Architecture
and
ROA Format

Matt Lepinski

BBN Technologies

Presentation Outline

❑ CP and CPS drafts

❑ Changes to architecture draft

❑ Open issue in ROA Format

❑ Questions

CP and CPS drafts

- Current Versions:
  - draft-ietf-sidr-cp-02
  - draft-ietf-sidr-cps-irs-02
  - draft-ietf-sidr-cps-isp-01

- No open issues, but need more review

Architecture Draft

- ❑ Changes in draft-ietf-sidr-arch-02
  - ◼ Example for use with private address space

  - ◼ Clarified scope: only IPv4 and IPv6 address families

  - ◼ Rewrite of manifest section
    (Note: Manifest section will be greatly condensed in -03)

- ❑ No open issues

ROA Format Draft

❑ No change to draft-ietf-sidr-roa-format-01

❑ Current version:
  ■ Exact match between ROA addresses and
    EE certificate RFC 3779 extension

  ■ Flag in ROA to format choose between
    • Exact match between ROA addresses and
      NLRI in route advertisement
    • NLRI in route advertisement may be more specific
      than IP address prefix in ROA

ROA Format Draft: Open Issue

❑ Current version:

    ■ Exact match between ROA addresses and EE certificate RFC 3779 extension

    ■ Flag in ROA to format choose between

        • Exact match between ROA addresses and NLRI in route advertisement

        • NLRI in route advertisement may be more specific than IP address prefix in ROA

ROA Format Draft: Open Issue

```
┌─────────────────────────────────────────────┐
:  ┌──────────────┐    ┌──────────────┐        :
:  │ Subscriber   │    │ Subscriber   │        :
:  │ (CA)         │    │ (CA)         │        :
:  │ 10.0/16      │    │ 10.1/16      │        :
:  └──────┬───────┘    └──────┬───────┘        :
└─────────│───────────────────│────────────────┘
          ▼                    ▼
   ┌──────────────┐    ┌──────────────┐
   │ Subscriber   │    │ Subscriber   │
   │ (shadow)     │    │ (shadow)     │
   │ 10.0/16      │    │ 10.1/16      │
   └──────┬───────┘    └──────┬───────┘
          ▼                    ▼
   ┌──────────────┐    ┌──────────────┐
   │ ROA          │    │ ROA          │
   │ 10.0./16     │    │ 10.1/16      │
   └──────────────┘    └──────────────┘
```
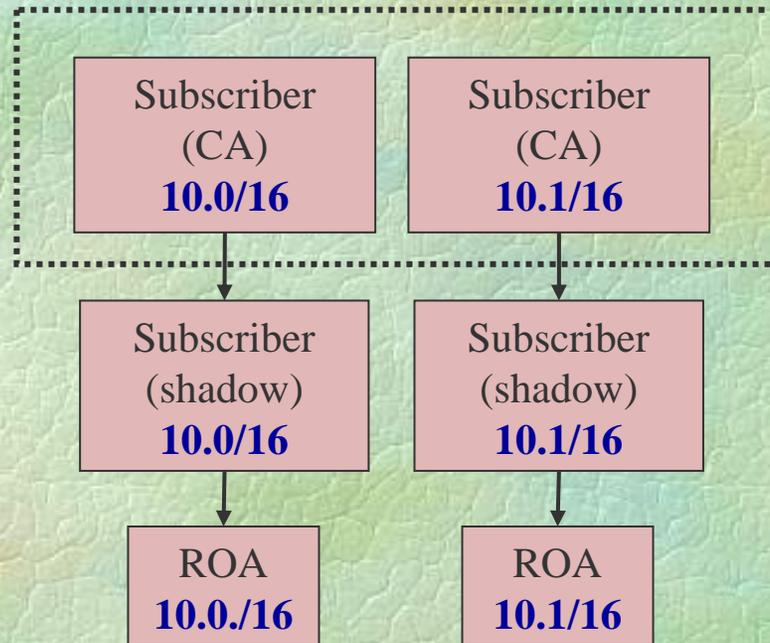
❑ An ISP with two CA certificates
  one for 10.0/16 and 10.1/16
  cannot authorize the advertisement of 10.0/15

ROA Format Draft: Open Issue

❑ Possible Resolutions

- ▪ This isn't a problem we need to address

  If the ISP wants to aggregate they must have an aggregate CA certificate

- ▪ Allow multiple signatures on a ROA

- ▪ Change the algorithm for matching ROAs to route advertisements to allow matching a less specific prefix.

Questions