# Requirements for RPKI Relying Parties

Stephen Kent & Di Ma

IETF95

# Problem Statement

- The RPKI has been well framed and standardized via a number of RFCs
- However, requirements imposed on Relying Parties (RPs) are scattered throughout numerous RFCs:
  - cert/CRL profile
  - ROA specification
  - Manifests specification
  - TAL specification, etc.
- This makes it hard for an implementer to be confident that he/she has addressed all of these requirements
- We propose to consolidate RP requirements in one document, with pointers to all the relevant RFCs

# What would this doc be like?

- To DEFINE the RP?
  - No. There is no standards language (e.g., MUST, SHOULD, MAY, ...) in this doc, as it is just POINTING to the docs that have the real requirements

- To do collecting?
  - Yes. This doc outlines the RP functions, summarizes them and then gives reference to those precise sections or paragraphs
  - This document will be updated to reflect new or changed requirements as these RFCs are updated, or new RFCs are written.

# Outline (1/2)

- Fetching and Caching RPKI Repository Objects
  - TAL acquisition and processing
  - Locating RPKI objects using Authority and Subject Information Extensions
  - Dealing with Key Rollover
  - Dealing with algorithm transition
  - Strategies for efficient cache maintenance
- Certificate and CRL Processing
  - Verifying Resource Certificate and Syntax
  - Certificate Path Validation
  - CRL Processing

# Outline (2/2)

- Processing RPKI Repository Signed Objects
  - Basic signed object syntax checks
  - Syntax and validation for each type of signed object
    - Manifest
    - ROA
    - Ghostbusters
    - Verifying BGPsec router certificate
  - How to Make Use of Manifest Data
  - What to Do with Ghostbusters Information
- Delivering Validated Cache to BGP Speakers

# Plan

- We will soon submit this doc as an I-D to IETF for discussion in SIDR after the I-D submission tool is reopened.

# THANKS!