BGPsec CSR & Certificate Issuance

20140725

IETF 90 – SIDR WG

Sean Turner – turners@iea.com

What's this about?

- Determining, finally, what goes in the subject field of a BGPsec speaker's certificate.
- Specification alignment.

What do we want in the end?

- Need to validate BGPsec signer's signature.
- The public key needed to perform this signature validation is NOT included in BGPsec message, and should not be for obvious security reasons.
- Instead it is located by matching the AS Number and SKI in BGPsec message to BGPsec signer's certificate in RPKI.

How does this data get in the cert?

- CSRs: BGPSEC supports two key generation methods: on-router and off-router.
  - On-router key generation means router generates PKCS #10, since whole point of on-router is that private key never leaves router.
  - Off-router key generation…don't much care whether PKCS #10 is generated on-router or off-router.
- Remember – the CA is always the final arbiter about what gets certified (i.e., what is actually included in the signed certificate).

Want a unified interface for the CA.

The Catch: Multiple ASNs in Cert.

- Without an honest to goodness hack job the subject field only supports including one ASN.
- Options to include more than one ASN:
  - AS Resource Identifier Extension
  - Don’t go there.

Specification Alignment

What’s in CSR’s subject field?

- RFC 6487 indicates:
  - [Subject] field MAY be omitted …
  - If present, the value of this field SHOULD be empty (i.e., NULL) …
  - This field is allowed to be non-empty only for a re-key/reissuance request …
- RFC 2986 (aka PKCS#10):

```
version INTEGER { v1(0) } (v1,...),
subject Name,
subjectPKInfo SubjectPublicKeyInfo{{PKInfoAlgorithms}},
```

- subject can’t be omitted but it can be NULL

Changes Needed

- RFC 6487:
  - OLD: This field MAY be omitted. If present, the value of this field SHOULD be empty (i.e., NULL)
  - NEW: This field SHOULD be empty (i.e., NULL)
  - Remains: in which case the CA MUST generate a subject name that is unique in the context of certificates issued by this CA.
- draft-ietf-sidr-bgpsec-pki-profiles:
  - Sec 3.2: Allow non-NULL subject names in CSR