UpDown RPKI LACNIC y Krill

Carlos Ortíz
cortiz@lacnic.net

Agenda

- RPKI
- UpDown
- Herramientas para probar UpDown
- Krill
- Integración servicio UpDown LACNIC - Krill

RPKI (Infraestructura de clave publica de recursos)

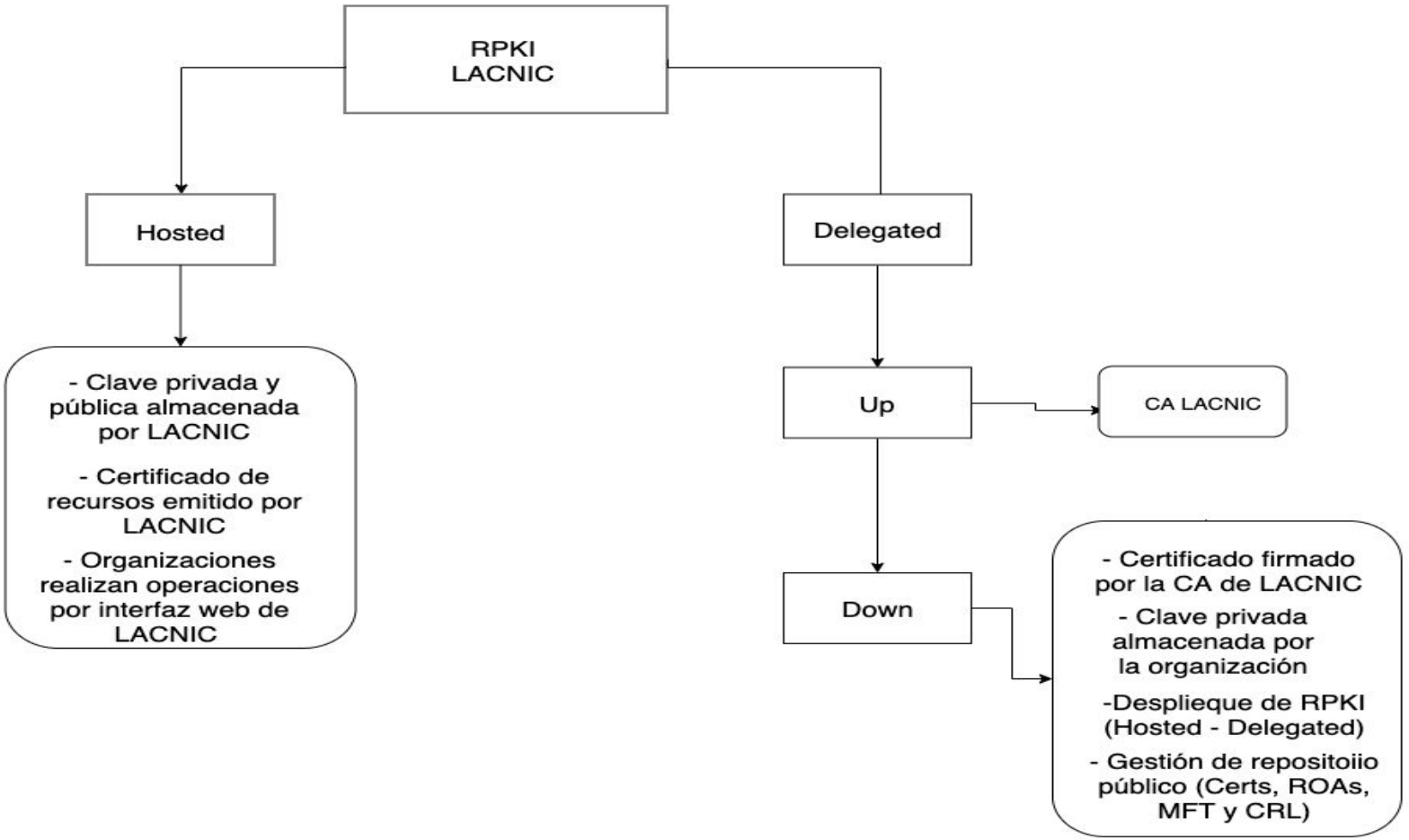
- Certificar la autorización a utilizar un recurso de internet.
- Modelo jerárquico de asignación de recursos por medio de los RIRs.
- Uso de certificados digitales X.509 v3 con extensiones para incluir recursos de internet (IPv4,IPv6,ASNs).
- Generación de objetos firmados digitalmente para soportar seguridad del enrutamiento, ROAs (Routing Origin Authorization).
- Repositorio público, íntegro y accesible por rsync y rrdp, donde se publican Certs, ROAs, MFT, CRLs.

RPKI - Implementación

- Hosteado:
  - LACNIC emite los certificados de recursos y almacena tanto claves públicas como privadas.
  - Los certificados se emiten a demanda de las organizaciones y son estas las que realizan operaciones por medio de una interfaz web provista por LACNIC.

- Delegado:
  - Estándar UpDown RPKI, protocolo de aprovisionamiento de certificados RPKI.
  - Simple interacción request / response.
  - Cliente almacena su clave privada y garantiza integridad del repositorio con todos sus objetos.

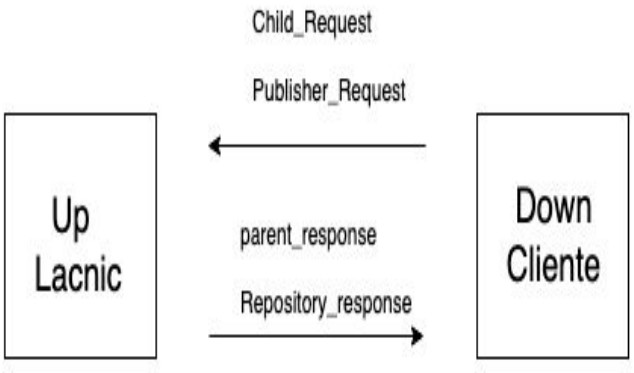
RPKI - Implementación



RPKI - UpDown

¿Cómo empezar?

1- Out-of-Band. RFC 8183



Seguir

2- Protocol for Provisioning Resource Certificate. RFC 6492

- List
- Issuance
- Revoke

UpDown RPKI

Herramientas:

- Certificate Authority Software:
  - Dragon Research Labs Certificate Authority
  - Krill

- Validadores:
  - FORT validator, by NIC.mx & LACNIC (en C).
  - RIPE NCC RPKI validator (en java)
  - Routinator 3000, by NLnet Labs (en Rust)
  - OctoRPKI, by Cloudflare (en Go)
  - Dragon Research Labs Validating Cache (en Python)
  - RPSTIR, by Raytheon BBN Technologies (En C)
  - OpenBSD rpki-client(1) (en C)

Krill

¿Que es?

- RPKI client software que permite a organizaciones correr su propio ecosistema RPKI.

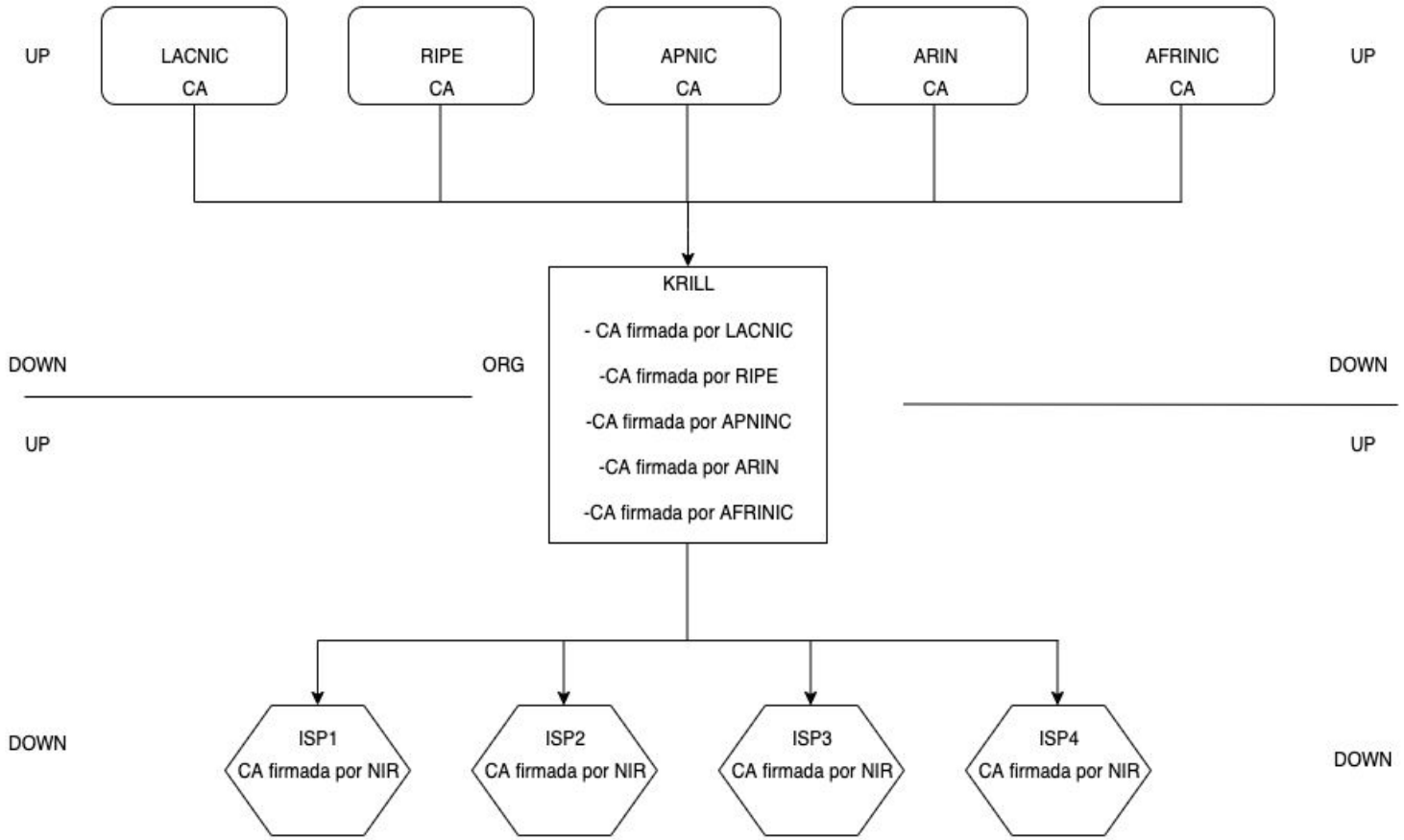
¿Características?

- Correr como child de diferentes RIRs (LACNIC,RIPE,ARIN,etc)
- Correr como parent de diferentes organizaciones. Ej (NIR, Grandes ISPs)
- Cuenta con servidor de publicación, es decir, una organización puede publicar los objetos generados de RPKI por sí mismos o darle a una tercera parte la posibilidad de publicación de los objetos.

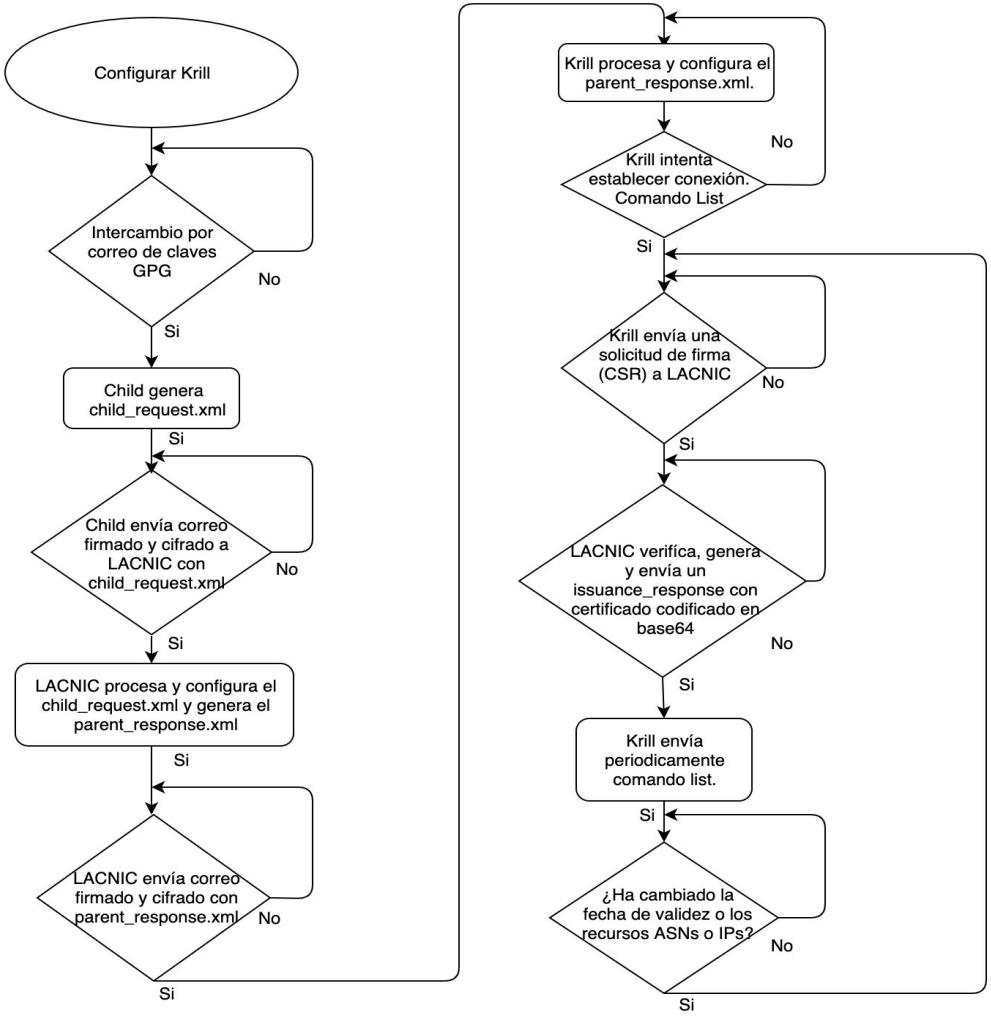
Información específica sobre Krill:
https://rpki.readthedocs.io/en/latest/krill/index.html

Repositorio git con proyecto Krill:
https://github.com/NLnetLabs/krill

Krill - funcionamiento



Integración servicio UpDown Lacnic - Krill



Updown - Despliegue del servicio

Disponible:

- Servicio Beta UpDown LACNIC, activo desde finales de 2019
- Servicio demo para pruebas

Dirigido:

- Grandes Organizaciones, que quieran proveer a sus clientes, de su propio sistema de gestión RPKI.

Resumen

- UpDown permite automatizar la gestión de certificados RPKI.

- El cliente (parte Down), contará con un certificado firmado por la CA de LACNIC.

- El cliente debe almacenar su clave privada y requiere desplegar RPKI en modo hosteado o delegado.

- El cliente debe generar un repositorio íntegro con todos los objetos presentes en RPKI (Certs, ROAs, MFT, CRLs).

- RPKI
- UpDown
- Herramientas para probar Updown
- Krill
- Integración servicio UpDown LACNIC - Krill