draft-ietf-sidrops-signed-tal-03

(not in last call)
Goals

- Allow RPKI Trust Anchor Key Rolls
- Learn from DNSSEC (RFC 5011)
- Soft landing into existing standards
- Leave a trail for outdated clients
Comment on -02

When is it safe to drop the old key?
Changes in -03

- Clarified phases.. I hope!
- Use distinct URIs for TA certificates in TAKs for each phase!
TAK Objects

TAK ::= SEQUENCE {
    version INTEGER DEFAULT 0,
    current ::= SEQUENCE SIZE (1..MAX) OF CurrentKey,
    revoked ::= SEQUENCE OF SubjectPublicKeyInfo
}

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

CertificateURI ::= IA5String

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm AlgorithmIdentifier,
    subjectPublicKey BIT STRING
}
Phase 0: Current situation
Phase 1: Add a TAK

➡ RPs which support TAK MUST use URIs in TAK
➡ TA operator can monitor which proportion of RPs support
Phase 2: Add key 'B'

Ship TA2 TAL with RPs, or even.. ship TA2.TAK?
Phase 3: Roll to TA 3

Graphical representation of the process flow from TA TAL through TA.CER to TA.TAK, with further connections to CA.MFT, CA.CRL, and GC.ROA.
Next?
Concerns?