APNIC Upgraded to Split Trust Anchor RPKI

SANOGXXI, January 28, 2013, Cox's Bazar, Bangladesh

Nurul Islam Roman, APNIC

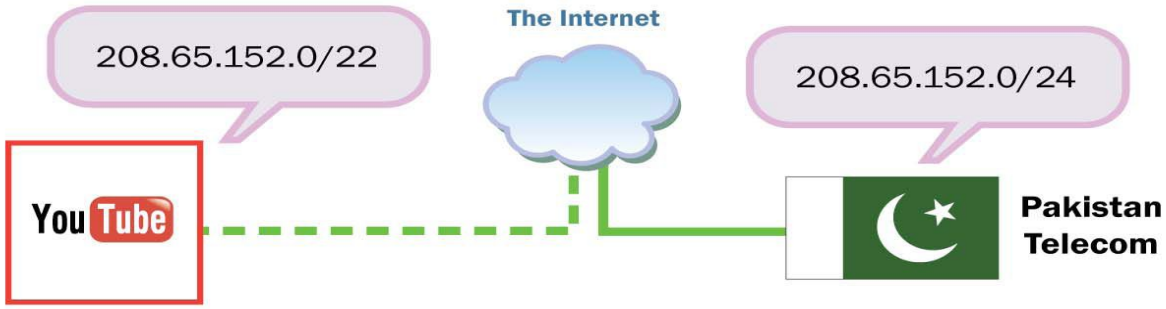
APNIC

APNIC Announcement on 25/10/2012

- Changes to its Resource Public Key Infrastructure (RPKI) system
- New “trust anchor” certificates
- Align RPKI model with the administrative and associated registry structure

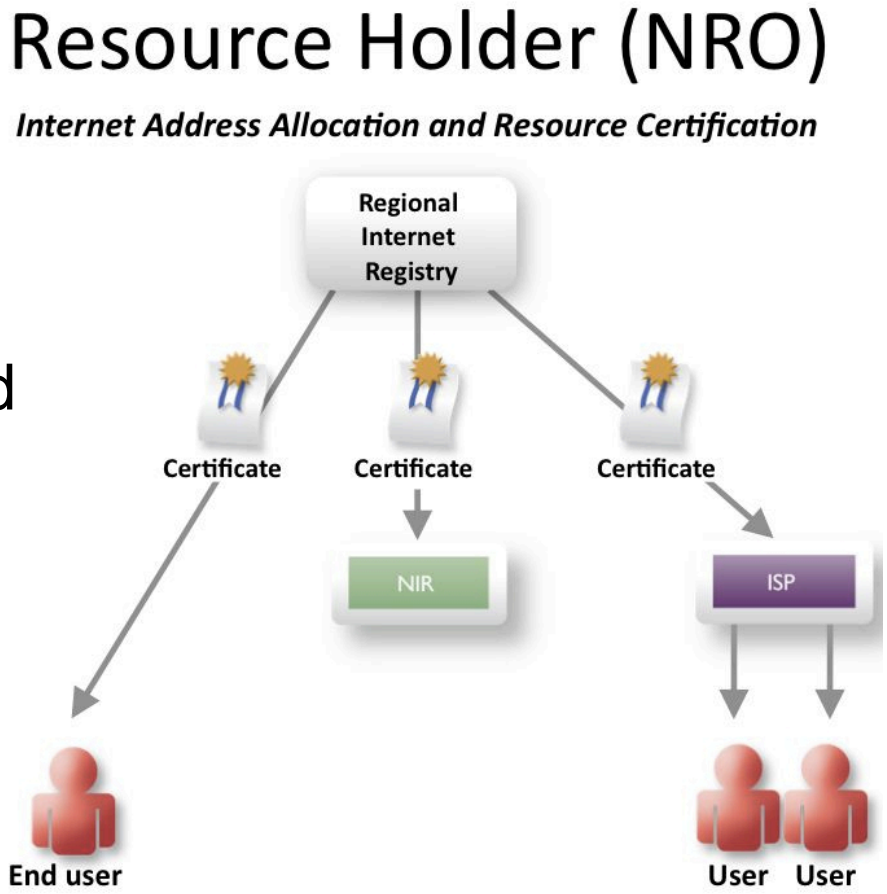
What is RPKI?

- Designed to secure the Internet's routing infrastructure
- Only the legitimate holder can advertise their prefix to the Internet
- Prevent those incidence of route hijacking (sometime by mistake)



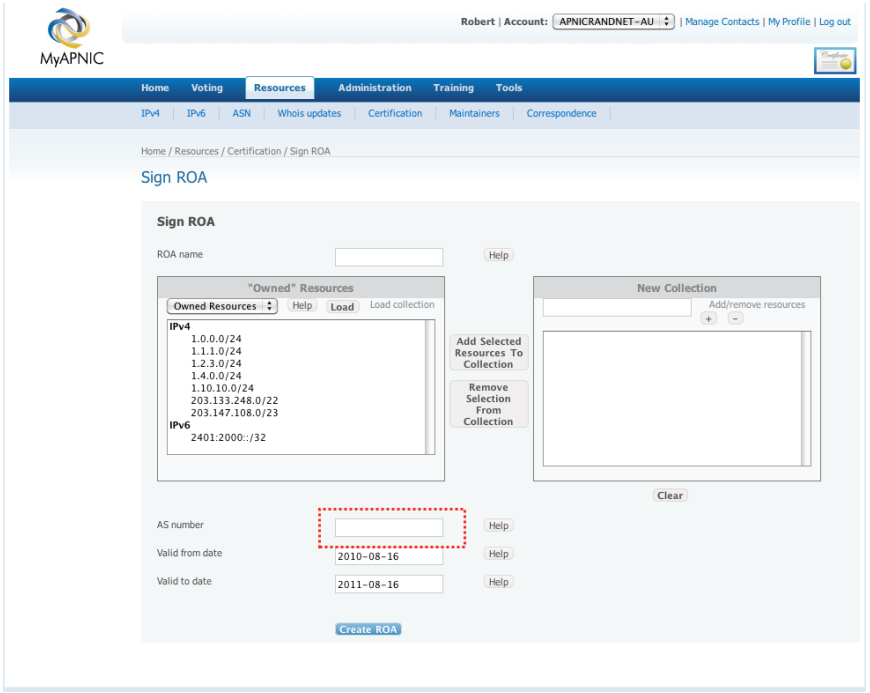
How It Works?

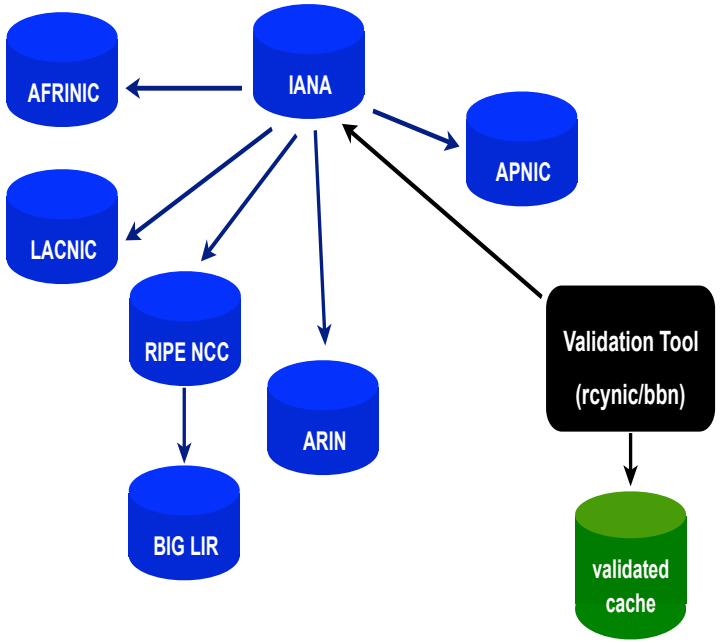
- Initially each RIR issued a self-signed trust anchors to the address they received from IANA
- Contains all resources from a **single trust anchor** managed by the RIR
- It was irrespective of their source



How It Works?

RPKI Validation: Distributed Repository





How It Works?

RPKI Validation: RPKI-RTR protocol


```
router bgp 65000
bgp log-neighbor-changes
bgp rpki server tcp 198.180.150.1 port 42420 refresh 60
```

How does it look in BGP table then?

BGP Table

RPKI Validation: RPKI-RTR protocol

```
router1#sh bgp ipv4 unicast
BGP table version is 45, local router ID is 203.176.189.15
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
   V 0.0.0.0          0.0.0.0                  0 i
*>  N 67.21.36.0/24    199.238.113.10                 0 3130 2914 293 3970 e
*>  V 85.118.184.0/21  199.238.113.10                 0 3130 2914 174 29485 29485 57785 i
*>  I 98.128.0.0/24    199.238.113.10           0     0 3130 i
*>  V 98.128.0.0/16    199.238.113.10           0     0 3130 i
*>  N 98.128.1.0/24    199.238.113.10           0     0 3130 i
*>  N 98.128.2.0/24    199.238.113.10           0     0 3130 i
```

```
route-map validity-0
    match rpki-invalid
    drop
route-map validity-1
    match rpki-not-found
    set localpref 50
// Valid defaults to 100
```

Use route-map to accept RPKI validated route

```
route-map validity-0
    match rpki-unknown
    set metric 50
route-map validity-1
    match rpki-invalid
    set metric 25
route-map validity-2
    set metric 100
```

What Is The New Challenge?

- Inter RIR transfer process is implemented now
- It requires an efficient way to reflect the changes to an RIR's resource holding
- Without revoking and reissuing the affected RIR trust anchor
- The split anchor model allows more granular updates, affecting only the certification path that covers the transferred resources

New Split Anchor Model

- APNIC has published five new self-signed certificates
- One for those address space given by IANA for this region
- Four for other self-signed certificates for resource acquired from each other RIR

What Changes For Operational Network?

- Organizations that RPKI origin validation on their router software need to make updates to their routing configuration
- If you already have the APNIC trust anchor you should refresh this with the complete new set of five
- Take note of any required configuration changes in your software

Find More…..

- APNIC to Upgrade to Split Trust Anchor RPKI:
  http://www.apnic.net/publications/news/2012/apnic-to-upgrade-to-split-trust-anchor-rpki
- Resource Public Key Infrastructure (RPKI) FAQ:
  http://www.apnic.net/services/services-apnic-provides/helpdesk/faqs/rpki/
- Resource certification
  http://www.apnic.net/services/services-apnic-provides/resource-certification

Questions?

APNIC

Thank you!

End of Session

APNIC