



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**

Certificados Emitidos por los RIR

LACNIC
Pablo Allietti

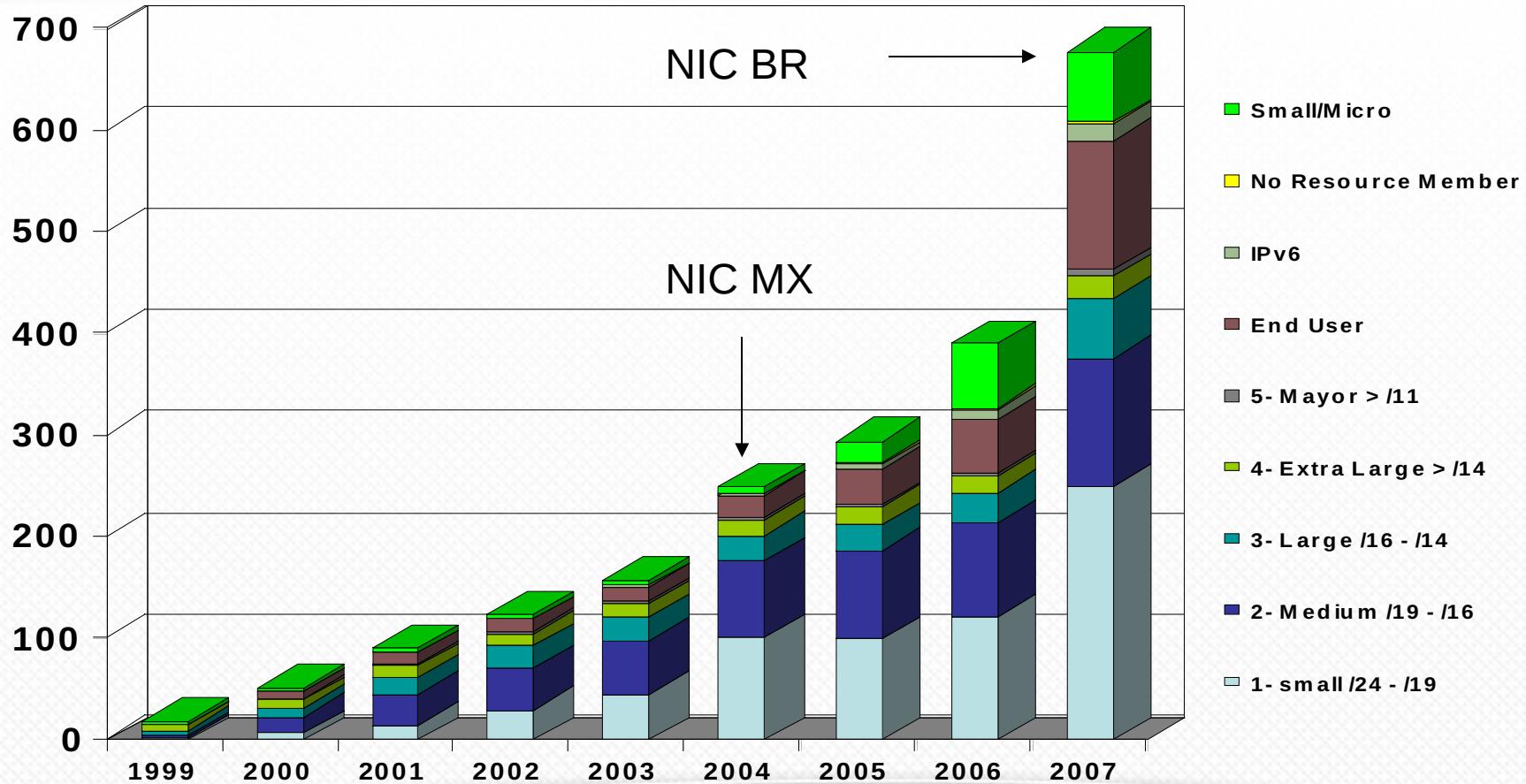


LACNIC

Registro Regional de Internet

- Administración de recursos Internet (IPv4, IPv6, ASN)
- Dos NIRs (Registros Internet Nacionales): México y Brasil.
- Completó 5 años el 31 de octubre pasado.
- Sede en Montevideo Uruguay.
- Servidores y servicios en SP Brasil con replica en Montevideo

LACNIC



Certificación

Concepto de “Notario”

- Entidad neutra encargada de certificar algo.
- Hace verificación/certificación de la autenticidad de algo.
- Entidad de confianza por personas/organizaciones en un contexto dado.

Certificación

Conceptos de Notario

- Nota o Certificado, válido y aceptado en un contexto.
 - **En general, donde el Notario es reconocido como valido y es confiable.**
- Nota o Certificado emitido en Uruguay quizás no sea aceptado en México. (necesidad de reconocer agente emisor y documento como validos)

Certificación

Conceptos de Notario

- Nota o Certificado que contiene un conjunto de información
 - **verificación y validación**
 - **sello de autenticación**
 - **reconocido como valido en un contexto**

Certificación Digital

Sigue estándares internacionales

- X.509, RFC 3280
- Definición de PKI (Public Key Infrastructure).

Información

- Identificación de un sujeto
- Contiene llave publica.
- Llave privada en poder del sujeto
- Indica que el Sujeto es quién dice ser y que posee el par de llaves

Certificado Digital

Certificado contiene básicamente

- Información del Sujeto
- Serial del certificado
- Emisor del Certificado
- Plazo de validez
- Llave publica del sujeto
- Otras informaciones opcionales (extensiones)

Certificado Digital

Version	Versión 3
Serial Number	
Signature Algoritm	ej. RSA
Issuer	Nombre del CA
Validid Period	no antes, no después
Subject	Nombre usuario
Subject Public Key	ID del algoritmo y llave
Extensions	otros campos

Certificado Digital

Notario (Certification Authority - CA)

- Organización conocida y aceptada en un contexto como autoridad certificadora
- Verifica información del sujeto. Y que posee llave privada cuya llave pública figurará en el certificado.
- Firma certificado con su llave privada (del CA) : Sello Digital de autenticidad.

Certificado Digital

Utilización

- **Usuario presenta credenciales (certificado digital)**
- **Firma información. Comprueba que posee el par de llaves**
- **Se verifica autenticidad de la firma**
- **Se verifica validez del certificado**
- **Se aceptan las credenciales**

Certificado Digital

Verificación de firma

- Con una parte del conjunto de llaves (publico/privada) se puede decodificar una información (firma digital).
- Con la llave privada se puede firmar (codificar) información.
- La cual se puede decodificar con la llave publica.
- Se verifica si la operación es exitosa, se confirma validad.
- Se verifica firma digital.

Certificación Digital

Verificación certificado

- ¿Como se verifica su validez?
- Certificados son firmados digitalmente por las Entidades Certificadoras (CA).
- Necesario verificar información del CA.
 - ¿CA conocido (confiable) en el contexto?
 - ¿Se posee información del CA?

Certificación Digital

Conceptos

- Trust Anchor (TA). Punto de confianza en un contexto de certificación digital.
- En general, un CA es un TA.
- Sistemas que hace uso de Certificación Digital, poseen información acerca del TA (o TAs) en el contexto de uso.
- Certificado Digital firmado por un CA que esta en la lista de TAs conocidos, se verifica su validez.

Certificación Digital

Conceptos

- TA puede variar de acuerdo con el contexto o usuario
- El punto de confianza para una persona o sistema puede ser distinto del utilizado por otra persona o otro sistema.

Certificación Digital

Conceptos

- Relaying Party (RP). Sistema que hace uso de un PKI.
 - **El RP define quién es su TA**
- Trust Anchor (TA). Punto de confianza
 - ***Puede* ser un Certificado Digital instalado en un sistema. Ejemplo, certificados de un browser.**
 - **Puede ser otra información. Depende del RP.**

Certificación Digital

Conceptos

- Issuer. Nombre/entidad que emite Certificado Digital (CA)
- Subject. Nombre/entidad sujeto de un Certificado (único por CA)
- Serial Number. Numero Serial del certificado. Cambia siempre que se emite nuevo certificado para la entidad.
- Certificate Revocation List (CRL). Lista de certificados revocados por un CA.

Certificación Digital

Proceso de validación

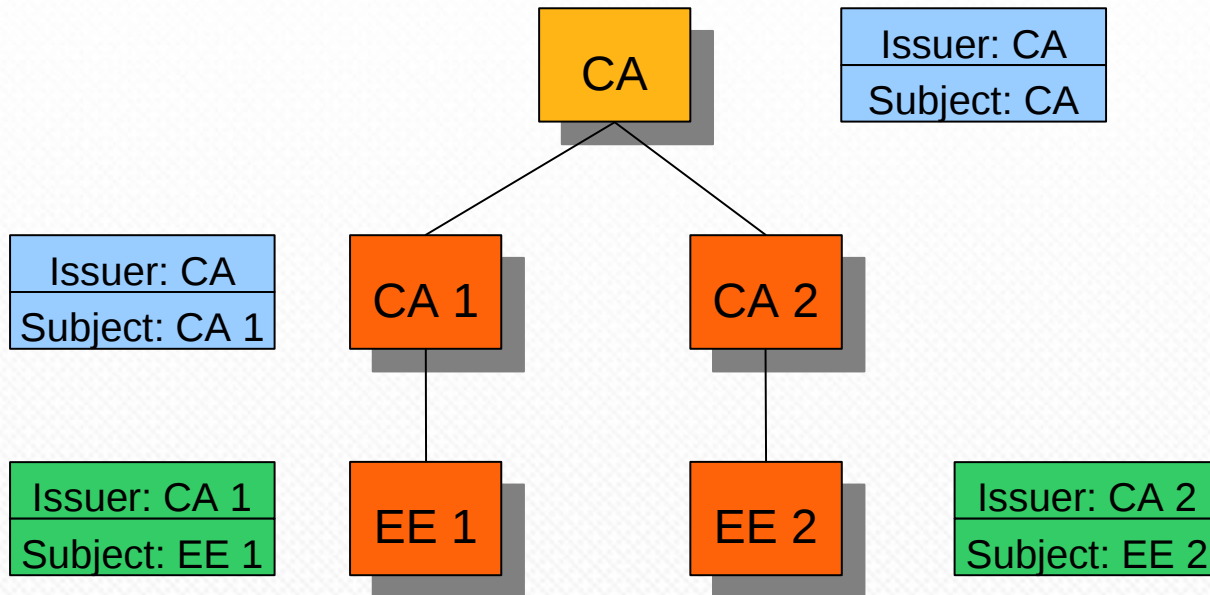
- Se verifica el Subject del certificado. Debe coincidir con identificación persona/sistema.
- Certificado con plazo valido (no antes de, no después de)
- Llave publica y firma digital valida.
- Firma del certificado valida (emitido por un CA confiable).
- No figura en la CRL de ese CA.

Certificación Digital

Cadena de certificación

- Un CA puede emitir certificados que habilitan a otras entidades a actuar como CA (Sub CA).
 - certificado con “flag” (Basic Constraints Extension)
- Jerarquía de CAs

Certificación Digital



Certificación Digital

Cadena de certificación

- Proceso de validación: verificación de certificados en la jerarquía hasta que sea considerado TA.
 - verificar nombre, plazo de validez, llaves, firma digital, CRL.
- No es necesario que el TA sea la raíz de la jerarquía.

Certificado Digital

Puede contener extensiones (criticas o no)

- Identificación de la llave y del Sujeto
- Utilización permitida de llave
 - **firma digital, codificación, firma de certificado, etc**
- Políticas del Certificado
- Nombre alternativo (e-mail, servidor DNS, URL, etc)
- Ubicación de repositorio.
- Recursos Internet

Certificación Digital de Recursos Internet

Certificados Digitales X.509

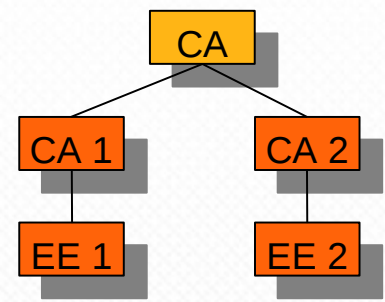
- Información del sujeto, plazo de validez, llave publica, etc

Con extensión:

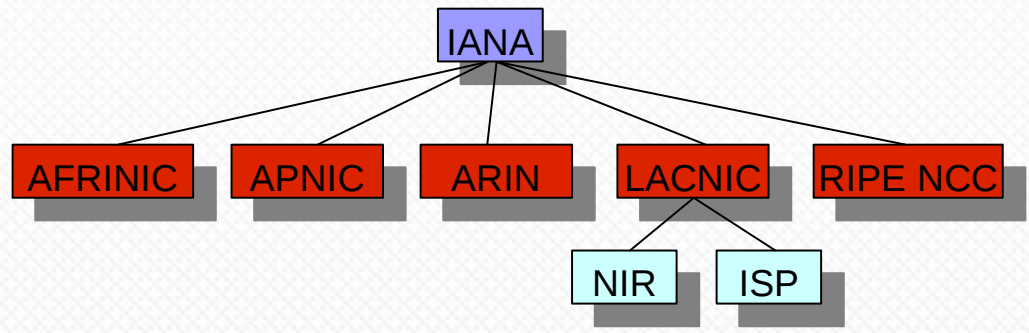
- RFC 3779 estándar IETF define extensión para recursos internet.
- Listado de IPv4, IPv6, ASN asignados a organización

Certificación Digital de Recursos Internet

PKI posee jerarquía de entidades Certificadoras



Distribución de Recursos Internet posee jerarquía.



Certificación Digital de Recursos Internet

Proceso de certificación

- Entidad de Asignación = Entidad Certificadora
 - Cadena de certificación
 - Puntos de Confianza (TA)
- La asignación implicaría la emisión de un certificado digital

Certificación Digital de Recursos Internet

¿Qué problema se intenta resolver?

- Derecho de uso de recursos
 - Whois, IRR no sería suficiente
- Seguridad en la Tabla de Rutas (BGP)
 - Inserción de rutas

Certificados para Recursos Internet

Certificado X.509

- Identificación sujeto, llave publica, plazo de validez, identificación CA, restricciones de uso, etc
- Extensión para Recursos Internet
 - **Mismo certificado contiene el listado de todos los recursos asignados por la Entidad de Asignación para esa entidad**
- Firma digital del CA

Asociación entre entidad, llave y recursos asignados

Certificados para Recursos Internet

Verificaría el derecho de uso de un conjunto de recursos por una entidad.

Llave para firmar otros certificados para subasignaciones. (Restricción CA habilitada)

Certificados especiales (EndEntity) utilizados para firmar objetos de ruta.

Certificados para Recursos Internet

Entidades que reciban Recursos actúan como CA

- ISP recibe asignación del NIR/RIR
- Hace subasignación para sus clientes
- Emite certificado con dichas subasignaciones
- Clientes pueden también emitir certificados

Certificados para Recursos Internet

Identificación del Sujeto

- **Certificados usuales, nombre entidad, país, etc**
- **Certificados de Recursos**
 - **Caracteres sin significado externo (AEFFDDEE)**
 - **Implicaciones legales para certificar nombre, identidad**
 - **Restringe la posibilidad de uso para otros fines**

Certificados para Recursos Internet

Su función

- **Certifica el derecho de uso de recursos indicados**
- **Para entidad dueña de llave privada cuyo par (llave pública) figura en certificado**

Certificado para Recursos Internet

Su uso

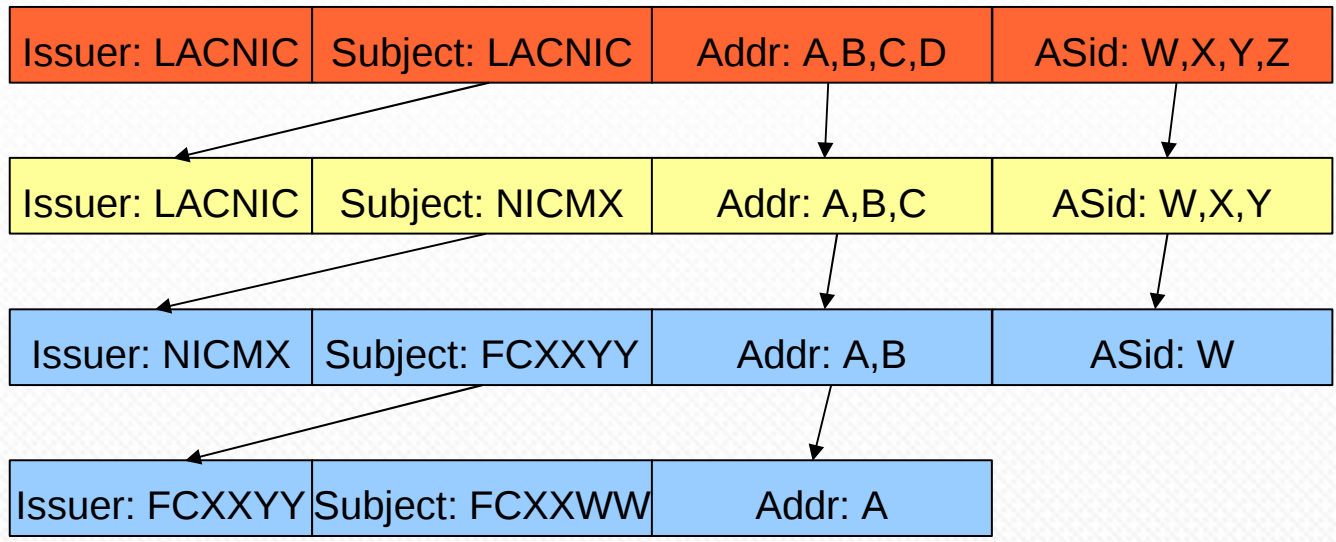
- En el contexto de Internet
- RIRs como Puntos de Confianza (TA)
 - **sin necesidad de nuevos CAs**

Certificado para Recursos Internet

Version	Versión 3
Serial Number	
Signature Algoritm	ej. RSA
Issuer	Nombre CA (Ej. LACNIC)
Validid Period	no antes, no después (1 año)
Subject	Ident. entidad (Ej, CN=FC3209809268)
Subject Public Key	ID del algoritmo y llave
Extensions	otros campos
Addr: 192.0.2.0 ASid: 65535	

Certificación de Recursos Internet

Cadena de certificación



Certificados para Recursos Internet

Asignaciones posteriores

- Inserción de nuevos recursos en el certificado
- Revocación certificado anterior
- Emisión de nuevo certificado (nuevo serial number)
 - sin necesidad de cambiar llaves privada/publica (sin impacto en la cadena)

Certificados para Recursos Internet

Entidad con asignación de distintos orígenes

- Certificado para cada grupo de recursos de cada entidad de asignación (ISP).
- Pueden tener misma identificación y par de llaves.
- Subasignación debe seguir cadena certificación apropiada.

Certificación de Recursos Internet

Proceso de validación

- **Verificación usual:**
 - **plazo de validez, sujeto, firma digital del CA, CRL**
- **Extensión Recursos Internet**
 - **Subconjunto de los recursos en certificado del CA**
- **En toda la cadena hasta un Punto de Confianza (TA)**

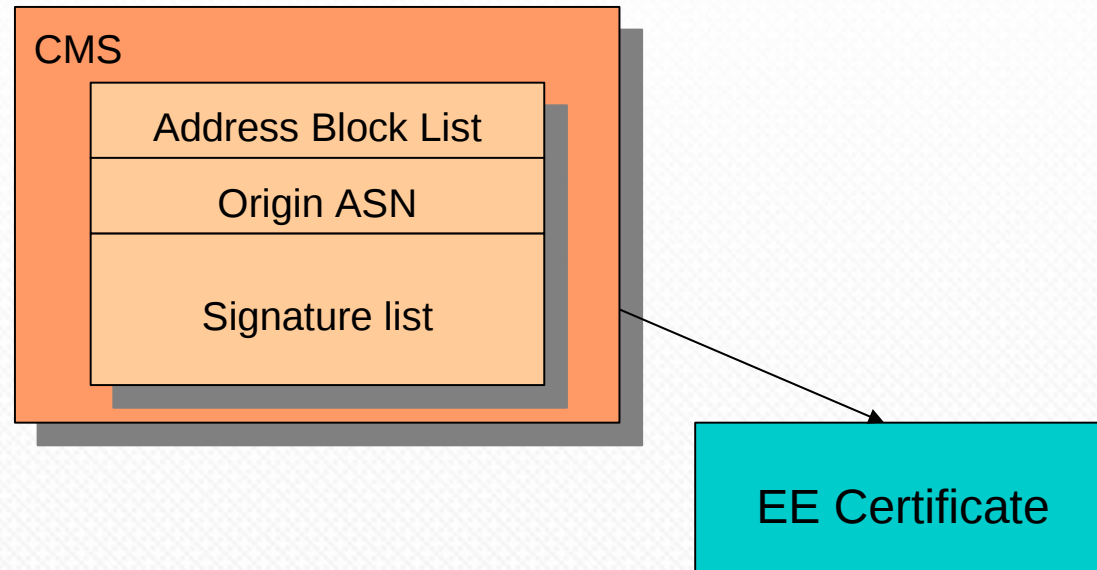
Certificados para Recursos Internet

ROA – Route Origination Authorization

- Objeto firmado con clave privada de entidad con asignación
- Indica autoridad para anunciar conjunto de direcciones
 - Objeto indica bloques que pueden ser anunciados con origen en un AS cualquier.
 - Se lo firma con su llave privada

Certificados para Recursos Internet

ROA – Route Origination Authorization



Certificados para Recursos Internet

Verificación ROA

- Formato del mensaje CMS.
- Certificado EE cuya llave se utilizo para firmar (ROA tiene identificación del certificado).
- Se verifica la firma digital.
- Se verifica que el certificado EE tiene los recursos indicados en la ROA.
- Se verifica validez del certificado EE.

Certificados para Recursos Internet

Otros detalles de ROA

- Estándares de certificación no recomiendan utilizar misma llave que firma certificado (CA) para firma otro objeto
 - **Necesidad de certificado EE, sin flag CA**
- Certificado EE contiene todo o parte del conjunto de recursos asignados
- Para cancelar una ROA, certificado EE es revocado (No existe CRL)

Certificados para Recursos Internet

Resumen del uso

- RIR asigna bloques y emite certificado para un ISP
- ISP desea anunciar bloques vía sus proveedores
- Emite certificados End Entity con bloques que va anunciar
 - **nuevos pares de llaves (sin necesidad de almacenarlas)**
- Crea las ROAs (una para cada anuncio distinto)
- Firma con llave del certificado End Entity
- Revoca certificado End Entity cuando ROA no es más válida

Certificados para Recursos Internet

Seguridad de la Tabla de Rutas

- ROAs podrían ser utilizadas por protocolos de ruteo
 - **Verificación online u offline**
- ROAs podría ser utilizadas para creación de filtros de rutas
 - **Cache local de certificados y ROAs validados**
- Pruebas con herramienta para verificación en línea (los operadores verificarían solicitudes de anuncios de clientes).

Certificación de Recursos Internet

¿Qué se está haciendo?

- RIRs en fuerza de trabajo (TaskForce) para un prototipo
 - PKI para recursos Internet
 - Comunicación con base de datos de recursos
 - Comunicación entre PKIs en la jerarquía (RIR/NIR/ISP)
 - Repositorio de certificados y ROAs
 - Pruebas de integración
- Puntos en discusión:
 - repositorio, transferencias, intercomunicación, TA

Certificación de Recursos Internet

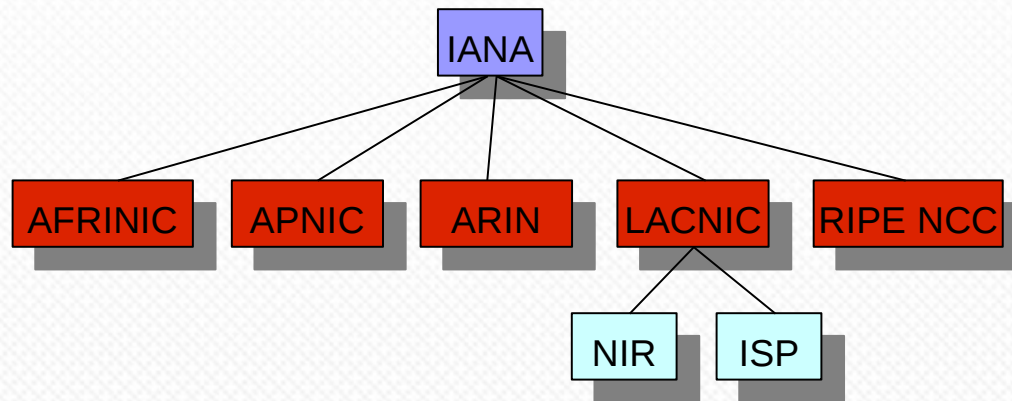
¿Qué se está haciendo?

- Prototipo externo para validación de certificados, ROAs
 - Copia de toda información
 - Validación
 - Base de datos para uso posterior

Certificación de Recursos Internet

Puntos de Confianza (TA)

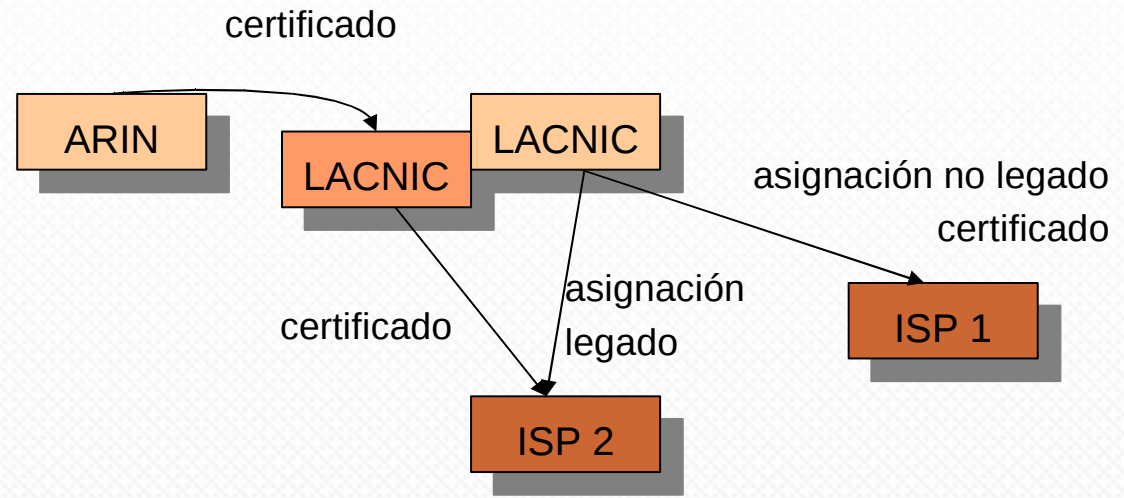
- 5 puntos (cada RIR un TA)
- IANA como TA y raíz de la jerarquía



Certificación de Recursos Internet

Bloques Legados

- cross certification



Certificación de Recursos Internet

Referencias

- ◉ Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile <http://www.ietf.org/rfc/rfc3280.txt>
- ◉ X.509 Extensions for IP Addresses and AS Identifiers <http://www.ietf.org/rfc/rfc3779.txt>
- ◉ A Profile for X.509 PKIX Resource Certificates <http://www.ietf.org/internet-drafts/draft-ietf-sidr-res-certs-08.txt> [DRAFT]
- ◉ A Profile for Route Origin Authorizations (ROAs) <http://www.ietf.org/internet-drafts/draft-ietf-sidr-roa-format-01.txt> [DRAFT]





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