Securing RPSL Objects with RPKI Signatures draft-ietf-sidr-rpsl-sig-03

Robert Kisteleki
robert@ripe.net

IETF78, Maastricht

Recap

```
inetnum:        193.0.0.0 - 193.0.7.255
netname:        RIPE-NCC
descr:          RIPE Network Coordination Centre
descr:          Amsterdam, Netherlands
remarks:        Used for RIPE NCC infrastructure.
country:        NL
admin-c:        AMR68-RIPE
admin-c:        BRD-RIPE
tech-c:         OPS4-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-MNT
mnt-lower:      RIPE-NCC-MNT
source:         RIPE
changed:        bit-bucket@ripe.net 20060221
```

Recap

```
inetnum:        193.0.0.0 - 193.0.7.255
netname:        RIPE-NCC
descr:          RIPE Network Coordination Centre
descr:          Amsterdam, Netherlands
remarks:        Used for RIPE NCC infrastructure.
country:        NL
admin-c:        AMR68-RIPE
admin-c:        BRD-RIPE
tech-c:         OPS4-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-MNT
mnt-lower:      RIPE-NCC-MNT
source:         RIPE
changed:        bit-bucket@ripe.net 20060221
signature:      v=1; c=rsync://.../...X.cer; m=sha256WithRSAEncryption;
   t=1234567890; a=inetnum+netname+country+status; b=bZbZbZ1iobnjc3i1fe...
```

Feedback, editing

- Lots of corrections / clarifications from Steve

Changes in -03

- New co-editor: Brian Haberman
- Significant re-shuffling of sections
  - Content is much more logically laid out
  - Structure is easier to follow
- Many wording changes, corrected grammar

Changes in -03

- Introduction now provides better rationale for signing RPSL objects
- Terminology: normalization -> canonicalization
- Signed attributes are of a set of mandatory + optional attributes

Changes in -03

- Better c14n rules
  - For c14ing ASN, IPv4 and IPv6 resources
  - For dates
  - For RPSL layout
- C14n now achieves resiliency regarding formatting changes

Changes in -03

- Other changes
  - Signature creation / verification is more algorithm-independent
  - Removed decision points (question marks)
  - Clarification on validity time in case of multiple signatures
- Defined which resources (mentioned in the object) should be covered by the RFC3779 extension of the certificate

Questions?