# How to Make Routing More Secure

## Resource Certification (RPKI)

Mirjam Kühne & Ivo Dijkhuis (RIPE NCC)

TF-CSIRT 45 | Poznan - Poland | 22 May 2015

# Overview



- Very brief introduction to the RIPE NCC
- IPv4 hijacking and IPv4 transfers
- Problem statement
  - Routing Security
- Possible solution
  - Resource Certification (RPKI)
- Making routing decisions
- Uptake of RPKI and future developments

# The RIPE Network Coordination Centre



- Established in 1992 by the RIPE community
  - Initially part of the academic network association
  - Since 1997 a membership association under Dutch law
  - Not for profit, independent, neutral, open
  - Main offices in Amsterdam; staff in Dubai and Moscow
- Funded by the membership
  - 11,500 members from 76 countries
  - Initially mostly ISPs and universities
  - Now also traditional industries, small Internet companies
- One of five Regional Internet Registries

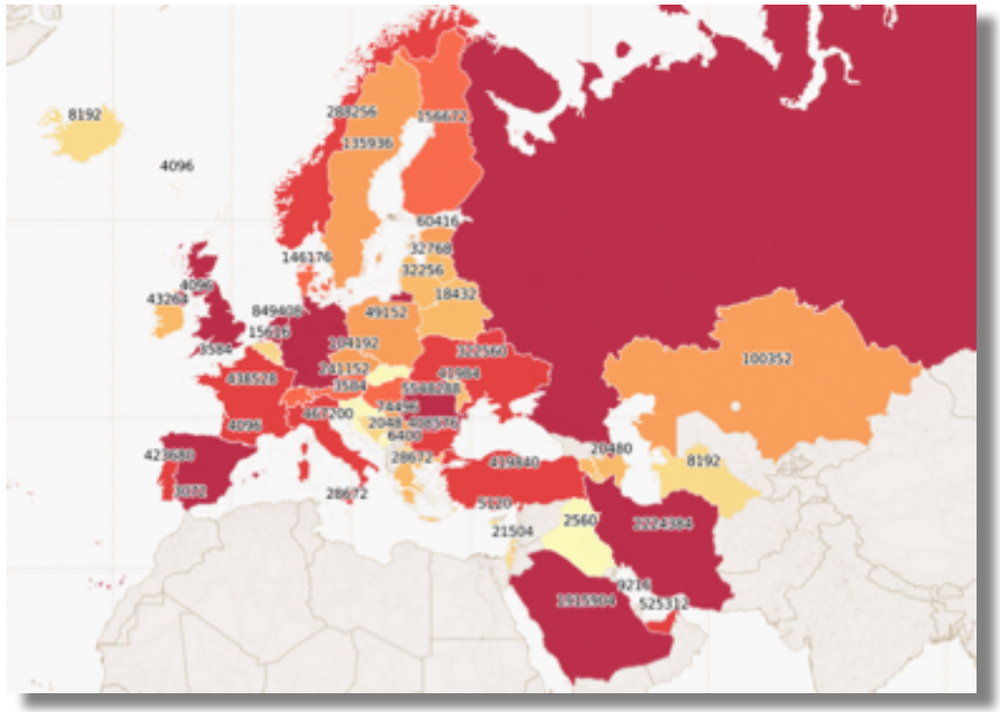
# Regional Internet Registries



# IPv4 Address Hijacking and Transfers



- Presented on IPv4 hijacking at TF-CSIRT in Rome
- Number of hijackings went down
  - Due to clean-up in RIPE Database
- Number of IPv4 transfer went up significantly
  - See recent post on RIPE Labs (labs.ripe.net)
- Transfers can create routing overlaps






RIPE NCC

# The Issue



- Network operators should only announce the IP block (IP prefix) they are the legitimate holder of
- However, errors can happen
  - Due to typos or
  - A bad person is trying to hijack a network by announcing a prefix maliciously

**So the question is:**

**Is this autonomous system (AS) really supposed to be announcing this IP address block?**

# The Solution - Resource Certification



- The Regional Internet Registries (RIRs) are the authority on who is the legitimate holder of resources in their region
  - IPv4 and IPv6 address blocks
  - Autonomous System Numbers
- Information is kept in the registry (whois database)
- Accuracy and completeness are key
  - Offers validatable proof of holdership

# Digital Resource Certificates



- Based on IETF standards
  - Secure Interdomain Routing (SIDR) working group
  - 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

**Digital certificate states that an Internet number resource has been registered by the RIPE NCC**



RIPE NCC

# Certification to Secure Internet Routing



- Resource holders can use their resource certificate to make statements about their BGP routing

Route Origin Authorisation (ROA):

*"I authorise this Autonomous System to originate these prefixes"*

- Also in a ROA: Maximum Prefix Length
  - The longest prefix the ASN may announce

# Example of ROA

***Route Origin Authorization (ROA)***

```
Origin ASN:          17771
Not valid Before:    2010-12-07 00:00:00
Not valid After:     2011-12-07 23:59:59
Prefixes:            2405:1e00::/32  (max length /48)
                     202.63.96.0/19  (max length /24)
                     49.238.32.0/19  (max length /32)
```


# Making Routing Decisions

RIPE NCC

# Route Origin Authorisations



- A ROA affects the RPKI validity of a BGP route
  - VALID: ROA found, authorised announcement
  - INVALID: ROA found, unauthorised announcement
  - UNKNOWN: No ROA found (resource not yet signed)

**Every operator is free to base any routing decision on these validity states**

# Validation in Practice



- All certificates and ROAs are published in a repository and available for download

- Software running on your own machine will periodically retrieve and verify the information
  - Cryptographic tools check all the signatures

- The result is a list of all valid combinations of ASN and prefix, the “validated cache”

# The RPKI Ecosystem



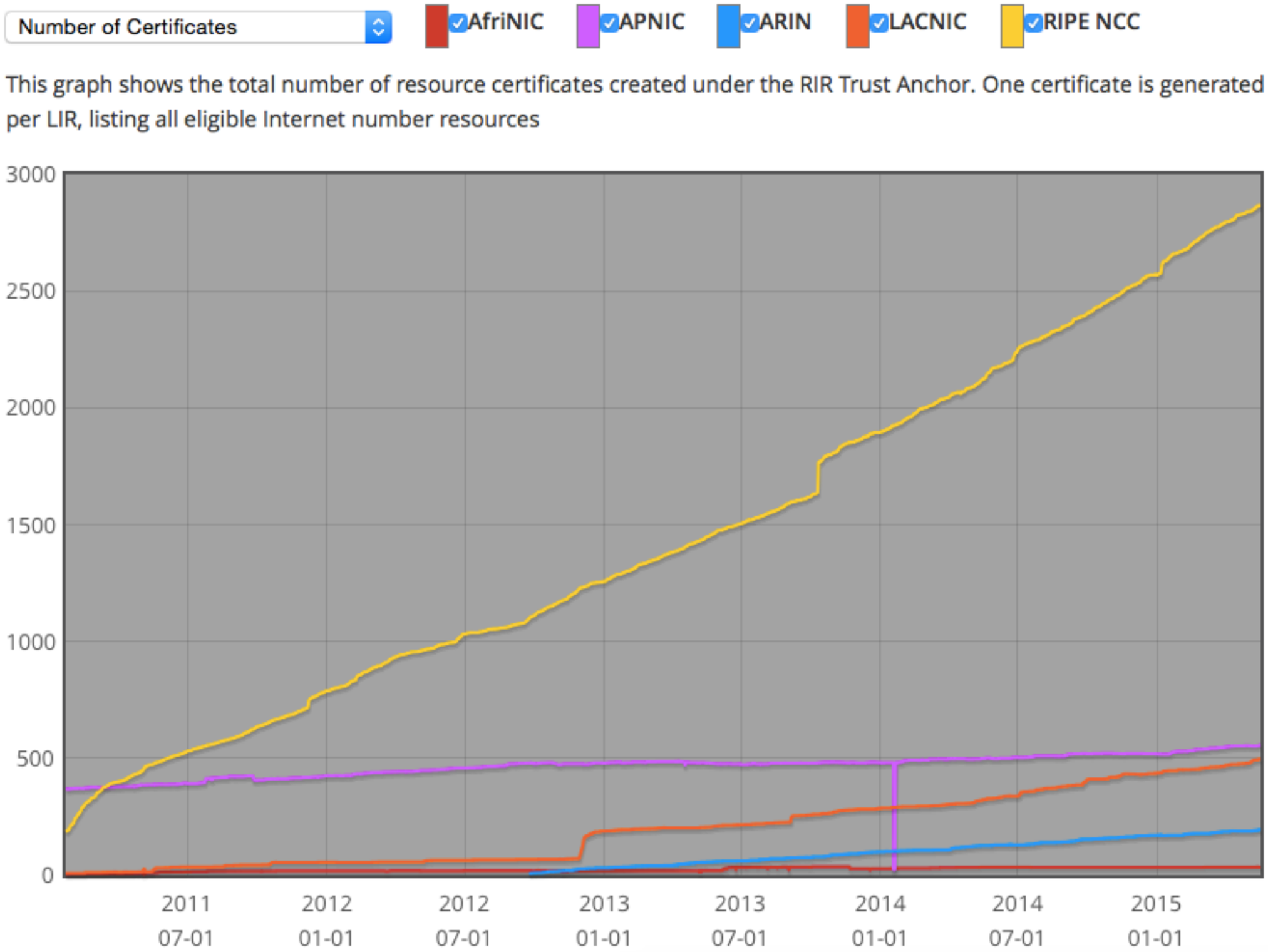
- Validated RPKI information can be sent to router, so operators can use it easily
- A production system since 2011
  - All RIRs offer the functionality to their members
  - All major router vendors offer native support
    - Cisco, Juniper, Alcatel Lucent, Quagga…
- Several open source tools to validate ROAs

# Uptake of RPKI

RIPE NCC

# RPKI Adoption



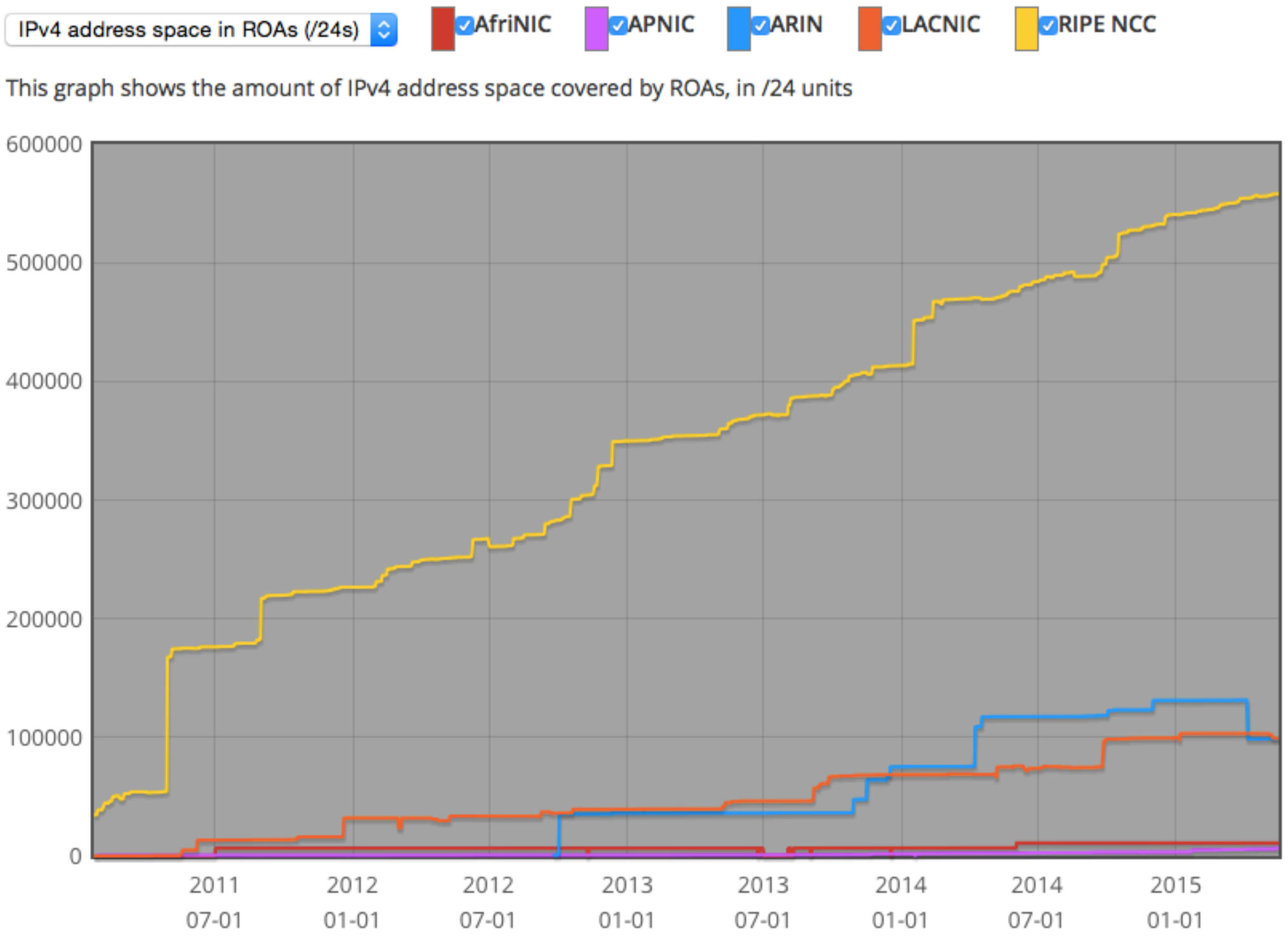





RIPE NCC

# RPKI Adoption








RIPE NCC

# Future Developments of RPKI



- Most major ISP have adopted RPKI
  - Deutsche Telekom, Telefonica, KPN, SFR, etc.
- Adoption by smaller ISPs accelerating now
- Path validation is being standardised
  - Making it impossible to “spoof” an AS
- Origin + Path validation offers full routing security

# Further References



- More information on the RIPE NCC web site

  www.ripe.net/certification

- RPKI Statistics

  http://certification-stats.ripe.net/

- RIPE Labs

  labs.ripe.net

- IETF SIDR WG

  https://datatracker.ietf.org/wg/sidr/charter/