draft-ietf-sidrops-signed-tal-06.txt

draft-ietf-sidrops-signed-tal-06.txt

The obviously required ‘in band’ signaling method to inform RP of key rollover events.

- Simple information model
  - Defines the “Trust Anchor Keys” (TAK) object (ASN1) to declare signed TALs
  - Defines validation requirements for a TAK to be well formed/valid
  - Requests an OID assignment, marks .tak as the file extension for Manifest
- Shows models of key rollover by use of the TAK in different scenarios

draft-ietf-sidrops-signed-tal-06.txt

- Changes in the draft
  - We added a paragraph to reflect Rob Kisteleki's feedback on the risk of a signal like this being mis-used to "steal" a TA
- Whats the scope and purpose? Why do this?:
  - This is mainly about planned key-roll. We believe it would be useful to not have to do vendor backed update to the TAL, to get planned key rolls done in wide-scale deployment.
    - HSM use can lead to key lockin, moving to new HSM vendor demands new keys
  - Pro:
    - No need to redistribute TALs (think docker, existing deployment and such)
  - Con:
    - Adds complexity
- Security:
  - If there is malicious access to key.. And corrupt change through signed TAL
  - Mitigation: redistribute new TAL after all through vendors, community channels

Is this a significant security risk?

In our view the security is not worsened by this.

If an attacker has the root key and access to a repo then they can already break everything.

Also, *that's why God invented HSMs.*

However, the complexity in TA and RP implementations is a real concern. More complexity does not always make more security

Implementation: APNIC has a testbed

- APNIC has deployed a testbed with different states of TAK
  - Single TA with a TAK for the current key
  - Two TAs with a TAK for the first key only
  - Two TAs with TAKs for both keys, and the first is revoked
  - Single TA with a TAK for the current key, and the key is revoked
- We invite RP vendors, developers to come and play, gain experience
  - Testbed: **https://rpki-testbed.apnic.net/signed-tal.html**
  - Code: **https://github.com/APNIC-net/rpki-signed-tal-demo**

Next Steps

- Feedback from testbed
  - Draft needs at least one more round of work based on deployment/testing experiences
- Open issues (Tim) regarding key limits (2 only? More?)

- Discuss on ML, aim for possible WGLC at next IETF?