draft-ietf-sidrops-signed-tal-02

Goals

- Allow RPKI Trust Anchor Key Rolls
- Learn from DNSSEC (RFC 5011)
- Soft landing into existing standards
- Leave a trail for outdated clients

Changes in -02

- Allow multiple active keys as in DNSSEC (recommended to use just two)
- Supports both planned and unplanned rolls
- No time and intent of next key included, because of unplanned rolls

Next steps!

- Speak now, or forever hold your peace!

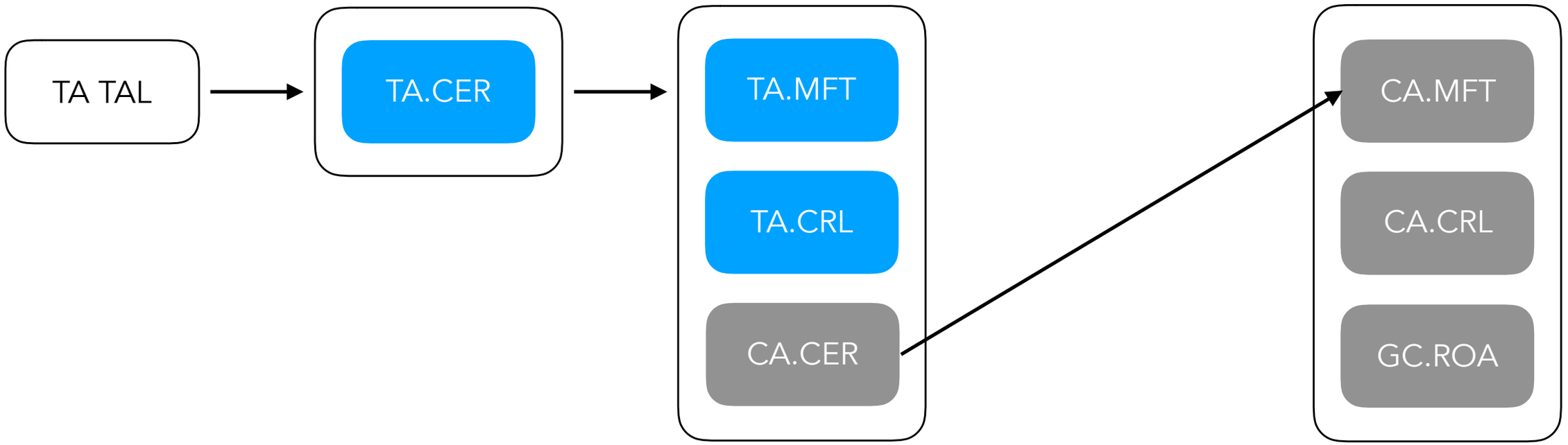
- Running code at IETF 104

- Do people want a hackaton?

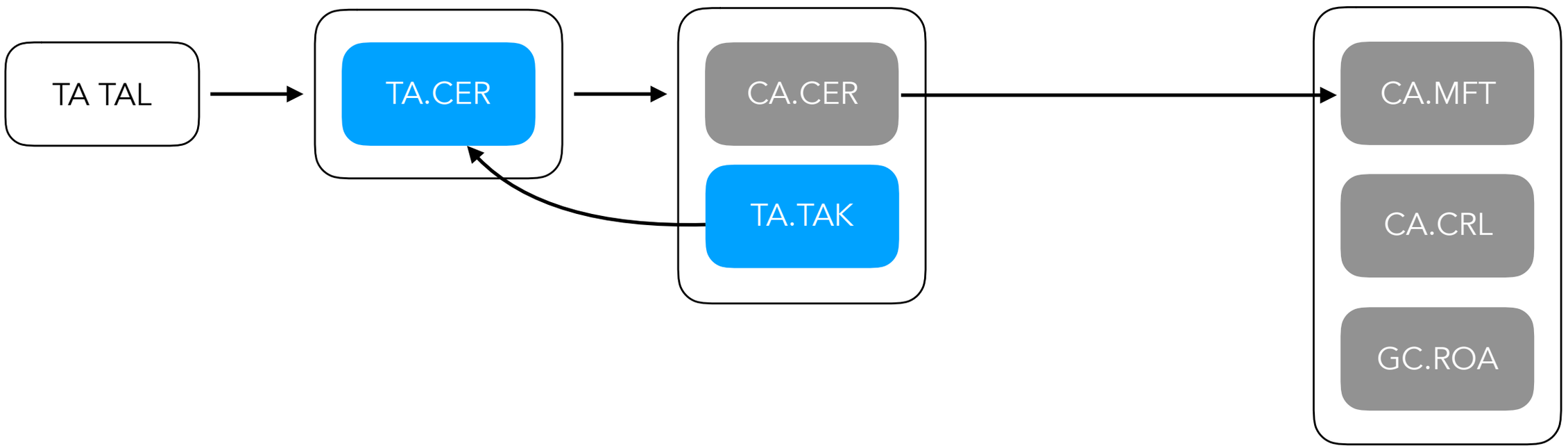
Concerns?

Photo by Koen Eijkelenboom on Unsplash

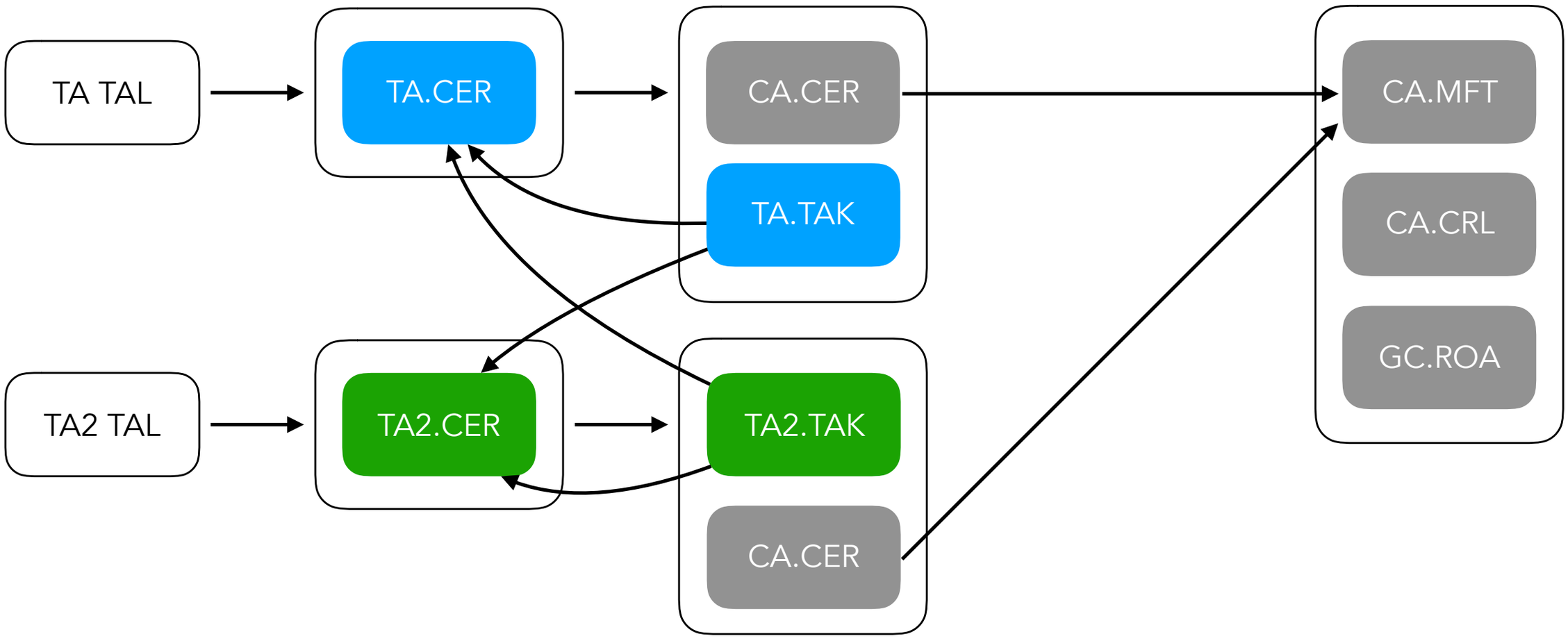
Current situation



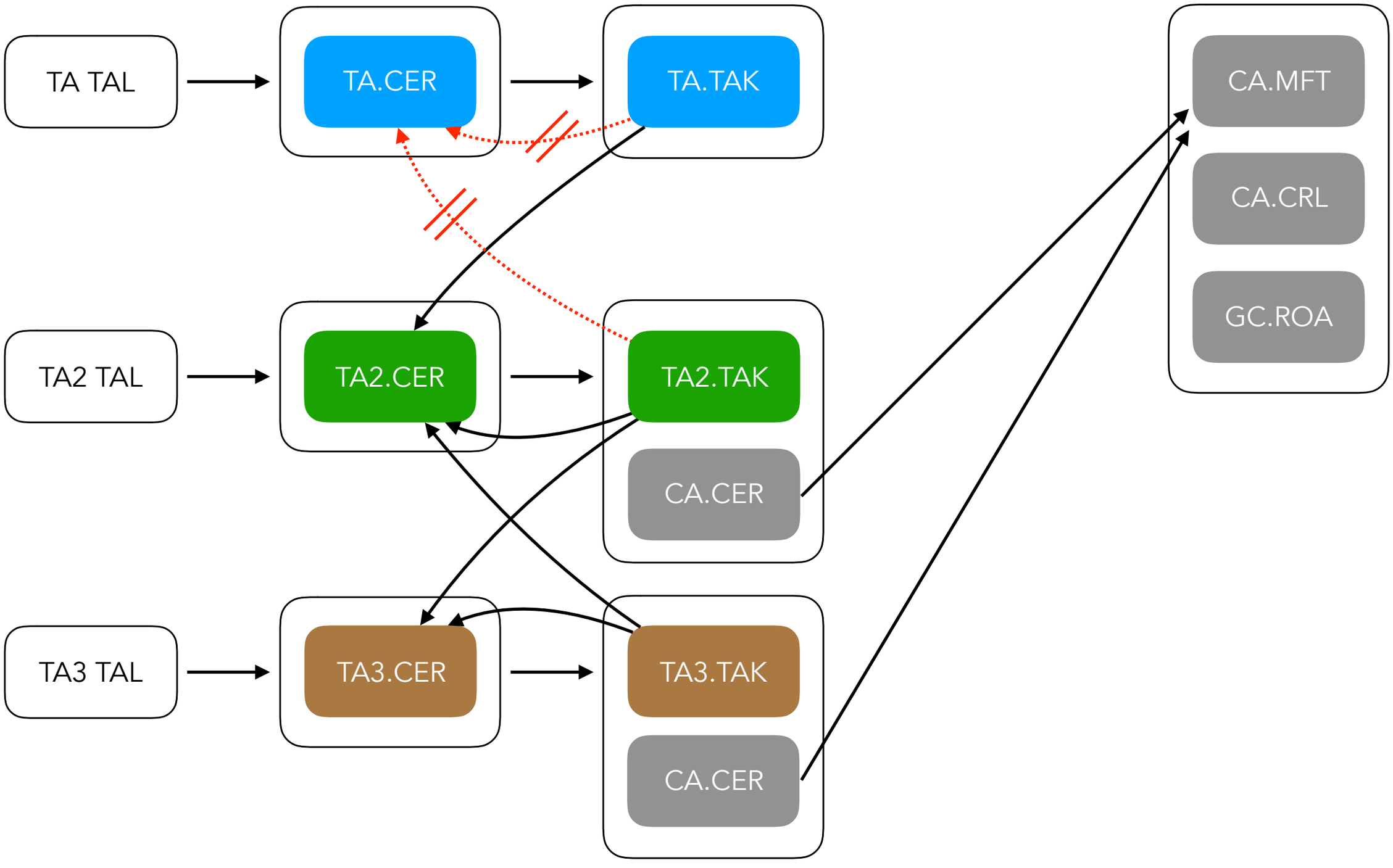
Opt-in, using 1 key



Using 2 keys


TA TAL
TA.CER
CA.CER
TA.TAK
CA.MFT
CA.CRL
GC.ROA
TA2 TAL
TA2.CER
TA2.TAK
CA.CER

Rolling to keys 2 & 3



Concerns?

Photo by Mikhail Vasilyev on Unsplash