



**RIPE
NCC**

RPKI and Routing Security

Presentation | September 2015

Yerevan Regional Meeting

- **Routing Registry**
 - route objects

- **RPKI** (Resource Public Key Infrastructure)
 - ROAs (Route Origin Authorisation)

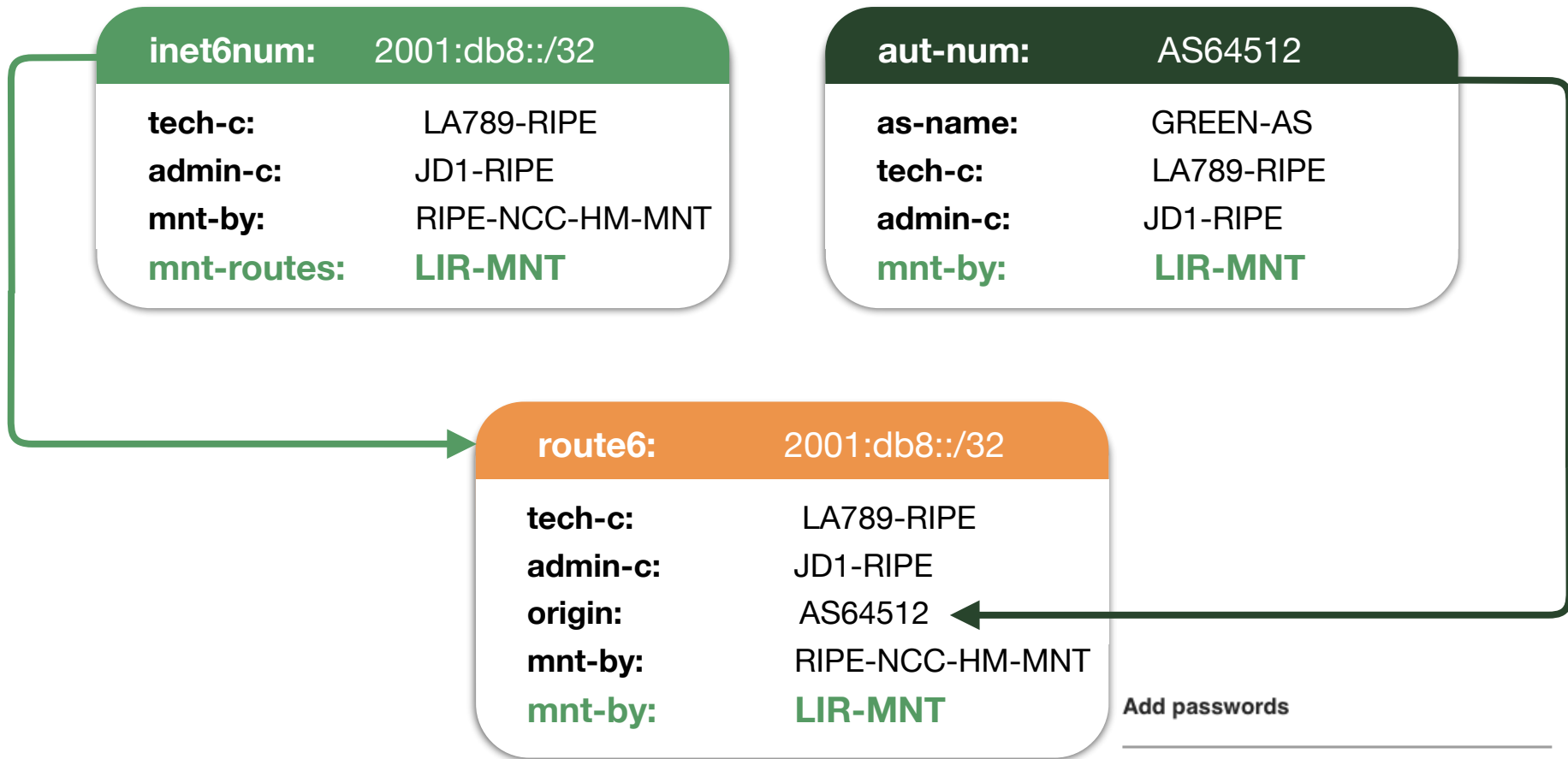
To be able to answer the question:

**Is that ASN authorised to originate
that address range?**

- **Number of public databases that contain routing policy information which mirror each other:**
 - RIPE, APNIC, RADB, JPIRR, Level3, ...
 - <http://www.irr.net>
- **RIPE NCC operates the RIPE Routing Registry**
 - Part of the RIPE Database
 - Part of the Internet Routing Registry

- **inetnum** = IPv4 address range
- **inet6num** = IPv6 address range
- **aut-num** = single AS number and routing policy
- **route, route6** = connects IP address range
and an AS number announcing it

Registering Routes



Add passwords

Session passwords

0 stored password(s) ?

12lir +





Introduction the the RPKI



To be able to answer the question:

**Is that ASN authorised to originate
that address range?**

- **Why yet another system?**
 - Lots of Routing Registries
 - Not all mirroring each other
 - Different levels of trustworthiness and authentication

- **RPKI replaces IRR or lives side by side?**
 - Side by side: different advantages
 - Security, almost real time, simple interface: RPKI
 - More info in: IRR

- **Easy to use tools**
 - No installation required
 - Easy to configure manual overrides
- **Tight integration with routers**
 - Supported routers have awareness of RPKI validity states
- **Stepping stone for AS-Path Validation**
 - Prevent Attacks on BGP

- **The authority on who is the registered holder of an Internet Number Resource in our region**
 - IPv4 and IPv6 Address Blocks
 - Autonomous System Numbers
- **Information is kept in the Registry**
- **Accuracy and completeness are key**

- **Based on open IETF standards (sidr)**
 - **RFC 5280: X.509 PKI Certificates**
 - **RFC 3779: Extensions for IP Addresses and ASNs**
 - **RFC 6481-6493: Resource Public Key Infrastructure**
- **Issued by the RIRs since 1 January 2011**
- **State that an Internet number resource has been registered by the RIPE NCC**

- **Resource Certification is a free, opt-in service**
 - Your choice to request a certificate
 - Linked to registration
 - Renewed every 12 months
- **Enhancement to our Registry**
 - Offers validatable proof of holdership





RPKI

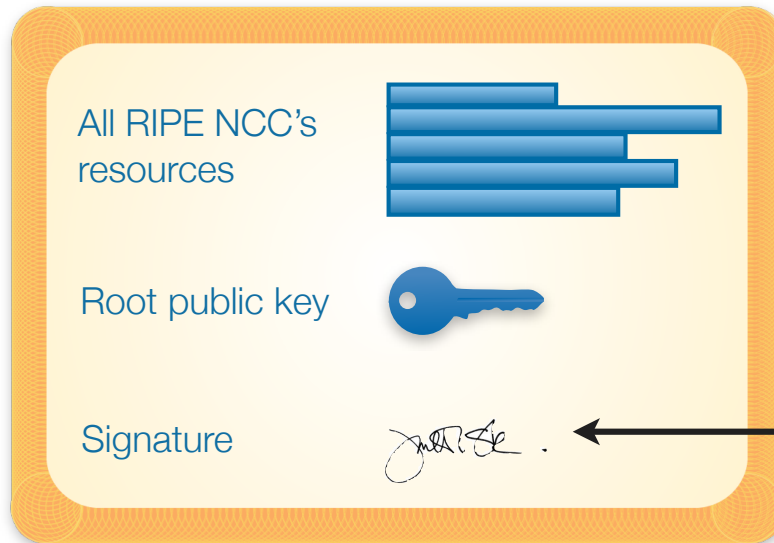
Setting it up:

The announcers side



- **RIPE NCC issues digital certificates**
 - To LIRs
 - To all resource holders
 - Upon request
- **Certificate lists all resources held by the member**

RIPE NCC's Root Certificate

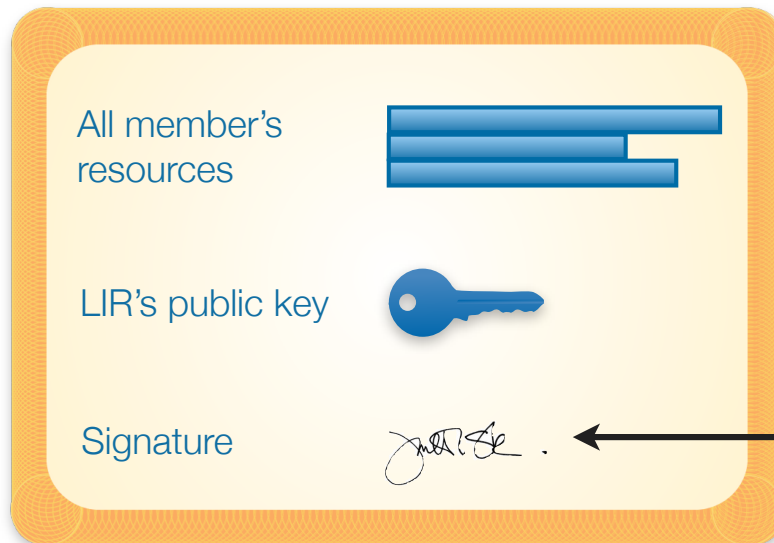


Root's (RIPE NCC) private key



sign

LIR's Certificate



LIR's private key



sign

- **LIRs can use their certificate to create a ROA for each of their resources (IP address ranges)**
 - Signed by the root's private key
- **ROA states**
 - Address range
 - Which AS this is announced from (freely chosen)
 - Maximum length (freely chosen)
- **You can have multiple ROAs for an IP range**
- **ROAs can overlap**

- A ROA is nothing more than a statement that:
 - specifies which AS can originate your prefix, and
 - what the maximum length of that prefix is...

Route Origin Authorisation

AS Number	Prefix	Maximum Length	Submit
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="submit"/>

41 BGP Announcements

4 ROAs

4 Valid 1 Invalid 36 Unknown

3 OK 1 Causing problems

BGP Announcements

Route Origin Authorisations (ROAs)

History

Search...

Create ROAs for selected BGP Announcements

Valid

Invalid

Unknown

<input type="checkbox"/>	Origin AS	Prefix	Current Status	
<input type="checkbox"/>	AS12654	2001:7fb:fe01::/48	UNKNOWN	
<input type="checkbox"/>	AS12654	2001:7fb:fe0c::/48	UNKNOWN	
<input type="checkbox"/>	AS12654	2001:7fb:fe0f::/48	UNKNOWN	
<input type="checkbox"/>	AS12654	2001:7fb:ff00::/48	UNKNOWN	
<input type="checkbox"/>	AS12654	2001:7fb:ff01::/48	UNKNOWN	
<input type="checkbox"/>	AS12654	2001:7fb:ff02::/48	UNKNOWN	
<input type="checkbox"/>	AS12654	2001:7fb:ff03::/48	UNKNOWN	

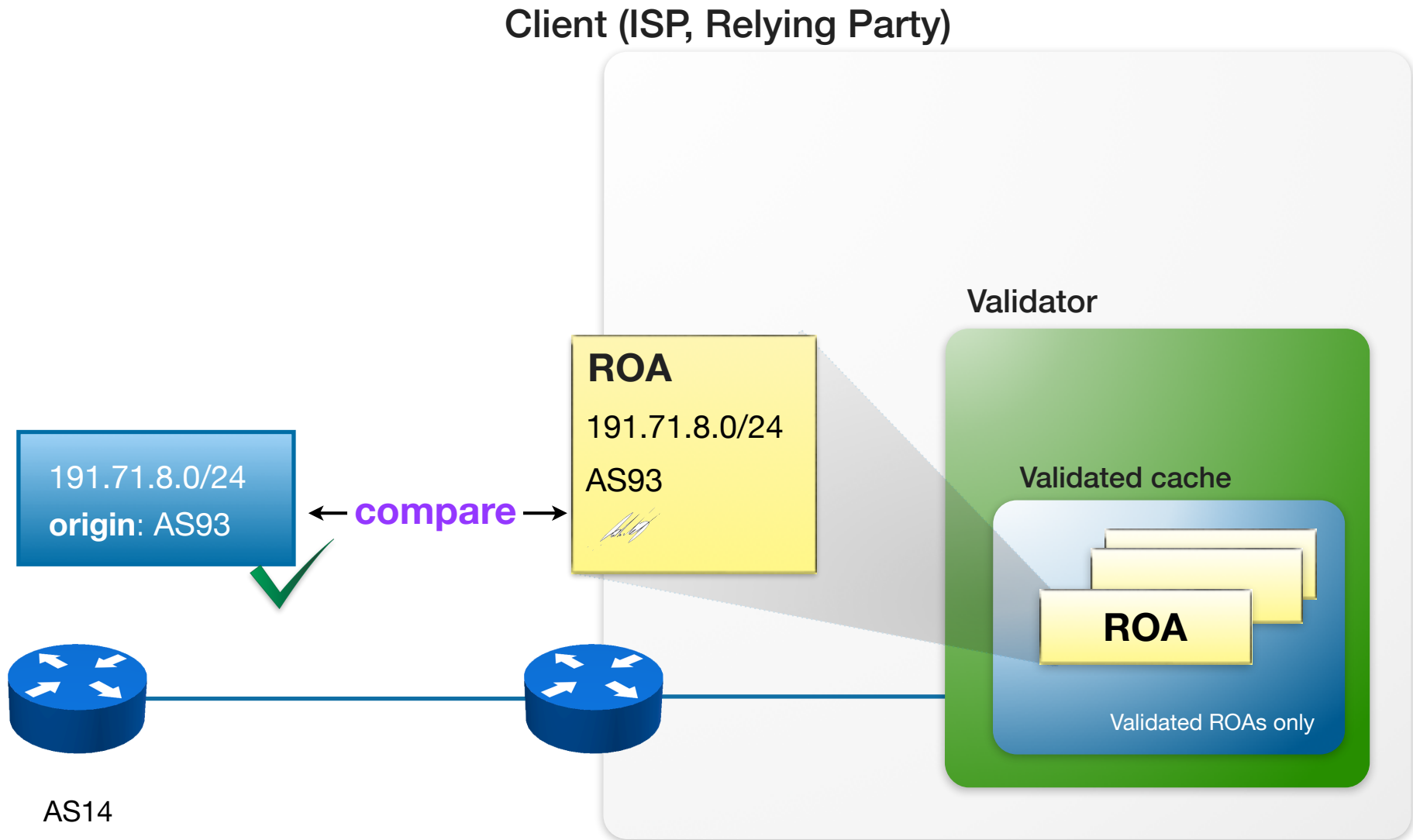
- **RIPE NCC maintains a Certificate Repository containing**
 - All the certificates
 - All the public keys
 - All the ROAs

Validation: The Relying Party's Side



- **The validator of the client can access RIPE NCC's Repository with all the certificates, public keys, ROAs**
- **It downloads everything and then performs validation, checking whether the certificates and ROAs are valid. Then it constructs a list of valid ROAs, which is its “validated cache”**

- **The Relying Party's router can connect and download the cache from the validator**
- Router can then compare any BGP announcements to the list of valid ROAs in the validated cache



- **valid**
 - There is a ROA in the validated cache that matches the BGP announcement of the peer, size matches too
- **unknown**
 - There is no ROA for that prefix in the cache
- **invalid**
 - There is a ROA for the prefix, but for a different AS
 - The size doesn't match

- **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)

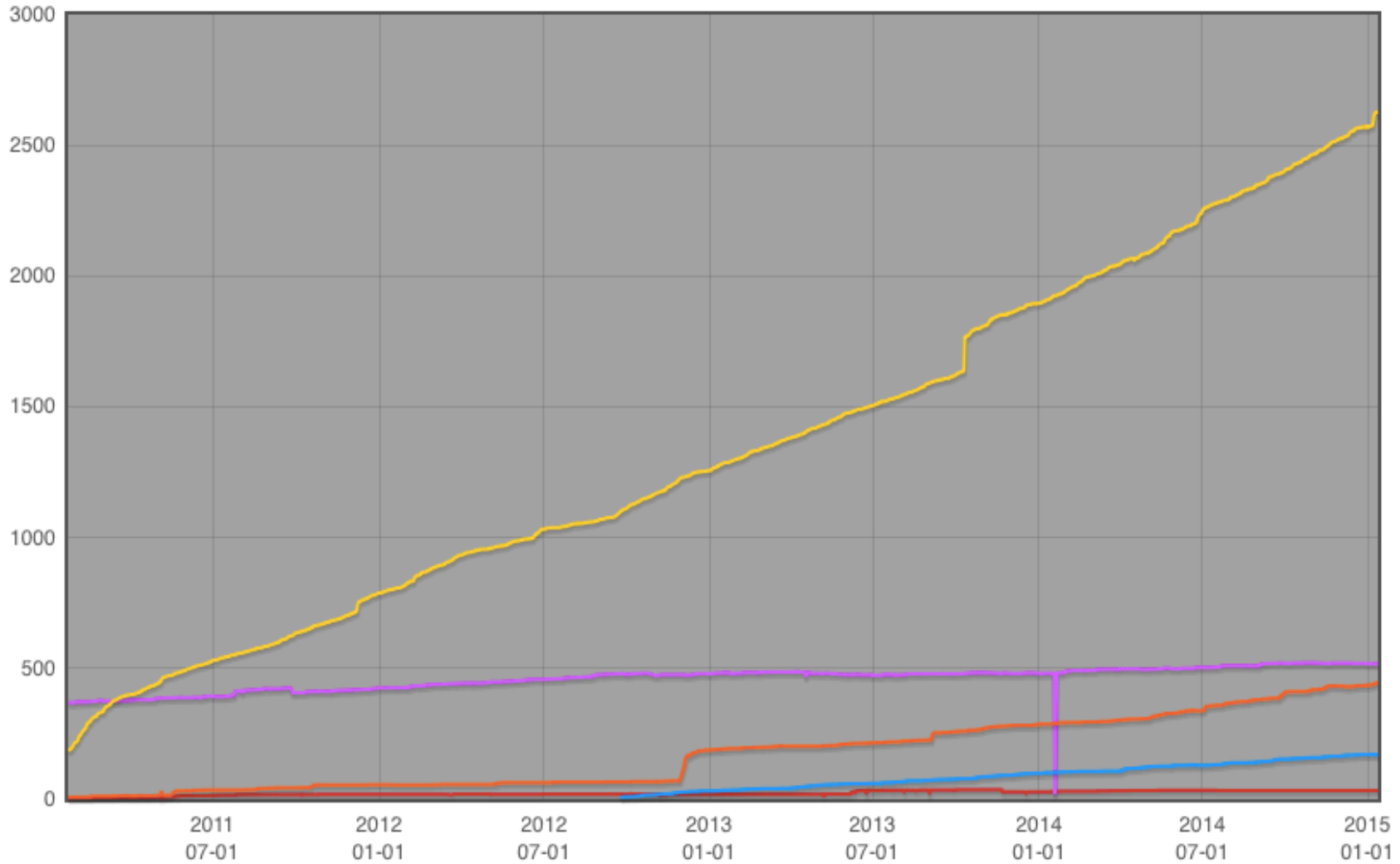
- **One click setup of resource certificate**
 - Automate key roll overs and signing
 - User has a valid certificate for as long as holder of the resources
 - Changes in holdership handled automatically
- **Hide all the crypto complexity from the UI**
 - Hashes, SIA and AIA pointers, etc.
- **Focus on creating and publishing ROAs**
 - Match your intended BGP configuration

- **Merge IRR ‘route’ object management in RPKI UI**
- **Replace rsync as protocol for fetching data**
 - something faster and more scalable (HTTP)
- **Support Inter-RIR transfers**
- **Production support for the delegated model**
- **Path Validation**

People Requesting a Certificate

Number of Certificates AfrinIC APNIC ARIN LACNIC RIPE NCC

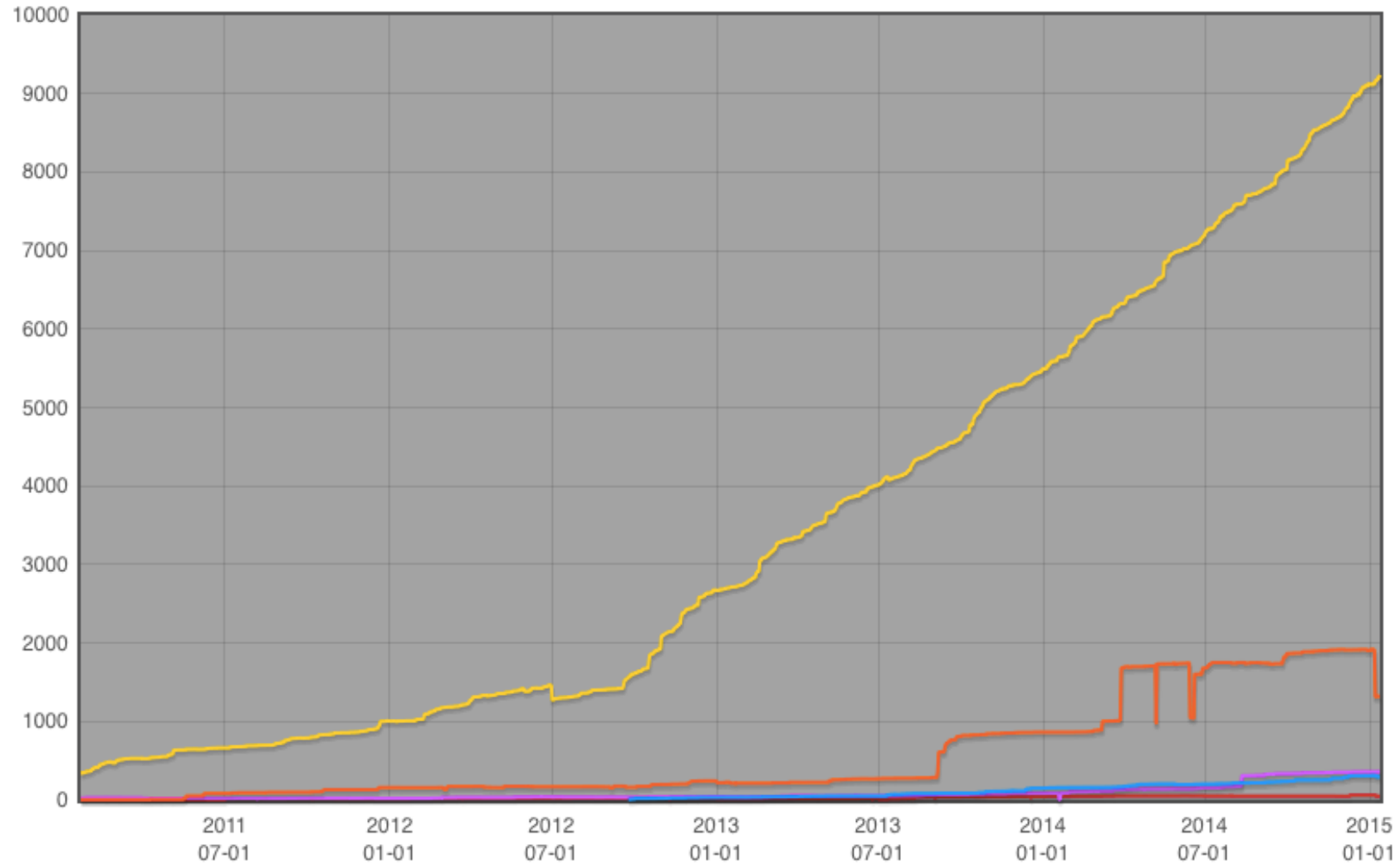
This graph shows the total number of resource certificates created under the RIR Trust Anchor. One certificate is generated per LIR, listing all eligible Internet resources



People Actually Creating ROAs

IPv4 prefixes in ROAs Afrinic APNIC ARIN LACNIC RIPE NCC

This graph shows the total amount of distinct IPv4 prefixes found in the ROAs



The End!

Край

Y Diwedd

Fí

Finis

النهاية

Соңы

ჟღერჟ

Liðugt

Ende

Finvezh

Кінець

Konec

Kraj

Ěnn

Fund

پایان

Lõpp

Beigas

Vége

Son

Kraj

An Críoch

הסוף

Fine

Endir

Sfârșit

Fin

Τέλος

Einde

Конец

Slut

Slutt

დასასრული

Pabaiga

Fim

Amaia

Loppu

Tmiem

Koniec