draft-ietf-sidr-bgpsec-pki-profiles-00
draft-ietf-sidr-bgpsec-algs-00

Sean Turner
Mark Reynolds
Steve Kent

IETF 82 – SIDR WG

Why do we even need these?

- BGPSEC has some refined requirements compared to draft-ietf-sidr-res-certs.
- Want to guarantee that BGPSEC has ***NO – NONE - NADA*** impact on RPKI relying parties compliant with draft-ietf-sidr-res-certs.

PKI Profiles Differences

- Subject Names (RECOMMENDED)
  - cn = "BGPSEC-" + 32-bit AS Number (hex)
    sn = 32-bit BGP Identifier
  - Identifies the router that speaks BGPSEC
- Subject Public Key Info
  - More on this later
- Added BGPSEC EKU
  - It's non-critical as per draft-ietf-sidr-res-certs
  - Wanted a surefire way for RPs to know this is a BGPSEC certificate

PKI Profiles Differences

- Subject Information Access
  - Omitted
  - The things verified with these certificate are data in BGPSEC Update messages. Thus, the SIA extension, which is used in the RPKI to point to repository data that is verified using the cert, is not relevant here.
- IP Resources
  - Omitted
  - BGPSEC certificates are all about AS numbers
- AS Resource Identifier Delegation
  - MUST be present
  - BGPSEC certificates are all about AS numbers

Algorithm Similarities & Differences

- Things that haven't changed:
  - Algorithm used to sign BGPSEC certificate
  - Algorithm used to sign CRLs in which revoked BGPSEC certificate serial numbers would appear
- BGPSEC uses ECDSA (on p-256) with SHA-256
  - Subject Public Key Information - from RFC 5480
  - Signature value in *BGPSEC* and Certificate Request is different - from RFC 3279
- Why?
  - Signatures, keys, and certificates all smaller

Impact on sidr-algorithm-agility?

- NO! (your eyes are not deceiving you)
- BGPSEC certificates are end-entity certificates.
- sidr-algorithm-agility is about CA key rollovers.
- So … the answer is still no.

Impact on draft-ietf-sidr-res-certs RPs?

- Still – none…
- The changed fields in these certificates would not be processed by the RP
- ECDSA key would not be used by the RP, because it is not needed to verify any data that the RP will ever see
- The lack of an SIA is not an issue, because there is no subordinate data to validate using this EE cert