
nic.br
Núcleo de Informação
e Coordenação do
Ponto BR
cgi.br
Comitê Gestor da
Internet no Brasil
registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

Tutorial
Segurança no Roteamento BGP
- RPKI modo delegado / Krill

ceptro.br nic.br cgi.br

Revisão - O que é RPKI?

- Estrutura desenvolvida para validar recursos de numeração
  - ASN e Prefixos IPs
    - Alocados
  - Utilizado no BGP

MANRS

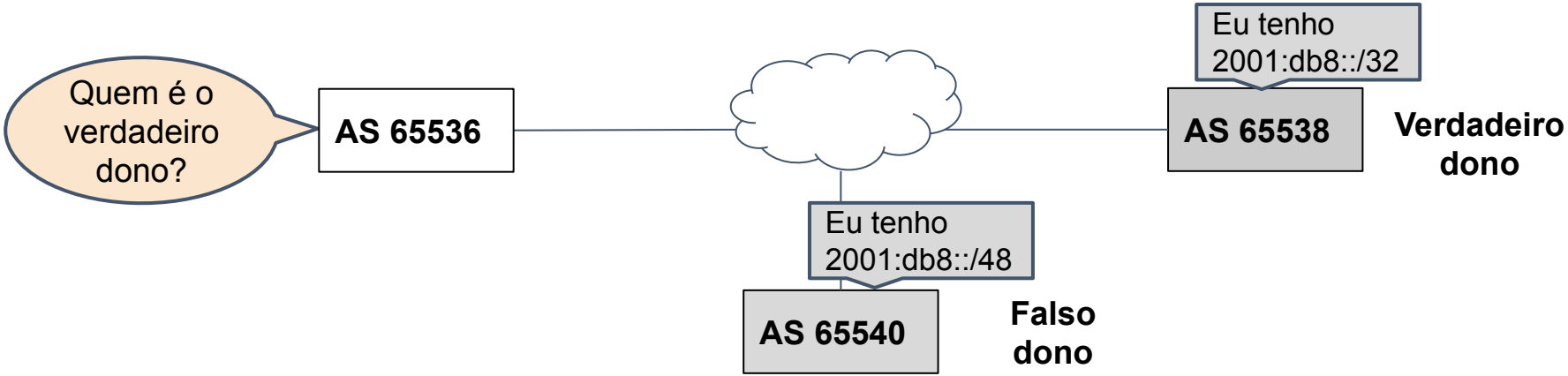
- Previne os problemas de BGP Hijacking
- A colaboração de todos os ASes é essencial!!!
- Faz parte do MANRS

Revisão - O que é RPKI?

ROTAS:

2001:db8::/32 ... 65538 i

2001:db8::/48 ... 65540 i

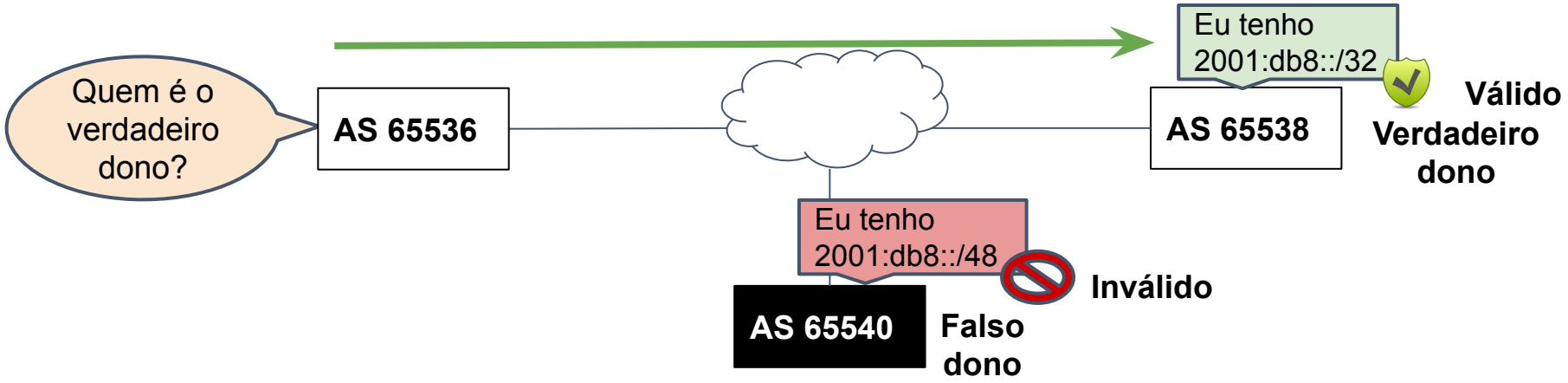


Revisão - O que é RPKI?

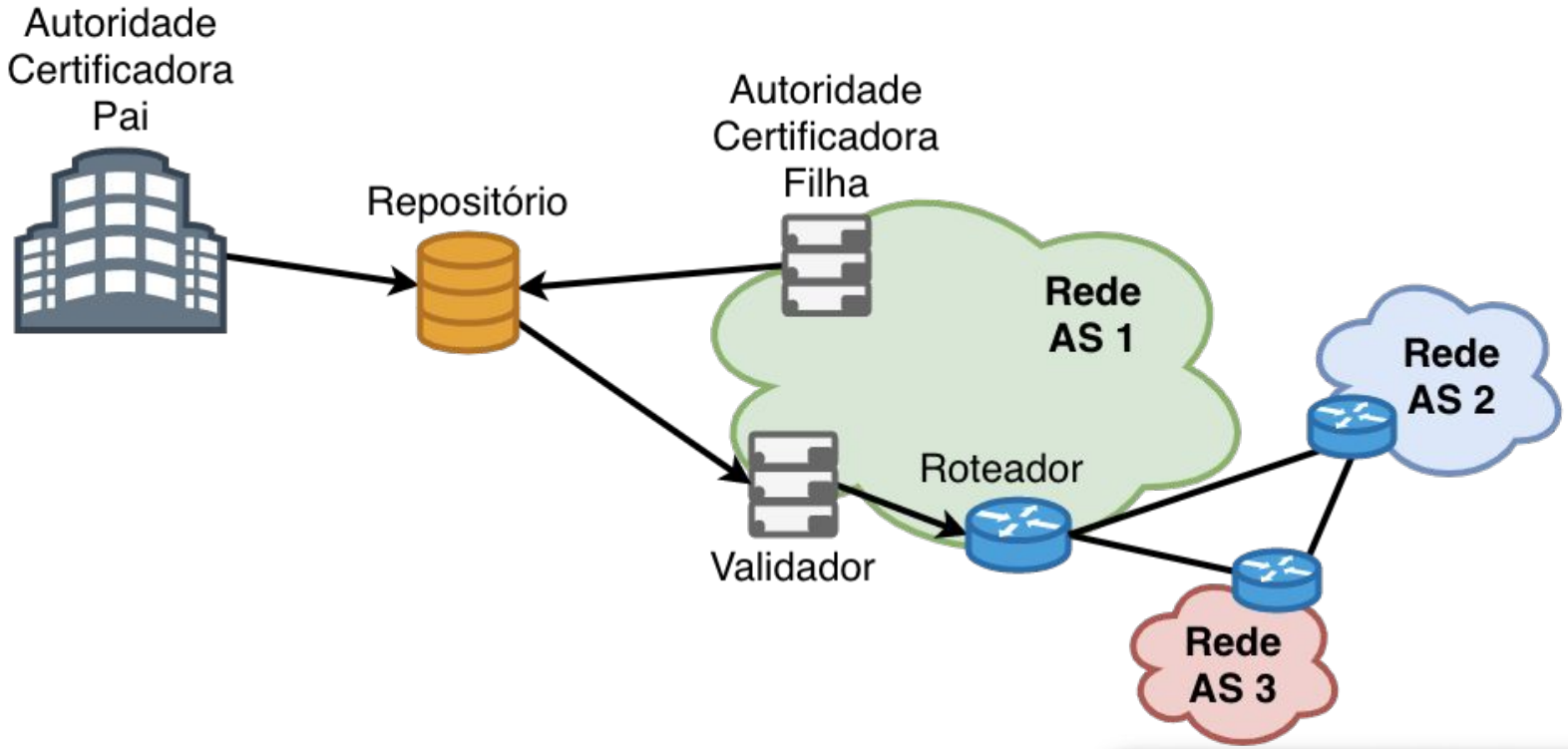
ROTAS:

2001:db8::/32 ... 65538 i

2001:db8::/48 ... 65540 i



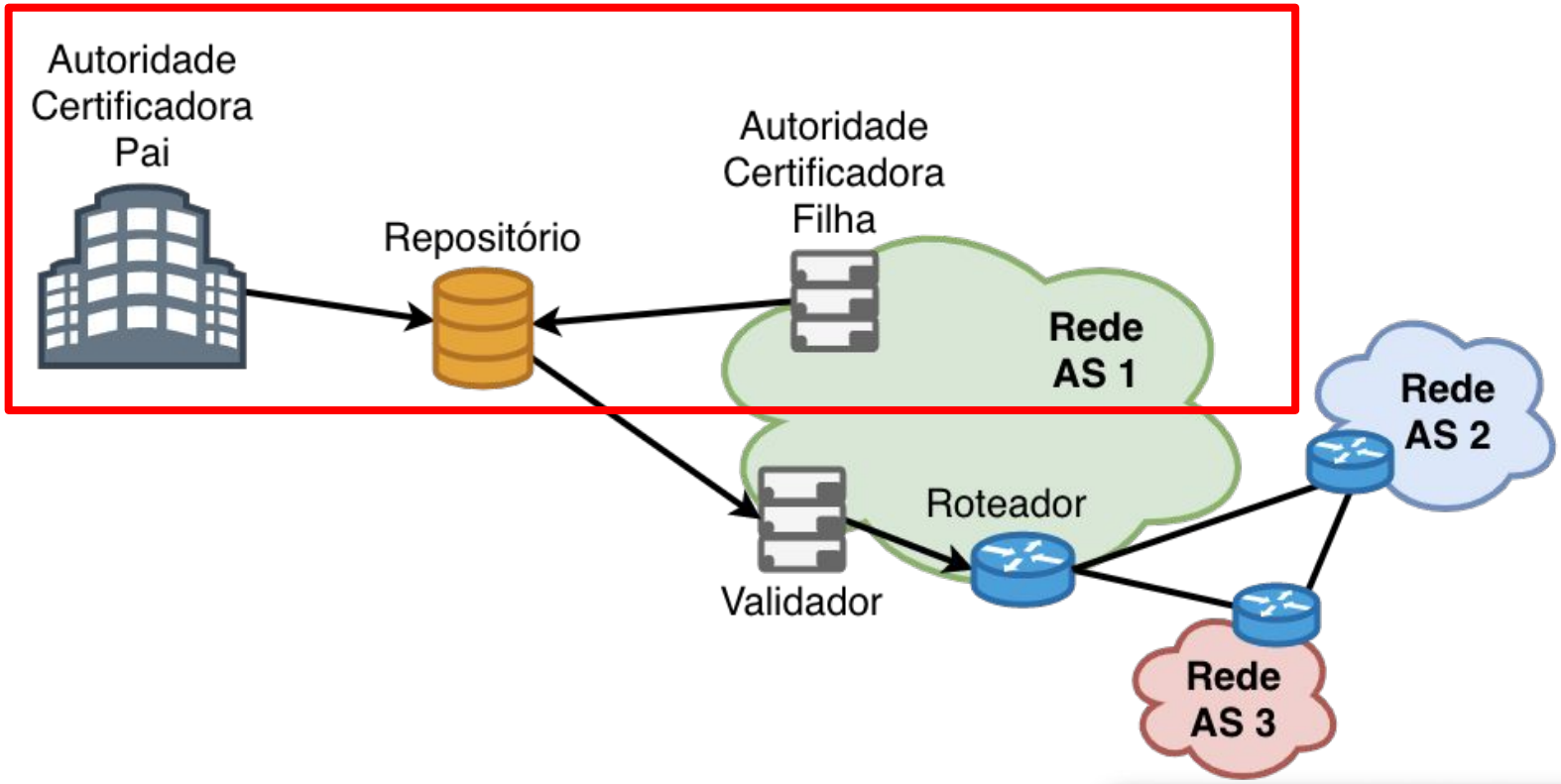
Revisão - O que é RPKI?



Revisão - O que é RPKI?

- Duas partes:
  - Certificação de recursos
    - Anunciar os prefixos no RPKI
    - Qualquer um que possuir recursos de IP pode aderir
  - Validação da Origem
    - Consultar prefixos anunciados no RPKI
    - Necessita uso de roteador compatível

Certificação de Recursos

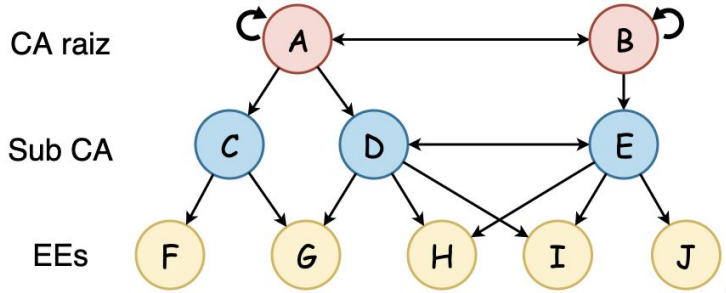


Certificação

- Certificação digital
  - Associa a chave pública com o seu dono
- Modelo PKI (Public Key Infrastructure)
  - Certificado contém chave pública assinada por uma Autoridade Certificadora ou Certificate Authority (CA).
  - Ex.: ICP-Brasil
- RPKI
  - Certificação de recursos
  - Associa a chave pública com os recursos

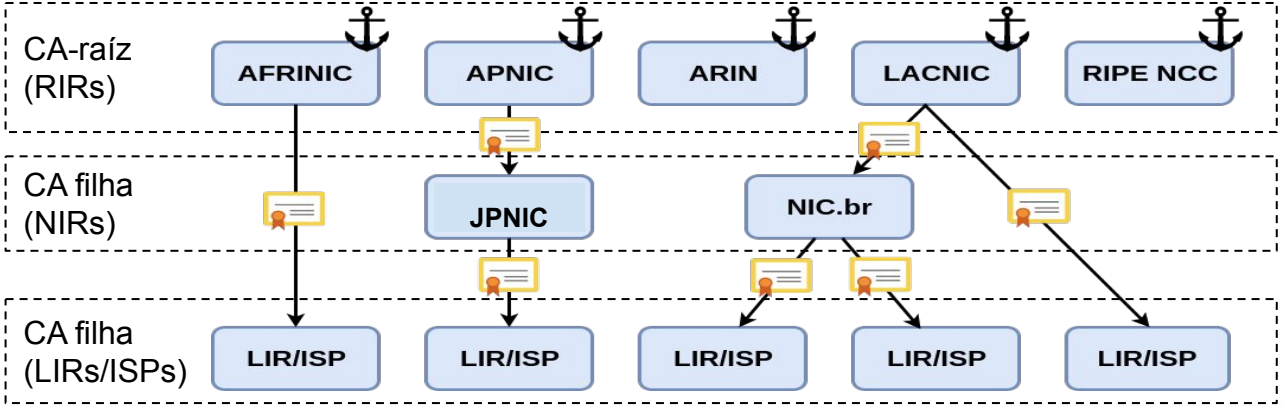
Modelo PKI

- Cadeias de certificação
  - CA (Certificate Authority) são entidades confiáveis e sua chaves públicas são amplamente conhecidas!
  - Usa-se a chave da CA raiz (auto-assinado) para assinar outras chaves na cadeia até as entidades finais ou End Entities (EEs).
  - Importante a proteção das chaves mais críticas (mais próximas da raiz).



Cadeia de certificação do RPKI

- RIRs -Trust Anchor
  - Confiabilidade implícita
  - Certificados auto-assinados
  - Certificam somente os recursos de sua própria hierarquia



Autoridade Certificadora

- CAs Certificate
  - Organizações que distribuem recursos de numeração
  - Detentores de recursos de numeração
- Certificados das End Entities
  - Validam os documentos assinados contidos no repositório RPKI
  - Cada certificado assina um documento

Cadeia de certificação do RPKI

- Cada RIR pode ser uma fonte autoritativa para a alocação de recursos:
  - Delegação de endereços IPs (IPv4 e IPv6)
  - Delegação de ASNs
- Funcionam como CA do par IPs-ASN e da chave pública do AS

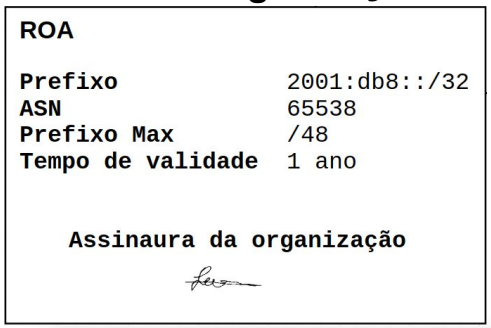
ROAs

- Route Origin Authorisation
  - Objeto assinado

“Eu autorizo o ASN XXXX a originar esse prefixo”.

- Elementos principais:
  - Nome da ROA
  - Número do AS (ASN)
  - Prefixo alocado e máximo permitido
  - Tempo de validade
  - Assinatura da organização
  - Responsável pelos recursos

ROA da organização



ROAs

- Todos os prefixos anunciados devem estar cadastrados em um ou mais ROAs
- Assinados e guardados em um repositório RPKI
  - Certificado contendo recursos de numeração
  - Declarações da origem das rotas para esses recursos
- Cada ROA contém apenas um ASN
  - Prefixos podem possuir mais de um ROA

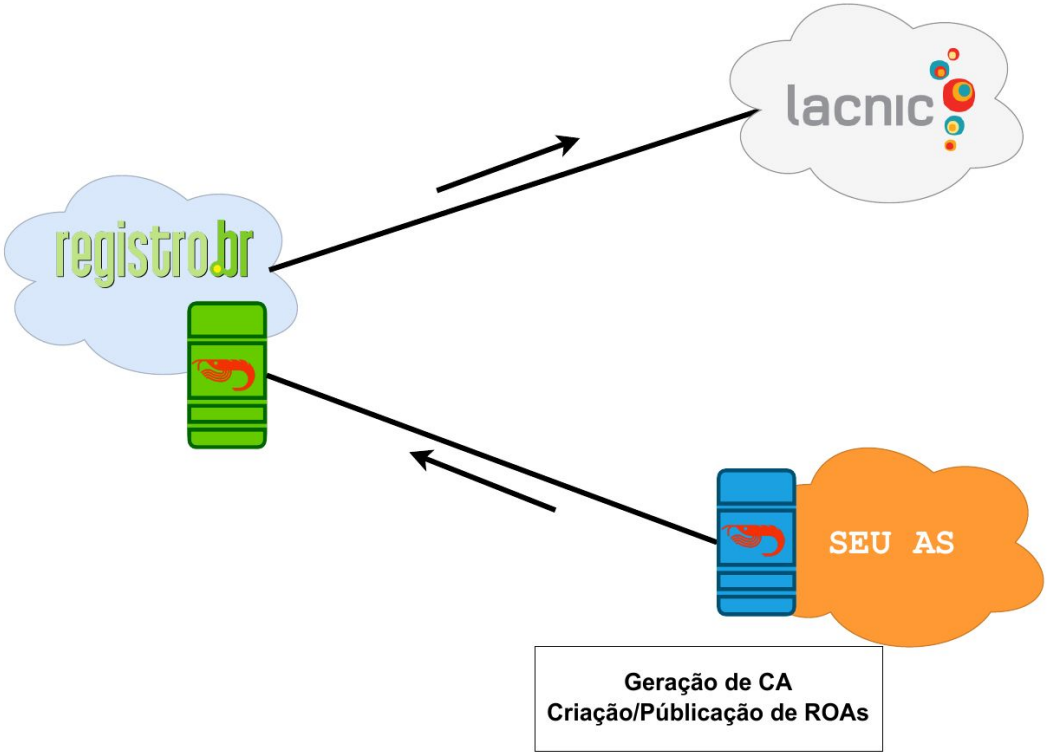
ROAs

- E se uma organização quiser alocar seus recursos para outros ASes?
- Duas opções:
  1. Gerar a ROA para os próprios anúncios do seu ASN
  2. Gerar um certificado CA para outra organização (e.g. AS cliente), então essa gera a própria ROA
- Se existir ROA para o prefixo, a origem da rota é validada
- Publicar ROA incorreta é pior do que não publicar!

Modos de operação no RPKI

- Existem dois modos de operação no RPKI:
  - Modo hospedado
    - LACNIC
  - Modo delegado
    - NIC.br

Modo Delegado



Modo Delegado

- Sistema distribuído de CAs
  - Foi desenhado para ser assim
- Facilita a automatização
- Centraliza o gerenciamento das ROAs na organização dona dos recursos
- Controle da chave privada pelo AS
- Permite delegar CAs filhos para clientes
- AS têm mais autonomia no RPKI

Modo Delegado

- Protocolo UpDown
  - Geração e validação do repositório
  - Cada CA armazena a própria chave privada
  - Envia seus certificados para assinatura da CA pai
  - Publicação de certificados e ROAs
    - Repositório próprio ou de terceiros

Modo Delegado

- O que eu preciso?
  - **Software CA**
    - Krill - NLnet Labs
  - **Servidor de publicação**
    - Servidor proprio (alta disponibilidade)
    - Servidor de terceiros (NIC.br)

O que é o Krill?

- Software open source
  - Criação, gerenciamento, publicação de CAs e ROAs
- Possui repositório próprio, mas permite a utilização de repositório de terceiros
- Funciona por linha de comando e por interface gráfica para usuário

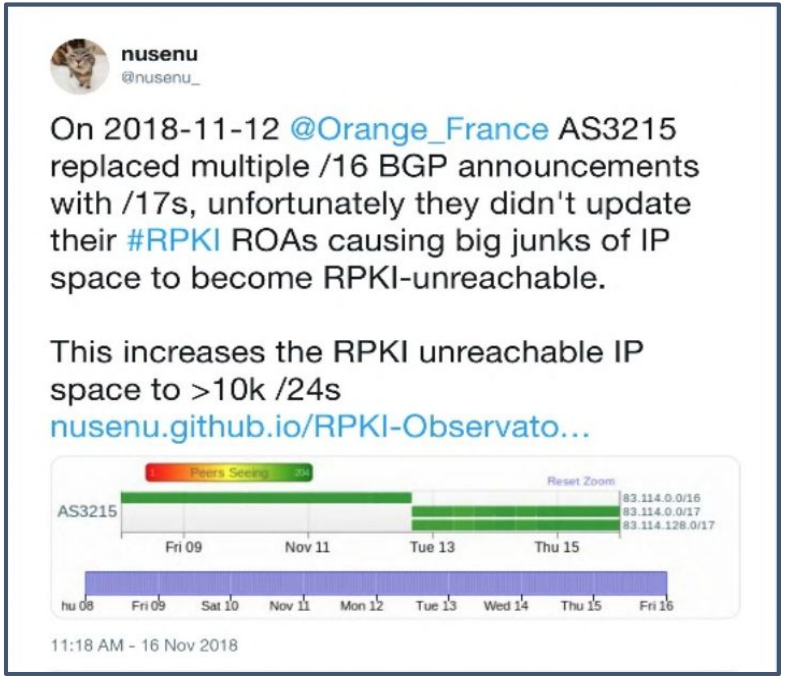
Servidor Krill?

- **É de extrema importância manter seu servidor Krill sempre ativo!**
  - Documentos do RPKI possuem prazo de validade
  - Atualizações automáticas e periódicas desses documentos são feitas pelo protocolo UpDown
  - Se o servidor Krill ficar inacessível e os documentos expirarem, as rotas válidas podem passar a ser consideradas desconhecidas

Manutenção é essencial!

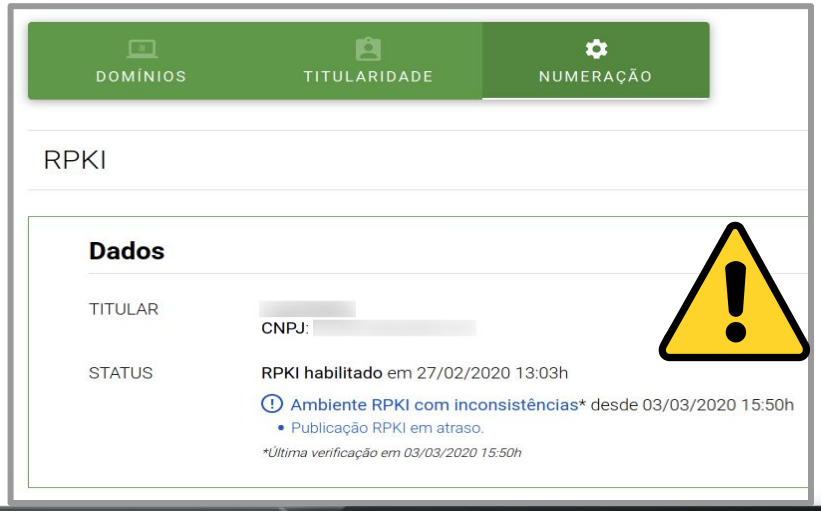
Não esqueça do RPKI!

Atualize as ROAs quando mudar os anúncios!



Monitoramento do RPKI pelo Registro.br

Para ajudar nessa fase inicial da implantação do RPKI, o Registro.br disponibilizou um serviço de monitoramento que informa se suas configurações de RPKI estão corretas.



Laboratório Krill

Obrigado!!!

Equipe de cursos do CEPTRO.br

cursosceptro@nic.br

ipv6@nic.br

nic.br cgi.br

www.nic.br | www.cgi.br