

# RPKI: Actualización sobre estándares en desarrollo

*Ricardo Patara*  
*NIC.BR*

# Introducción

- RPKI - Resources PKI
  - “Public Key Infraestructure” (PKI)  
Certificates - (X.509)
  - Extensión para información de Recursos Internet (RFC 3779)

# Introducción

- RPKI
  - Indican “derecho de uso” de Recursos Internet
  - Sin información de nombre de organizaciones
  - Detentor de clave privada comprueba su derecho de uso.

# Desarrollo

- Registros Regionales (RIR), involucrados desde hace aproximadamente 4 años
- Brindar más “confiabilidad” en información de registro
- Herramienta para indicar “derecho de uso”
  - Otras aplicaciones/uso van a surgir

# Estándares

- “Working Group” en la IETF (SIDR)
  - Todavía no hay RFCs o estándares publicados
  - No impide el desarrollo
  - Coordinación entre los RIRs
  - Solución única y compatible

# Estándares - drafts

- “draft-ietf-sidr-res-cert-18 - “A Profile for X.509 PKIX Resources Certificate”
- Trata de especificar un profile para los certificados RPKI y su uso
- Información esperada en cada campo
- Validación, CRL, etc

# Estándares - drafts

- “draft-ietf-sidr-repos-struct-04 - “A Profile Protocol for Resources Certificate Repository Structure”
- Profile para estructura de repositorios, donde se publican los certificados y materiales firmados
- Propuesta para esquema de nombre, contenido de repositorio, manifest, etc

# Estándares - drafts

- “draft-ietf-sidr-rescerts-provisioning-06 - “A Protocol for provisioning Certificates”
- Define “framework” para interacción entre emisor y receptor de Certs RPKI.
- Protocolo para ISP solicitar Certs al IR. Así como para status, revocación, etc.
- “Up/down”, sistema delegado

# Estándares - drafts

- “draft-ietf-sidr-cp-08 - “Certificate Policy (CP) for the Resource PKI (RPKI)”
- Toda PKI debe tener una “Politica de Certificación”. Ese documento define una para la RPKI.
- Roles de participantes, uso soportado, ciclo de vida, operación, seguridad, etc

# Estándares - drafts

- “draft-ietf-sidr-roa-validation-06 -  
“Validation of Route Origination using the  
Resource Certificate PKI and ROAs”
- Define semántica para la ROA
- Posible uso de la RPKI para validar origen  
de rutas y derecho de uso de recursos.

# Estándares

- Drafts más importantes para la infraestructura cerca del ratificación
- Es lo más importante para los RIRs en ese momento
- Posibilita brindar mayor “confiabilidad” a información de registro (derecho de uso)
- Otros usos vendrán (otros entornos)

¿Comentarios/Dudas?

Danki!