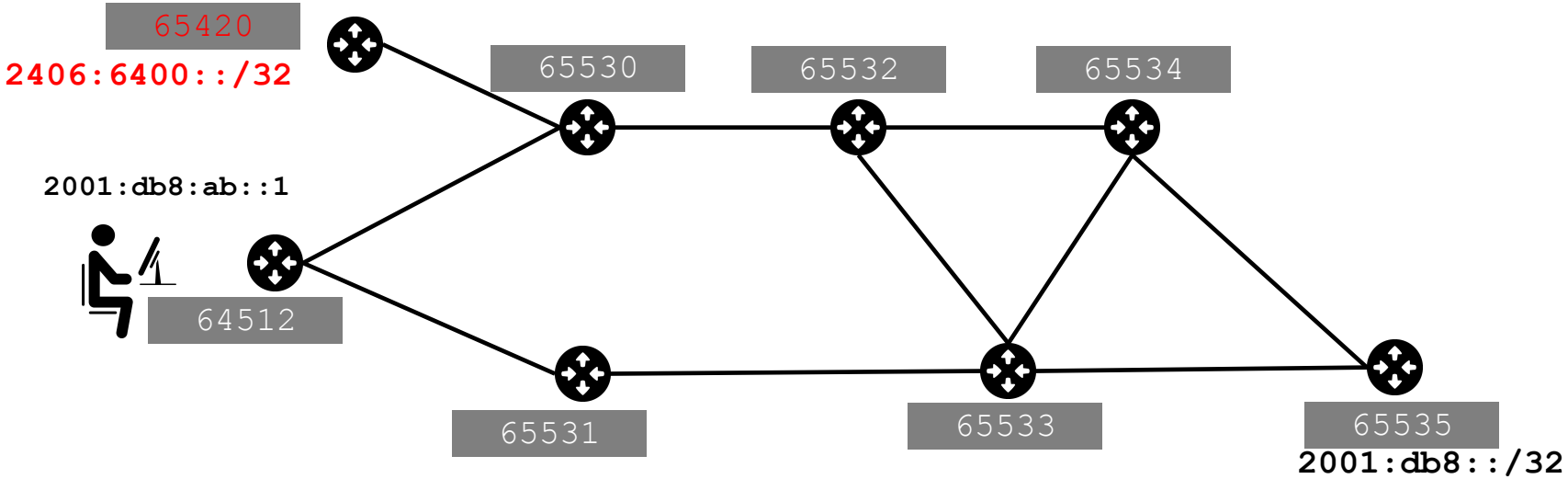
Route Hijacking and the role of RPKI in Securing Internet Routing Infrastructure

Fakrul Alam

Senior Training Officer
APNIC
fakrul@apnic.net

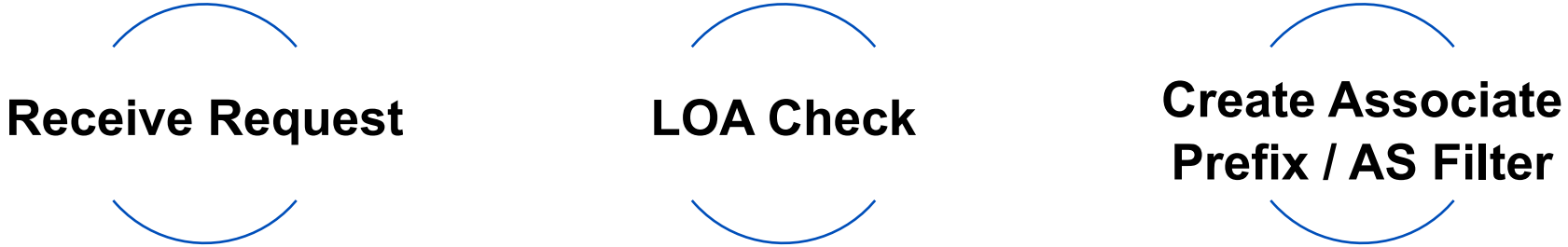
BGP 101

Network	Next Hop	AS_PATH	Age	Attrs
> 2406:6400::/32	2001:df2:ee00::1	65531 65533 65535	05:30:49	[{Origin: i}]
> 2406:6400::/32	**2001:df2:ee11::1**	**65530 65420**	**05:30:49**	**[{Origin: i}]**

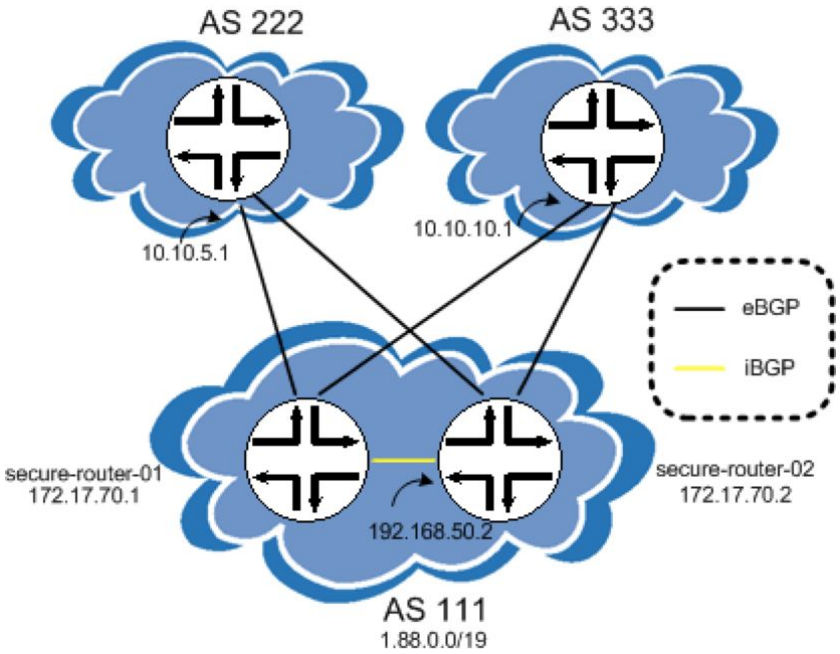


Current Practice

- Filtering limited to the edges facing the customer
- Filters on peering and transit sessions are often too complex or take too many resources
- Check prefix before announcing it



Filter Where?



- Secure BGP Templates
  - http://www.cymru.com/gillsr/documents/junos-bgp-template.htm
  - https://www.team-cymru.org/ReadingRoom/Templates/secure-bgp-template.html

RPKI

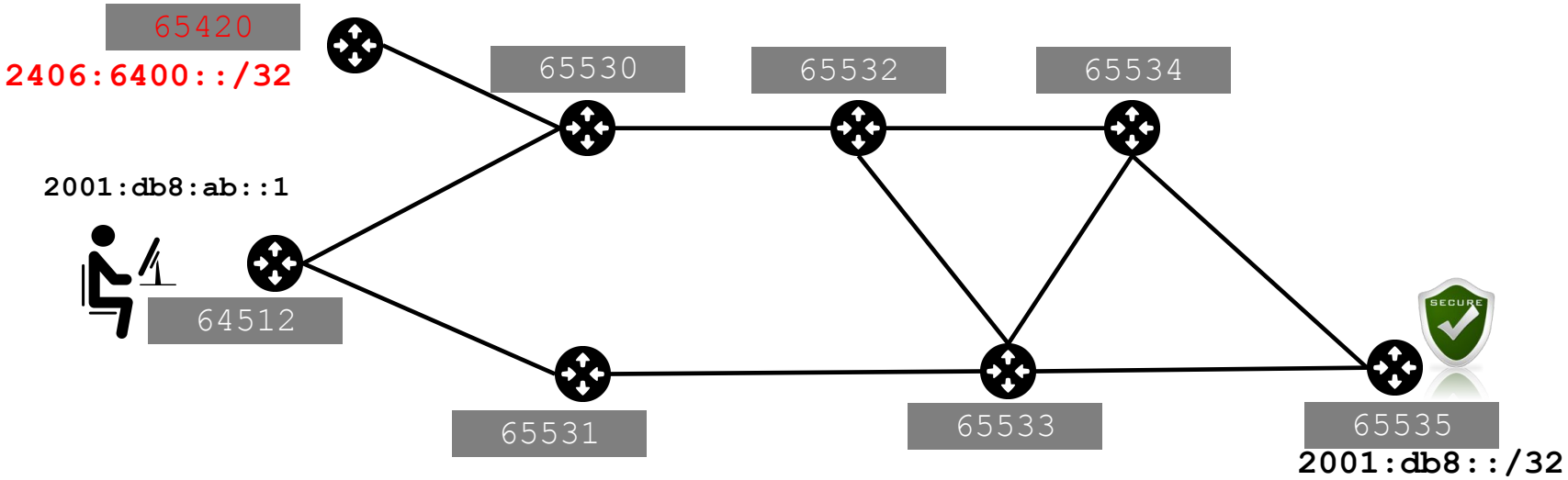
Resource Public Key Infrastructure

IP Address & AS Number

Digital Certificate

BGP 101 + RPKI

```
Network                 Next Hop            AS_PATH                    Age         Attrs
 V*>  2406:6400::/32    2001:df2:ee00::1    65531 65533 65535          05:30:49    [{Origin: i}]
 I >                    2001:df2:ee11::     65530 65420                05:30:49    [{Origin: i}]
 2406:6400::/32         1
```



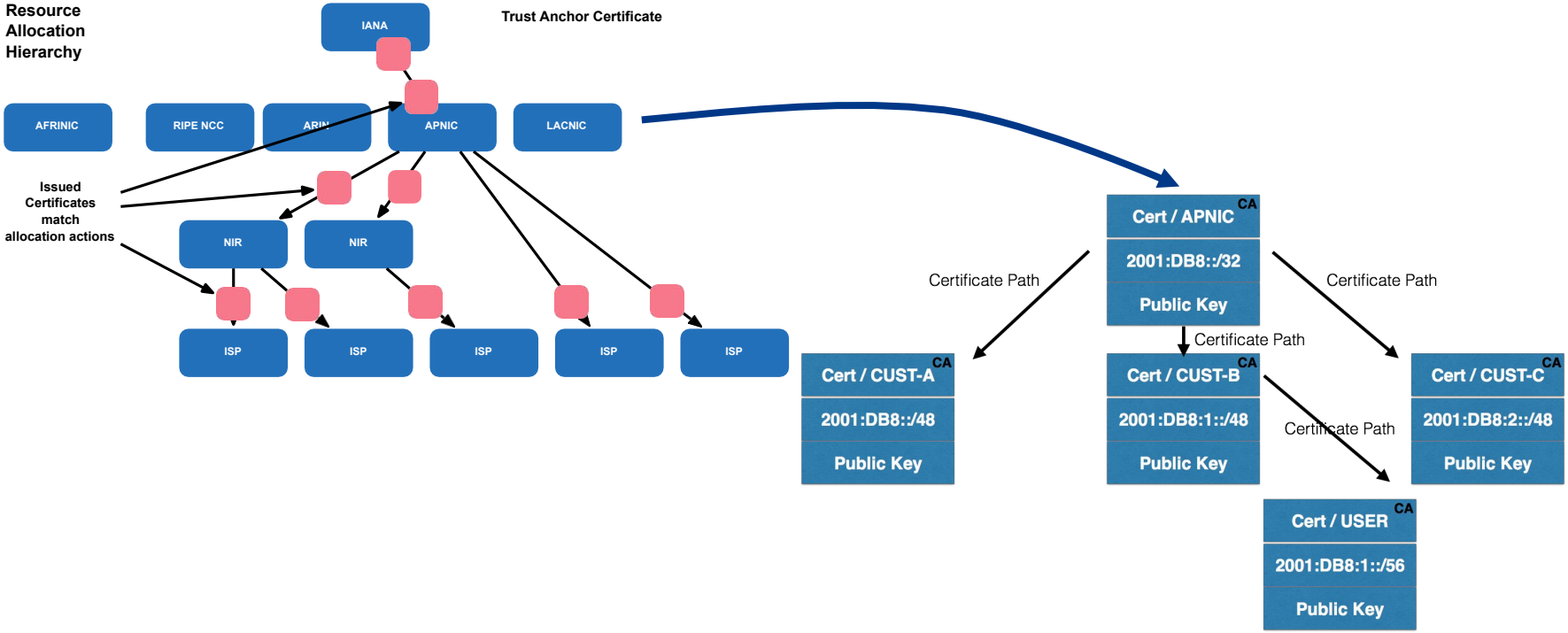
PKI In Other Application

- **HTTPS**
  - Web Address as **RESOURCE**
  - Hierarchical Trust Model
  - CA as the root of the **TRUST**
  - Browser does the **VERIFICATION**
- **DNSSEC**
  - Zone as **RESOURCE**
  - Hierarchical Trust Model
  - . as the root of the **TRUST**
  - DNS Resolver does the **VERIFICATION**

What About RPKI?

The Eco System

RPKI Trust Anchor



RPKI Implementation

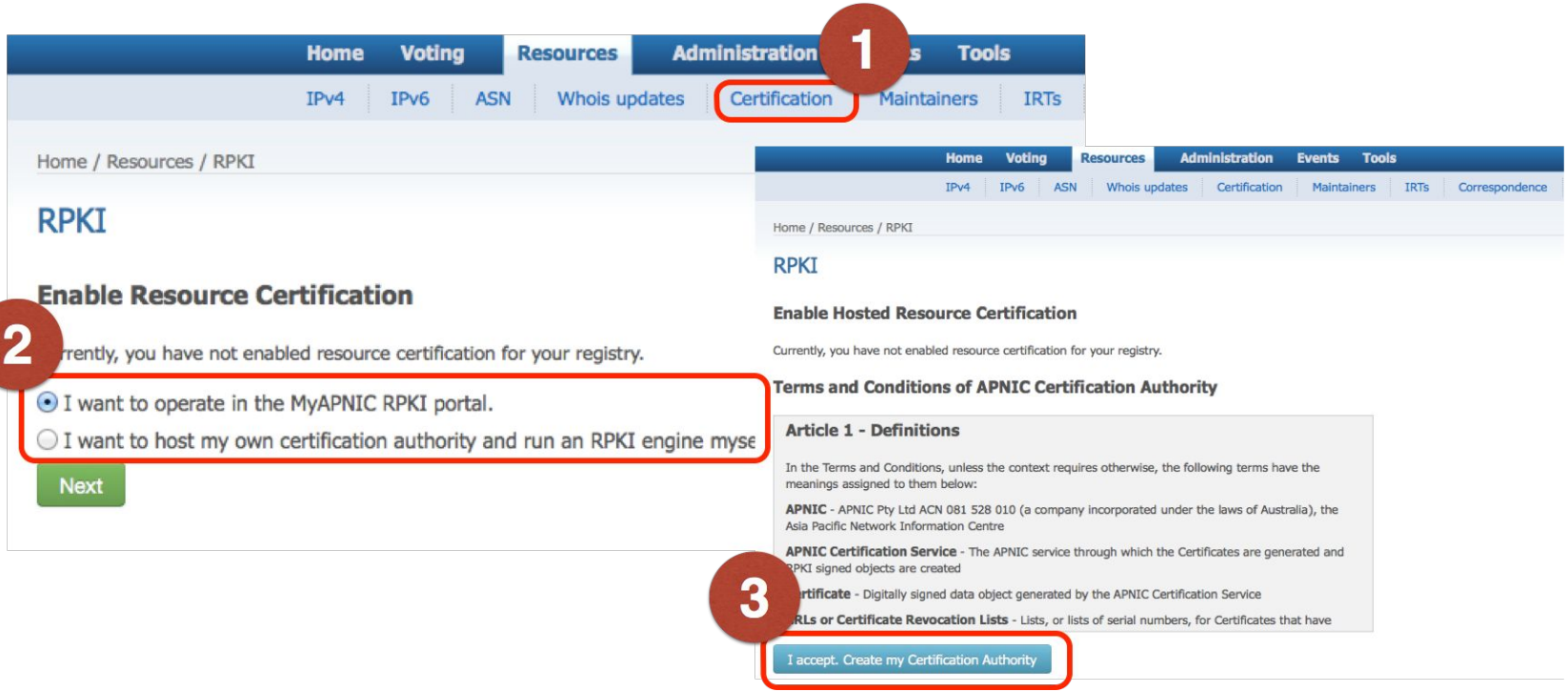
1. Publish ROA

2. RPKI Cache Validator

3. Router Configuration

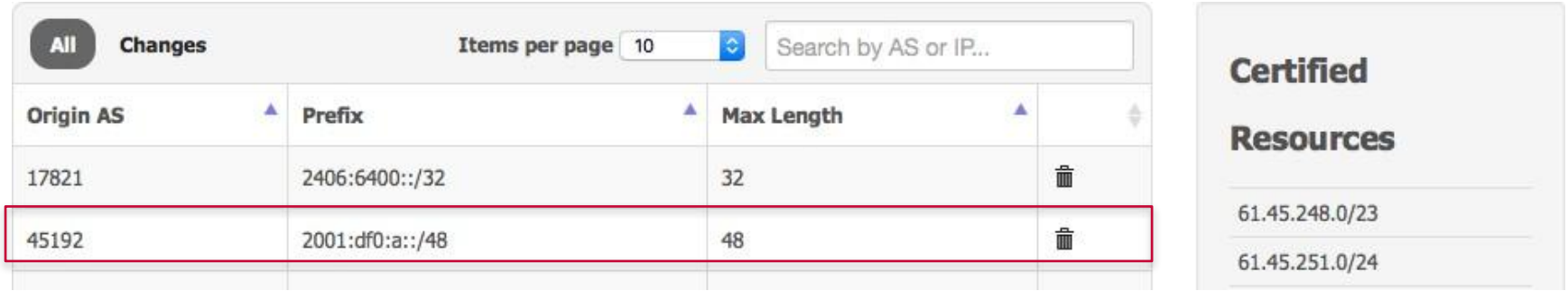
- **As an Announcer/LIR**
  - You choose if you want certification
  - You choose if you want to create ROAs
  - You choose AS, max length
- **As a Relying Party**
  - You can choose if you use the validator
  - You can override the lists of valid ROAs in the cache, adding or removing valid ROAs locally
  - You can choose to make any routing decisions based on the results of the BGP Verification (valid/invalid/unknown)

Activate RPKI engine



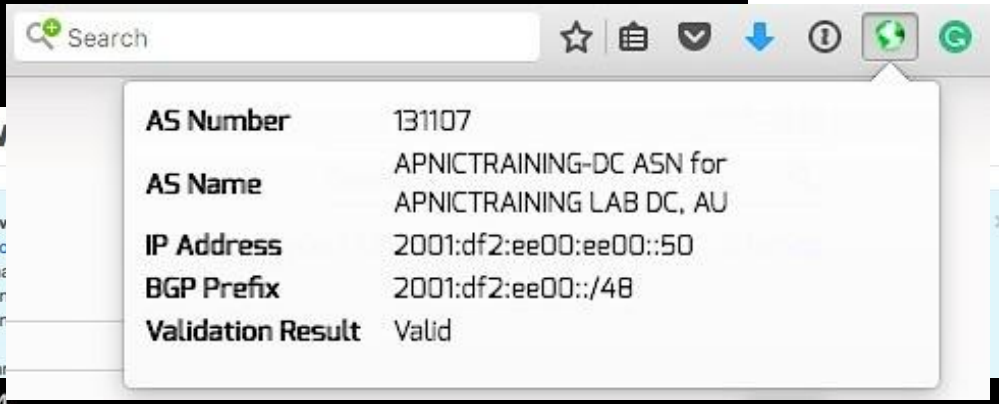
Create ROA

- Create ROA for smaller block.



How Do We Verify?

```
whois -h whois.bgpmon.net " --roa 45192 202.125.97.0/24"
0 - Valid
------------------------
ROA Details
------------------------
Origin ASN:       AS45192
Not valid Before: 2016-06
Not valid After:  2020-07
Trust Anchor:     rpki.ap
Prefixes:         202.125
```



BGP Preview

This page provides a preview
- The RIPE NCC Route Co
- BGP announcements tha
- The validation rules defin
- The validated ROAs four

Please note that the BGP an

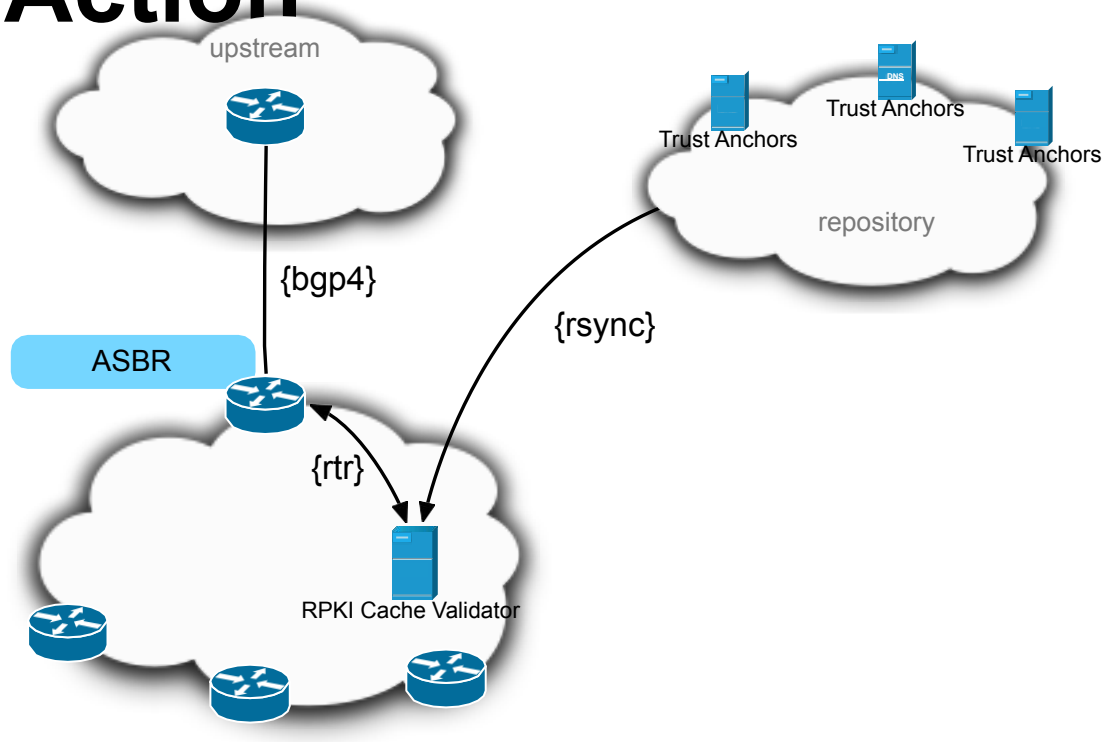
```
fakrul@gobgp:~$ gobgp global rib 202.125.96.0/24
    Network          Next Hop            AS_PATH                  Age        Attrs
V*> 202.125.96.0/24  202.12.29.113       4608 24115 4826 131107   00:06:26   [{Origin: i} {Med: 0} {LocalPref: 100}]
```

ASN	Prefix	Validity
131107	202.125.96.0/24	VALID

First Previous 1 Next Last

Showing 1 to 1 of 1 entries (filtered from 691,209 total entries)

RPKI in Action



- {bgp4} Routers validate updates from other BGP peers
- {rtr} Caches feeds routers using RTR protocol with ROA information
- {rsync} Caches retrieves and cryptographically validates certificates & ROAs from repositories

RPKI Implementation Issues

RPKI Data Violation : Invalid ASN

- Invalid origin AS is visible

```
fakrul@gobgp:~/go$ gobgp global rib 213.192.242.0/23
   Network             Next Hop             AS_PATH                  Age        Attrs
I*> 213.192.242.0/23    202.12.29.113        4608 1221 4637 1273 12541 01:22:01   [{Origin: i} {Med: 0} {LocalPref: 100}]


fakrul@gobgp:~/go$ whois -h whois.bgpmon.net " --roa 12541 213.192.242.0/23 "
2 - Not Valid: Invalid Origin ASN, expected 8903
```

- From private ASN!

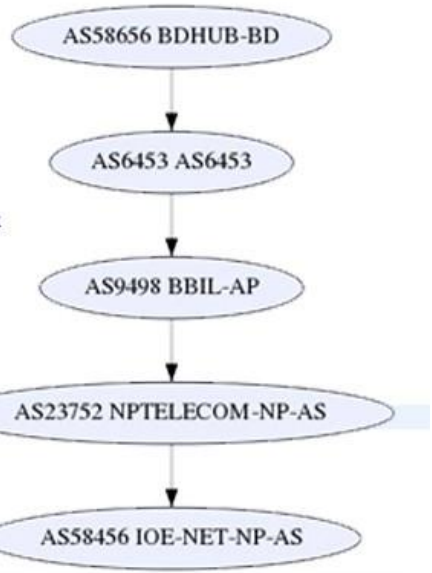
```
fakrul@gobgp:~/go$ gobgp global rib 103.10.77.0/24
   Network             Next Hop             AS_PATH                                  Age        Attrs
I*> 103.10.77.0/24      202.12.29.113        4608 1221 4637 174 9498 58587 45951 65530 01:20:25   [{Origin: i} {Med: 0} {LocalPref: 100}]


fakrul@gobgp:~/go$ whois -h whois.bgpmon.net " --roa 65530 103.10.77.0/24"
2 - Not Valid: Invalid Origin ASN, expected 45951
```

RPKI Data Violation : Fixed Length Mismatch

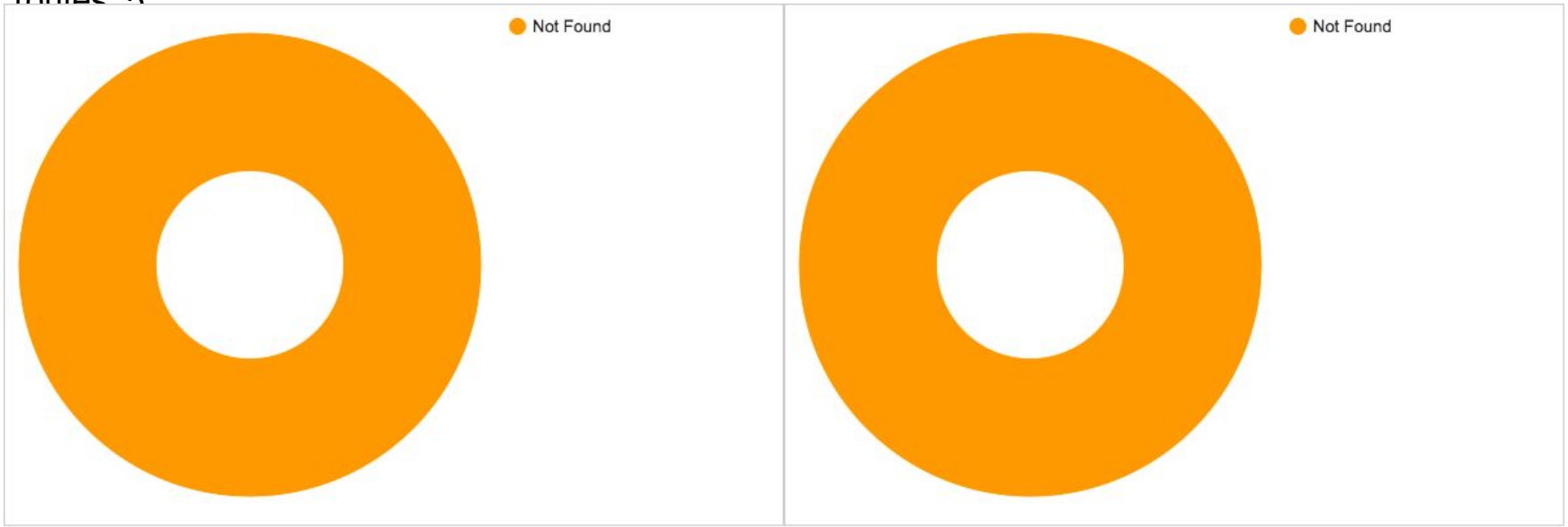
- Most of the cases involve an invalid prefix (fixed length mismatch)
  – Further allocation to the customer


```
{
  "validated_route": {
    "route": {
      "origin_asn": "AS58456",
      "prefix": "202.70.91.0/24"
    },
    "validity": {
      "state": "Invalid",
      "reason": "as",
      "description": "At least one VRP Covers the Route Prefix
      "VRPs": {
        "matched": [],
        "unmatched_as": [
          {
            "asn": "AS23752",
            "prefix": "202.70.64.0/19",
            "max_length": 19
          }
        ],
        "unmatched_length": []
      }
    }
  }
}
```

Fiji

Total ASNs delegated by RIR: 8, Visible IPv4 routes: 50, Visible IPv6 routes: 5



This graph generated on Mon 21 Nov 2016 15:23:20 AEST

http://rpki.apnictraining.net/output/fj.html

Moving Forward

- RPKI adoption is growing
  - You are encouraged to create ROA. Experiment, test, play and develop
  - You can implement in you infrastructure and do origin validation
- Something to consider
  - Upgrade at least ASBRs to RPKI capable code
  - In most cases, operators create ROAs for min length and advertise longest prefix
  - Some ROAs are invalid due to further allocation to customers
- https://www.apnic.net/ROA

Data Collection

- GoBGP
  - https://github.com/osrg/gobgp
- RPKI Dashboard
  - https://github.com/remydb/RPKI-Dashboard
- RIPE RPKI Statistics
  - https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html
- RIPE Cache Validator API
  - http://rpki-validator.apnictraining.net:8080/export

Thank You