RPSL + RPKI
Just a Heads Up

Robert Kisteleki

You know this already

```
aut-num:        AS3333

as-name:        RIPE-NCC-AS

descr:          Reseaux IP Europeens Network Coordination Centre (RIPE NCC)

org:            ORG-RIEN1-RIPE

import:         …

export:         …

admin-c:        …

status:         ASSIGNED

mnt-by:         …

created:        2002-08-13T12:58:13Z

last-modified:  2015-05-05T04:26:20Z

source:         RIPE
```

- Assuming that:
  - You know what RPKI is
  - You are participating in it and got your resources certified (e.g. by the RIPE NCC)
- This mechanism would allow you to put RPKI to good use by signing your RPSL objects
  - So the contents can be verified even outside the RIPE Database
  - Meaning "the legitimate resource holder declares the following"
- Using a DKIM-style approach
- Here's how…

You know this already

```
aut-num:        AS3333

as-name:        RIPE-NCC-AS

descr:          Reseaux IP Europeens Network Coordination Centre (RIPE NCC)

org:            ORG-RIEN1-RIPE

import:         …

export:         …

admin-c:        …

status:         ASSIGNED

mnt-by:         …

created:        2002-08-13

signature:      v=1; c=rsync://.....; m=sha256WithRSAEncryption; t=9999999999;

                a=aut-num+as-name+descr+import+export; b=<base64 data>

source:         RIPE
```

RIPE NCC

Further notes

- This is applicable to inetnum, aut-num, route…
    - Objects that have resources as primary key
    - Multiple signatures could be used for route objects
    - For other objects a single signature is fine
- It's not meant to replace RPSS but can be used in combination with it
- Can be used in the context of the previously mentioned "Cross-registry Authentication for IRR Data" topic, or independently from it
- Interested? Search for "sidr rpsl-sig" to learn more

RIPE
NCC

Questions?