

(More than an) APNIC Policy implementation update

George Kuo
34th TWNIC OPM
8 October 2020



Congratulations!



RPKI ROA 簽署率98%
RPKI Validator 全台啟動 46家業者

Overview

- A brief introduction to the Policy Development Process (PDP)
- Policy implementation status from APNIC 50
 - prop – 132: RPKI ROAs for unallocated and unassigned APNIC address space
 - prop – 125 Validation of “abuse-mailbox” and other IRT emails

Policies, proposals and the PDP

- APNIC policies determine the way Internet number resources (IP addresses and ASNs) are distributed, registered and managed in the Asia Pacific
- A policy proposal is a formal, written submission that outlines an idea for a new policy; if a policy proposal is successful it will become a policy
- Policy Development Process (PDP) is the procedure for discussing and deciding proposed changes to APNIC policies

Important values of the PDP



Anyone can participate in submitting proposals, discussing policies and making decisions

Open

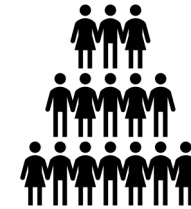
開放參與



Policy documents, policy mailing list, and Policy SIG are accessible to all

Transparent

資訊公開透明



PDP is driven by people from the community

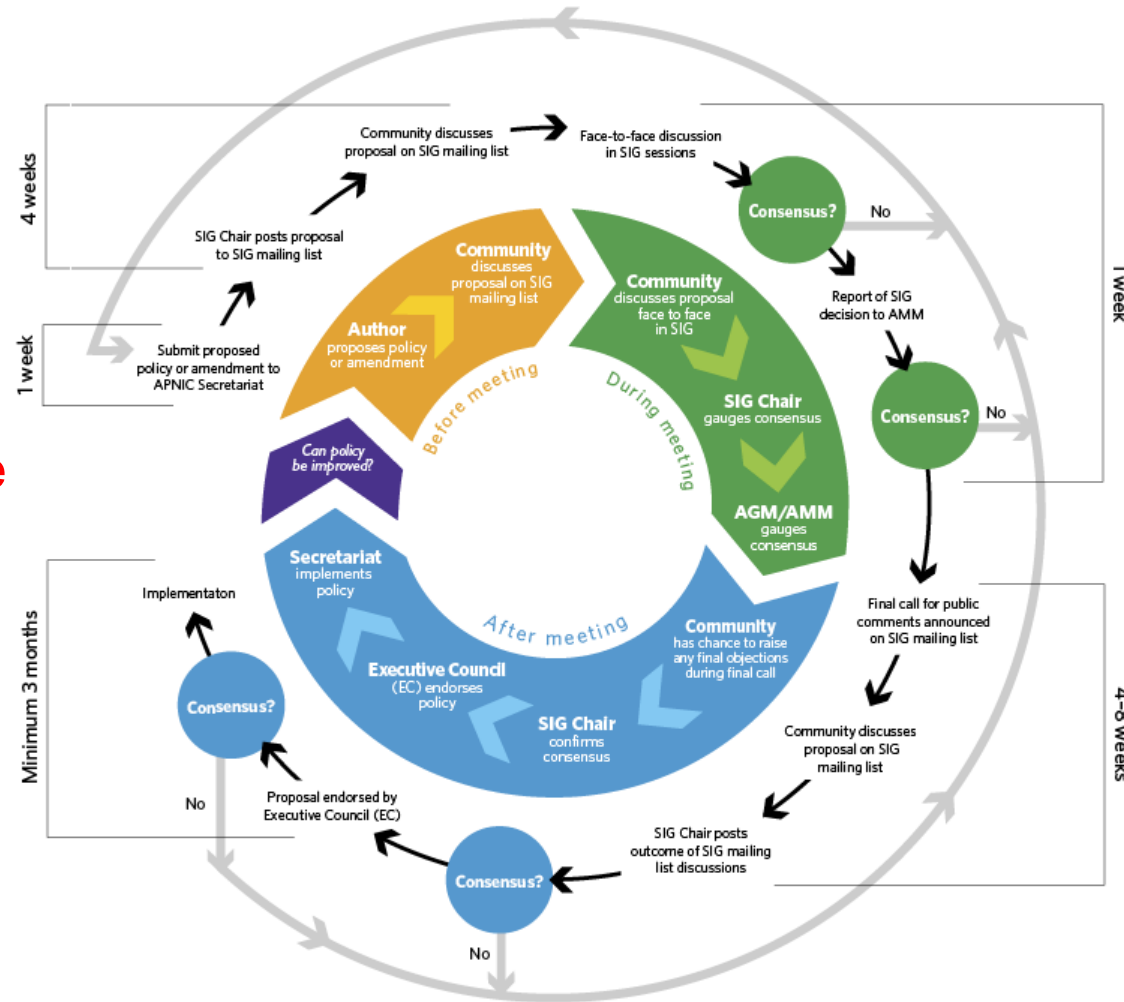
Bottom-up

由社群主導

From policy proposals to implementation

APNIC Secretariat facilitates policy discussion and stays neutral in the debate

Start here



RPKI ROAs for unallocated and unassigned APNIC address space

prop-132

prop-132 v3

4. Proposed policy solution

APNIC will create AS0 (zero) ROAs for all the unallocated and unassigned address space (IPv4 and IPv6) for which APNIC is the current administrator. Any resource holder (APNIC member) can create AS0 (zero) ROAs for the resources they have under their account/administration.

A RPKI ROA is a positive attestation that a prefix holder has authorised an AS to originate a route for this prefix whereas, a RPKI ROA for the same prefixes with AS0 (zero) origin shows negative intent from the resource holder that they don't want to advertise the prefix(es) at this point but they are the rightful custodian.

Only APNIC has the authority to create RPKI ROAs for address space not yet allocated to the members and only APNIC can issue AS0 (zero) RPKI ROAs. Once they RPKI ROA is issued and APNIC wants to allocate the address space to its member, simply they can revoke the RPKI ROA and delegate the address space to members. (this proposal doesn't formulate operational process).

<https://www.apnic.net/community/policy/proposals/prop-132>

Proposal history



<https://www.apnic.net/community/policy/proposals/prop-132>

Resource Public Key Infrastructure (RPKI)


- RPKI uses hierarchical Public Key Infrastructure that binds Internet number resources to a public key via certificates (x.509 certificate standards)
 - The hierarchy of resource certificates are aligned to the Internet number resource allocation structure
- Via the resource certification service, resource holders can encrypt and sign BGP routing advertisements digitally by creating 'ROAs' (Route Origin Authorizations)




RFC 6483

- AS0 is reserved by IANA so that it may be used to identify non-routed networks
- A ROA with a subject of AS0 (AS0 ROA) is an attestation by the holder of a prefix that the prefix described in the ROA, and any more specific prefix, should not be used in a routing context

prop-132 implementation

- APNIC's RPKI system now publishes and maintains an AS0 ROA for all undelegated resources recorded in APNIC's registry
- It is a fully deployed service with systems monitoring 24/7 integrated into our operations platforms
- Undelegated resources are the IPv4 and IPv6 addresses listed as 'available' or 'reserved' in the daily published delegated statistics files
- <http://ftp.apnic.net/stats/apnic/>



	delegated-apnic-ipv6-assign.>	29-Sep-2020 01:18	78 MD5 signature
	delegated-apnic-latest	29-Sep-2020 01:18	3.1M APNIC delegated internet number resources
	delegated-apnic-latest.asc	29-Sep-2020 01:18	189 PGP signature

prop-132 implementation

- Deploy an initial testbed operated on the 'Krill' system from NLNet Labs
 - A temporary, soft-keyed Trust Anchor (TA) in a Trust Anchor Locator (TAL) file created based on the daily delegated files
 - The 'repository' published inside APNIC's VM on the test network
- Introduce a delay to prevent accidental exclusions (if delegated stats files are out of synchronization with the registry)
 - Approx. around five mins, after live updates to the registry (delegations or returns) occur, apply updates to both main RPKI and AS0 RPKI state

Similar AS0 ROA policies in other region?

RIR	Status
APNIC	Implemented
AFRINIC	Under discussion
ARIN	No proposal
LACNIC	Consensus reached, awaiting implementation
RIPE NCC	Proposal withdrawn

What's next?

- Be sure to keep your ROAs updated!
- Try Route Origin Validation (ROV) and share your experience
 - Invalid advertisements (advertisements that contradict ROA information) may be discarded or de-preferenced

Validation of “abuse-mailbox” and other IRT emails

prop-125

Incident Response Team (IRT) object

```
inetnum:      103.10.232.0 - 103.10.232.255
netname:      APNIC-RD
descr:        APNIC R&D Anycast
country:      AU
org:          ORG-ARAD1-AP
admin-c:      GM85-AP
tech-c:       GM85-AP
abuse-c:      AA1412-AP
status:       ASSIGNED PORTABLE
remarks:      /24 for APNIC R&D Anycast research
remarks:      -----
remarks:      To report network abuse, please contact mnt-irt
remarks:      For troubleshooting, please contact tech-c and admin-c
remarks:      Report invalid contact via www.apnic.net/invalidcontact
remarks:      -----
mnt-by:       APNIC-HM
mnt-routes:   MAINT-AU-APNIC-GM85-AP
mnt-irt:      IRT-APNICRANDNET-AU
last-modified: 2020-07-15T13:10:56Z
source:      APNIC
```

```
irt:          IRT-APNICRANDNET-AU
address:      PO Box 3646
address:      South Brisbane, QLD 4101
address:      Australia
e-mail:       abuse@apnic.net
abuse-mailbox: abuse@apnic.net
admin-c:      AR302-AP
tech-c:       AR302-AP
auth:         # Filtered
remarks:      abuse@apnic.net was validated on 2020-08-10
mnt-by:       MAINT-AU-APNIC-GM85-AP
last-modified: 2020-08-10T06:42:59Z
source:      APNIC
```

prop- 125 v1

2. Objective of policy change

The Internet community is based on collaboration. In many cases, however, this is not enough and we all need to be able to contact those LIRs which may be experiencing a problem in their networks and may not be aware of the situation.

This proposal aims to solve this problem by means of a simple, periodic verification of IRT object emails, and establishes the basic rules for performing such verification and thus avoids unnecessary costs to third parties who need to contact the persons responsible for solving the abuses of a specific network.

The proposal guarantees that the cost of processing the abuse falls on the LIR whose client is causing the abuse (and from whom they receive financial compensation for the service), instead of falling on the victim, as would be the case if they had to resort to the courts, thus avoiding costs (lawyers, solicitors, etc.) and saving time for both parties.

<https://www.apnic.net/community/policy/proposals/prop-125>

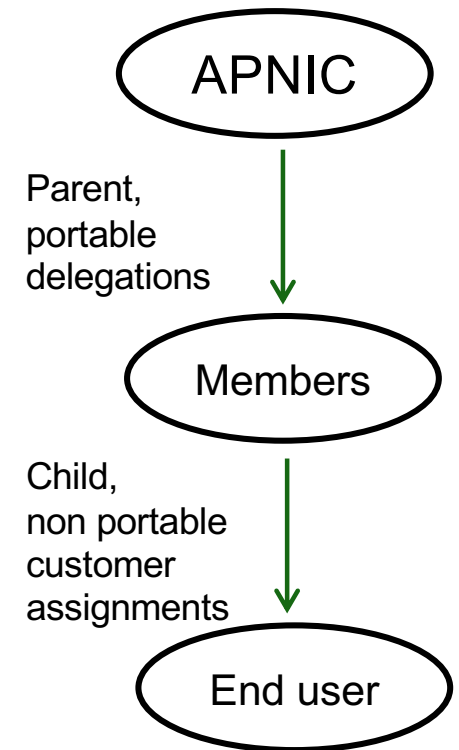
Proposal history



<https://www.apnic.net/community/policy/proposals/prop-125>

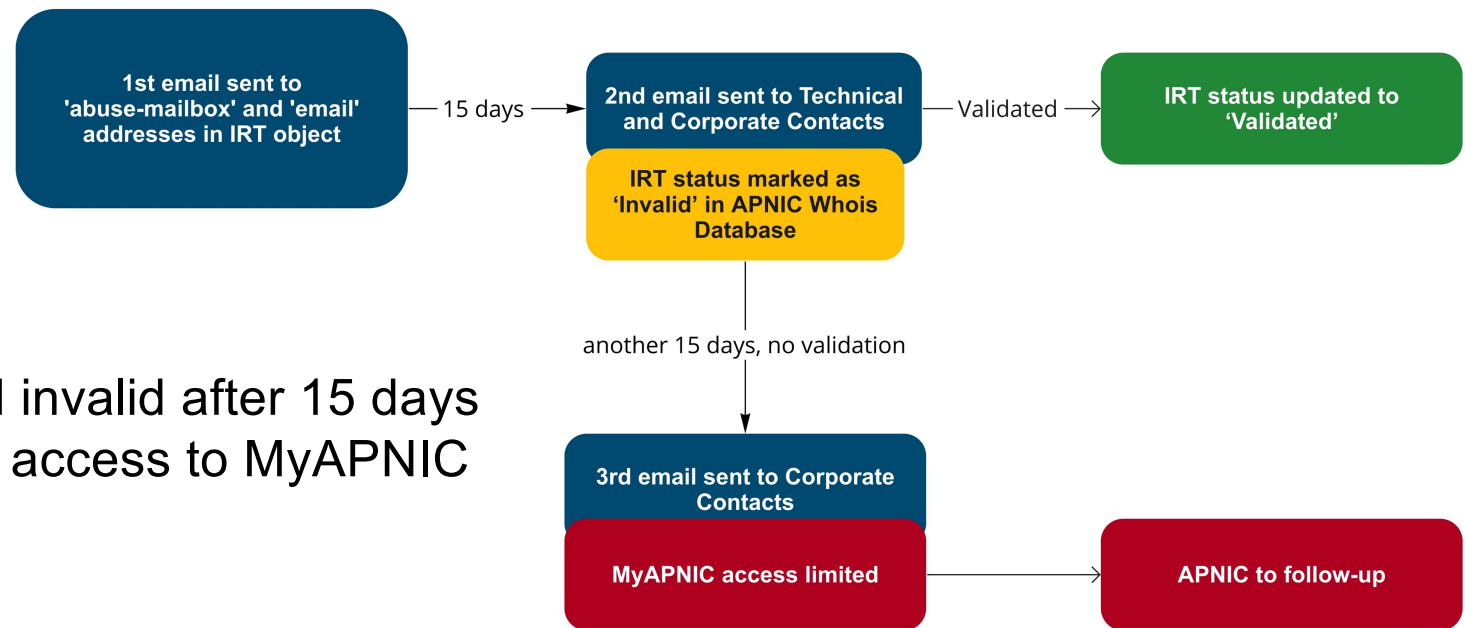
prop-125 implementation

- Phase one – completed
 - Validations for all IRTs associated with portable delegations
 - Created new escalation mailbox (escalation-abuse@apnic.net)
- Phase two – completed
 - Validations for all IRTs associated with non-portable customer assignments
- Phase three – ongoing
 - Improved UI/UX and resolved software issues reported from Members
 - Added 'abuse-c' attribute to whois records
 - MyAPNIC restriction to be reinstated soon



Validation process

- Frequency
 - Every six months
- Failure to validate
 - IRT objects marked invalid after 15 days
 - Restricted Member access to MyAPNIC after 30 days
- Requirement
 - Abuse-mailbox responsive to legitimate reports
 - Validation requests responded to by human



Some stats on validation

In the last six months:

- 5,779 Members requested to validate emails
- 6,845 email validation requests issued
- 6,003 email validation requests confirmed
- 87.7% validation rate

As of Sep 2020

Feedback from APNIC Members

Software vendor:

“I am concerned about clicking links sent to verify my IRT. Hopefully, there is a better way.”

Internet Service Provider:

“Is this email for validate IRT contact? Any evidence that your email is from APNIC? As I receive many spam mail and hacker mail, so it is hard for me to trust and click on any links without knowing it is real or fake account.”

Feedback from APNIC Members

Banking/Financial

“These emails are pretty problematic – they have a link to click on and it asks to validate an email address. These are very suspect in an email. I had to look at the email header to verify it did indeed come from APNIC.

University/CERT

“This type of automated testing is an abuse of our abuse address, is mindless robotic punishment of client organizations without regard to the impact upon those organizations and without any consideration of the realities of email deliverability or the pressures on abuse or other addresses of an organization from spam and other email threats.

I would suggest you cease this automated testing.”

APNIC Secretariat recommendations

- Investigate using other methods of validation, instead of unique links in emails
- Change validation cycle from every six months to once annually
- Consider deprecating the 'email' attribute in IRT objects and validating only 'abuse-mailbox'. Members will then only be required to validate one email address

Have your say and let us know if you have any suggestions!

Similar IRT policy in other region?

RIR		Status
APNIC	Validation of “abuse-mailbox” and other IRT emails	Implemented
AFRINIC	“Abuse Contact Policy Update (Draft 6)”	Under discussion
ARIN	ARIN-prop-264: Validation of Abuse-mailbox	Abandoned
LACNIC	LAC-2018-5: Registration and validation of abuse contact	Consensus reached, awaiting implementation
RIPE NCC	Validation of abuse-mailbox	Proposal withdrawn

What's next?

- Continue working with the community to amend the policy to address current concerns
 - Negative feedback about the overall process
 - Many raising security concerns about clicking on email links
- Simplifying the process and reducing the frequency of validation should help alleviate some of the pain points
- Find the balance between ease of validation and achieving the policy goal — to ensure accurate and contactable network abuse contacts

Your participation benefits all

FUTURE CONFERENCES

You are invited to attend

- APRICOT 2021 and APNIC 51
 - Online only (<https://www.2021.apricot.net/>)
 - 22 February to 4 March 2021
- APNIC 52
 - Hopefully in person and online
 - Sapporo, Japan
 - 8 to 16 September 2021

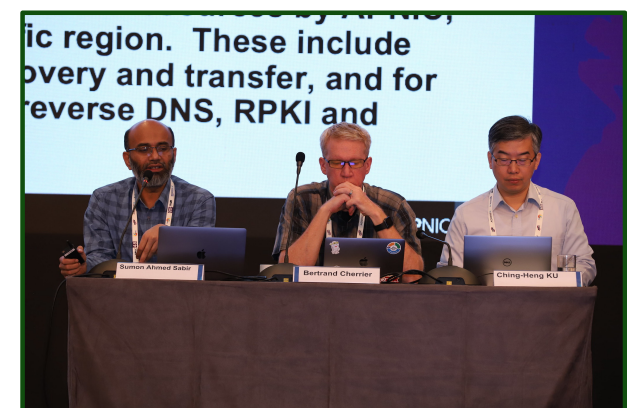
By participating you can...



Make new friends



Hear from experts



Help develop policies



Polish tech skills



Share your experience



Promote your organization

References

- <https://tools.ietf.org/html/rfc6483>
- <https://www.apnic.net/community/participate/maillinglists/>
- <https://www.apnic.net/community/policy/proposals/>
- <https://www.apnic.net/community/policy/process/>
- <https://conference.apnic.net/50/assets/files/APCS790/prop-125-implementation-updateV2.pdf>
- <https://conference.apnic.net/50/assets/files/APCS790/prop-132-Implementation.pdf>
- <https://www.apnic.net/events/conferences/>
- <https://academy.apnic.net/en/course/policy-development-process-course/>
- <https://training.apnic.net/>