Resource Certification

Robert Kisteleki

CISSP, science group manager
RIPE NCC

robert@ripe.net

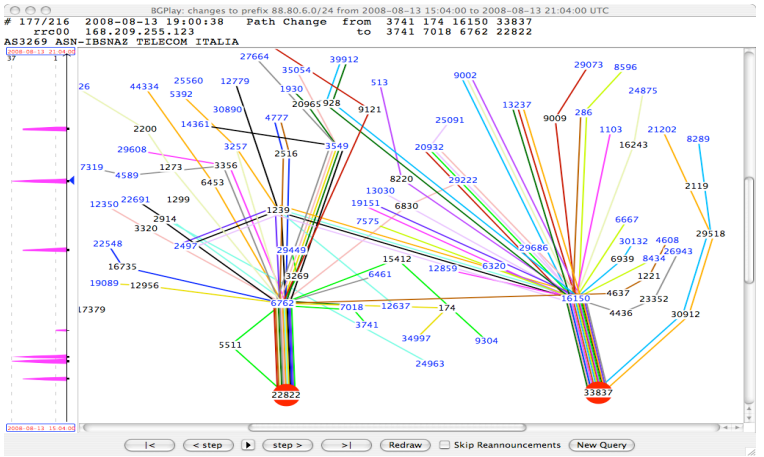
Contents

- Motivation for Resource Certification (RPKI)
- Architecture overview
- Participating in RPKI
- Most importantly: use cases
- Status update

Motivation

Why is the RIPE NCC pursuing RPKI?

- Allow better route filtering, preparations for secure routing
  - See recent IP hijacks (YouTube, The PirateBay, I-root)
  - Solve the chicken-and-egg problem
- There is increasing interest in trusted data
- Post IPv4 exhaustion data accuracy
  - See resource transfers



Overview

Goal:

- Mirror the way of existing resource delegation
- Issue x.509 certificates along with the assignment or allocation of Internet number resources
- The holder of the certificate can prove its right to use that resource by signing some data “with the certificate”
- Works on all levels of resource delegation
  - (IANA ->) RIR -> LIR -> ISP -> customer

Overview

An RPKI certificate:

Pointer to issuer (AIA):	rsync://…/….cer
Pointer to own repository (SIA):	rsync://…/…/
Public key information:	…
Issuer name:	RIPE
Subject name:	Zt4bwert234gfQ
Resources:	193/16
	AS99999
Issuer's signature	

Important: this is **not** an identity certificate!

Participating in RPKI

Internet Registries can:

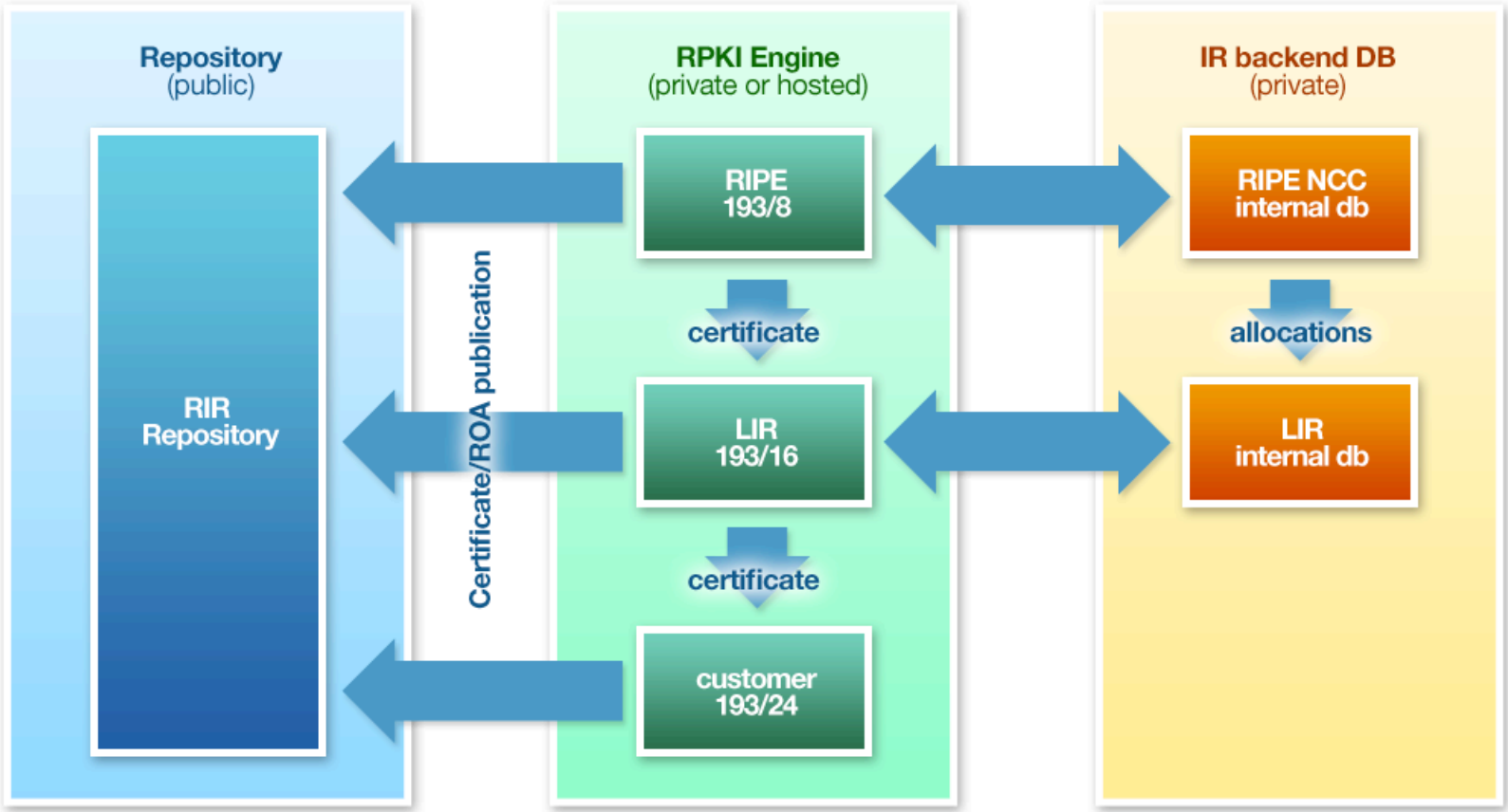
- Receive their certificates from their “upstreams”
- Issue certificates to their clients (or themselves)
- Sign data with operative content using their own certificates

It’s not a trivial task:

- Manage multiple “upstreams” / “downstreams”
- Manage key and certificate lifecycle (multiple CAs, key rollovers, revocations, …)
- It should require as little manual work as possible

Participating in RPKI

Enter the “RPKI Engine”:



Participating in RPKI

In order to participate in RPKI, an IR needs:

- RPKI engine software and an infrastructure to run it
- On the higher levels: Hardware Security Module(s)
- Good back-end database of resource delegations
- Mandatory documents:
  - Certificate Policy
  - Certification Practice Statement

The NCC intends to help LIRs with most of these as services!

Services for RPKI

Intended RIPE NCC services for LIRs:

- Certify LIR resources using the NCC's own RPKIE
- Provide hosted RPKI services for LIRs:
  - Run the LIR's RPKI Engine & give real control to the LIR
  - Provide the necessary public repository
- Access to these services:
  - Planned through the normal channels (ie. LIR portal)
  - But likely with enhanced (strong) authentication

Services for RPKI

Potential, related services:

- central cache for certificates (repository collection)
- certificate validation
- object validation
- repository service
- others?

Certificate uses, operational interests

Some use cases:

- ROAs - against hijacks
- enabling S*BGP
  - against "Revealed: The Internet's Biggest Security Hole”
- Customer sign-up
- Help with transfers (live and/or non-live networks)
- Potential service: ROA2RPSL
- RPSLSIG
- Bogon filtering - BOAs?

Certificate uses, operational interests

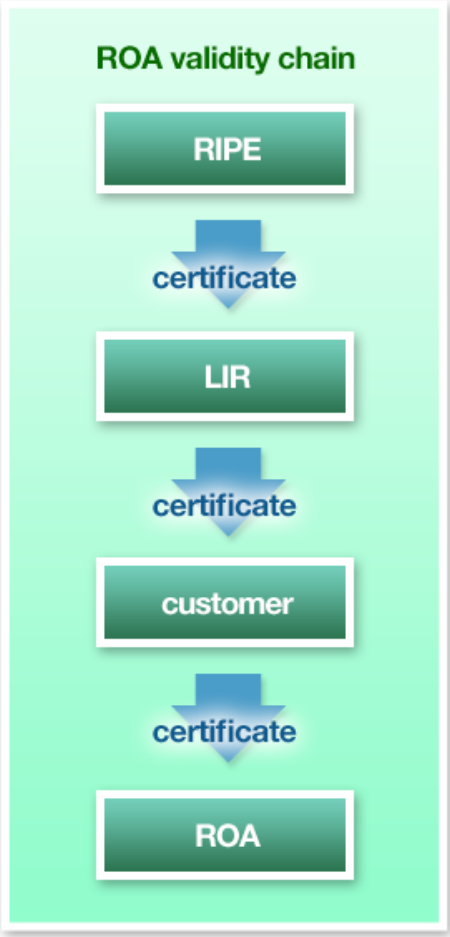
ROA – Route Origination Authorization

- Using my certificate covering a prefix, I can formally, verifiably authorize an AS to announce that prefix
- It does not mean that the AS will actually announce that prefix!
  - It's a unilateral statement
  - Not equivalent to an IRR route[6] object
  - Can be useful for constructing route filters
  - At a later stage (some form of) this can be in *BGP

Certificate uses, operational interests

ROA – Route Origination Authorization

Prefix:	10.0.0.8/8
Authorised AS:	AS99999
Signer certificate:	rsync://…/….cer
Valid from:	2008-05-01T08:00:00Z
Valid until:	2009-05-01T08:00:00Z
Prefix holder's signature	



Certificate uses, operational interests

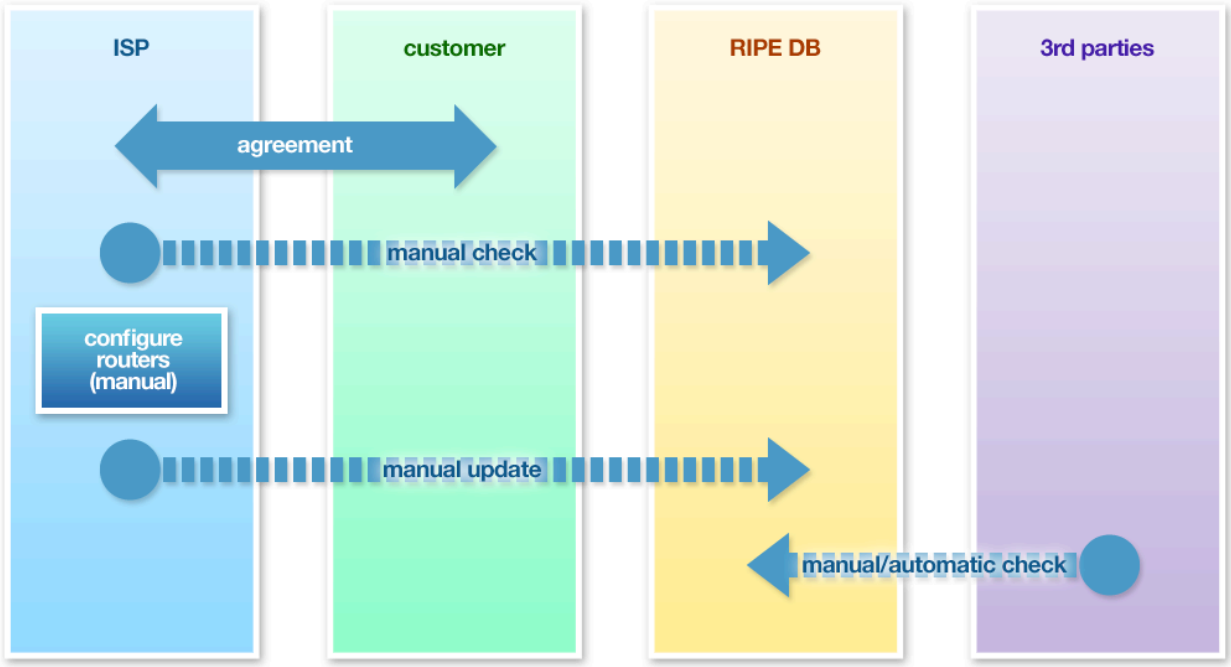
A note on sBGP

- sBGP uses a hierarchical CA model – just as RPKI
- RPKI certificates could be used with sBGP:
  - sBGP Origin Authentication (OA) ~ RPKI ROA
  - Route Attestation (RA) is possible as peers can have certificates proving they control a specific AS
- It's still a long way from here…

Certificate uses, operational interests

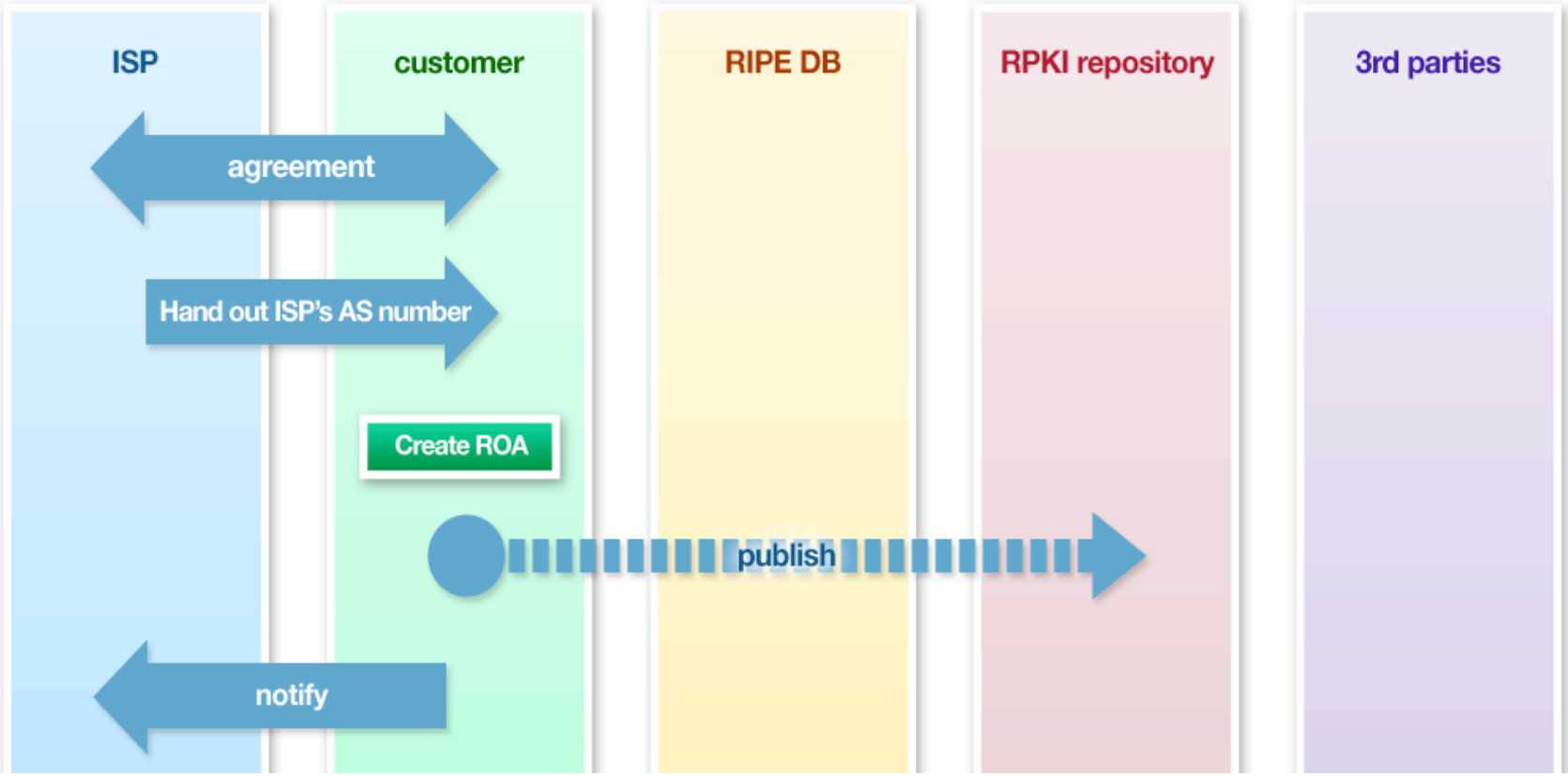
Customer sign-up – without RPKI

- Suppose you have a potential customer
- How do you verify their claim over a resource?



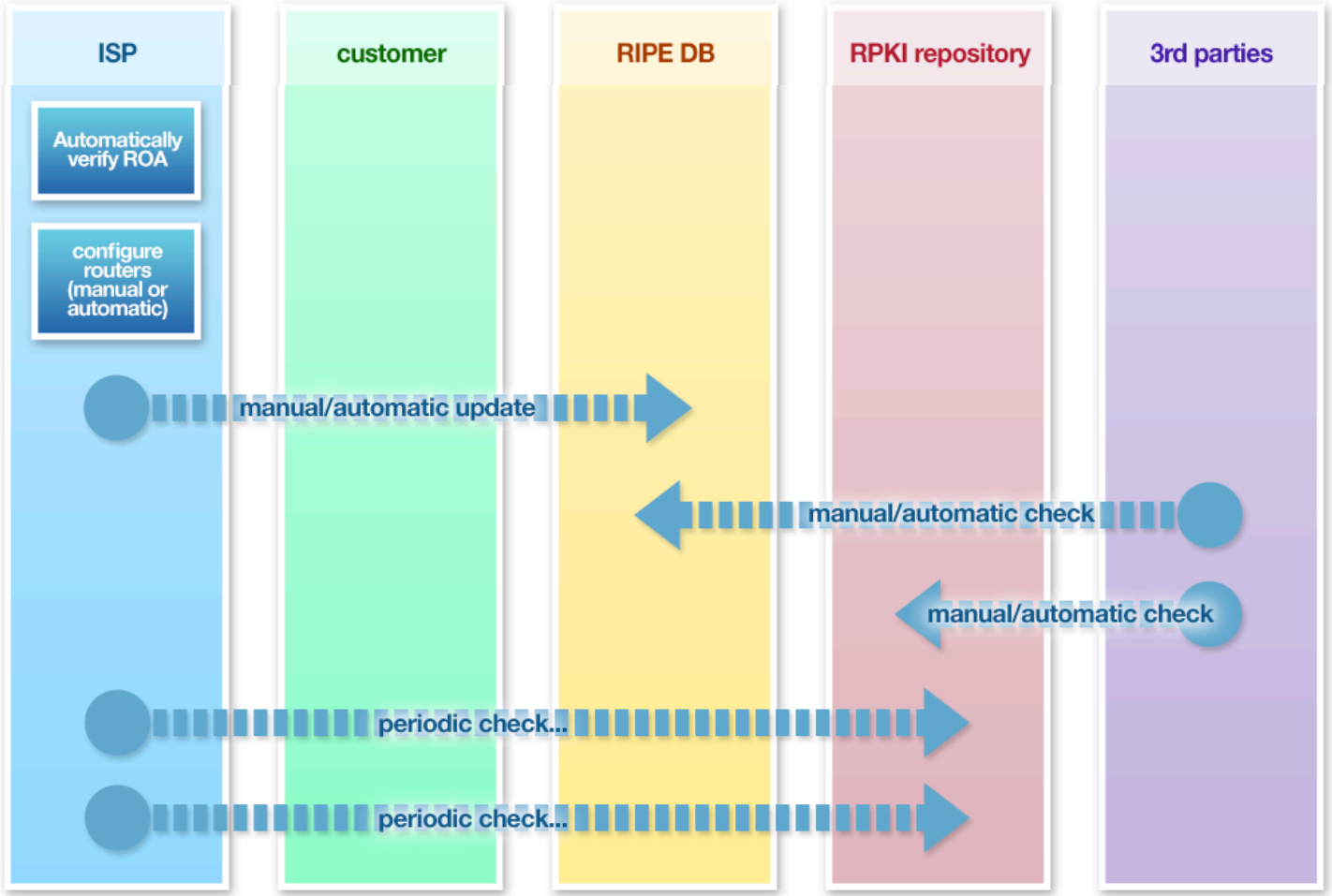
Certificate uses, operational interests

Customer sign-up – with RPKI (1)



Certificate uses, operational interests

Customer sign-up – with RPKI (2)



Certificate uses, operational interests

Resource transfers (live and/or non-live networks):

- Suppose that a resource is about to change hands
  - The sending and receiving party can mutually sign an electronic agreement using RPKI objects
  - Verification of such a document is almost trivial
  - After manual checks over policy / legal / etc. aspects, the receiving party's resources are extended with the new resource
  - The receiving party can now issue ROAs, physical network transfer can now be done
  - After network transfer, the resource is revoked from the sender's certificate(s)

Certificate uses, operational interests

Potential service: ROA2RPSL

- Originally Ruediger Volk's idea
  - Collect all valid ROAs from around the globe
  - Unwrap content and publish it in a new IRR-like database
    - Do this regularly (eg. every day) and make the results public
  - Operators can use data from the new, more trusted IRR without changing their tools!
  - Caveat: ROAs and IRR route objects are semantically different!
- Meant as a temporary service until there's takeup of ROAs and/or RPKI in general.

Certificate uses, operational interests

Combining RPKI and RPSL: RPSL Signatures

- General idea: use RPKI to sign RPSL objects “natively”, by extending RPSL syntax
- It could raise the trust level of RPSL data by providing “object security” as an addition
- Especially handy when there’s no channel security
- It can survive transfers of objects between IRRs
- For example:
  - Prefix and AS holder both sign a route object, thereby expressing their agreement on it.

Certificate uses, operational interests

Combining RPKI and RPSL: RPSLSIG

An example:

```
route:      193.32.254.0/24
descr:      Marks and Spencer
origin:     AS2856
mnt-by:     BTNET-MNT
signature:  v=1;c=rsync://…/….cer; m=sha1-
  rsa;t=2009-03-01T10:31:02T;a=route+descr+origin+mnt-
  by; b=324kjndfg9083GAD4sEW32…
signature:  v=1;c=rsync://…/….cer; m=sha1-
  rsa;t=2009-03-02T11:11:01T;a=route+descr+origin+mnt-
  by; b=9ds3D4sW3234tj11wdhuon…
source:     RIPE
```

Who to trust?

Remember:

- In any PKI (including RPKI) it's ultimately the relying party's choice who they use as Trust Anchors ("root CAs")
- For RPKI, RIRs are a natural choice
  - But just as every other party, RIRs will only certify what **they** allocate/assign
  - Everyone will probably use multiple TAs
- IANA can also be a single (or an additional) TA if/ when they join in

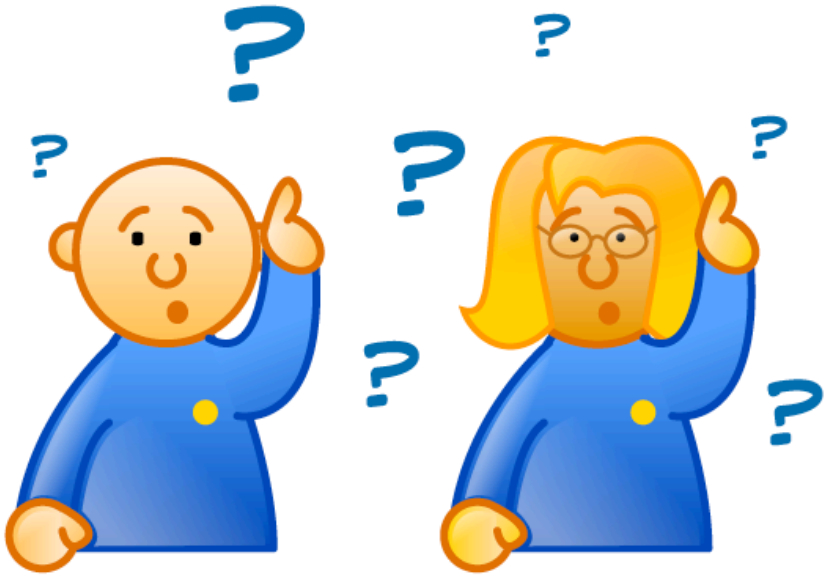
RPKI activities

- The “inter-RIR RPKI design team” is practically finished working.
- Protocol work is still being done at IETF SIDR WG
- Most RIR’s are at various stages of implementation
- As for RIPE NCC:
  - Certification Task Force is there to advise the NCC
    - Expect a “RIPE resource certification policy” proposal soon!
  - Implementation of hosted RPKI Engines is under way
  - We invite you to participate in testing the system as it is being developed, so you can have a sneak peek and give feedback on what you’d like to have!

Summary

Resource certification (RPKI):

- It is coming to an IR near you
- It is meant to work with little operational overhead
- The RIPE NCC is preparing for it, with active involvement and support from the community
- It is meant to help operators mainly in
  - Determining legitimacy of resource holdership
  - Securing routing configurations



Questions?