ROA Format

Matt Lepinski
BBN Technologies

Changes since -02

- The EE certificate used to verify a ROA MUST be included in the CMS wrapper of the ROA.
- The signed attributes ContentType and MessageDigest MUST be included in the CMS wrapper for the ROA, other signed attributes may be included.
- As proposed in Philidelphia, the syntax of the ROA was changed to allow the issuer to authorize the advertisement of prefixes up to a given maxLength.

Format Change: maxLength

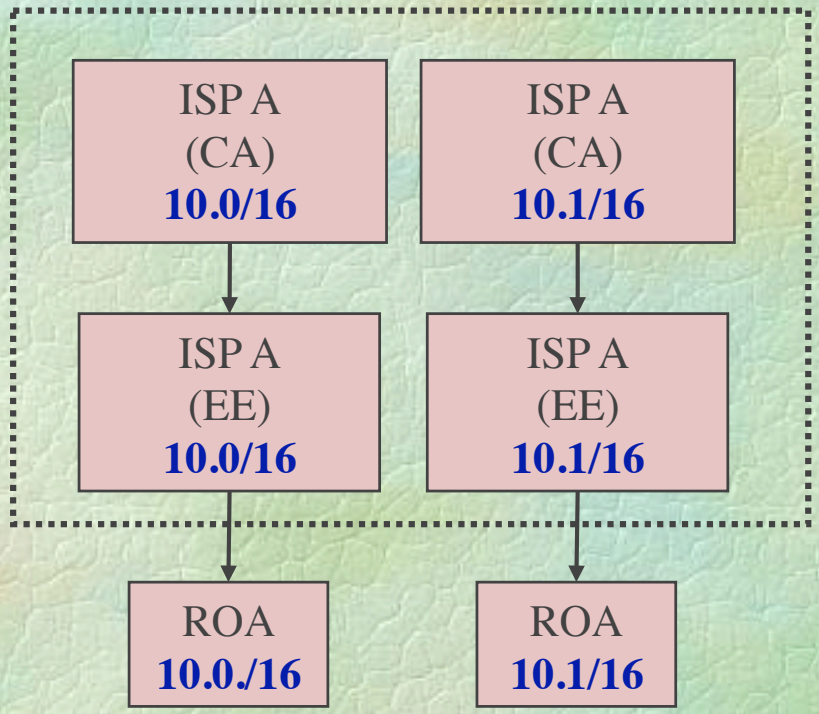
```
RouteOriginAttestation ::= SEQUENCE {
        version [0] INTEGER DEFAULT 0,
        asID  ASID,
        ipAddrBlocks SEQUENCE OF ROAIPAddressFamily
}
ROAIPAddressFamily ::= SEQUENCE {
        addressFamily OCTET STRING (SIZE (2..3)),
        addresses SEQUENCE OF ROAIPAddress
}
ROAIPAddress ::= SEQUENCE {
        address IPAdress,
        maxLength INTEGER OPTIONAL
}
```

Open Issue: Equivalence of ROAs

- The following ROA prefixes are logically equivalent
  - 10.0/15-16, 192.168/16
  - 10.1/16, 192.168/16, 10.0/15-16
  - 10.0/15, 10.0/16, 10.1/16, 192.168/16
- Question: Should we mandate a "canonical" choice among equivalent ROAs?
- Goals:
  - Make comparing ROA prefixes and RFC 3779 prefixes as easy as possible
  - Allow one to easily determine if two ROAs are logically equivalent?

    [Is there a need for this?]
- Strawman: Compress to as few prefixes as possible, then sort as per RFC 3779 (ignoring maxLength)

Open Issue: Multiple Signatures



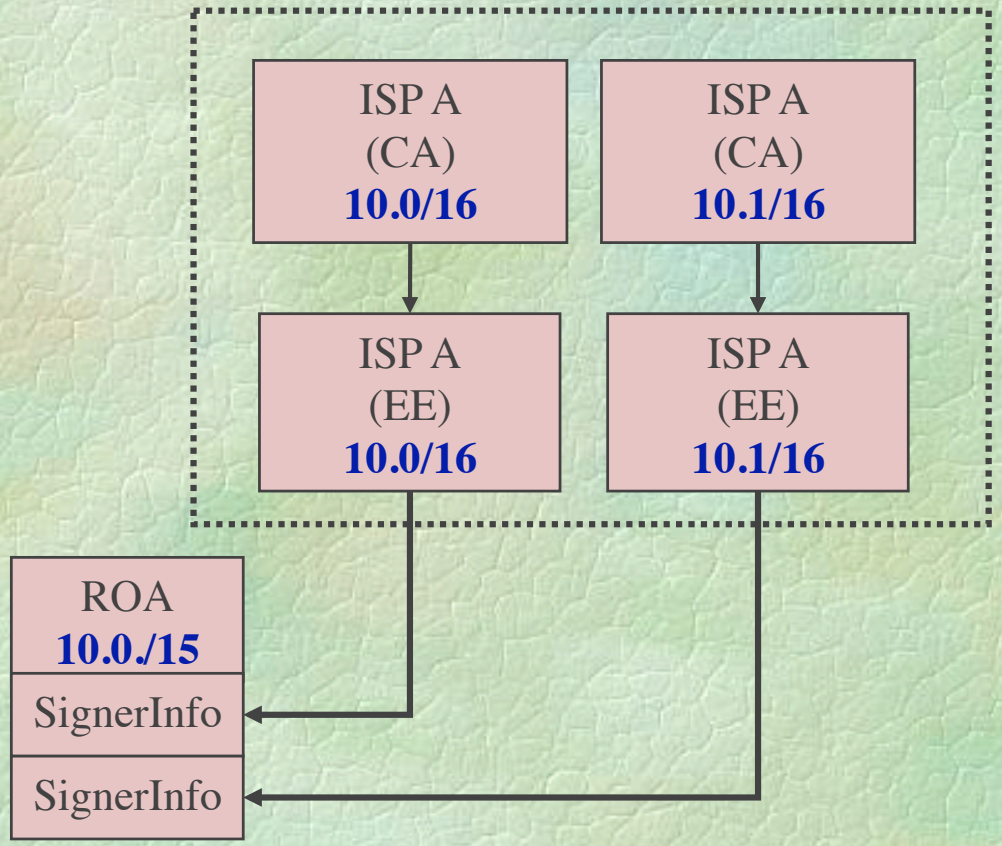
A single ISP with two CA certificates

one for 10.0/16 and 10.1/16

cannot authorize the advertisement of 10.0/15

Open Issue: Multiple Signatures

- Proposed Solution
  - Allow multiple signatures on a ROA



Open Issue: Multiple Signatures

- 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

Thank You