

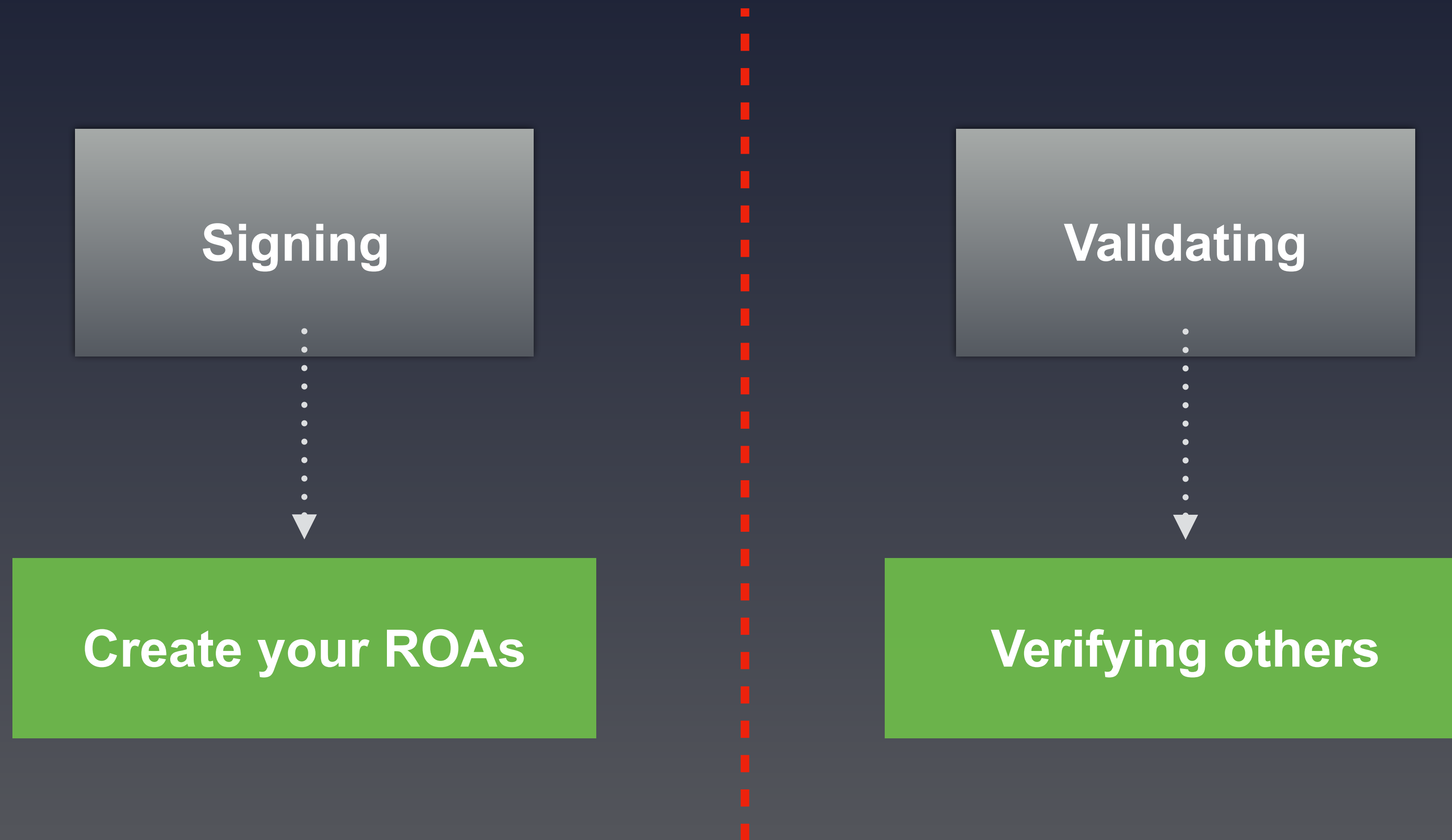


RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE NCC Open House

The Future of RPKI

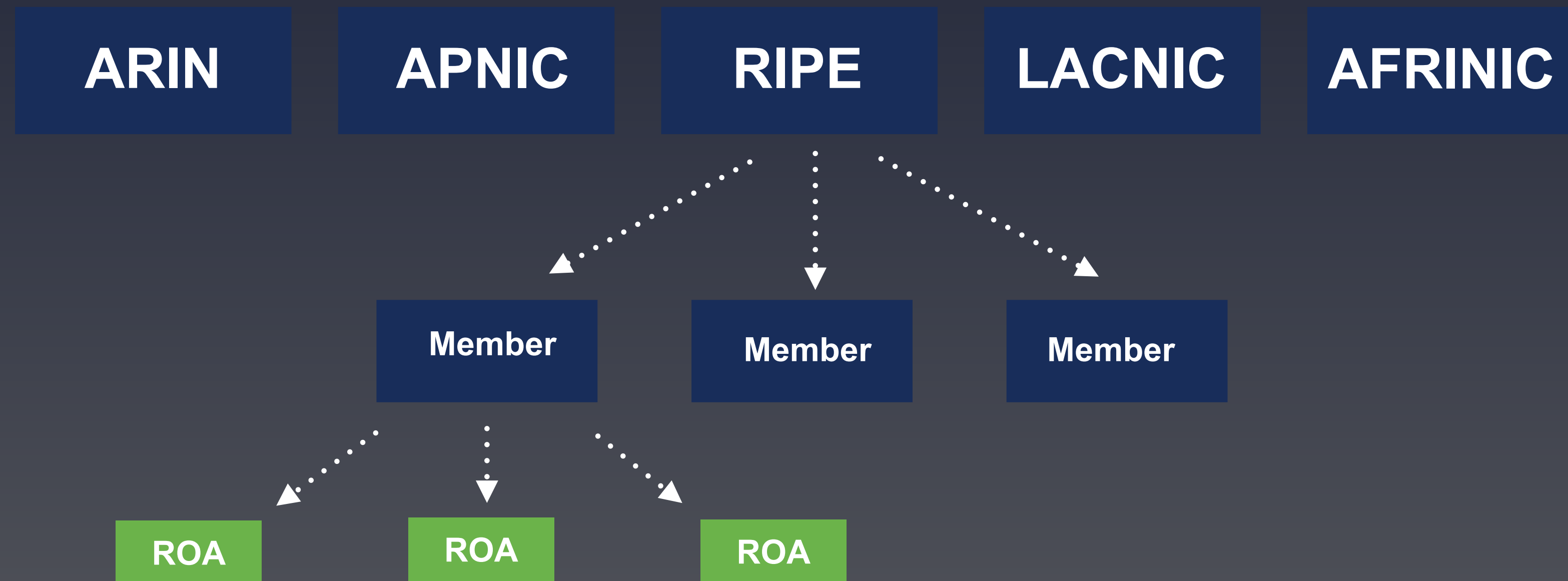
Two Elements of RPKI



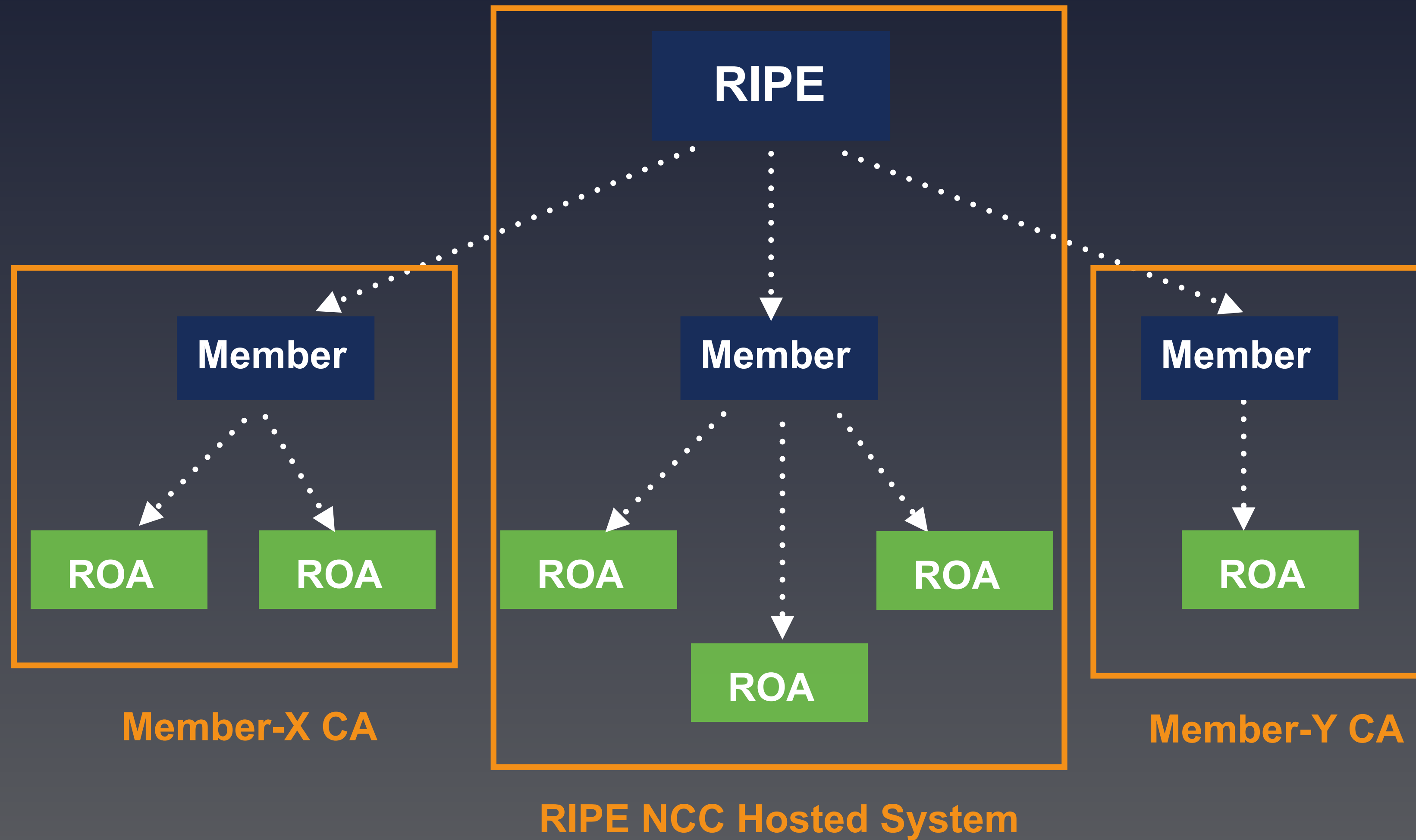
RPKI Certificate Structure



Certificate hierarchy follows allocation hierarchy



Hosted or Delegated RPKI





RPKI Trends

2020: The Year of RPKI



- Serious uptake in Route Origin Validation at transits and IXPs
- Resulting in decrease of Invalid RPKI BGP announcements
- High uptake in signing objects at other Regional Internet Registries
- All major routing vendors are now on board
- Increase in delegated RPKI
- Also some outages at different Trust Anchors

Status of Transit and Cloud



Name	Type	Details	Status
Telia	Transit	Signed & Filtering	Safe
Cogent	Transit	Signed & Filtering	Safe
GTT	Transit	Signed & Filtering	Safe
NTT	Transit	Signed & Filtering	Safe
Hurricane Electric	Transit	Signed & Filtering	Safe
Tata	Transit	Signed & Filtering	Safe
PCCW	Transit	Signed & Filtering	Safe
RETN	Transit	Partially Signed & Filtering	Safe
Cloudflare	Cloud	Signed & Filtering	Safe
Amazon	Cloud	Signed & Filtering	Safe
Netflix	Cloud	Signed & Filtering	Safe
Wikimedia Foundation	Cloud	Signed & Filtering	Safe
Scaleway	Cloud	Signed & Filtering	Safe

More Work Underway



Name	Type	Details	Status
Telstra	Transit	AS1221 done, AS4637 planned	Partially Safe
AT&T	ISP	Signed & Filtering peers	Partially Safe
Google	Cloud	Signed & Filtering planned	Partially Safe
You?	?	?	?


How About IXPs?





Name	Type	Details	Status
LINX	IXP	Signed & Filtering	Safe
AMS-IX	IXP	Signed & Filtering	Safe
Netnod	IXP	Signed & Filtering	Safe
DE-CIX	IXP	Signed & Filtering	Safe
INEX	IXP	Signed & Filtering	Safe
LONAP	IXP	Signed & Filtering	Safe
NL-IX	IXP	Signed & Filtering	Safe
FRANCE-IX	IXP	Signed & Filtering	Safe
UAE-IX	IXP	Signed & Filtering	Safe
MSK-IX	IXP	Signed & Filtering	Safe
MIX-IT	IXP	Signed & Filtering	Safe


So, How Bad Are Things?




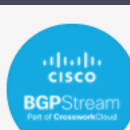
 Cisco BGPStream @bgpstream · 31 dec. 2020 ...
BGP,HJ,hijacked prefix AS206688 185.59.178.0/24, AS_GMFIO, GB,-,By AS1828 UNITAS, US, bgpstream.com/event/266050


 Cisco BGPStream @bgpstream · 31 dec. 2020 ...
BGP,HJ,hijacked prefix AS206688 185.59.178.0/24, AS_GMFIO, GB,-,By AS1828 UNITAS, US, bgpstream.com/event/266050

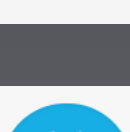
 Cisco BGPStream @bgpstream · 31 dec. 2020 ...
BGP,HJ,hijacked prefix AS6401 216.129.73.0/24, ALLST-6401, CA,-,By AS7385 ALLSTREAM, US, bgpstream.com/event/266018


 Cisco BGPStream @bgpstream · 30 dec. 2020 ...
BGP,HJ,hijacked prefix AS701 100.1.66.0/24, UUNET, US,-,By AS265724 Teneda Corporacion CIA. LTDA, EC, bgpstream.com/event/265991


 Cisco BGPStream @bgpstream · 30 dec. 2020 ...
BGP,HJ,hijacked prefix AS200485 185.104.156.0/24, NASSIRAQ, IQ,-,By AS136970 YISUCLOUDLTD-AS-AP YISU CLOUD LTD, HK, bgpstream.com/event/265969


 Cisco BGPStream @bgpstream · 30 dec. 2020 ...
BGP,HJ,hijacked prefix AS3473 137.232.111.0/24, DNIC-AS-03473, US,-,By AS5323 DNIC-ASBLK-05120-05376, US, bgpstream.com/event/265930


 Cisco BGPStream @bgpstream · 30 dec. 2020 ...
BGP,HJ,hijacked prefix AS265123 143.202.166.0/23, Connect Viradouro Proved,-,By AS6762 SEABONE-NET TELECOM ITAL, bgpstream.com/event/265925


 Cisco BGPStream @bgpstream · 30 dec. 2020 ...
BGP,HJ,hijacked prefix AS212643 194.124.64.0/24, CODETINI-AS, NL,-,By AS57878 PRAGER-IT, AT, bgpstream.com/event/265920

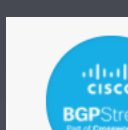
 Cisco BGPStream @bgpstream · 29 dec. 2020 ✓
BGP,HJ,hijacked prefix AS3356 45.82.206.0/24, LEVEL3, US,-,By AS57878 PRAGER-IT, AT, bgpstream.com/event/265917


 Cisco BGPStream @bgpstream · 29 dec. 2020 ✓
BGP,HJ,hijacked prefix AS3356 2.59.175.0/24, LEVEL3, US,-,By AS57878 PRAGER-IT, AT, bgpstream.com/event/265916


 Cisco BGPStream @bgpstream · 29 dec. 2020 ✓
BGP,HJ,hijacked prefix AS52797 177.39.238.0/24, ISH Tecnologia SA, BR,-,By AS55002 DEFENSE-NET, US, bgpstream.com/event/265891


 Cisco BGPStream @bgpstream · 29 dec. 2020 ✓
BGP,HJ,hijacked prefix AS3 103.151.128.0/24, MIT-GATEWAYS, US,-,By AS7 DSTL, EU, bgpstream.com/event/265885


 Cisco BGPStream @bgpstream · 29 dec. 2020 ✓
BGP,HJ,hijacked prefix AS4134 61.29.243.0/24, CHINANET-BACKBONE No.31,-,By AS138607 HHC-AS-AP HK HERBTECK CO, bgpstream.com/event/265880


 Cisco BGPStream @bgpstream · 29 dec. 2020 ✓
BGP,HJ,hijacked prefix AS59050 192.23.191.0/24, CLOUD-ARK Beijing Cloud,-,By AS7468 CYBEREC-AS-AP Cyber Expr, bgpstream.com/event/265877

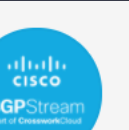
 Cisco BGPStream @bgpstream · 29 dec. 2020 ✓
BGP,HJ,hijacked prefix AS267751 45.167.121.0/24, LANTECH SOLUCIONES SOCIE,-,By AS131578 BFSUNET Beijing Foreign , bgpstream.com/event/265876

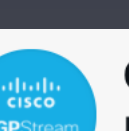
 Cisco BGPStream @bgpstream · 28 dec. 2020 ✓
BGP,HJ,hijacked prefix AS62717 38.69.142.0/24, HARMONIZE-NETWORKS, CA,-,By AS18997 RUNETWORKS, CA, bgpstream.com/event/265838


 Cisco BGPStream @bgpstream · 28 dec. 2020 ✓
BGP,HJ,hijacked prefix AS22611 216.194.165.0/24, INMOTION, US,-,By AS23980 YU-AS-KR Yeungnam University, KR, bgpstream.com/event/265835

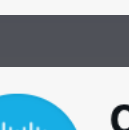
 Cisco BGPStream @bgpstream · 28 dec. 2020 ✓
BGP,HJ,hijacked prefix AS6939 184.105.139.0/24, HURRICANE, US,-,By AS23980 YU-AS-KR Yeungnam University, KR, bgpstream.com/event/265834

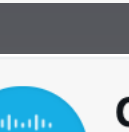
 Cisco BGPStream @bgpstream · 28 dec. 2020 ✓
BGP,HJ,hijacked prefix AS9534 121.122.16.0/24, MAXIS-AS1-AP Binariang B,-,By AS23980 YU-AS-KR Yeungnam Univer, bgpstream.com/event/265833

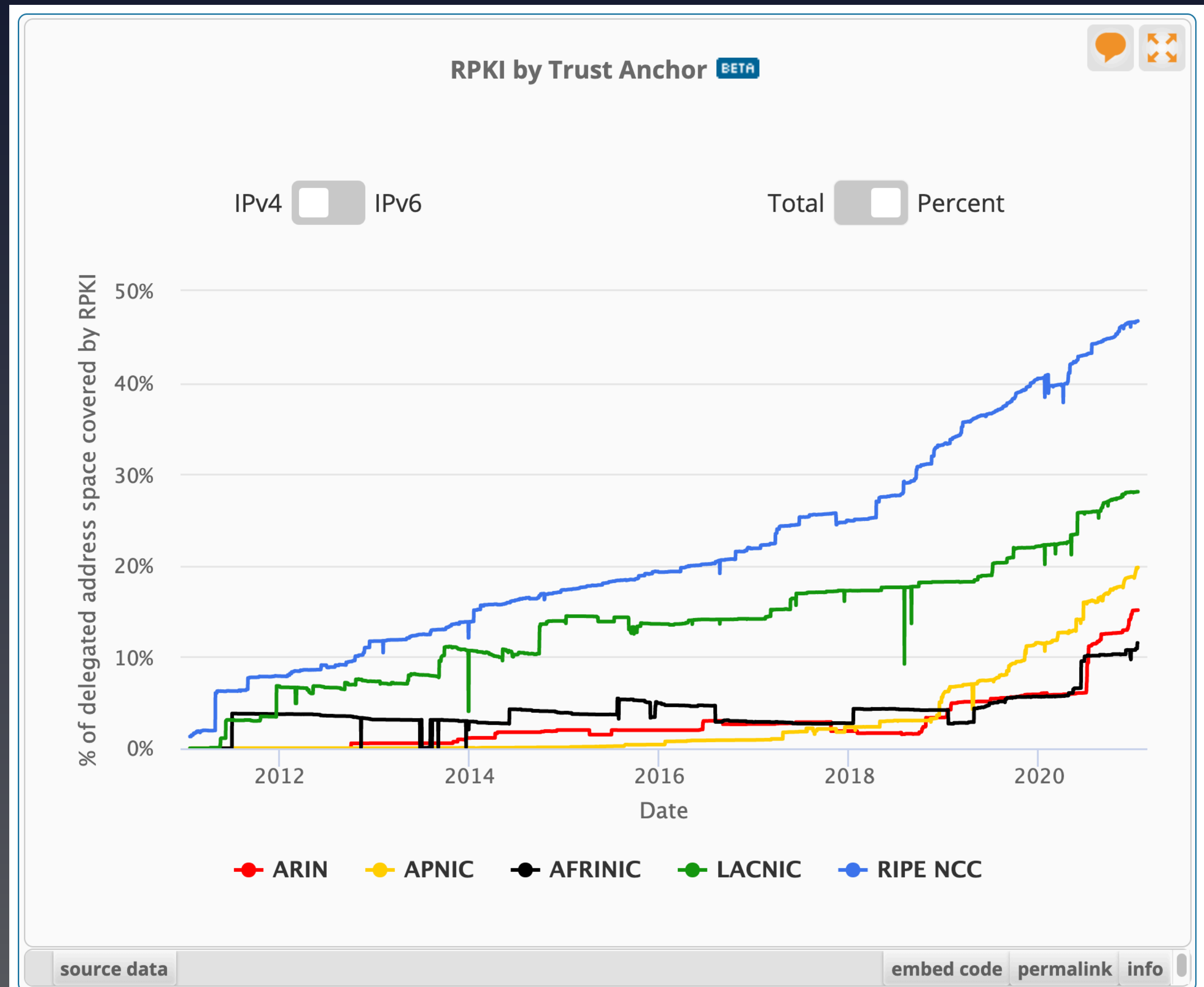
 Cisco BGPStream @bgpstream · 28 dec. 2020 ✓
BGP,HJ,hijacked prefix AS14987 104.152.52.0/24, RETHEMHOSTING, US,-,By AS23980 YU-AS-KR Yeungnam University, KR, bgpstream.com/event/265832

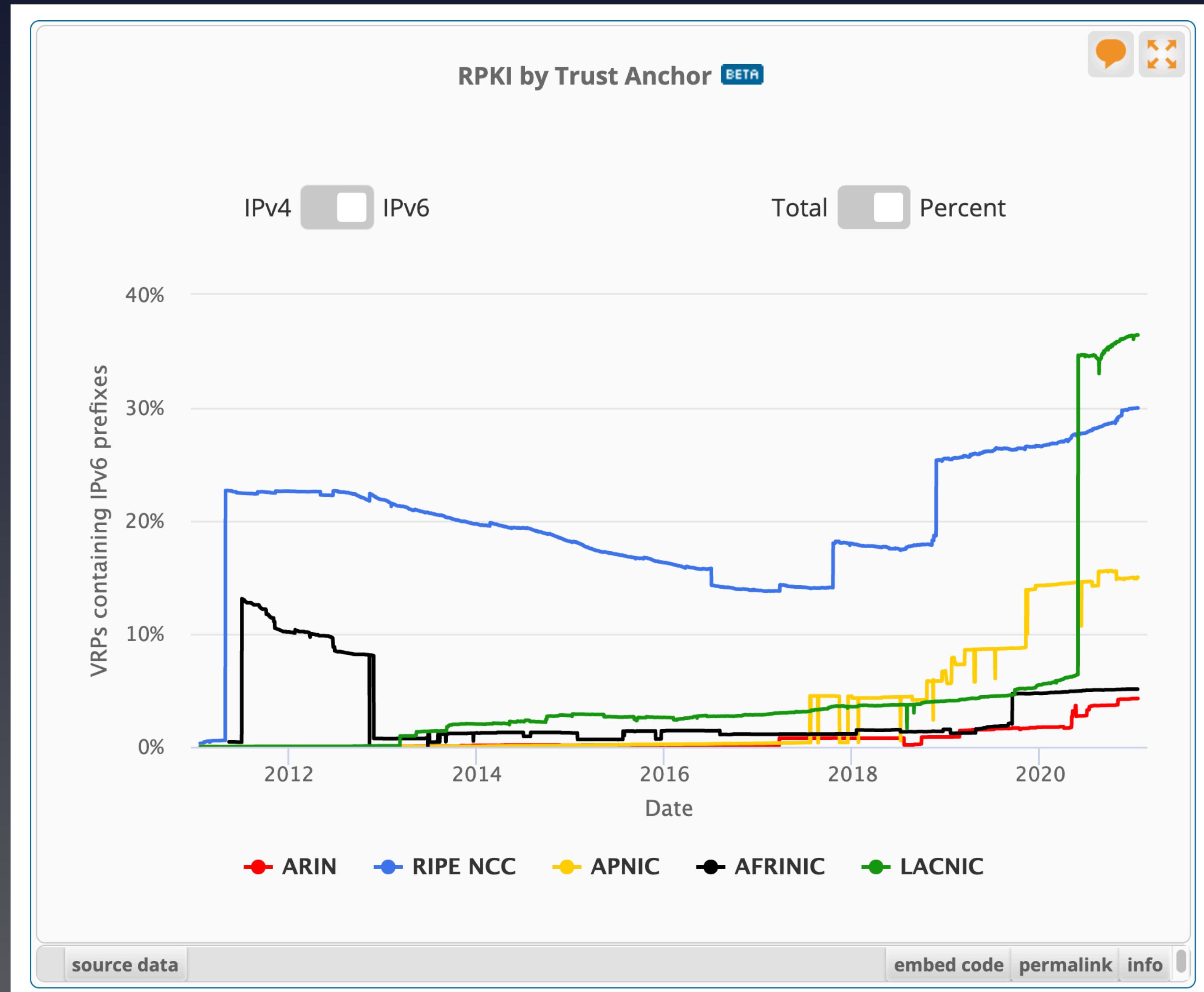
 Cisco BGPStream @bgpstream · 27 dec. 2020 ✓
BGP,HJ,hijacked prefix AS65545 45.188.207.0/24, -,By AS268625 NETFAST TELECOMUNICACOES E MULTIMIDIA LTDA, BR, bgpstream.com/event/265779

 Cisco BGPStream @bgpstream · 27 dec. 2020 ...
BGP,HJ,hijacked prefix AS7377 44.136.161.0/24, UCSD, US,-,By AS56199 THOMAX-AU THOMAX TECH SYD, AU, bgpstream.com/event/265774

 Cisco BGPStream @bgpstream · 26 dec. 2020 ✓
BGP,HJ,hijacked prefix AS204544 5.56.132.0/24, MOBINHOST, IR,-,By AS41689 FCP-NETWORK, IR, bgpstream.com/event/265766

 Cisco BGPStream @bgpstream · 26 dec. 2020 ✓
BGP,HJ,hijacked prefix AS208675 45.89.137.0/24, ZARINPAL, IR,-,By AS41689 FCP-NETWORK, IR, bgpstream.com/event/265764





Key Takeaways



- Creating a ROA helps – a lot!
- Most large transit providers and IXPs perform Route Origin Validation (ROV)
- Many ISPs that have BGP customers don't. **This is problematic.**
- Just ROV is not the holy grail for all BGP mishaps.
 - We really need Path Validation



Plans for the Future of RPKI

At the RIPE NCC

Focus on Resiliency



- Significant improvements in metrics/monitoring finalised
 - Usage of Prometheus with Grafana for visualisations
 - Hooking up with SMS alerting for engineers on 24/7 duty
- Deployment of rsync/RRDP into AWS in progress
 - Multiple regions/availability zones with aim of very high availability
 - RRDP is already in AWS but with simpler architecture – the goal is to also move rsync to similar architecture
 - Redundant fully functional infrastructure in our current data centres to provide very high resiliency being evaluated by the teams

Focus on Security



- Performed an RFC compliance audit
- Building an RPKI specific audit framework in SOC 2 type II
- For 2021:
 - Publish a report from the RFC compliance audit
 - Performing SOC 2 type II audit, publish a SOC 3 report
 - Performing penetration test
 - Performing Red Team test

Upcoming Work from the IETF

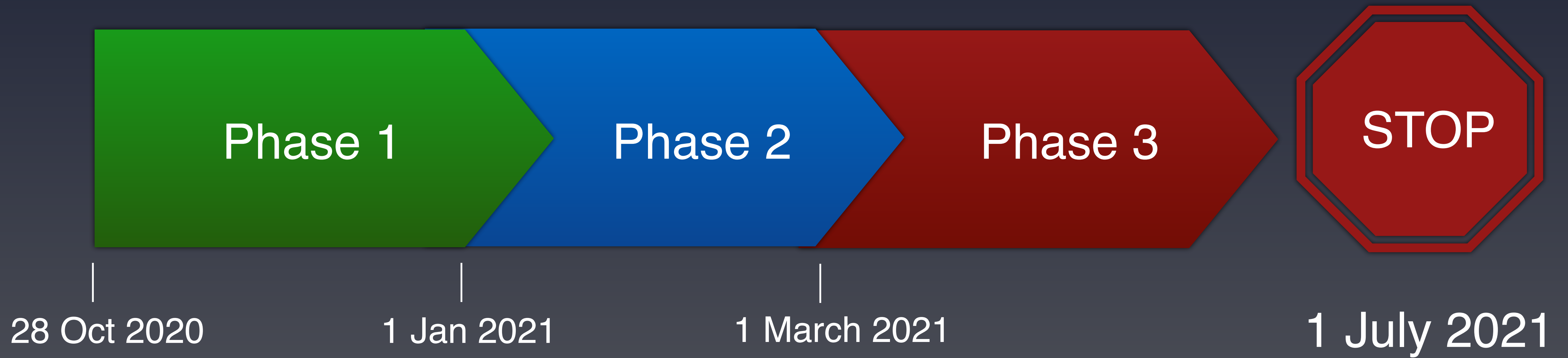


- Autonomous System Provider Authorisation (ASPA)
 - <https://tools.ietf.org/html/draft-ietf-sidrops-aspa-profile-04>
- Validation Reconsidered
 - <https://tools.ietf.org/html/rfc8360>
- Resource Tagged Attestations (RTA)
 - <https://tools.ietf.org/html/draft-michaelson-rpki-rta-02>



Deprecating the RIPE NCC Validator

Timeline



Phase 1



- 28 October 2020 - 31 December 2021
- Work continues as normal:
 - Features
 - RFC implementations
 - Policy implementations (AS0 in other regions)
 - Bug fixes
 - Security fixes
- Community will be informed of future timeline

Phase 2



- 1 January 2021 - 28 February 2021
- No new features will be implemented
- Continued work on:
 - RFC implementations
 - Policy implementations (AS0 in other regions)
 - Bug fixes
 - Security fixes
- Training material and website will be updated

Phase 3



- 1 March 2021 - 30 June 2021
- No more work on RFC and policy implementations
- Continued work on:
 - Bug fixes
 - Security fixes
- On 1 July 2021, we will archive the RIPE NCC RPKI Validator

Alternatives



- All are open source:
 - Routinator - <https://github.com/NLnetLabs/routinator/>
 - FORT - <https://github.com/NICMx/FORT-validator/>
 - OctoRPKI - <https://github.com/cloudflare/cfrpki>
 - RPKI-client - <https://rpki-client.org/>
 - Prover - <https://github.com/lolepezy/rpki-prover>
 - Rpstir2 - <https://github.com/bgpsecurity/rpstir2>



Questions



nathalie@ripe.net
rpki@ripe.net