with 06, it can't be used to revoke TA.cer

Phase 3



- TA.tak revokes current key (sets revoked to true)
- TA publishes new TAL (TA2.tal) and withdraws previous TAL
- All RPs move to TA2.cer

Phase 4



- TA publishes long-lived TAK at TA.tak, along with CRL and manifest, and removes other objects, so that clients validating at TA.cer will still find TA2.cer

Testbed

- https://github.com/APNIC-net/rpki-signed-tal-demo
  - Takes a TAL path as its argument, prints debug information, and replaces the TAL if required
  - Can be used with existing RP clients
- https://rpki-testbed.apnic.net/signed-tal.html
  - Various TALs for testing
    - Single TA with TAK for current key
    - Single TA with TAK for current key, TAK has new URL
    - Two TAs with TAKs, first key unrevoked
    - Two TAs with TAKs, first key revoked
    - Single TA with TAK for current key, and key is revoked

Next steps

- Working group last call