RPKI – Resource Public Key Infrastructure
Validación de Origen en BGP

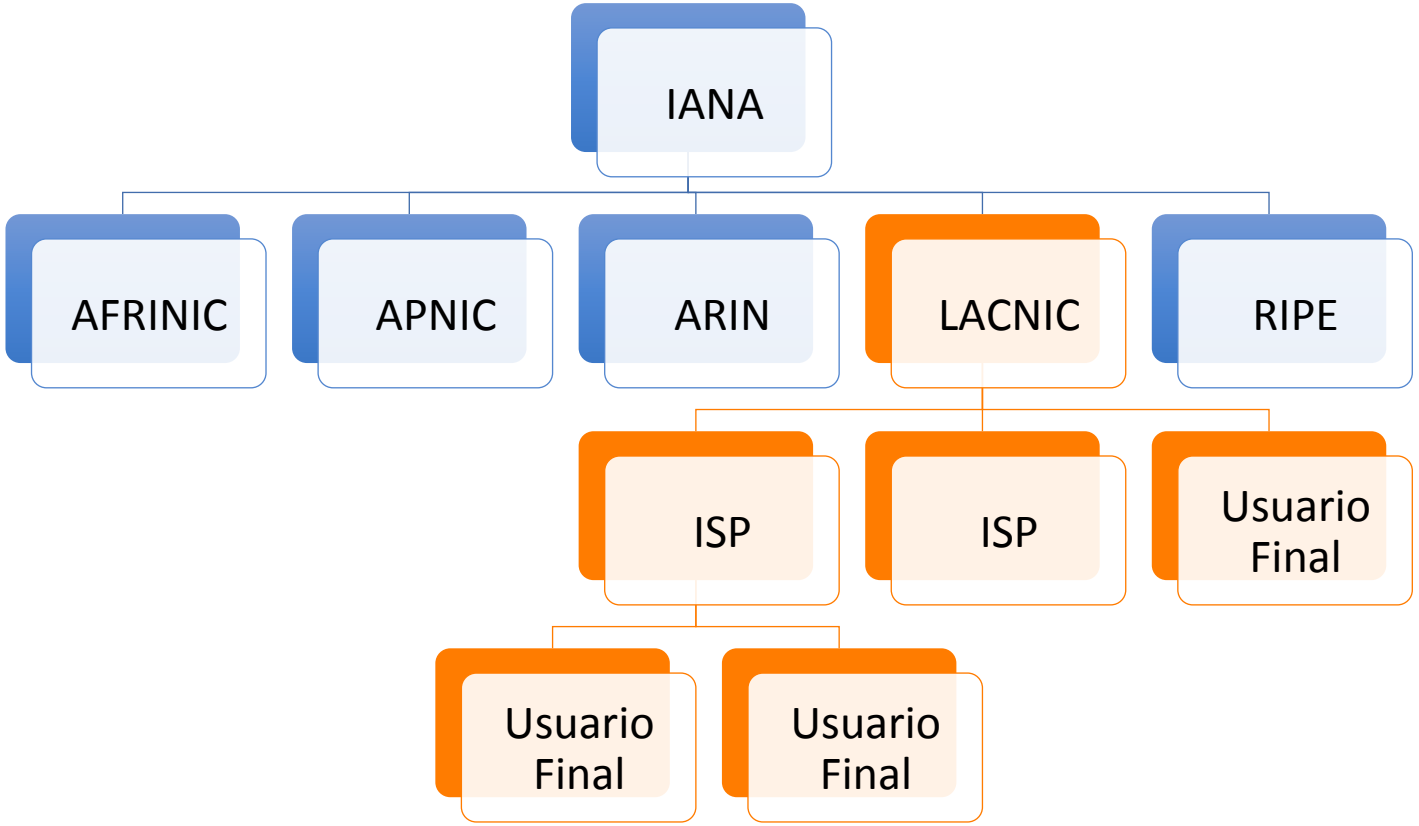
Guillermo Cicileo
guillermo@lacnic.net

Autoridad Nacional para la Innovación Gubernamental
innovamos para ti

lacnic

Secuestro de rutas

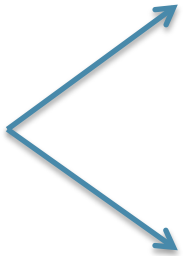
Distribución de Recursos de Numeración de Internet



¿Quién puede usar un recurso?

- Una organización al obtener recursos de Internet (IPv6/IPv4/ASN)
  - Indica a su upstream/peers cuales son los prefijos que va a anunciar
  - Vía e-mail, formas web, IRR (Internet Routing Registry)

Proveedores/peers: verifican derecho de uso



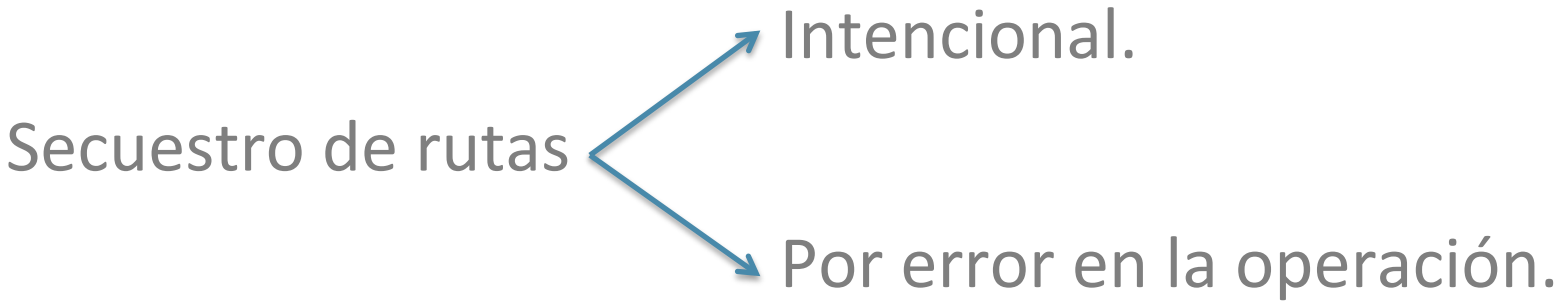
Whois RIRs: Información no firmada, no utilizable directamente para ruteo

Whois IRR: Información no firmada, pocos mecanismos para autentificación de derecho de uso

- La verificación no siempre es todo lo meticulosa que debería ser
- La integridad del sistema depende de la **confianza entre peers**

Secuestro de rutas

- Acción de anunciar a Internet prefijos NO autorizados.



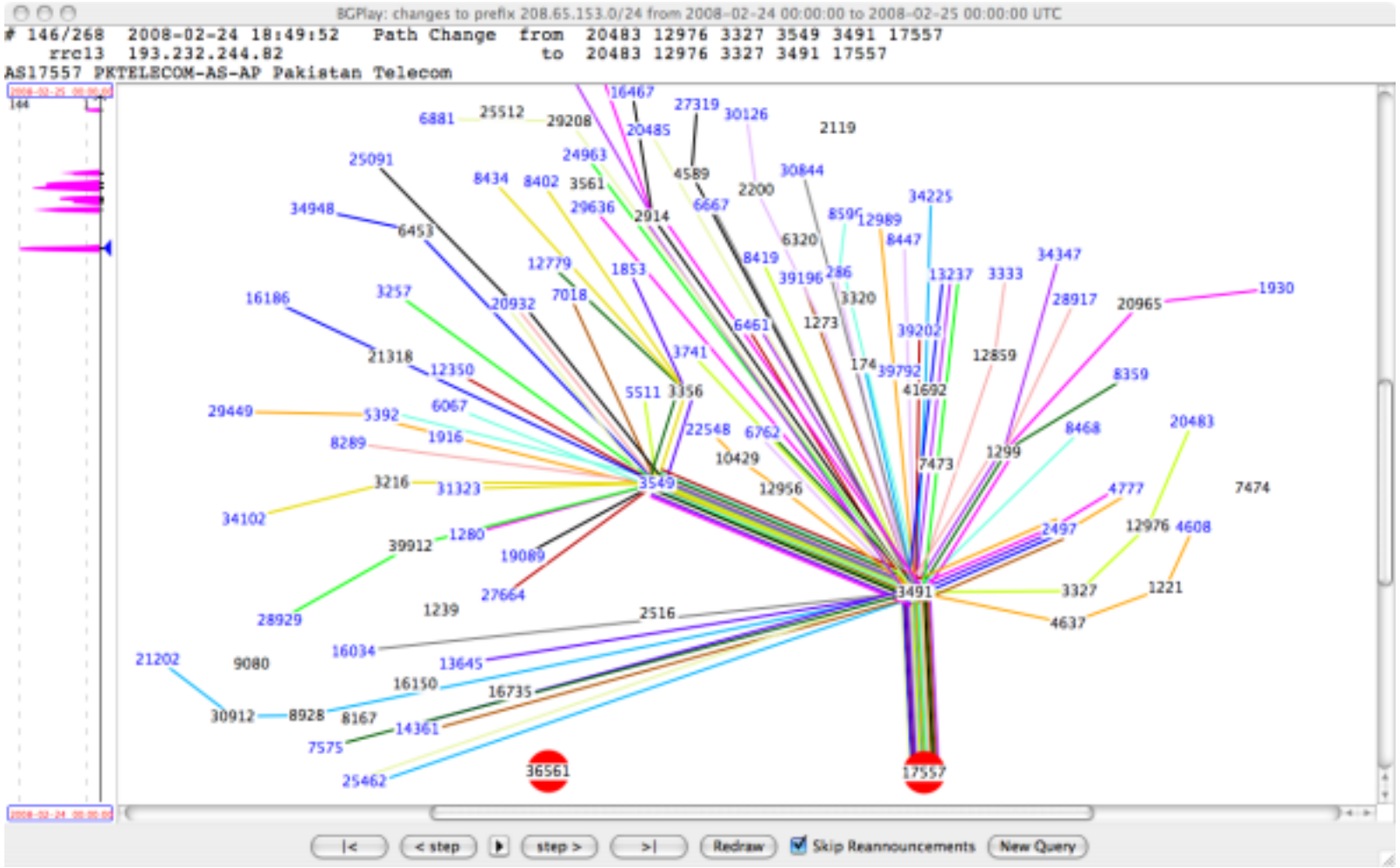
Varios secuestros de rutas vienen ocurriendo en los últimos años.

- Casos más conocidos:
  - Pakistan Telecom vs. You Tube (2008)
  - China Telecom (2010)
  - **Casos en nuestra región**

Pakistan Telecom vs. YouTube

- El Domingo 24 de Febrero de 2008 Pakistan Telecom (AS 17557) anunció el prefijo 208.65.153.0/24 sin autorización
- El upstream provider PCCW Global (AS3491) reenvió este anuncio al resto de Internet, resultando en que YouTube quedó inaccesible
- Análisis detallado (por RIPE NCC): http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study
- Video en YouTube sobre el evento: http://www.youtube.com/watch?v=IzLPKuAOe50

Pakistan Telecom vs. YouTube



Secuestro de rutas

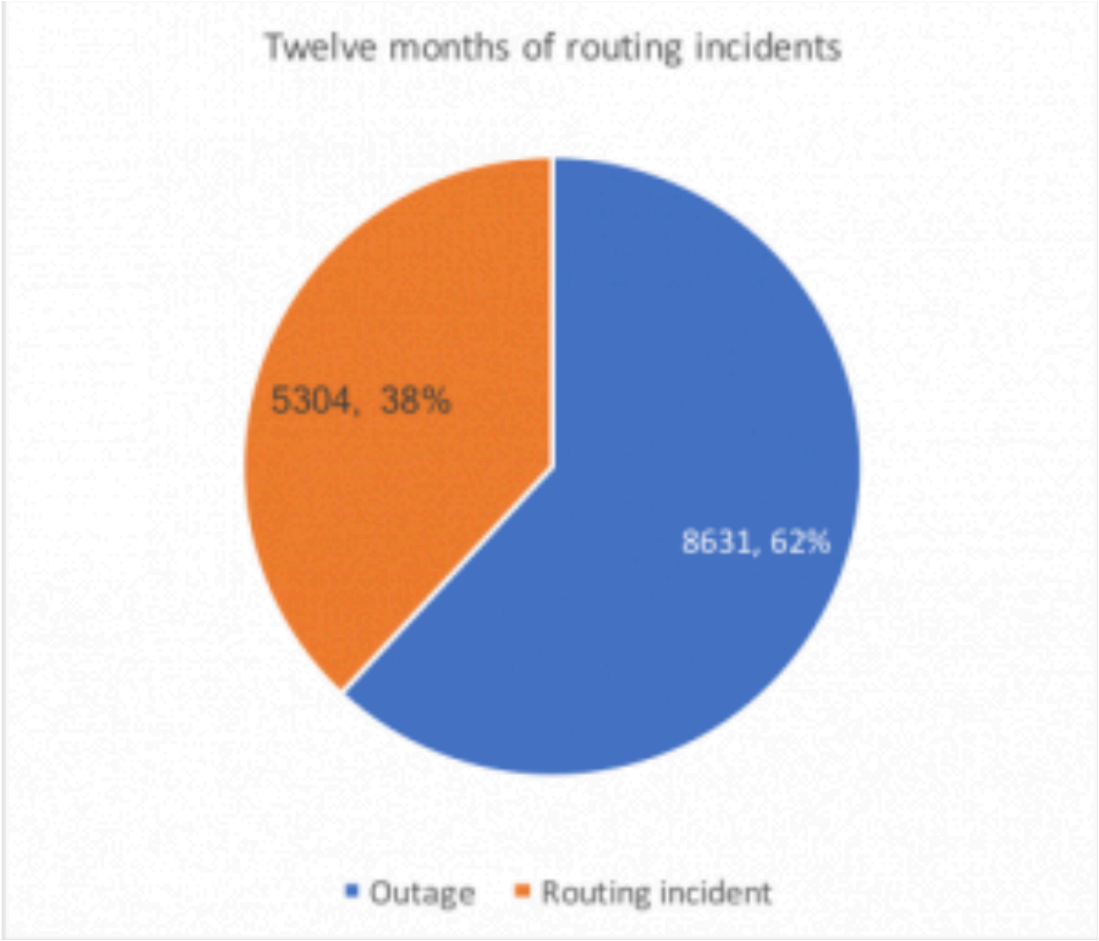
- La mayoría de los secuestros de rutas ocurridos hasta ahora han sido redirecciones de tráfico
  - El problema es detectado por inaccesibilidad del sitio original (ej: caso YouTube)
- Eventualmente publicación temporal de prefijos para hacer spamming
- Sin embargo, en un trabajo de 2008, presentado en DEFCON 16, Pilosov-Kapela demuestran la posibilidad de re-enrutar tráfico sin prácticamente dejar evidencias
  - De esa manera, el tráfico puede ser analizado y procesado sin ser notado

Algunos incidentes recientes

- **Abril 2017:** MasterCard, Visa y más de dos docenas de otras compañías de servicios financieros afectados
  - Grandes cantidades de tráfico fueron enrutados brevemente a través de una telco rusa.
  - Durante varios minutos, Rostelecom estaba generando 50 prefijos para muchos otros Sistemas Autónomos, secuestrando su tráfico.
- **Abril 2018:** Secuestro de DNS de Amazon mediante BGP para robar Crypto moneda:
  - eNet / XLHost (AS10297) sufrió una violación que permitió a los atacantes hacerse pasar por el servicio de DNS autorizado de Amazon.
  - Los usuarios de redes que aceptaron las rutas secuestradas (incluido el servicio DNS recursivo de Google) enviaron sus consultas DNS a un servicio DNS impostor incrustado en AS10297.
  - Si estos usuarios intentaban visitar myetherwallet.com, el servicio impostor DNS no los dirigiría a Amazon Web Services (que normalmente aloja el sitio), sino a un conjunto de direcciones IP rusas, según CloudFlare.
  - Tener en cuenta que los usuarios necesitaron hacer clic a través de las alertas de fallas de certificados en sus navegadores, pero eso no los detuvo.
  - Ver https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/

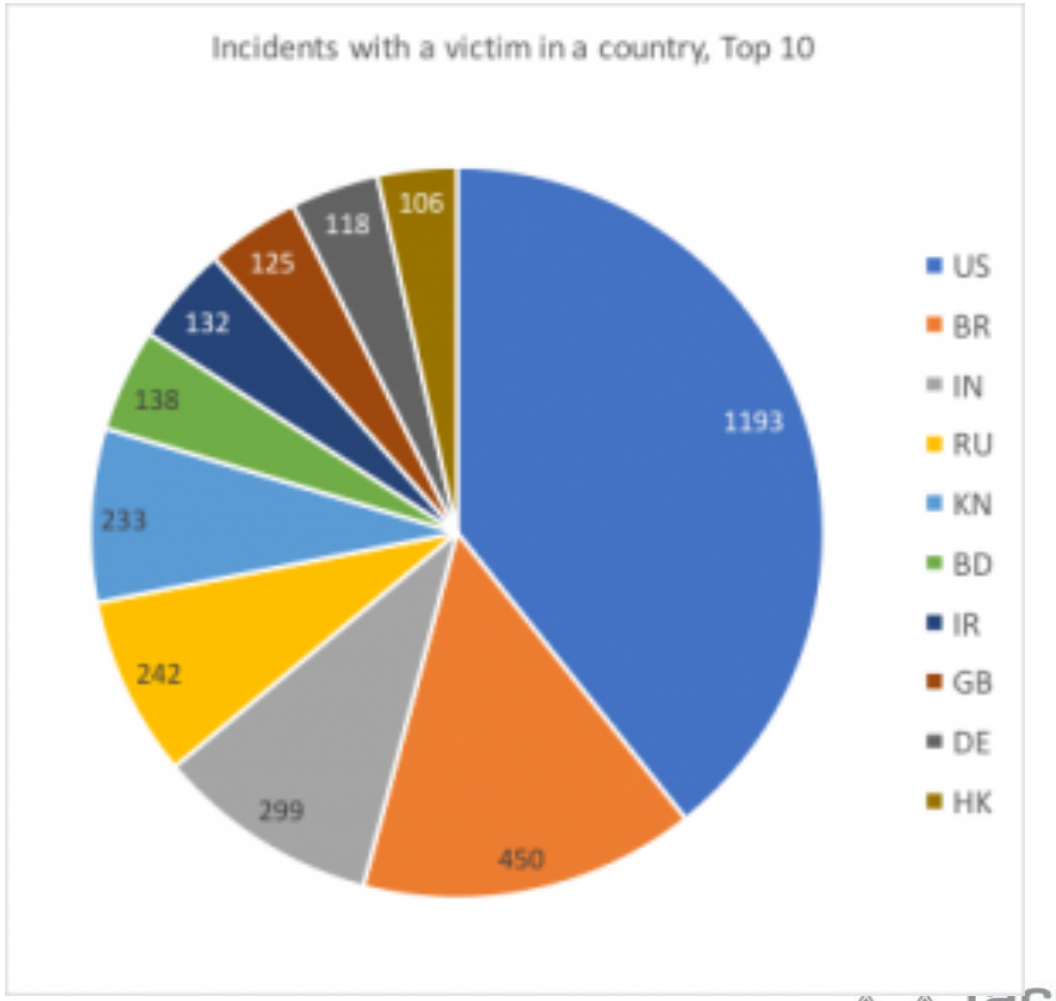
Incidentes de ruteo en 2017

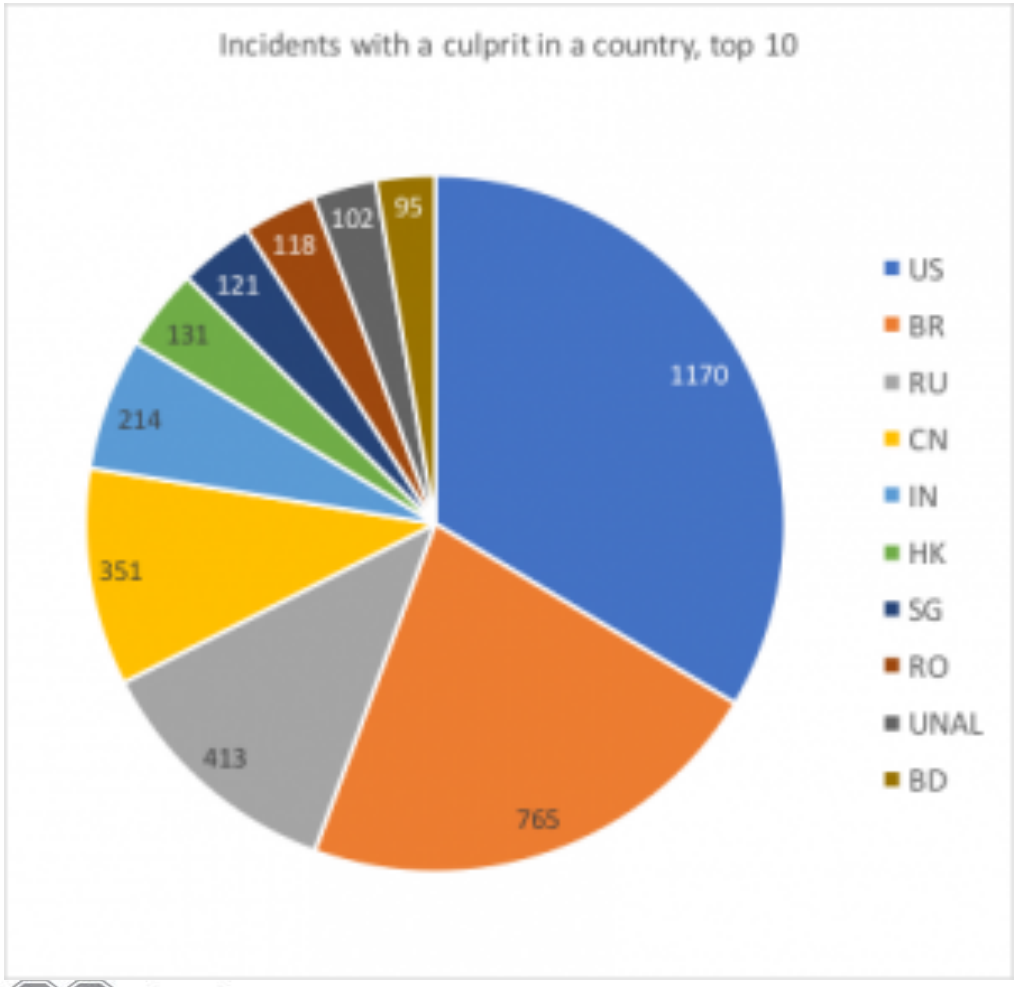
- Aprox. 14.000 incidentes de ruteo (ya sea por leaks/ hijacks o desconexiones)
- Más del 10% de los Sistemas Autónomos de Internet afectados
- 3,106 Sistemas Autónomos fueron víctimas de al menos un incidente de ruteo
- 1,546 redes causaron al menos un incidente.



Fuente: https://blog.apnic.net/2018/01/24/14000-incidents-routing-security-2017/

Países afectados y países que originaron incidentes





RPKI

¿Qué es RPKI?

- RPKI (Resource Public Key Infrastructure)
- Validación del derecho de uso de un recurso

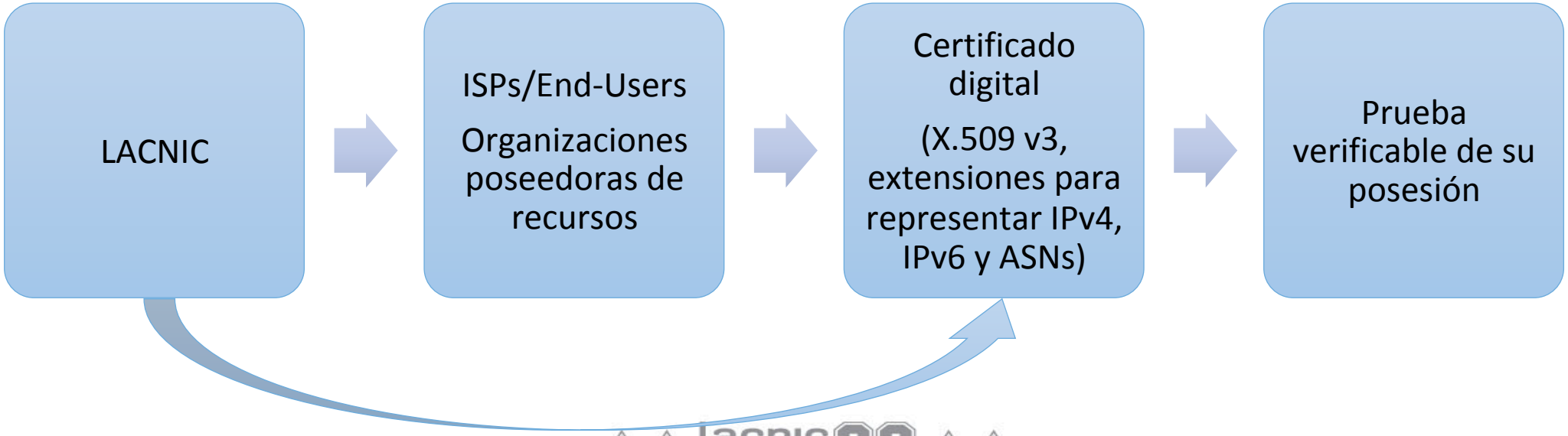
IPv4
IPv6
Sistema Autonomo

- Combina:
  - Modelo jerárquico de asignación de recursos a través de los RIRs
  - Uso de certificados digitales basados en el estándar X.509

- Estandarizado en el IETF, grupo de trabajo SIDR, RFCs 6480 – 6492
  - Gran trabajo de los RIRs en la implementación

RPKI

- Define una infraestructura de clave pública especializada para ser aplicada al enrutamiento
  - En particular, para BGP

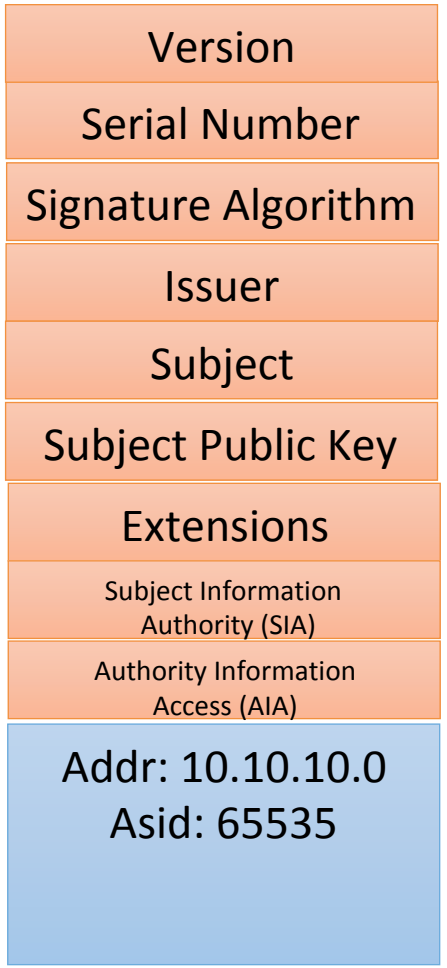


¿Qué compone la solución RPKI?

- Public Key Infrastructure de recursos (IP+ASN+certificados)
- Objetos firmados digitalmente para soportar seguridad del enrutamiento (ROAs)
- Un repositorio distribuido que almacena los objetos PKI y los objetos de enrutamiento firmados (ROAs+CRL+MNF)
- Un Mecanismo de **validación de prefijos**

Certificados de recursos

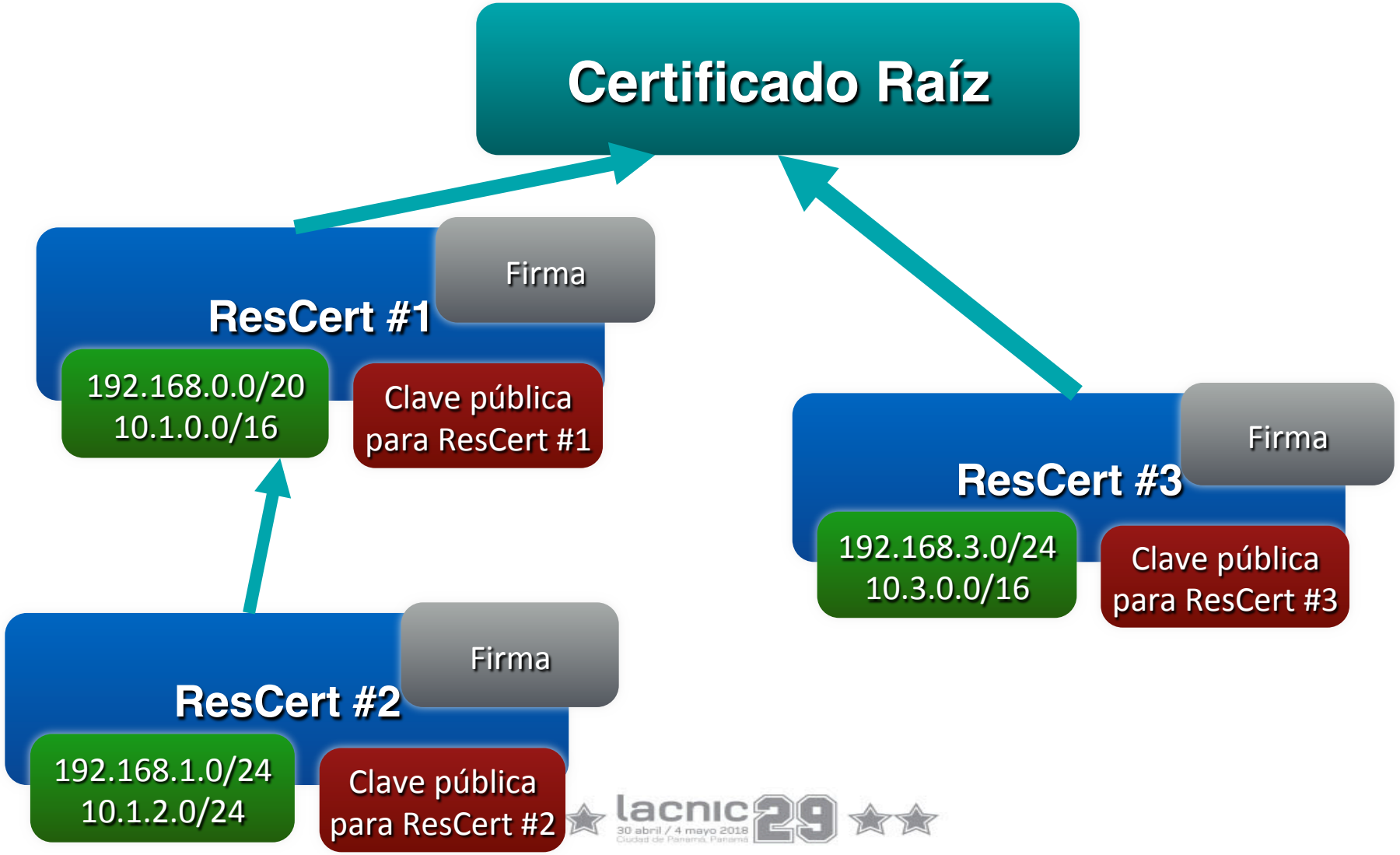
- Certificados Digitales X.509
  - Información del sujeto, plazo de validez, llave publica, etc
- Con extensión:
  - RFC 3779 estándar IETF define extensión para recursos internet.
- Listado de IPv4, IPv6, ASN asignados a una organización



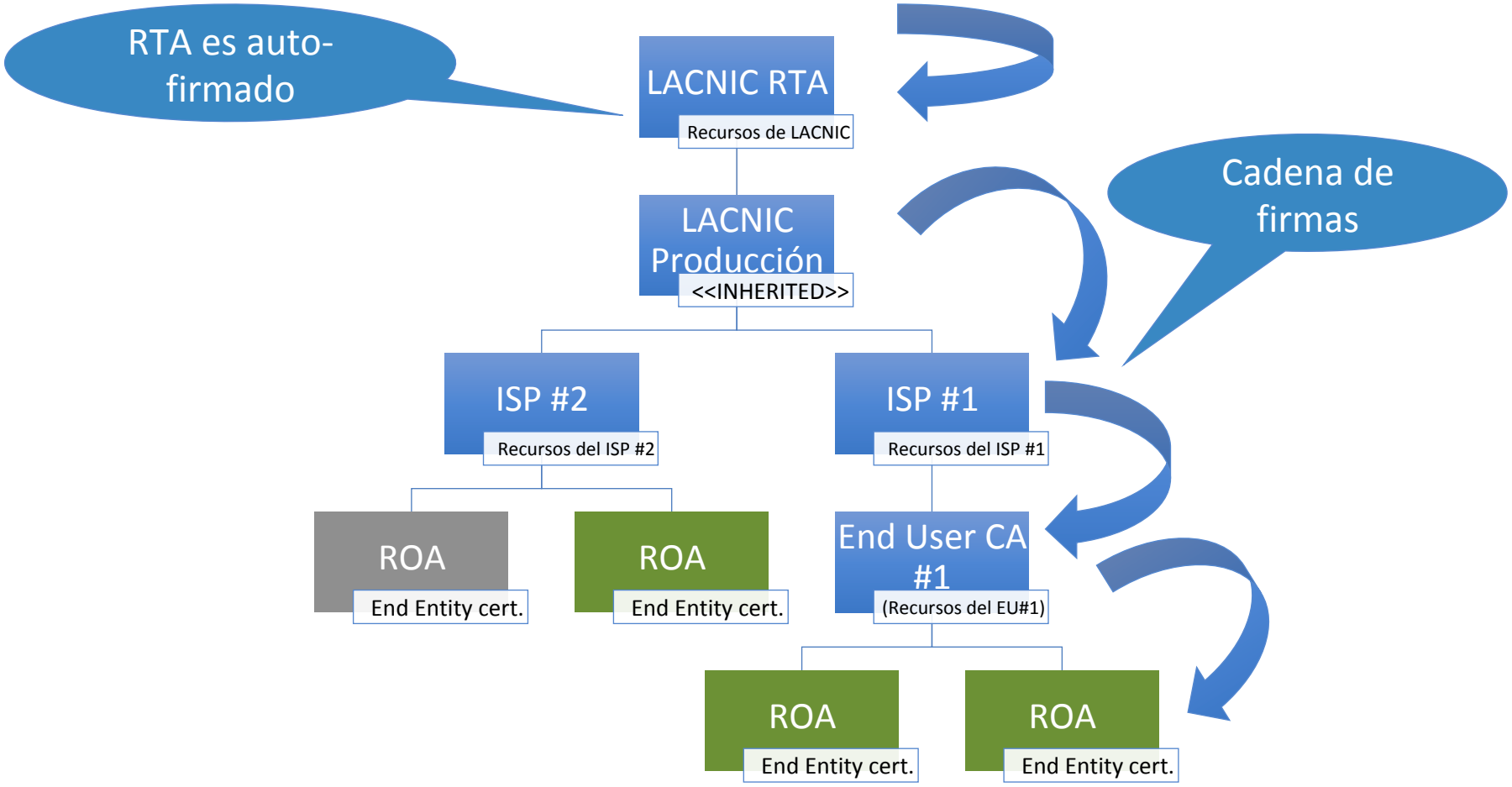
Certificados de Recursos

No se almacena ninguna identidad en el certificado, el campo “Sujeto” se setea a una cadena de caracteres hasheada

PKI de Recursos



Estructura de la RPKI de LACNIC



RPKI

- Los ISPs u organizaciones pueden ***definir y certificar los anuncios de rutas que autorizan*** realizar
  - Mediante objetos digitales llamados ROAs
  - Firmados con la clave privada del certificado
- Es un gran paso hacia un enrutamiento más seguro
  - Permite la validación del sistema autónomo que origina un anuncio por BGP (validación de origen).

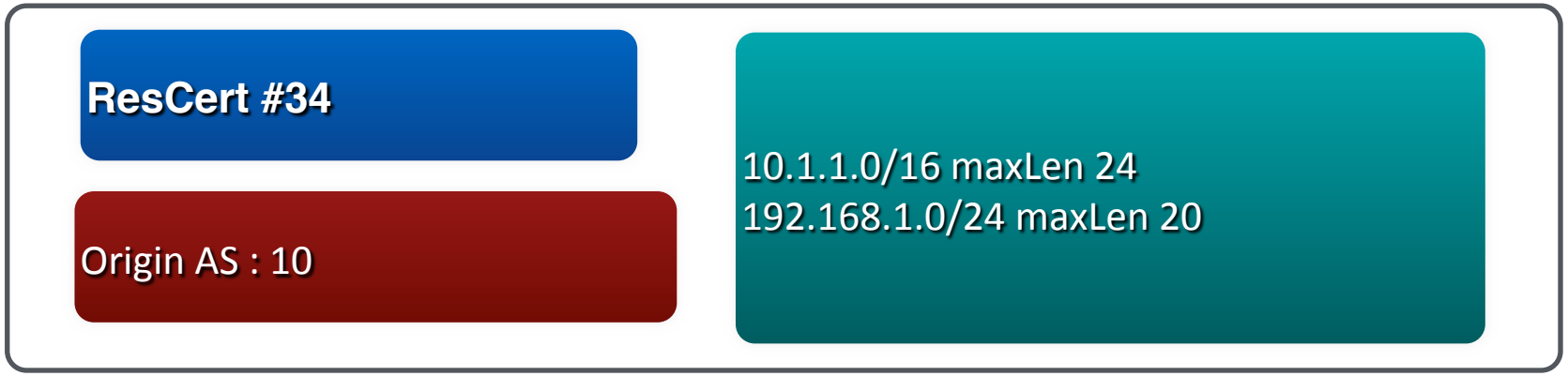
ROAs

- Usando certificados podemos crear objetos que describan el origen de un prefijo

- ROAs: Routing Origin Authorization
  - Los ROAs contienen información sobre el AS de origen permitido para un conjunto de prefijos
  - Los ROAs son firmados usando los certificados generados por RPKI
  - Los ROAs firmados son copiados al repositorio

ROAs

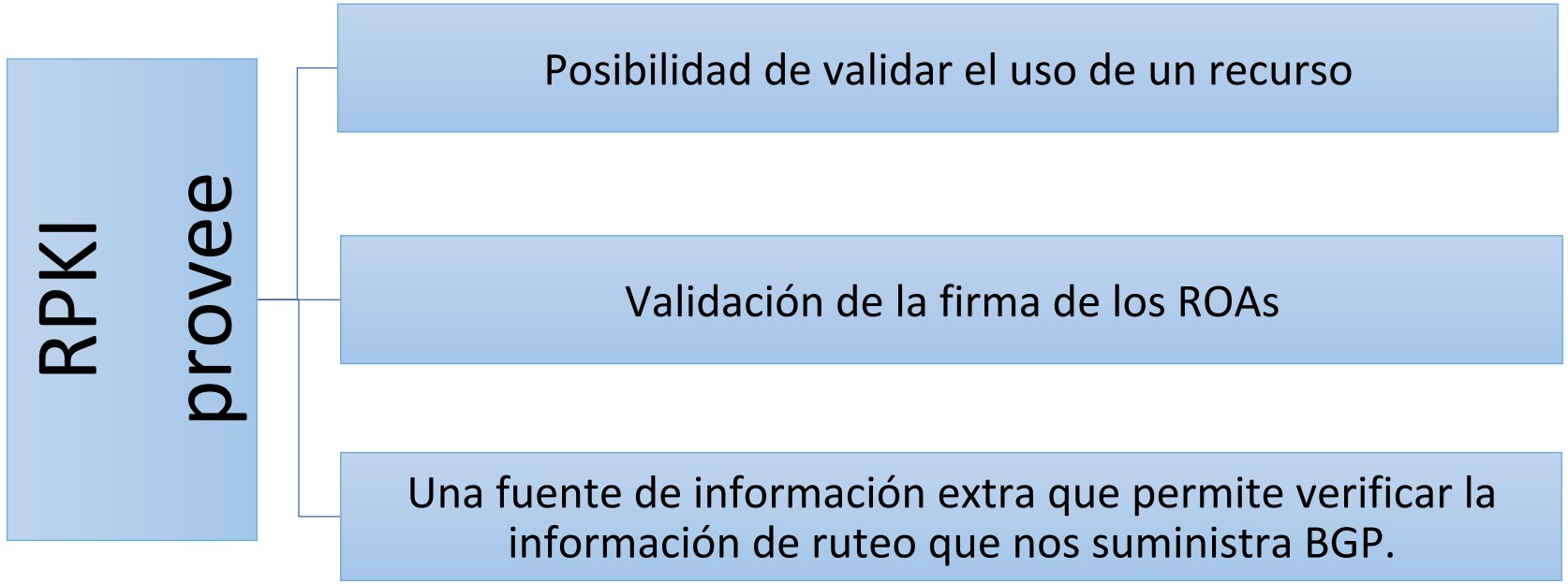
- Usando la cadena de certificados podemos crear objetos firmados que describan el origen de un prefijo.



- ROAs: Routing Origin Authorization
  - Los ROAs contienen información sobre el AS de origen permitido para un conjunto de prefijos.
  - Los ROAs son firmados usando los certificados generados por RPKI.
  - Los ROAs firmados son copiados en un repositorio publicamente accesible

Validación

- Un router podría entonces utilizar los ROAs para validar una ruta y eventualmente, rechazarla



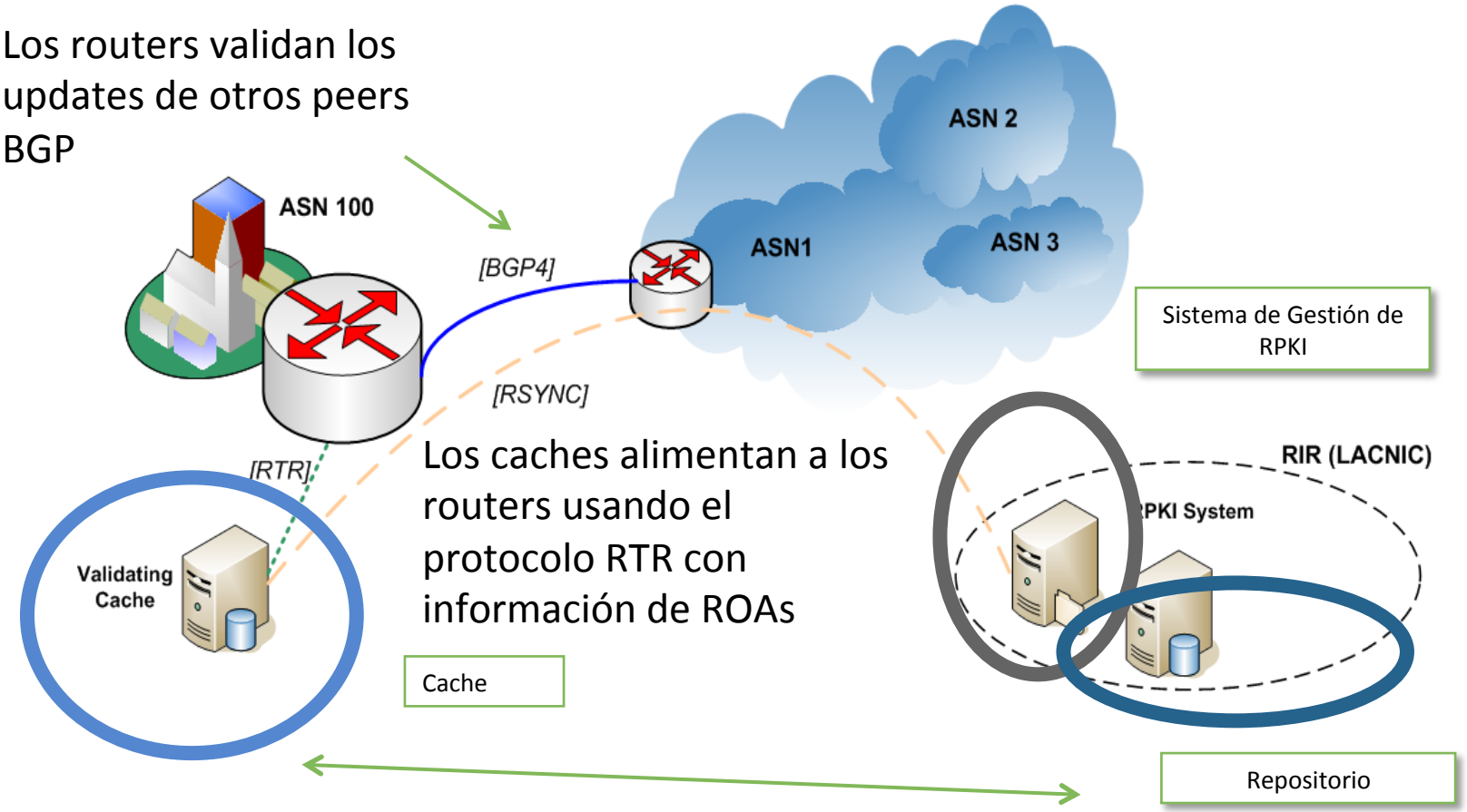
Validación

- Mediante RPKI es posible validar el derecho a uso de un recurso por parte de una organización
- Posibilidades:

- Construcción de filtros para anuncios utilizando BGP (Border Gateway Protocol).
- Construcción de reglas de enrutamiento basadas en la validez criptográfica de los prefijos anunciados
- Firma de información en servicios de Whois o en objetos RPSL (Routing Policy Specification Language).

RPKI en acción

Los routers validan los updates de otros peers BGP



Los caches traen y validan criptográficamente los certificados y ROAs de los repositorios

RPKI en acción (ii)

- El proceso de validación a nivel de la infraestructura de enrutamiento está dividido en dos
  - Validación de los ROAs como objetos firmados
    - Lo realiza el caché validador
  - Validación de la información recibida en los UPDATE de BGP
    - Lo realizan los “bgp speakers” de la red
- Existe un protocolo de comunicación entre caché y routers (RTR) que está definido en la RFC 6810

RPKI en funcionamiento (iii)

- En el caché
  - Se bajan por RSYNC los contenidos de los repositorios RPKI
  - Se validan los certificados y ROAs
    - Criptográficamente (cadena de firmas)
    - Inclusión correcta de recursos
- En los routers
  - Se construye una base de datos con la relación entre prefijos y AS de origen

Validación de Origen

- Los routers arman una base de datos con la información que reciben de los caches
- Esta tabla contiene
  - Prefix, Min length, Max length, Origin-AS
- Aplicando un conjunto de reglas, se asigna un estado de validez a cada UPDATE de BGP
- Los operadores de red pueden usar el atributo “validez” para construir políticas de ruteo
- El estado de validez puede ser:
  - Válido: El AS de origen y el Largo Máximo coinciden con la información del ROA
  - Inválido: La información del ROA no coincide
  - No encontrado: No hay un ROA para el prefijo dado

Validación de Origen

UPDATE 200.0.0.0/9
ORIGIN-AS 20

VALID

- max_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Validación de Origen

UPDATE 200.0.0.0/22
ORIGIN-AS 20

INVALID

[x_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Validación de Origen

UPDATE 200.0.0.0/9
ORIGIN-AS 66

INVALID

[prefix_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Validación de Origen

UPDATE 189.0.0.0/9
ORIGIN-AS 66

NOT FOUND

	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Políticas de Ruteo con Validación de Origen

- Usando el atributo de validez de BGP los operadores de red pueden construir políticas de ruteo
- Por ejemplo:
  - A las rutas con estado “valid” asignarles mayor preferencia que a las rutas con estado “not found”
  - Descartar rutas con estado “invalid”
- MUY IMPORTANTE: RPKI es una fuente de información! Los operadores son libres de usarla como les parezca mejor

Interacción con BGP

- El estado **{valid, invalid, not found}** de un prefijo puede hacerse pesar en la selección de rutas

```
route-map rpki permit 10
match rpki invalid
set local-preference 50

route-map rpki permit 20
match rpki incomplete
set local-preference 100

route-map rpki permit 30
match rpki valid
set local-preference 200
```

Conclusiones

- El sistema de ruteo es uno de los pilares de Internet
  - Sin embargo, aún es vulnerable a ataques y a configuraciones erróneas
- Se ha hecho un gran avance (RPKI, Origin Validation)
- Pero es necesario seguir trabajando
  - Despliegue (Filtrado, RPKI, Origin Validation)
  - Seguimiento de la operación de RPKI: WG SIDRops de la IETF
- Los certificados de recursos y los ROAs son una herramienta para quienes tienen recursos asignados
  - Importante: firmar los recursos y definir los ROAs que especifican los anuncios de rutas

Preguntas?

Muchas gracias…

Autoridad Nacional para la Innovación Gubernamental
innovamos para ti

lacnic