

# **RPKI**

## **Resource Public Key Infrastructure**

ceptro.br nice.br cgi.br

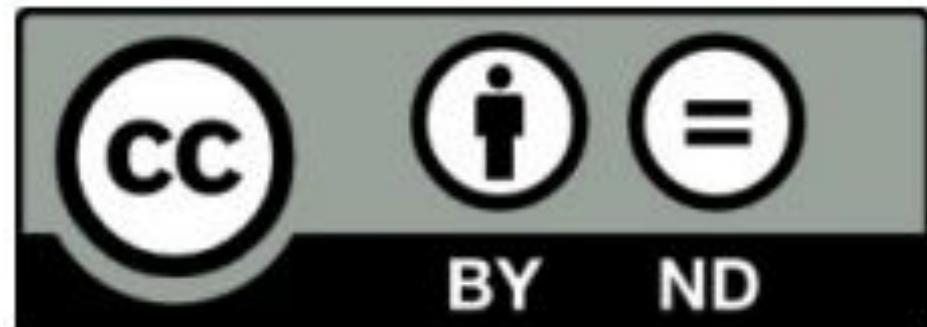
# Licença de uso do material

Esta apresentação está disponível sob a licença

**Creative Commons**

**Atribuição - Sem Derivações 4.0 Internacional (CC BY-ND 4.0)**

<https://creativecommons.org/licenses/by-nd/4.0/legalcode.pt>



**Você tem o direito de:**

- **Compartilhar** - copiar e redistribuir o **material** em qualquer suporte ou formato para qualquer fim, **mesmo que comercial**.
- *O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.*

**De acordo com os termos seguintes:**

- **Atribuição** - Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso. Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do **Curso de Boas Práticas Operacionais para Sistemas Autônomos do CEPTRO.br/NIC.br**, e que os originais podem ser obtidos em <http://ceptro.br>. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.
- **Sem Derivações** - Se você remixar, transformar ou criar a partir do material, você não pode distribuir o material modificado.

Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: [info@nic.br](mailto:info@nic.br).



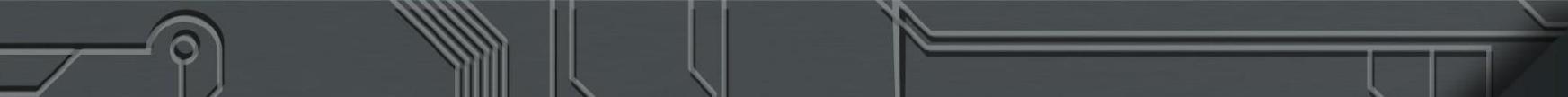
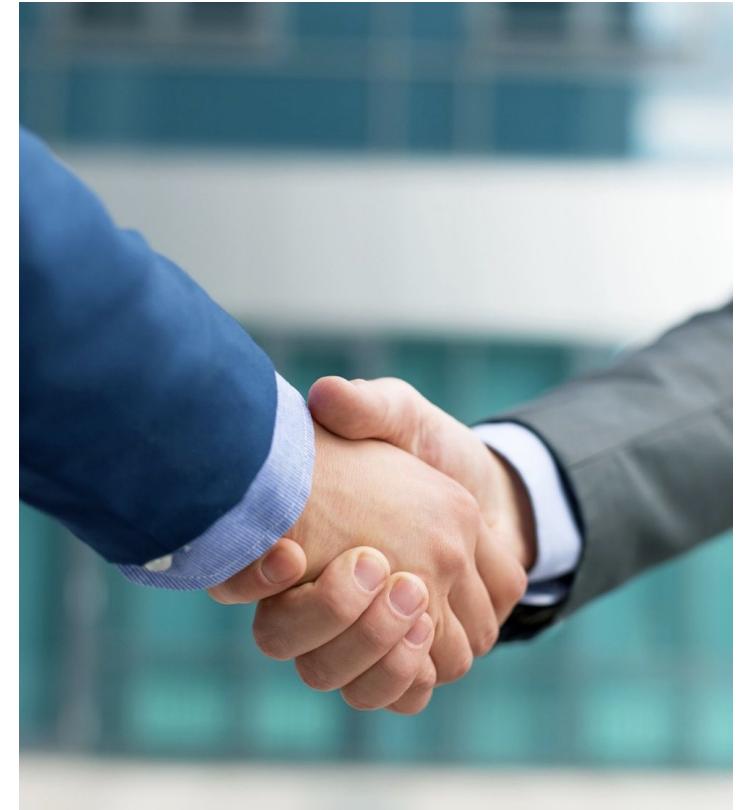
# BGP Hijacking

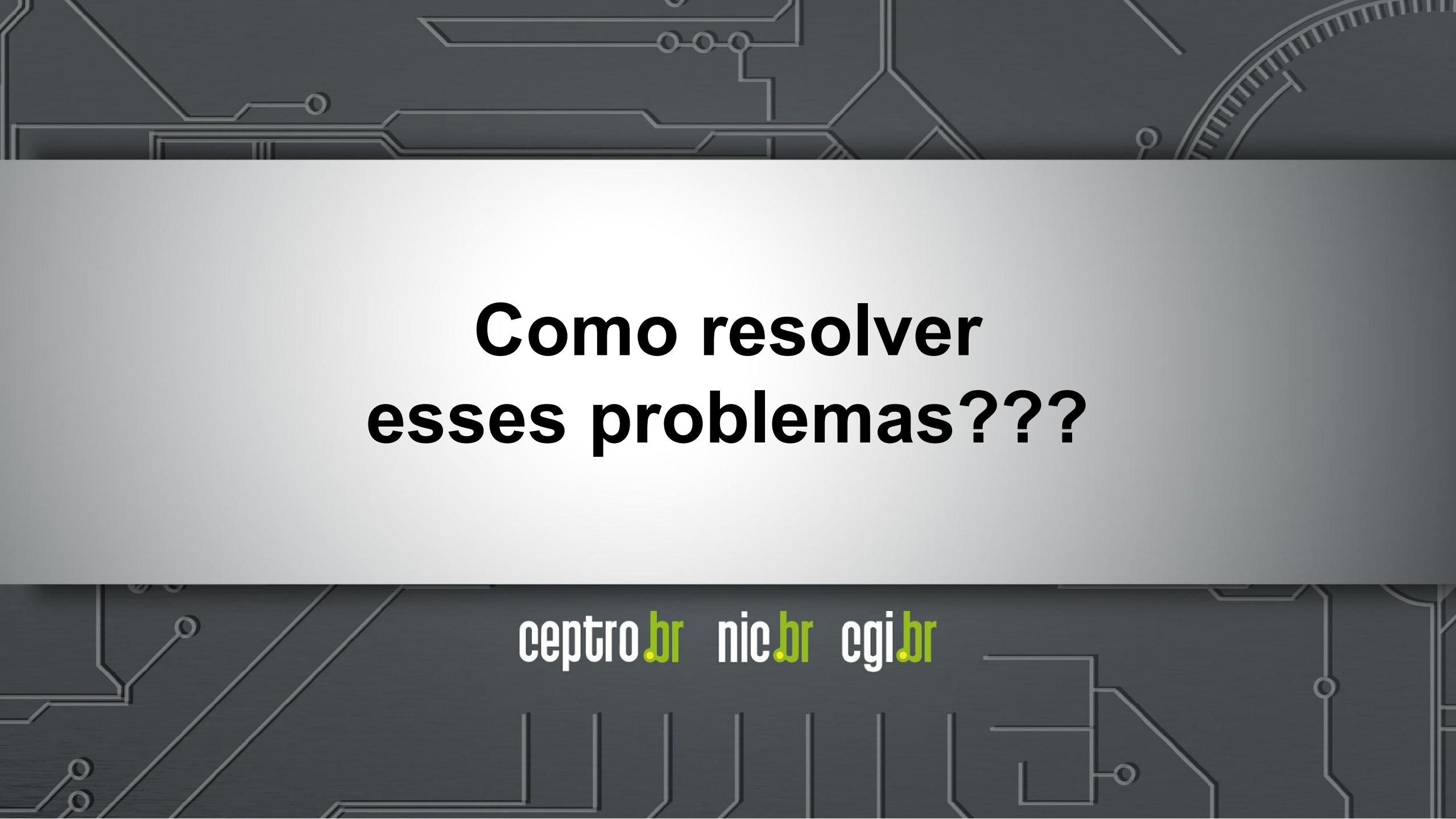
- Anúncio de prefixos não autorizados
  - "Sequestro do prefixo"
- Motivos:
  - Erro de configuração
  - Fat finger
  - Proposital



# Por que isso acontece?

- A Internet funciona com base na cooperação entre Sistemas Autônomos (ASes):
- É uma “*rede de redes*”
- São mais de **100.000** redes diferentes, sob gestões técnicas independentes
- A estrutura de **roteamento BGP** funciona com base em cooperação e confiança
- O BGP não tem validação dos dados





# Como resolver esses problemas???

ceptro.br nic.br cgi.br



MANRS



# *Resource Public Key Infrastructure (RPKI)*

faz parte do  MANRS!!!

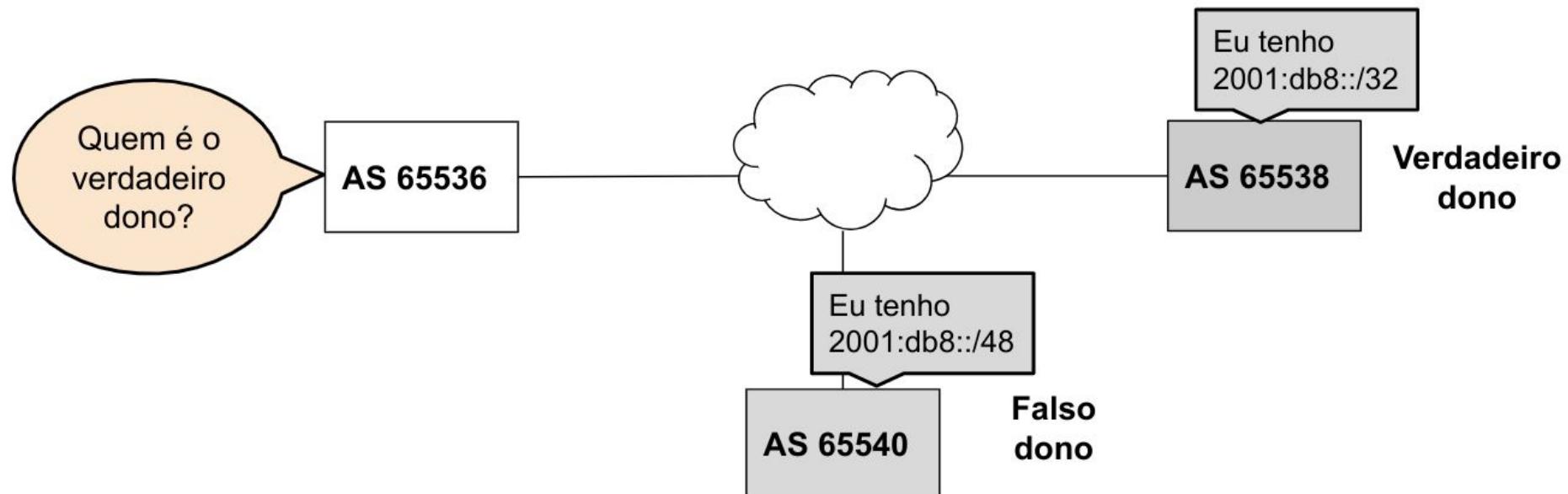
# O que é RPKI?

- Estrutura desenvolvida para validar recursos de numeração
  - ASN e Prefixos IPs
    - Alocados
  - Utilizado no BGP
- Previne os problemas de BGP Hijacking
- **A colaboração de todos os ASes é essencial!!!**

# O que é RPKI?

- ROTAS:

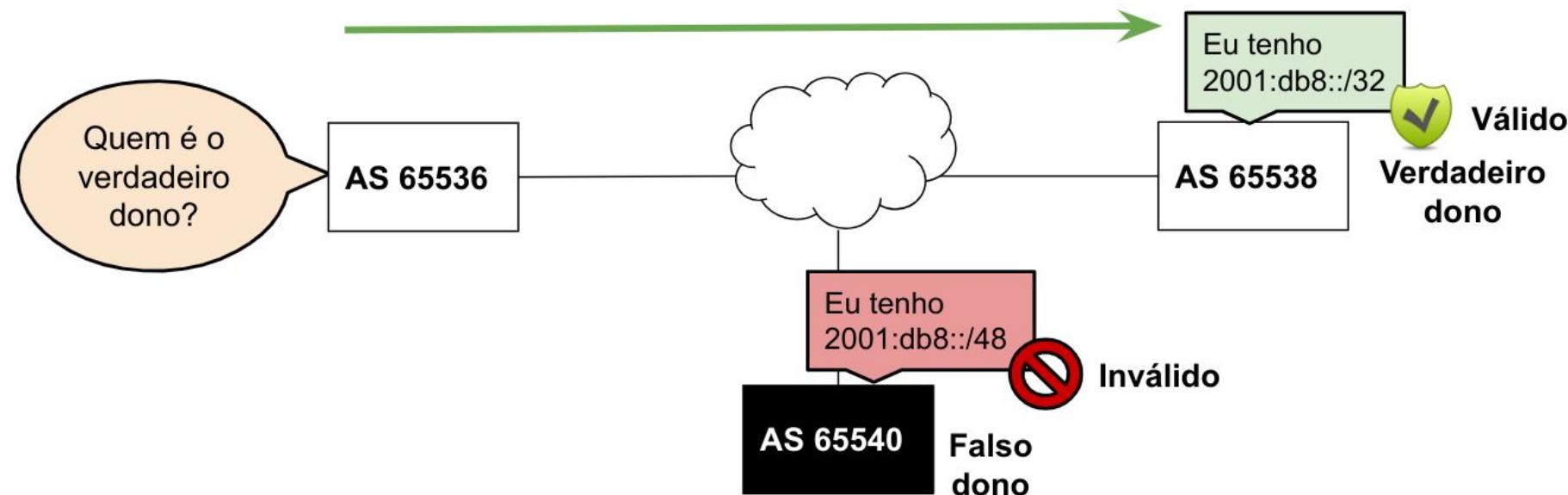
- **2001:db8::/32 ... 65538 i**
- **2001:db8::/48 ... 65540 i**



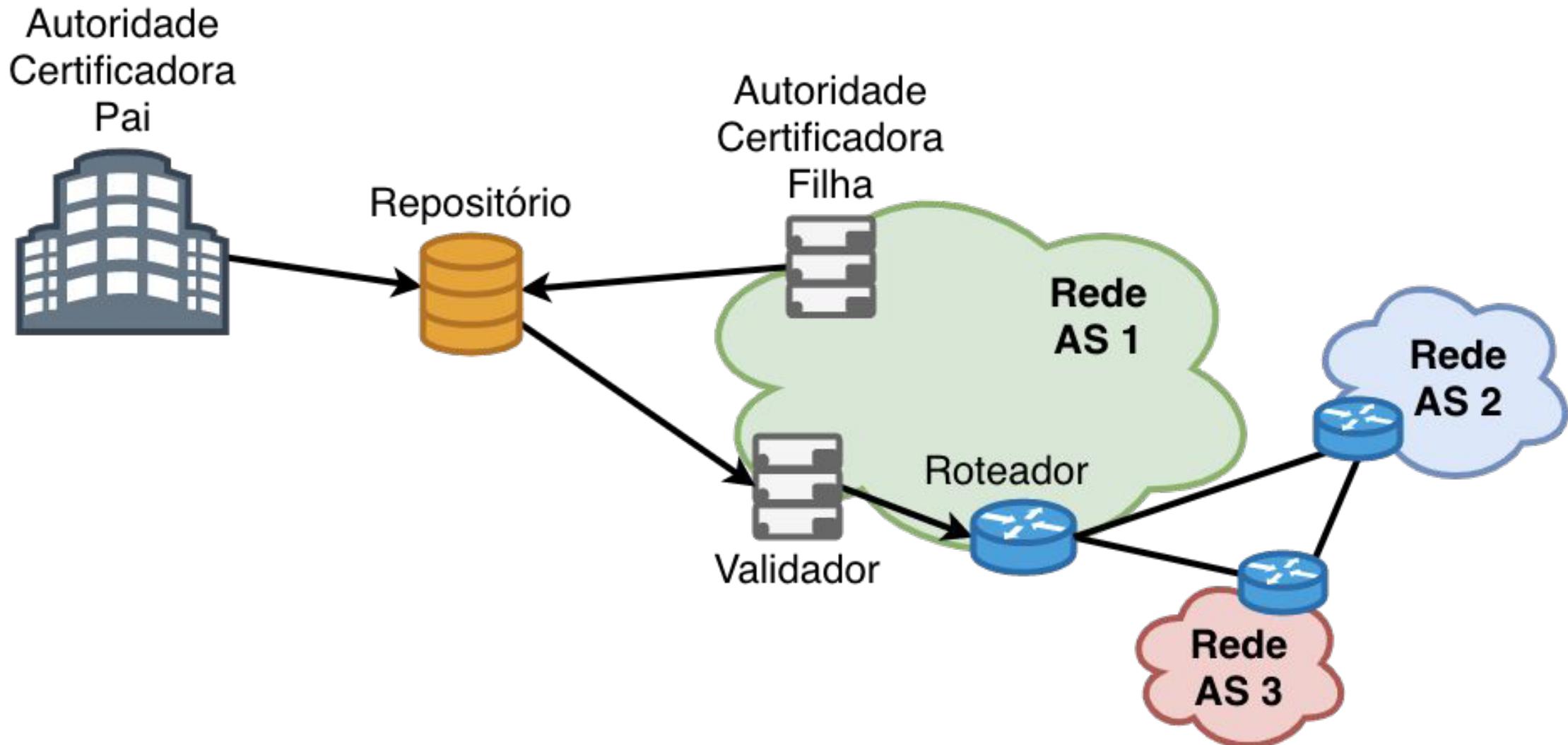
# O que é RPKI?

- ROTAS:

- **2001:db8::/32 ... 65538 i**
- **2001:db8::/48 ... 65540 i**



# Estrutura do RPKI



# Estrutura do RPKI

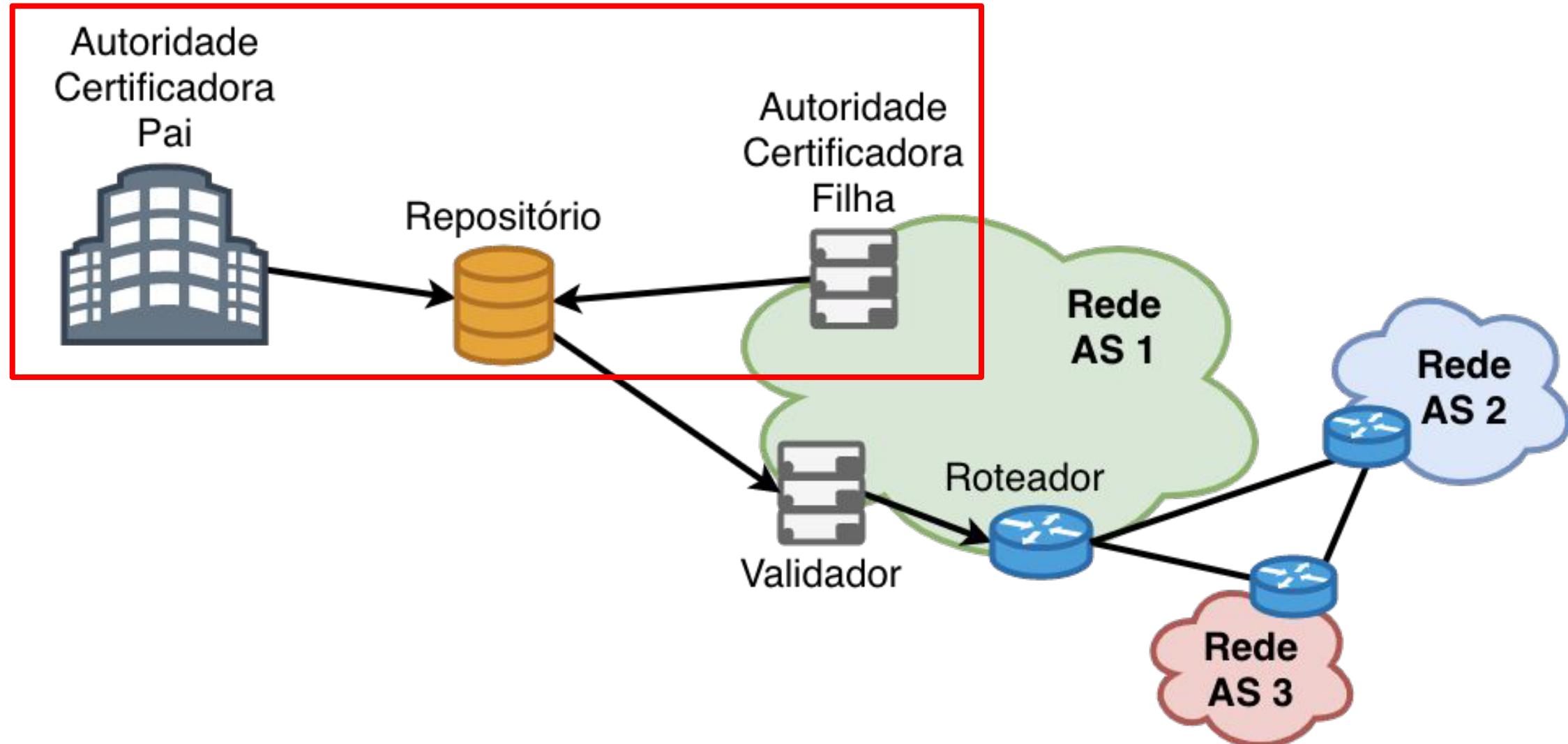
- Duas partes:
  - Certificação de recursos
    - Anunciar os prefixos no RPKI
    - Qualquer um que possuir recursos de IP pode aderir
  - Validação da Origem
    - Consultar prefixos anunciados no RPKI
    - Necessita uso de roteador compatível

# **Parte I:**

# **Certificação de Recursos**

ceptro.br nic.br cgi.br

# Certificação de Recursos



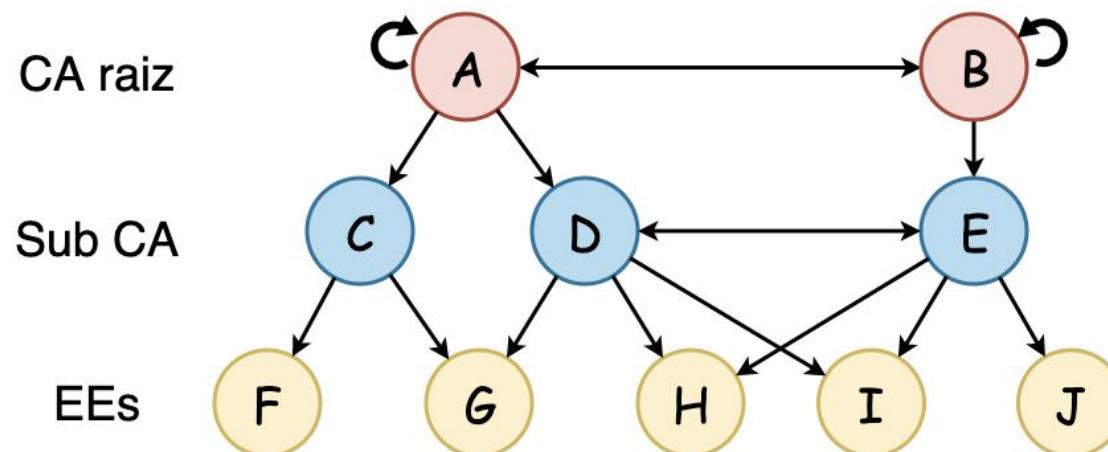
# Certificação

- 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**

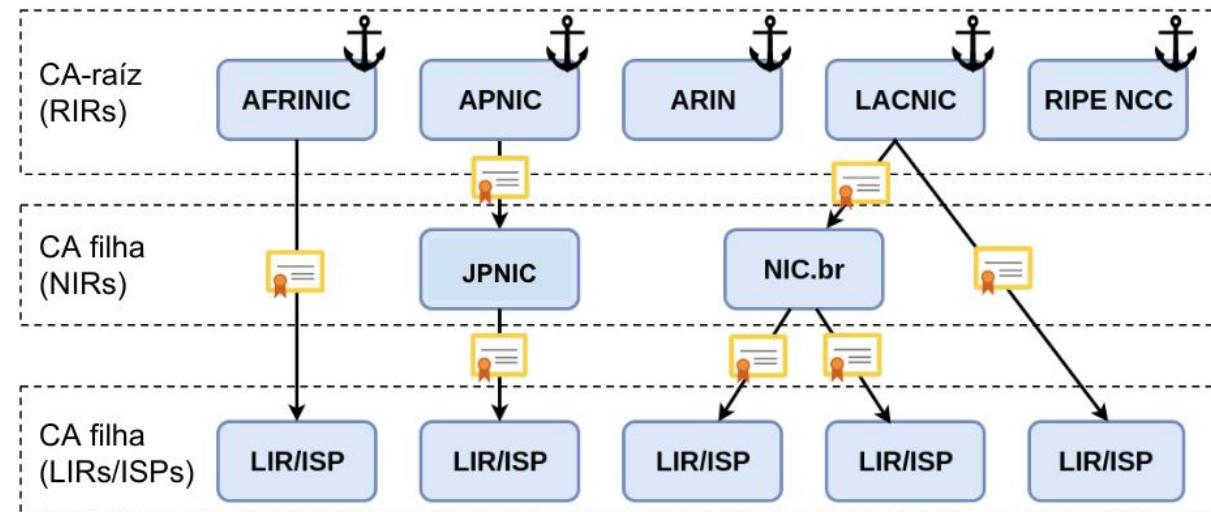
- CA (Certificate Authority) são entidades confiáveis e sua chaves públicas são **amplamente conhecidas!**
- Usa-se a chave da CA raiz (auto-assinado) para assinar outras chaves na cadeia até as entidades finais ou End Entities (EEs).
- Importante a proteção das chaves mais críticas (mais próximas da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

**ROA**

<b>Prefixo</b>	2001:db8::/32
<b>ASN</b>	65538
<b>Prefixo Max</b>	/48
<b>Tempo de validade</b>	1 ano

**Assinatura 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!

# Como verificar existência de ROAs

The screenshot shows the Cloudflare RPKI Route Validator interface. At the top, there's a navigation bar with tabs: Statistics, Route Validator (which is active), BGP Routes, and Resource Explorer. Below the tabs, there are input fields for PREFIX: 200.160.0.0/20 and ASN: 22548. A large green box displays the validation results: "Validating route 200.160.0.0/20 from origin AS22548" and "✓ Valid". It also mentions "1 covering ROA found". Below this box, there's a section titled "Covering ROAs:" with a table:

Trust Anchor	Prefix	Max Length	ASN	Expiration	Match
LACNIC	200.160.0.0/20	24	22548	in 5 months	✓

RPKI Portal - Route Validator: <https://rpki.cloudflare.com/>

# Como verificar existência de ROAs

The screenshot shows the Routinator Prefix Check interface. On the left, there's a sidebar with options like ASN Lookup, Data Freshness, and RPKI status. The main area is titled "VALIDATION" and shows results for the prefix 200.160.0.0/20 from AS22548, which is marked as "VALID". It also states "At least one VRP Matches the Route Prefix". Below this, a table lists "Matched VRPs" with columns for Prefix, Max Length, and ASN. A section for "RELATED PREFIXES" shows the best matching prefix from allocations and BGP, with a table for BGP Origin ASN and RPKI Status.

Prefix or IP Address (optional)  
200.160.0.0/20

Origin ASN (optional)  
AS22548

Validate

ASN Lookup ?  
 Validate Prefixes for ASN found in BGP

Origin ASN Validation Source ?  
 Longest Matching Prefix  
 Exact Match only

Data Freshness ?  
RPKI 2025-10-22 17:18:55 UTC  
(6 minutes ago)

VALIDATION

Results for 200.160.0.0/20 - AS22548 VALID

At least one VRP Matches the Route Prefix

Matched VRPs	Prefix	Max Length	ASN
	200.160.0.0/20	24	AS22548

RELATED PREFIXES

Best Matching Prefix in Allocations and/or BGP REGION LACNIC

Prefix	BGP Origin ASN	RPKI Status
> 200.160.0.0/20 ALLOCATED	AS22548	<span style="background-color: #c8f7e4; border: 1px solid #2e71a1; padding: 2px 5px; border-radius: 5px;">VALID</span>

> 48 allocated to the same organization REGION LACNIC

Routinator - Prefix Check: <https://rpki-validator.ripe.net/ui/>

# Visualizando uma ROA

The screenshot shows the Cloudflare RPKI Resource Explorer interface. At the top, there are navigation links: Statistics, Route Validator, BGP Routes, and Resource Explorer (which is active). Below these are search fields for KEY ID, TRUST ANCHOR, ASN, PREFIX, and PREFIX MATCH (with options for Less Specific and More Specific).

The main area has two tabs: Resource List (active) and Hierarchical View. The Resource List tab shows a table with one row of data:

ASN	Prefix	Max Length	IP Family	Trust Anchor	Emitted	Expiration
AS22548	200.160.0.0/20	/24	IPv4	LACNIC	3/17/2025	in 5 months

Below the table, detailed information about the ROA is provided:

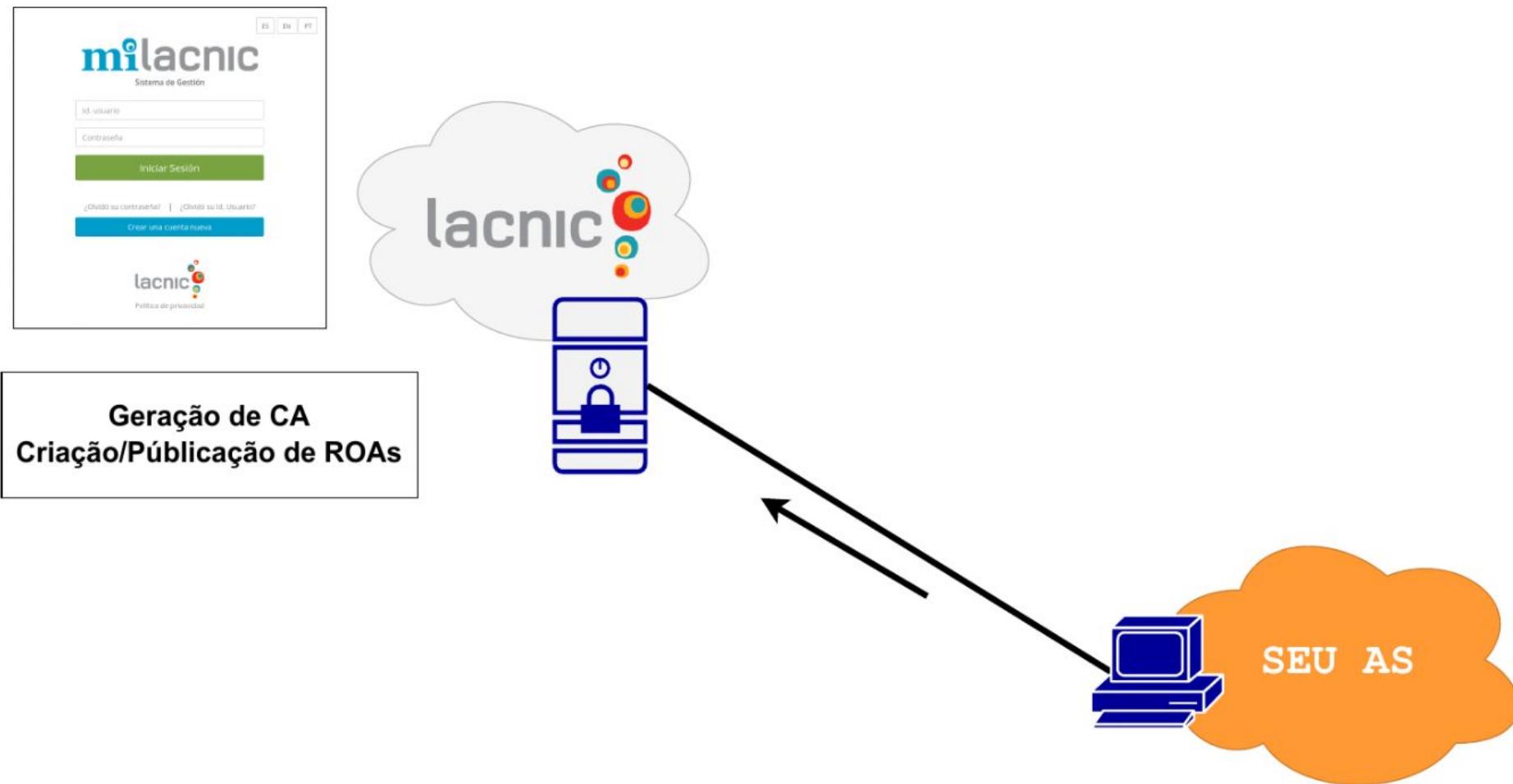
**Prefix:** 200.160.0.0/20  
**Max Length:** /24  
**ASN:** 22548  
**Emitted:** Mon, 17 Mar 2025 17:44:01 GMT  
**Validity:** Mon, 17 Mar 2025 17:39:01 GMT - Mon, 16 Mar 2026 17:44:01 GMT  
**Trust Anchor:** LACNIC  
**Name:** 3082010A0282010100CF8B50CF4B206EFB7C79AB956F8ACC25F41A265D816F45C0722AEDA037B0901934EAC9971D2FC9BCA9DCDB4DBD35D3F3F5990B915E6009F972D3141E04806491071CEE3C4CB682C8C107AE9B8DF49092183F41E343FF1BB9D3520D5C9F822271  
**Key:** ad10d9774dae626fac7329dad131f8ae903c4d9e

RPKI Portal - Resource Explorer: <https://rpki.cloudflare.com/?view=explorer>

# Modos de operação no RPKI

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

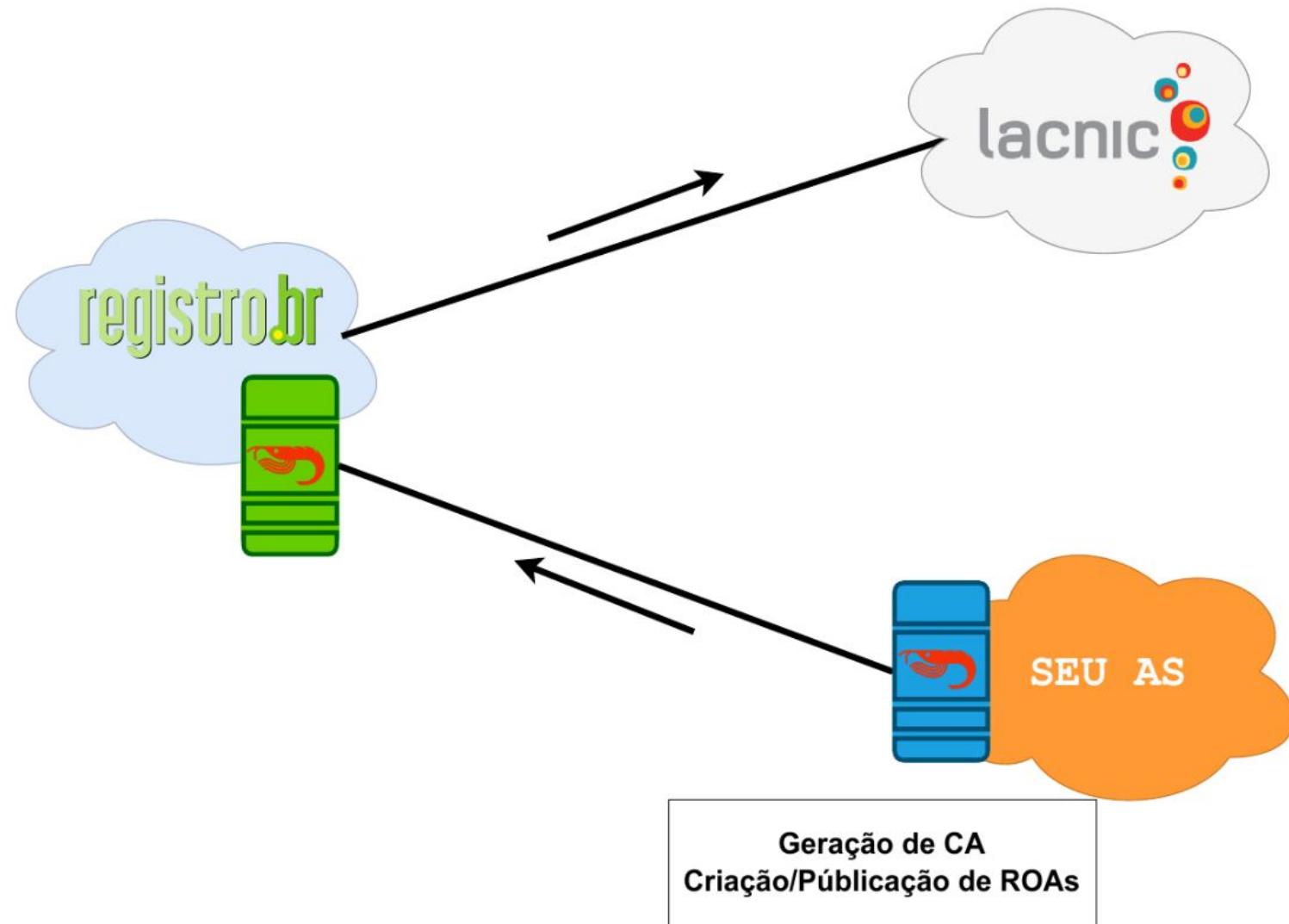
# Modo Hospedado



# Modo Hospedado

- Incentivar a adoção do RPKI
- **RIRs:**
  - Emitem e armazenam os certificados de recursos
  - Armazenam as chaves públicas e privadas
  - Oferecem interface web para os participantes
- AS depende do RIR para realizar suas ações no RPKI

# 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 tem 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

# Repositório RPKI

- Armazenam
  - **Resource Certification**
    - Certificados X.509 + extensão para IPs e ASNs (RFC 3779)
  - **Certificate Revocation List (CRL) - RFC 5280**
  - **Manifests (RFC 6486)**
    - Lista de documentos assinados por um AS
  - **Route Origin Authorisation (ROA) - RFC 6482**
    - Contém a lista de prefixos que podem ser anunciados por um ASN

# 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



# 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.

The image displays two side-by-side screenshots of a web-based RPKI monitoring tool. Both screenshots feature a top navigation bar with three tabs: 'DOMÍNIOS' (Domains), 'TITULARIDADE' (Ownership), and 'NUMERAÇÃO' (Numbering). The left screenshot, under the 'RPKI' heading, shows a 'Dados' (Data) section with a 'TITULAR' (Holder) field containing a blurred CNPJ number and a 'STATUS' (Status) field stating 'RPKI habilitado em 27/02/2020 13:03h' and 'Ambiente RPKI OK'. A large green circular icon with a white checkmark is overlaid on the right side of this screenshot. The right screenshot, also under the 'RPKI' heading, shows a similar 'Dados' section but with a yellow warning icon. It lists a 'TITULAR' with a blurred CNPJ and a 'STATUS' showing 'RPKI habilitado em 27/02/2020 13:03h'. Below this, a warning message states 'Ambiente RPKI com inconsistências\*' from '03/03/2020 15:50h' due to 'Publicação RPKI em atraso.' A small note at the bottom indicates the 'Última verificação em 03/03/2020 15:50h'.

# Manutenção é essencial!

**Não esqueça do RPKI!**

**Atualize as ROAs quando mudar os anúncios!**

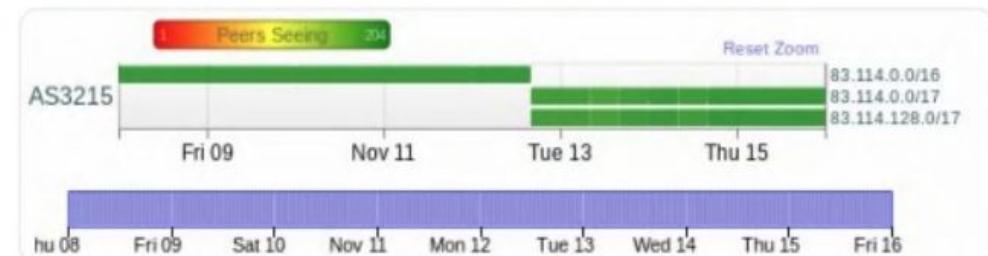


nusenu  
@nusenu\_

On 2018-11-12 @Orange\_France AS3215 replaced multiple /16 BGP announcements with /17s, unfortunately they didn't update their #RPKI ROAs causing big junks of IP space to become RPKI-unreachable.

This increases the RPKI unreachable IP space to >10k /24s

[nusenu.github.io/RPKI-Observato...](https://nusenu.github.io/RPKI-Observatory/)

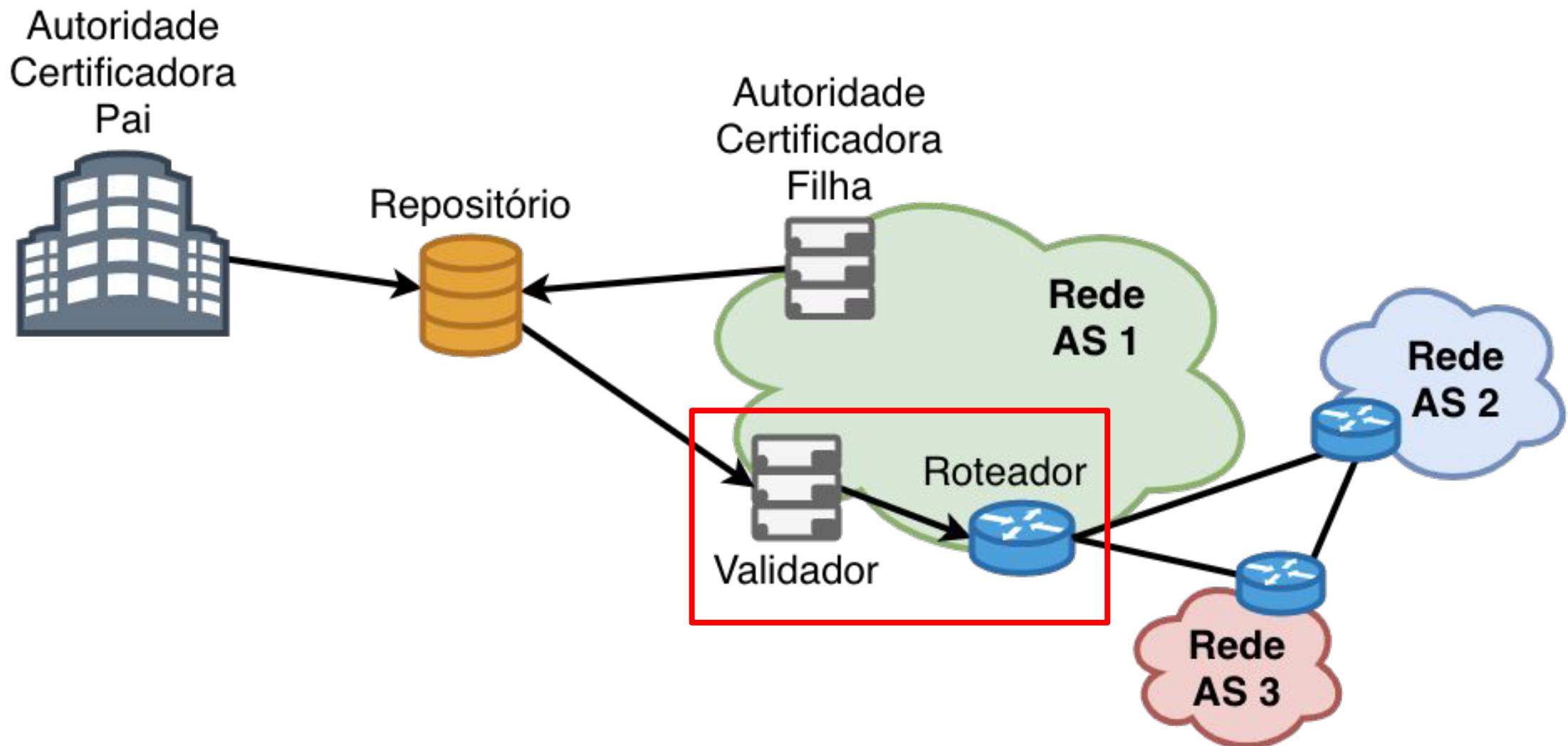


11:18 AM - 16 Nov 2018

# Parte II: Validação da Origem

ceptro.br nic.br cgi.br

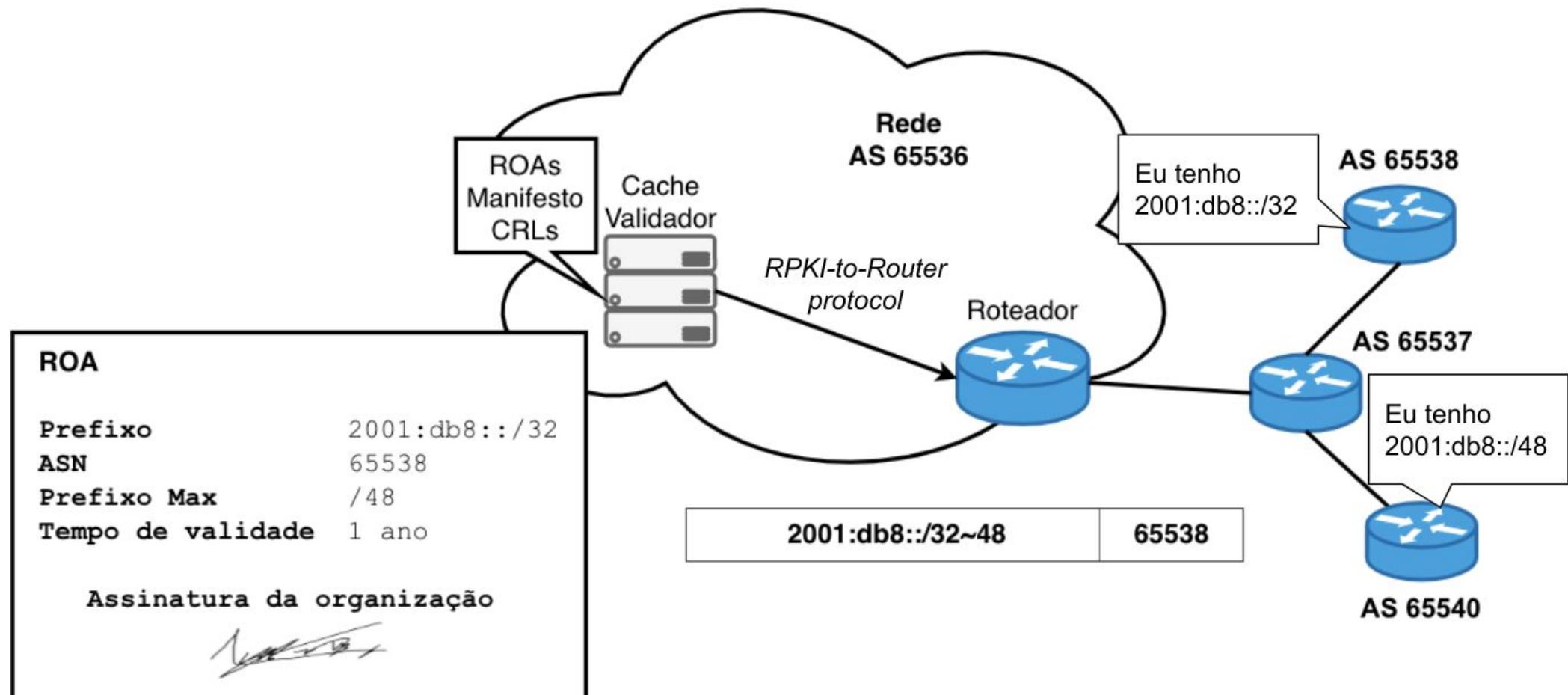
# Validação da Origem



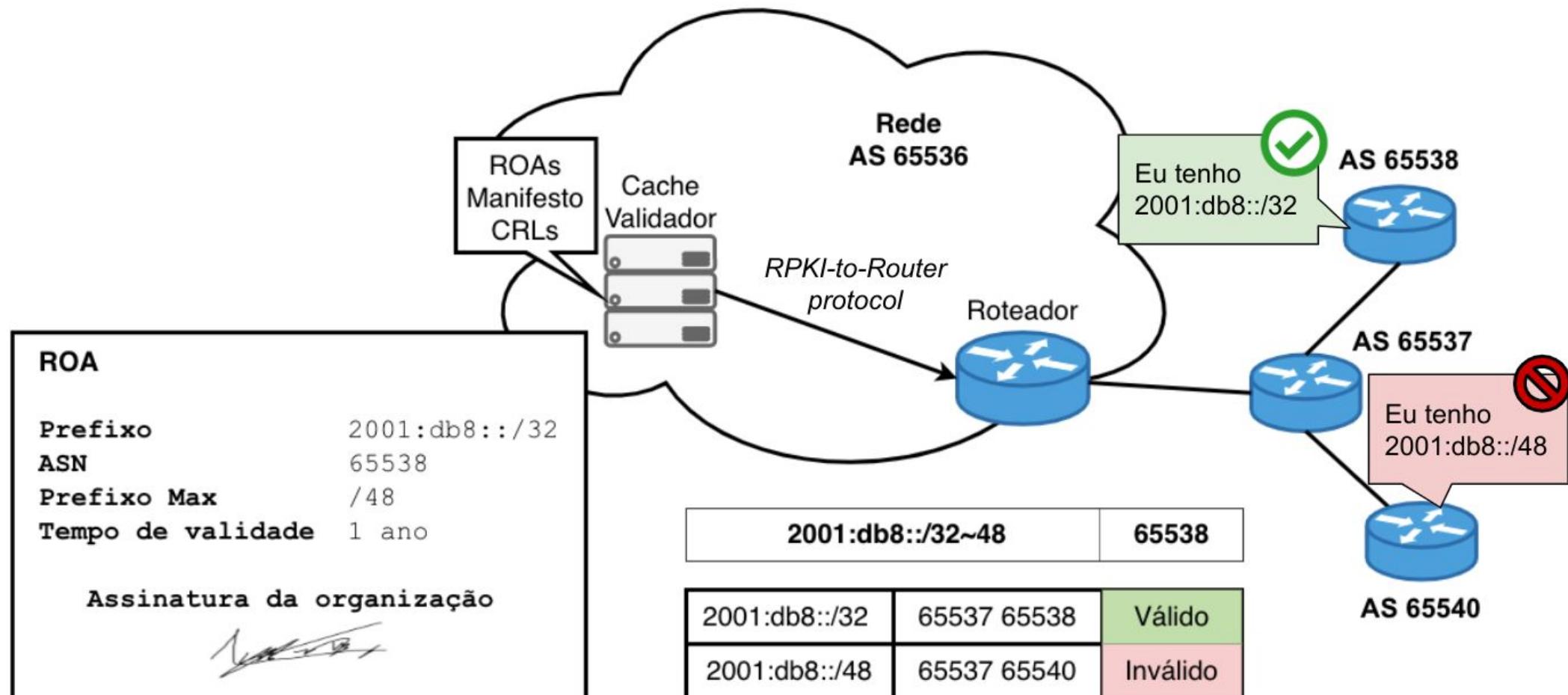
# Validação da Origem

- **Validador**
  - Validação dos objetos certificados
  - Software que acessa fontes confiáveis e cria um cache da informação validada
- **Roteador**
  - Validação das rotas
  - BGP habilitado para usar o RPKI
  - Obtém informações do validador e utiliza para influenciar o roteamento

# Validação da Origem



# Validação da Origem



# Roteador

Exemplo:

	<b>AS de Origem</b>	<b>Prefixo</b>	<b>Prefixo Max.</b>
ROA	65536	10.0.0.0/16	/18

Válida	65536	10.0.128.0/17
Inválida	65536	10.0.0.0/24
Desconhecido	65540	10.0.0.0/8

# Validador

- Existem vários softwares disponíveis:
  - **ROUTINATOR**
  - FORT (LACNIC)
  - **RIPE validator**
  - RTRlib (bird, FRR, Quagga...)
  - **OctoRPKI & GoRTD (Cloudflare)**
- Trust Anchor Locator (TAL) já vem incorporados
  - Localizador para os 5 RIRs

# Roteador

- Recebem VRPs do validador e utilizam para tomar decisões de roteamento
- Uma rota pode ser classificada como:
  - **Válida:** A origem e o prefixo máximo estão de acordo com a informação do ROA
  - **Inválida:** A informação não está de acordo com o ROA
  - **Desconhecido:** Não existe ROA para o prefixo verificado

# Roteador

- Suporte a validação na origem
- **Hardware**
  - **Juniper**
    - Junos versão 12.2 e superiores
  - **Cisco**
    - IOS release 15.2 e superiores
    - Cisco IOS/XR desde a 4.3.2
  - **Nokia**
    - Release R12.0R4 e superiores rodando no 7210 SAS, 7750 SR, 7950 XRS ou VSR.

# Roteador - Software

- Existem vários softwares com suporte a RPKI:
  - BIRD
  - OpenBGPD
  - FRRouting
  - GoBGP
  - VyOS

Fonte: <https://rpki.readthedocs.io/en/latest/rpki/router-support.html>



# Recomendações

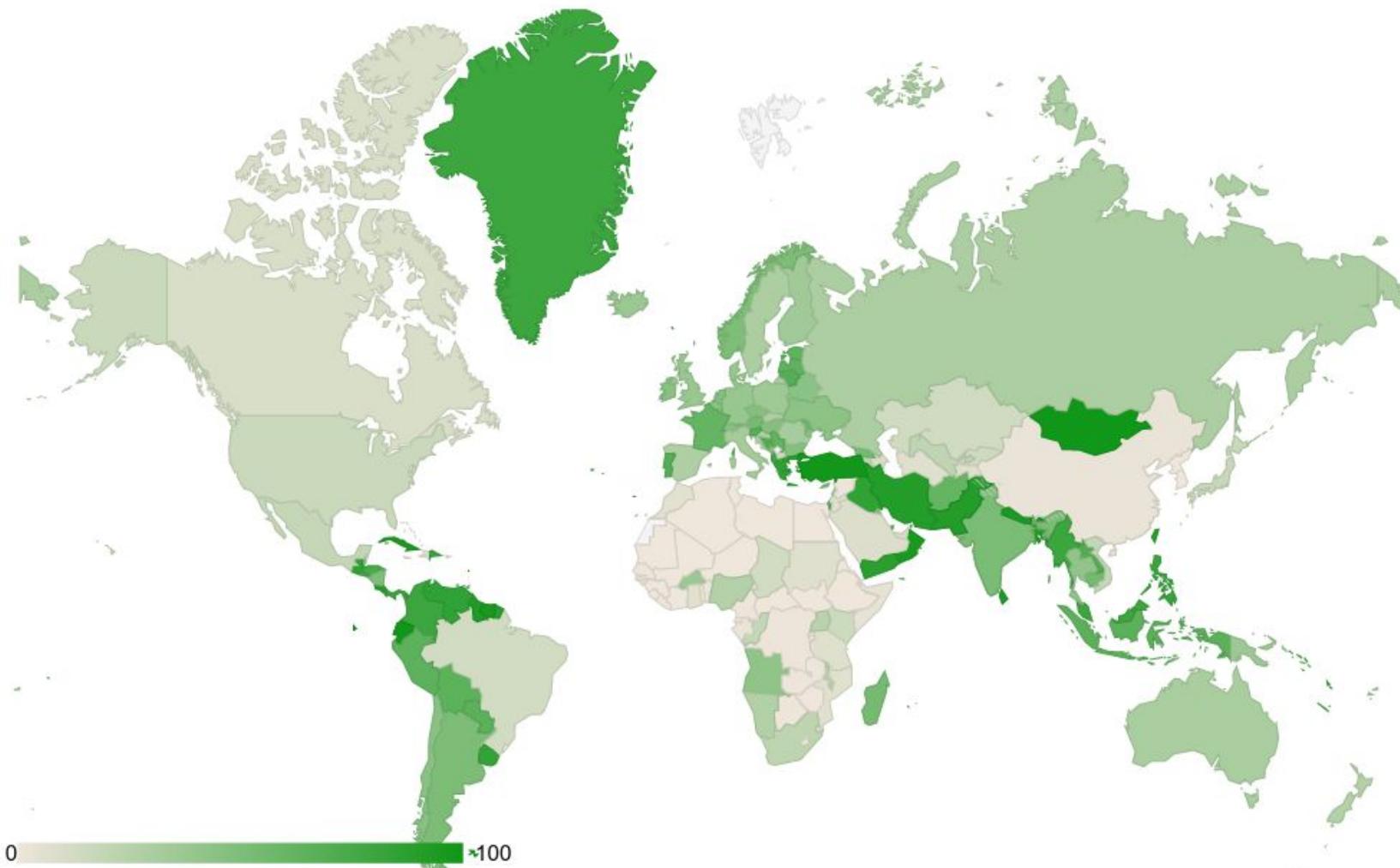
- Políticas de roteamento podem ser estabelecidas em cima da validação das rotas
  - Alterar preferências
  - Atribuir communities
  - Aplicar filtros

# Adoção do RPKI



Fonte: [https://monitor.fortproject.net/en/rpki\\_map](https://monitor.fortproject.net/en/rpki_map)

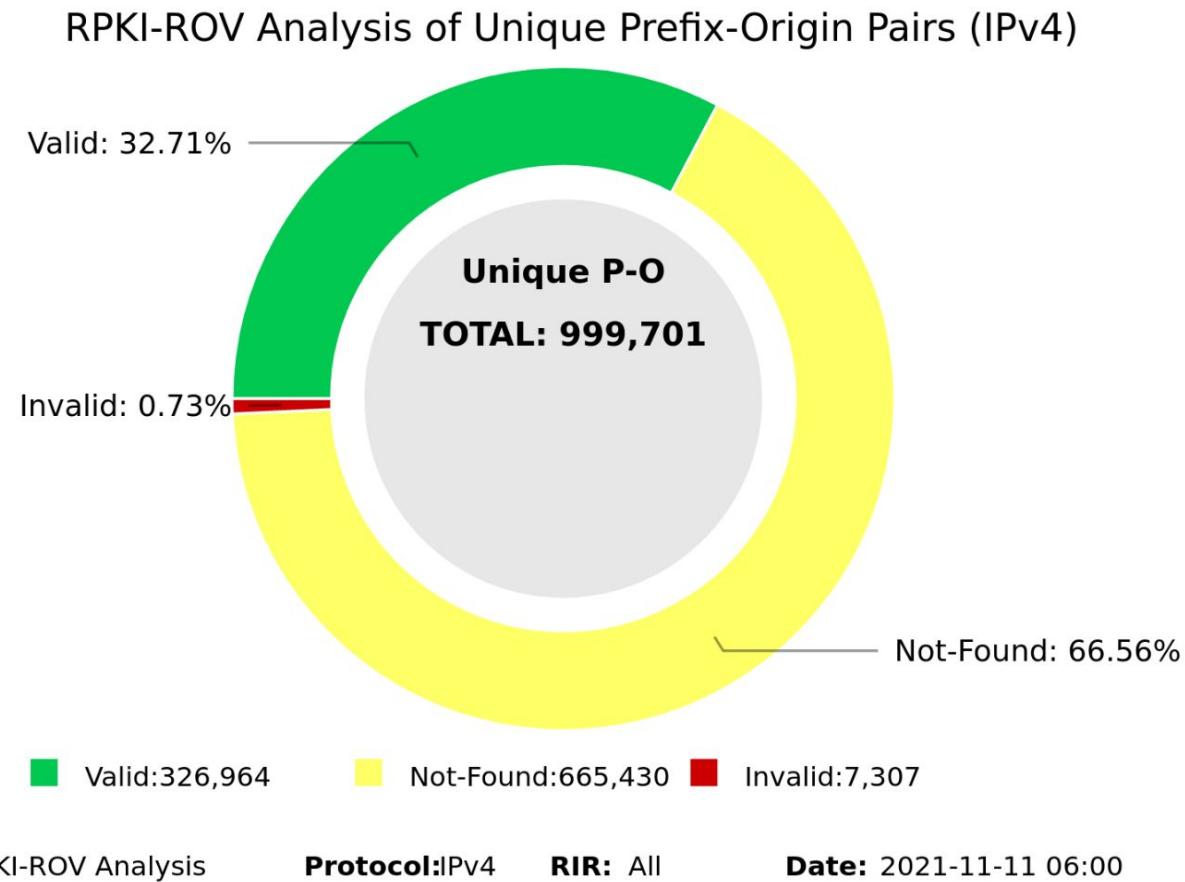
# Adoção do RPKI



Fonte: <https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html>

# Validação de Rotas

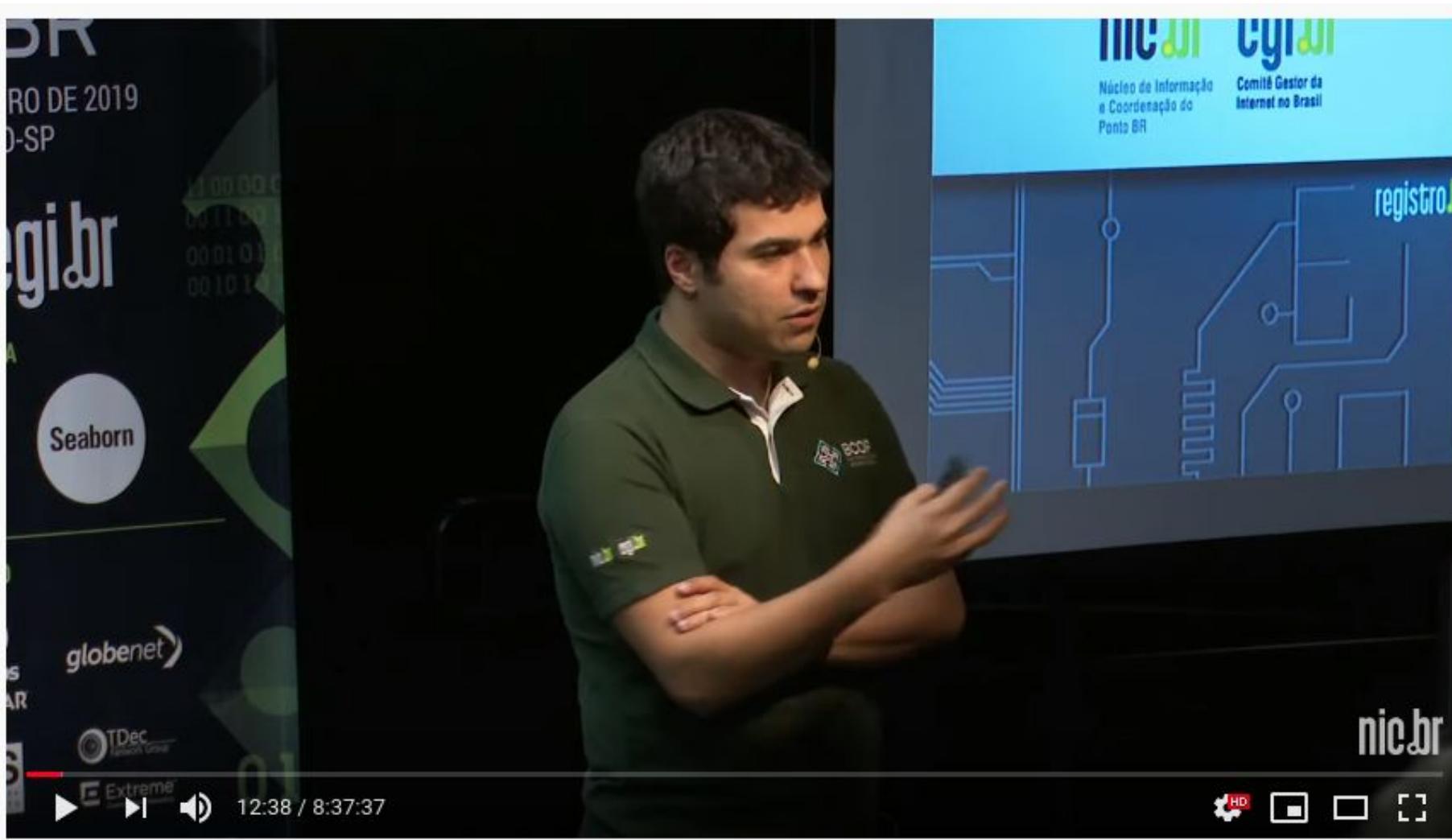
- Análise da tabela completa do BGP em relação aos prefixos anunciados nos RPKIs



Fonte: <https://rpki-monitor.antd.nist.gov/?p=0&s=0>



# Saiba mais



<https://www.youtube.com/watch?v=A6F3OswNyh8>

# Saiba mais



<https://www.youtube.com/watch?v=jSvMCjPoFME>



# Saiba mais



<https://www.youtube.com/watch?v=mvQ2GxslhKo>

# Dúvidas?



# Patrocínio Super Like



# Apoio de Mídia



editora  
**novatec**

# Obrigado!

CEPTRO.br Cursos: [cursosceptro@nic.br](mailto:cursosceptro@nic.br)

CEPTRO.br IPv6: [ipv6@nic.br](mailto:ipv6@nic.br)



nic.br cgi.br

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)