

# Cross-registry authentication

What way forward?

Chairs: Job Snijders & Rob Evans

# Agenda

- Why the need for cross-registry auth?
- Possible directions
  - A. Flattening maintainer objects across registries
  - B. Some RPKI based approach
  - C. Autnum auth constraint removal (and nothing else)
  - D. RDAP
  - E. .... ?
- Open microphone segment
- Conclusion / define work items

# Why?

- Currently organisations create ‘alien’ autnum objects in the RIPE db to authorise route-object creation
- Situations where inetnum is in RIR A, autnum in RIR B, are complicated today
- Many organisations have the same maintainer object in many different registries (example: MAINT-NTTCOM-BB exists in RIPE, RADB & NTTCOM)
- This leads to tons of superfluous objects

# Direction A – flattening the mntner namespace (job)

- We could:
  - Extend RPSL to allow foreign references
    - “mnt-by: SNIJDERS-MNT@RIPE”
  - Or define new protocol (NRTMv4?) which provides a quorum between registries to find which maintainer object lives where.
    - Flatten the mntner namespace
    - IRRs announce to others which mntners they manage
    - No end-user tool changes required
    - No RIR lock-in for end-users

**Looking at:** afrinic.db, altdb.db, apnic.db, arin.db, bboi.db, bell.db, gt.db, jpirr.db, level3.db, nttcom.db, radb.db, rgnet.db, ripe.db, savvis.db, tc.db

Colliding mntner objects: **939 (1.1% of total)**

Mntner objects in two registries: **906**

Mntner objects in **3 IRRs: 26, 4 IRRs: 7, 5 IRRs: 0**

Largest colliding DBs: **RIPE (4702), Level3 (874), APNIC (826), RADB (311), SAVVIS (211)...**

# Direction B (Tim)

- RPKI based authorisation on IRR objects for seamless enduser experience

# Route Objects in RIPE Database across RIRs

		ASN				
		afrinic	apnic	arin	lacnic	ripe ncc
p r e f i x	afrinic	33840	11	12	1	5861
	apnic	2	1622	53	1	353
	arin	33	26	4992	8	4509
	lacnic	0	4	34	2537	482
	ripe ncc	22	81	1276	77	216375

- 1830 objects with RPSL-MNT only, 10782 mix, 260587 own maintainer
- Most route objects for RIPE NCC registered aut-nums
- Most other objects have ASN and Prefix in same RIR, except 1276 with ARIN aut-num, and RIPE NCC prefix

# RPKI signatures

route: 10.0.0.0/24 ◀.....  
origin: AS65001 ◀.....  
mnt-by: PFX-MNT .....  
mnt-by: AS-MNT .....

current situation

- referential integrity problematic (X-RIRs)

route: 10.0.0.0/24 ◀.....  
origin: AS65001 ◀.....  
mnt-by: PFX-MNT .....  
signature: AS-RPKI .....

RPKI instead of remote maintainer

- server can validate
- user can validate
- (draft in IETF)

route: 10.0.0.0/24 ◀.....  
origin: AS65001 ◀.....  
signature: PFX-RPKI .....

or even.. ROA like

- only require PFX
- allow sign vs mntner

Note: RPKI signatures can also have use in e.g. aut-num objects for policy



# IRR Data Quality

pxf RIR	# announced	# objects	% valid	% invalid	% accuracy	% adoption
AFRINIC	14501	39734	49% (0.4%)	26% (0.4%)	65% (49%)	77% (1%)
APNIC	148136	2166	0% (0.9%)	2% (0.4%)	15% (66%)	3% (1%)
ARIN	191562	9862	2% (0.7%)	2% (0.2%)	56% (80%)	5% (1%)
LACNIC	79189	3060	2% (24%)	1% (1%)	56% (96%)	5% (25%)
RIPE NCC	153758	218179	77% (9%)	18% (1%)	80% (90%)	97% (10%)

- At least for LACNIC ROAs (in parentheses) look like a better alternative
- RIPE NCC RPKI validator 2.19 will export ROAs in route object format (beta)  
<https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources>

# Direction C (Job)

- Lighten the authorisation constraints which are required today for route-object creation:
  - No longer require the autnum to authorize a route-object, only require the inetnum owner to sign off on it
  - No cross-registry protocol required
  - Lots of superfluous autnum objects can then be removed from RIPE DB

# Direction D – RDAP (Andy)

- Fully define Autnum and Route objects in RDAP
- Define POST for RDAP for creating Route objects
  - Route objects live in the RIR-of-the-Prefix
  - POST to RIR-of-the-AS
  - Use redirects to RIR-of-the-Prefix with RIR-signed tokens to authenticate one client with both RIRs
- Use RDAP bootstrap for POST destination

# Open microphone

- What are direction E, F, G?

# Conclusion

- Definition of work items
- Volunteers?