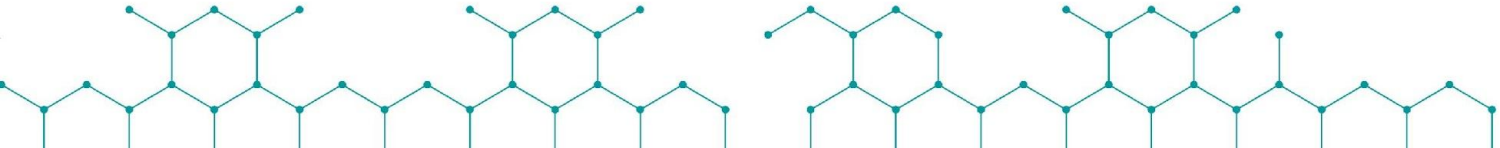
SEMANA DE CAPACITAÇÃO

Parceria

Realização

Segurança no roteamento com RPKI

Semana de Capacitação - Edição Especial On-line



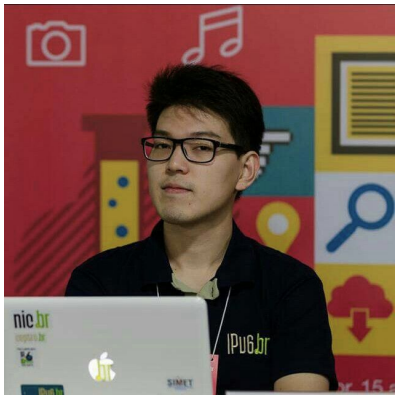
ceptro.br

Equipe de cursos do Ceptro.br

Instrutores

Eduardo Barasal Morales

Andrea Erina Komo

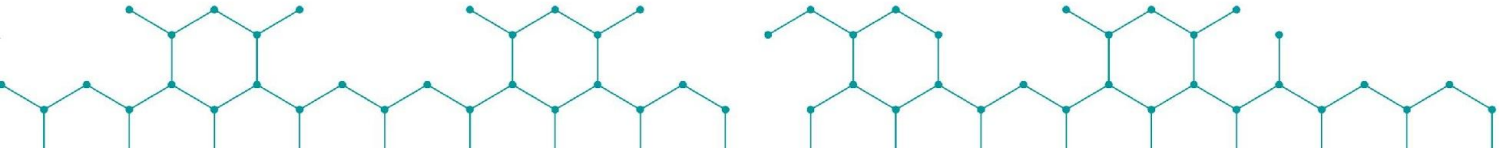


Tiago Jun Nakamura

ceptro.br

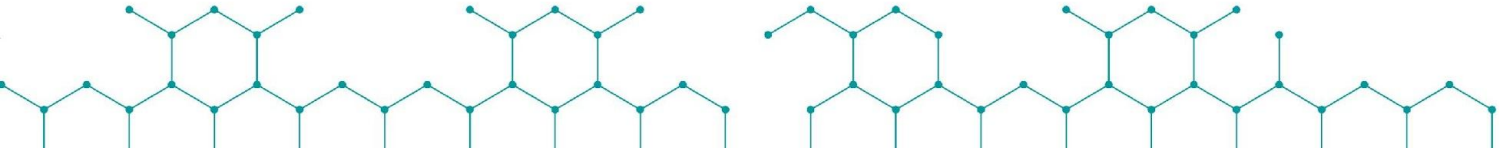
Agenda

- Roteamento BGP e vulnerabilidades de segurança
- Iniciativa MANRS
- Conceitos de segurança: Criptografia e Certificação digital
- RPKI
  - Certificação de recursos
    - Componentes do RPKI
    - Como participar e anunciar suas rotas no RPKI
  - Validação na origem
    - Como validar as rotas aprendidas
    - Políticas atribuídas às validações



ceptro.br

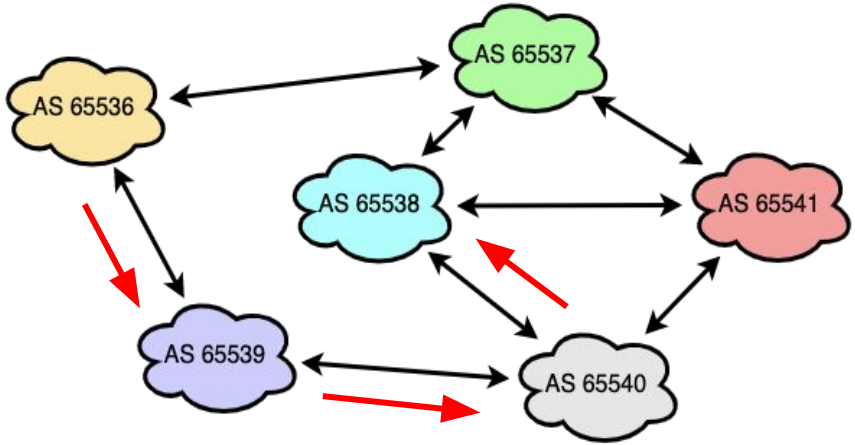
Conceitos de Roteamento



ceptro.br

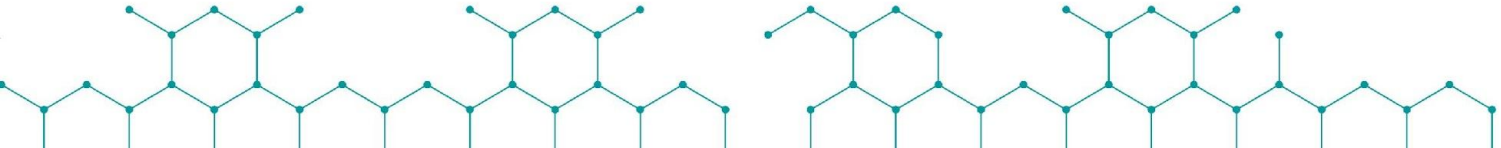
O que é BGP?

- Definida na RFC 4271 - *Border Gateway Protocol*
- Protocolo de roteamento usado para trocar informações dos caminhos entre as diferentes redes, isto é, redes sob gerência de **Sistemas Autônomos** ou ***Autonomous Systems*** **(AS)** distintos.

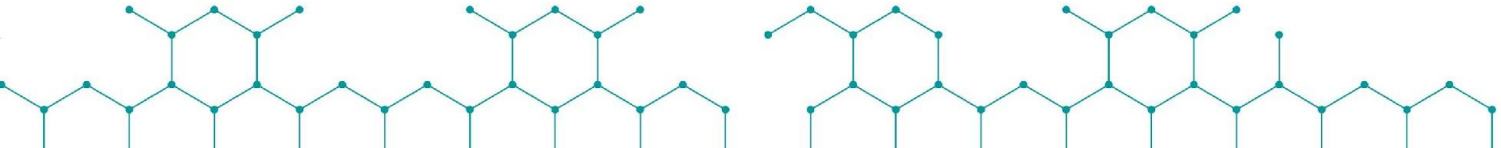


O que é BGP?

- Usado no *backbone* da Internet pelos ASes
- Após a configuração, confia-se que as rotas anunciadas estão corretas
- Tem várias opções diferentes para implementação de políticas de tráfego
  - Prefixo mais específico
  - Menor caminho
  - Políticas internas



Problemas de segurança em roteamento



ceptro.br

Ataques nos últimos anos

Mutually Agreed Norms for Routing Security (MANRS) 27 April 2018 EN ES

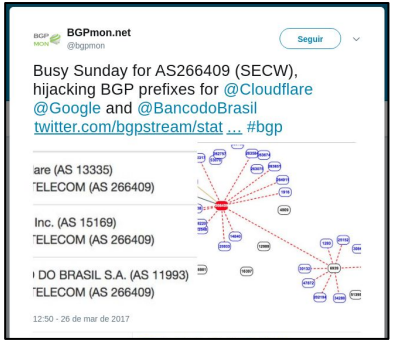
What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets

https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/

Mutually Agreed Norms for Routing Security (MANRS) 28 August 2017 EN FR ES

Google leaked prefixes – and knocked Japan off the Internet

https://www.internetsociety.org/blog/2017/08/google-leaked-prefixes-knocked-japan-off-internet/



https://twitter.com/bgpmon/status/846087079763177472

Mutually Agreed Norms for Routing Security (MANRS) 15 November 2018

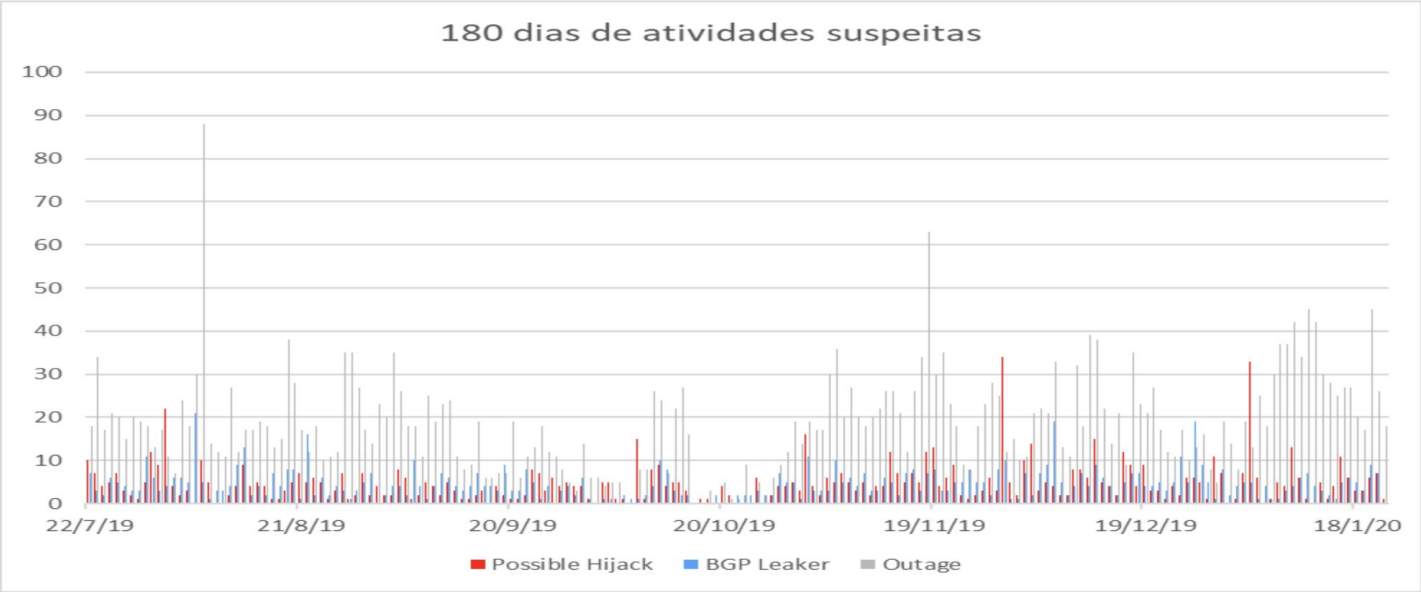
Route Leak Causes Major Google Outage

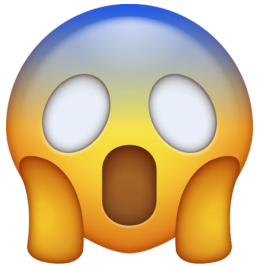
https://www.internetsociety.org/blog/2018/11/route-leak-caused-a-major-google-outage/

https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/

ceptro.br

Nenhum dia sem um incidente!!!





Fonte: https://bgpstream.caida.org/

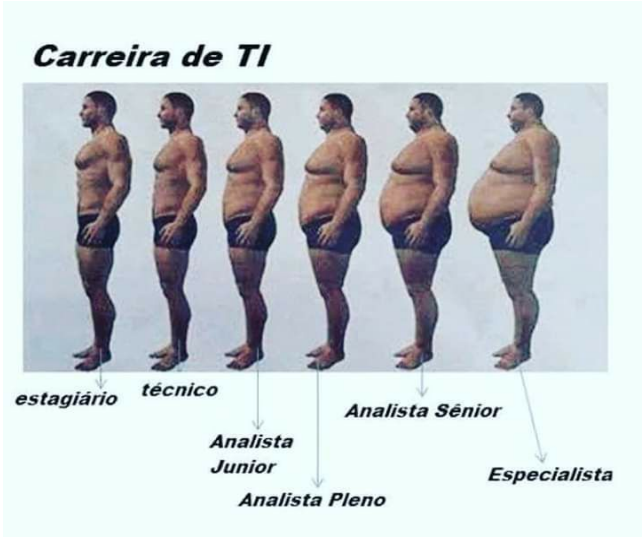
ceptro.br

Por que isso acontece?

- A Internet funciona com base na cooperação entre Sistemas Autônomos (ASes):
  - É uma “rede de redes”
  - São mais de 60.000 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

BGP *Hijacking*

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

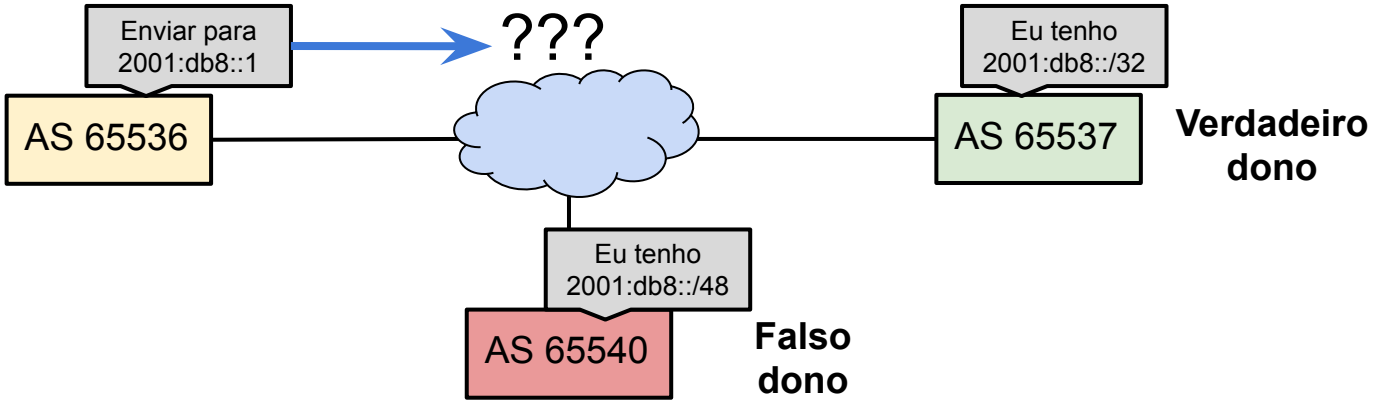


Problema 1

ROTAS:

2001:db8::/32 … 65537 i

2001:db8::/48 … 65540 i

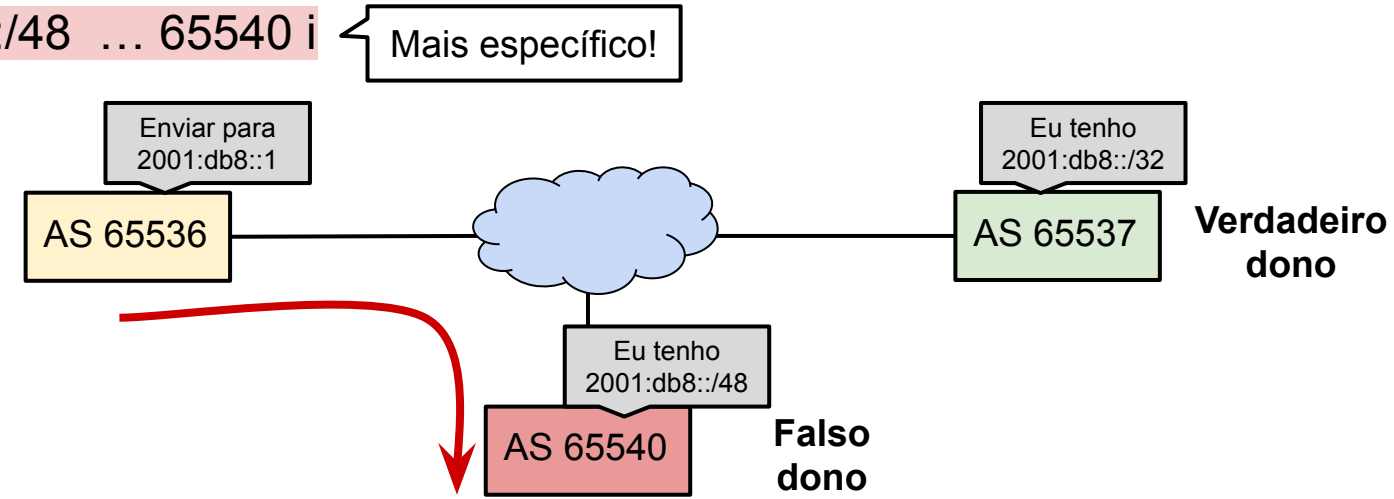


Problema 1

ROTAS:

2001:db8::/32 … 65537 i

2001:db8::/48 … 65540 i

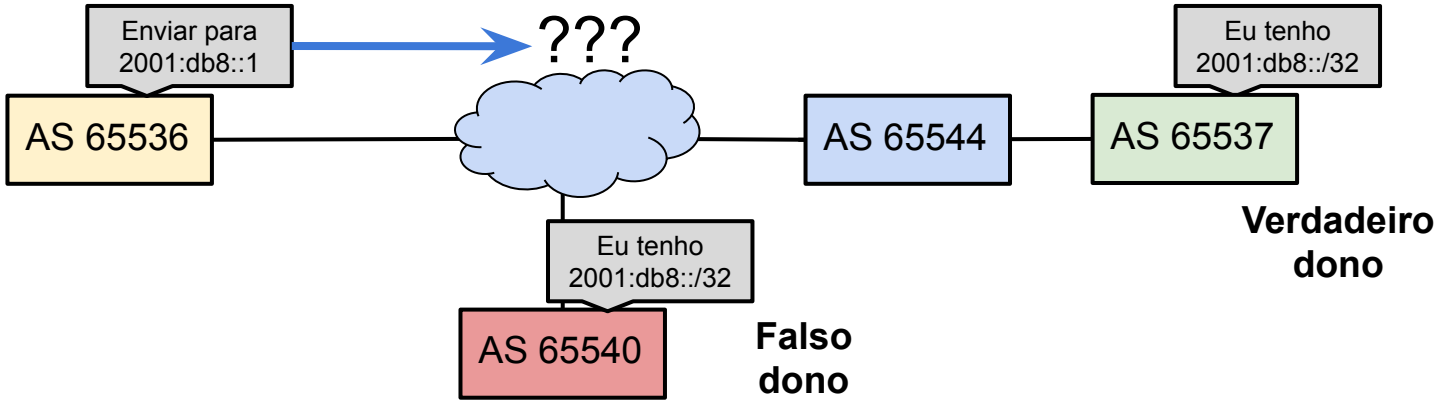


Problema 2

ROTAS:

2001:db8::/32 … 65544 65537 i

2001:db8::/32 … 65540 i

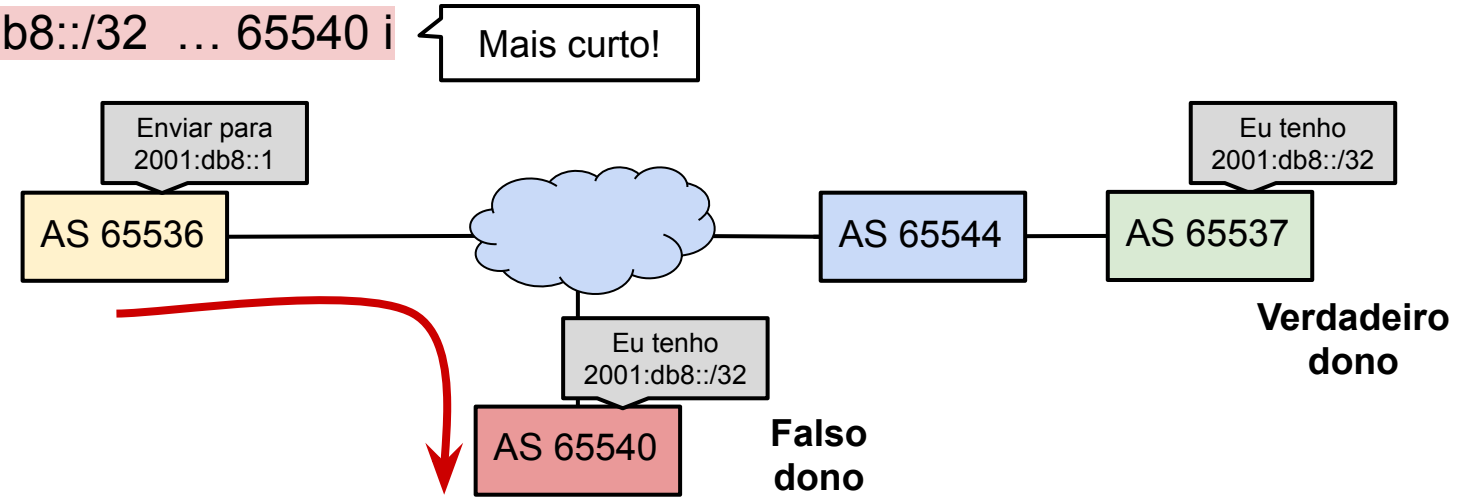


Problema 2

ROTAS:

2001:db8::/32 … 65544 65537 i

2001:db8::/32 … 65540 i

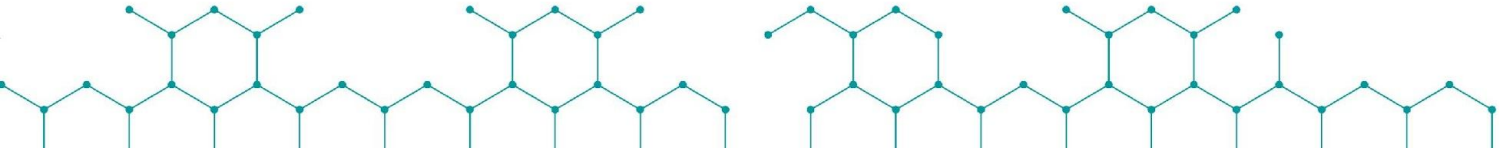


Como resolver esses problemas???

ceptro.br

MANRS

- *Mutually Agreed Norms for Routing Security* (MANRS)
- Iniciativa global
- Apoio da ISOC
- Consiste em 4 ações principais
  - Filtros
  - Anti-Spoofing
  - Coordenação
  - Validação Global

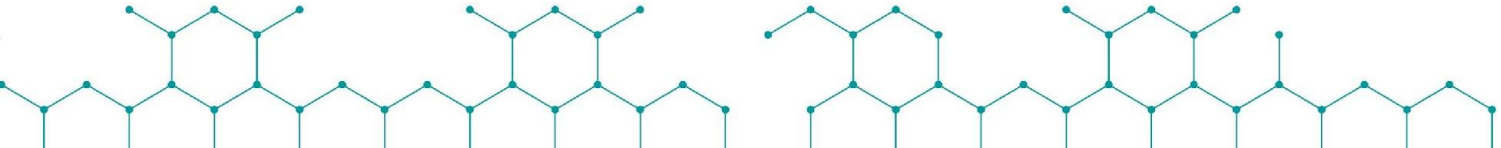


ceptro.br

MANRS

- Site do Projeto https://www.manrs.org/
- Você pode assinar o projeto
  - Solicite que seus clientes e *upstreams* também assinem o projeto https://www.manrs.org/participants/
- Faça o tutorial https://www.manrs.org/tutorials/
- ***Resource Public Key Infrastructure*** **(RPKI) faz parte do MANRS!!!**

Resource Public Key Infrastructure (RPKI)



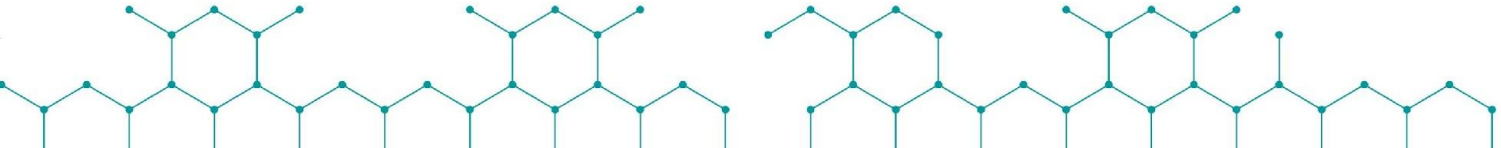
ceptro.br

O que é RPKI?

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

- Previne os problemas de BGP *Hijacking*

- **A colaboração de todos os ASes é essencial!!!**

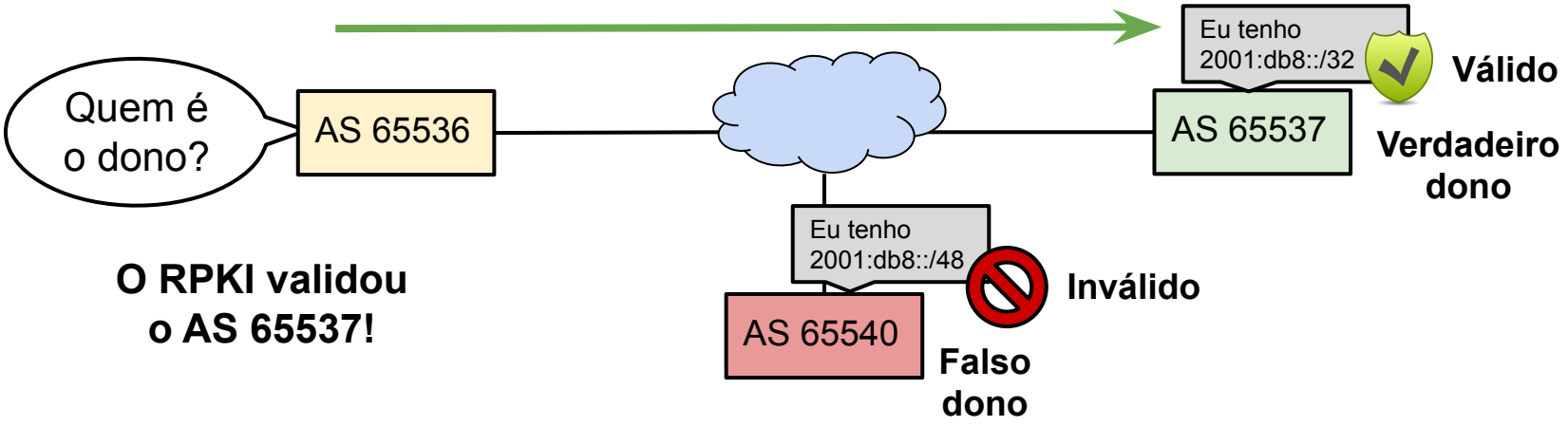


O que é RPKI?

ROTAS:

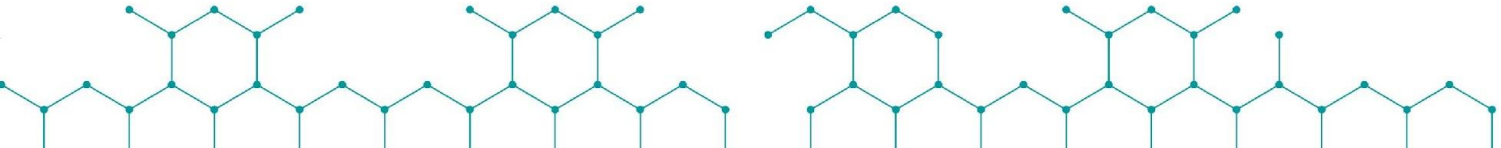
2001:db8::/32 … 65537 i

2001:db8::/48 … 65540 i



ceptro.br

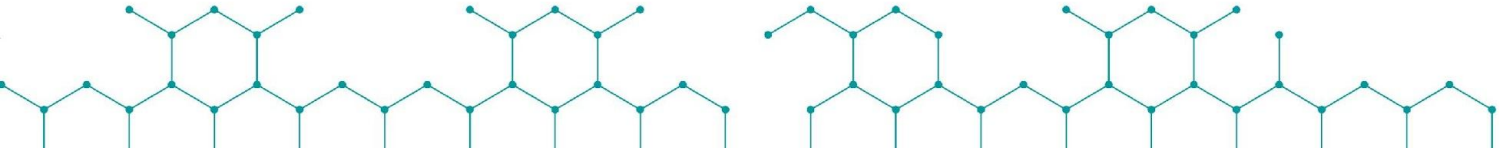
Conceitos de Segurança



ceptro.br

Serviços de segurança

- Serviços básicos de segurança:
  - Disponibilidade
  - Confidencialidade
    - Privacidade
  - Integridade
  - Autenticidade
  - Irretratabilidade ou não-repúdio

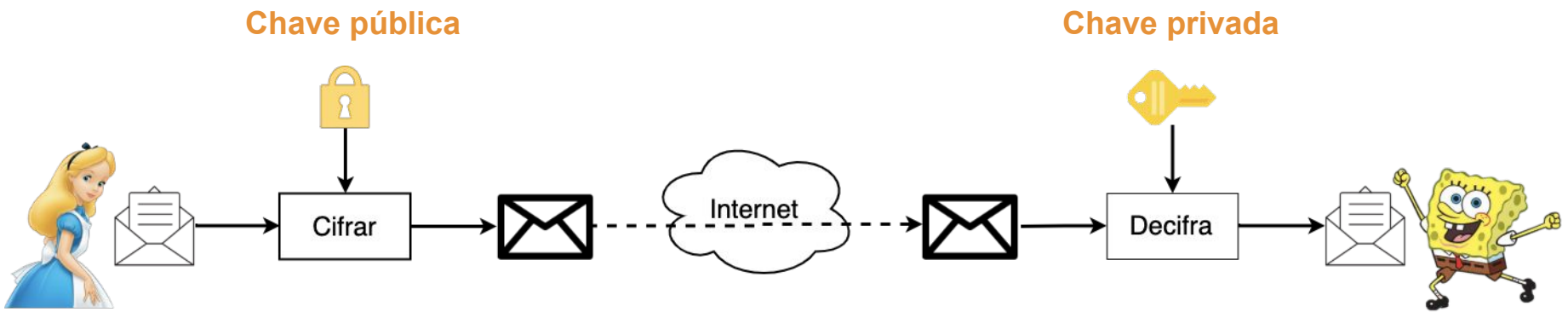


Criptografia assimétrica

- Formada por duas chaves criptográficas distintas e relacionadas
  - Chave pública: amplamente conhecida 
  - Chave privada: segredo do seu dono 
- Transformações feitas usando uma chave somente podem ser invertidas com o uso da outra chave.

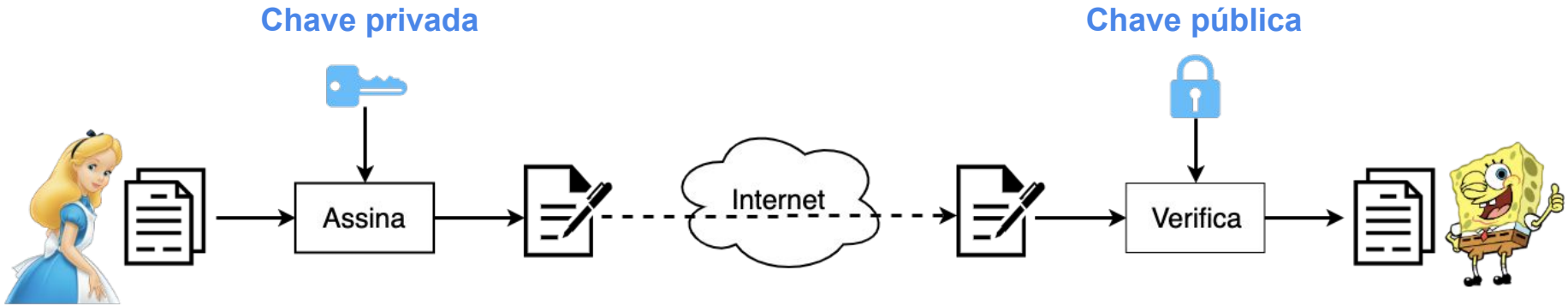
Criptografia assimétrica

- Cifração: confidencialidade

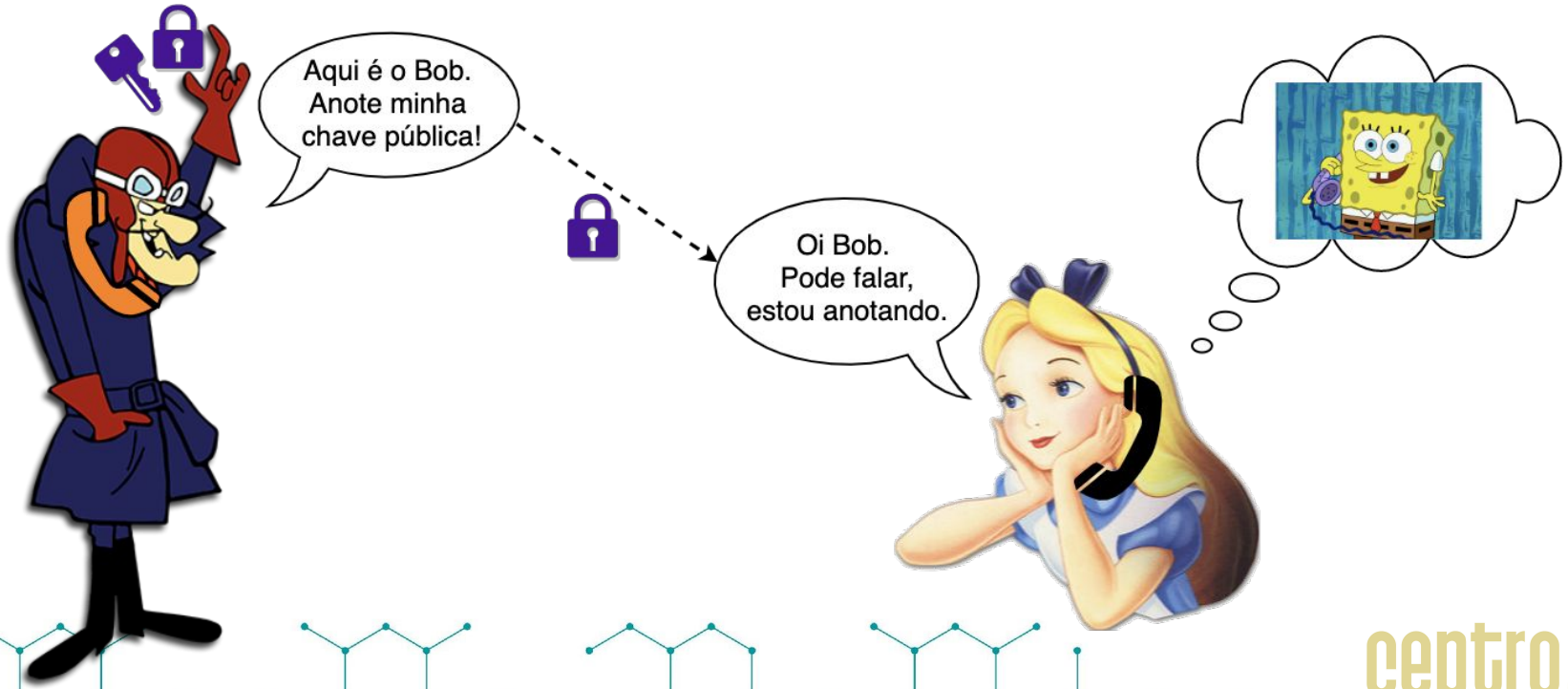


Criptografia assimétrica

- Assinatura digital:
  integridade, autenticidade e irretratabilidade

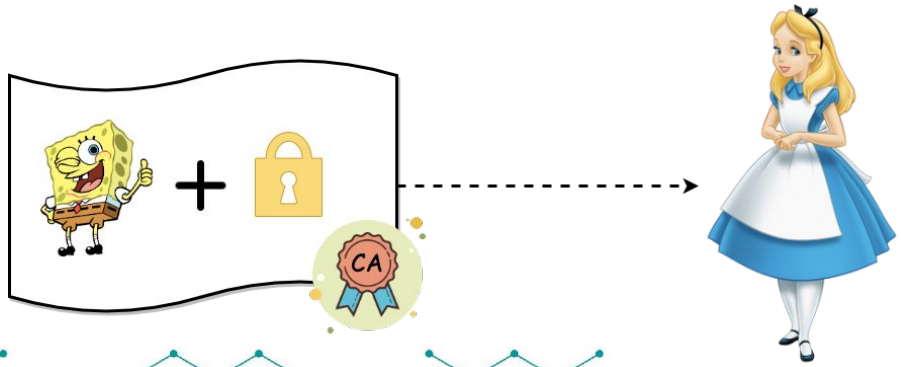


Como garantir a credibilidade de uma chave pública?



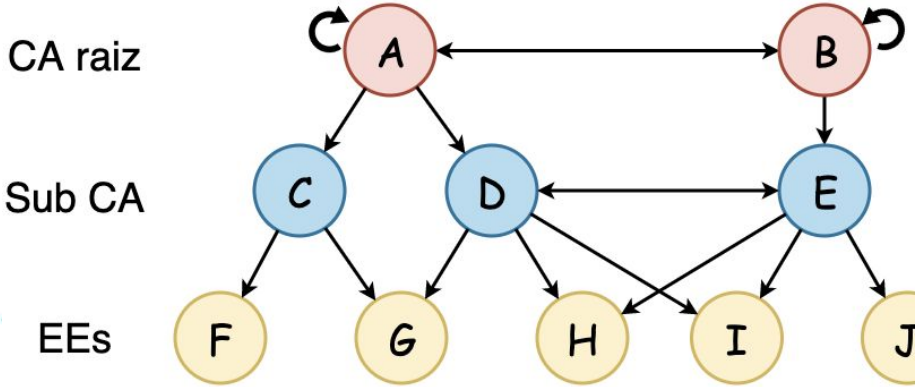
Certificados digitais

- Documento que associa a chave pública com o seu dono.
- Modelo **PKI (*Public Key Infrastructure*)** ou ICP (Infraestrutura de Chaves Públicas): certificado contém chave pública de Bob assinada por uma ***Certificate Authority*** (**CA**) ou **Autoridade Certificadora**.

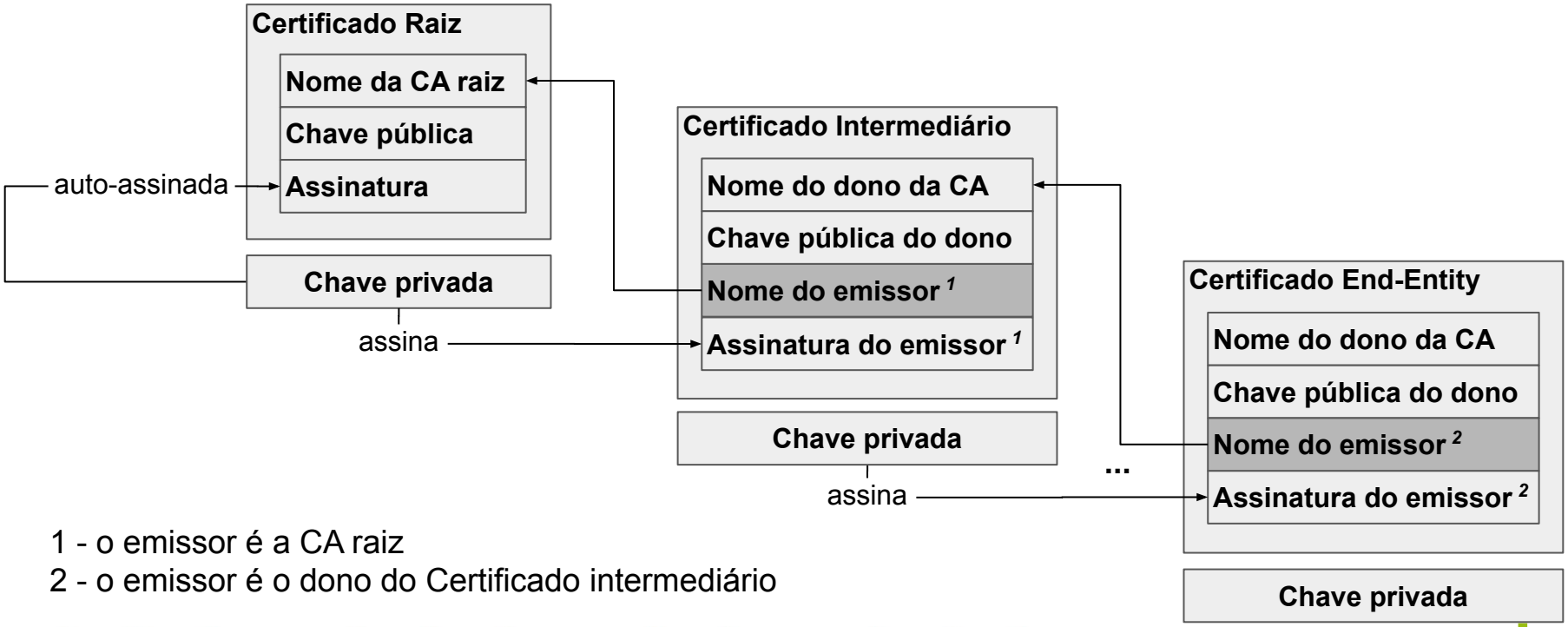


Infraestrutura de Chaves Públicas

- Modelo PKI: cadeias de certificação
  - **CA** 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 *End Entities* (EEs) ou Entidades Finais.
  - Proteção das chaves mais próximas da raiz é mais crítica.



Cadeia de certificação PKI



1 - o emissor é a CA raiz
2 - o emissor é o dono do Certificado intermediário

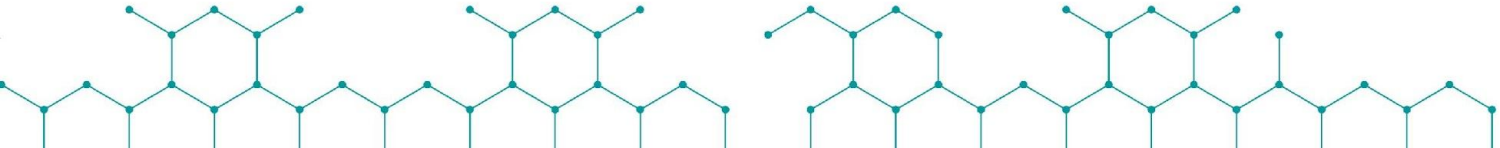
ceptro.br

Outros detalhes de PKI

- X.509
  - Padrão utilizado para criação dos certificados no modelo PKI.

- CRL (*Certificate Revocation List*)
  - "Lista negra" de certificados que tiveram suas chaves privadas comprometidas e não expiraram ainda.

Segurança no roteamento com RPKI



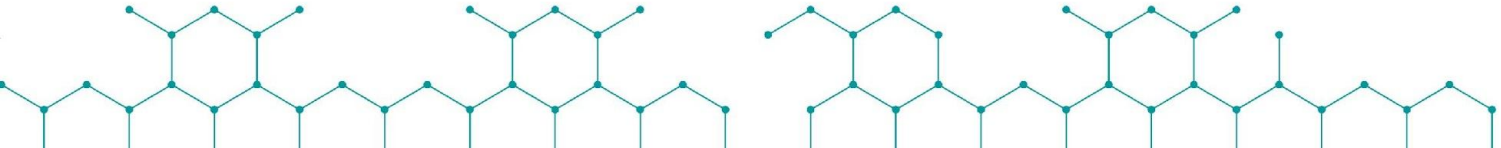
ceptro.br

Estrutura do RPKI

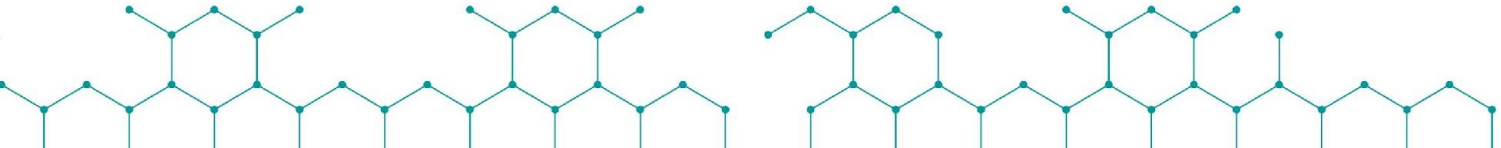
Duas partes:

- 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

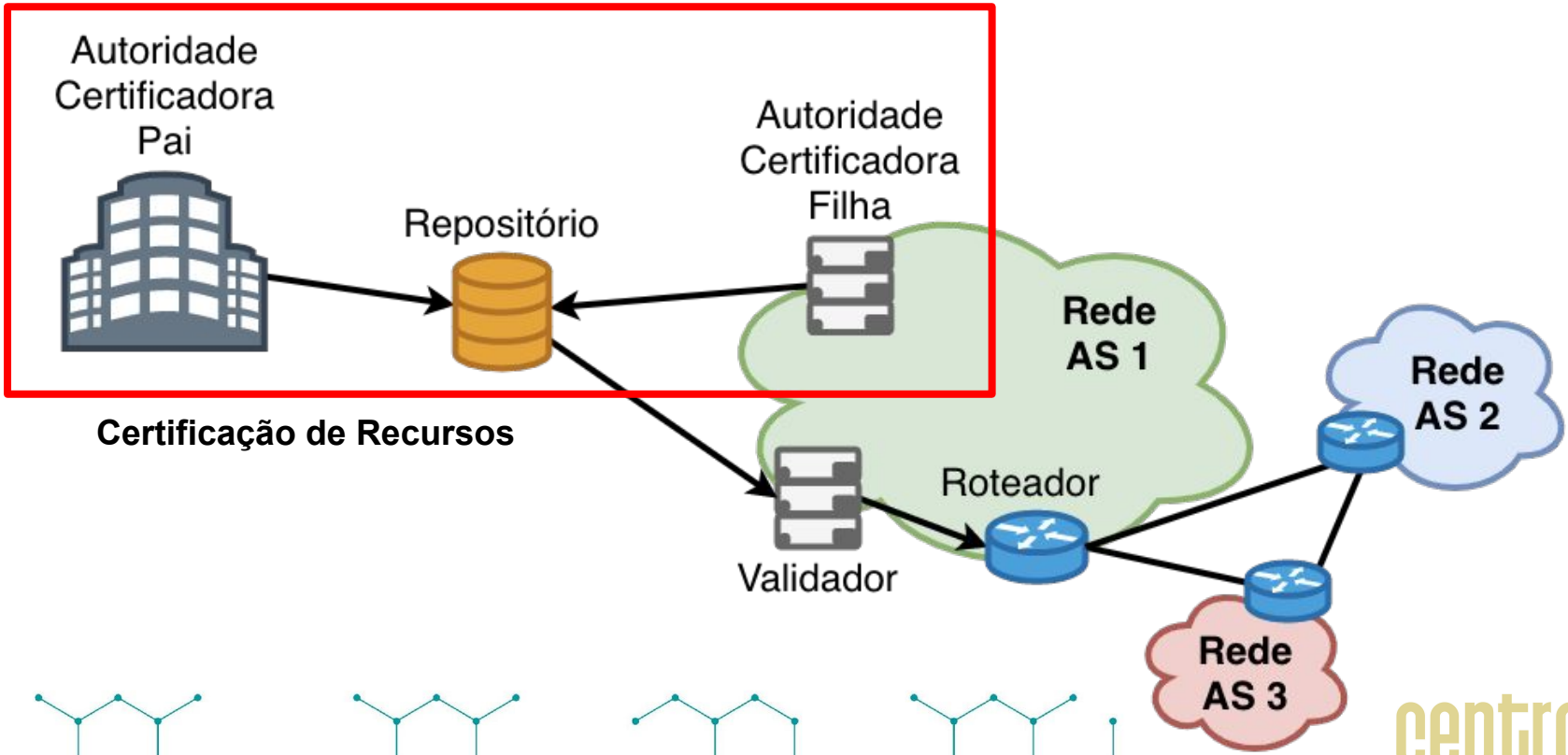


Parte I: certificação de recursos



ceptro.br

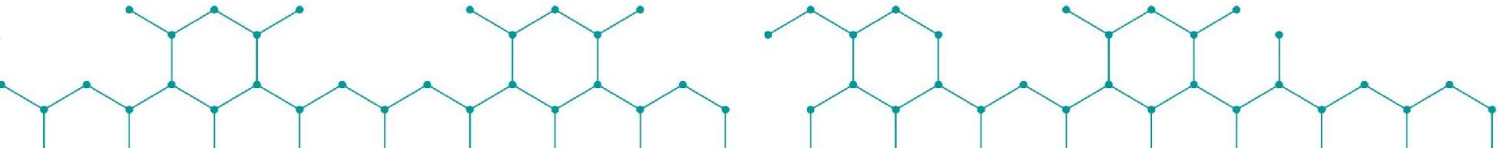
Estrutura do RPKI



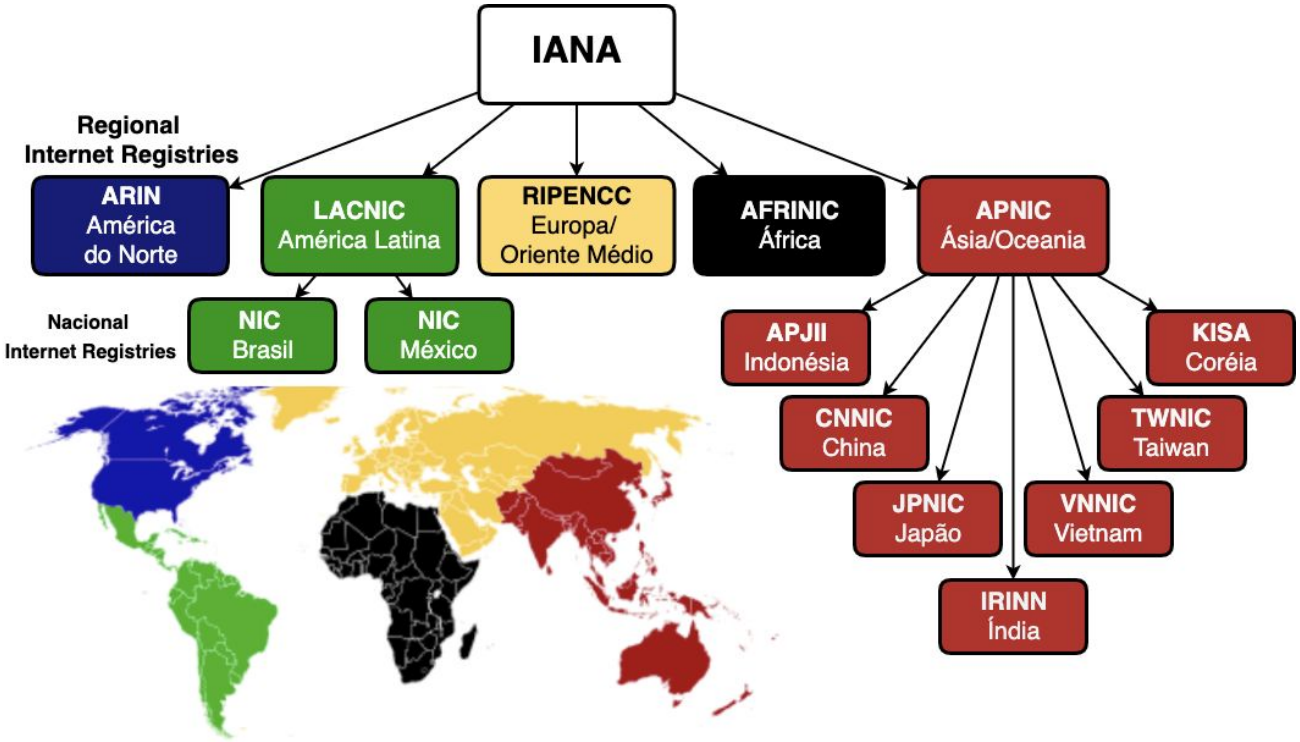
Certificação de Recursos

RPKI: Certificar as alocações de IPs e ASNs

- Como?
  - Cadeia de certificação
    - Aproveita a hierarquia de alocação de recursos numéricos existente
  - Certificados X.509 + extensão para IPs e ASNs (RFC 3779) - *Resource Certification*
    - Validar as chaves públicas e recursos de numeração



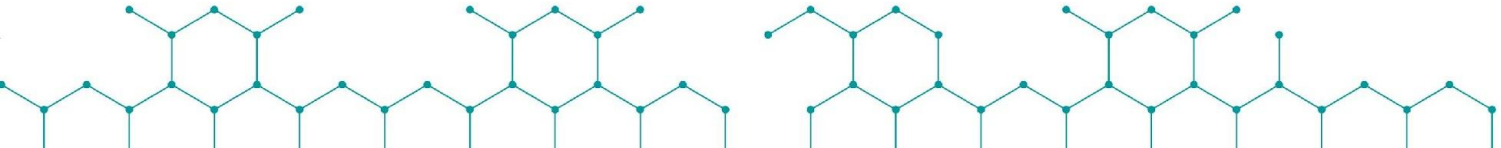
Distribuição de recursos numéricos



Cadeia de certificação do RPKI

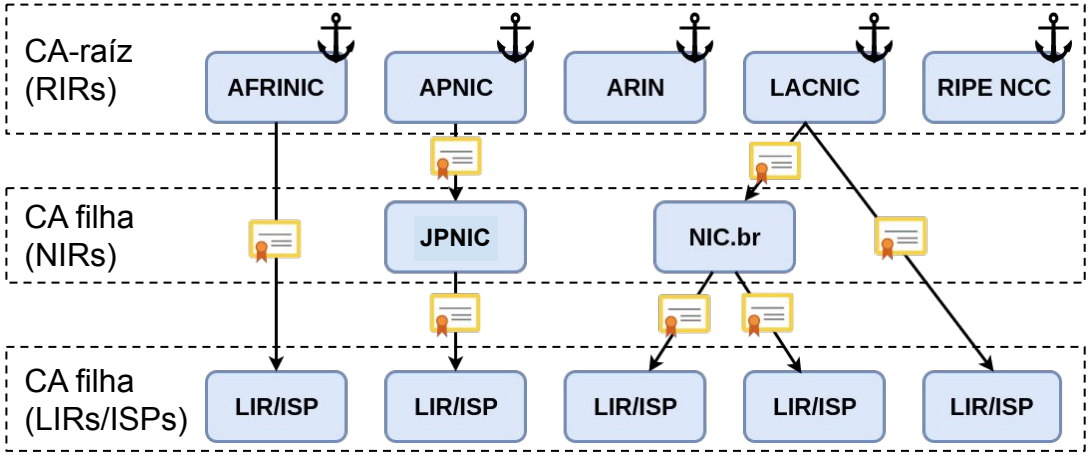
- Cada RIR pode ser uma fonte autoritativa para a alocação de recursos
  - Delegação de endereços IPs (IPv4 e IPv6)
  - Delegação de ASNs

- Funcionam como CA certificando o par IPs-ASN e a chave pública do AS



Cadeia de certificação do RPKI

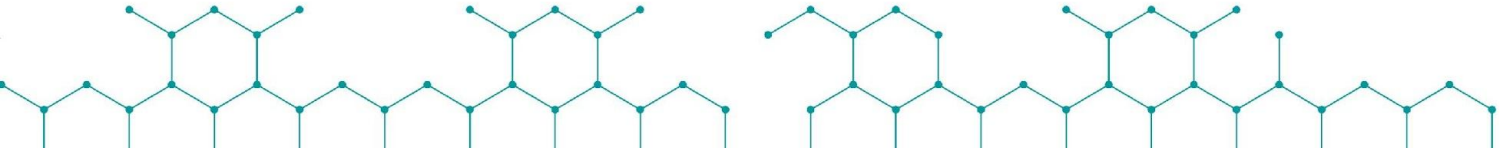
- RIRs
  - *Trust Anchor*
    - Confiabilidade implícita
    - Certificados auto-assinados (CA raiz)
  - Certificam somente os recursos de sua própria hierarquia



Cadeia de certificação do RPKI

- CAs certificam
  - Organizações que distribuem recursos de numeração
  - Detentores de recursos de numeração

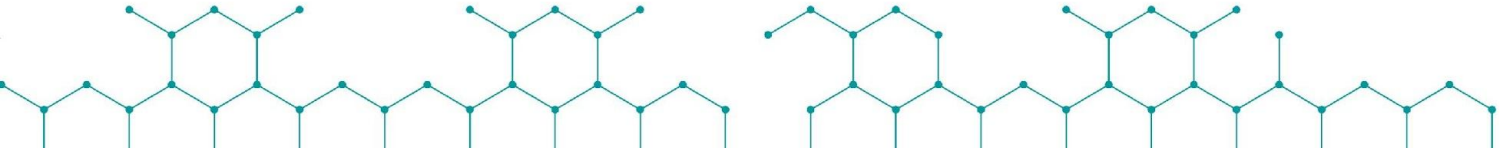
- Certificados das *End Entities*
  - Validam os documentos assinados contidos no repositório RPKI
  - Cada certificado assina um documento



ceptro.br

Documentos do repositório RPKI

- Certificados digitais
- *Certificate Revocation List* (CRL) - RFC 5280
- *Route Origin Authorisation* (ROA) - RFC 6482
  - Contém a lista de prefixos que podem ser anunciados por um ASN
- *Manifest* - RFC 6486
  - Contém a lista de todos os documentos assinados por um AS



Documentos do repositório RPKI

Com base nas informações contidas nos arquivos do repositório RPKI, é possível estabelecer as **políticas de roteamento** que **aumentam a segurança no BGP**.

ROAs

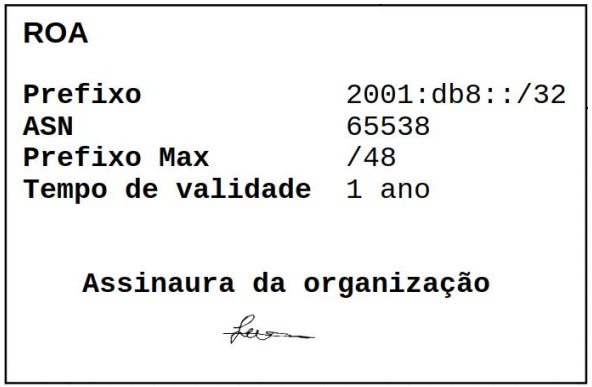
- *Route Origin Authorisation*
  - Objeto assinado

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

Elementos principais:

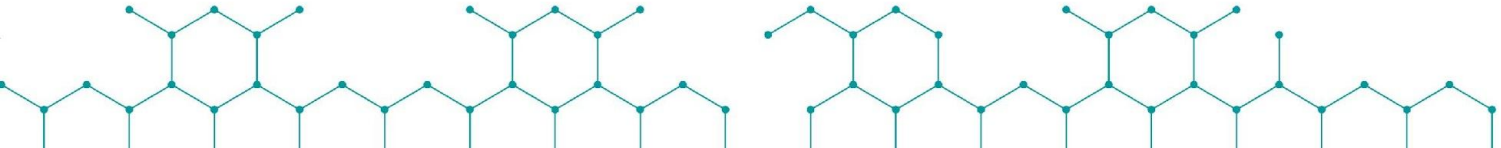
- Nome da ROA
- Número do AS (ASN)
- Prefixo alocado e máximo permitido
- Tempo de validade
- Assinatura da organização dona dos recursos

ROA da organização



ROAs

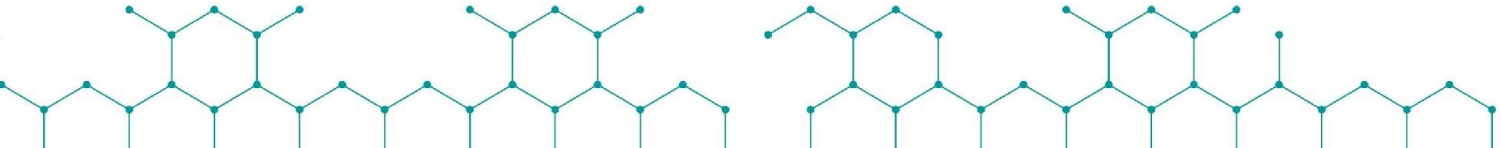
- Todos os prefixos anunciados devem estar cadastrados em um ou mais ROAs
  - Assinados e guardados em um repositório RPKI
    - Certificado contendo recursos de numeração
    - Declarações da origem das rotas para esses recursos
- Cada ROA contém apenas um ASN
  - Prefixos podem possuir mais de um ROA



ceptro.br

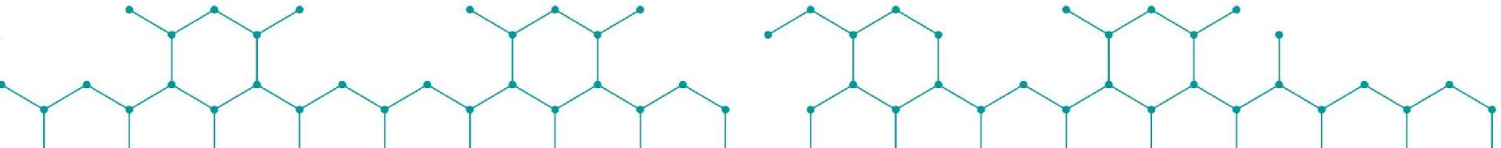
ROAs

- Alocações no ROA devem vir da organização responsável pelos recursos (CA certificada como detentora dos recursos)
- Armazenados em repositórios públicos confiáveis de alta disponibilidade



ROAs

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

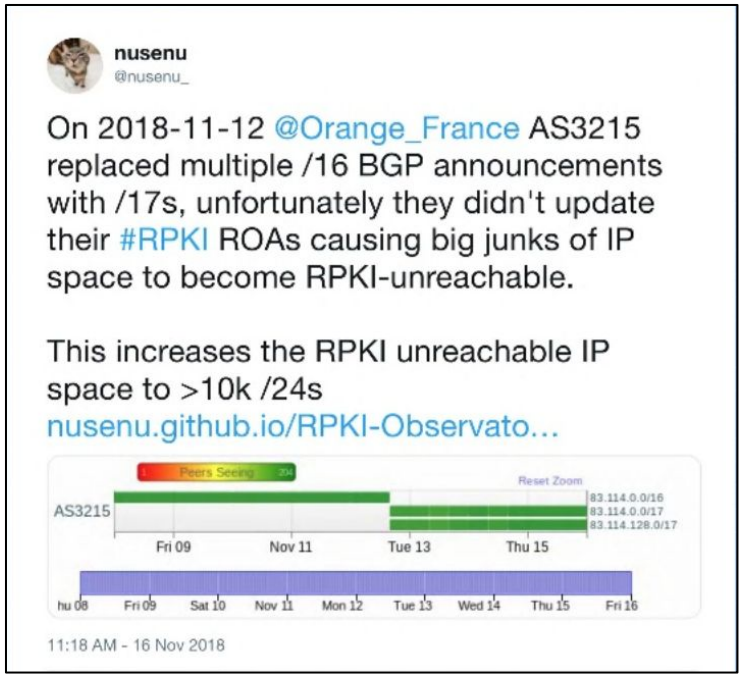


ceptro.br

Manutenção é essencial!

Não esqueça do RPKI!

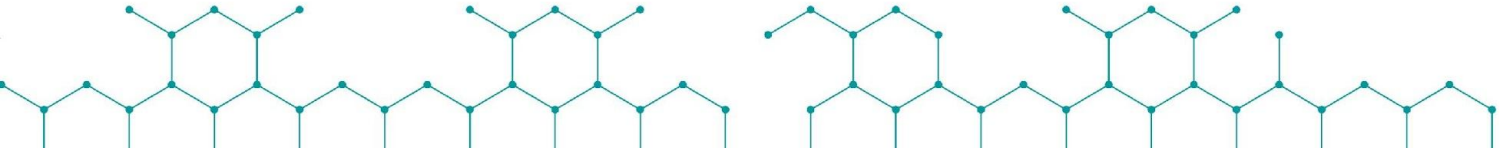
Atualize os ROAs quando mudar os anúncios!



ceptro.br

Modos de operação no RPKI

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

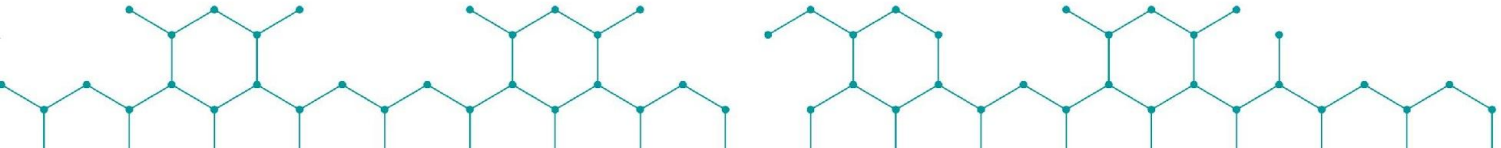


Modo Hospedado

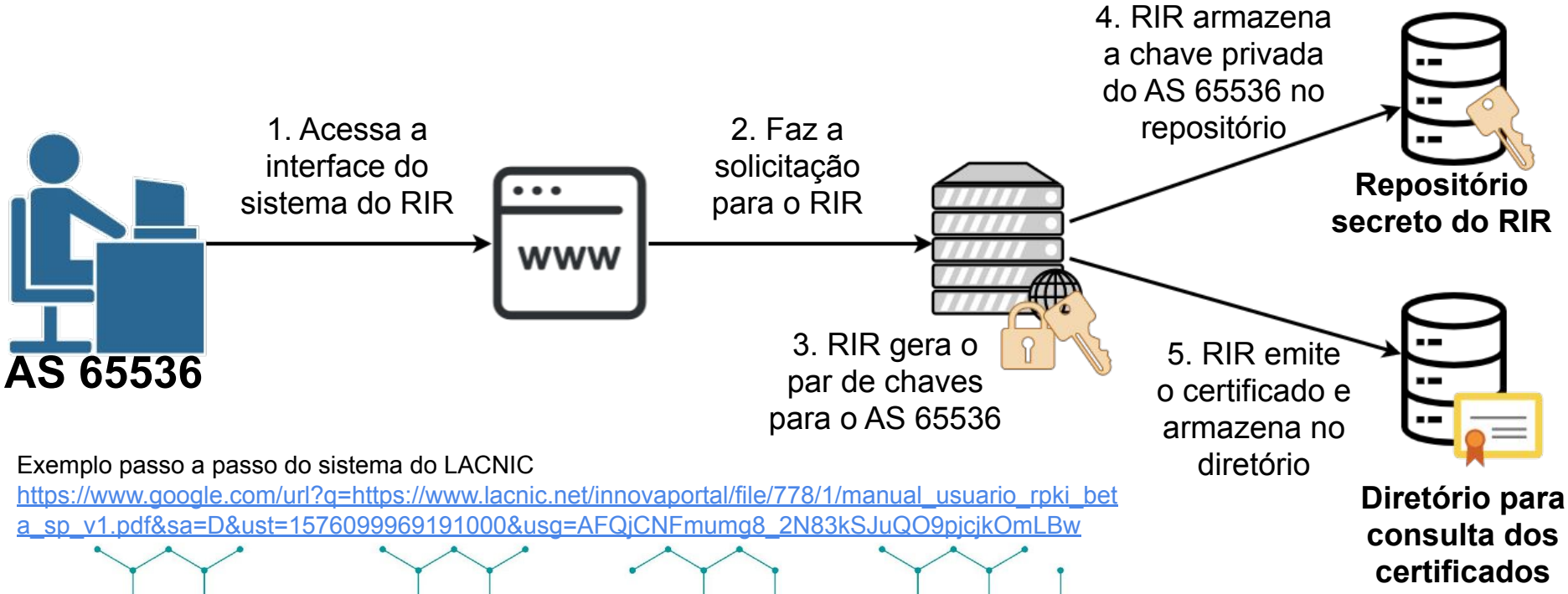
- Incentivar a adoção do RPKI

- 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



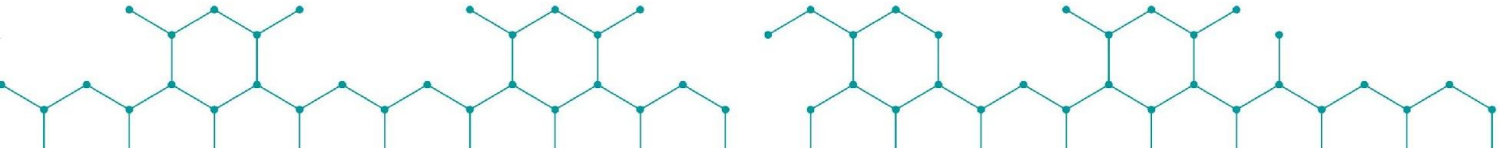
Modo Hospedado



Exemplo passo a passo do sistema do LACNIC
https://www.google.com/url?q=https://www.lacnic.net/innovaportal/file/778/1/manual_usuario_rpki_beta_sp_v1.pdf&sa=D&ust=1576099969191000&usg=AFQjCNFmumg8_2N83kSJuQO9pjcjkOmLBw

Modo Delegado

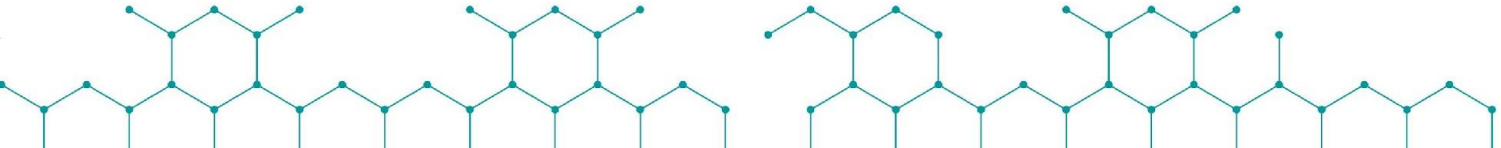
- Sistema distribuído de CAs
  - Foi desenhado para ser assim
- Facilita a automatização
- Centraliza o gerenciamento das ROAs na organização dona dos recursos
- Controle da chave privada pelo AS
- Permite delegar CAs filhos para clientes
- AS tem mais autonomia no RPKI



ceptro.br

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



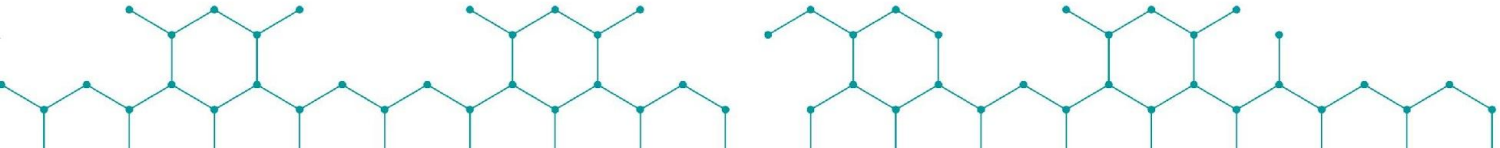
ceptro.br

Modo Delegado

O que eu preciso?

- **Software CA**
  - **Krill - NLnet Labs**
  - rpkid - Dragon Research Labs

- **Servidor de publicação**
  - Próprio (alta disponibilidade) ou de **terceiros** (NIC.br)



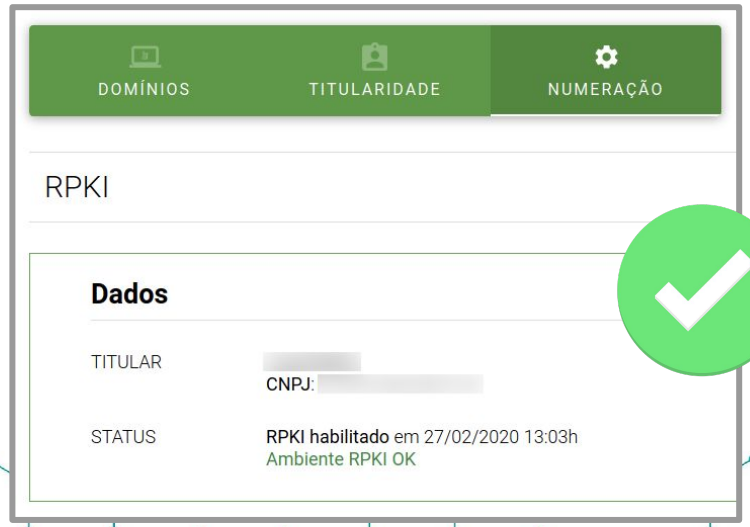
ceptro.br

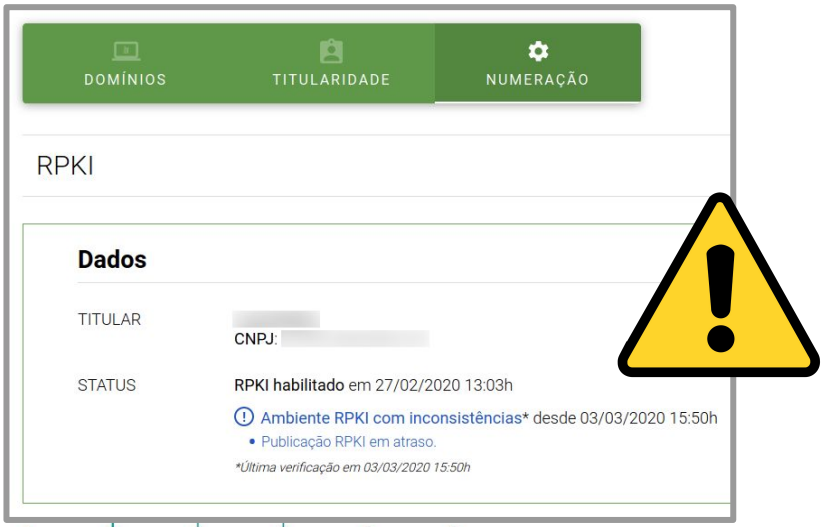
Servidor Krill

- **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**

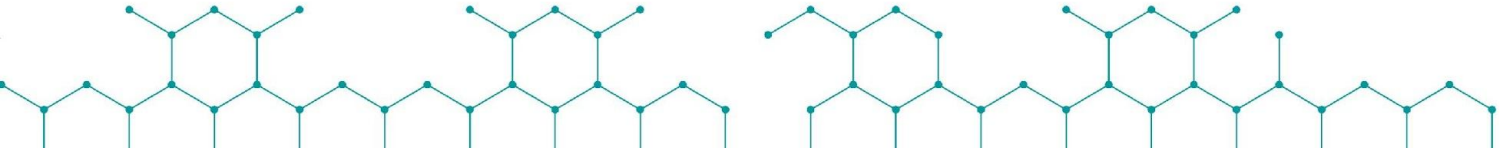
Monitoramento do RPKI pelo Registro.br

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.



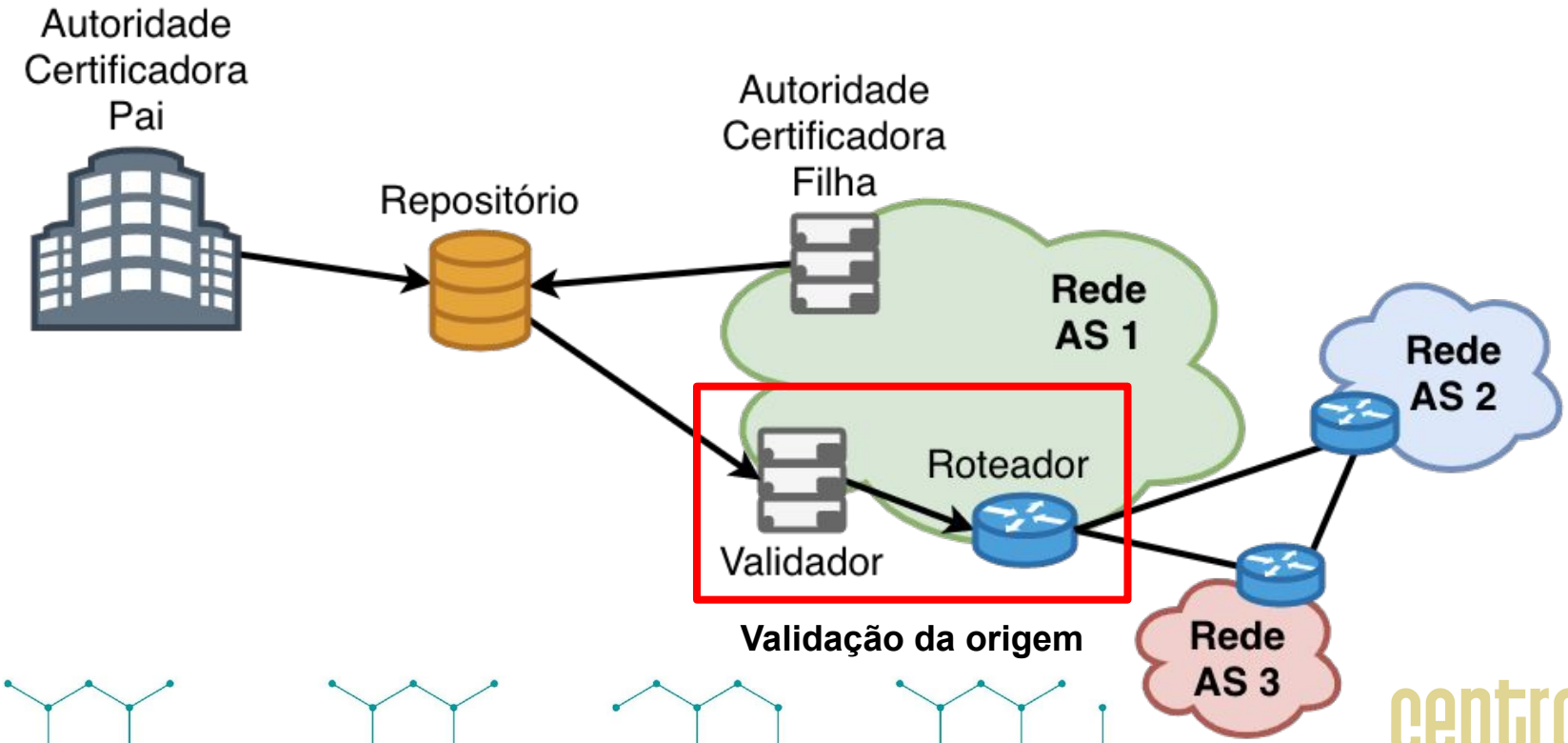


Parte II: validação na origem



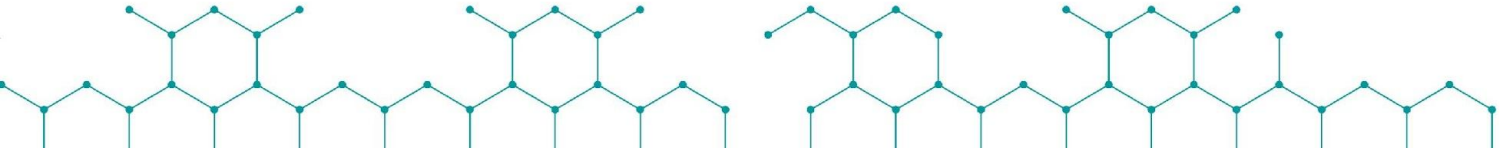
ceptro.br

Estrutura do RPKI

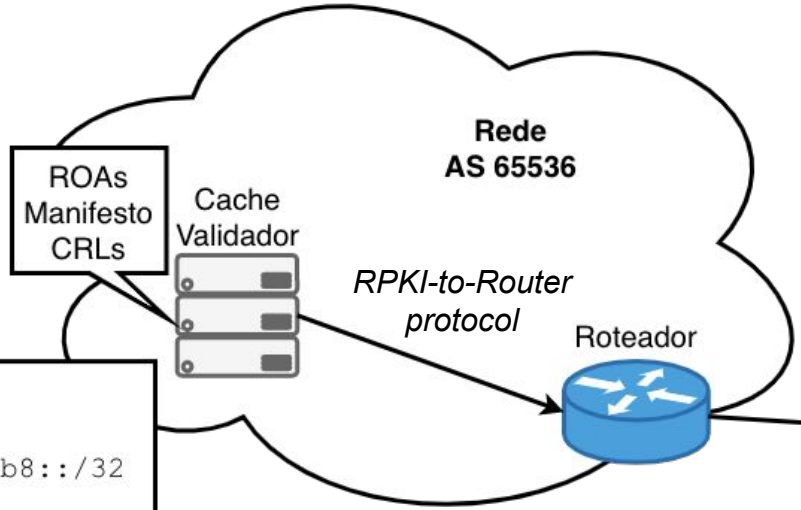


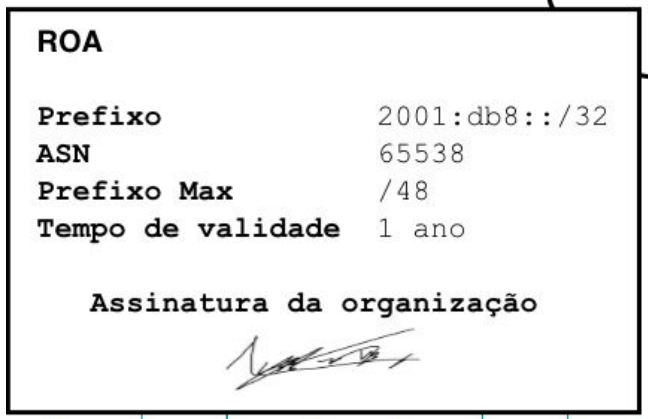
RPKI: Validação da origem

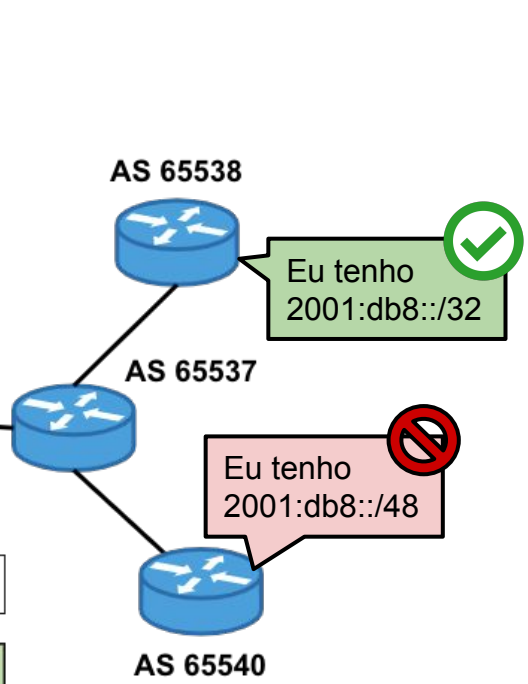
- **Validador**
  - Validação dos objetos certificados
  - Software que acessa fontes confiáveis e cria um cache da informação validada
- **Roteador**
  - Validação das rotas
  - BGP habilitado para usar o RPKI
  - Obtém informações do validador e utiliza para influenciar o roteamento



RPKI: Validação da origem







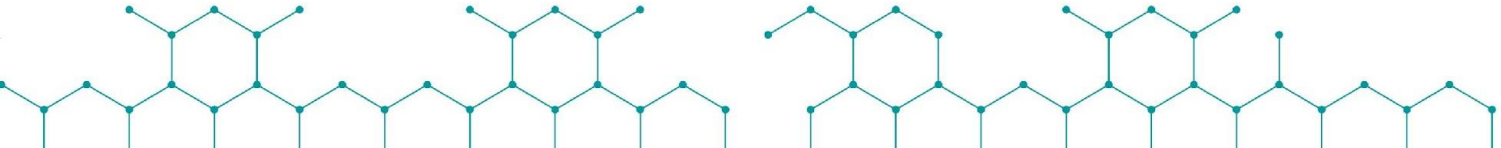
2001:db8::/32~48	65538

2001:db8::/32	65537 65538	Válido
2001:db8::/48	65537 65540	Inválido

ceptro.br

Validador

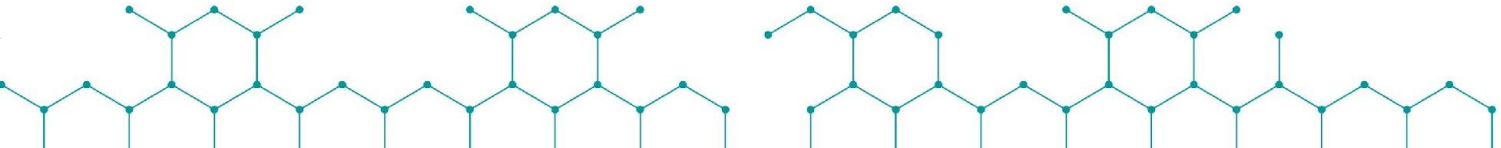
- Conexão com repositórios confiáveis (RIPE, LACNIC,...)
  - *Rsync* ou *RPKI Repository Delta Protocol* (RRDP)
- Cache
  - Atualizações periódicas
- Validação
  - Verificação das assinaturas dos ROAs e certificados
  - Geração de *Verified ROA Payloads* (VRP)
- Envia VRPs para o roteador usando o protocolo *RPKI-to-Router* (RTR)



ceptro.br

Validador

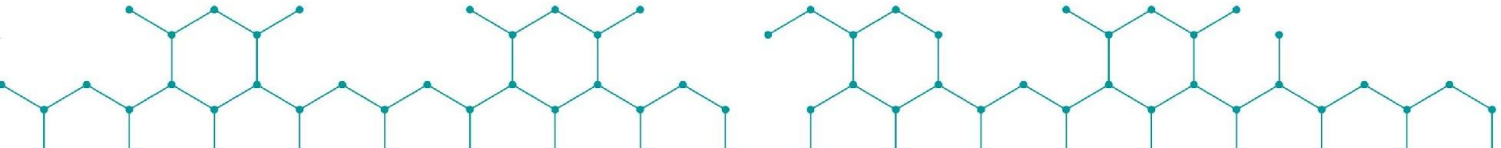
- Existem vários softwares disponíveis:
  - Routinator - NLnet Labs
  - Dragon Research toolkit
  - RIPE validator
  - RTRlib (bird, FRR, Quagga...)
  - OctoRPKI & GoRTR (Cloudflare)
  - FORT Validator - NIC.MX e LACNIC
- Recomenda-se a utilização de mais de um validador distinto.



ceptro.br

Roteador

- Suporte a validação na origem bastante amplo
- 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.

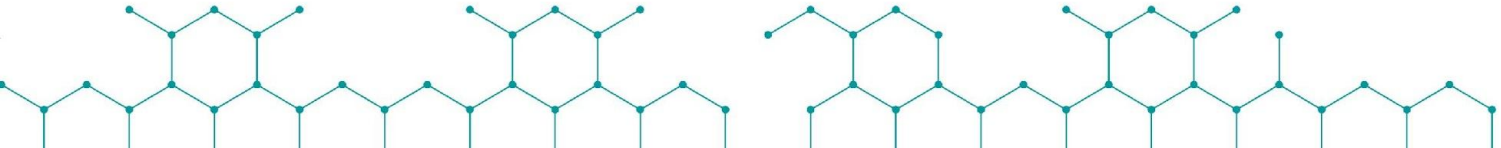


ceptro.br

Roteador

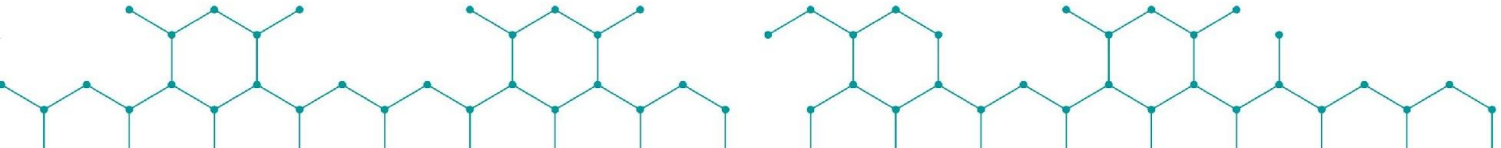
- Existem vários softwares com suporte a RPKI:
  - BIRD
  - OpenBGPD
  - FRRouting
  - GoBGP
  - VyOS

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



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



ceptro.br

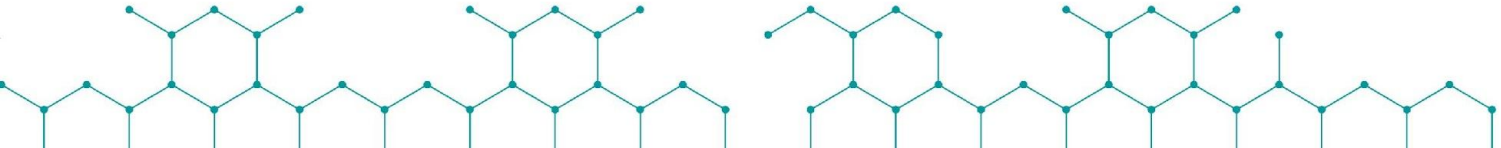
Exemplo de validações

Classificação	AS de Origem	Prefixo BGP
Válida	65536	10.0.0.0/16
Válida	65536	10.0.128.0/17
Inválida	65536	10.0.0.0/24
Inválida	65540	10.0.0.0/18
Desconhecido	65536	10.0.0.0/8
Desconhecido	65540	10.0.0.0/8

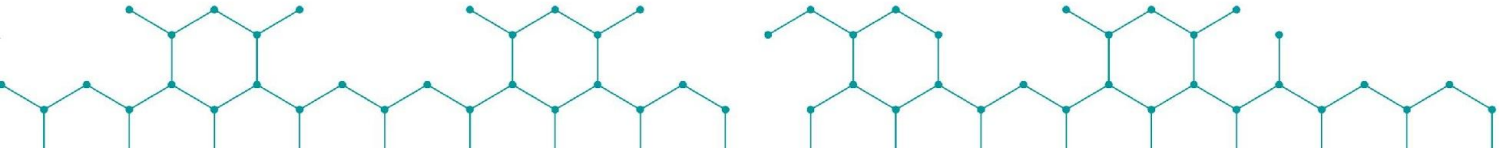
ROA	
AS de Origem	65536
Prefixo	10.0.0.0/16
Comprimento Max	/18

Roteador

- Políticas de roteamento podem ser estabelecidas em cima da validação das rotas
  - Alterar preferências (*local preference*)
  - Atribuir *communities*
  - Aplicar filtros



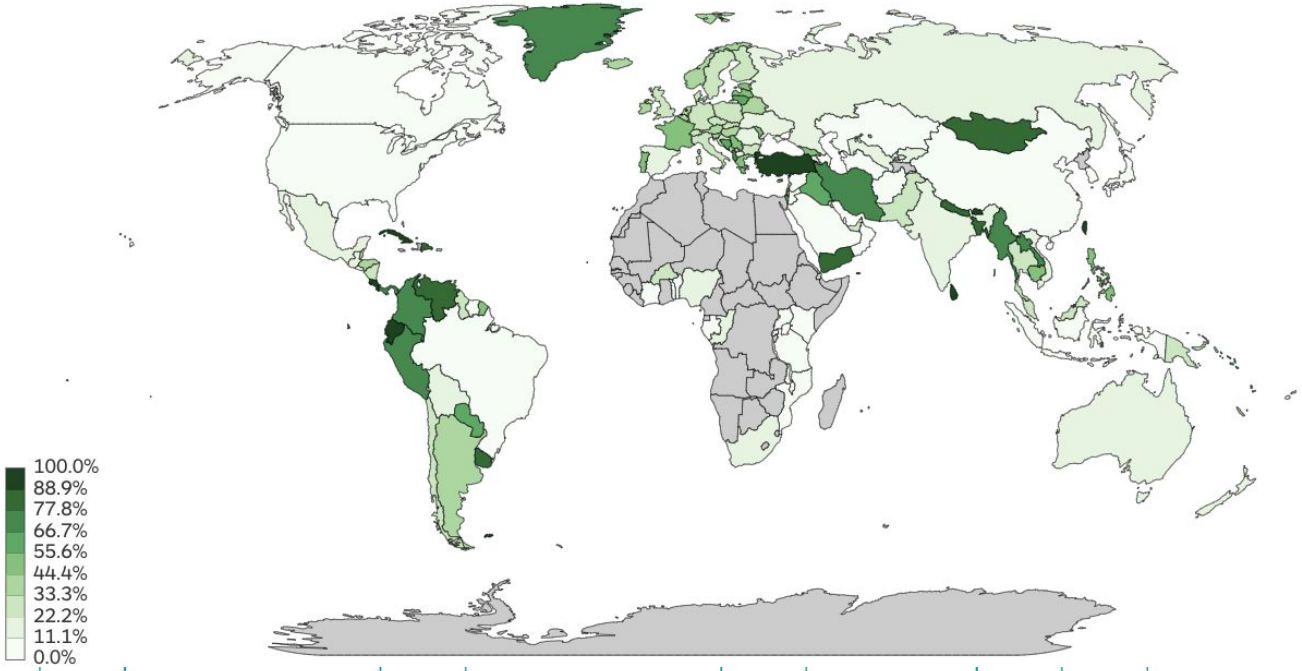
Como estamos?



ceptro.br

Colaboração é essencial: Adoção do RPKI

Fonte: https://www.nlnetlabs.nl/projects/rpki/rpki-analytics/

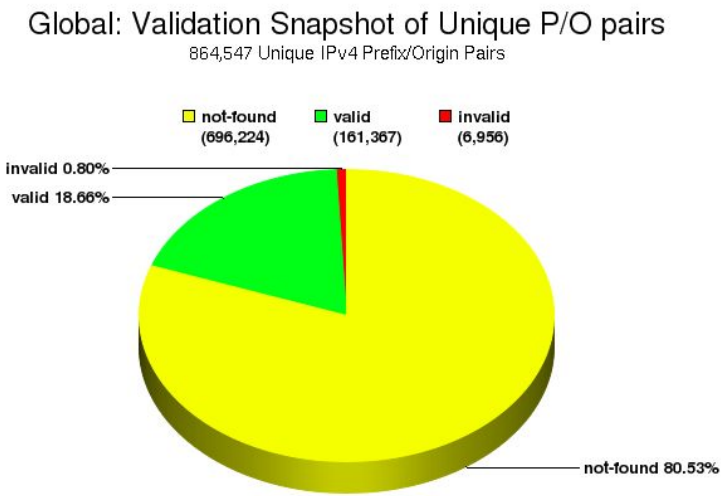


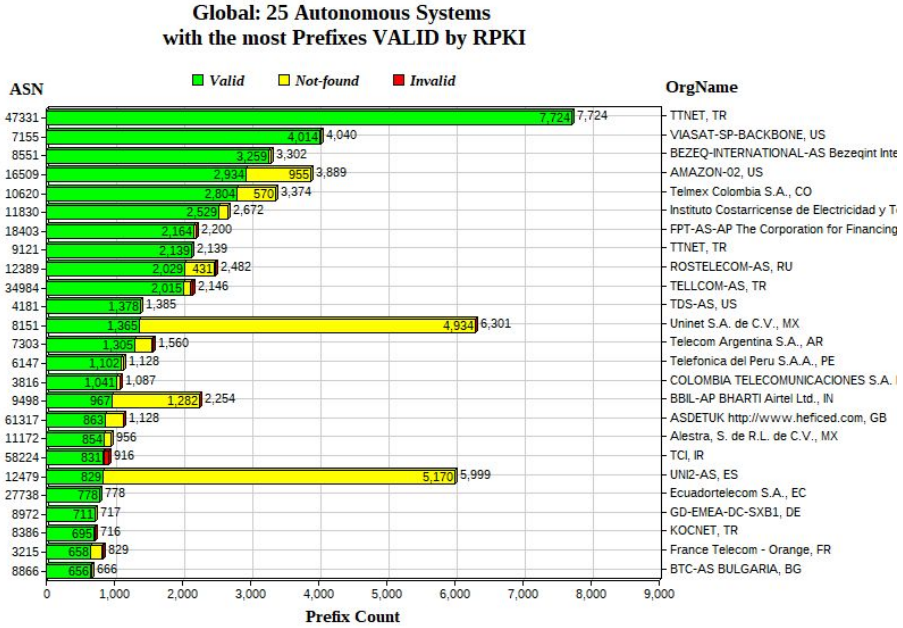
ceptro.br

Validação de rotas

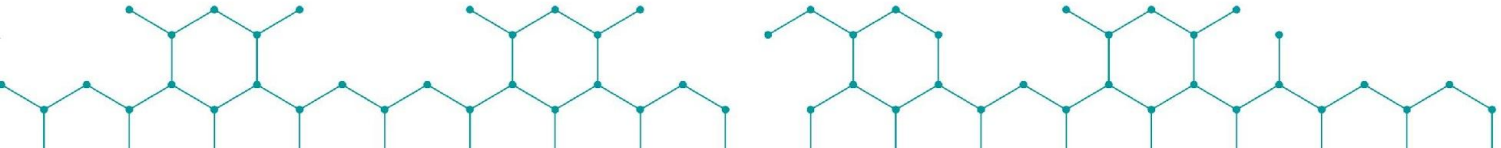
Análise da tabela completa do BGP em relação aos prefixos anunciados nos RPKIs

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





Agora, mão na massa!



ceptro.br

OBRIGADO!

cursosceptro@nic.br

Parceria

Realização