

# Securing RPSL Objects with RPKI Signatures draft-ietf-sidr-rpsl-sig-02

Robert Kisteleki  
robert@ripe.net

IETF77, Anaheim

# 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=bZbZbZ1iobnjc3ilfe...
```

# Changes in -02

- Switch to sidr-rpki-algs for specifying the possible signature algorithms
- The list of signed attributes per object type is now explicitly specified, the signer can no longer choose additional attributes they want to sign
- Minor language changes

# Feedback, editing

- Lots of corrections / clarifications from Steve, still processing them
- Not much from anyone else recently

## Authorship:

- Looking for co-author(s)

Questions?