RPKI Deployment with IXPs

Rapporteur: Matthias Wählisch <m.waehlisch@fu-berlin.de>
Internet Exchange Points interconnect ...
The problem of outsourcing security?

• Route servers are vital at IXPs
• IXP members send BGP updates to route server
• Route server distributes BGP update to members

If you care about Internet security

1. Either you deploy route origin validation++ on your own
   If you don’t do, you cannot verify the route server stream ...

2. Or you trust the route server
   Then you benefit from origin validation by route server
Four options how IXPs get *(not)* involved into RPKI

- Do nothing
- Provide RPKI Cache
- Tagging
- Filtering

draft-ietf-sidrops-route-server-rpki-light
Validation, tagging, and filtering of invalids – cool stuff!

Legacy route server (as of Oct 20, 2017)
757 v4 peers, 614 v6 peers
opt-out filtering

Falcon route server
201 v4 peers, 160 v6 peers
opt-in filtering

Route server
111 peers
filtering
Cache server, validation, tagging, and opt-out filtering of invalids (to come) – cool stuff!

“Currently we only tag routes based on (IRR and) RPKI Validation, but we had a survey with our members and they voted to enable route filtering by default on ‘invalid ROA’ and ‘IRR not found’ states. We plan to deploy filtering by default by the end of the year.” [Arnaud Fenioux, 2017]
Validation, tagging

NAP Ecuador
Public caches @

- bknix
- INX
- nap1
- INAP
Considering RPKI in the future
Thanks!

Randy Bush, Arnaud Fenioux, Aris Lambrianidis, Carlos Marcelo Martinez Cagnazzo, Tim Bruijnzeels, …
November 14, 2017:
One more RPKI implementation available

RPKI Prefix Origin Validation merged into FRR master branch, based on RTRlib, more see
https://rtrlib.realmv6.org/
https://github.com/FRRouting/frr/