Signed TAL
**Problem Statement**

- TALs distributed / configured with deployed RPs

  rsync://rpki.example.org/rpki/hedgehog/root.cer
  rsync://rpki.example.org/rpki/warthog/root.cer

  MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDxGUG5hbtCXvvh4AOzjhDkJShl22gn/loIIm9IeDATlwp44vhQ6L/xvuk7W6Kfa5ygmqQ+xOZ0wTWPrUBqAfYqPNxokuivzyvqVZVDec0EqS78q58mSp9nbtxmLRW7B67SJCBSzjfa5XpVYXEgYAjkk3fpmefU+AcxtxvHB50VPIaBfPcs80ICMgHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrGe0WSDc3fr3erLueagpiLsFjwwpX6F+Ms8vqz45H+DKmYKVPSstZjCCq9aJ0qANT90tnfSDOS+aLRpJZryCNyvvBHxZXqj5YCGKtwIDAQAB

  • What if I want to use https? Or additional URIs?
  • What if I want to do a planned roll of the key? (HSM vendor lock-in)
Going Forward - disclaimer

• Made draft to have a structured discussion about one possible way forward - not married to it, no pregnancies

• Not against solutions that included unplanned key rolls, but..
  • It’s a problem I fortunately do not have today
  • I don’t have a great idea about how to solve it
  • I believe a solution to this should not delay a solution to the practical use cases of changing URIs and a planned key roll
Signed TAL

RP

TAL

TA

MFT

CRL

CER

CER

TAL
Key Roll

• Prepare new
  – Publish ALL object of old under new (except TAL)
  – Publish TA certificate
  – Publish TAL under old TA

• Staging (24 hours ?): publish old AND new

• Keep old?
  – Just a long-lived CRL, MFT and TAL pointing at new, so that RPs can find new
  – Destroy old key
New URIs

- **Add URI**
  - MUST publish certificate before publishing TAL

- **Remove URI**
  - SHOULD still publish certificate for 24 hours (?)

- **Withdraw TAL**
  - SHOULD withdraw TAL after 24 hours (?)
Summary and going forward

• Adopt as WG item and discuss further?

• Again, not married to the proposal - it’s intended as a start of conversation, but our use case is real
Questions