Certificación de Recursos RPKI

Elaborado por Telefónica Móviles México
Dirección comercial de Carriers y Operadores
Ingeniería de Core IP

Tabla de contenido

1 Introducción

En la actualidad las conexiones entre las distintas organizaciones que se conforman la conectividad de Internet (sean carriers, proveedores de contenido o clientes finales) están basadas en un sistema de confianza mutua, donde cada parte confía que la rutas IP enviadas y recibidas son propias de la organización y no serán maliciosamente alteradas.

Este modelo de confianza está abierto a potenciales errores, abusos y ataques (explotando vulnerabilidades de enrutamiento). En tanto que la Red sea cada vez más grande el riesgo es mayor, por lo que a pesar del despliegue de filtros de protección y los controles de los administradores de red de cada organización, es posible que quien anuncie una ruta en Internet no esté autorizado a hacerlo. Esto se conoce como "secuestro de rutas", y es un hecho ocurre de manera recurrente; en especial con las direcciones no asignadas.
Las actividades maliciosas que típicamente se realizan con rutas secuestradas son:

- Envíos de spam,
- Tráfico Black-holeing,
- Captura de tráfico para su inspección o alteración,
- Fraude de identidad en un nivel de aplicación,
- Ataques de DDoS (Distributed Denial of Service),
- Desestabilización de la red.

Un ejemplo de lo anterior fueron los casos conocidos de alto impacto a nivel mundial, donde entidades no autorizadas perpetraron tráfico ajeno:

- YouTube vs. Pakistan Telecom (Feb 2008)
- China Telecom (2010)
- Google en Europa del este (varios AS, 2010)

Para mitigar esta inseguridad de Red, la certificación de recursos constituye un esfuerzo mundial para brindar una infraestructura de llave pública (o *PKI*) robusta, comúnmente llamada ***RPKI*** (***Resource Public Key Infraestructure***), para la firma digital de los recursos de Internet.

2 Objetivo

El objetivo de una estructura de seguridad de enrutamiento (automatizada) es permitir a los usuarios de redes públicas de Internet verificar la autenticidad del derecho a uso del titular actual sobre los recursos públicos de Internet, a través del uso de certificados digitales, con el fin de asegurar que la información sea correctamente transmitida por Internet y que corresponda con los registros e intenciones del titular del *pool* de recursos en cuestión.

Mediante el uso de certificados digitales, el titular de los recursos podrá crear objetos firmados ***(ROAs - Routing Origin Authorization)*** usando su llave privada, con los cuales podrá demostrar digitalmente que posee el derecho de uso de dichos objetos (uno o varios prefijos de direcciones IP) y autorizar su anuncio a través de un **Número de Sistema Autónomo** (**ASN**) de origen especificado.

El contenido de un ROA identifica un único ASN autorizado por el titular de espacio de direcciones para originar rutas y una lista de uno o más prefijos de direcciones IP que serán anunciados, por lo que sería necesario crear un ROA para cada ASN autorizado. Por ejemplo, un ROA debería establecer lo siguiente: Telefónica Móviles México, cuyo ASN es 7438 con un prefijo 200.39.0.0/19.

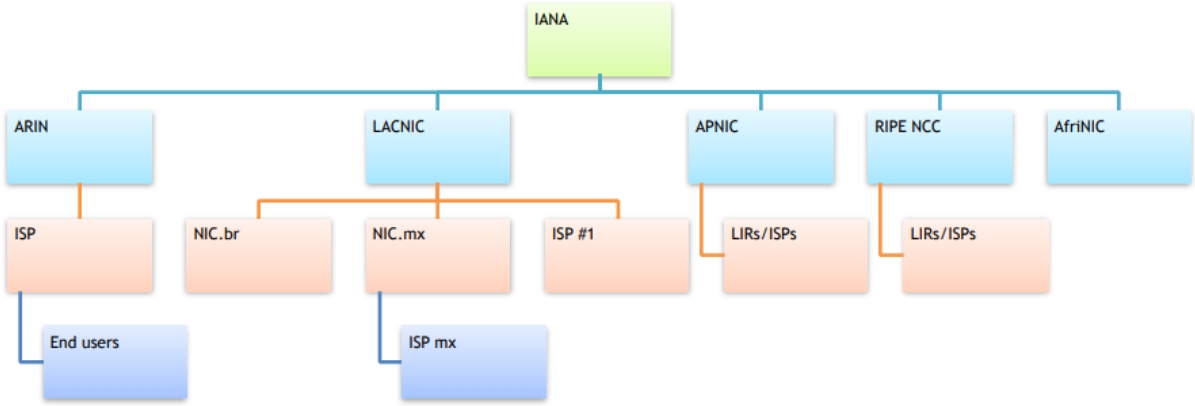
A partir del último trimestre del presente año 2019 algunos ISPs y proveedores de contenido estarán validando el origen de rutas y posiblemente descartando tráfico en caso de no contar con esta certificación.

Por tal motivo, Telefónica México en virtud del cuidado y seguridad de sus clientes y operadores que directa o indirectamente cruzan tráfico IP de Internet a través de nuestra red ha creado este manual invitando a cada aliado tecnológico a que certifique sus recursos de Internet (ASNs y prefijos IPv4 e IPv6) a través del uso de ROAs.

3 Certificación de Recursos y Creación de ROA's

Previo a la creación de los certificados la organización debe contar con el usuario con el que solicitaron recursos (ASNs Público y Direccionamiento Público IPv4 y/o IPv6) y les hayan sido asignados.

Los recursos son asignados por diferentes organismos dependiendo la región geográfica en la que se encuentre el cliente:

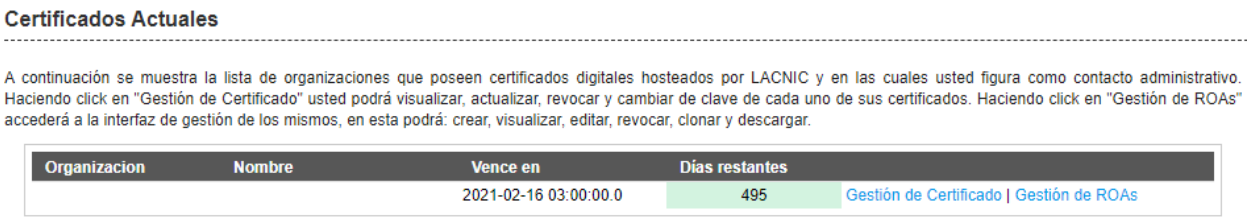


En el caso de Latinoamérica y el Caribe es **LACNIC,** Asociación para el Registro de Direcciones de Internet**,** de donde basamos este manual para crear los Certificados, para iniciar se debe ingresar al siguiente URL:

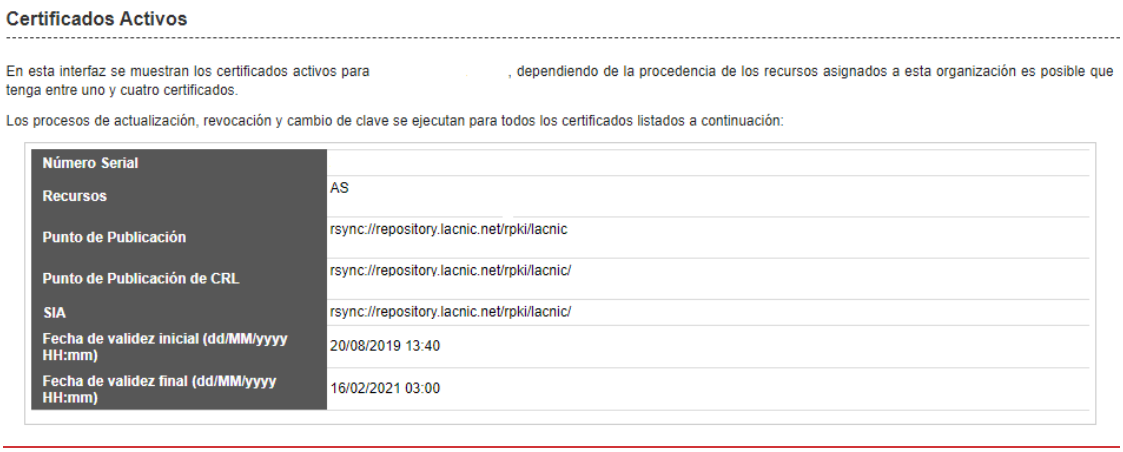
https://rpki.lacnic.net/rpki-hosted-web/login

El enlace anterior solicitará el usuario y contraseña que tengan creado en LACNIC para poder certificar sus recursos:

LACNIC tiene registrada la información de la Organización a la que previamente haya asignado ASN y Direccionamiento Público mostrando la siguiente información:

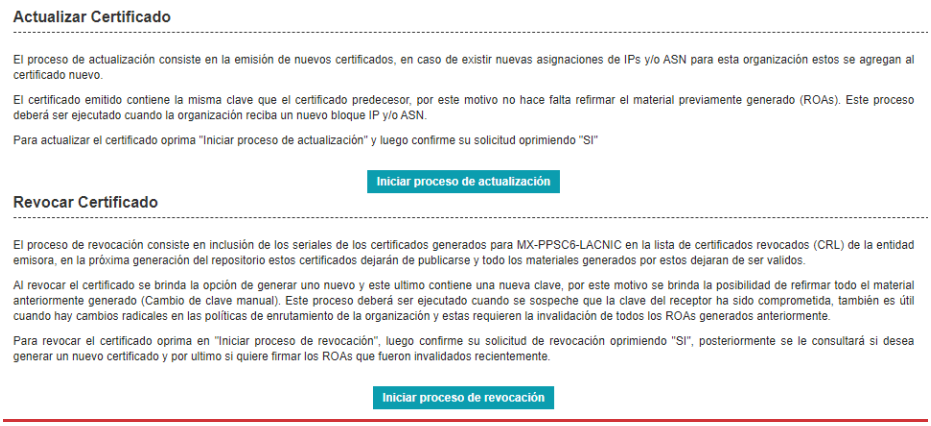


Se tendrán 2 opciones ***Gestion de Certificados*** y ***Gestión de ROAs***, procedemos a seleccionar la primera Opción:



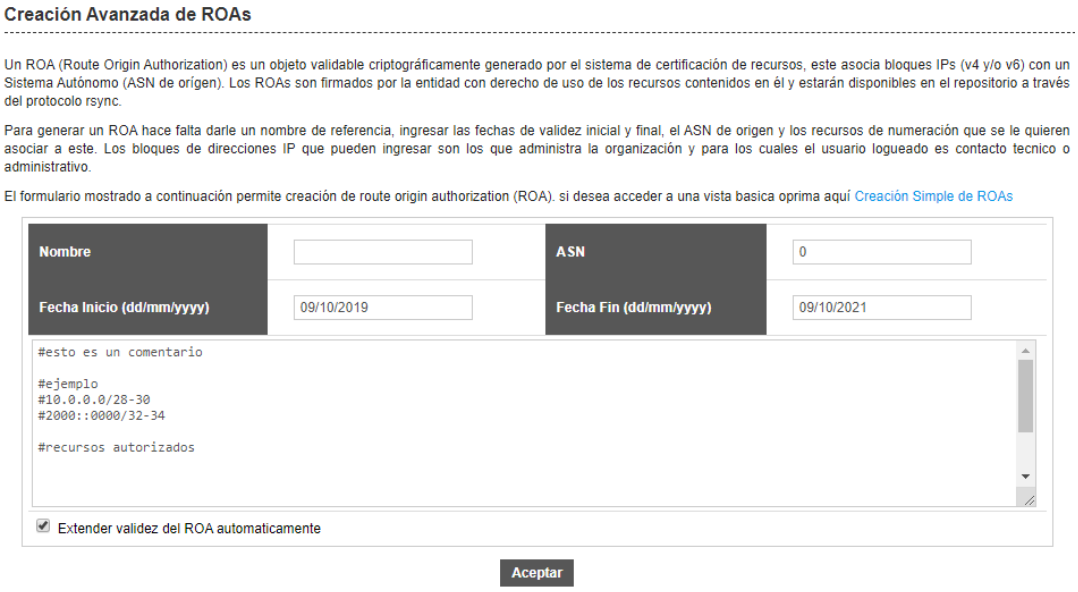
Al hacer esto se generan en automático los certificados, en este certificado se muestran los recursos con que la Organización cuenta y los repositorios que se harán públicos para el registro de Origen.

Si alguna información es incorrecta o se requiere modificar se puede solicitar seleccionando actualizar o revocar el certificado.



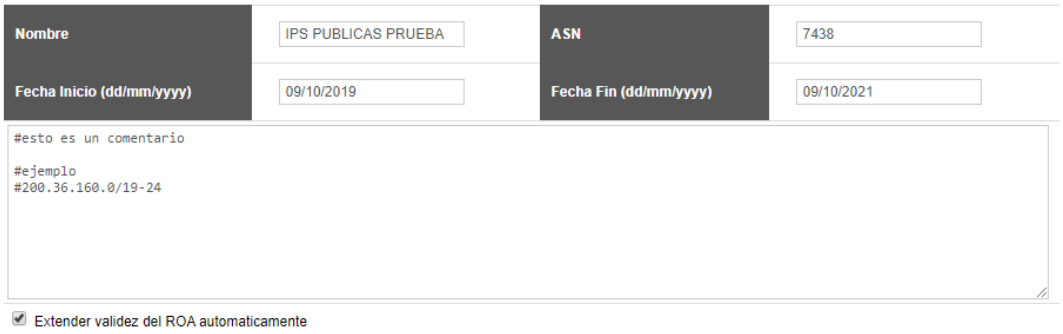
Una vez creado el certificado se deben generar los ***ROAs*** (***Routing Origin Authorization***).

Los ROAs contienen información sobre el AS de origen permitido para un conjunto de prefijos y son firmados usando los certificados generados por RPKI.



Donde se deben indicar los siguientes campos:

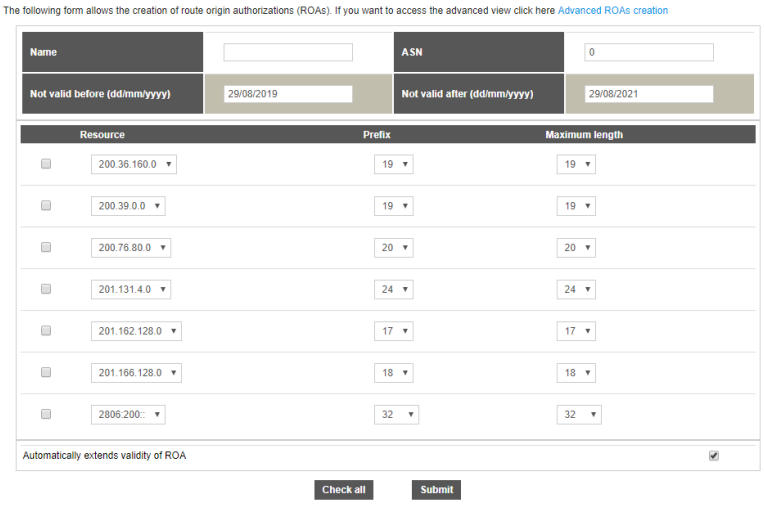
- **Nombre:** El nombre es descriptivo, no es necesario indicar algún contacto o persona responsable.
- **ASN:** Número de Sistema Autónomo público de la organización.
- **Segmentos:** Bloque de direccionamiento público asignado por LACNIC, se puede indicar el *Maximum Length* que corresponde a la segmentación del bloque hasta un máximo de /24, ejemplo:



El segmento 200.36.160.0/19-24 significa que el Bloque de IPs Públicas es /19 y se puede publicar a Internet como segmentos /24, la segmentación de las subredes se indica con el guion medio.

Después de llenar los campos se debe dar click en el Checkbox **Aceptar**.

La creación de ROAs también se puede hacer manualmente o en el modo simple que ya viene precargado, seleccionando "***Creación Simple de ROAs***":



Donde se deben indicar los siguientes campos:

- **Nombre:** El nombre es descriptivo, no es necesario indicar algún contacto o persona responsable.
- **ASN:** Número de Sistema Autónomo público de la organización.
- **Segmentos:** Bloque de direccionamiento público asignado por LACNIC, al igual que la forma manual se debe indicar el segmento y con un guion medio indicar como se segmentará con un máximo /24.

Una vez llenado los campos anteriores seleccionamos ***Aceptar*** para crear los ROAs.

Nombre	ASN	Cer Serial	Fecha Inicio	Fecha Fin	Días restantes	Recursos	
ROA	7438		2019-08-27 00:00:00.0	2021-08-27 00:00:00.0	728	200.36.160.0/19-24,	Editar Editar Avanzado Revocar Duplicar

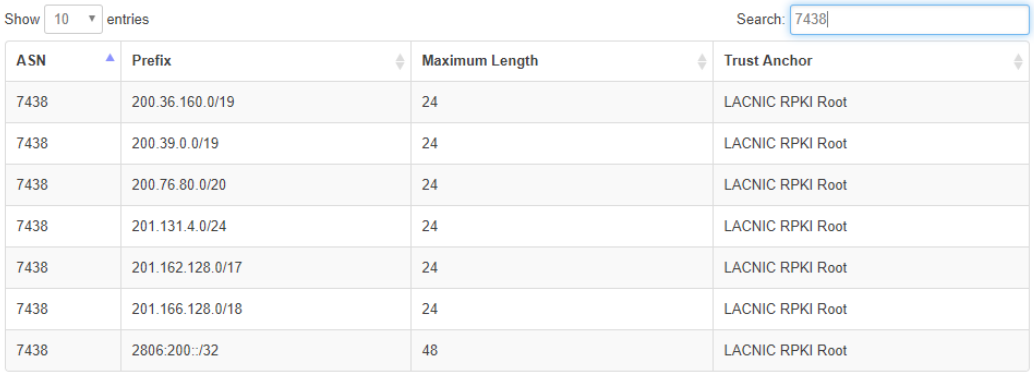
En la imagen anterior se muestra el ROA creado que deberá ser ingresado en el repositorio público y de esta forma se certificarán los recursos de la organización para saber la Denominación de Origen de los Direccionamientos Públicos.

4 Validación

Una vez creado el certificado ROA este se hará público y tomará algunas horas para publicarse´.

En http://localcert.ripe.net:8088/roas

Donde se puede validar que los ROAs que ya fueron certificados. En el caso de Telefónica Móviles México, cuyo ASN es 7438 tenemos:



Show 10 entries Search: 7438

ASN	Prefix	Maximum Length	Trust Anchor
7438	200.36.160.0/19	24	LACNIC RPKI Root
7438	200.39.0.0/19	24	LACNIC RPKI Root
7438	200.76.80.0/20	24	LACNIC RPKI Root
7438	201.131.4.0/24	24	LACNIC RPKI Root
7438	201.162.128.0/17	24	LACNIC RPKI Root
7438	201.166.128.0/18	24	LACNIC RPKI Root
7438	2806:200::/32	48	LACNIC RPKI Root

De esta forma podemos observar que los recursos asignados ya cuentan con ROA y LACNIC es la fuente certificadora.
En caso de necesitar más información al respecto del tema pueden consultar la página de LACNIC, entrando al apartado de Servicios → Certificación de Recursos (RPKI)

(https://www.lacnic.net/980/1/lacnic/certificacion-de-recursos-rpki)

5 Referencias

https://www.lacnic.net/502/1/lacnic/informacion-general-sobre-certificacion-de-recursos-rpki

https://www.lacnic.net/innovaportal/file/502/1/rpki-update.pdf

https://www.iar.mx/jsf/static_content/services/current_services/resources_certification/rpkInfrastructure.jsf#