draft-rhansen-sidr-rfc6487bis-00

Richard Hansen, BBN
rhansen@bbn.com

RFC 6487 bis

- “A Profile for X.509 PKIX Resource Certificates”
- Changes incorporated:
  - all 3 verified errata
  - RFC 7318 (update)
  - two changes that were submitted as errata but deemed substantive
    - http://www.rfc-editor.org/errata_search.php?rfc=6487&rec_status=9

Errata 3168: Inconsistency re: allowed cert extensions

- Summary:
  - Sections 1 and 8 say that no other certificate extensions are allowed.
  - Section 4.8 says how to handle unknown extensions.
  - Fix Section 4.8 to agree with Sections 1 and 8.
- Submitted 2012-03-26, rejected 2013-05-06
- SIDR mailing list discussion threads:
  - http://thread.gmane.org/gmane.ietf.sidr/4168
  - http://thread.gmane.org/gmane.ietf.sidr/5837
- No objections to the proposed wording at the time.

Errata 3174: CRL AKI format underspecified

- Summary:
  - Section 5 says that the CRL must include the AKI extension.
  - It doesn't say:
    - Which optional fields MAY/SHOULD/MUST be present/absent
    - How to generate the `keyIdentifier` value
  - Fix by referring to Section 4.8.3 (AKI for resource certs)
- Submitted 2012-04-03, rejected 2013-05-06
- SIDR mailing list discussion thread:
  - http://thread.gmane.org/gmane.ietf.sidr/4314

Next Steps?

- Working group adoption
- Incorporate router cert updates from draft-ietf-sidr-bgpsec-pki-profiles

Backup Slides

3168 Change to Section 4.8

- Before:

  A certificate-using system MUST reject the certificate if it encounters **a critical extension it does not recognize; however, a non-critical extension MAY be ignored if it is not recognized [RFC5280].**

- After:

  A certificate-using system MUST reject the certificate if it encounters **an extension not explicitly mentioned in this document. This is in contrast to [RFC5280] which allows non-critical extensions to be ignored.**

3174 Change to Section 5

- Before:

  An RPKI CA MUST include the two extensions, Authority Key Identifier and CRL Number, in every CRL that it issues.

- After:

  An RPKI CA MUST include the two extensions, Authority Key Identifier and CRL Number, in every CRL that it issues. **The Authority Key Identifier extension MUST follow the same restrictions as in Section 4.8.3 above.**