LACNIC

Latin American and **Caribbean** Internet Addresses Registry
Registro de Direcciones de Internet para **América Latina** y **Caribe**
Registro de Endereços da Internet para **América Latina** e **Caribe**

Certificación de Recursos Internet

Ricardo Patara

¿Qué es?

PKI - "*Public Key Certificate Infrastructure*".

Cada certificado indica la "autenticidad" acerca de alguna información.

Contiene "llave pública"

Firmado y asignado por una entidad "confiable" (CA - *Certificate Authority*)

¿Qué es?

- **Certificado de Recursos, también conocida como RPKI**
- **Una PKI como otras:**
  - **Certificado de llaves públicas, firmado por una CA y indicada autoridad acerca de alguna información**
  - **Pero, tiene algunas peculiaridades:**
    - **Extensión para Recursos Internet (RFC 3779).**
    - **No autentica nombre/sujeto**

¿Qué es?

- RPKI
  - RFC 3779: Listado de IP (v4, v6) y ASN.
  - Certifica solamente “derecho de uso” de Recursos Internet
    - No puede ser utilizado para identificar/autenticar la identifidad del “sujeto” del certificado.
      - *Implicaciones legales. Fuera del escopo*

¿Cual es el problema?

- Actualmente hay pocas formas de evitar uso no autorizado de bloque IP (uso de bloque asignado a otros)
- Información de registro ni siempre actualizada con frecuencia
- Información en los Registros de Rutas Internet (IRR), no siempre "confiables"

¿Cual es el problema?

- Hay casos bien conocidos de incidentes de “secuestros de trafico”.
- Ha sido demostrado con éxito que el “man in de middle” en el sistema de rutas, sin que las partes perciban.
- Con el agotamiento inminente del IPv4, muy probable que ocurra “reutilización” de bloques IPv4. La demostración del “derecho de uso” pasa a ser muy importante

¿Cual es la propuesta?

- **Principal motivación: aumentar la seguridad del sistema de rutas**
- **RPKI como un mecanismos para una infra estructura más segura**
- **Atestado de "derecho de uso"**
- **"Objectos firmados" autorizando el anuncio de bloques IPs.**

¿Cual es la propuesta?

X.509 Certificate

Unique ID

CA bit: on

AIA, SIA

Public key

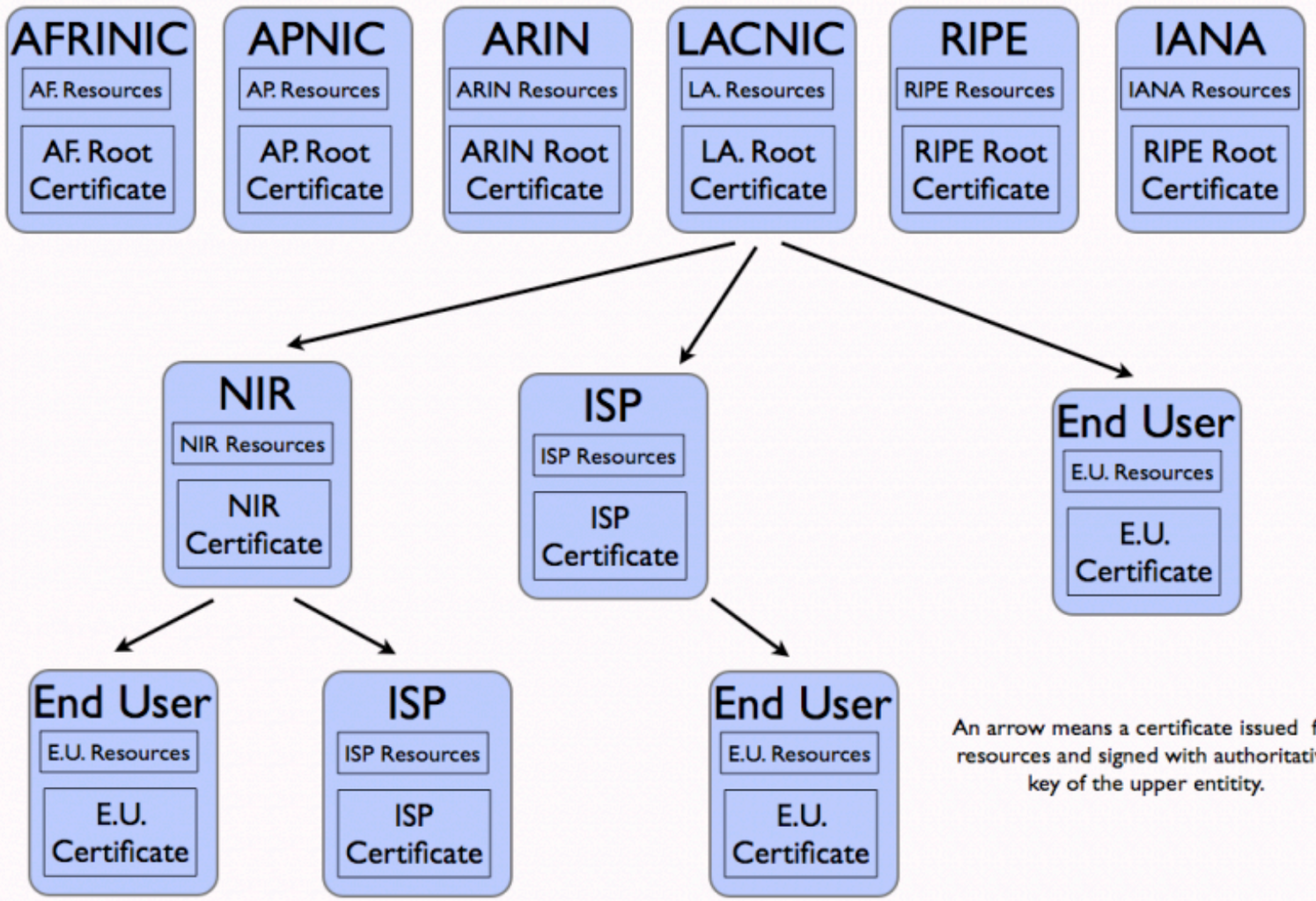
Resources

Digital signature

¿Cual es la propuesta?

- Asignación/distribución de recursos siguida por emisión de certificado
- Cada Registro (RIR, NIR, ISP) actual como un CA
- Repositorio público de certificados y objetos firmados.
- Sistemas delegados e hospedados

¿Cual es la propuesta?



Operación

- **Entidad con el derecho de uso de un recurso**
  - **Emite un certificado para un fin especifico (*end entity)*, con listado de bloques para los cuales se tiene derecho de uso. Firmado por certificado CA.**
    - **Utiliza llave privada, cuya llave par publica figura en el certificado, para firmar "Objetos de Autorización" (qué ASN puede anunciar ciertos bloques IP)**

Operación

- Objetos firmados publicados en repositorios públicos
- Proveedores pueden hacer uso de dicho objeto para determinar derecho de anunciar y usar las IPs indicadas. Con eso, toman decisión de aceptar o no dicho anuncio de ruta.
- Proceso de verificación
  - Objeto firmado con referencia a certificado que lo firmo.
  - Cada certificado tiene referencia a los certificados “superiores”
  - Se sigue “cadena” hasta punto de confianza

Formalización

- IETF (Internet Engineering Task Force)
  - SIDR (Secure InterDomain Routing) Working Group
  - Arquitectura, profile de los certificados, Política de Certificados, TA, objetos de autorización de rutas.

Desarrollo

- RPKI es una estructura básica
- Herramientas y mecanismos necesitan ser implementados para la seguridad del sistema de rutas.
- ISPs a usar dicho sistema y herramientas
- Propuesta bastante reciente de fabricantes para toma de decisión de rutas basado en RPKI

Desarrollo

- **RIRs como promotores de la tecnología**
  - **APNIC con un sistema en producción/operacional**
  - **RIPE y ARIN con sistemas beta.**

- **LACNIC, involucrado en el proceso de estandarización desde su inicio. Más recientemente, esfuerzos dedicados a codificación. Sistema basado en Java en cooperación con RIPE.**

Desarrollo

- Planes para tener una versión operación en LACNIC en hasta fines de 2009
  - Interfaz Web interface para administración de llaves y certificados
  - Firma de objetos
  - Repositorio
  - Planes futuros: protocolos para sistemas delegados (top/down)

Resumen

- Estructura básica
- Herramientas necesitarán ser desarrolladas para aumentar seguridad de sistemas de rutas.
- Participación y colaboración de la comunidad es necesaria.

LACNIC

Latin American and **Caribbean** Internet Addresses Registry
Registro de Direcciones de Internet para **América Latina** y **Caribe**
Registro de Endereços da Internet para **América Latina** e **Caribe**

Muchas Gracias