The -bis goals:

- Clarify the requirements for presence/absence of *IP Address and AS Identifiers* X.509 certificate extensions
- Strengthening of the ASN.1 formal notation
- Incorporate all Verified Errata
- Provide an example of ROA payload
- Improve readability
- Maintain full compatibility with what’s deployed
IP Address and AS Identifiers X.509 certificate extensions in ROA EEs

• All ROAIPAddress entries must be contained by the IP Address certificate extension.

• On the other hand, the ASID is an arbitrary value set by the IP Address resource holder.

• Documenting that the AS Identifiers extension MUST NOT be present, aids future developers in understanding the ASID does not need to be contained in the certificate chain.
Feasibility of disallowing AS Identifiers

- There are 0 (zero) ROAs in the wild (out of 143,098 ROAs) that contain an AS Identifiers extension in their EE certificate (27-Mar-2023)
- No known Open source CA implementations set the extension in ROA EEs.
- Open source RP implementations either ignore the presence of the extension, or mark the ROA as invalid (if it were present).
Strengthening the ASN.1 notation

RouteOriginAttestation ::= SEQUENCE {
    version [0] INTEGER DEFAULT 0,
    asID ASID,
    ipAddrBlocks SEQUENCE [- (SIZE (1..MAX)) - ] {+(SIZE (1..2))}+ OF ROAIPAddressFamily
}

ASID ::= INTEGER {+(0..4294967295)+}

ROAIPAddressFamily ::= SEQUENCE {
    addressFamily OCTET STRING [-(SIZE (2..3)), - ] {+(SIZE (2)), +}
    addresses SEQUENCE (SIZE (1..MAX)) OF ROAIPAddress
}

ROAIPAddress ::= SEQUENCE {
    address IPAddress,
    maxLength INTEGER {+(0..128)+} OPTIONAL
}

IPAddress ::= BIT STRING {+(SIZE (0..128))}+

!!!100% compatible with every published ROA!!!
Incorporating Verified Errata

- **Errata 3166**: EE certificate MUST NOT use “inherit” element
- **Errata 5881**: missing id-ct-routeOriginAuthz Object Identifier in ASN.1 notation
- **Errata 5609**: Table of Contents missing IANA Considerations entry
Appendix B. Example ROA eContent Payload

Below an example of a DER encoded ROA eContent is provided with annotation following the '# character.'

```bash
$ echo 302402023CCA301E301C04020002301630090307002001067C208C30090307002A0EB24000000 \
| xxd -r -ps \
| openssl asn1parse -i -dump -inform DER
0:d=0 hl=2 l= 36 cons: SEQUENCE
  2:d=1 hl=2 l=  2 prim: INTEGER           :3CCA  # asID 15562
  6:d=1 hl=2 l= 30 cons: SEQUENCE
  8:d=2 hl=2 l= 28 cons: SEQUENCE
10:d=3 hl=2 l=  2 prim: OCTET STRING
   0000 - 00 02
14:d=3 hl=2 l= 22 cons: SEQUENCE
16:d=4 hl=2 l=  9 cons: SEQUENCE
18:d=5 hl=2 l=  7 prim: BIT STRING
   0000 - 00 20 01 06 7c 20 8c ...
27:d=4 hl=2 l=  9 cons: SEQUENCE
29:d=5 hl=2 l=  7 prim: BIT STRING
   0000 - 00 2a 0e b2 40 ..@  # 2a0e:b240::/48
0007 - <SPACES/NULS>
```

# RouteOriginAttestation
# ipAddrBlocks
# ROAIPAddressFamily
# addressFamily
# IPv6
# addresses
# ROAIPAddress
# address
# 2001:67c:208c::/48
# ROAIPAddress
# address
# 2a0e:b240::/48
Working Group Last Call?

Please email feedback to

sidrops@ietf.org, or
draft-ietf-sidrops-rfc6482bis@ietf.org

or, open issues at

https://github.com/job/draft-rfc6482bis