A Profile for Trust Anchor Material for the Resource Certificate PKI

Geoff Huston
SIDR WG
IETF 74
Background

• This has been the topic of WG discussion
  – who should be putative TA for the RPKI
  – how should TA material be published

• Focus the discussion by creating a document to address Trust Anchors for the RPKI
  – Removed section 6.3 from Res Cert profile draft
  – Created a new draft with this material
  – draft-ietf-sidr-ta-00.txt
Who?

- Draft is silent on prescribing roles for bodies:
  
  "This document does not nominate any organizations as default trust anchors for the RPKI."

- Reasons for this position:
  - This task falls outside of IETF WG direction relating to conventional protocol parameter registry functions
  - The standard technology specification should encompass use in a broad spectrum of contexts including various forms of private use as well as public

- However, the document does observe that:
  
  "for most RPs, the IANA is in a unique role as the default TA for representing public address space and public AS numbers."
How?

• No change from previous TA specification in draft-ietf-sidr-res-certs
  – (aside from some terminology clarifications)
• Two-Tier Model of Trust Anchor
  – Allows for variation in resources held at the “root” while keeping the trust anchor material constant
  – Can be used in a variety of contexts, both public and private
  – Aligns with the TA work in PKIX WG (draft-ietf-pkix-ta-format-01)
1. External Trust Anchor Certificate - ETA
2. Certificate Revocation List for ETA
3. ETA EE Certificate (for CMS Object Verification)
etA TA Certificate
Issuer: etA
Subject: etA
CA: True
(no 3779 ext)
Signed: etA

etA EE Certificate
Issuer: etA
Subject: etA EE
CA: False
(no 3779 ext)
Signed: etA

CRL of etA
Issuer: etA
Signed: etA

RPKI TA Certificate
Issuer: RPKI TA
Subject: RPKI TA
CA: True
3779 Exts
Signed: RPKI TA

4. RPKI TA Certificate
5. CMS packaging of the RPKI TA Certificate

**CMS Signed Object**

- **CMS Header**
  - **ETA EE Certificate**
    - Issuer: ETA
    - Subject: ETA EE
    - CA: False (no 3779 ext)
    - Signed: ETA

- **CMS Payload**
  - **RPKI TA Certificate**
    - Issuer: RPKI TA
    - Subject: RPKI TA
    - CA: True
    - 3779 Exts
    - Signed: RPKI TA

- **ETA TA Certificate**
  - Issuer: ETA
  - Subject: ETA
  - CA: True (no 3779 ext)
  - Signed: ETA

**CRL of ETA**

Signed: ETA EE