Infraestructura de clave pública para certificación de recursos (*RPKI*)

Arturo Servín – Carlos M. Martínez

Agenda

- Asignación de recursos en Internet
  - Relación entre registros y usuarios de los recursos
- Enrutamiento en Internet
- Secuestro de rutas
- Certificación de recursos
- ROAs
- Referencias

¿Qué es LACNIC?

- LACNIC administra los recursos de numeración de Internet para América Latina y parte del Caribe asegurando que todas las partes interesadas tengan un acceso equitativo a esos recursos, trabajando basados en el espíritu de servicio a la comunidad

- Es una organización basada en Membresía, sin fines de lucro, establecida jurídicamente en Uruguay y reconocida como Organismo Internacional por el estado uruguayo

¿Qué no es LACNIC?

- Proveedor de servicios de Internet
- Entidad reguladora
  - La regulación del mercado de telecomunicaciones es competencia de los gobiernos
- Controlador de contenidos de páginas de Internet
- Policía de Internet
  - LACNIC no ataca redes
  - LACNIC no manda spam ☺
- Registro de nombres de dominios
  - Pero si LACNIC es la raíz del espacio reverso (in-addr.arpa e ip6.arpa)

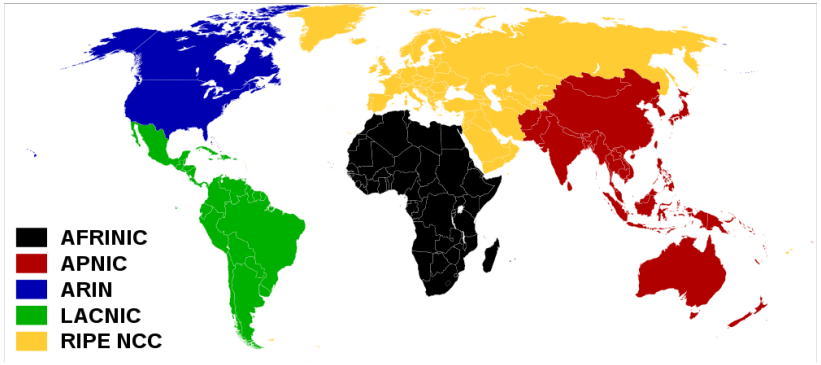
¿Cuáles Recursos de Numeración de Internet?

- Recursos fundamentales para el crecimiento y despliegue de Internet:
  - Direcciones IPv4
  - Direcciones IPv6
  - Números de Sistema Autónomo
- Servicios
  - Directorio Whois
  - DNS inverso
  - RPKI

Registros de Internet Regionales (RIR)

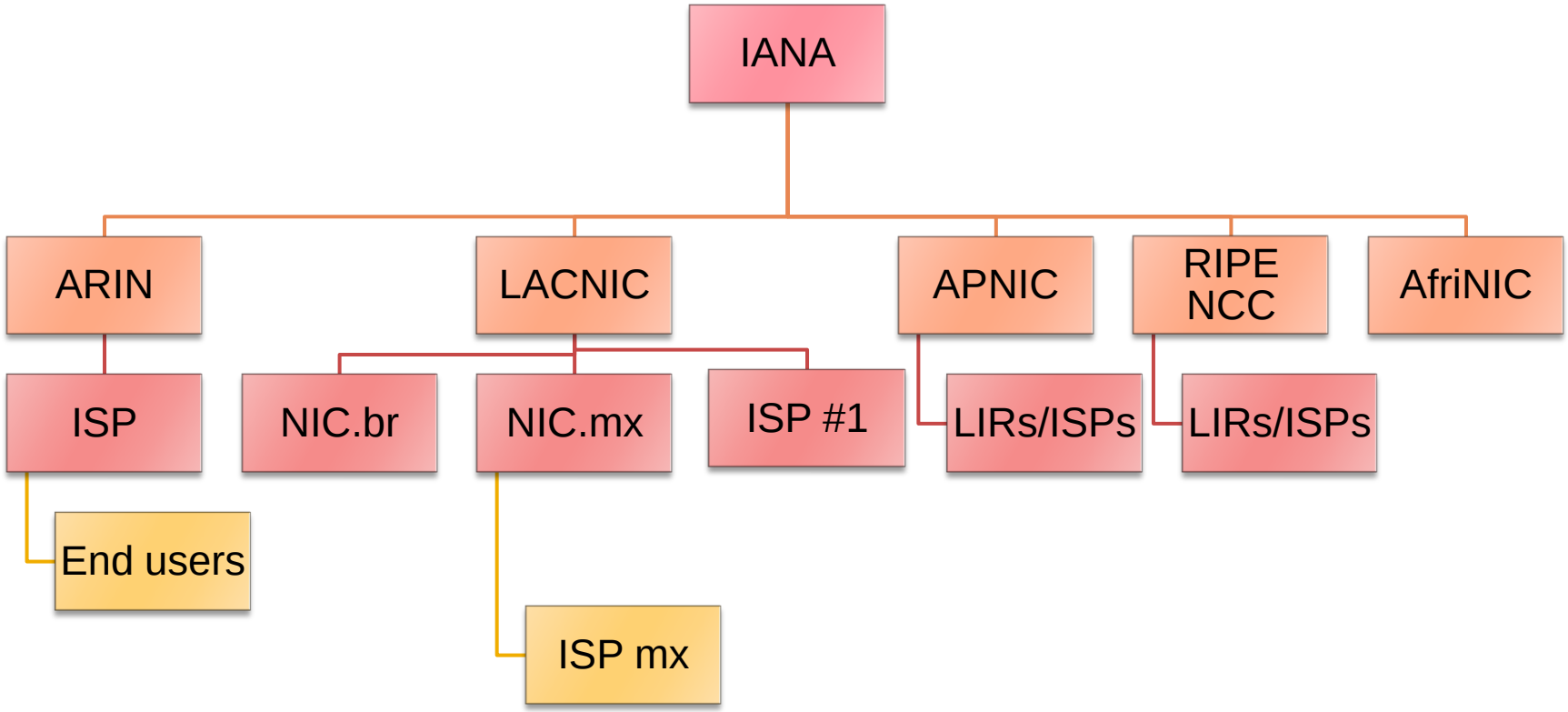
Gestión de recursos de numeración en Internet (i)

- Recursos
  - Direcciones IPv4
  - Direcciones IPv6
  - Sistemas autónomos
    - 16 y 32 bits



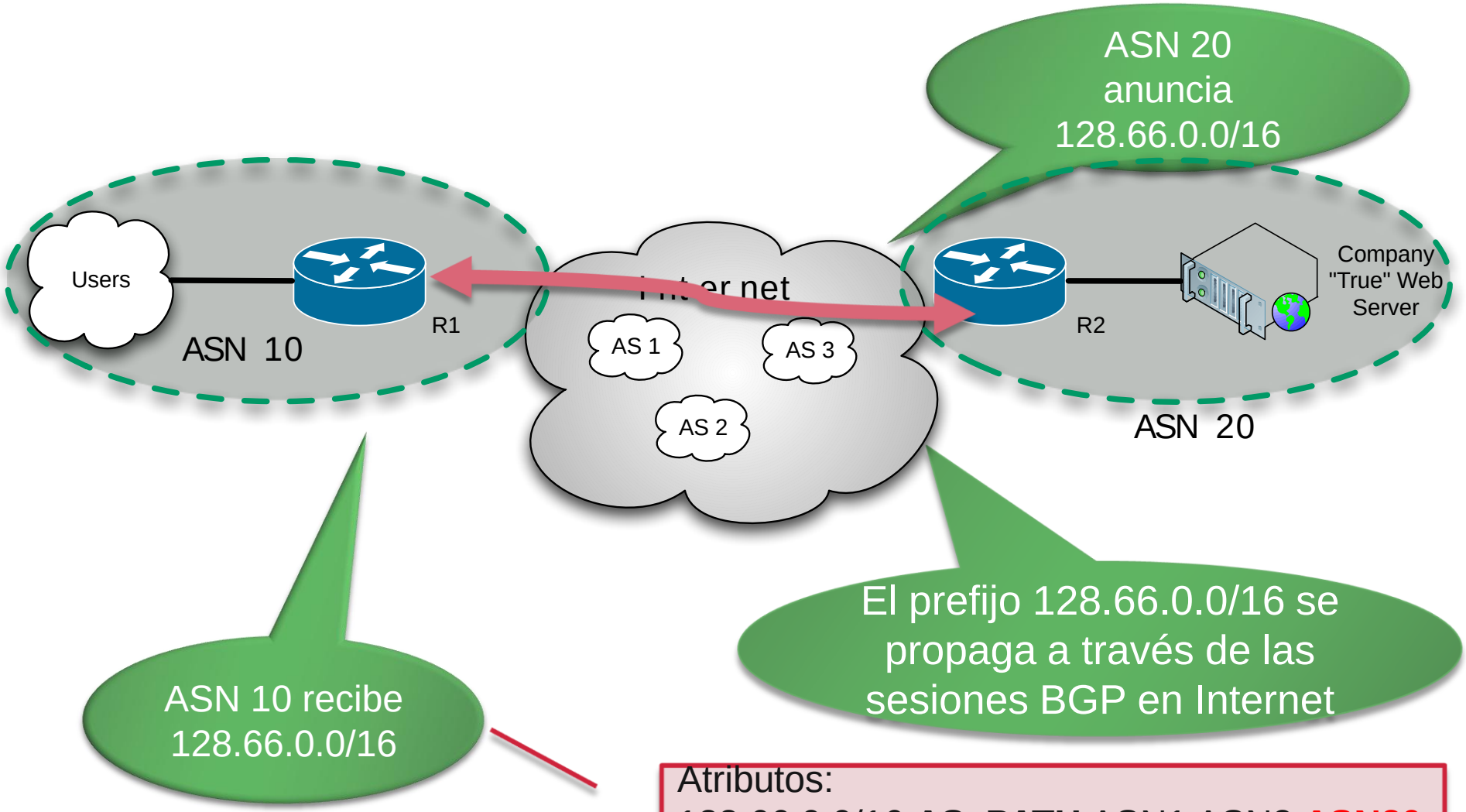
- Documento fundacional: RFC 2050
  - "*IP Registry Allocation Guidelines*"
- Cada RIR es **fuente autoritativa de información sobre la relación "usuario" <-> "recurso"**
  - Cada RIR opera su base de datos de registro

Gestión de recursos de numeración en Internet



- Cada RIR es **fuente autoritativa de información sobre la relación "usuario" <-> "recurso"**

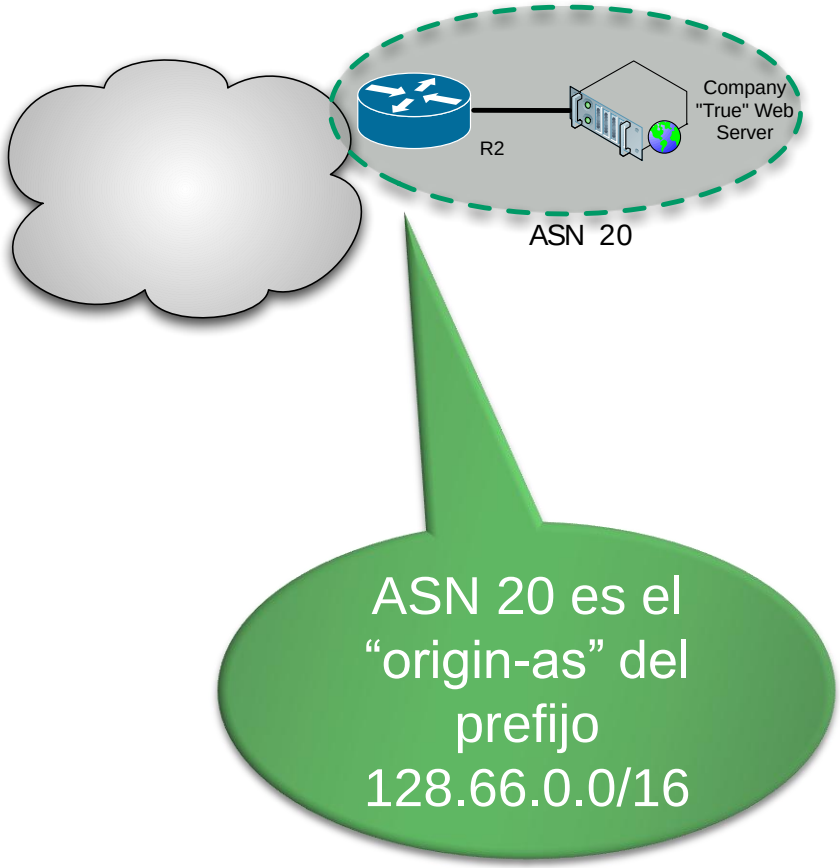
Enrutamiento en Internet en un slide



Atributos:
128.66.0.0/16 **AS_PATH** ASN1 ASN3 **ASN20**

Enrutamiento en Internet (ii)

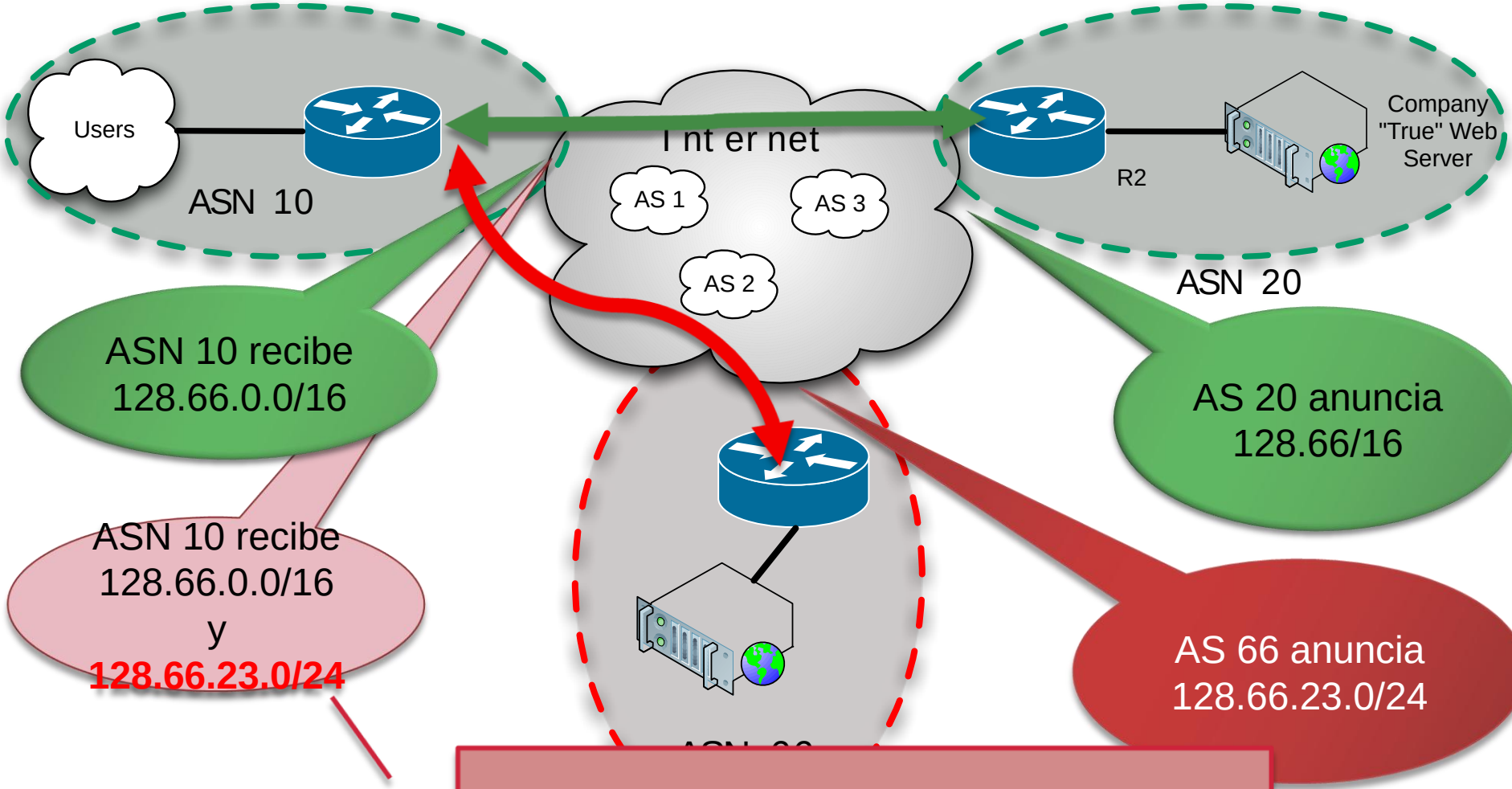
- BGP elije rutas de acuerdo a un **algoritmo de decisión** y a los valores de los **atributos**
- AS_PATH y AS de origen
  - AS_PATH es la lista de sistemas autónomos recorridos por un UPDATE dado
  - Incluye el AS que origina el anuncio (“origin-as”)



Secuestro de rutas

- Cuando un participante en el routing en Internet anuncia un prefijo que no esta autorizado a anunciar se produce un "*secuestro de ruta*" (*route hijacking)*
- Malicioso u causado por error operacionales
- Casos más conocidos:
  - Pakistan Telecom vs. You Tube (2008)
  - China Telecom (2010)
  - Google en Europa del este (varios AS, 2010)
  - **Casos en nuestra región (enero/febrero de 2011)**

Secuestro de rutas (ii)



Resource PKI (i)

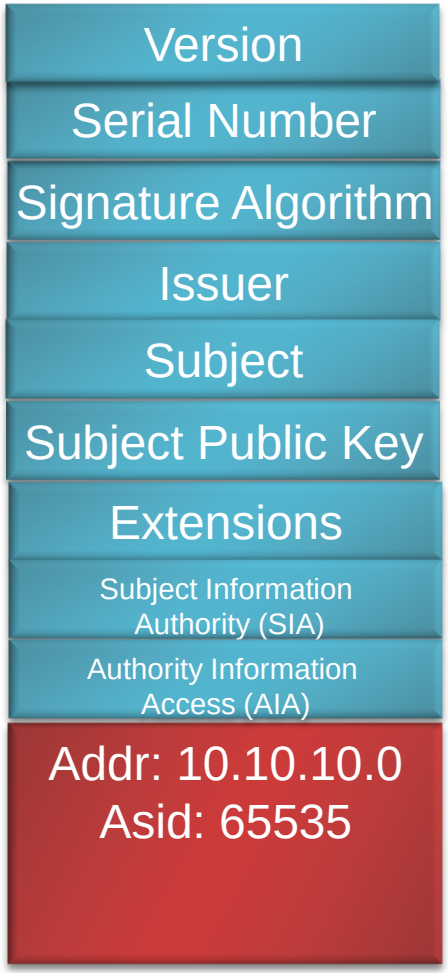
- Objetivos:
  - Emitir certificaciones digitales de autorización de uso de recursos
  - Proveer una técnica para validar la autoridad asociada a un anuncio BGP y validar el "**origen de una ruta**"
- El emisor de la información de ruta "**firma**" la información de "AS de origen"
- Para validar certificados e información de enrutamiento se utilizan:
  - Las propiedades del cifrado de clave pública (certificados)
  - Las propiedades de los bloques CIDR

Resource PKI (ii)

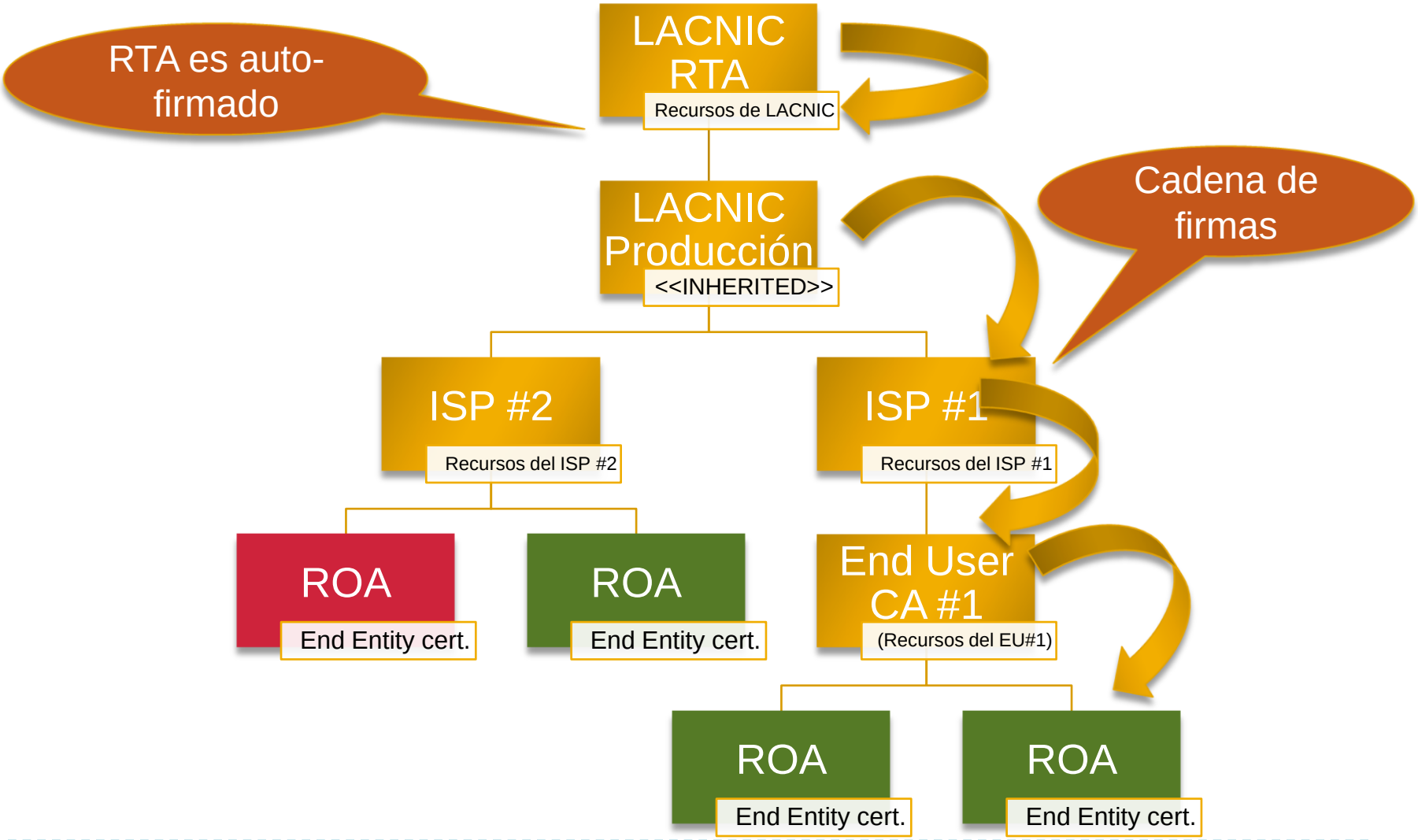
- Certificación de recursos
  - Uso de certificados X.509 v3
  - Uso de extensiones RFC 3779 en certificados que permiten representar recursos de Internet (direcciones v4/v6, ASNs)
  - Mecanismo de **validación de prefijos**
- Esfuerzo de estandarización:
  - SIDR working group en IETF
- Esfuerzo de implementación
  - RIRs

Certificados con extensiones RFC 3779

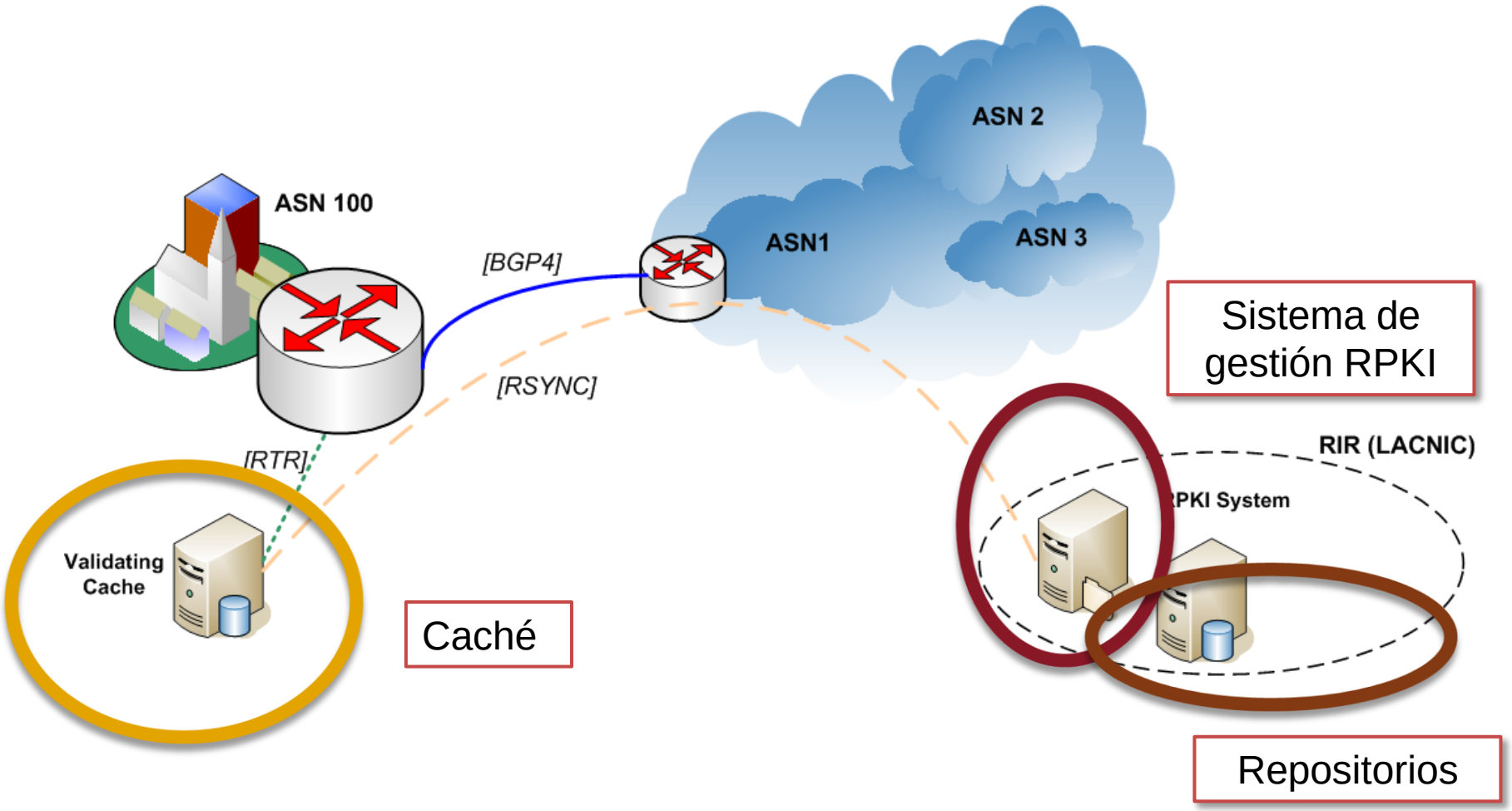
- Sección “IP Delegation”
  - Valor especial “INHERITED”
- Sección “AS Delegation”
  - Valor especial “INHERITED”
- Proceso de validación
  - Se validan las **cadenas de firmas**
  - Se valida la inclusión de recursos (CIDR) de hijos hacia padres



Estructura de la RPKI



Resource PKI (iii)



Route Origin Authorizations: ROAs (i)

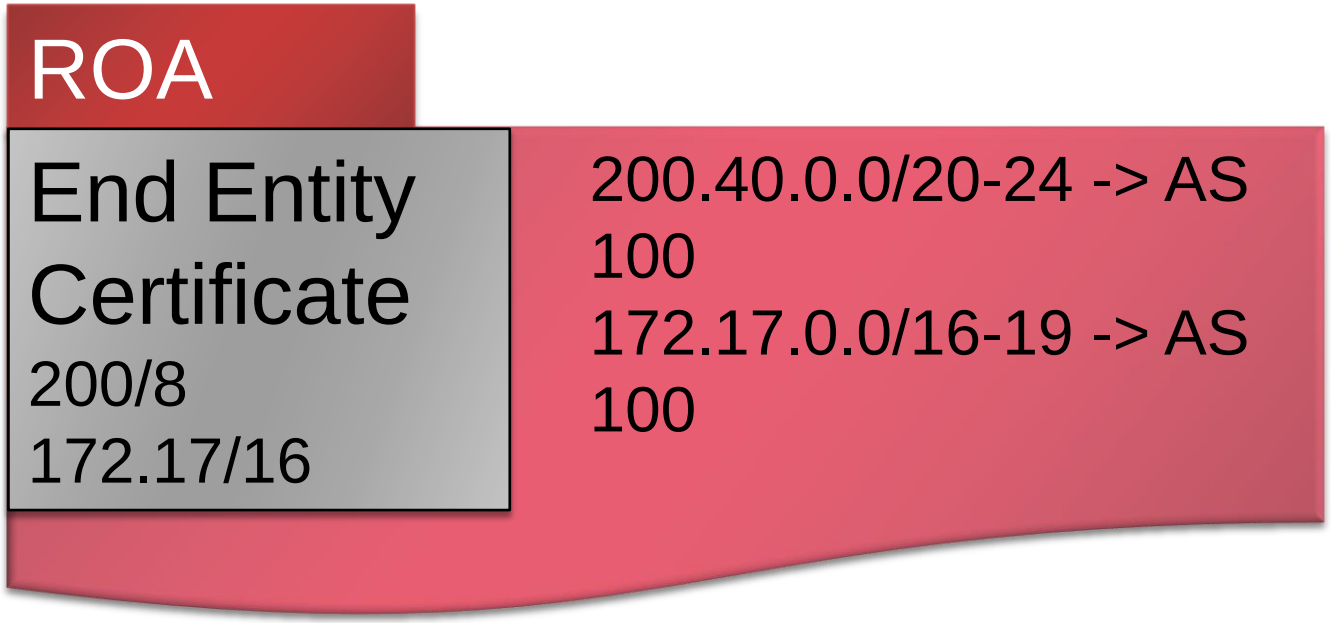
- Un ROA (simplificado) contiene esta información:

Prefijo	Largo_Máximo	AS Origen	Valido_Desde	Valido_Hasta
200.40.0.0/17	20	6057	2011-01-02	2012-01-01
200.3.12.0/22	24	28000	2011-01-07	2012-01-06

- Este ROA afirma que:
  - "*El prefijo 200.40.0.0/17 será anunciado por el sistema autónomo 6057 y podrá ser fraccionado en prefijos de hasta 20 bits de largo. Esto será valido desde el 2 de enero de 2011 hasta el 1 de enero de 2012*"
- Además
  - El ROA contiene el material criptográfico que permite **verificar** la validez de esta información contra la RPKI

ROAs (iii)

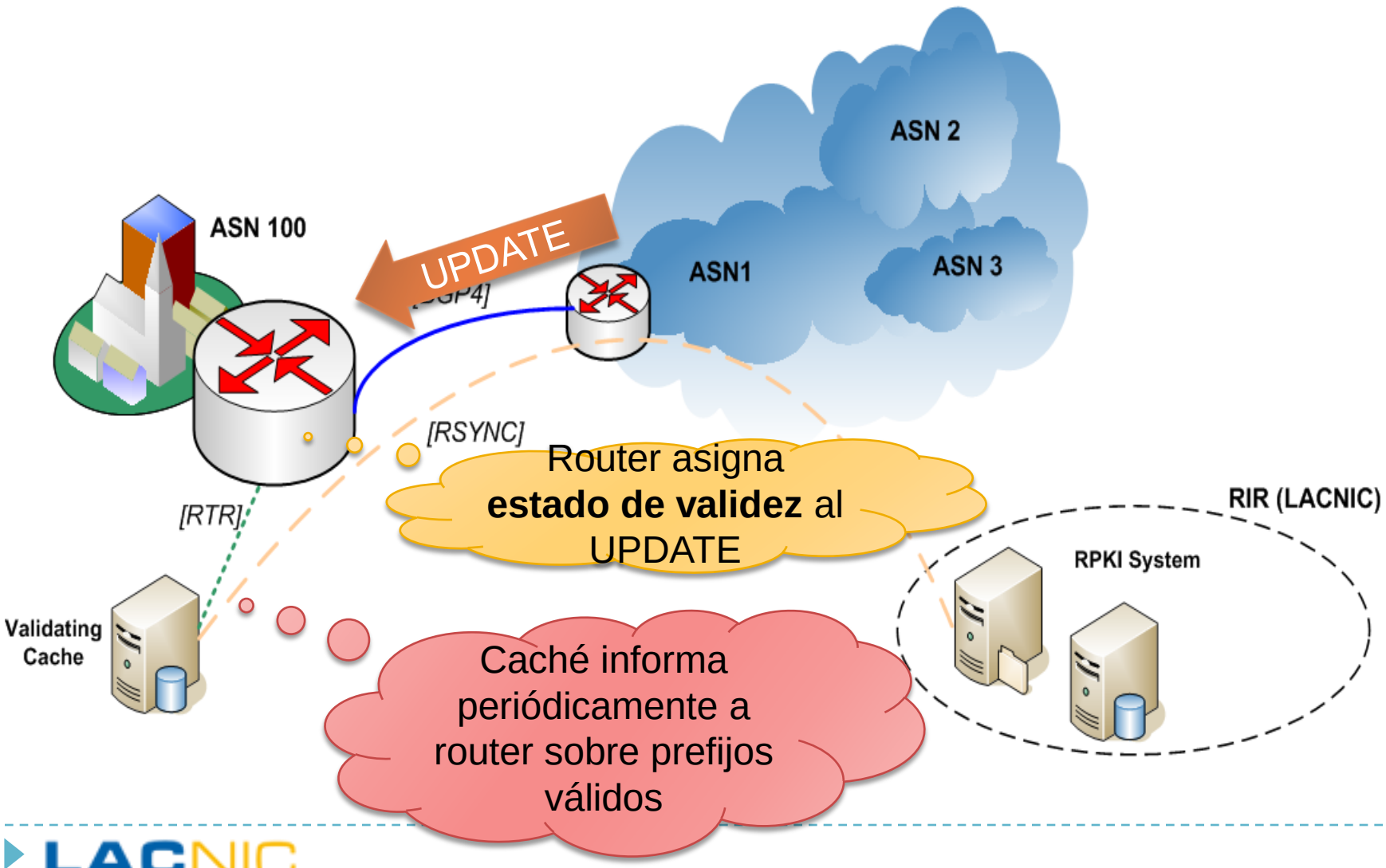
- Los ROA contienen
  - Un certificado End Entity con recursos
  - Una lista de “route origin attestations”



ROAs (iii) - Validación

- El proceso de validación de los ROAs involucra:
  - La validación criptográfica de los certificados end entity (EE) que están contenidos dentro de cada ROA
    - Certificado de recursos de la organización
    - Certificado de recursos del RIR
  - La validación CIDR de los recursos listados en el EE respecto de los recursos listados en el certificado emisor
    - Inclusión en los recursos listados en el EE
    - Inclusión en los recursos del certificado de la organización
  - La verificación de que los prefijos listados en los route origin attestations están incluidos en los prefijos listados en los certificados end entity de cada ROA

RPKI en funcionamiento



Interación con BGP

- Los routers construyen una tabla con la información que reciben del caché
- Esa tabla contiene
  - Prefijo
  - Largo mínimo
  - Largo máximo
  - AS de origen
- En funcion de un conjunto de reglas se le asigna a cada prefijo un **estado de validez**
  - {VALID, INVALID, NOT_FOUND}

Interacción con BGP (ii)

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 “UPDATE pfx” **no** encuentra ninguna entrada que lo cubra en la BdeD -> “**not found**”
- Si el “UPDATE pfx” si encuentra al menos una entrada que lo cubra en la BdeD y además el AS de origen del “UPDATE pfx” coincide con uno de ellos -> “**valid**”
- En el caso anterior, si **no** coincide ningun AS de origen -> “**invalid**”

Interacción con BGP (iii)

UPDATE
200.0.0.0/9
ORIGIN-AS 66

INVALID

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

- Si el “UPDATE pfx” **no** encuentra ninguna entrada que lo cubra en la BdeD -> “**not found**”
- Si el “UPDATE pfx” si encuentra al menos una entrada que lo cubra en la BdeD y además el AS de origen del “UPDATE pfx” coincide con uno de ellos -> “**valid**”
- En el caso anterior, si **no** coincide ningun AS de origen -> “**invalid**”

Estado actual de RPKI en LACNIC

- RPKI en modo “hosted” está en producción desde el 1-1-2011
  - http://rpki.lacnic.net
- ¿Quienes pueden utilizarlo?
  - Todos los miembros de LACNIC a través de sus contactos técnicos y administrativos
- ¿Que funcionalidades están disponibles?
  - Creación del certificado de recursos
  - Creación, modificación y revocación de ROAs
- ¿Donde reside el repositorio de LACNIC?
  - rsync://repository.lacnic.net/rpki/

Referencias

- RPKI LACNIC: http://rpki.lacnic.net
- Estadísticas RPKI: http://www.labs.lacnic.net/~rpki
- RPKI Demo:
  - Acceso: http://rpkidemo.labs.lacnic.net
  - Documento de uso: http://www.labs.lacnic.net/drupal/acceso-al-demo-rpki
- IETF SIDR Working Group: http://tools.ietf.org/wg/sidr/
- RIPE Repository Validator:
  - http://labs.ripe.net/Members/agowland/ripe-ncc-validator-for-resource-certification

¡Muchas gracias por su atención!

Nombre Autor (nombre @ lacnic.net)