draft-ietf-sidrops-signed-tal-10

IETF 114 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

Feedback on 07 (1)

- Review other approaches to TA rollover and consider relevance
  - RFC 4210: Certificate Management Protocol (CMP)
    - Section 4.4: Root CA Key Update
      - Also part of RFC 7030: Enrollment over Secure Transport
    - Sign old with new, and new with old, to facilitate TA transition
    - Appears to be motivated by two factors:
      - TA distribution is out-of-band (clients may be using old or new)
      - Client may receive certificates from other sources
    - The aim with signed TAL is to have TA distribution be in-band, though, and all relevant certificates are in the RPKI repository, so it’s not clear that this model is applicable

Feedback on 07 (2)

- Review other approaches to TA rollover and consider relevance
  - RFC 8649: Hash Of Root Key Certificate Extension
    - Include hash of new TA key in existing TA certificate, so that client can transition on seeing new TA certificate
    - Per Tim’s comments on the list:
      - Possible issues with RPs not ignoring the extension
      - Unable to transition from previous TAL data once certificate has been replaced
    - The model in 8649 involves a single TA certificate issued ahead of time, but RPKI supports arbitrary reissuance of that certificate – would need additional guidance around what to do when the value changes, and so on

Feedback on 07 (3)

- Review other approaches to TA rollover and consider relevance
  - Web PKI
    - Unable to find anything about rollover in this context
    - It appears that root CA operators simply issue new standalone root CA certificates as required, and cross-certification is used to facilitate the transition

Feedback on 07 (4)

- Review other approaches to TA rollover and consider relevance
  - RFC 5011: Automated updates of DNSSEC TAs
    - Client sets acceptance timer on seeing a new key, as a precaution
    - If the new key remains unchanged for the period of the acceptance timer, then add the new key as a TA
    - Same model now adopted in signed TAL
      - Acceptance timer period is 30 days (arbitrary figure)
      - Will address (some) concerns around consequences of key compromise

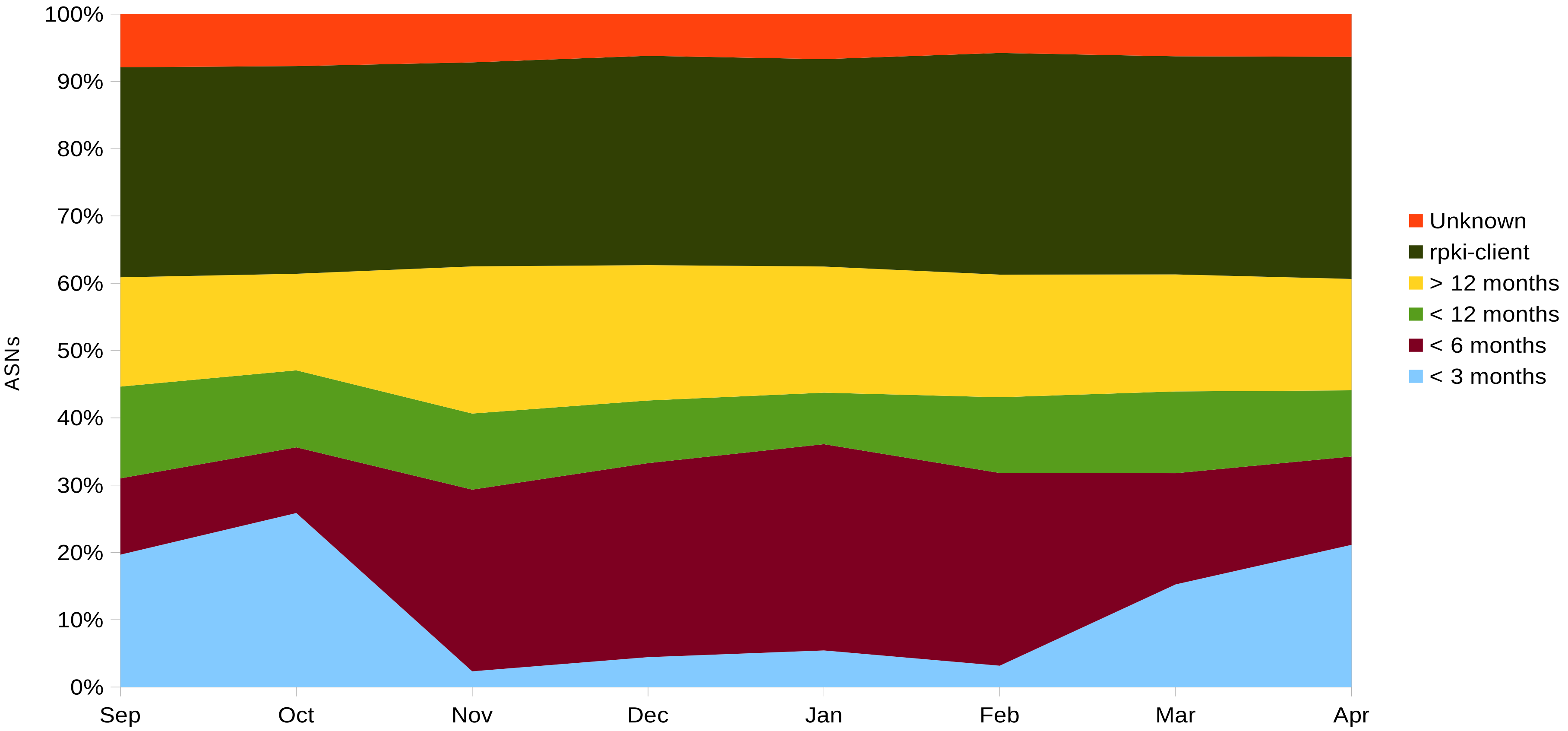
Feedback on 07 (5)

- The term ‘revoked’ is misleading in context, since clients with TAL data for the revoked key will still trust data returned by that key
  - Avoid the term ‘revoked’ in the TAK object and the document
  - Advise TAs to reuse previous TA certificate URLs for new keys, when they are no longer maintaining the previous key
    - An attempt to make use of that certificate URL for an attack based on previous TAL data will then at a minimum not go unnoticed

Other changes

- The successor key now includes a reference to the predecessor key
  - As an additional check to ensure that the successor key is configured correctly and is expecting to operate as a successor key
- Discussion of use of TAK objects as substitute for TAL data
- (Further security suggestions/updates are pending: they did not make the document deadline for this meeting)

Validators – how up to date?



Next steps

- Feedback?