

ROA Content Proposal

November 2006

Geoff Huston

EE Resource Certificates

- End Entity (no-CA) Certificates used as one-off ROA signing certificates
 - EE cert can be used for a single-use ROA signing
 - Private key is destroyed after a single use
 - EE Cert SIA is a pointer to the object that has been signed with the corresponding private key
 - ROA validity and resource attributes are controlled by the associated EE certificate(s)

What Information is required for a ROA?

1. Originating AS
2. IP Address Set
3. Period of the Authority (Start & End Times)
4. Information to allow a relying party to validate that:
 - The address set is valid
 - The ROA was generated by the address holder
 - The ROA has not been altered
 - The ROA is valid

What Information is required for a ROA?

1. Originating AS
In the ROA
2. IP Address Set
In the EE Cert (or in the ROA?)
3. Period of the Authority (Start & End Times)
In the EE Cert
4. Information to allow a relying party to validate that:
 - The address set is valid
 - The ROA was generated by the address holder
 - The ROA has not been altered
 - The ROA is validIn the EE Cert, plus a Trust Anchor set

ROA Template (1)

ROA Contents:

1. AS Number
2. Address Resource Set
3. Signature(s) across the join of items 1 + 2
4. Pointers to EE Cert(s)

Alternate ROA Template (2)

ROA Contents:

1. AS Number
2. Pointers (URLs) of EE Cert(s)
3. Signature(s) across the join of items 1 + 2

Alternate ROA Template (3)

ROA Contents:

1. AS Number
2. EE Cert(s)
3. Signature(s) across the join of items 1 + 2

Alternate ROA Template (4)

ROA Contents:

1. AS Number
2. Hash(es) of EE Cert(s)
3. Signature(s) across the join of items 1 + 2