



# Certificación de Recursos en LACNIC.

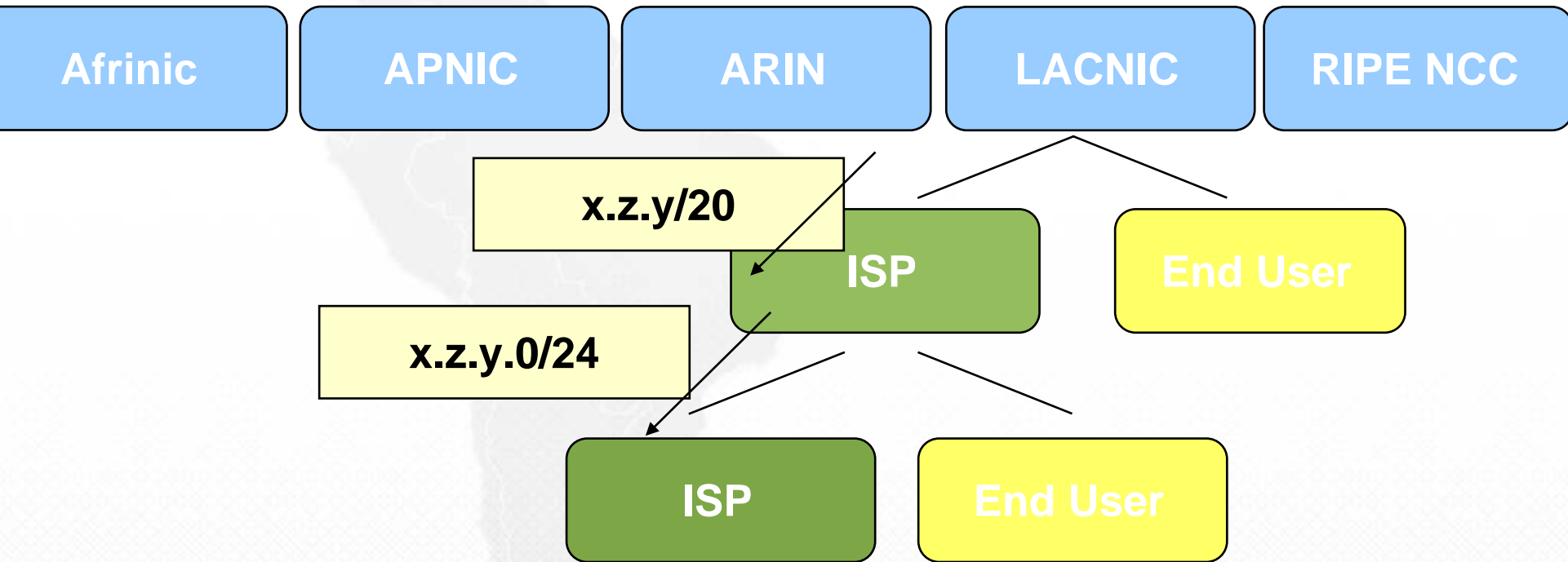
Roque Gagliano

[roque@lacnic.net](mailto:roque@lacnic.net)

LACNIC



# Distribución de direcciones en Internet.





# ¿Cuáles son los problemas de seguridad en Routing?

**El grupo RPSEC del IETF estudió las amenazas genéricas de los protocolos de routing y particularmente identificó la reclamación ilegítima de recursos (overclaiming).**

**El problema es cómo transpasamos el derecho de uso de un recurso (direcciones o ASNs).**



## El mundo que conocemos:

Hoy un ISP recibe un bloque de direcciones por parte de LACNIC, llena la información correspondiente en el whois y registra sus reversos de DNS.

Cada ISP indica a su upstream cuales son los prefijos que va a anunciar a través de diferentes mecanismos, como por ejemplos:

- ◆ **A través de formulario web o planilla de datos.**
- ◆ **Utilizando Registros de Routing (IRR).**



# Ejemplo: Sprint (ASN 1239)

## BGP Request

To request initiation or modification of Sprint BGP services, please fill out the form. Please see the [BGP Routing Policy page](#) before filling out this form.

Note that you can CC yourself on this mail, so that you may receive a copy of you

FROM:  (Your E-Mail) \*  
TO: SprintLink Support Team  
CC:  (up to 1 email add  
SUBJECT: BGP4 Request

### 1. CONTACT INFORMATION:

Company Name:   
Contact Name:   
Contact's Phone#:  \*  
Contact Hours:

### 2. YOUR CIRCUIT: ( only ONE is required ) \*

[Private Line\(s\) #:](#)  \*

-OR-

[Network Address:](#)  \* (e.g. "4xxxxxxx")

### 3. Serial IP Addresses:

Provider	IP Address
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

## 5. YOUR SESSION:

Multi-Homed:

Yes \*  No

\* Special Customer arrangements are required for non-multihomed customers.

YOUR AS#:

\*

Routes Received from Sprint: \*\*

- No Routes  
 Partial Routes (Sprint routes and Sprint customer routes)  
 Full routes

\*\* Sprint provides three options for BGP4 routes:

Option	# Routes	CPU/Mem. Requirement
No Routes	1 (default)	2500/3000 or equivalent (2MB RAM)
Partial Routes	- 80,000	3600/7200 or equivalent with 128+ MB RAM
Full Routes	- 200,000	7500/12000 or equivalent with 256+ MB RAM (512+ MB recommended)

**NOTE:** Customers are required to create route filters on their side to prevent invalid announcements received from customers to maintain network stability. Sprint also reserves the right to choose the most appropriate customer basis. The decision criteria are based on router capacity, availability and maintenance. Please note that we will construct an access list to fit your needs.

Route Filter Type:

IP Blocks Permitted:

Prefix

Subnet mask

Please select   
Please select   
Please select   
Please select   
Please select   
Please select   
Please select   
Please select   
Please select   
Please select

Default Route?\*

Yes  No

\* A default route provides backup in the event of failure of other static links you may have to other providers. A default route is not permitted on a router with less than 16 Mb.

Load Balancing?

Yes  No

[Loopback Address:](#)

(Required if load balancing chosen)



## ¿Qué es lo que el carrier hace luego?

- ◆ El Carrier debería verificar el derecho a uso por parte de sus clientes a los recursos que solicita rutear y configurar filtros ( prefix-lists ) adecuados en sus interfaces a sus clientes.
- ◆ ¿Cuáles son la fuentes de información que cuenta?
  - ◆ **Whois de los RIRs: No está pensado para información de routing, información no es firmado, muchas veces la información básica (nombre de entidad) no es actualizada.**
  - ◆ **Whois de los IRRs: No hay (en general) buenos mecanismos de autenticación para introducir la información, información no es firmada.**



## Secuestro de direcciones:

- ◆ Ocurre todo el tiempo en Internet, en especial de direcciones no distribuidas (281 el 28/05/2009).
- ◆ El problema es cuando se secuestran prefijos en operación, sea por error operacional o por actividad maliciosa.
- ◆ Particularmente es dañino cuando el ataque se hace con prefijos más específicos.
- ◆ Un ejemplo muy divulgado es el ataque a YouTube que ocurrió en Febrero 2008 por parte de Pakistan Telecom:

<http://www.ripe.net/news/study-youtube-hijacking.html>

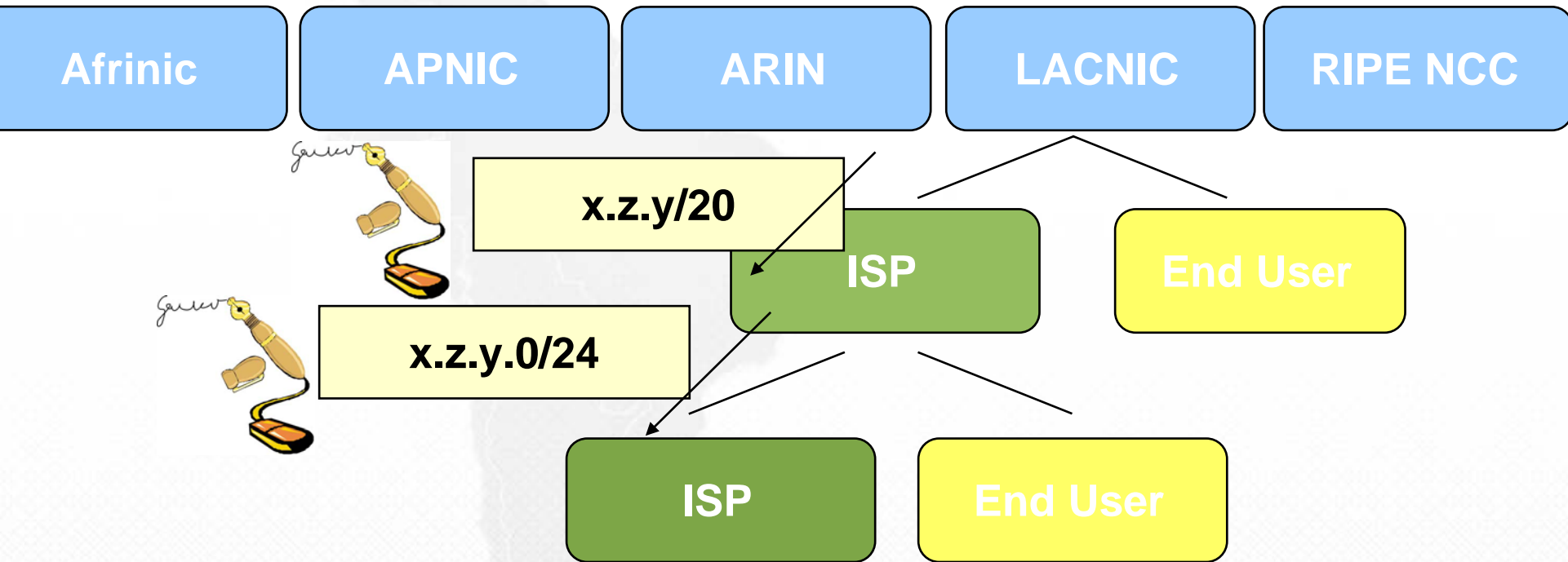


## Certificación de Recursos.

- ◆ El proyecto de certificación de recursos es un esfuerzo para brindar la infraestructura para la firma digital del transpaso del derecho de uso de los recursos de Internet.
- ◆ El proyecto de Certificación de Recursos implementa un Infraestructura de Clave Pública (PKI), por lo que hereda el nombre RPKI (Resource Public Key Infrastructure).
- ◆ La certificación de recursos no brinda seguridad en sí misma, pero establece la infraestructura para que los ISPs puedan desarrollar herramientas y metodologías mejorar la seguridad del routing entre dominios.



# Certificación de Recursos.





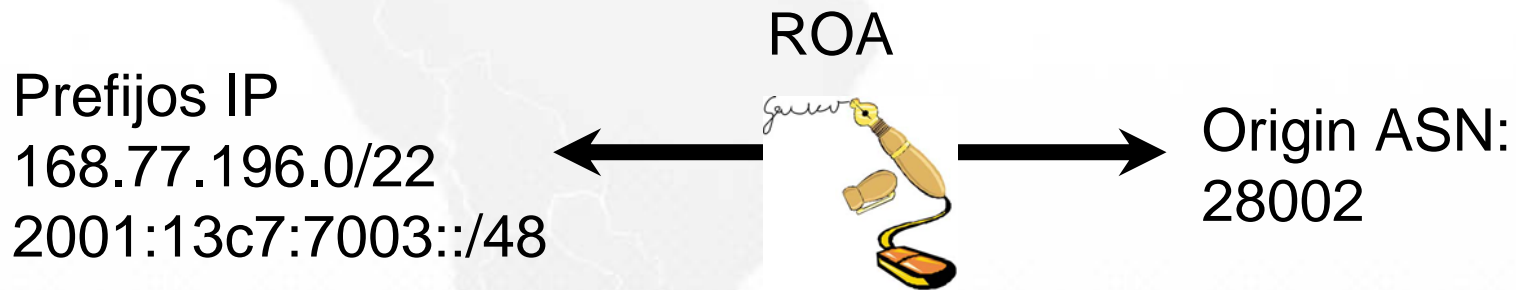
## Certificación de Recursos.

- ◆ Para cada distribución o asignación de recursos LACNIC va a entregar un certificado digital X509v3 que incluye la lista de recursos y la firma digital utilizando la clave privada de LACNIC.
- ◆ La estandarización se hace en el WG SIDR del IETF.
- ◆ Los certificados dentro del RPKI tienen tres características importantes:
  - ◆ **La identidad del receptor (subject) no es relevante. RPKI no tiene como objetivo identificación.**
  - ◆ **Los certificados emitos por LACNIC permiten la generación de sub-CAs por los ISPs (CA bit=1).**
  - ◆ **Se implementan extensiones para representar direcciones IP y ASN en un certificado x509v3.**



## ¿Qué hace un ISP con los certificados?

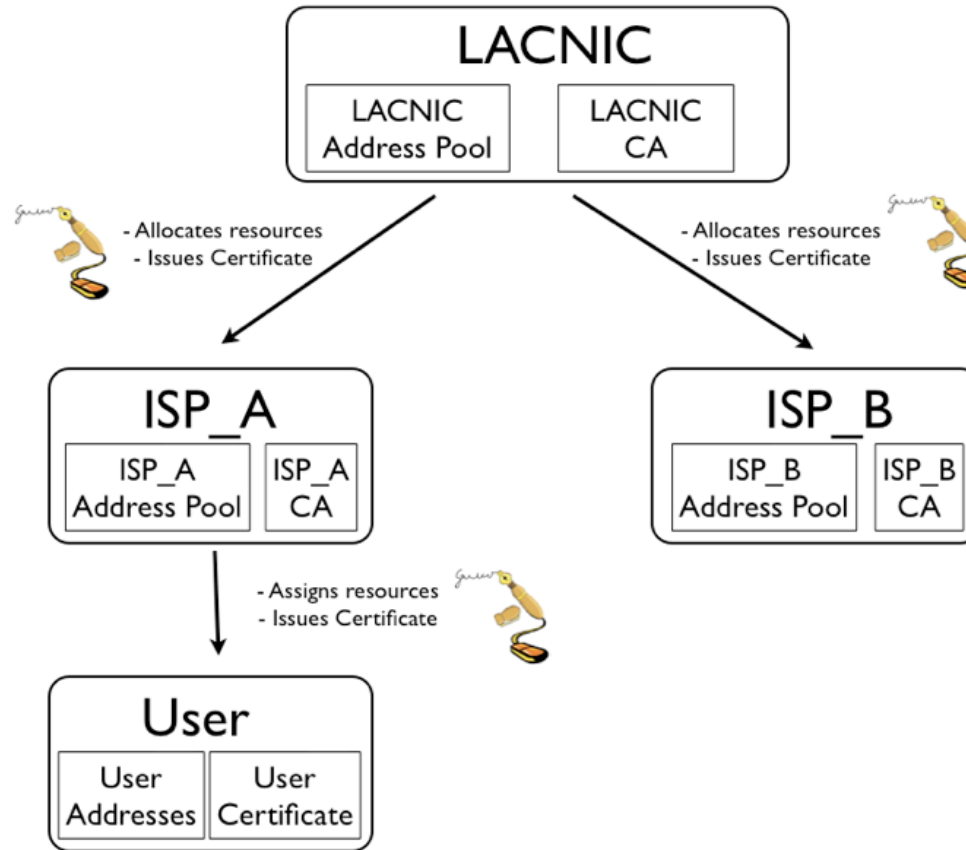
- ◆ El ISP va a poder tomar la clave privada de sus certificados y firmar material criptográfico, en especial un ROA (Route Origin Authorizations):



- ◆ Los certificados y todo el material criptográfico se almacena en repositorios de acceso públicos.
- ◆ Estos pueden ser usados para verificar derecho de uso de un prefijo IP por determinado ASN de Origen o generar filtros automáticamente.



# Infraestructura RPKI:





## Servicios a Brindar en el RPKI por una CA:

- ◆ **Emisión de certificados hijos cuando existen cambios en la base de registro o a demanda de un usuario.**
- ◆ **Revocación de certificados hijos en forma centralizada o a demanda de un usuario.**
- ◆ **Emisión periódica de CRL para certificado del CA.**
- ◆ **Publicación de Certificado del CA y de certificados hijos en repositorio público (rsync).**



## Servicios de una entidad final

- ◆ **Los miembros (ej. ISP) que reciben sus certificados CA por parte de una CA madre necesitarán los siguientes servicios:**
  - ◆ **Administrar su CA y dar los mismos servicios anterior para sus CA hijas (por ejemplo ISP emite certificado para Usuario Final u otro ISP).**
  - ◆ **Solicitar emisión o revocación de certificados a la CA madre en caso de ser necesario.**
  - ◆ **Generar material criptográfico (Ej. ROAs) para sus recursos.**
  - ◆ **Mantener un repositorio público.**



## Modelos de Servicios:

- ◆ **LACNIC está pensando en dos modelos de servicio:**
  - ◆ **Delegado:** En este caso LACNIC sólo implementaría los servicios básicos, el miembro implementa su propia CA. El ISP almacena su clave privada y gestiona su repositorio público.
  - ◆ **Alojado:** En esta caso LACNIC implementa para el miembro tanto los servicios básicos como los servicios de entidad final a través de, por ejemplo, una interfaz web. En este caso la clave privada del miembro de LACNIC es alojada en el sistema de gestión de LACNIC. Creemos que en esta familia estarán la gran mayoría de los miembros de LACNIC.



## Modelo Delegado (ej. NIR)



En el modelo delegado la CA madre (LACNIC) y la hija (NIR) implementan las mismas interfaces. Las claves privadas residen en el dominio de cada CA. La comunicación se realiza a través del protocolo "TOP/DOWN".



# Protocolo "TOP/DOWN".

- ◆ Mensajería basados en XML sobre HTTPS.
- ◆ Autenticación de dos vías ("Two-ways") basada en TLS con certificados de Business CA.
- ◆ El contenido XML es a su vez firmado utilizando un "blob" CMS, donde la misma clave que TLS(que brinda la encriptación) puede ser utilizada.

Mensaje  
HTTPS:  
Transporte, autenticación  
y  
confidencialidad

Blob CMS: Firma digital  
asegura integridad

Mensajería  
XML

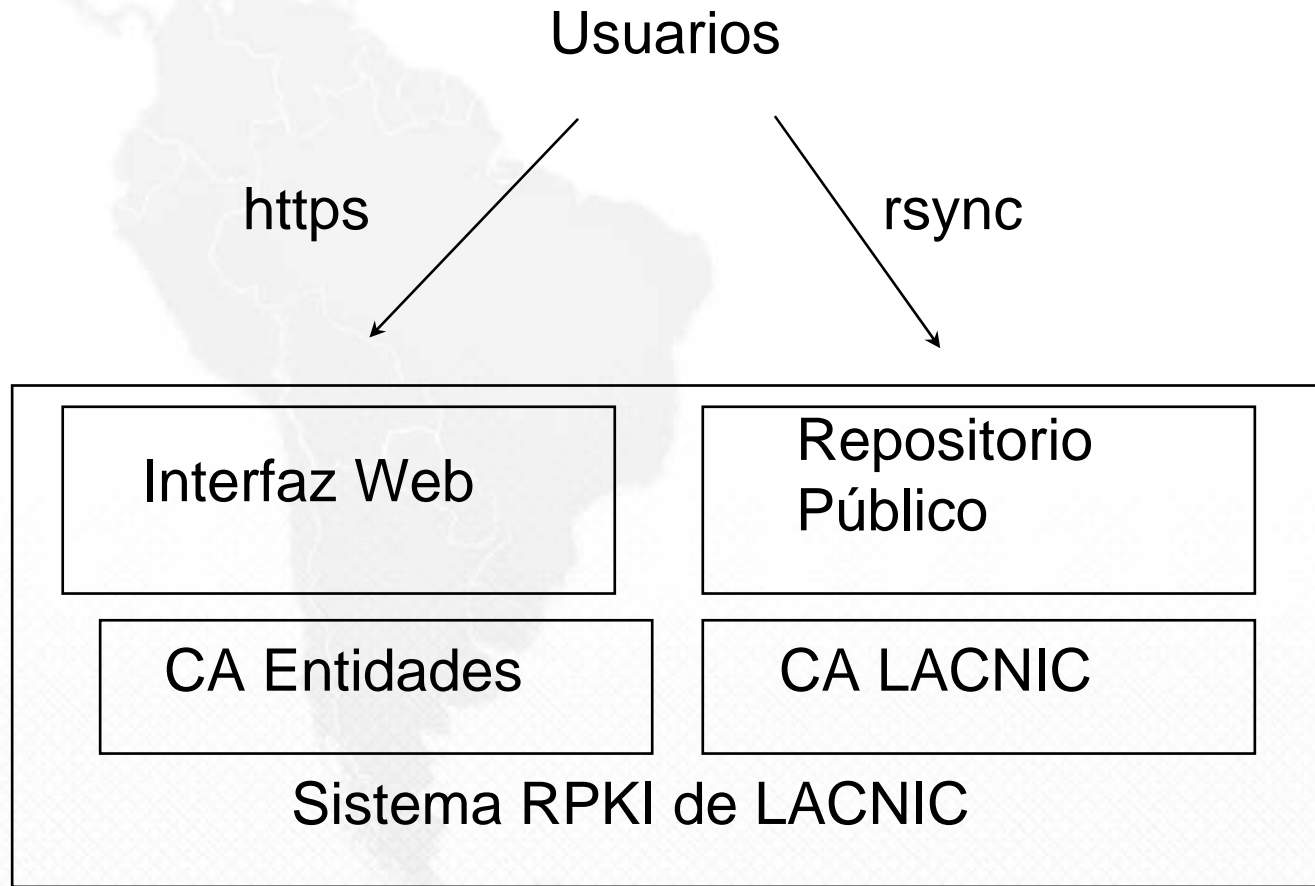


## Modelo Alojado:

- ◆ **En este caso LACNIC va a almacenar el CA del miembro brindando una interfaz (en principio web) para poder realizar las tareas:**
  - ◆ Solicitar emitir Certificado propio/generar nuevas claves.
  - ◆ Solicitar revocar Certificado propio.
  - ◆ Emitir material Firmado.
  - ◆ Gestionar Repositorio Público, descargar todo el material.



# Modelo Alojado:





## Herramientas de Validación.

- ◆ Necesarias para validar los ROAs.
- ◆ Lo que hacen es recorrer la jerarquía RPKI de abajo hacia arriba.
- ◆ Herramienta ya disponible:
  - ◆ **RIPE: Tiene Herramienta disponible con fuentes, sólo para quienes participan de su programa beta.**



## Desarrollo en LACNIC:

- ◆ LACNIC ha comenzado su desarrollo con los siguientes principios:
  - ◆ Comenzaremos con el servicio delegado.
  - ◆ Utilizaremos tecnologías JEE, en particular basados en la implementación de RIPE NCC.
  - ◆ Utilizaremos técnicas de gestión ágil de proyectos.
  - ◆ Implementación delegada a continuación.
  - ◆ Clave del CA de LACNIC y de los servicios alojados serán alojadas en HSM con FIPS 4 cuando puesto en producción.
- ◆ LACNIC planea tener una implementación beta para finales del 2009.
- ◆ Vamos a necesitar TESTERS!.



## Tareas Realizadas por LACNIC:

- ◆ Recursos Dedicados Full-Time.
- ◆ Contratación de consultores sobre temas específicos JEE.
- ◆ Capacitación en Gestión Ágil (scrum).
- ◆ Difusión:
  - ◆ Presentación en LACNIC XI
  - ◆ Presentación en GTER 12.
  - ◆ Presentación en reunión de CITEC.
  - ◆ Próximamente: página web con información sobre RPKI.



**MUCHAS GRACIAS**

**Preguntas ????**