Internet Number Registry Services the Next Generation

RDAP and RPKI

Overview

- What are registry services
- Today's registry services
  - whois
- The next generation…
  - Registration Data Access Protocol (RDAP)
  - Resource Public Key Infrastructure (RPKI)

Registries?

- Organisations running registry services
  - With authority for registration of some “Public Resource”
- Public databases describing status of resources
  - Land titles, vehicle registrations, phone numbers
  - Internet registries - Domain Names, protocols, INRs
  - e.g. .com, .th, IPv4, IPv4, ASNs
- Internet Registries
  - Authoritative registry/database function
  - Public registry service function
  - gTLDs, ccTLDs
  - RIRs, NIRs, LIRs, ISPs…

Registry services (INRs)

- whois
  - Query service on TCP port 43 (RFC 812, 1982)
  - Very simple service
  - Query and response are not standardised
- Registration Data Access Protocol (RDAP) (NEW since 2015)
  - API for access to “whois” registry data
  - Automation, AAA, i18N, redirection, extensibility
- Resource Public Key Infrastructure (RPKI) (since 2010)
  - PKI for INRs
  - Cryptographically verifiable “ownership” of INRs

whois

whois command line

```
$ whois -h whois.apnic.net 210.17.9.242

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '210.17.0.0 - 210.17.127.255'

% Abuse contact for '210.17.0.0 - 210.17.127.255' is 'ethanchen@taiwanmobile.com'

inetnum:        210.17.0.0 - 210.17.127.255
netname:        TTN-TW
descr:          Taiwan Telecommunication Network Services Co.,LTD.
descr:          110 , 8F , No 89 , Sung Jen RD , Taipei
country:        TW
admin-c:        IP11-AP
tech-c:         IP11-AP
remarks:        service provider
mnt-by:         MAINT-TW-TWNIC
mnt-irt:        IRT-TFN-TW
mnt-lower:      MAINT-TTN-AP
status:         ALLOCATED PORTABLE
last-modified:  2011-06-01T04:13:58Z
source:         APNIC
```

Query to port 43

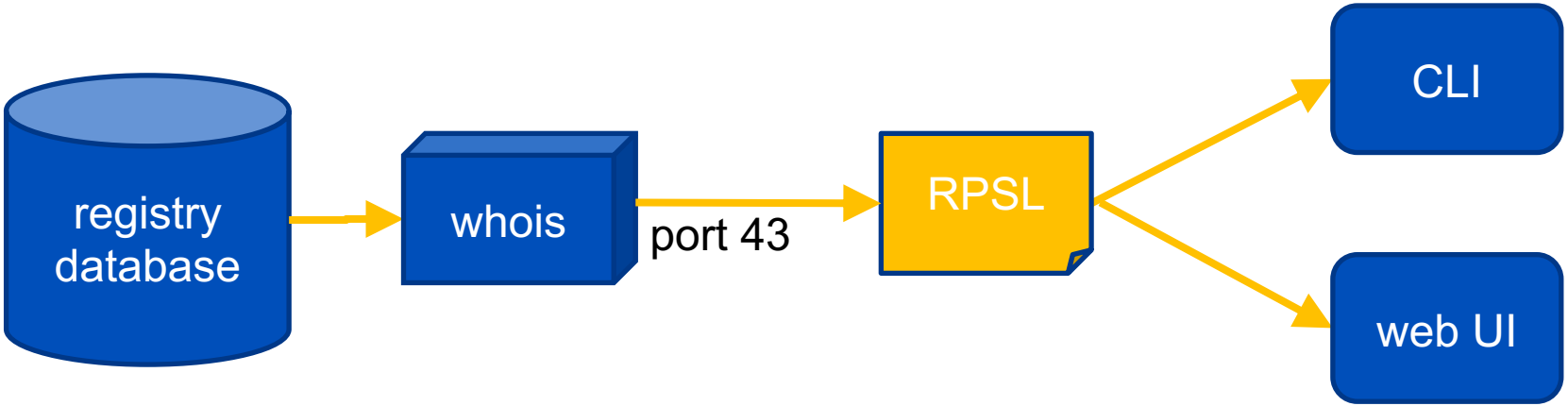
"Blob" reply – undefined

whois www interface

HTML wrapper

Same blob

whois at APNIC



Whois – limitations

- “blob” query and result formats
  - Registry-specific questions and answers (eg RPSL)
  - Automation is difficult
- No AAA model
  - Built for public service only
- Most servers serve US-ASCII only
  - i18n is undefined
- No redirection
  - User/client must find the right server

RDAP

Registration Data Access Protocol

RDAP

- RDAP is the successor to the ageing WHOIS protocol.
  - Stardardised by IETF
- Query: REST
  - REpresentational State Transfer - via HTTP
  - Query defined within URL issued to RESTful server
  - Inherits useful features from HTTP/HTTPS (AAA, redirection…)
- Response: JSON
  - JavaScript Object Notation
  - Standardised text representation of structured data
  - Easily used by JavaScript/HTML5, Java, Perl, Python…

* Source: RDAP.org

RDAP JSON raw

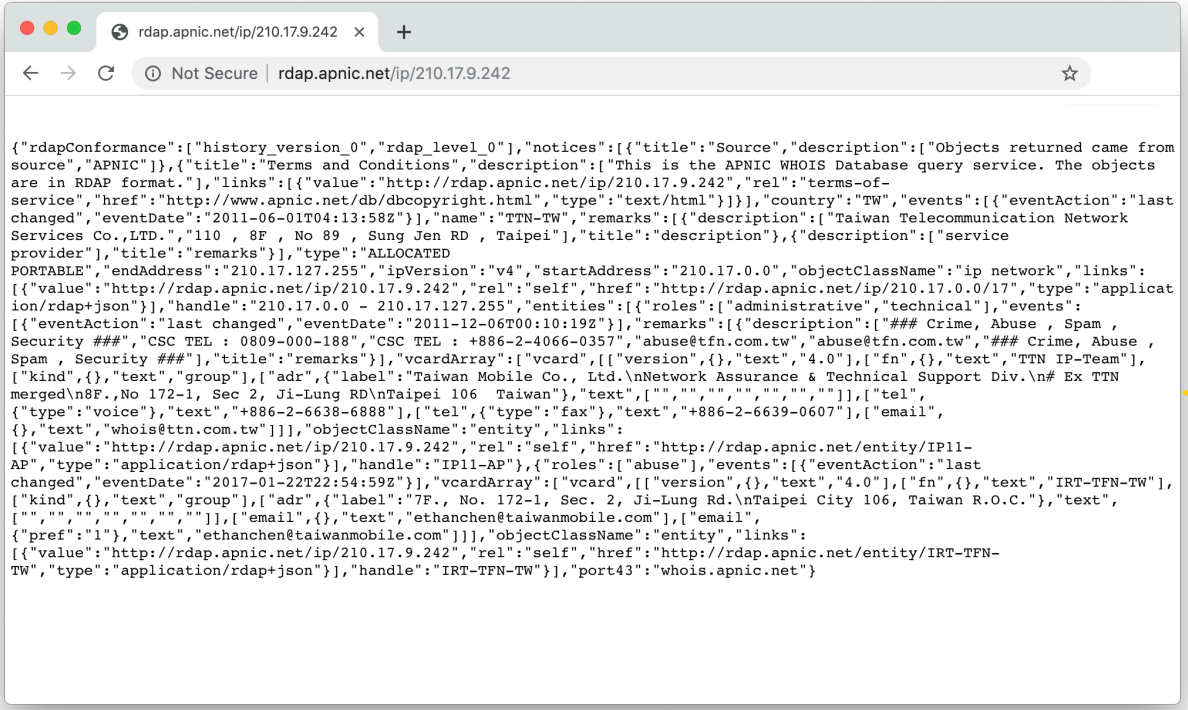
$ curl http://rdap.apnic.net/ip/210.17.9.242


```
{"rdapConformance":["history_version_0","rdap_level_0"],"notices":[{"title":"Source","description":["Objects returned came from
source","APNIC"]},{"title":"Terms and Conditions","description":["This is the APNIC WHOIS Database query service. The objects are in
RDAP format."],"links":[{"value":"http://rdap.apnic.net/ip/210.17.9.242","rel":"terms-of-
service","href":"http://www.apnic.net/db/dbcopyright.html","type":"text/html"}]}],"country":"TW","events":[{"eventAction":"last
changed","eventDate":"2011-06-01T04:13:58Z"}],"name":"TTN-TW","remarks":[{"description":["Taiwan Telecommunication Network Services
Co.,LTD.","110 , 8F , No 89 , Sung Jen RD , Taipei"],"title":"description"},{"description":["service
provider"],"title":"remarks"}],"type":"ALLOCATED
PORTABLE","endAddress":"210.17.127.255","ipVersion":"v4","startAddress":"210.17.0.0","handle":"210.17.0.0 -
210.17.127.255","objectClassName":"ip
network","links":[{"value":"http://rdap.apnic.net/ip/210.17.9.242","rel":"self","href":"http://rdap.apnic.net/ip/210.17.0.0/17","type
":"application/rdap+json"}],"entities":[{"roles":["abuse"],"events":[{"eventAction":"last changed","eventDate":"2017-01-
22T22:54:59Z"}],"vcardArray":["vcard",[["version",{},"text","4.0"],["fn",{},"text","IRT-TFN-
TW"],["kind",{},"text","group"],["adr",{"label":"7F., No. 172-1, Sec. 2, Ji-Lung Rd.\nTaipei City 106, Taiwan
R.O.C."},"text",["","","","","","",""]],["email",{},"text","ethanchen@taiwanmobile.com"],["email",{"pref":"1"},"text","ethanchen@taiw
anmobile.com"]]],"handle":"IRT-TFN-
TW","objectClassName":"entity","links":[{"value":"http://rdap.apnic.net/ip/210.17.9.242","rel":"self","href":"http://rdap.apnic.net/e
ntity/IRT-TFN-TW","type":"application/rdap+json"}]},{"roles":["administrative","technical"],"events":[{"eventAction":"last
changed","eventDate":"2011-12-06T00:10:19Z"}],"remarks":[{"description":["### Crime, Abuse , Spam , Security ###","CSC TEL : 0809-
000-188","CSC TEL : +886-2-4066-0357","abuse@tfn.com.tw","abuse@tfn.com.tw","### Crime, Abuse , Spam , Security
###"],"title":"remarks"}],"vcardArray":["vcard",[["version",{},"text","4.0"],["fn",{},"text","TTN IP-
Team"],["kind",{},"text","group"],["adr",{"label":"Taiwan Mobile Co., Ltd.\nNetwork Assurance & Technical Support Div.\n# Ex TTN
merged\n8F.,No 172-1, Sec 2, Ji-Lung RD\nTaipei 106  Taiwan"},"text",["","","","","","",""]],["tel",{"type":"voice"},"text","+886-2-
6638-6888"],["tel",{"type":"fax"},"text","+886-2-6639-0607"],["email",{},"text","whois@ttn.com.tw"]]],"handle":"IP11-
AP","objectClassName":"entity","links":[{"value":"http://rdap.apnic.net/ip/210.17.9.242","rel":"self","href":"http://rdap.apnic.net/e
ntity/IP11-AP","type":"application/rdap+json"}]}],"port43":"whois.apnic.net"}
```


HTTP “get”

JSON reply

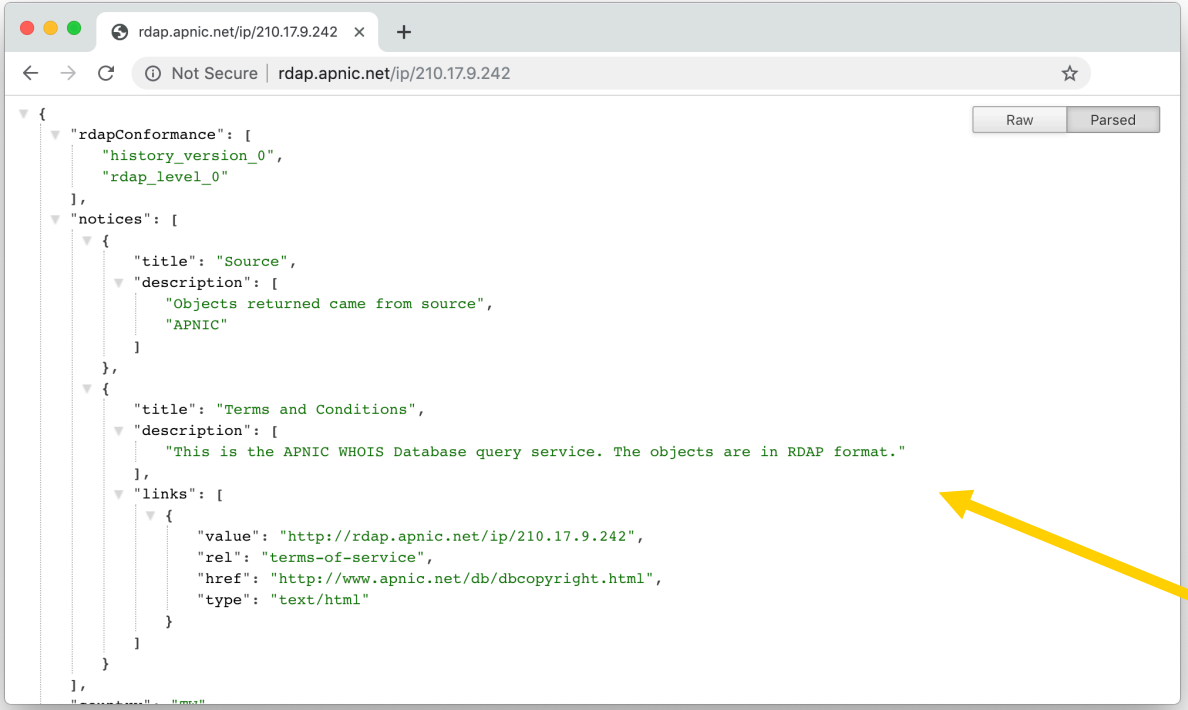
RDAP JSON raw



Web client

JSON reply

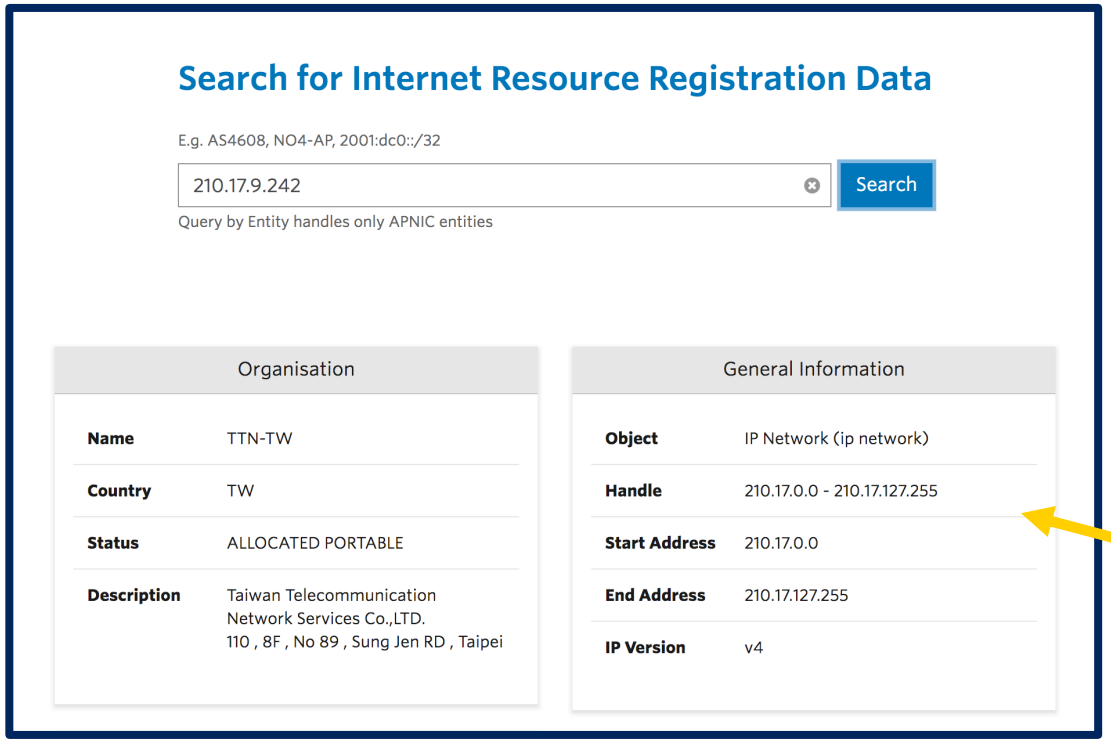
RDAP JSON formatted



Browser plugin

Structured JSON

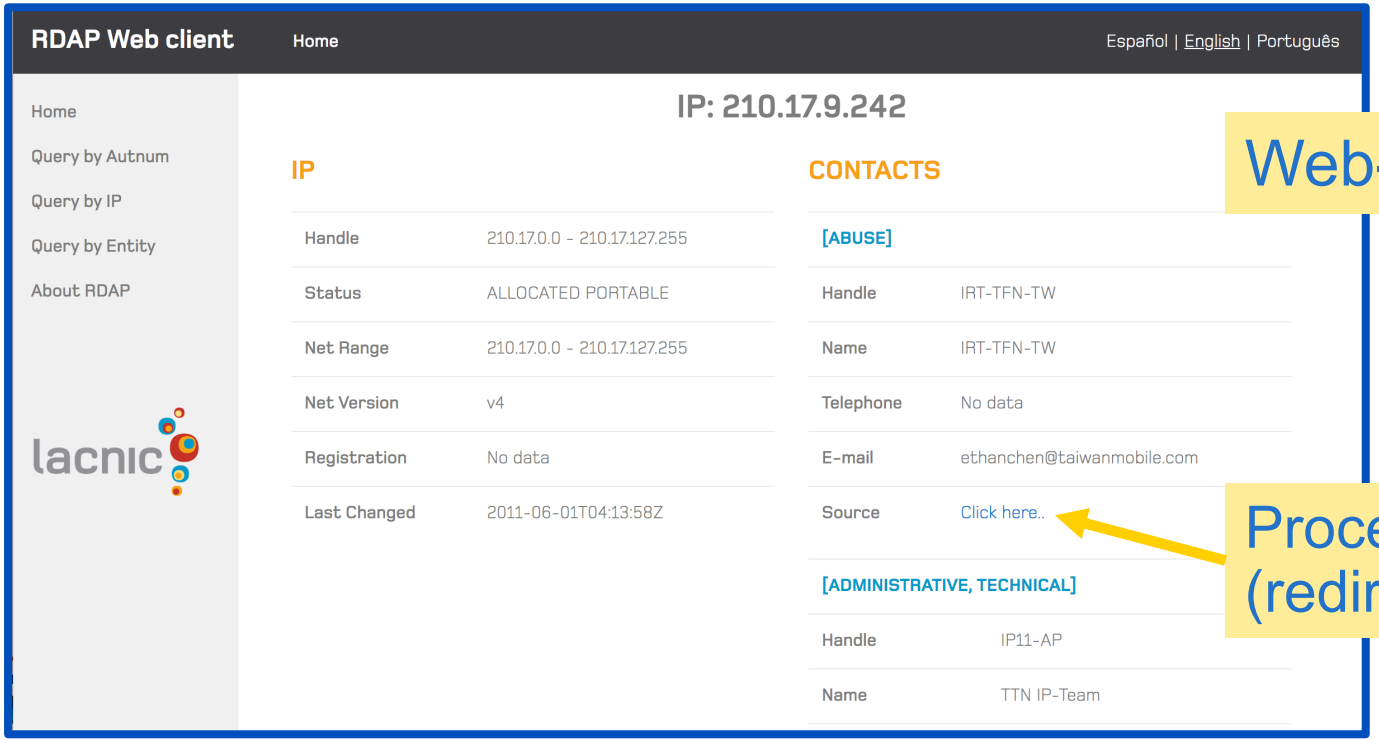
RDAP client



Web-based client

Processed result

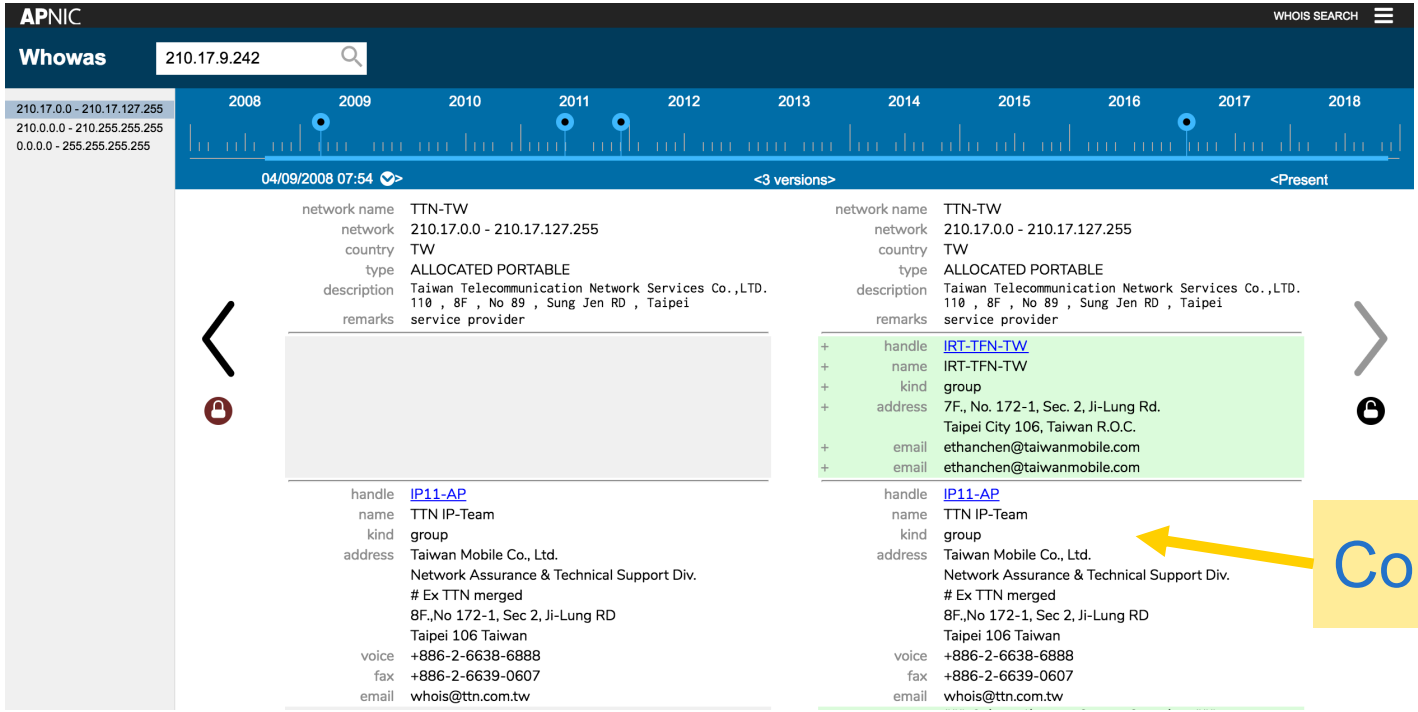
RDAP client



Web-based client

Processed result (redirected)

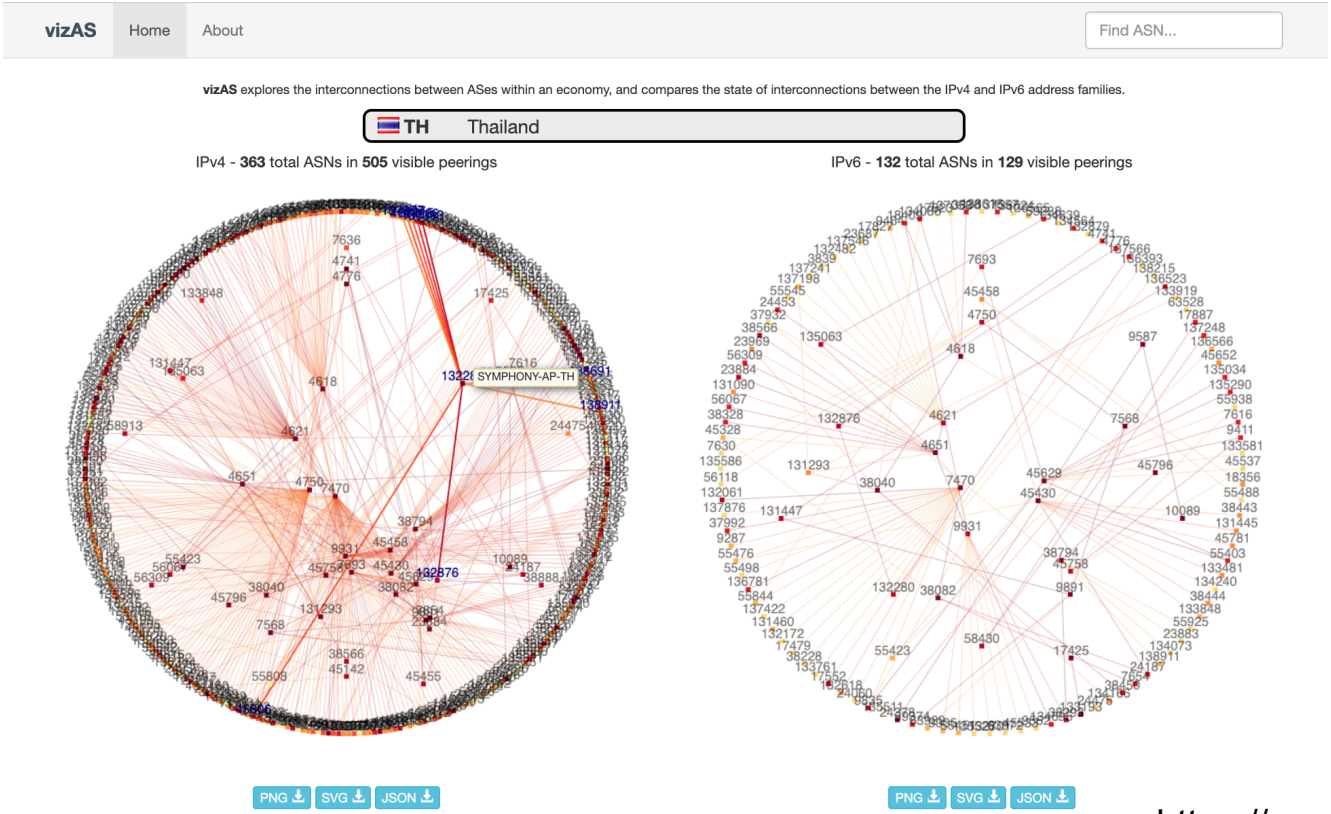
RDAP application (whowas)



Complex result

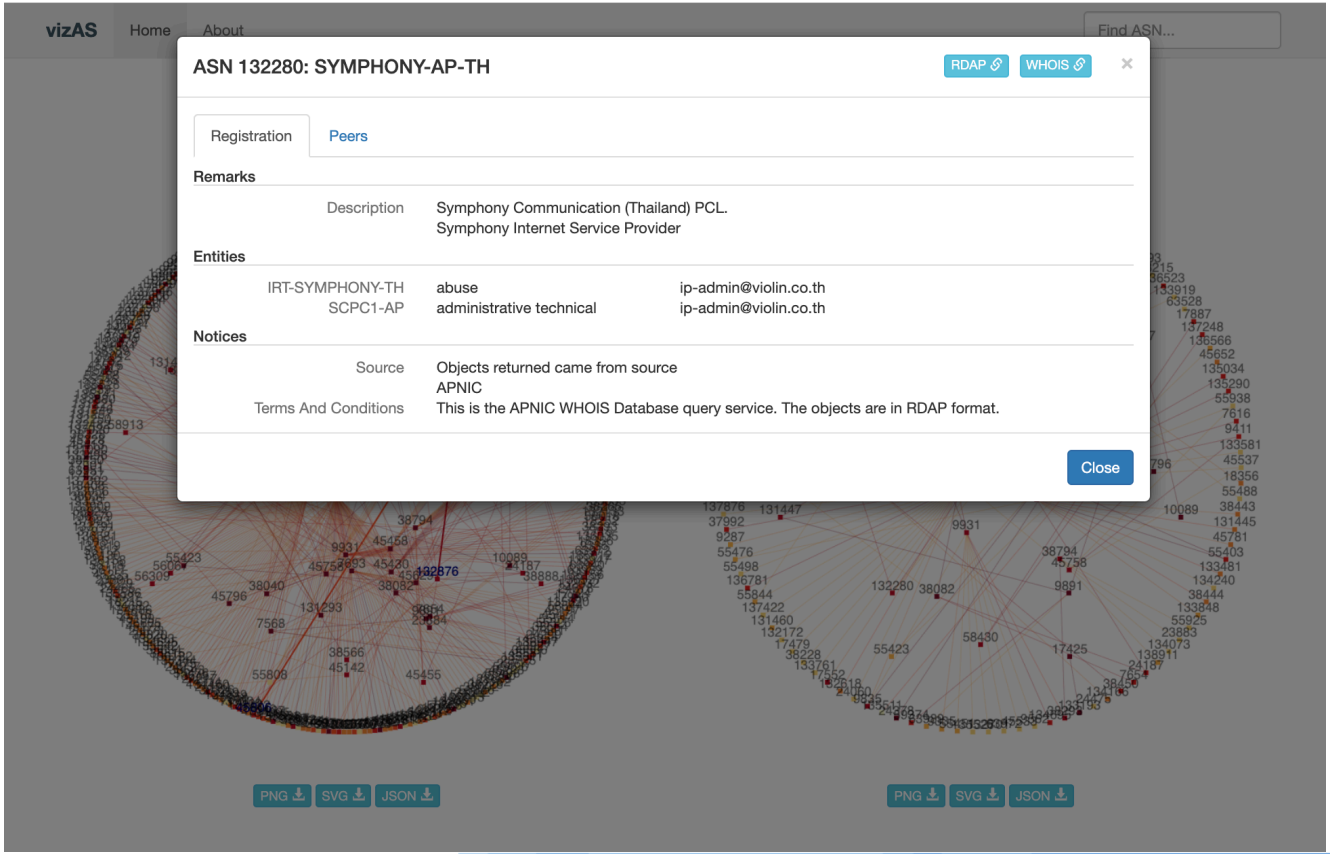
https://www.apnic.net/whowas

RDAP application (vizAS)

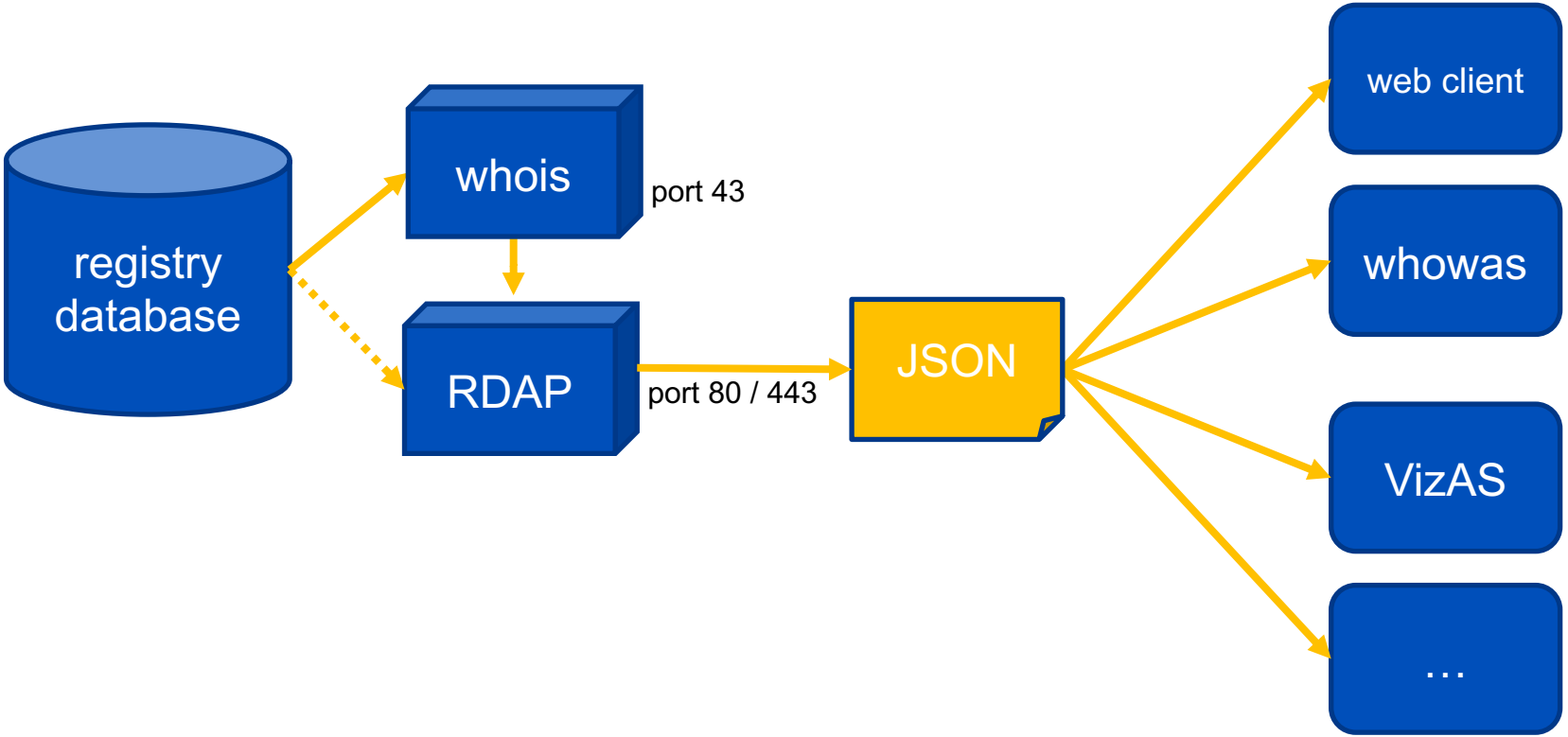


https://www.apnic.net/vizas

RDAP application (vizAS)



RDAP


registry database
whois
port 43
RDAP
port 80 / 443
JSON
web client
whowas
VizAS
…

RDAP benefits

- Automation – JSON input to common programming languages
  - Integration with firewall, NMS, IPAM…
- “Differentiated Access”
  - If needed
- Speaks your language (and character set)
  - Can implement server-side or in-client language preference
- One stop query
  - Will auto-redirect to the right authoritative server
- Web protocol is CDN friendly
  - Serve local, via anycast or DNS redirection methods
  - Cacheable, survives DDoS longer since distributed

APNIC RDAP Status

- First implemented May 2015
  - Adjunct service query to WHOIS radix tree (in memory)
  - Rewrote RPSL on-the-fly
- Re-implemented into WHOWAS Late 2016
  - Static in-memory data model. Fast response
- Working with NIRs
  - Hope to serve <nir>.rdap.apnic.net more-specific service
- APNIC region-wide consistent service model goal for 2019
  - Working with NIRs and other RIRs

RPKI

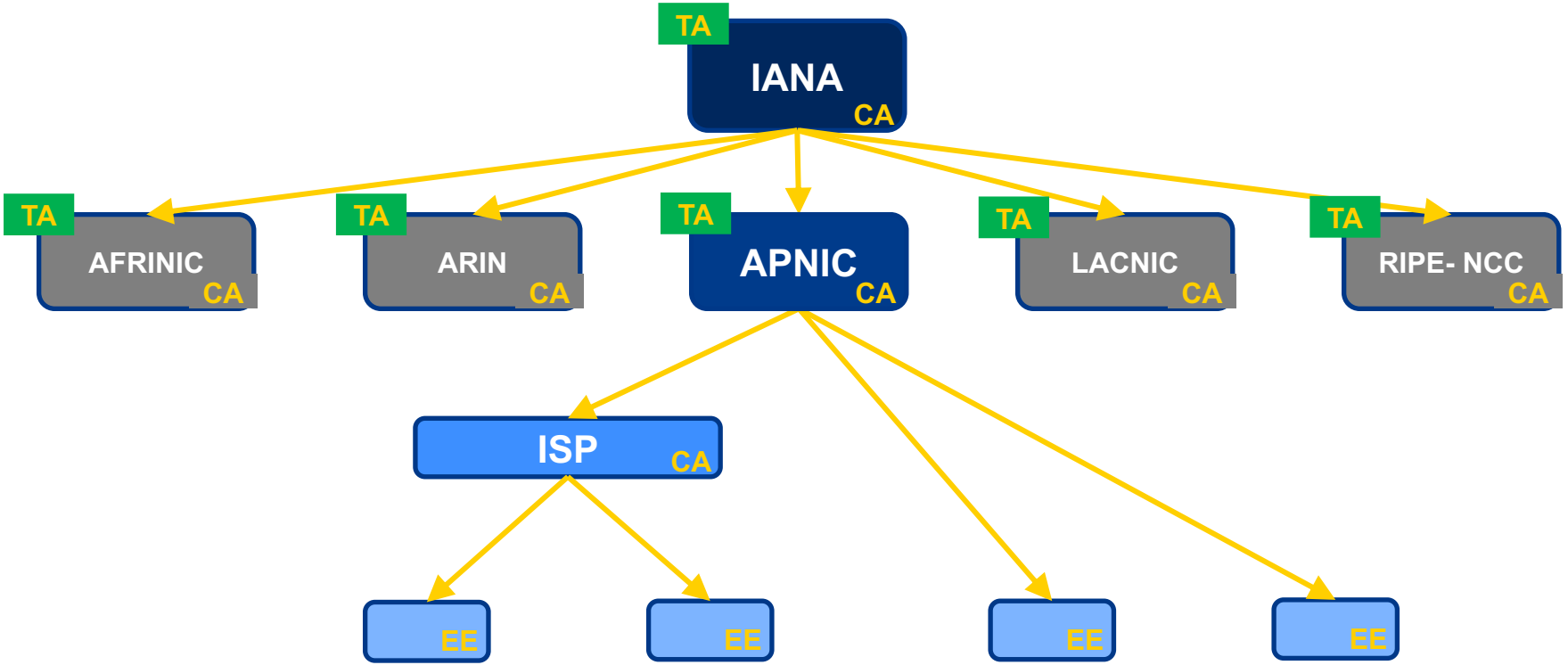
Resource Public Key Infrastructure

RPKI

- **RPKI** is a public key infrastructure (PKI) framework, designed to secure BGP routing
  - Based on X.509 PKI standards
- **RPKI** adds INR information to X.509 certificates issued to resource holders
  - Representing “ownership” and other status
  - Certification hierarchy follows INR delegation hierarchy

IANA ➔ RIR ➔ NIR ➔ ISP ➔ …

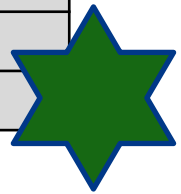
RPKI hierarchy



RPKI application: ROA

- Route Origin Authorization
  - List of prefixes with ASN authorized to announce
  - Signed by the prefix holder with RPKI certificate

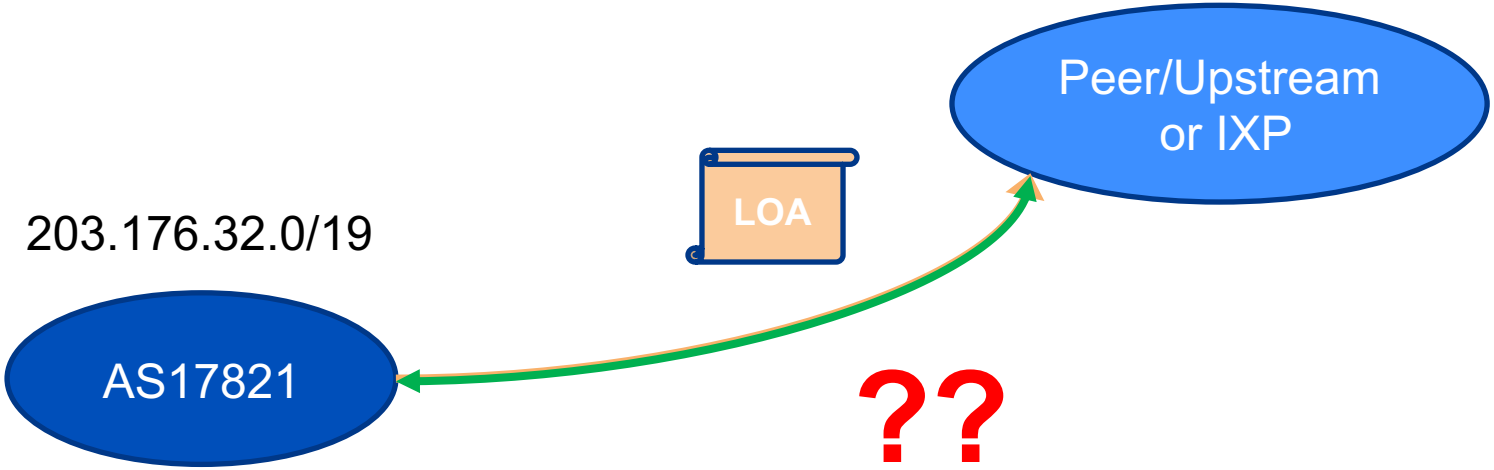
Prefix	203.176.32.0/19
Max-length	/24
Origin ASN	**AS17821**



- ROV relies on the integrity of the ROA
  - If valid, can now be used to construct route filters

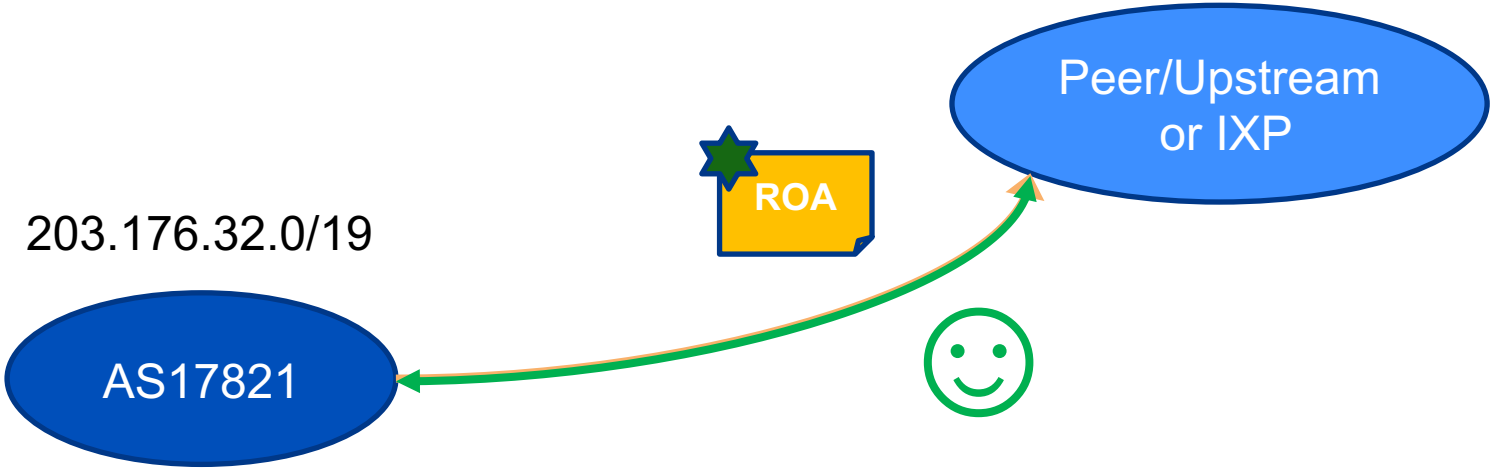
Route Origin Validation (ROV)

- Using RPKI Route Origin Authorisation (ROA)



Route Origin Validation (ROV)

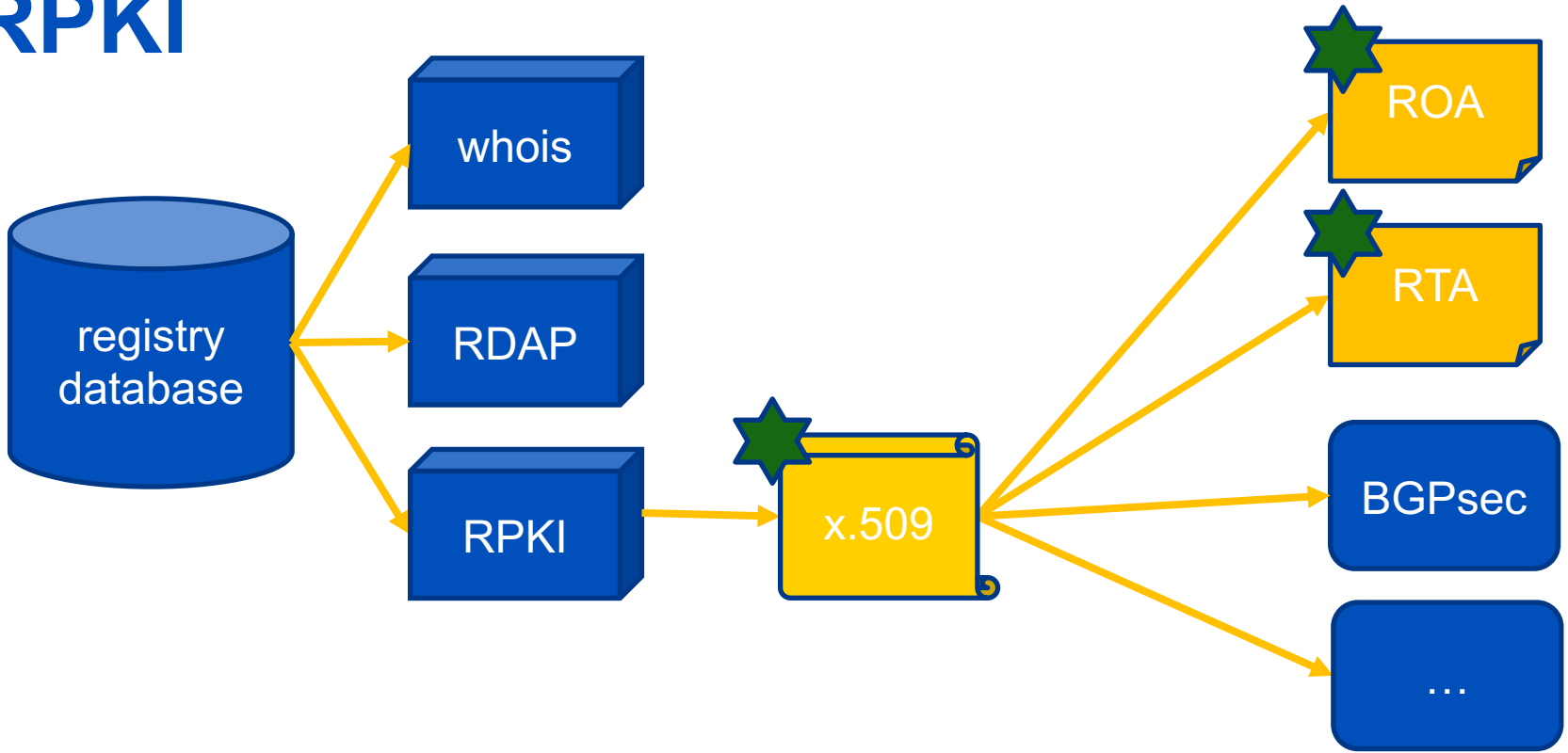
- Using RPKI Route Origin Authorisation (ROA)



RPKI application: RTA

- Resource Tagged Attestation
  - Use of RPKI cert to sign an arbitrary object
- RTA application: LOA
  - Replace existing informal “letter of authority” practice
  - Now digitally secured and can be automated
- Pilot implementation
  - In development at APNIC (via MyAPNIC)
  - IETF draft in progress

RPKI

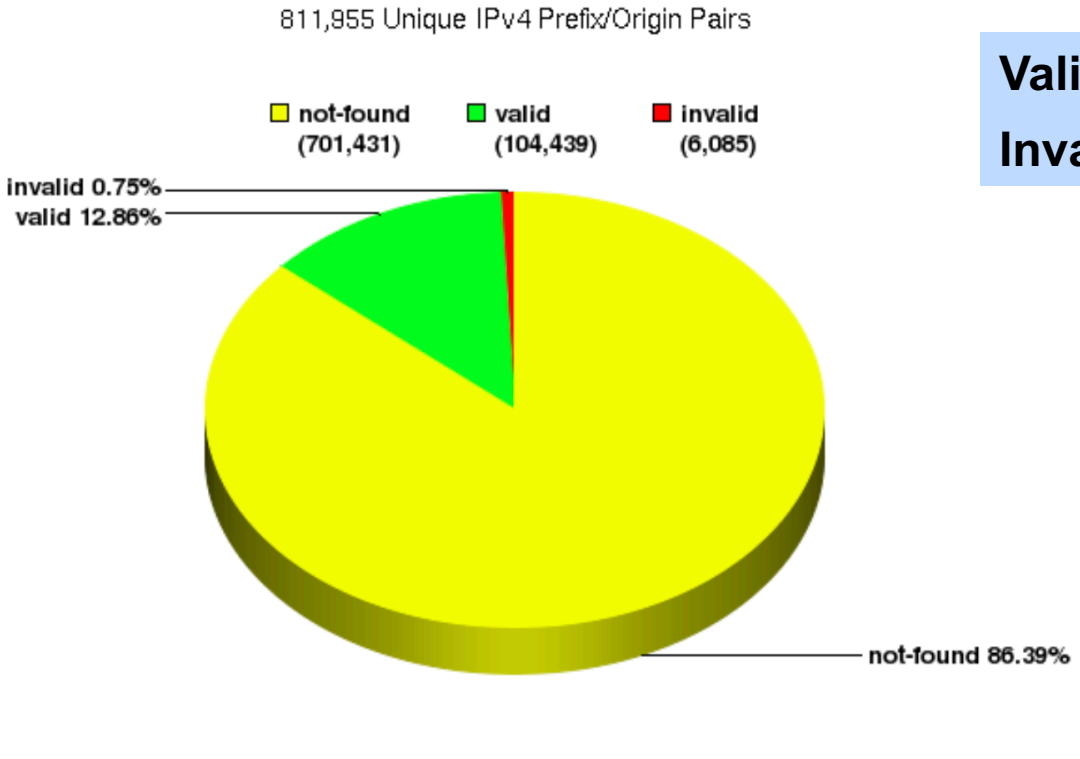


RPKI at APNIC

RPKI Service Models

- Hosted service
  - APNIC performs CA functions on behalf of members
  - Manage keys, repository etc
  - Generate certificates for resource delegations
  - This “Member CA” is separate from the “APNIC CA”
- Provisioning model
  - Member operates full RPKI system including CA
  - Communication with APNIC via provisioning protocol
  - This is live at JPNIC, CNNIC and TWNIC (IDNIC in progress)

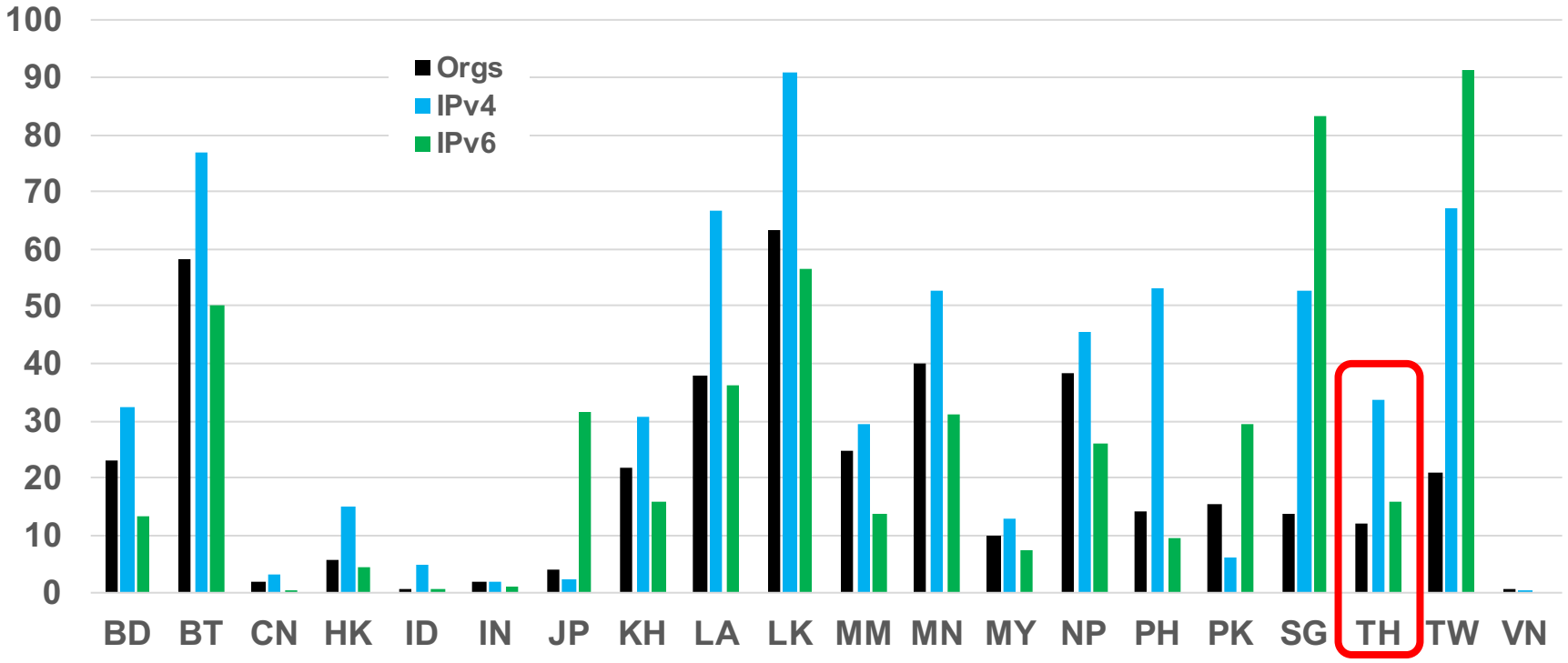
ROA deployment – Global



Valid	12.85%
Invalid	0.75%

https://rpki-monitor.antd.nist.gov

ROA deployment – Regional



RPKI benefits

- Improved in-band verification of resource custodianship
  - Much safer than manually checking whois or IRR database
  - Ease of automation
- Primary application: Secure Origin (ROA)
  - A first step to preventing many attacks on BGP integrity
  - BGP Path remains a problem which is under development
  - Related information such as IRR Policy can now leverage strong proofs of validity (end the maintainer-authority problem in RADB/IRR)
- Also: secure attestation (RTA)
  - And more in future?

How do I start?

- Create ROAs to better protect your own routes
  - Encourage your peers/customers to do the same
  - Encourage your IXP to implement ROV in the RS
- Then
  - Set up route validation at your own border routers
  - Using public or IXP validator, or your own
- APNIC members, use MyAPNIC
  - We can help!
  - Please contact APNIC Helpdesk
  - And…

Over to Tashi…

pwilson@apnic.net