draft-weiler-sidr-trust-anchor-format

Samuel Weiler

IETF78, Maastricht

28 July 2010

RPKI Trust Anchor Challenges

- List of resources changes
- Certficate changes
- Don't want to change relying party configuration ("trust anchor")

A Simpler Alternative

- Current doc: A compound trust anchor with new ASN.1 blobs, OR ....

A Simpler Alternative

- Current doc: A compound trust anchor with new ASN.1 blobs, OR ....
- New doc: A URI to a cert and the public key from that cert

  rsync://rpki.example.org/rpki/foo/root.cer
  MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
  GUG5hbtCXvvh4AOzjhDkSHlj22gn/1oiM9leDA
  Kfa5ygmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvq
  nbtxmLRW7B67SJCBSzfa5XpVyXYEgYAj

Usage

- Retrieve the self-signed certificate at the URI
- Compare the key to the certificate's key
- Check the signature on the certificate
- Other usual cert checks (CRL, etc.)

Adopt?