Architecture and ROA Format

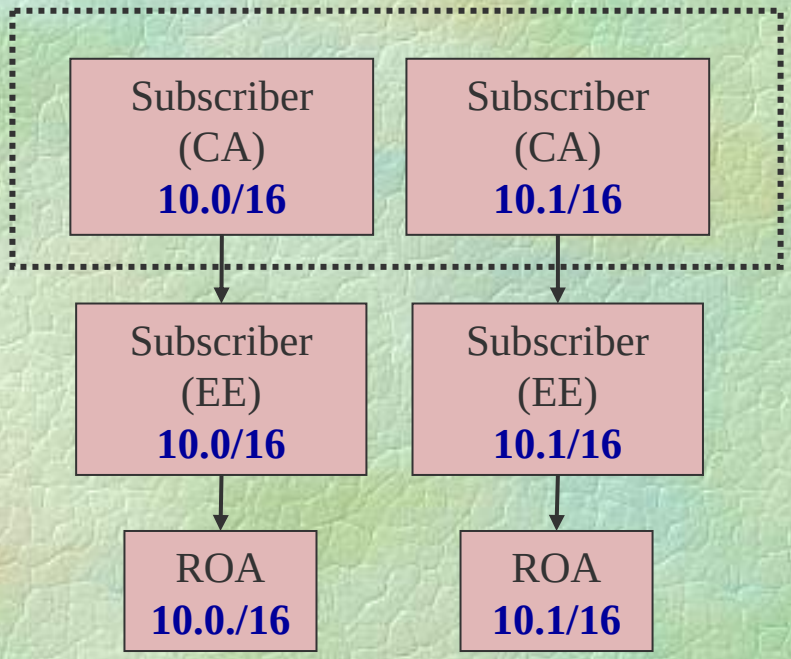
Matt Lepinski

BBN Technologies

Architecture Draft

- Nearing Completion --- Please Read!
- Changes in draft-ietf-sidr-arch-03
  - Replaced manifest specification with brief description and reference to draft-ietf-sidr-rpki-manifest
- Open Issues
  - draft-huston-sidr-repos-struct:
    - This needs to be a working group item!
  - Guidance for using ROAs to validate BGP UPDATES
    - Current text is inadequate
    - Cite draft-huston-roa-validation ?

ROA Format Draft: Key Open Issue



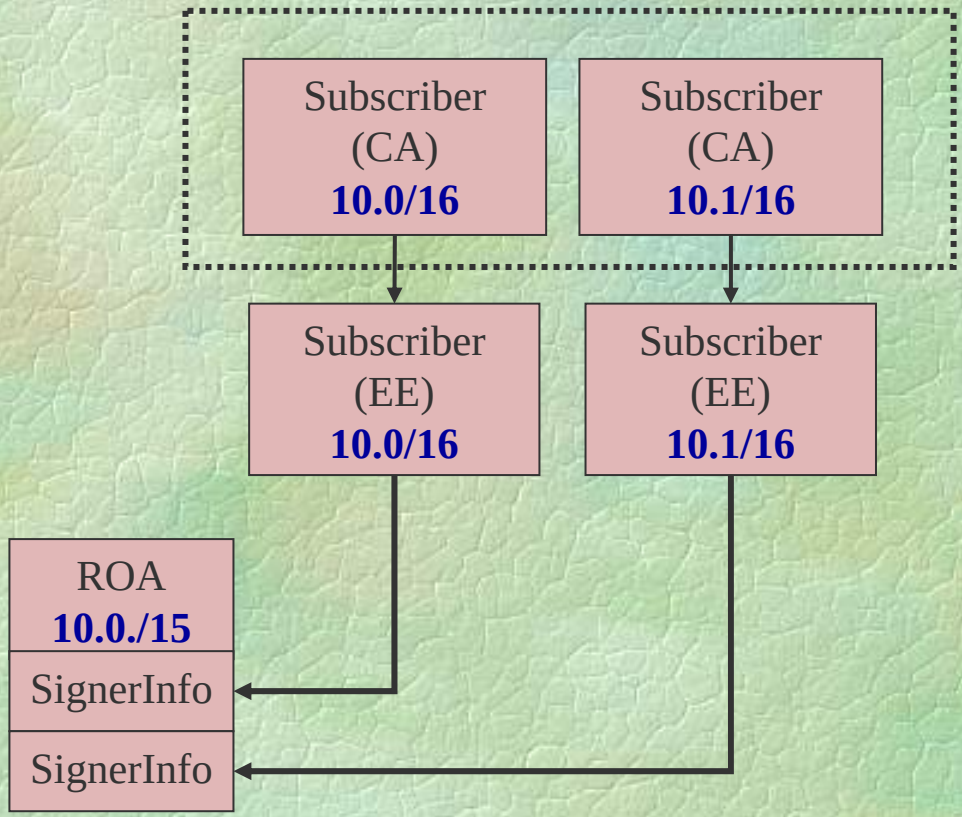
An ISP with two CA certificates

one for 10.0/16 and 10.1/16

cannot authorize the advertisement of 10.0/15

ROA Format Draft: Key Open Issue

- Proposed Solution
  - Allow multiple signatures on a ROA



ROA Format Draft: Key Open Issue

- Validity of ROAs with multiple signatures:
  - A ROA is valid if and only if:
    - The ROA complies with the syntax specification
    - EVERY signature on the ROA can be verified by a valid end-entity certificate
    - The union of the IP addresses in the end-entity certificates is EQUAL to the IP addresses in the ROA
  - All invalid ROAs are treated the same, regardless of whether or not they contain a verifiable signature

ROA Format Draft: Hash Functions

- Current draft specifies one MUST use SHA-256
- In the future, we may want to allow for use of another digest algorithm
- Possible migration approaches:
  - Issue duplicate ROAs
    (one for each digest algorithm)
  - Specify the ROA validation logic so that SignerInfo objects with unsupported digest algorithms are ignored

Thank You