• Draft describes the ASN.1 detached signature model
• OID already allocated, conforms to SIDR OID namespace, legal object in Manifests
• Designed as standalone validation B2B tool, only TA required by RP
  • B2B contexts which need ‘proof of possession’
  • BYO IP, Letter of Authority
• Encompasses multi-sign model, because RPKI can lead to more than one entity (key) over a set of Internet Number Resources
• Based on CMS
• No substantive changes to draft, added authors to reflect implementation.
• Implementation: **we now have two implementations**
  • APNIC: system released some years ago
  • NLNet labs implemented RTA with funding from APNIC
    • This is compile-time selectable, but works entirely self-hosted
• There are now 4 out of 5 RIR which support self-hosted RPKI
  • Krill works under APNIC, ARIN, LACNIC and RIPE
  • No modification of the RPA to deploy
• Basic model: do stuff, sign with your resources, private is fine
  • What kind of things to sign? Whatever you want!
Next steps

• Adoption?
• Or, is this better suited to another WG?