I-D.ietf-sidrops-rp Update

Di Ma and Stephen Kent

IETF 101, London, UK

Clarifications

- 1) We are not suggesting that implementers skip reading those RFCs in full
  - Our draft is intended to be a guide to help implementers get the essentials of RP functionalities scattered in different RFCs. Anyone who wants to comprehend (and especially to implement) RPKI cannot be exempted from reading all the RPKI RFCs
  - One might see the RP requirements document as a "Manifest" for all necessary RP functions ☺

- 2) Implementers need to know more than what RP requirements are
  - They need to know how to reflect these functions as they are designing software
  - To that end, this draft has generalized RP requirements that are segmented with orthogonal functionalities in different sections

Overview

- Adopted before IETF 100th meeting
- Current version： -01
  - First update since adopted
- Intended Status: Informational
  - This document provides a single reference point for requirements for RP software for use in the RPKI
  - It cites requirements that appear in several RPKI RFCs, making them segmented with orthogonal functionalities in different sections

Changes from -00 to -01 (1/2)

- Fetching and Caching RPKI Repository Objects (Section 2)
  - Adding RRDP [RFC8182] as an instance when mentioning synchronization mechanisms supported by targeted repositories
- Verifying Resource Certificate and Syntax (Section 3.1)
  - Providing more detailed references to RFC 6487
- Certificate Path Validation （Section 3.2）
  - Adding a paragraph that indicates the amended procedure to handle accidental over-claiming as specified in [I-D.ietf-sidr-rpki-validation-reconsidered]

Changes from -00 to -01 (2/2)

- How to Make Use of Manifest Data (Section 4.3)
  - If a Manifest is stale or invalid (see [RFC6486]) and an RP has no way to acquire a more recently valid Manifest, the RP is expected to contact the repository manager via Ghostbusters record (if available) and then make a decision according to local (RP) policy (Used to be TBD)

- Security considerations
  - Filling the blank by saying the RP is so critical to BGP message exchanges that RP implementations are expected to offer cache backup management and to employ secure transport (e.g., IPsec) with BGP speakers to protect validated cache delivery in a hostile environment

QUESTIONS?