Res Certs Changes
draft-ietf-sidr-res-certs-05.txt

Sandy Murphy

Sparta, Inc

Geoff’s Summary

- The only change was to 3.9.7 where the SIA field was augmented with an id-ad, allowing a end entity certificate to reference thepublication point of object(s) that have been signed with the key set of which the public key is referneced in the end entity certificate.

  In the context of secure BGP architectures this allows ROAs and potentially other forms of signed objects to be distributed by mechanisms other than BGP itself, and allow third parties to validate BGP information without having to make changes to BGP.

My understanding of other changes

- Based only on the diffs of the latest version to the -02 version
- I’ve left out wording changes

From the “diffs” – overlapping resources

- Removed restriction that two certs issued by same CA can not cover the same resources
- Previous language would complicate/prevent ISP from issuing ROAs for portions of its own space that it had sub-allocated
  - Have /18, suballocate /20
  - Probably still want to be able to originate routes for the /20, for traffic engineering, etc.

From the “diffs” – changes to crypto

- Previous language said “MUST be SHA-256”
- Now says “minimum of SHA-256, may also be SHA-384 or SHA-512”
- Reason: future agility

From the “diffs” – access form URIs

- Previous language said RSYNC must be present
- Now says other access form URIs may be used
  - Regularizes references to access forms

From the “diffs” – AIA vs reissued certs

- Previous language did not refer to reissuance of a CA cert
  - Problem is that the CA’s subordinate certs refer to point of publication of the CA’s cert in AIA field
  - Don’t want to have to reissue all subordinate certs if CA cert is reissued
- New language suggests SHOULD use persistent URL for CA cert
  - Or have subject keep superior’s current cert in its own publication space and have AIA point to that

From the “diffs” – AIA field

- Previous language said AIA field is assigned by CA and MUST be omitted from the request
- New language says it MAY be omitted, and the CA MAY choose what is specified if one is supplied (see change about subject keeping superior’s cert in its own publication space – subject needs to specify AIA)