Securing RPSL Objects with RPKI Signatures draft-ietf-sidr-rpsl-sig-01.txt

Robert Kisteleki
robert@ripe.net

IETF75, Stockholm

Changes in 01

- Minor textual changes
- Added text to require URL safeness for certificate references
- Text normalization:
  - Dropped uppercase/lowercase conversion
  - Added tab-to-space conversion
- Added document structure to separate signature creation and validation steps

Changes in 01

Added a section to clarify "number resource coverage”:

- The EE certificate referred to in the signature (which can be used to validate the signature) must have an RFC3779 extension
- This extension must have number resources that are relevant to the object
  - Ie. the IP address of an inetnum object

Changes in 01

Added a section to clarify the validity period of the signature:

- It's essentially the intersection of:
  - The validity time(s) of the certificate(s) used to verify the signature(s) on the object
  - The signing time and expiration time (if it exists) of the signature(s) themselves

Plans

- Make text more normative
- Further language clarifications
- Add an appendix with one or more example signatures
- Provide running code

Questions?