An Update on the CP and on the CPS Templates

Steve Kent

BBN Technologies

CP & CPS templates

- Just one CP for the whole RPKI
  - No significant changes since last meeting
  - Need feedback from RIRs and ISPs
- One CPS template for RIRs (and NIRs)
  - A lot of changes, to add more specific text that will be applicable to RIRs
  - Need to hear from NIRs to see if this works for them too
- One CPS template for ISPs (LIRs)
  - No significant changes since last meeting
  - Need to work with a couple of ISPs to see what may be common, to have a more complete CPS template

New CPS Template Assumptions

- Each RIR will
  - Use the certificate protocol defined in draft-ietf-sidr-rescerts-provisioning-00.txt for certificate issuance, rekey, and modification requests, and for revocation requests
  - Operate a business PKI (BPKI) separate from the resource PKI (RPKI), using the BPKI to authenticate users for issuance of RPKI certificates
  - Use the repository system to publish RPKI certificates
  - Assume implicit acceptance of an RPKI certificate by a user unless the user requests revocation
- Plus some place holder assumptions about timeliness of certificate & CRL processing

What remains for an RIR to fill in?

- Section 5
  - Discussion of physical, personnel, and procedural security for the CA
- Section 6
  - A few details related to CA key pair generation, activation and destruction
  - Discussion of computer security controls for the CA
- Section 8
  - A discussion of security assessments, if applicable
- Section 9
  - Legal stuff that your attorney needs to complete

Bottom Line

- The CPS for RIRs has many fewer places where whole paragraphs need to be created by an RIR
- I worked with the APNIC staff via e-mail exchanges over a few days, plus a 2 day visit to their site, to complete their CPS (except Section 9)!
- But, if an RIR does not already have a CP and CPS for a business PKI, they need two more documents
  - Can't just use all of the CP/CPS template for the RPKI, because the BPKI is different!
  - But, much of the data compiled for Sections 5, 6, 8, and 9 will be applicable