Introduction:

• This document describes:

  • The X.509 cert. profile to be used in SEND that was missing in RFC 3971.

  • Extended Key Usage values.

  • Certification Revocation Solicitation (CRS) and Advertisement (CRA) messages.

  • version-00 was the individual I-D.
Certificate Profile.

- We will be using the SIDR WG Cert Profile.
- Deployment models: RFC 3971 defined two deployment models: centralized and decentralized. We introduced two new deployment models: local and public.
Deployment models:

- Administrative Domain (ex. ISP, enterprise)
  - Host
  - Local
  - TA
  - Certs and CRL Repository.

- Administrative Domain
  - Host
  - Public
  - TA
  - Certs and CRL Repository.
Trust Anchors (I):

- We added section 5.1 to discuss Trust Anchor material selection.
- Old text mentioned SIDR “default trust anchor”, but that has changed.
- We could have either an RFC3779 cert as TA or a non RFC3779 cert using [draft-ietf-sidr-ta-02].
- In a local deployment ::/0 TA is an option.
Trust Anchors (II):

ETA CA Certificate
- Issuer: <ETA>
- Subject: <ETA>
- SIA: <URI>
- Signed: ETA (self-signed)

ETA Repository Publication Point
- CMS Signed Object
- CMS Attributes and Signer Info
- ETA EE Certificate
  - Issuer: <ETA>
  - Subject: <ETA EE>
  - SIA: <URI>
  - CRL: <URI>
  - Signed: ETA
- CMS Signed Data
  - RTA CA Certificate
    - Issuer: <RPKI TA>
    - Subject: <RPKI TA>
    - CRL: <URI>
    - SIA: <URI>
    - IP: <IP Addresses>
    - AS: <AS Numbers>
    - Signed: RPKI TA (self-signed)

ETA CRL
- Issuer: <ETA>
- CRL List
- Signed: ETA
Extended Key Usage Values

• No changes since version 00.
CRL profile and revocation

• By using SIDR Cert. Profile, there is no support for OCSP.

• Hosts needs to get not only the CERTs but also the CRLs to validate a certificate path.

• In-band exchange of CRL between the host and the router will be performed using two new SEND messages:
  • Certificate Revocation Solicitation (CRS).
  • Certificate Revocation Advertisement (CRA).

• We still need to define these messages in -02.
• Questions?