draft-ietf-sidrops-signed-tal-12

IETF 115 SIDROPS Working Group
Recap

- Signal to relying parties that the TA key or certificate URLs have changed, by way of a Trust Anchor Key (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 from 10 → 11

• Note that RPs can opt for manual/user-directed transition while still getting the benefits of the TAK model

• Note that TAK objects distributed out of band have similar security properties to TAL files

• Document security considerations around ‘temporary’ compromise: where attacker has access to HSM (or similar) for a period of time, but there’s no direct exposure of the private key
Changes from 11 → 12

- Add comments to the ASN.1 structure, to mirror the structure of TALs per RFC 8630

```
TAKey ::= SEQUENCE {
    Comments
        SEQUENCE SIZE (0..MAX) OF UTF8String,
    CertificateURIs
        SEQUENCE SIZE (1..MAX) OF CertificateURI,
    SubjectPublicKeyInfo
        SubjectPublicKeyInfo
}
```
Implementation work since IETF 114

• APNIC server-side and client-side demo implementations updated for version 12
  – https://github.com/APNIC-net/rpki-signed-tal-demo

• Client-side object validation by Job
  – https://github.com/openbsd/src/commit/ee2a33daaeea41bd3caa3faa3d08e73f5cec094a

• Initial TAK-encoding work by Tim
  – https://github.com/NLnetLabs/rpki-rs/pull/240
To discuss

• Update the ‘RPKI Signed Objects’ registry heading to avoid confusion as to certificates and CRLs not being listed?

• Remove the TA compromise section?

• Add text about ‘certified’ destruction of keypair materials?
Next steps

- Updates for additional suggestions from Job
- Editorial: consolidating server-side instructions and purpose of acceptance timer
- More implementations