A Unified RPKI Certification Practices Statement (CPS)

Steve Kent

BBN Technologies

Context

- RFC 3647 (Informational) provides an outline and explanatory text for defining
  - A certificate policy (CP)
  - A certification practice statement (CPS)
- This RFC is very widely cited
  - Essentially every large scale PKI publishes a CPS and uses the outline from 3647 as its model
  - When a certificate issuer publishes a certificate policy (CP), it also tends to follow the format defined in this RFC
- There is one outline in 3647; it nominally applies to both CP and CPS documents

RPKI CP vs. CPS

- We already have a CP for the RPKI: RFC 6484
- In many places the CP says:
  The CPS for each CA MUST specify …
- Every CA in the RPKI ought to generate a CPS, for the benefit of all relying parties
  - But a CA that does not issue CA certificates to other organizations (a leaf CA) probably does not really need to publish a CPS
  - A CPS is important for a CA that issues CA certificates (to other organizations) to publish a CPS, for the benefit of those organizations

Why Publish a CPS Template?

- Our goal is to make life easier for RPKI CAs
- This document is slated to be an Informational RFC
- The template is not binding on any CA in the RPKI
- It will provide a good starting point for RPKI CAs
  - Some text is likely to be common among all CAs
  - Where possible, we have adopted a “fill-in-the-blank” approach for CPS sections
  - There are still a few essay questions ☺

Why do we have one New CPS I-D?

- We previously wrote two I-Ds, each of which was a template for a CPS: one for registries and and one for ISPs
- Both are out of date (2 years old)
- These documents were not updated to align with the final (RFC 6484) version of the RPKI CP
- We have combined the two CPS templates into one document, which is aligned with the RPKI CP
- There were not enough differences to warrant separate documents, and we've made the template more general to accommodate both types of CAs

Status

- A -00 version was posted on July 9
- We request that the WG adopt it as a replacement for the two previously-approved CPS templates
- We solicit comments from the WG, especially from IANA, RIRs, and large ISPs
- Our goal is to make any required revisions and publish this as an (Informational) RFC by the end of 2012

Questions?