RPKI Certificate Policy Status Update

Stephen Kent

BBN TECHNOLOGIES

Changes from July

- At the July 2009 IETF meeting I briefed the many changes made to the CP as a result of review and editing by Andrei (on behalf of the RIRs)
- These changes were generally well received, but there were a few suggestions for additional changes
  - Make the IESG be responsible for maintaining the CP
  - Make the document a BCP instead of Informational
  - Provide a definition for RPKI signed objects, rather than just examples

Changes Due to WGLC Comments

- Improve the RPKI signed object definition
- Clarify that the use of names that are not meaningful to people apply to all Subjects

What we did, and What's Left to Do

- We failed to denote this as a standards track document targeted towards BCP status
- We changes to reflect the IESG as the entity responsible for maintaining the CP
  - Parts of section 9 were not modified (an oversight)
- We defined RPKI signed objects based on standards track RFCs issued by SIDR WG
  - We need to make this more general, to account for life after the SIDR WG
- We will revise the text on name types

RFC Status Revision

"Intended Status: Informational"

becomes

"Intended Status: Best Current Practice"

Revised text for 3.1.1

- The distinguished name for every CA and end entity consists of a single Common Name (CN) attribute with a value generated by the issuer of the certificate. Optionally, the serialNumber attribute may be included along with the common name (to form a terminal relative distinguish name set), to distinguish among successive instances of certificates associated with the same entity.

This text removes the distinction previously accorded RIRs and IANA names, and aligns with the SIDR architecture document

Revised RPKI Signed Object Text

"An RPKI-signed object, is a digitally-signed object (other than a certificate or CRL), declared to be such by a standards track RFC issued by the SIDR WG, …"

becomes

"An RPKI-signed object is a digitally-signed object (other than a certificate or CRL), declared to be such by a standards track RFC, ..."

Section 9.12.1 Revised Text

9.12.1. Procedure for amendment

"The procedure for amendments to this CP is via written notice from IANA and the Regional Internet Registries (RIRs)."

becomes

"The procedure for amending this CP is via written notice from the IESG in the form of a new (BCP) RFC that updates or obsoletes this document."

Section 9.12.2 Revised Text

9.12.2. Notification mechanism and period

"The IANA and the RIRs will provide at least one month's advance notice of a change to this CP."

becomes

"The IESG will provide at least a six month advance notice of any changes to this CP."

Section 9.12.3 Revised Text

9.12.3. Circumstances under which OID must be changed

"If the IANA and the RIRs judge that the change(s) will not materially reduce the acceptability of certificates for RPKI purposes, then there will be no change to the CP OID. If they judge that the change(s) will materially change the acceptability of certificates for RPKI purposes, then there will be a new CP OID."

becomes

"If the IESG judges that changes to the CP do not materially reduce the acceptability of certificates issued for RPKI purposes, there will be no change to the CP OID. If the IETF judges that changes to the CP do materially change the the acceptability of certificates for RPKI purposes, then there will be a new CP OID."

Two More Changes

- Though not mentioned on the list, we discovered an additional error that will be fixed:
  - The informative references to RSA and to RFC 2119 will be deleted