RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Hardening the core of the Internet

DNSSEC and RPKI

APTLD79 Virtual Meeting

Ondřej Caletka, Nathalie Trenaman (RIPE NCC)

Agenda

DNSSEC part

- Basic DNS principles
- DNS vulnerabilities
- DNSSEC introduction
- DNSSEC key types
- Parent-child interaction
- How to deploy DNSSEC

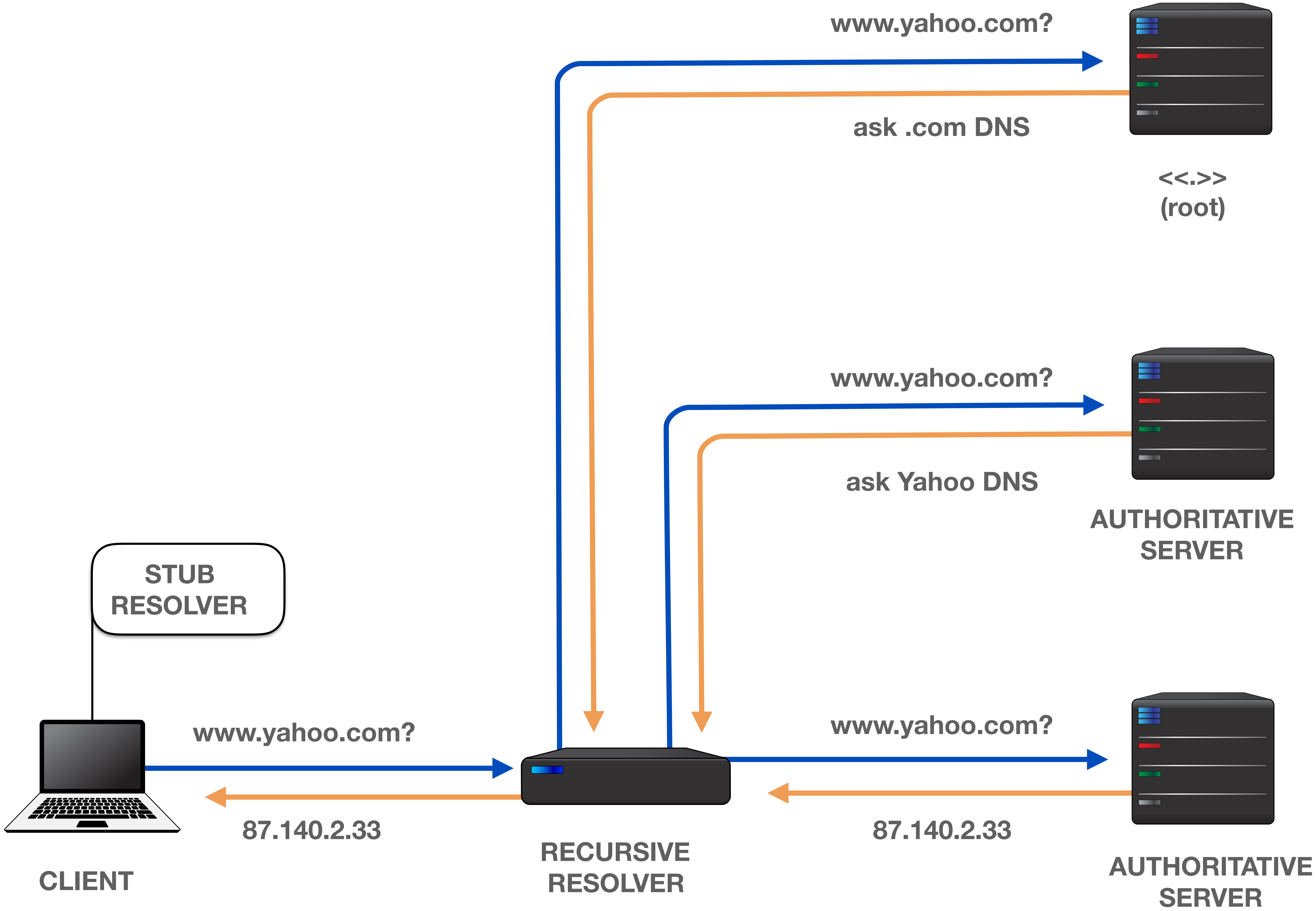
RPKI part

- Introduction to Routing Security
- Internet Routing Registry
- Resource Public Key Infrastructure
- Router Origin Authorization
- Router Origin Validation

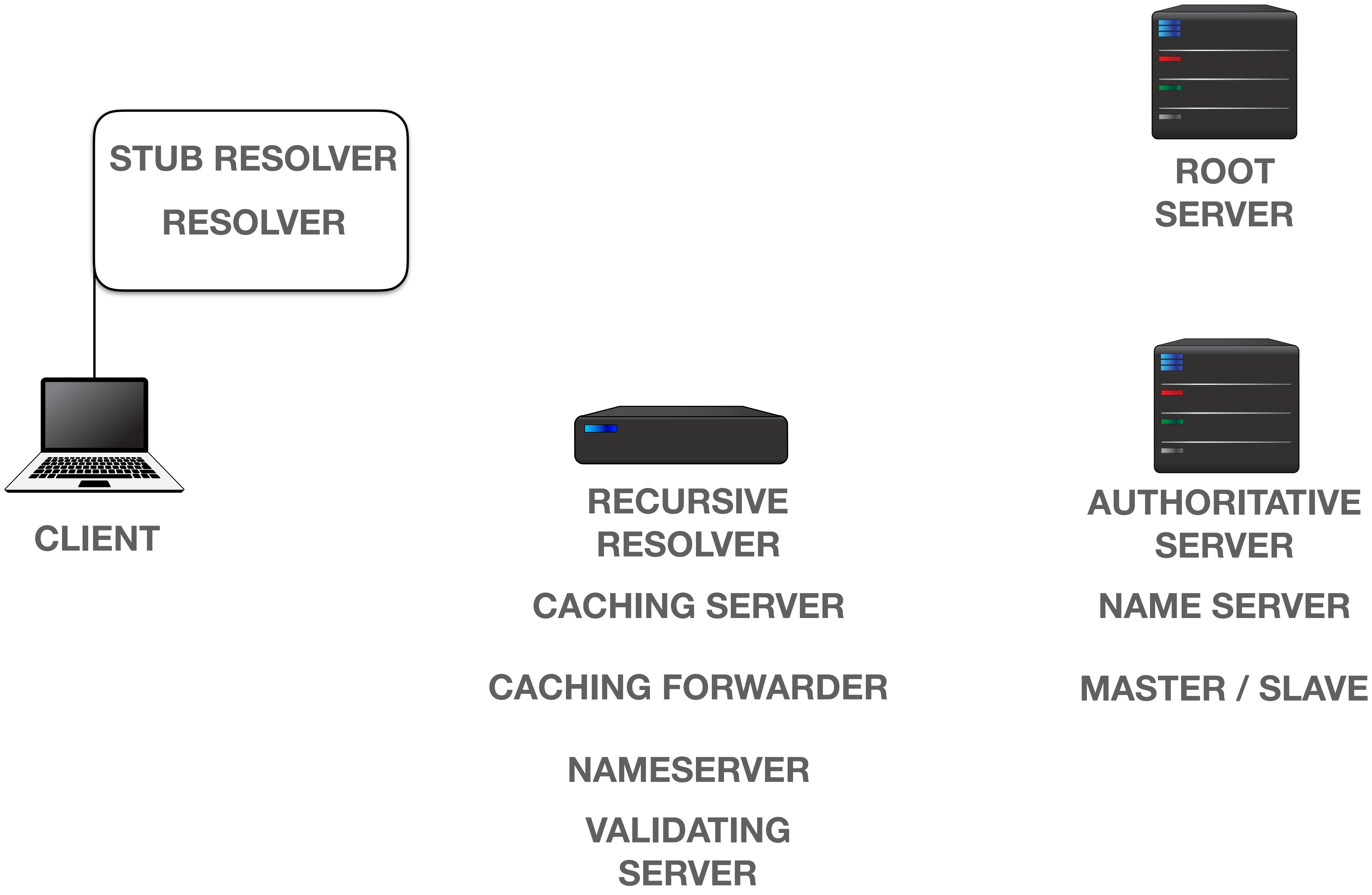
DNS

Basic principles

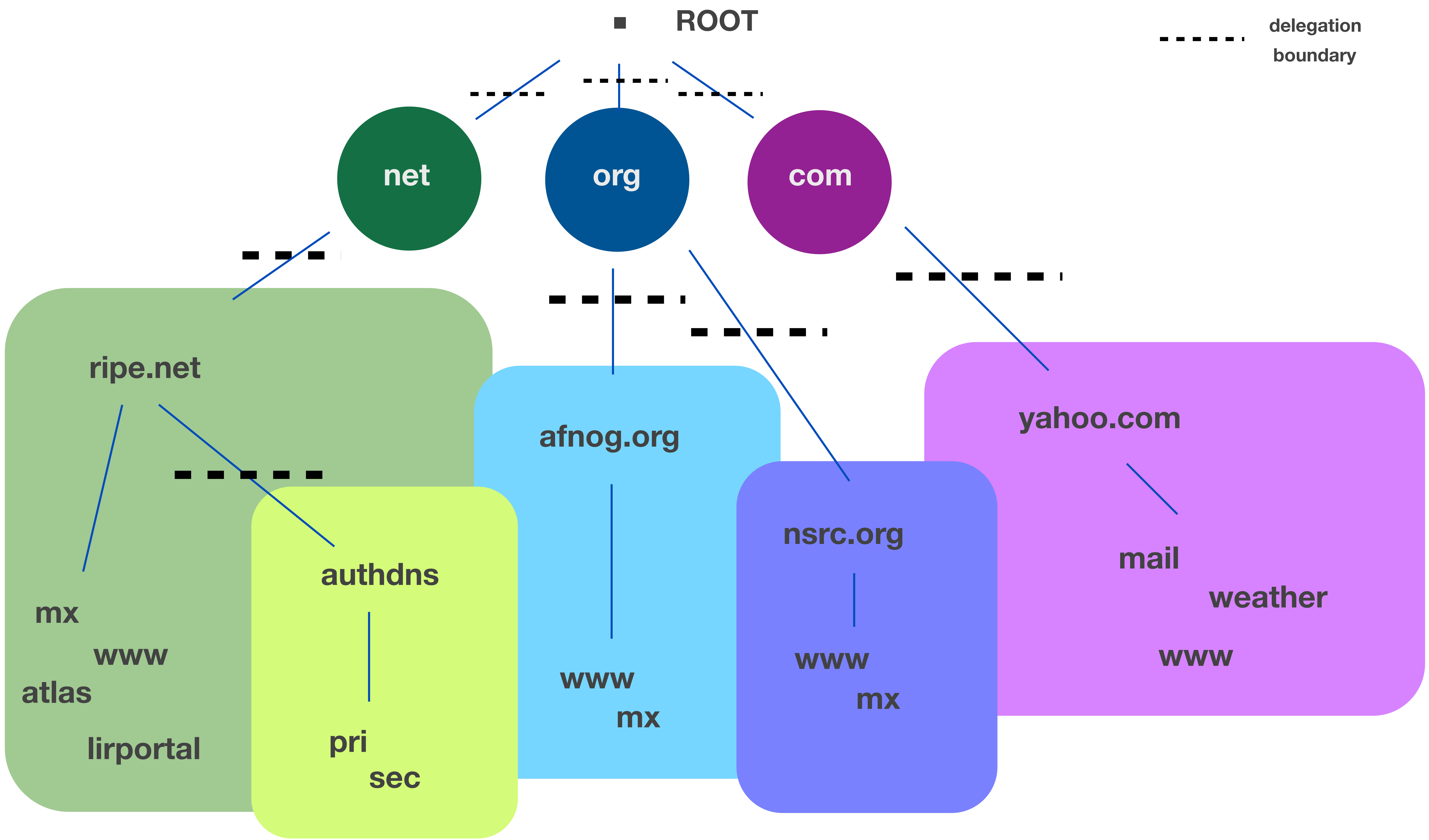
Example of a DNS query



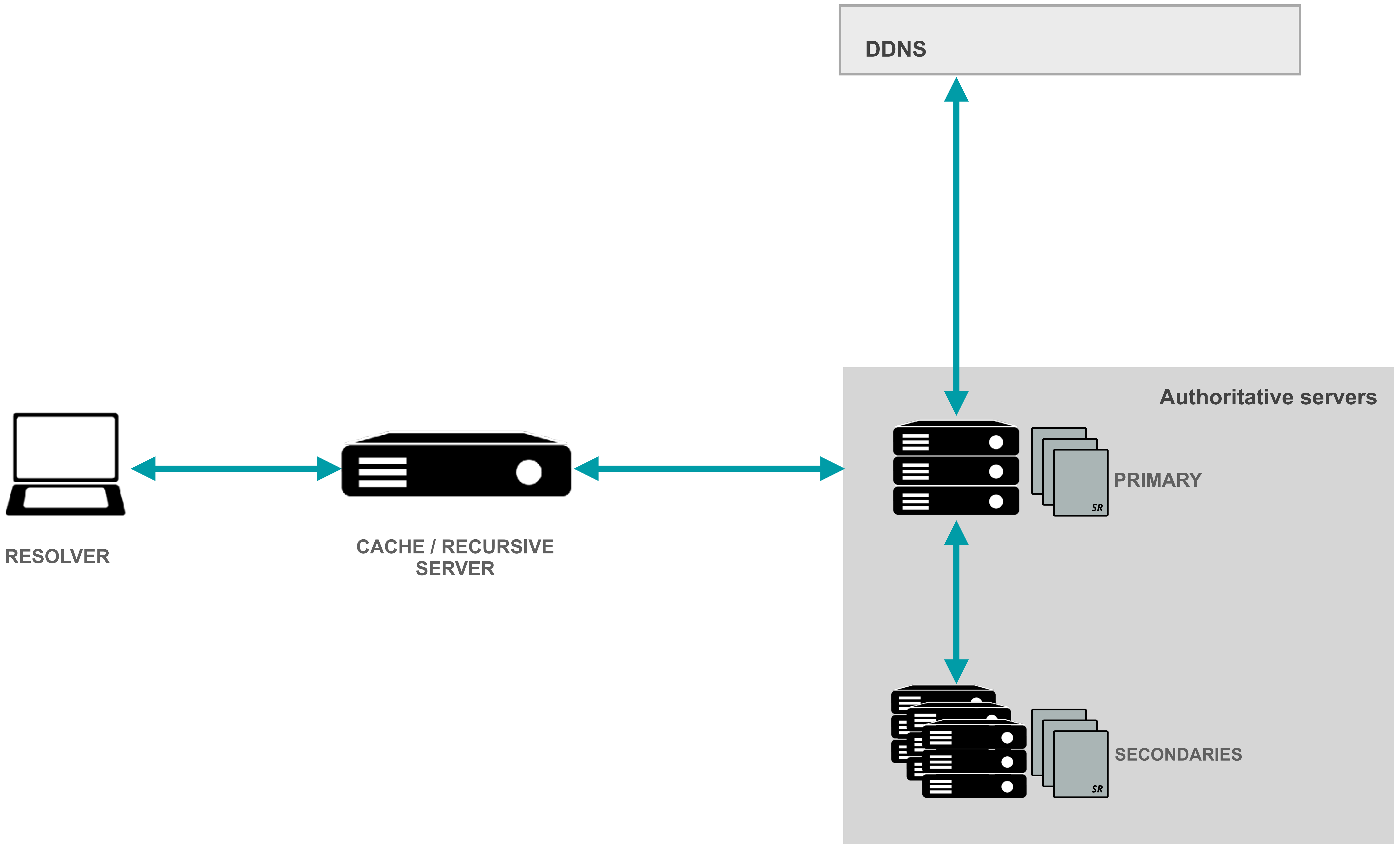
Terminology



Delegation


ROOT
delegation boundary
net
org
com
ripe.net
mx
www
atlas
lirportal
authdns
pri
sec
afnog.org
www
mx
nsrc.org
www
mx
yahoo.com
mail
weather
www

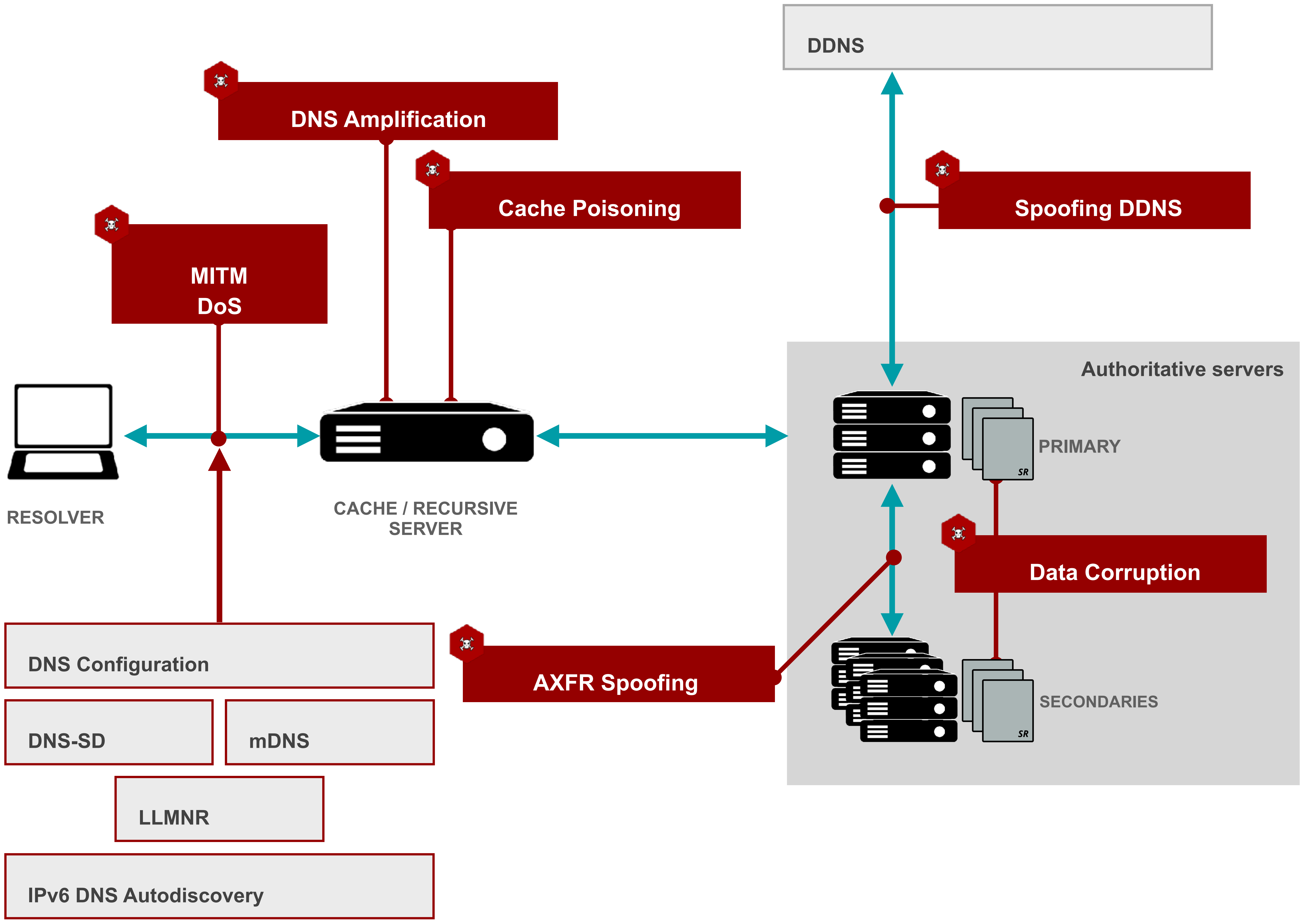
DNS Data Flow



DNS

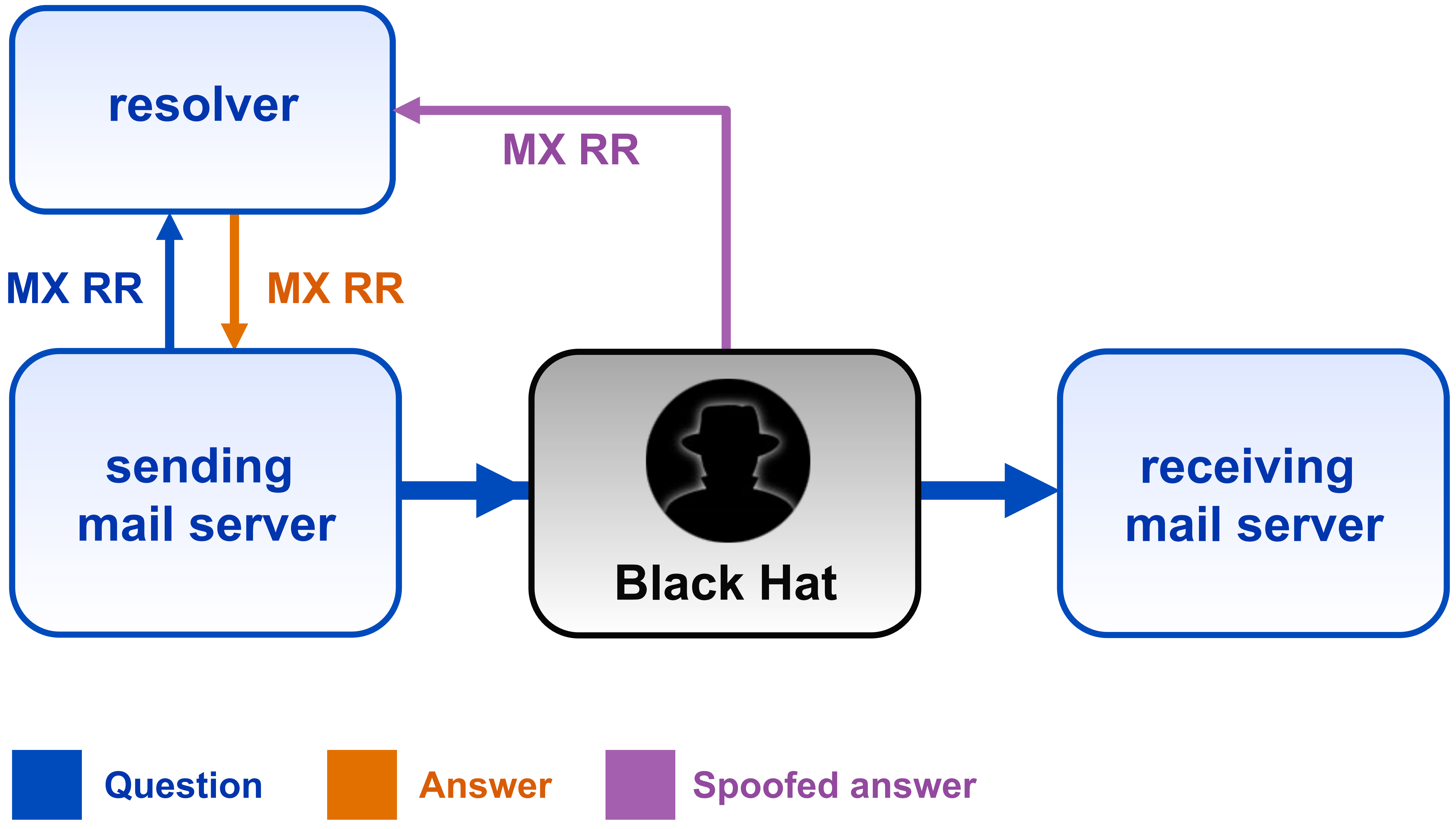
Vulnerabilities

DNS Vulnerabilities



DNS exploit example

- Mail goes to the server in the MX resource record
- Path only visible in the email headers



Factors making DNS attacks feasible

- Using UDP makes it easy to send spoofed datagrams
- Only 16-bit transaction id make brute force guessing possible
- Fragmentation of large datagrams presents another family of vulnerabilities
- Broken resolver implementations using predictable outgoing port number
- Side-channel attacks like SAD DNS (2020)

Real world example: MyEtherWallet attack in 2018

- BGP hijack of IP prefixes used by Amazon Route53
- Fake authoritative DNS servers installed on hijacked prefixes
- DNS responses redirected MyEtherWallet.com to a phishing site
- Cache of DNS resolver was poisoned
- Cryptocurrencies were stolen

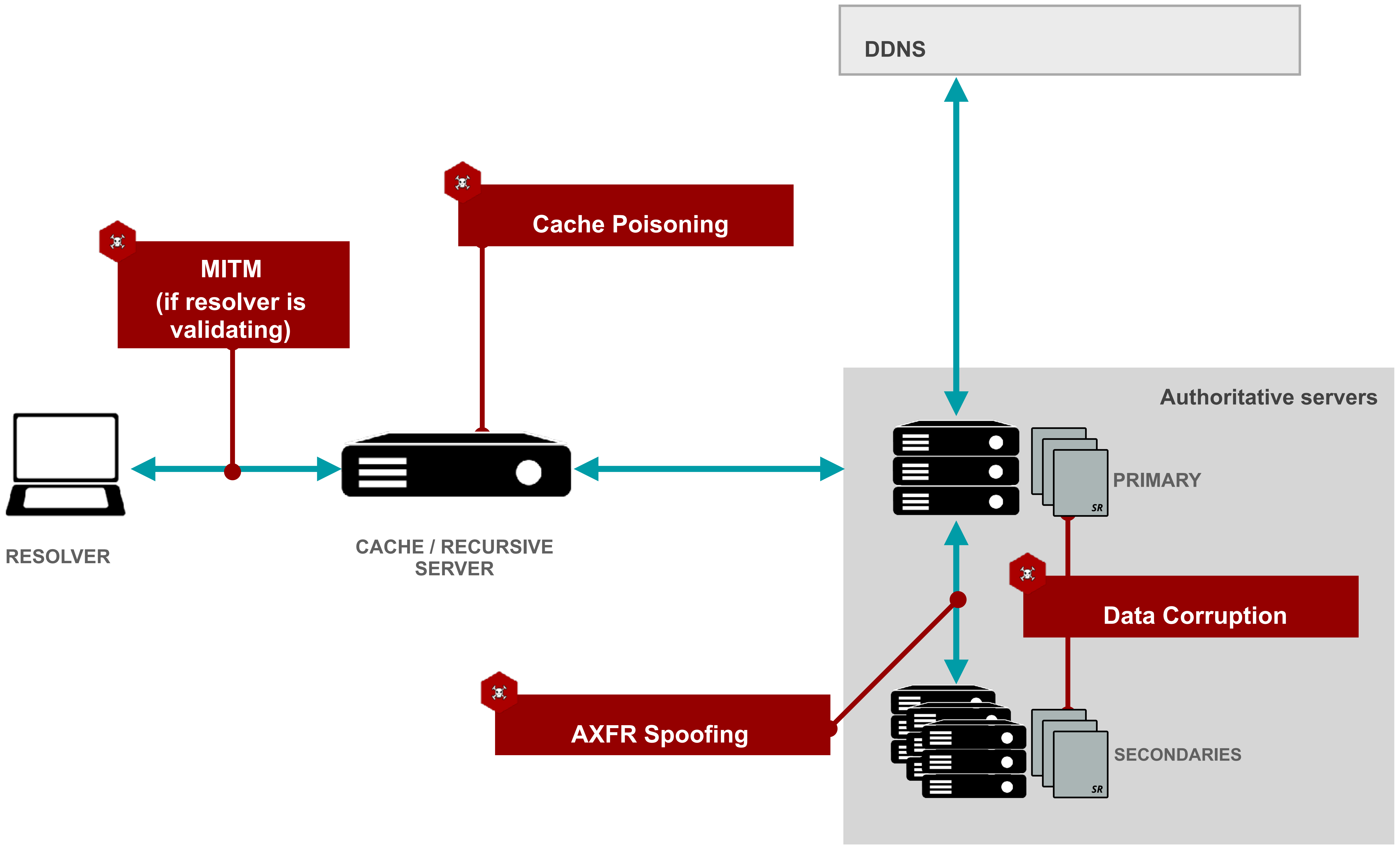
DNSSEC

Adding trust to the DNS

What is DNSSEC

- A solution to secure DNS data with asymmetric cryptography
- Provides authenticity and integrity, but no confidentiality (encryption) of data
- Publisher signs data with a private key and publish the signatures and public key inside the DNS zone
- A fingerprint of the zone's public key is published in its parent
- Validator checks signatures and filters out compromised data
- A backward-compatible protocol allowing a gradual rollout

DNSSEC Protected Vulnerabilities



DNSSEC Summary

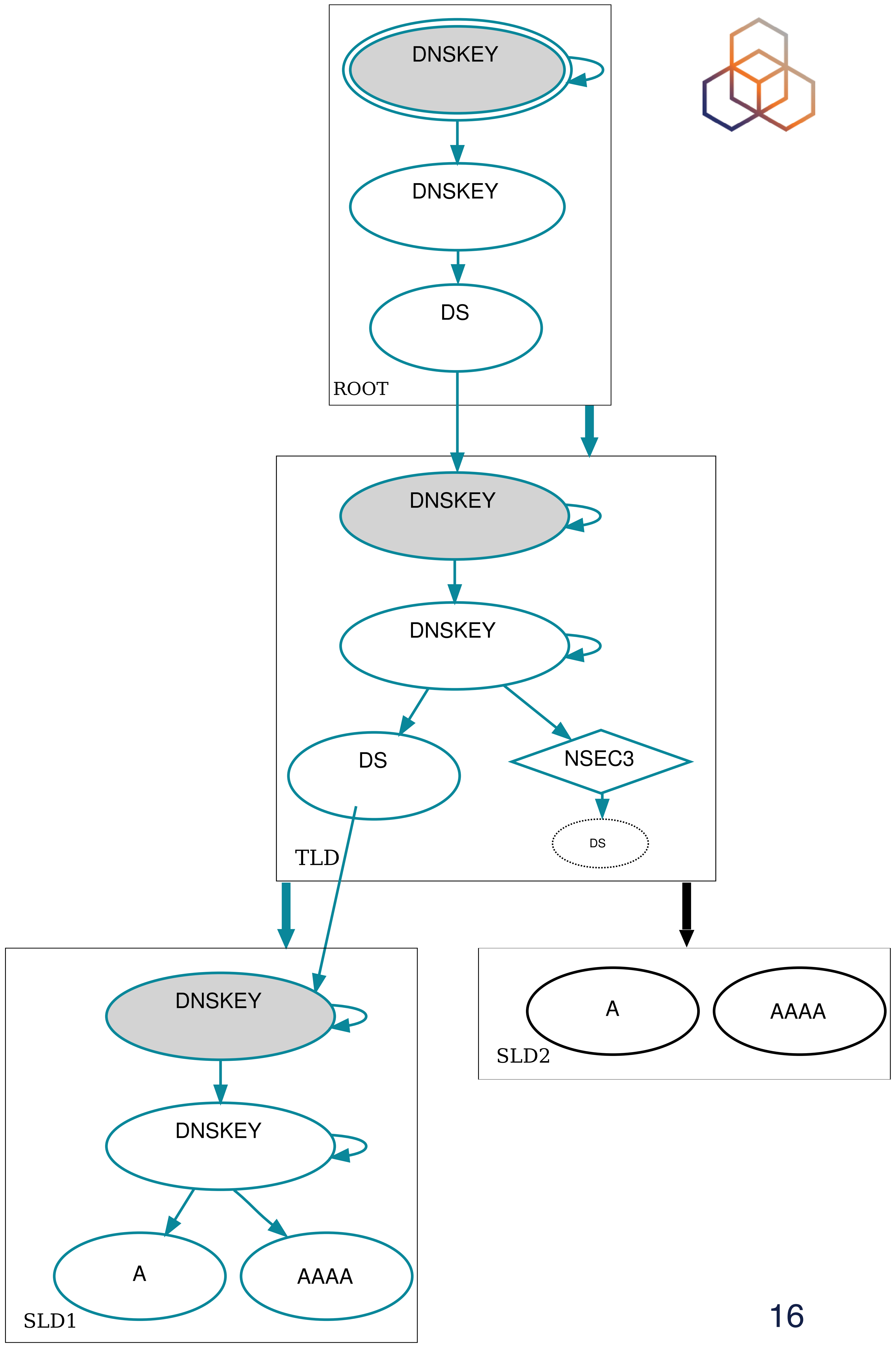
- Signing the Resource Records Sets with **private key**

public key   signature

- Publishing **DNSKEY**s and **RRSIG**s inside the zone
- Children sign their zones with their **private key**
    - Parent guarantees authenticity of child's key by signing the hash of it (**DS**)

Delegation Signer

- Repeat for parent …
    - …and grandparent



DNSSEC Example

ripe.net.

```
www.ripe.net   IN A 193.0.0.214
www.ripe.net   IN RRSIG A … 26523 ripe.net.
ripe.net       IN DNSKEY 256 26523 … ripe.net.
ripe.net       IN RRSIG DNSKEY 32987 … ripe.net.
ripe.net       IN DNSKEY 257 32987 … ripe.net.
```

net.

```
ripe.net   IN DS 26523 8 1 …
ripe.net   IN RRSIG DS … 43249 net.
net        IN DNSKEY 256 43249 … net.
```

Who is validating DNSSEC data?

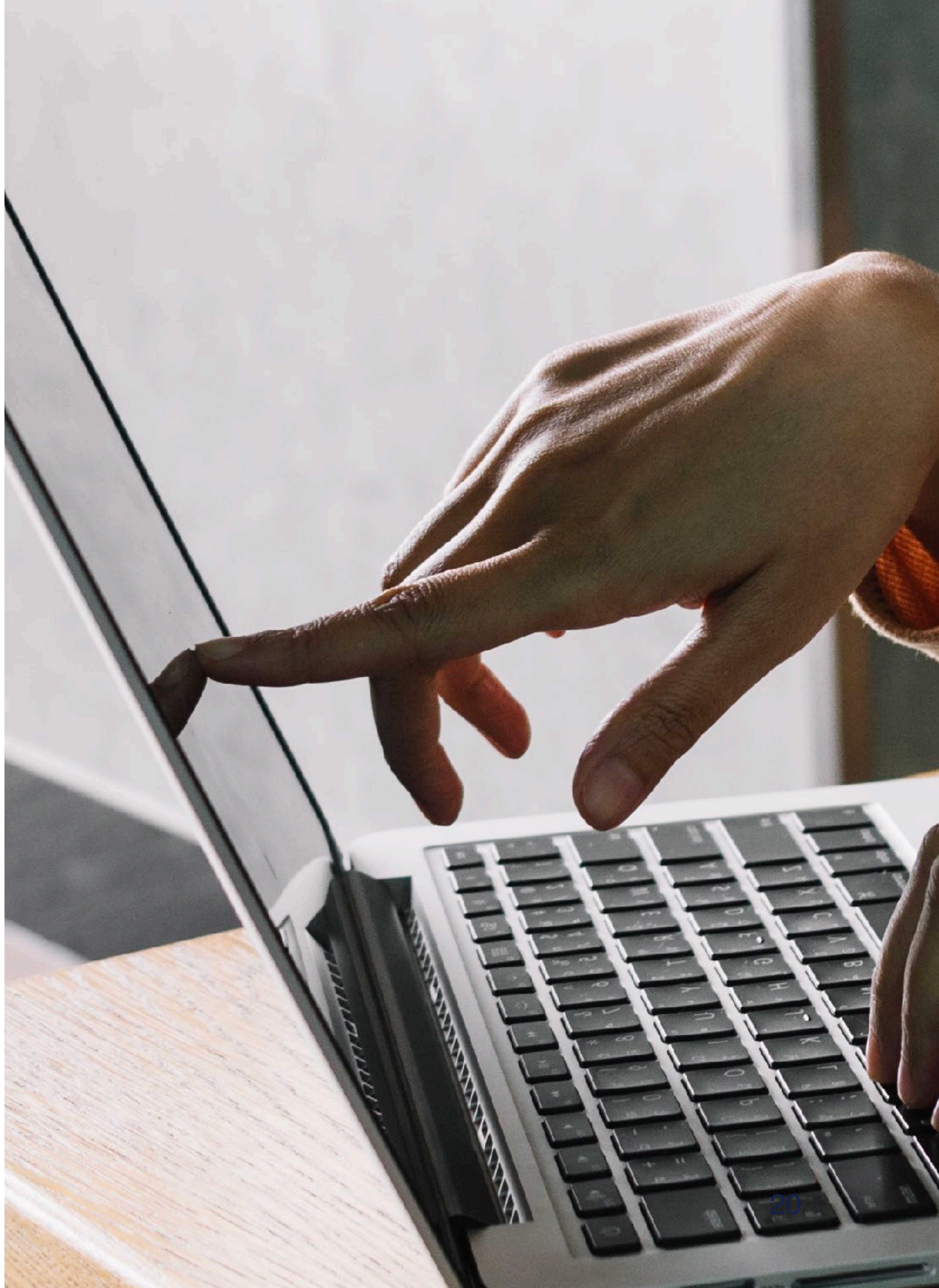
- Mostly caching/recursive servers
- It is expected to shift validation closer to the user for specific protocols like DANE
- No integrity is guaranteed between validator and end user
- Forged data are hidden from end users
- According to APNIC Labs measurements, more than 30 % of internet users are using DNSSEC-validating resolver

Validation results

- **Secure**
  - Validator can build chain of signed records from trust anchor all the way down to the desired record
- **Insecure**
  - Validator found a signed proof of an unsigned subtree
- **Bogus**
  - It was not possible to build chain of signed records
  - May indicate attack, configuration error, data corruption or clock difference
- **Indeterminate**
  - There is no trust anchor configured for that particular subtree

Demo time!

Determining validation status from output of command dig



DNSSEC secure

```
$ dig www.ripe.net

; <<>> DiG 9.16.11 <<>> www.ripe.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64151
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.ripe.net.          IN A

;; ANSWER SECTION:
www.ripe.net.       76532   IN    A   193.0.6.139

;; Query time: 13 msec
;; SERVER: 192.168.178.1#53(192.168.178.1)
;; WHEN: Tue Feb 16 13:40:50 CET 2021
;; MSG SIZE  rcvd: 57
```

authenticated data

DNSSEC insecure/indeterminate

```
$ dig www.aptld.org

; <<>> DiG 9.16.11 <<>> www.aptld.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12671
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.aptld.org.          IN A

;; ANSWER SECTION:
www.aptld.org.      6764 IN   A    93.125.99.132

;; Query time: 9 msec
;; SERVER: 192.168.178.1#53(192.168.178.1)
;; WHEN: Tue Feb 16 13:47:44 CET 2021
;; MSG SIZE  rcvd: 58
```

no ad flag

DNSSEC bogus

```
$ dig www.dnssec-failed.org

; <<>> DiG 9.16.11 <<>> www.dnssec-failed.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 25519
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.dnssec-failed.org.        IN A

;; Query time: 297 msec
;; SERVER: 192.168.178.1#53(192.168.178.1)
;; WHEN: Tue Feb 16 13:51:03 CET 2021
;; MSG SIZE  rcvd: 50
```

server failure

no answer returned

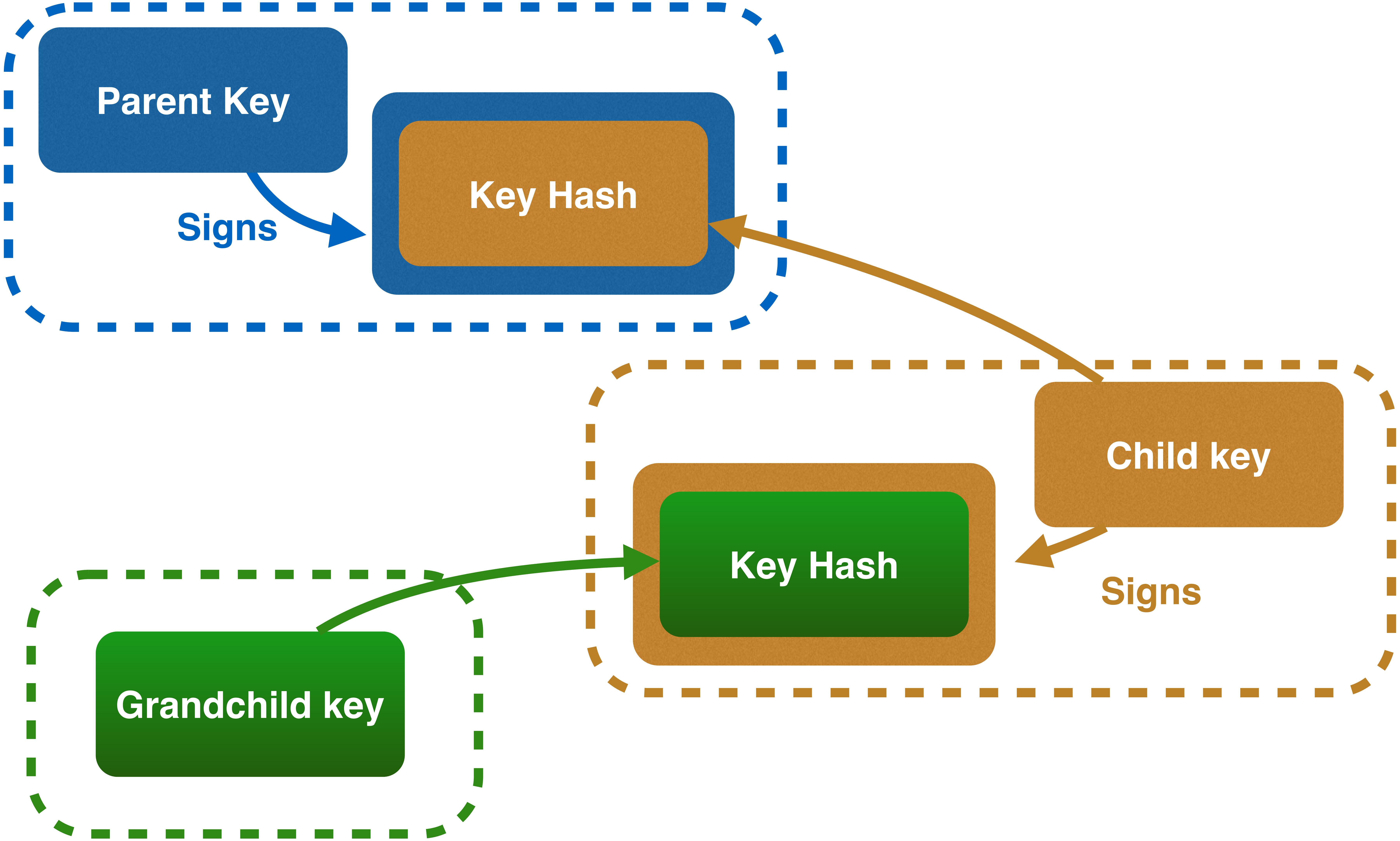
Is this DNSSEC problem?

```
$ dig www.dnssec-failed.org +cdflag

; <<>> DiG 9.16.11 <<>> www.dnssec-failed.org +cdflag
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15702
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:          checking disabled
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.dnssec-failed.org.        IN  A

;; ANSWER SECTION:                      answer returned
www.dnssec-failed.org. 6380     IN A 68.87.109.242
www.dnssec-failed.org. 6380  IN A 69.252.193.191

;; Query time: 1 msec
;; SERVER: 192.168.178.1#53(192.168.178.1)
;; WHEN: Tue Feb 16 13:53:37 CET 2021
;; MSG SIZE  rcvd: 82
```

DNSSEC

Key types

DNSSEC Made simple



Key problem

- Interaction with parent administratively expensive
  - Should only be done when needed
  - Bigger keys are better

- Signing zones should be fast
  - Memory restrictions
  - Space and time concerns
  - Smaller keys with short lifetimes are better

Key functions

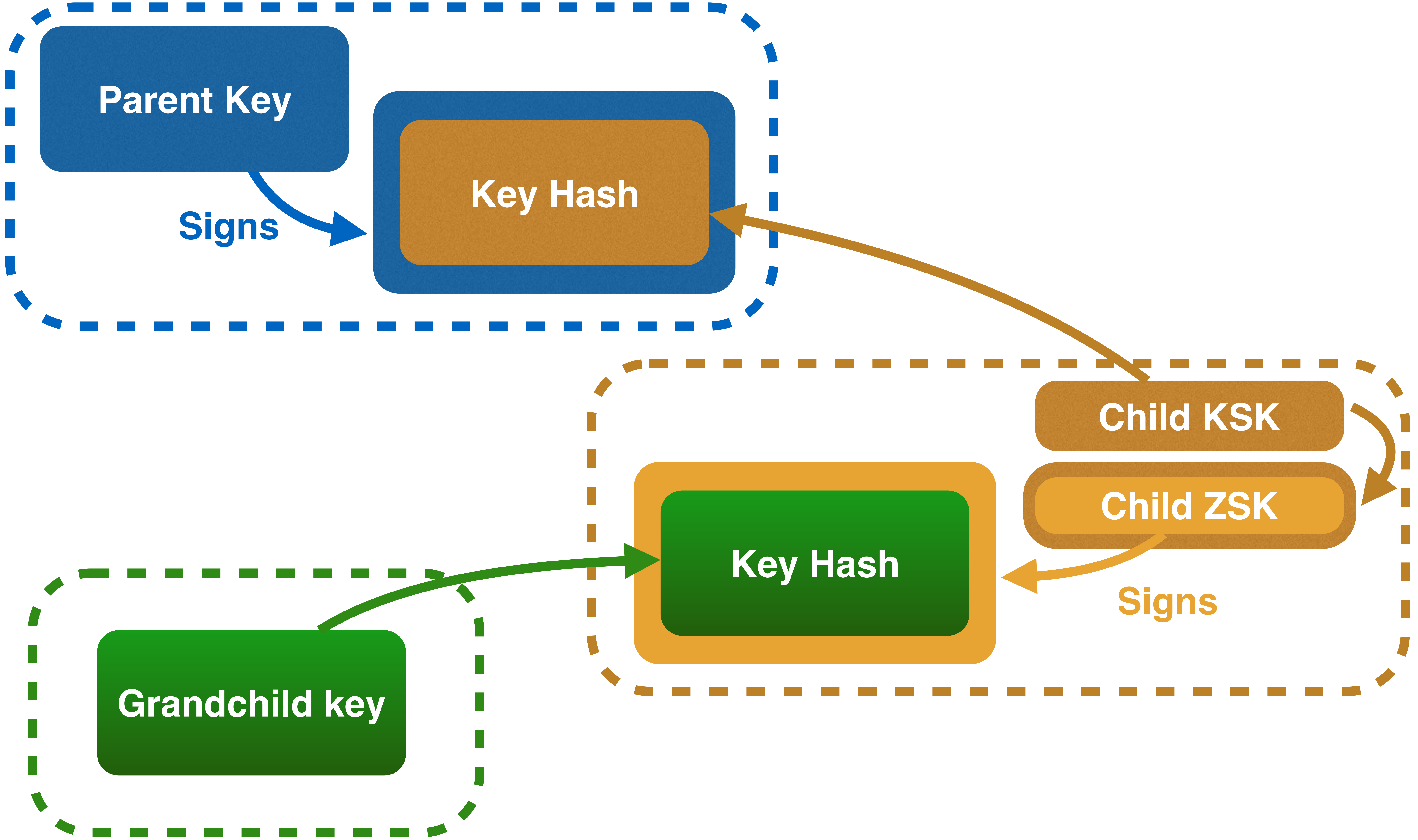
- Large keys are more secure
  - Can be used longer
  - Large signatures => large zonefiles
  - Signing and verifying computationally expensive
- Small keys are fast
  - Small signatures
  - Signing and verifying less expensive
  - Short lifetime

More than one key

- Key Signing Key (KSK) only signs DNSKEY RRset - all public keys
- Zone Signing Key (ZSK) signs all records in zone

- Parent DS points to child's KSK
    - Parent's ZSK signs DS
    - Signature transfers trust from parent key to child key

Key split - ZSK and KSK



Zone Signing Key - ZSK

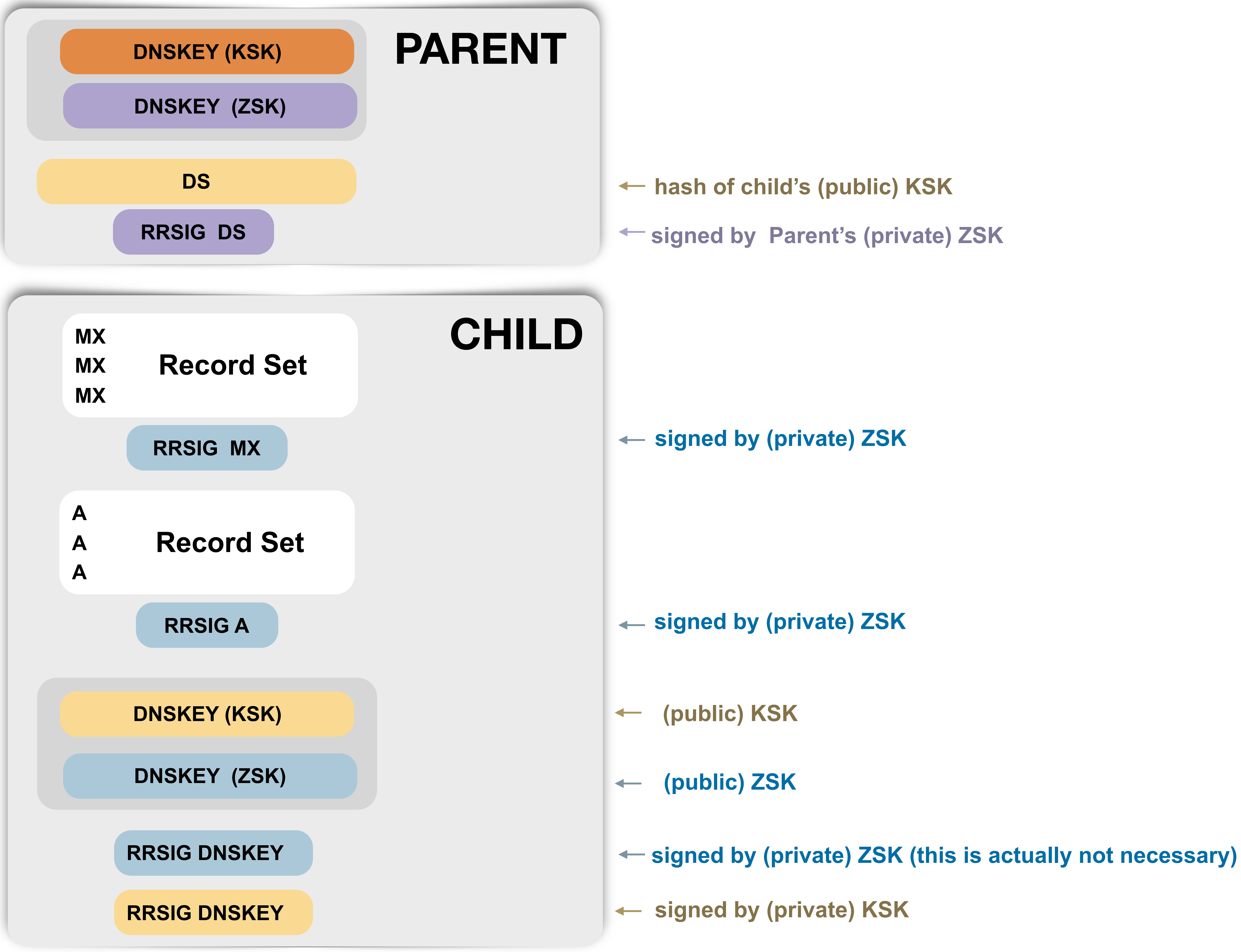
- Used to sign **all data** in the zone
- Can be **lower strength** than the KSK
- No need to coordinate with parent zone if change is needed
- Can be changed **very often**

Key Signing Key - KSK

- Only signs the public keys of the zone – **KSK** and **ZSK**
- Delegates trust to the **ZSK**
- Serves as a **trust anchor** – is referenced from the parent zone
- Its replacement requires **changing DS record** in the parent zone

Combined Signing Key - CSK

- Only one key that signs all records and also serves as trust anchor
- Used mostly in small deployments with ECC-based algorithms:
  - unlike RSA, key size is fixed for Elliptic-curve algorithms
  - keys are small, fast to sign and secure at the same time
  - therefore KSK/ZSK split may not be necessary



PARENT
DNSKEY (KSK)
DNSKEY (ZSK)
DS
RRSIG DS
hash of child's (public) KSK
signed by Parent's (private) ZSK
CHILD
MX
MX
MX
Record Set
RRSIG MX
signed by (private) ZSK
A
A
A
Record Set
RRSIG A
signed by (private) ZSK
DNSKEY (KSK)
DNSKEY (ZSK)
(public) KSK
(public) ZSK
RRSIG DNSKEY
RRSIG DNSKEY
signed by (private) ZSK (this is actually not necessary)
signed by (private) KSK

DNSSEC

Parent-child interaction

Building the chain of trust

- Each DNS zone is self-contained
  - publishes actual DNS data, their signatures and a public key to check them
- The Chain of trust is built by inserting fingerprint of the public key to the parent zone
  - if there is no DS record in the parent zone, the zone is always considered insecure
- TLD registry and registrars have to support publishing DS records
- Two possible ways:
  - publishing user-provided DS record directly
  - calculating their own DS records out of user-provided DNSKEY

Automating secure delegation updates

- Child zone publishes special CDS and/or CDNSKEY record
- Parent zone operator periodically scans all the child zones for such records
- DS records in the parent zone are updated according to CDS or CDNSKEY contents
  - for already secure zones, this update is authorised by DNSSEC signatures
  - for insecure zones, another mechanism has to be deployed to avoid spoofing

DNSSEC

How to deploy it

How to deploy DNSSEC

- On a resolver: almost no effort needed; on by default for:
  - BIND
  - Unbound
  - Knot Resolver
- On the authoritative side: proper planning is necessary (DNSSEC Practice Statement)
  - Key and Signature Policy: what algorithm to use, how often to change the keys
  - Where to store keys
  - Adapt provisioning system
  - Prepare for disaster recovery

Who deploys DNSSEC validation

- Most cloud resolvers (Google, Quad9, Cloudflare,…)
- It is on by default for most common open source DNS resolvers
- According to APNIC Labs measurements, more than 30 % of internet users are using DNSSEC-validating resolver
- Only signed domains are protected by DNSSEC validation
- The path between validating resolver and client has to be protected, for instance:
  - DNS-over-TLS
  - DNS-over-HTTPS

Which domain names are signed

- The root zone itself
- 1371 out of 1504 Top Level Domains (91 %)
- Second Level Domain numbers vary a lot per different TLDs:
  - 3.3 million domains under .COM (2 %)
  - 3.4 million domains under .NL (56 %)
    - there is registration fee discount for DNSSEC-enabled domains
  - 800 000 domains under .CZ (60 %)
  - 515 000 domains in .EU (14 %)

111 ccTLDs are still without DNSSEC

Tony Finch
@fanf

Replying to @fanf

One less flag:

111

3:46 PM · Feb 5, 2021

There is still work to do

- The bulk of DNSSEC-protected domain names come from web hosting companies
- DNSSEC is usually on-by-default by the hosting company
- Many high-value domains are still not protected
  - complex task for Content Delivery Networks, where DNS responses are dynamic
  - no/hard support by many registrars
  - lack of understanding of the DNSSEC technology

Questions

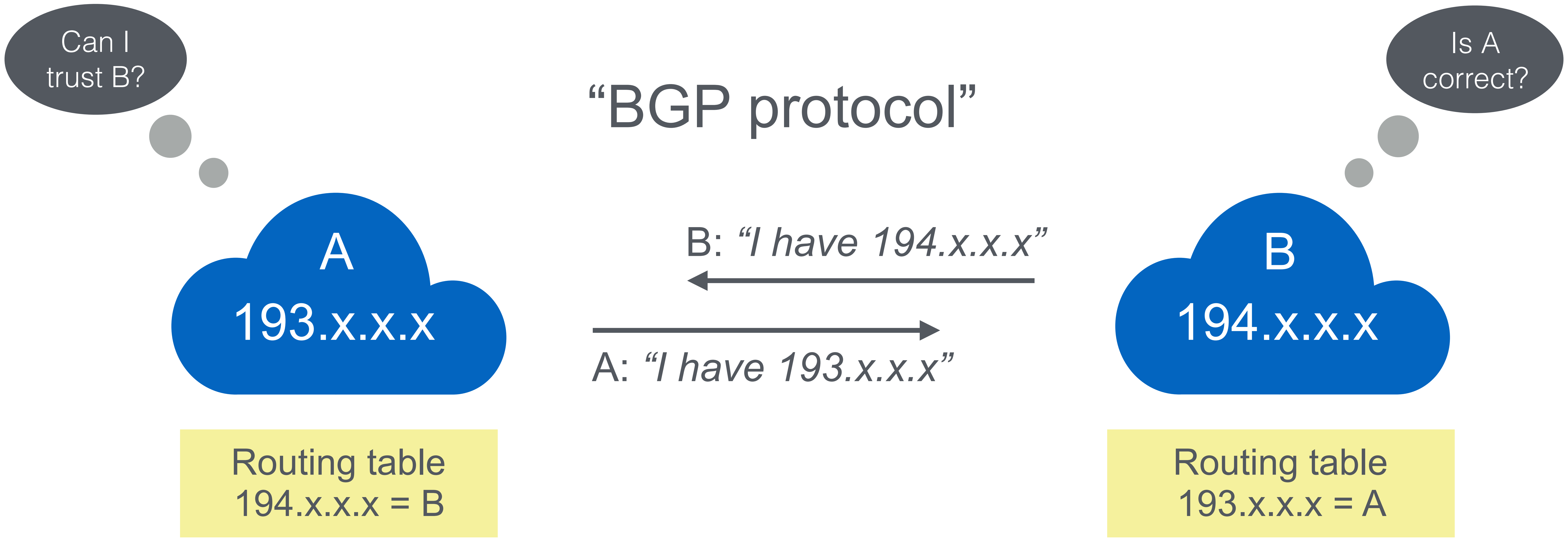
Let’s take a
5 minutes
break!


WELCOME
WE ARE
OPEN
PLEASE COME IN

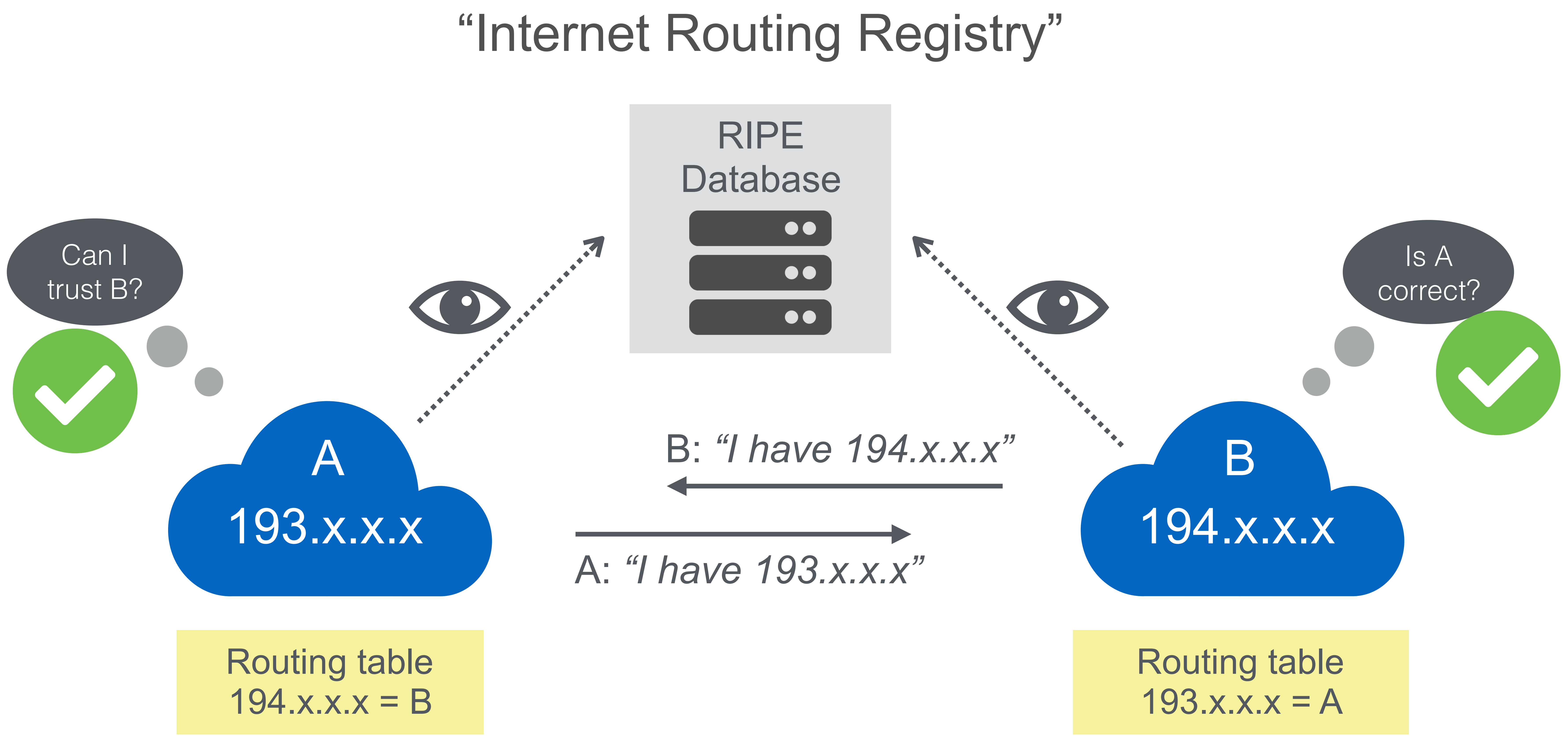
RPKI

Introduction to Routing Security

Routing on the Internet



Routing on the Internet



Accidents happen

- Fat fingers
  - 2 and 3 are really close on our keyboards

- Policy violations
  - Oops, we did not want this to go on the public Internet
  - Infamous incident with Pakistan Telecom and YouTube

Incidents are Common

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

Internet Routing Registry

Internet Routing Registry

- Many exist, most widely used
  - RIPE Database
  - APNIC Database
  - RADB

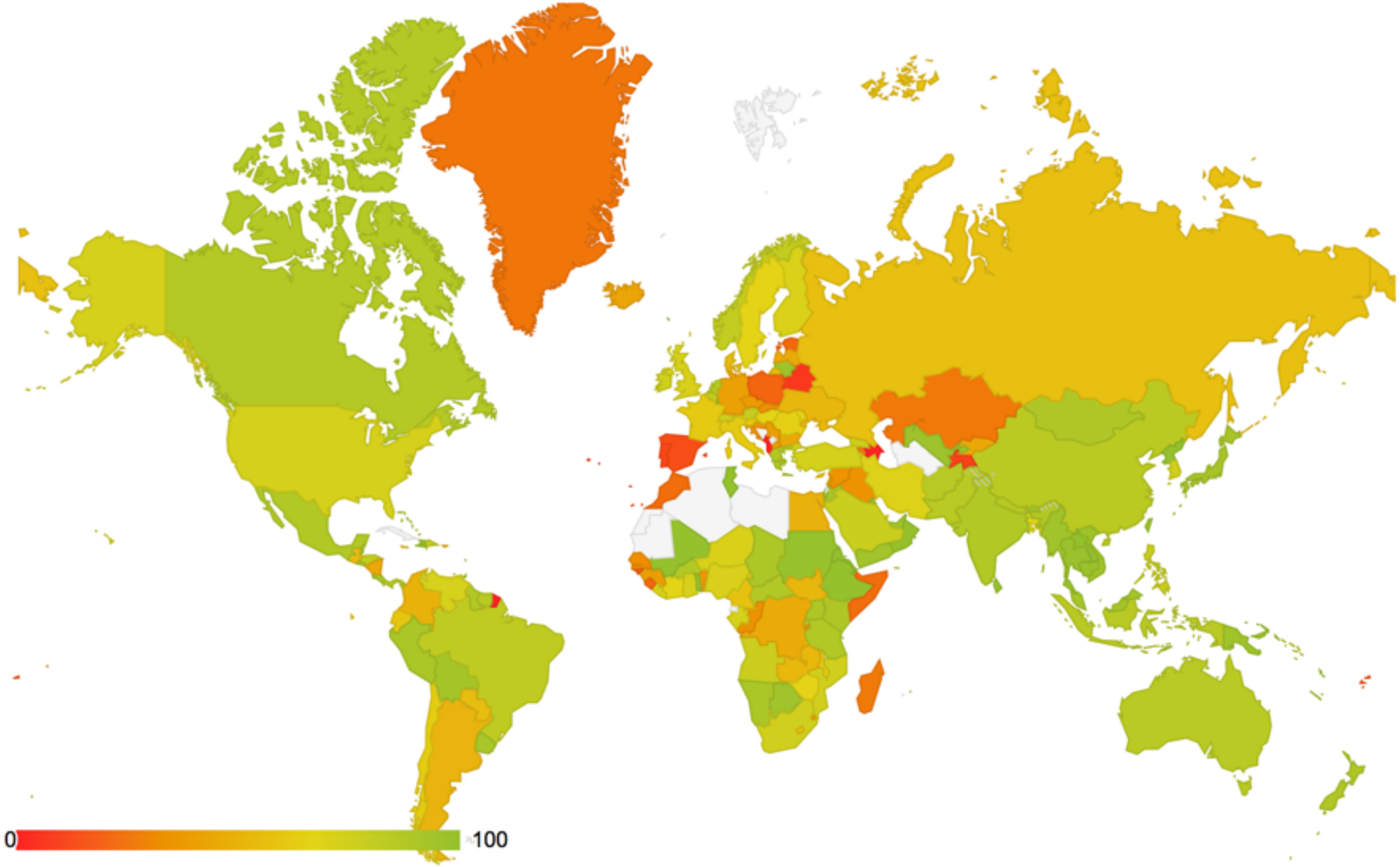
- Verification of holdership over resources
  - RIPE Database for RIPE Region resources only
  - RADB allows paying customers to create any object
  - Lots of the other IRRs do not formally verify holdership

Problem Statement

- Some IRR data cannot be fully trusted
  - Accuracy
  - Incomplete data
  - Lack of maintenance

- Not every RIR has an IRR
  - Third party databases need to be used (RADB, NTTCOM)
  - No verification of who holds IPs/ASNs

Problem Statement



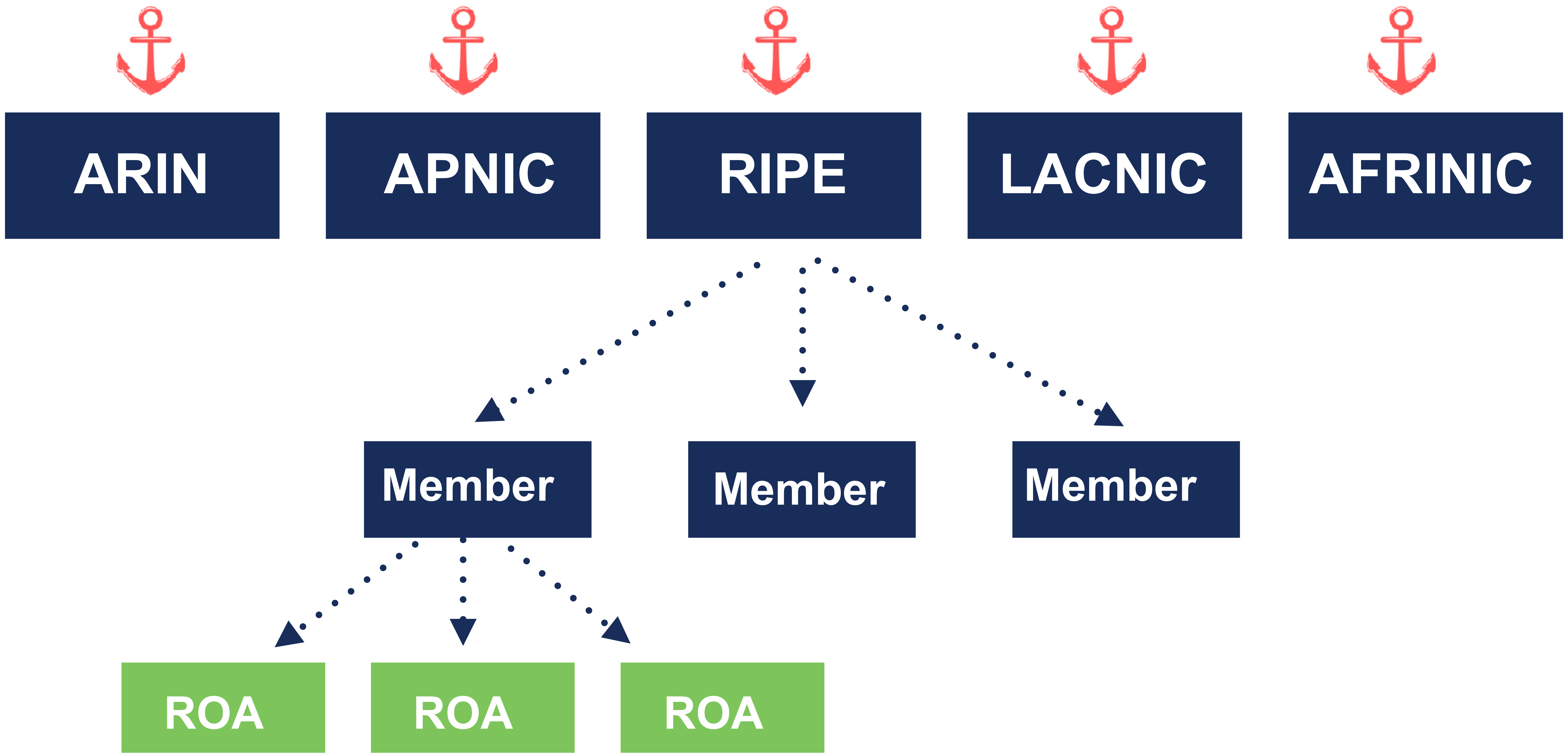
Resource Public Key Infrastructure (RPKI)

Resource Public Key Infrastructure

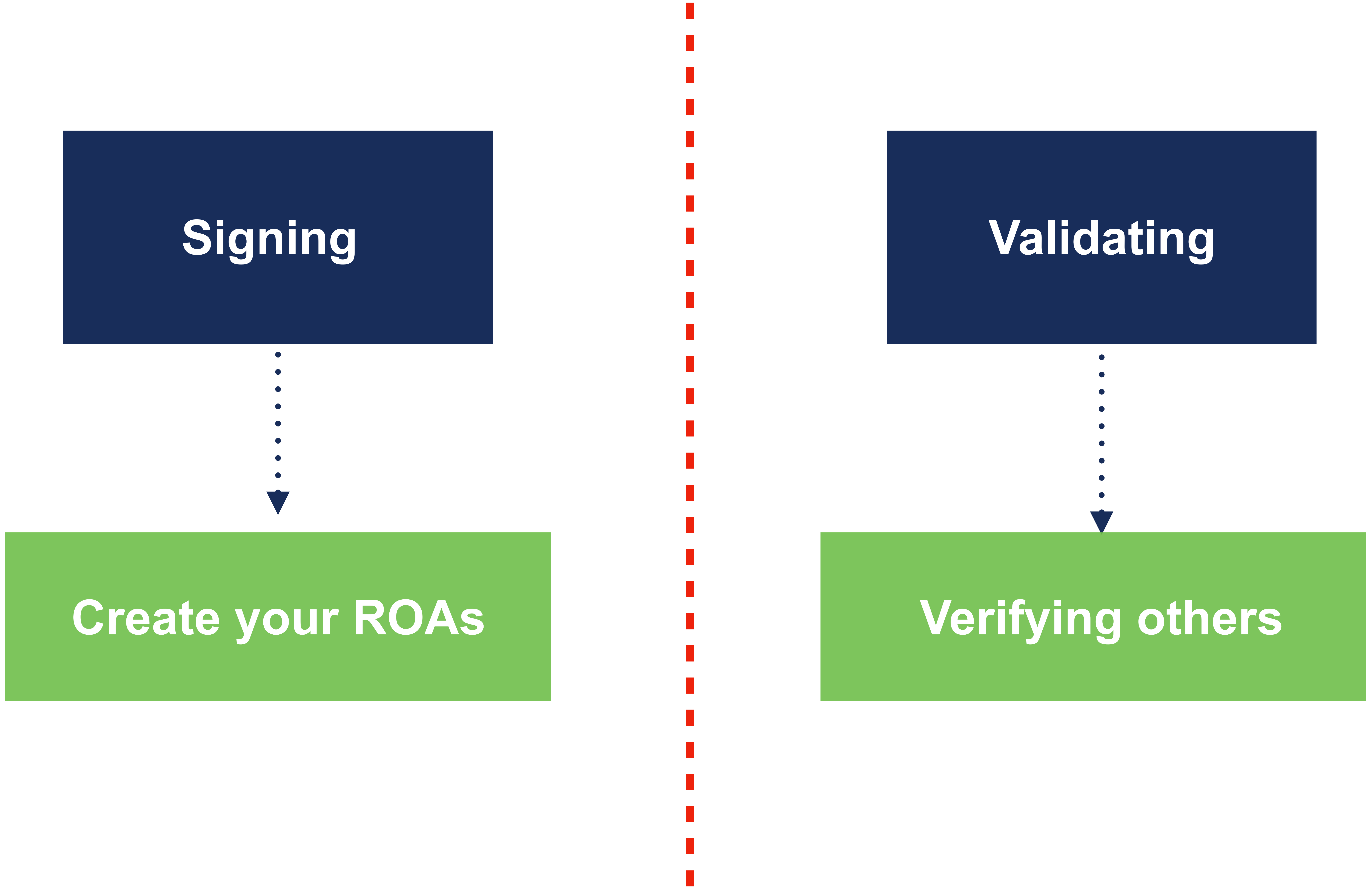
- Ties IP addresses and AS numbers to public keys
- Follows the hierarchy of the IP address registries
- Allows for authorised statements from IP address holders
  - AS X is authorised to announce my prefix Y
  - Signed, holder of Y

RPKI Certificate Structure

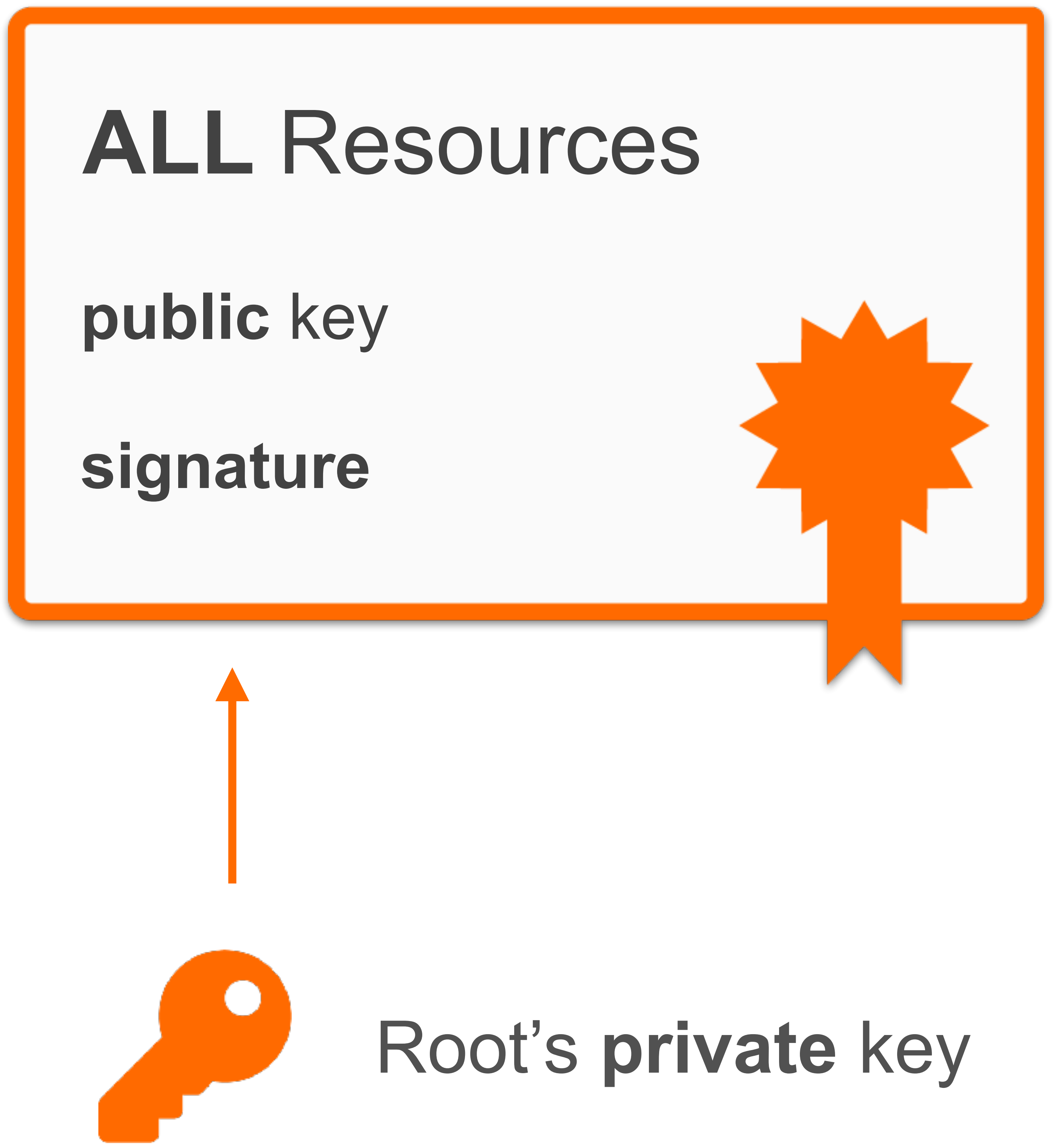
Certificate hierarchy follows allocation hierarchy



Two Elements of RPKI



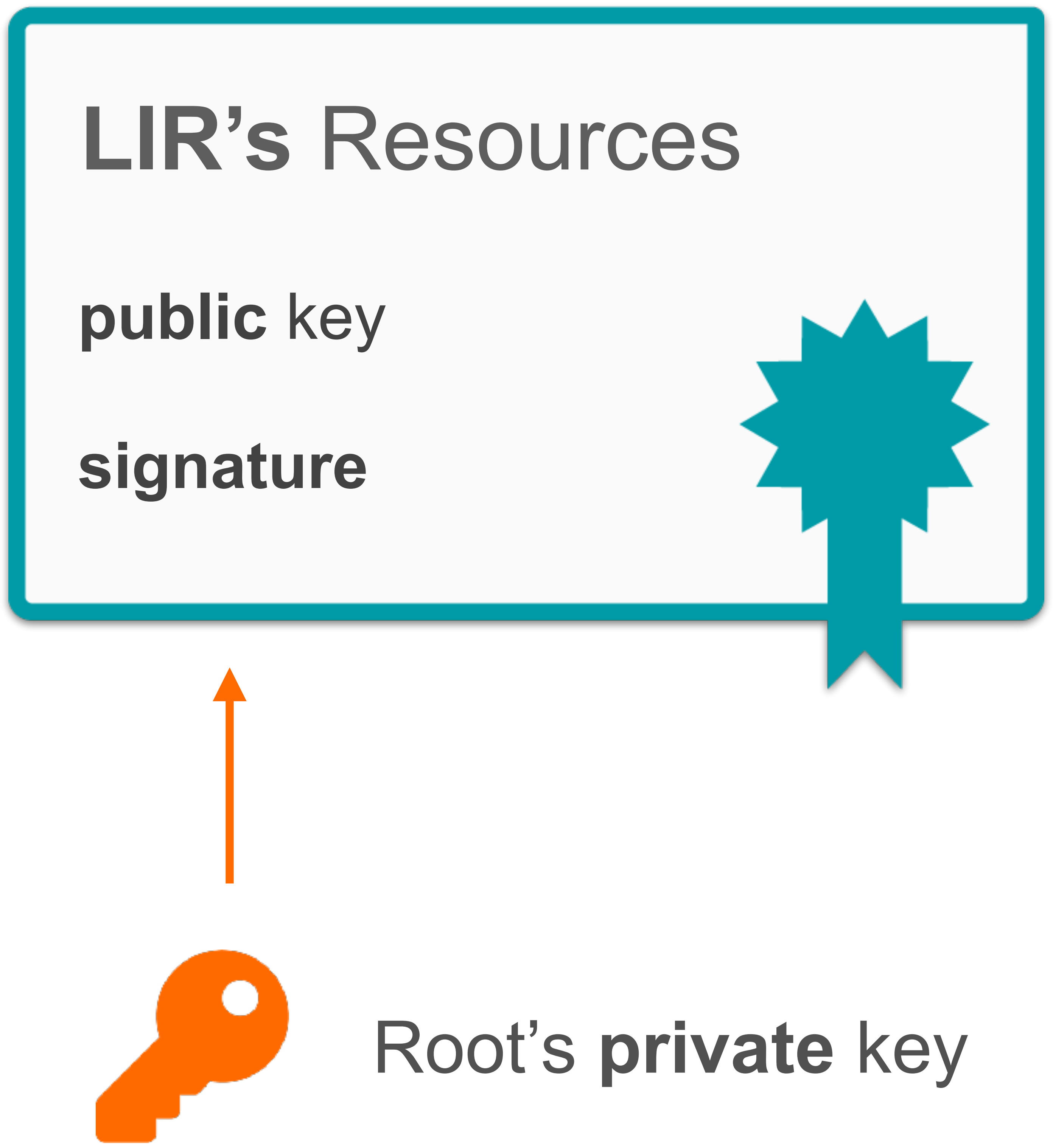
RPKI Chain of Trust



RIPE NCC Root Certificate

Self-signed

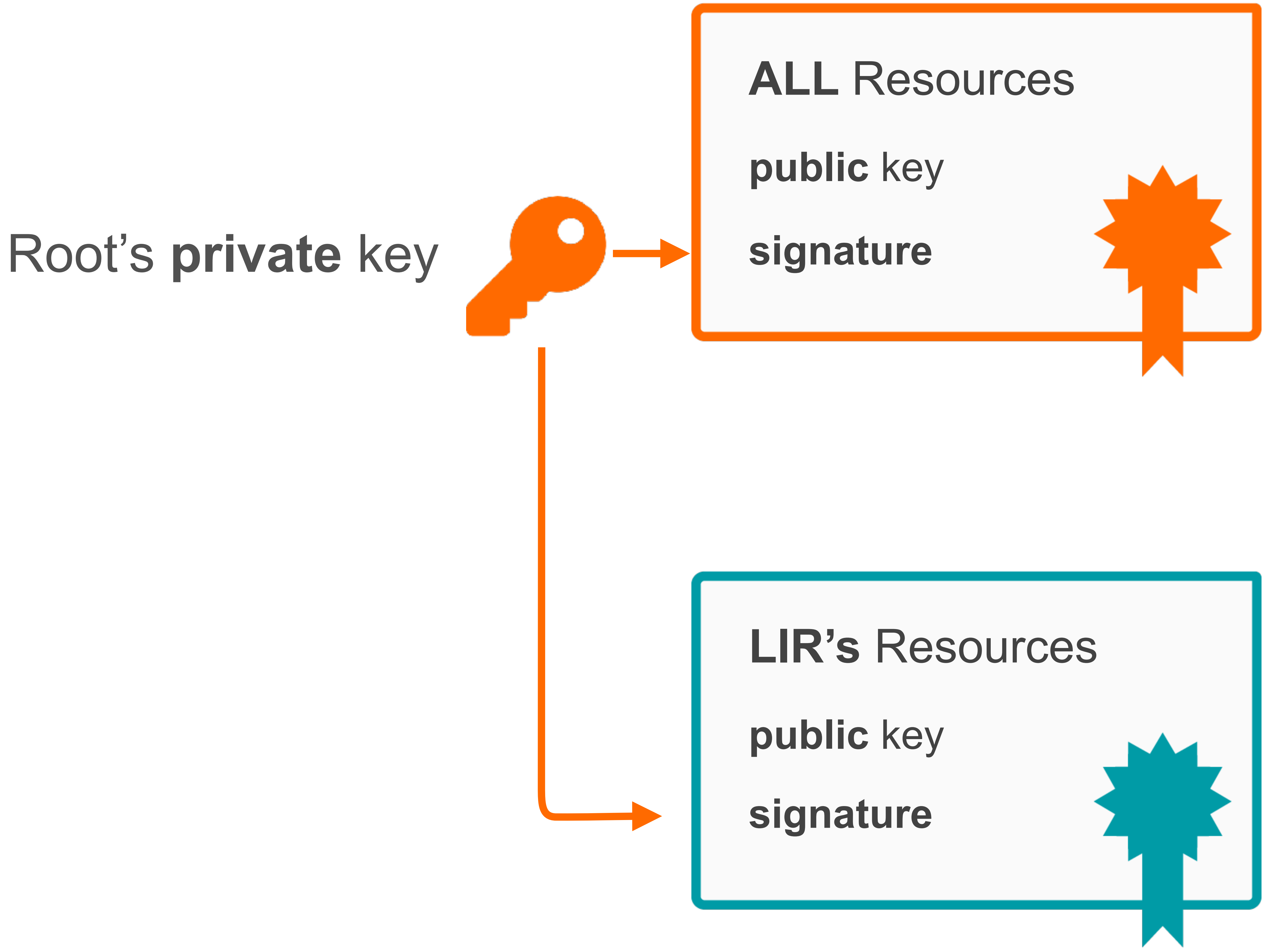
RPKI Chain of Trust



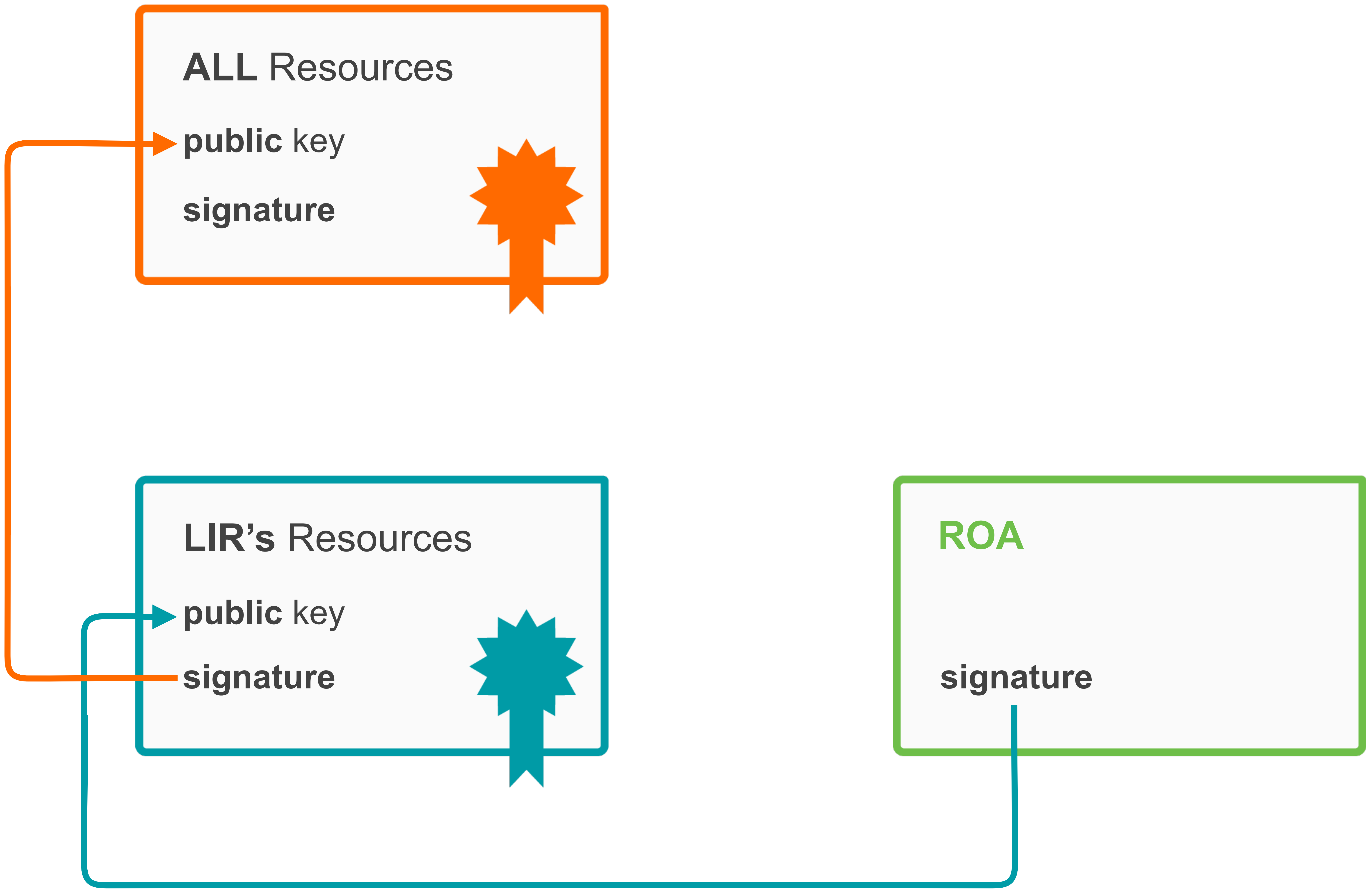
LIR Certificate

Signed by the Root private key

RPKI Chain of Trust



RPKI Chain of Trust



Route Origin Authorisation

Route Origin Authorisation

ROA

signature

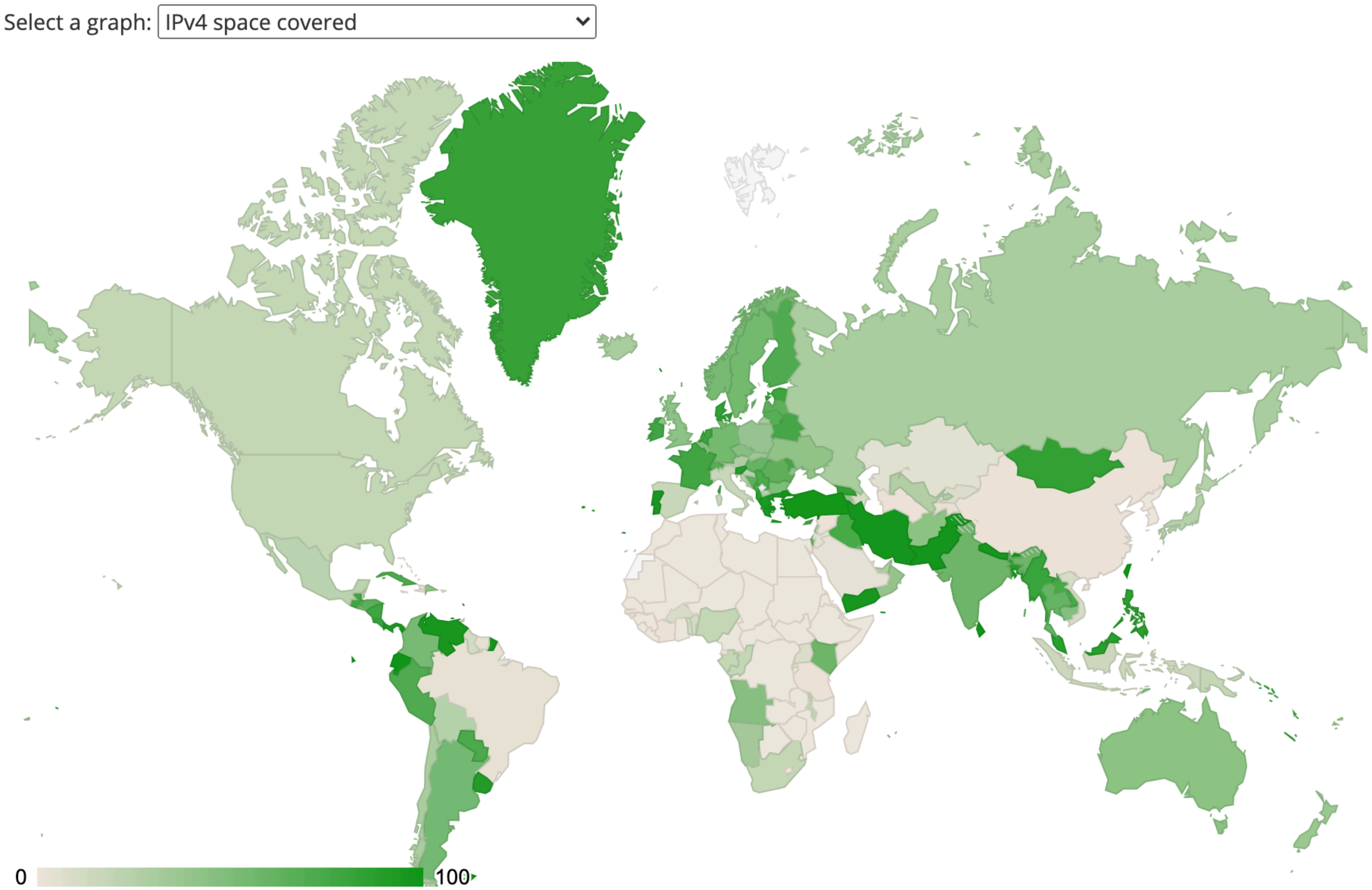
LIR’s **private** key

Prefix

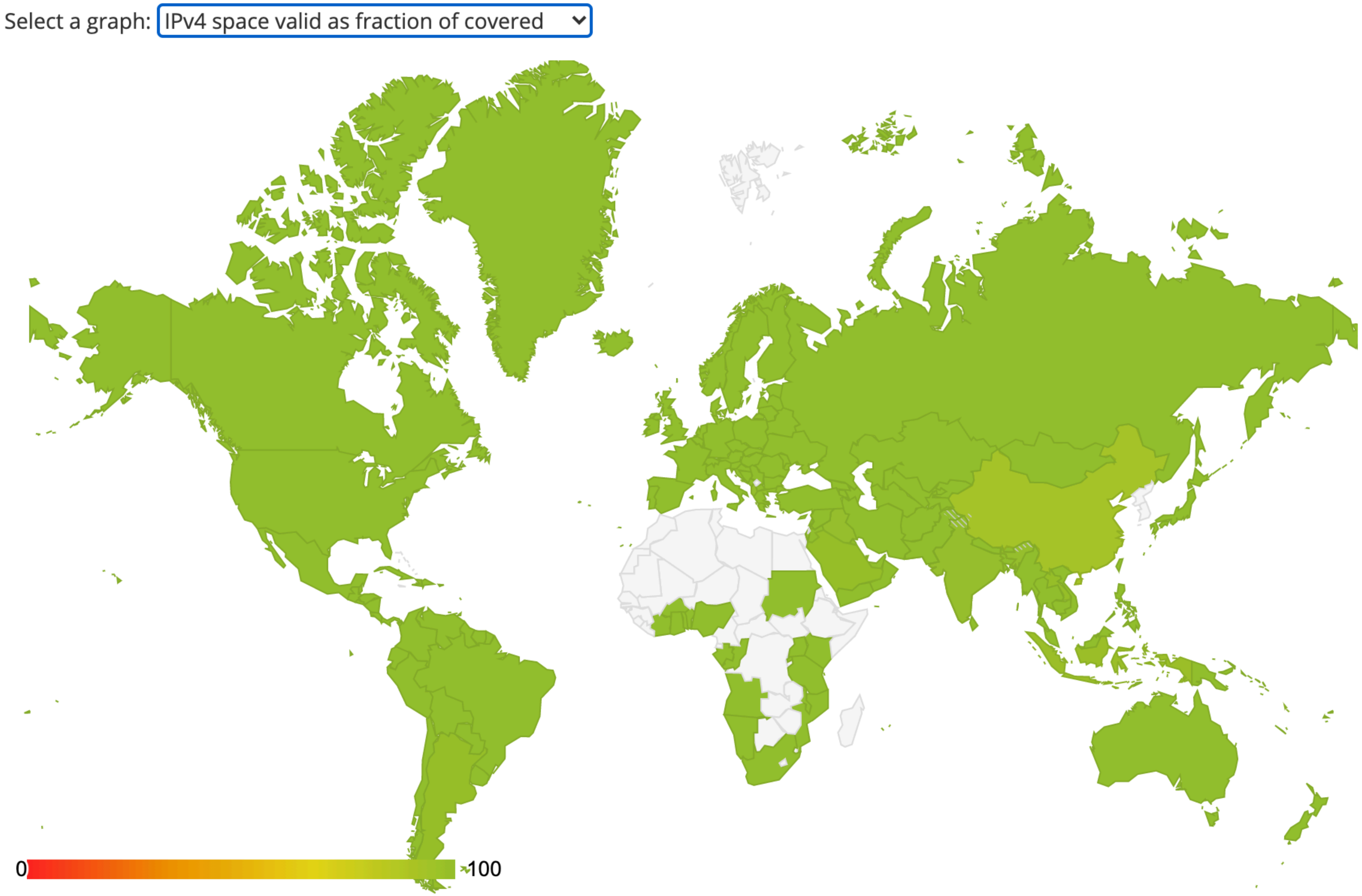
is authorised to be announced by

AS Number

Coverage ROAs



Accuracy ROAs

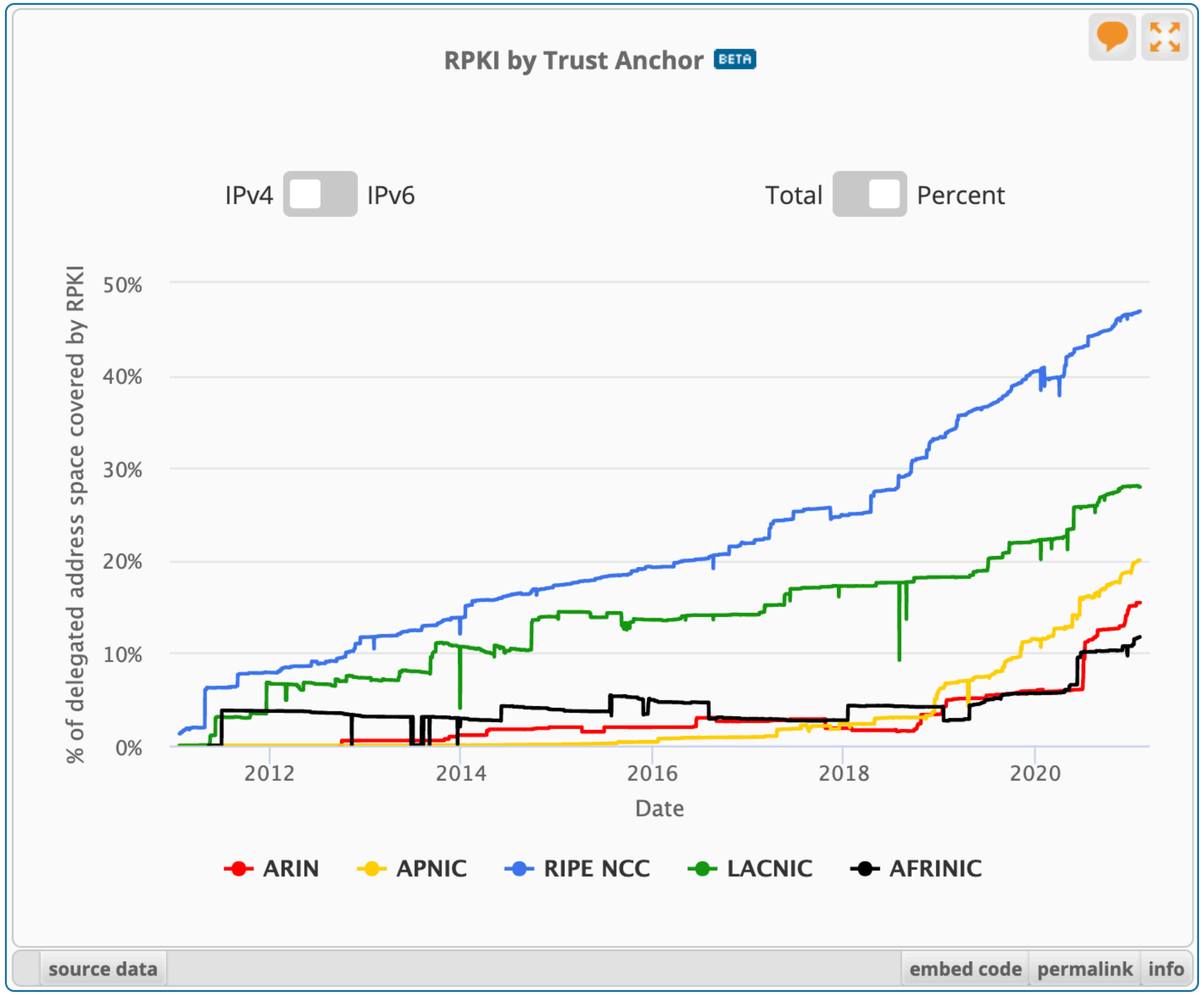


ROAs in some Asia Pacific countries

Country	% Prefixes	% Addreses	Accuracy
AU	26%	44%	100,0%
KZ	12%	5%	100,0%
JP	12%	25%	100,0%
MN	99%	85%	100,0%
AE	36%	29%	99,9%
IR	90%	97%	99,9%
RU	27%	31%	99,9%
PK	91%	97%	99,8%
IN	43%	57%	99,4%
ID	39%	15%	97,6%
CN	2%	2%	93,2%

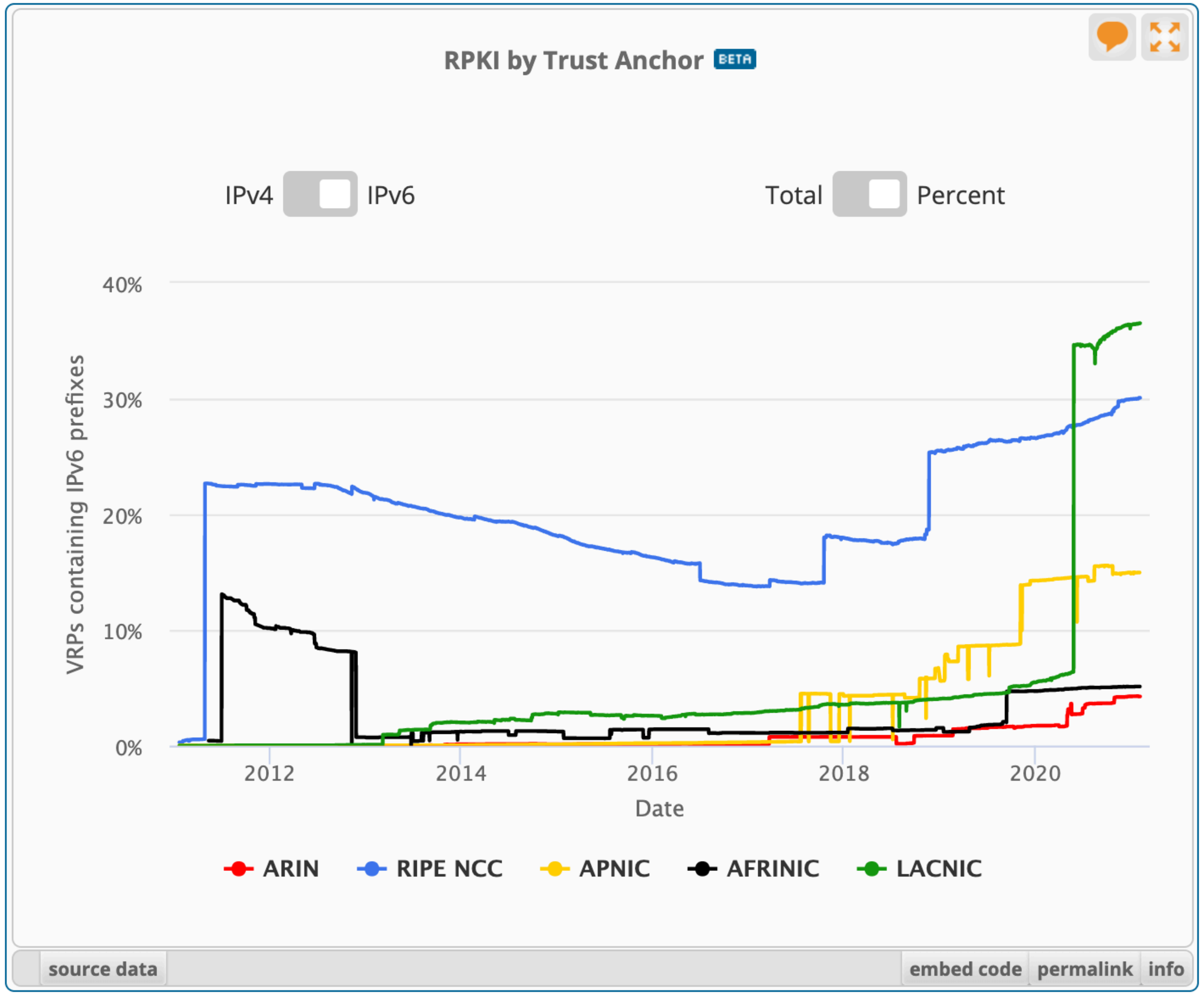
source: https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html

Number of ROAs Globally IPv4



- Source: https://stat.ripe.net/widget/rpki-by-trust-anchor

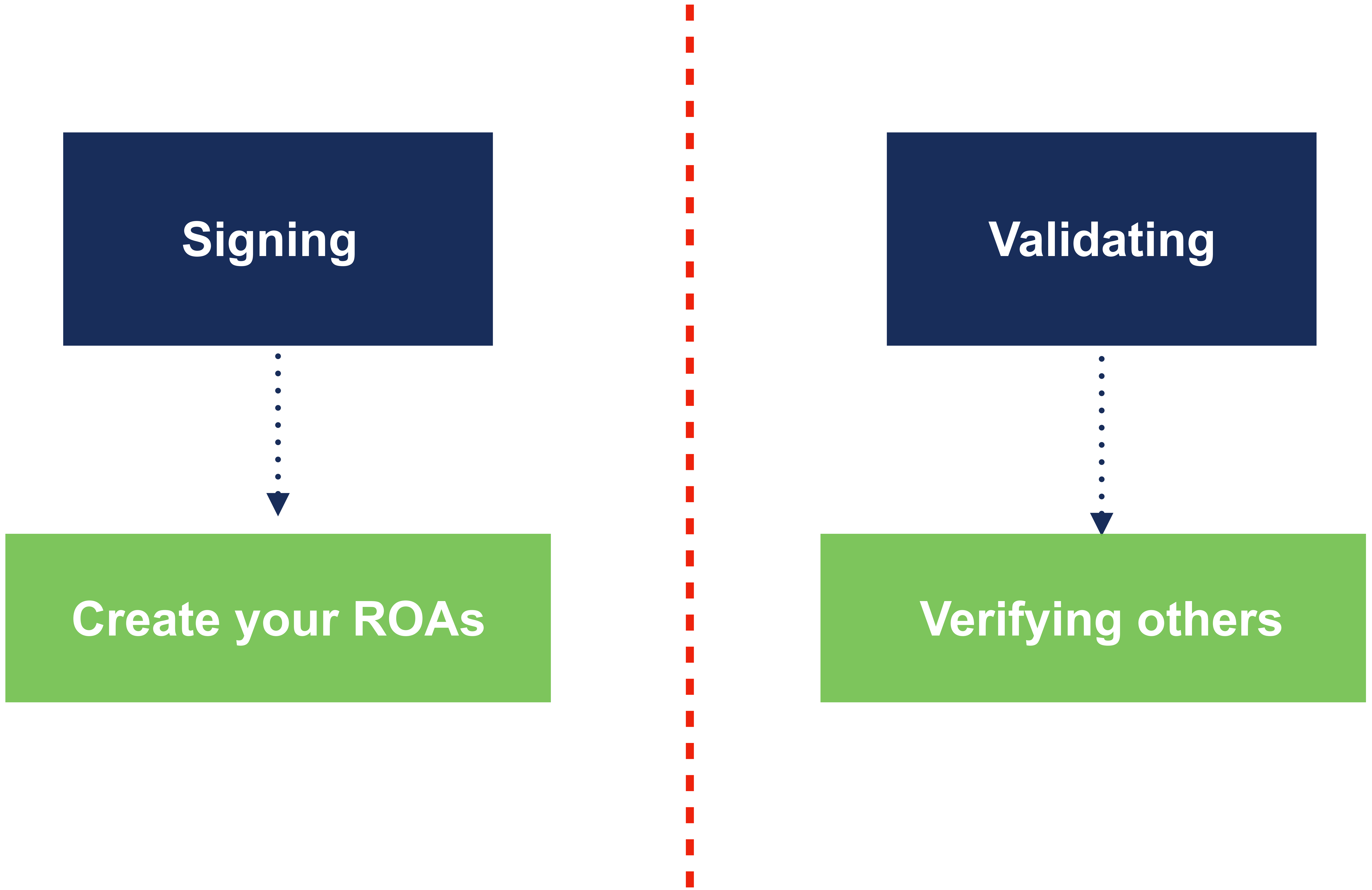
Number of ROAs Globally IPv6



- Source: https://stat.ripe.net/widget/rpki-by-trust-anchor

Route Origin Validation

Two Elements of RPKI



2020: The Year of RPKI

- Serious uptake in Route Origin Validation at Internet Exchange Points and Transit Providers
- Resulting in decrease of invalid BGP announcements
- High uptake in signing objects at all Regional Internet Registries
- All major router vendors are now on board

- Also some outages at different Trust Anchors

Status of Transit and Cloud Providers

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

- Source: isbgpsafeyet.com

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?	?	?	?

- Source: isbgpsafeyet.com

Why This Matters for TLDs

- Route hijacks are a threat to the availability of the DNS
- A successful hijack can make a domain name server unreachable
  - Or cause DNS queries to be diverted to malicious servers

- ROAs are important to state routing intentions
  - So validating parties can make secure routing decisions

- Registrars play an important role in protecting domain names
- Creating ROAs is easy!

How To Get Started?

- Read up! This is a great starting point:
  - https://rpki.readthedocs.io/en/latest/
- Create your ROAs
  - In my.apnic.net or my.ripe.net
- Share your experience or ask for advice
  - https://www.ripe.net/mailman/listinfo/routing-wg/
  - https://www.apnic.net/community/participate/sigs/routing-security-sig/

Questions

RIPE NCC
Academy

Learn something new today!

academy.ripe.net

RIPE NCC Certified Professionals

LAUNCHING SOON

https://www.ripe.net/certifiedprofessionals

Ёnn
Соңы
An Críoch
Y Diwedd
پایان
Ende
Vége
Endir
Koniec
Finvezh
վերջ
Кінець
Son
დასასრული
Finis
הסוף
Tmiem
Liðugt
Lõpp
Amaia
Loppu
Kpaj
Slutt
Kraj
Sfârşit
النهاية
Конец
Konec
Fund
Fine
Fin
Einde
Fí
Край
Beigas
Τέλος
Fim
Slut
E1
N1
D2
Pabaiga