Request to SIDROPS

Sandy Murphy, Chris Morrow
SIDR co-chairs

Router Keying for BGPsec

- draft-ietf-sidr-rtr-keying-14
- In answer to a request to sidr from operator for advice of how to get public/private keys and certs into routers
- Went to wglc
- Got one review, addressed same
- Got a second review
- Need review of comments

e.g., Substance

- Like:
- Requirement for validation that cert's public key corresponds to private key – how is correspondence validated? also done at router?
- Is the case of a router that has multiple ASNs (multiple private keys) included? How does router choose key + cert to use for which BGPsec session?
- Does router need to validate cert matches an AS it is configured to use?

e.g., Process

- Draft is standards track with few of the usual MUSTs
  - Is this draft intended to be the standard way to do keying? A recommended way? One good way?
  - If a standard, is there more of the text that should be mandatory?

e.g., Clarity

- Section 8 and "key material"
- Section 7 – last two paragraphs
- Discussion of choice of security services in PKCS#8, PKCS#7, protected channel, etc
- Operator overloaded term (beating heart, organization, AS, management station, etc.) ☺
- Mostly a matter of editing, rather than determining wg intent

Request

- Please comment
- On the draft
- There has to be something in there you have an opinion on.