
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

# RPKI:
## Uma proteção para roubo de prefixos no BGP

ceptro.br nic.br cgi.br

# Agenda
# Motivação e conceitos fundamentais

- Parte I: Motivação
  - Problemas de segurança em roteamento
    - BGP *Hijacking*
  - MANRS
    - RPKI
- Parte II: Conceitos fundamentais
  - Conceitos de roteamento
    - BGP
  - Conceitos de segurança
    - Criptografia
    - Certificação digital

# Agenda
# RPKI

- Parte III: Certificação de recursos
  - Componentes do RPKI
    - ROAs
  - Modos de operação
  - Como entrar na cadeia de certificação do NIC.br?
  - Como anunciar seus recursos no RPKI do NIC.br?
- Parte IV: Validação na origem
  - Como é feita a validação?
    - Tipos de rotas
  - Conversa sobre Boas práticas/ Recomendações
    - Políticas em relação às rotas validadas

# Parte I
# Motivação

# Problemas de segurança em roteamento

# Ataques na mídia nos últimos anos

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

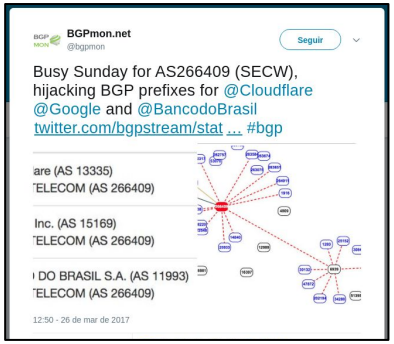
What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets

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

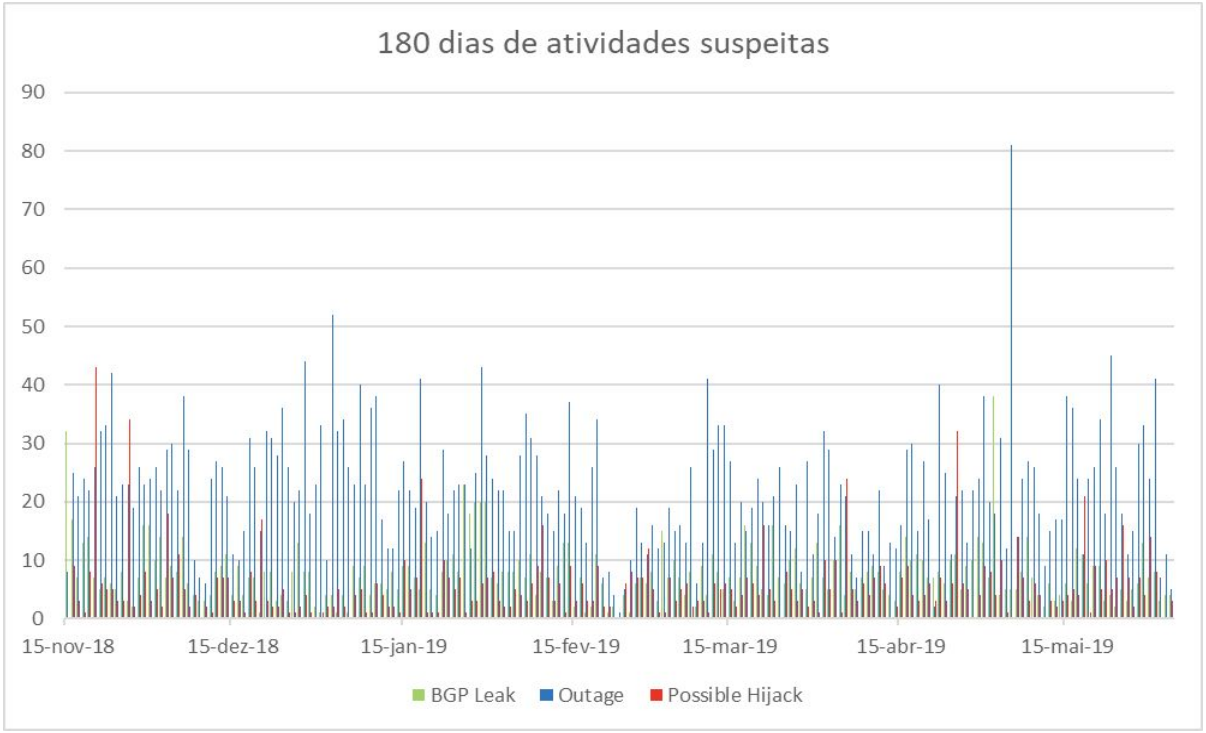
Mutually Agreed Norms for Routing Security (MANRS) 15 November 2018

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/

# Nenhum dia sem um incidente!!!




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

# 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


# BGP *Hijacking*

Caso notável:

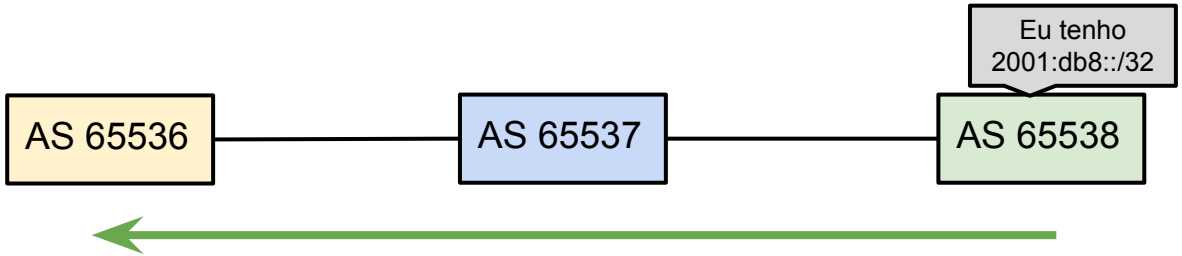
2008 - Pakistan Telecom (AS 17557)

- Anuncia o prefixo 208.65.153.0/24 sem autorização
    - Tráfego do Youtube é redirecionado para o Paquistão (https://youtu.be/IzLPKuAOe50)

# Cenário inicial

**ROTAS:**

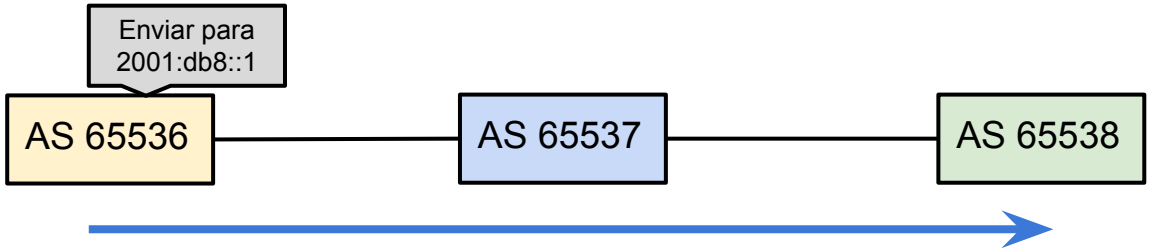
2001:db8::/32  65537 65538 i



# Cenário inicial

**ROTAS:**

2001:db8::/32  65537 65538 i

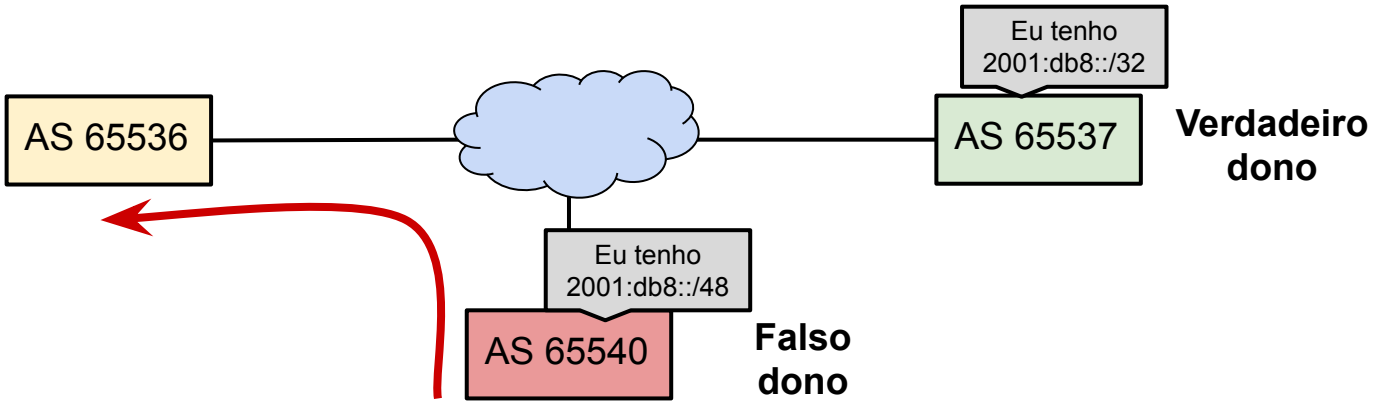


# Problema 1

**ROTAS:**

2001:db8::/32 … 65537 i

2001:db8::/48 … 65540 i

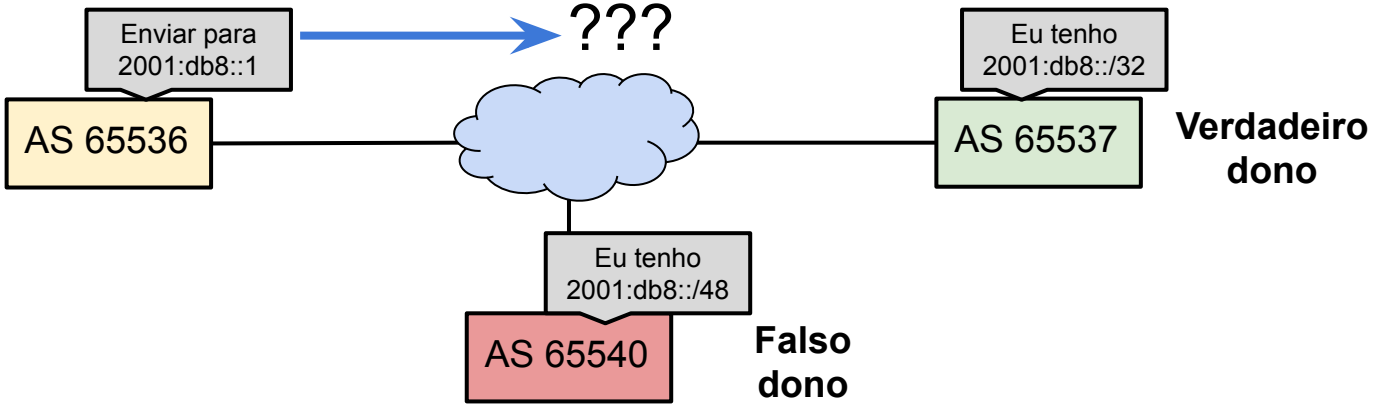


# Problema 1

**ROTAS:**

2001:db8::/32 … 65537 i

2001:db8::/48 … 65540 i



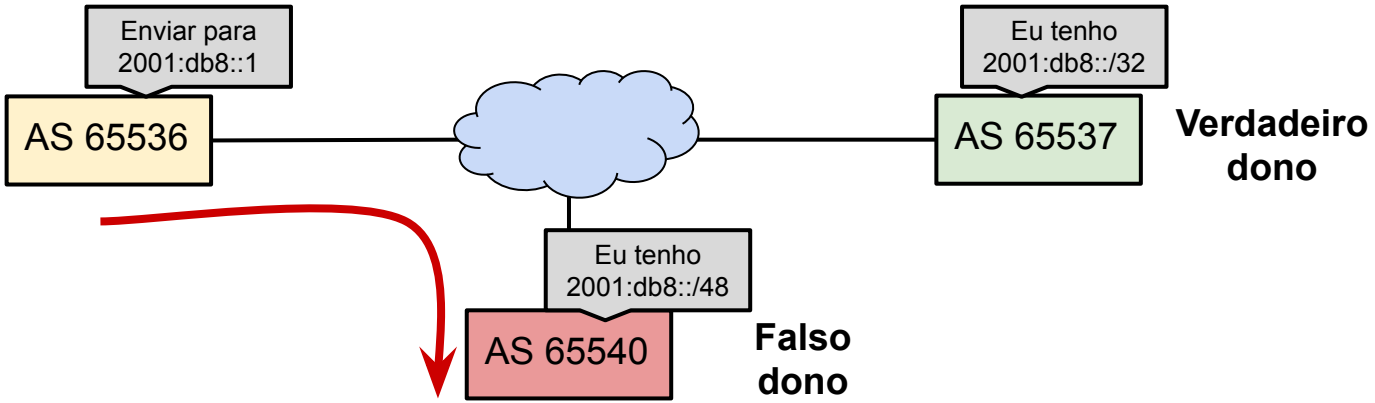
# Problema 1

**ROTAS:**

2001:db8::/32 … 65537 i

2001:db8::/48 … 65540 i

Mais específico!

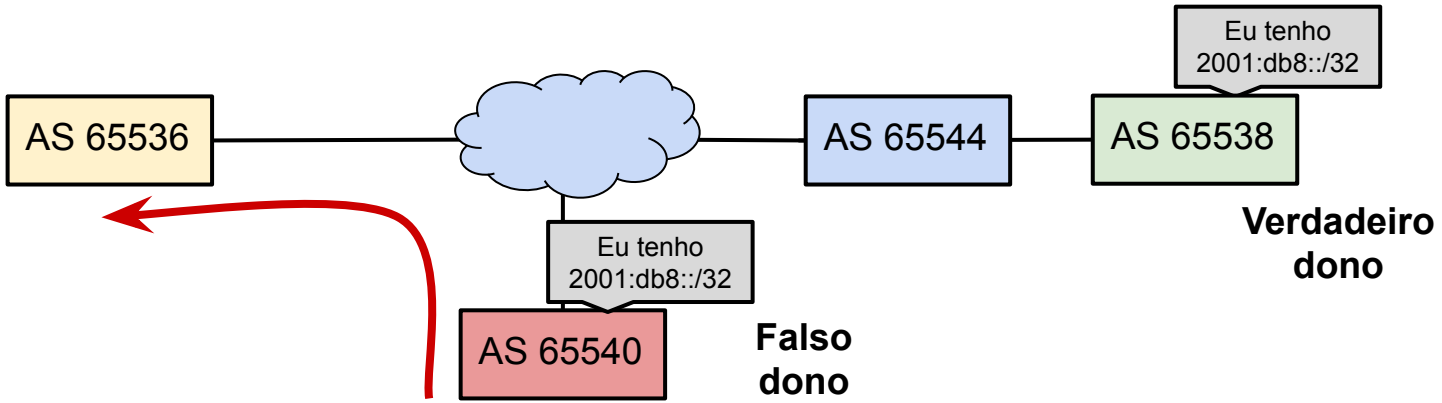


# Problema 2

**ROTAS:**

2001:db8::/32 … 65544 65538 i

2001:db8::/32 … 65540 i

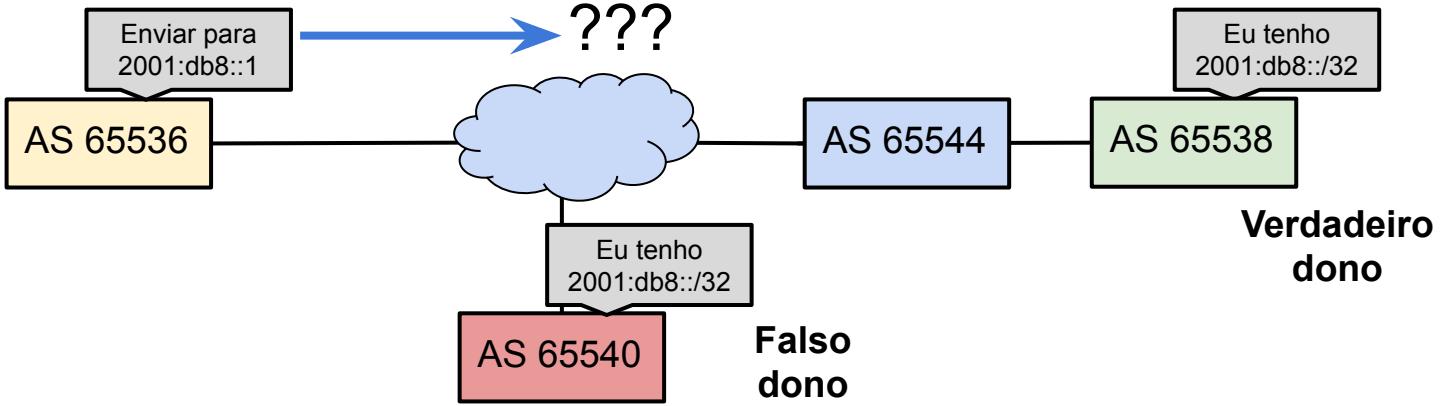


# Problema 2

**ROTAS:**

2001:db8::/32 … 65544 65538 i

2001:db8::/32 … 65540 i



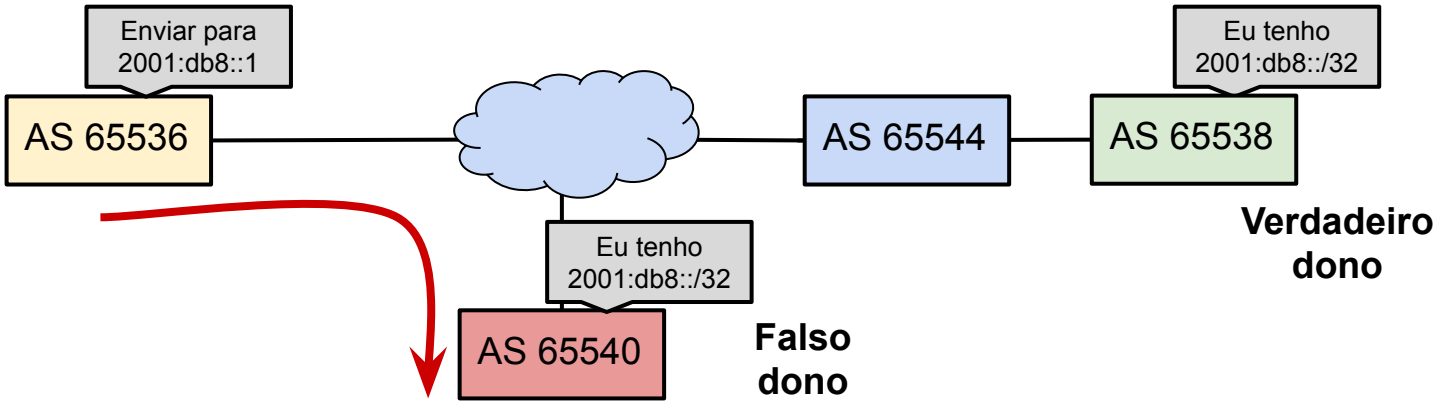
# Problema 2

**ROTAS:**

2001:db8::/32 … 65544 65538 i

2001:db8::/32 … 65540 i

Mais curto!



# Como resolver esses problemas???

MANRS

# MANRS

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

MANRS

# 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!!!**

MANRS

# *Resource Public Key Infrastructure* (RPKI)

# 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*

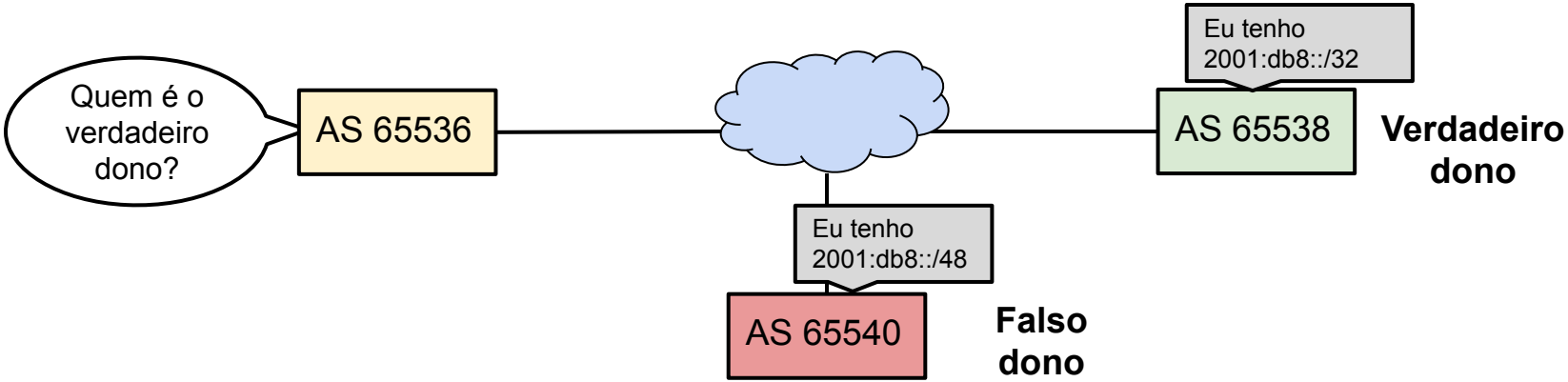
- **A colaboração de todos os ASes é essencial!!!**

# O que é RPKI?

**ROTAS:**

2001:db8::/32 … 65538 i

2001:db8::/48 … 65540 i

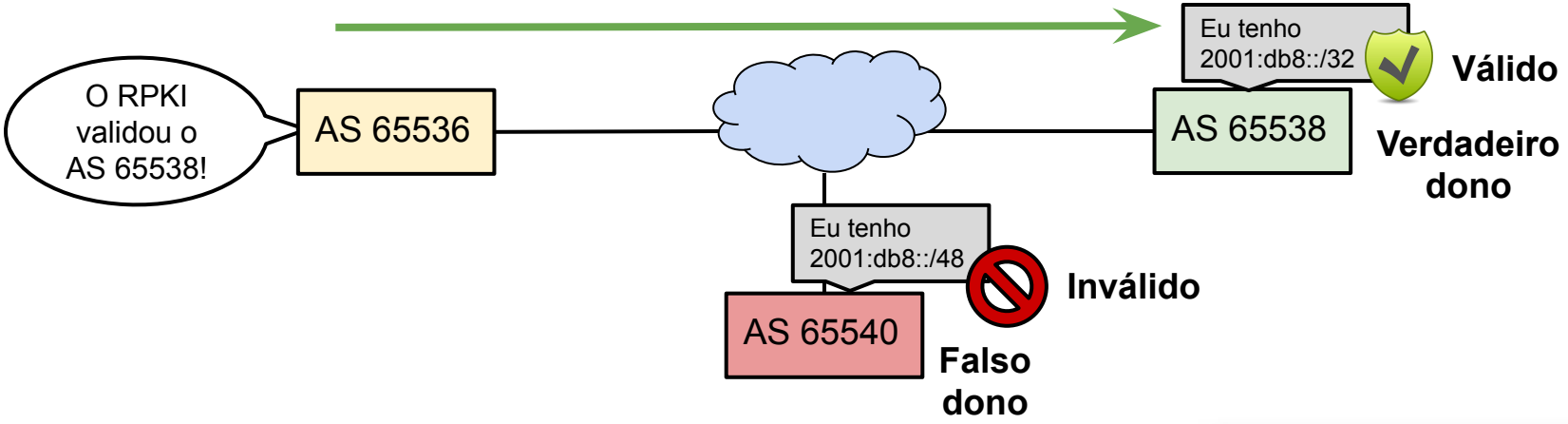


# O que é RPKI?

**ROTAS:**

2001:db8::/32 … 65538 i

2001:db8::/48 … 65540 i



# RPKI

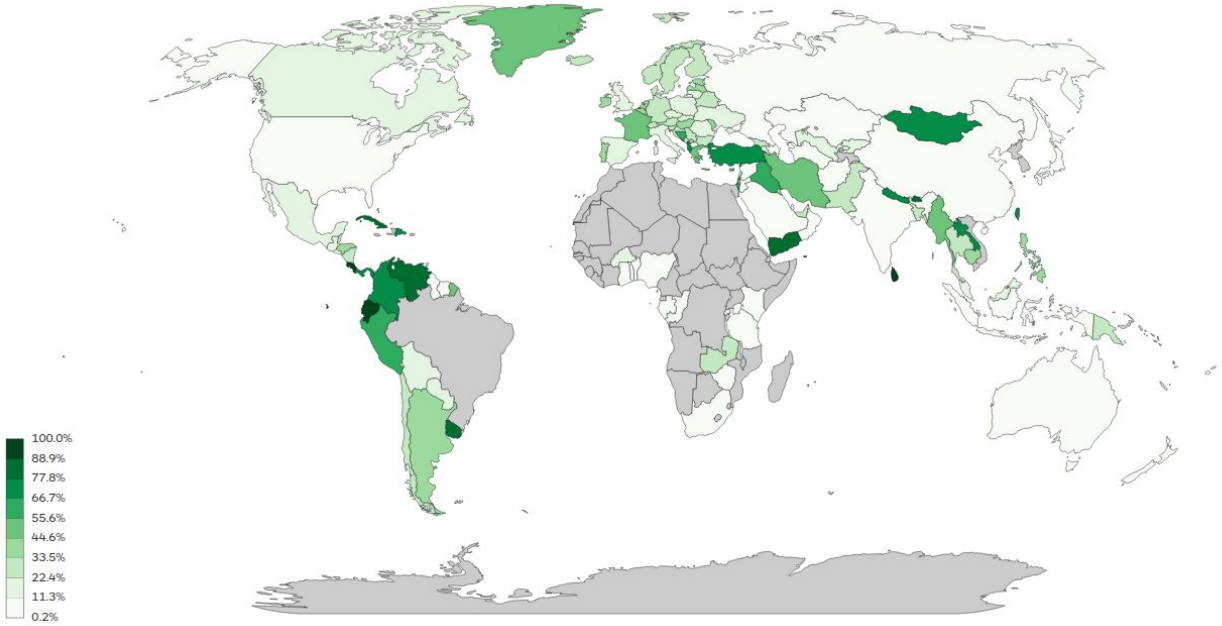
Vídeo - *Resource Certification Explained* (NRO)

- https://youtu.be/rH3CPosGNjY

Vídeo - *Why it's time to deploy* RPKI

- https://youtu.be/Y9vbbxr-GbI

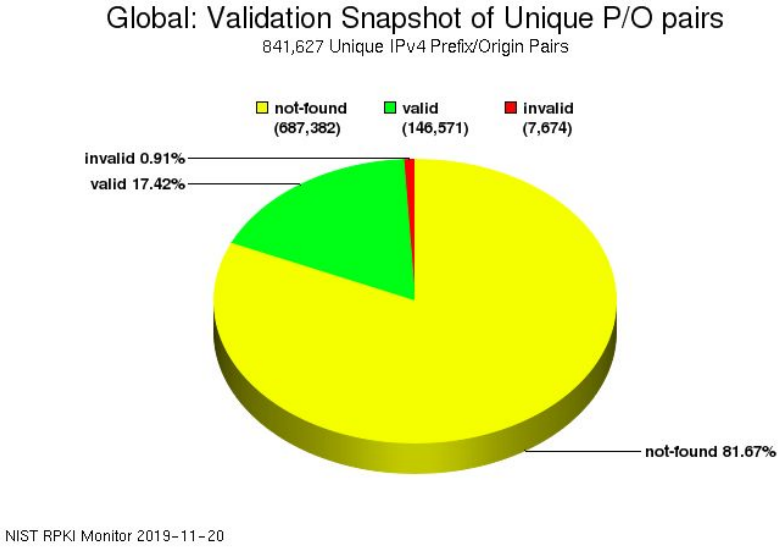
# Colaboração é essencial: Adoção do RPKI

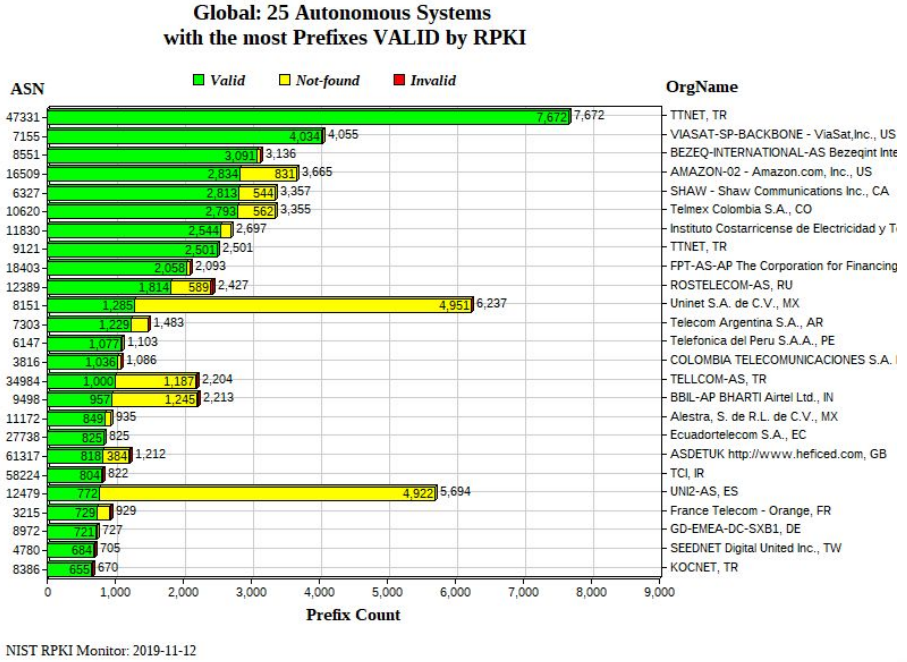



Fonte: https://www.nlnetlabs.nl/projects/rpki/rpki-analytics/

# Validação de rotas

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



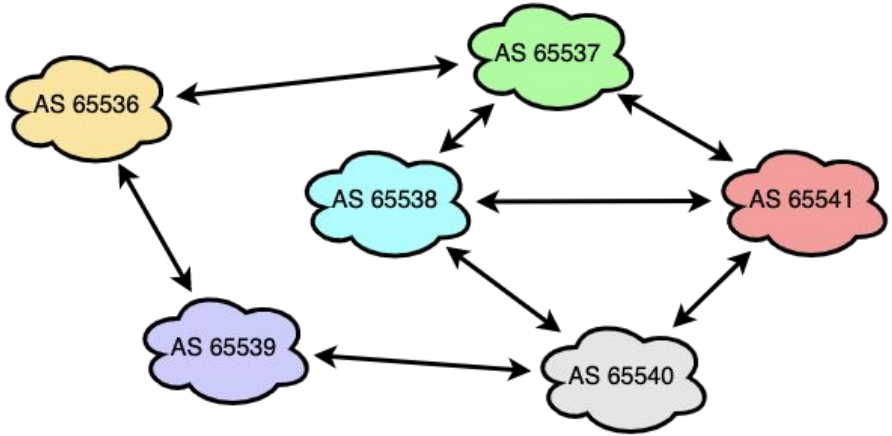




Fonte: https://rpki-monitor.antd.nist.gov/?p=0&s=0

# Parte II
# Conceitos fundamentais

# 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?

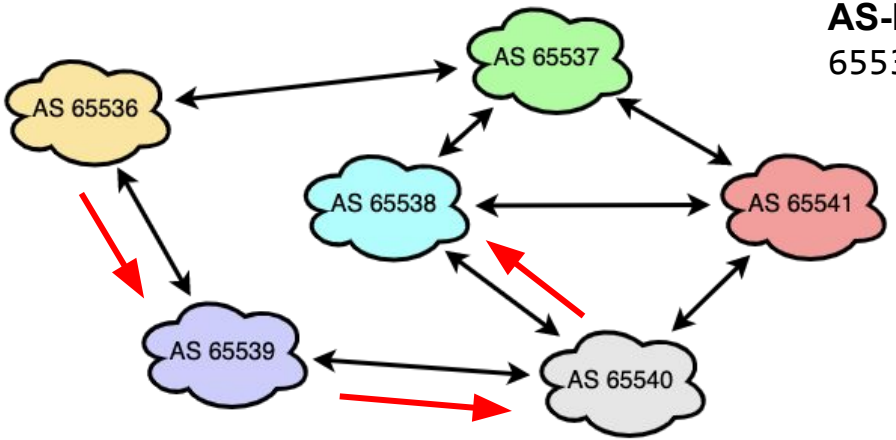
- O BGP é um protocolo do tipo “*path vector*”
- Trabalha com updates incrementais
- Tem várias opções diferentes para implementação de políticas de tráfego
- Usa o *Classless Inter-Domain Routing* (CIDR)
- Usado no *backbone* da Internet pelos ASes

# Funcionamento do BGP

- O BGP:
  - Aprende os diversos caminhos por meio dos protocolos iBGP e eBGP
  - Seleciona o melhor caminho e coloca-o na tabela *Routing Information Base* (RIB)
  - O melhor caminho é enviado para os vizinhos externos (eBGP)
  - Políticas são aplicadas para influenciar a seleção do melhor caminho

# O que é *path vector*?

- Uma rota é composta pela informação de destino e do caminho (*path*) até o destino, incluindo diversos atributos desse caminho.




**AS-PATH**

```
65539 65540 65538 i
```

# BGP

- Após a configuração, confia-se que as rotas anunciadas estão corretas
- Um anúncio pode influenciar escolha do melhor caminho
  - Prefixo mais específico
  - Menor caminho
  - Políticas internas

# BGP

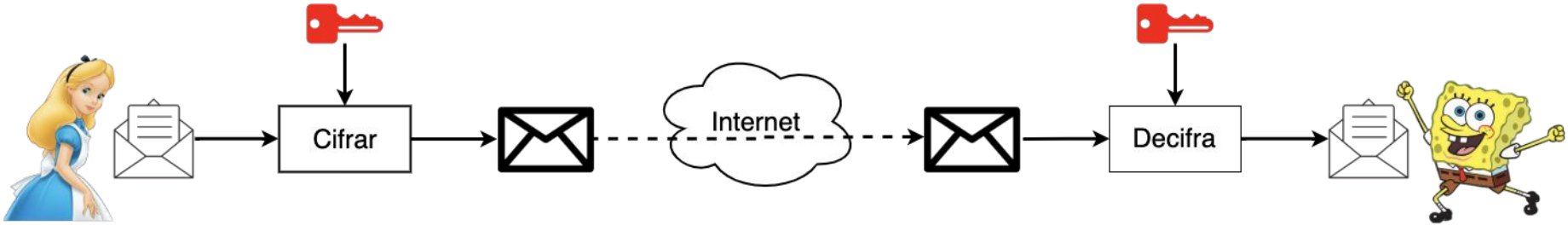
- **AS-PATH**
  - **Bem conhecido e mandatório**
  - **Indica o caminho para se chegar a um destino**, incluindo todos os ASes intermediários
  - Enviado em mensagens de UPDATE
    - Junto com o AS de origem do anúncio (*origin-as*).
  - É **usado** para:
    - **Detectar loops**
    - **Aplicar políticas**

# Conceitos de Segurança e certificação digital

# Criptografia simétrica

- Transformação matemática inversível cujo cálculo depende, no sentido direto (cifração) e no sentido inverso (decifração), de uma mesma informação secreta: a chave criptográfica.

- Provê apenas confidencialidade.

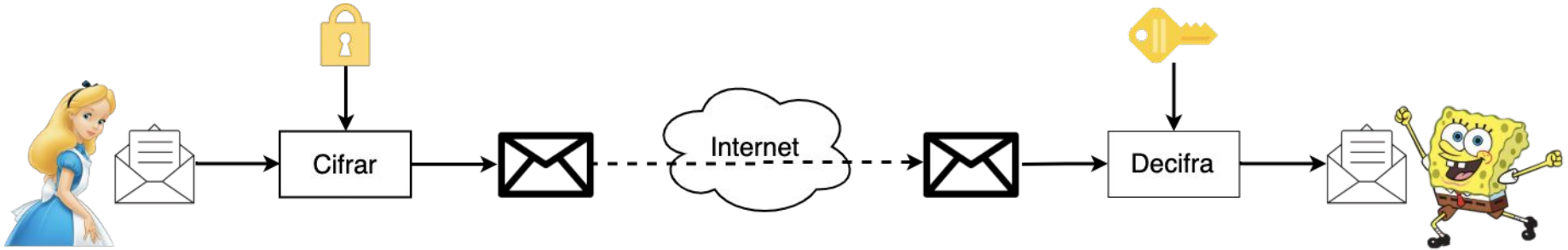


# Criptografia assimétrica

- 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 a outra chave.

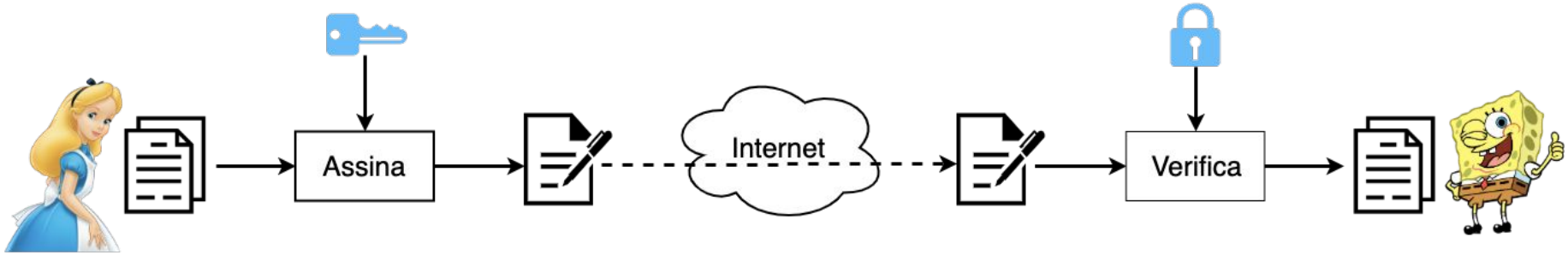
# Criptografia assimétrica

- Cifração: confidencialidade

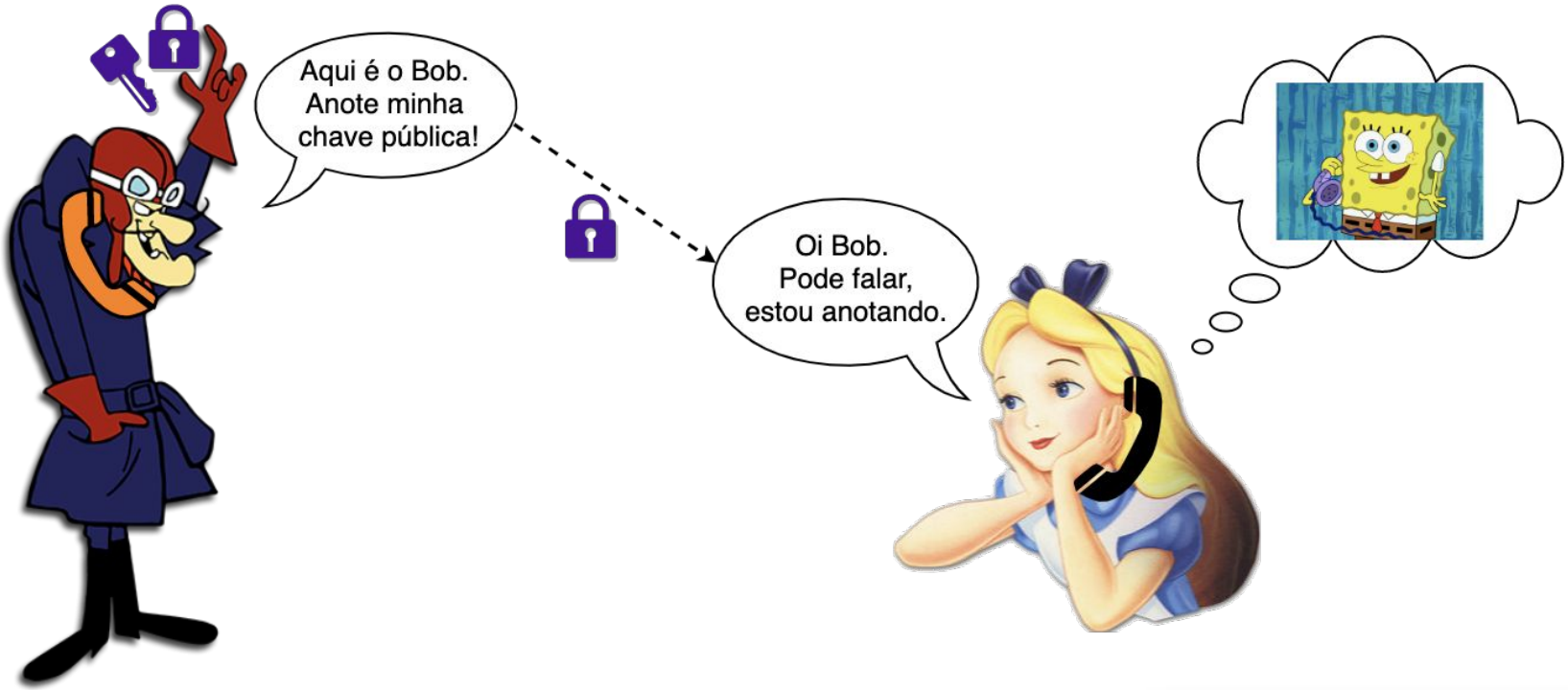


# Criptografia assimétrica

- Assinatura digital: integridade, autenticidade e irretratabilidade

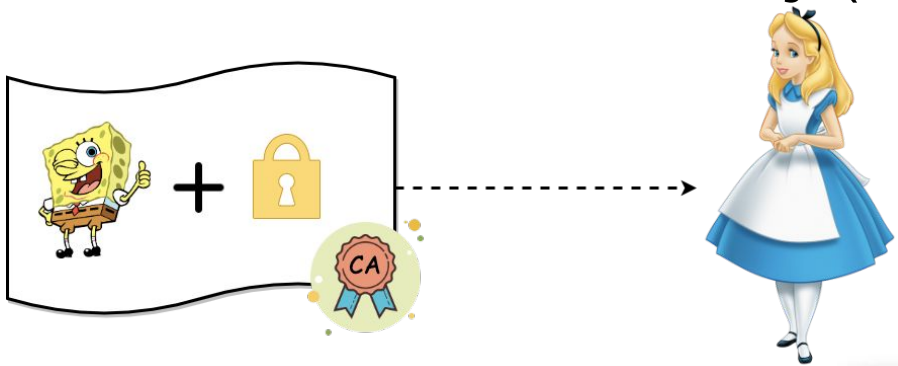


# Como garantir a credibilidade de uma chave pública?



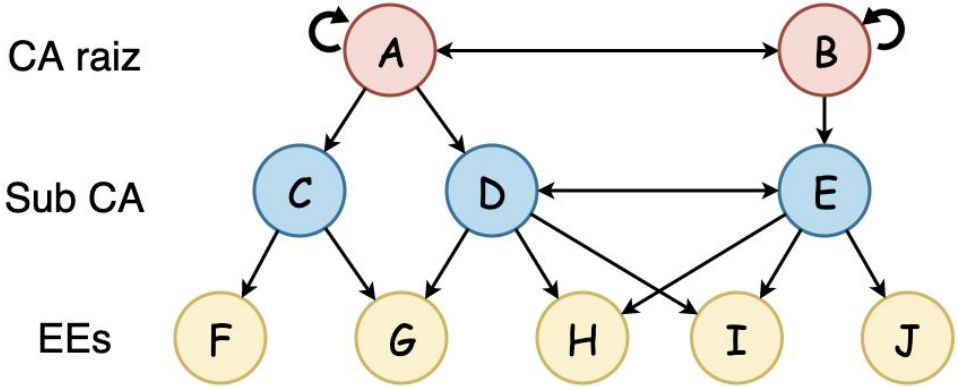
# Certificados digitais

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

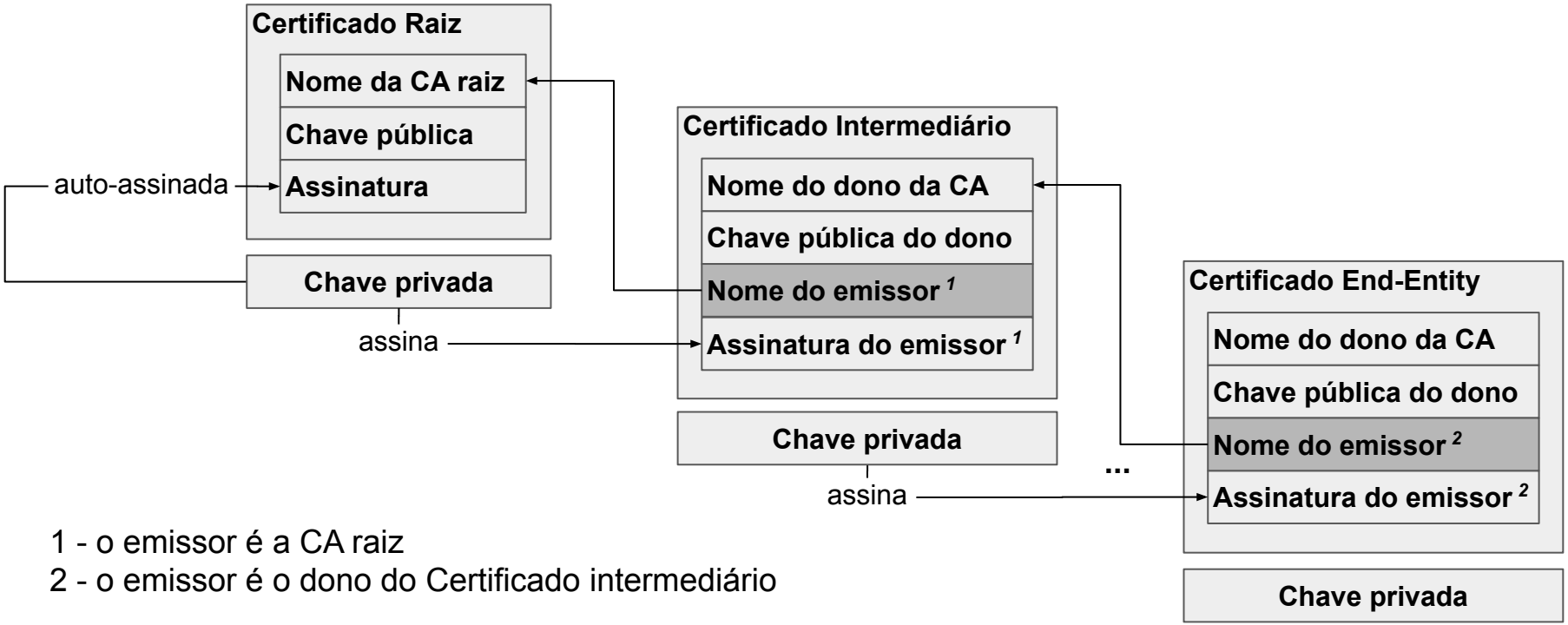


# Infraestrutura de Chaves Públicas

- 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 entidades finais ou *End Entities* (EEs).
  - Proteção das chaves mais críticas (mais próximas da raiz).

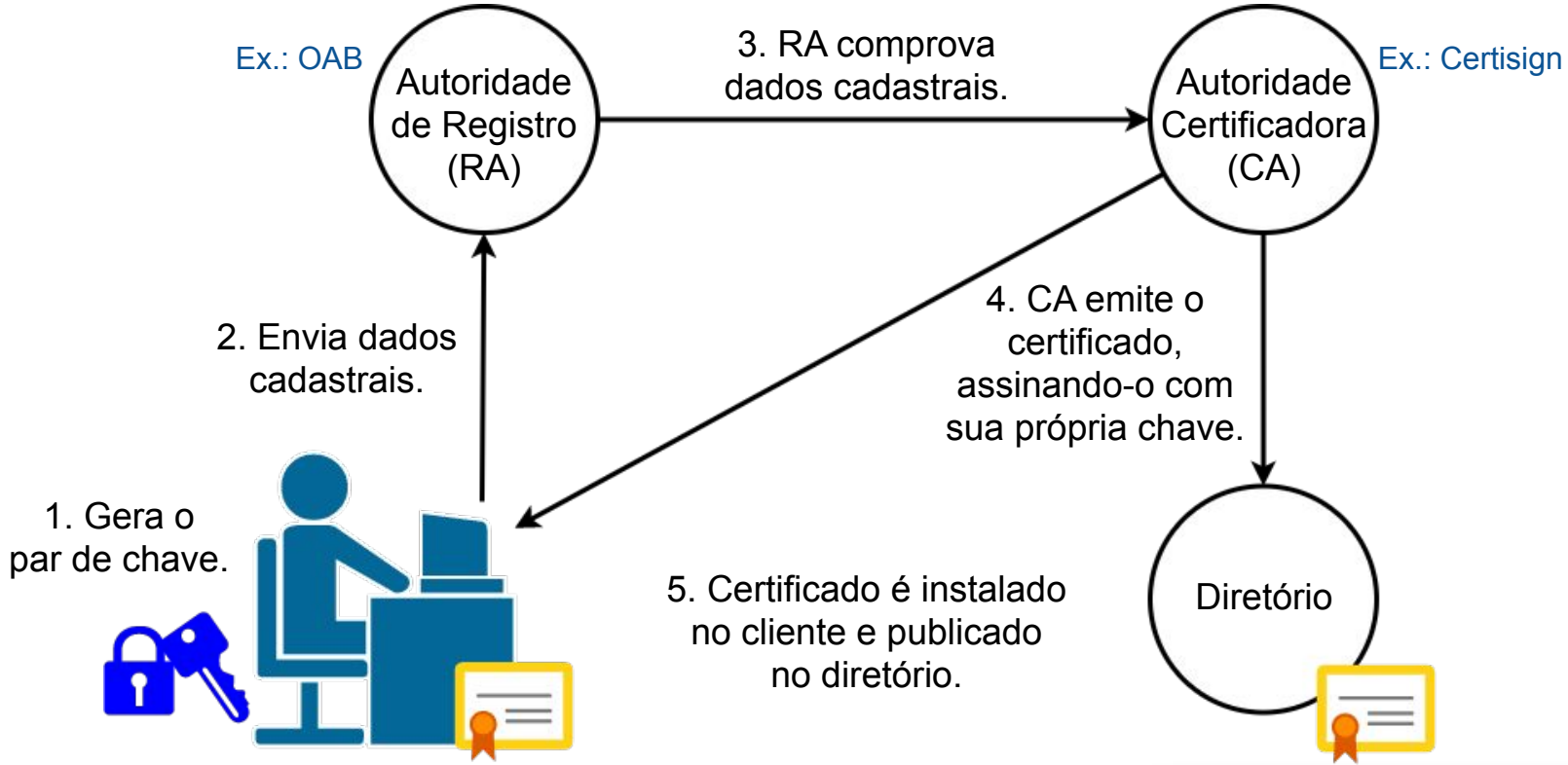


# Cadeia de certificação




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

# Processo de certificação PKI



# 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.

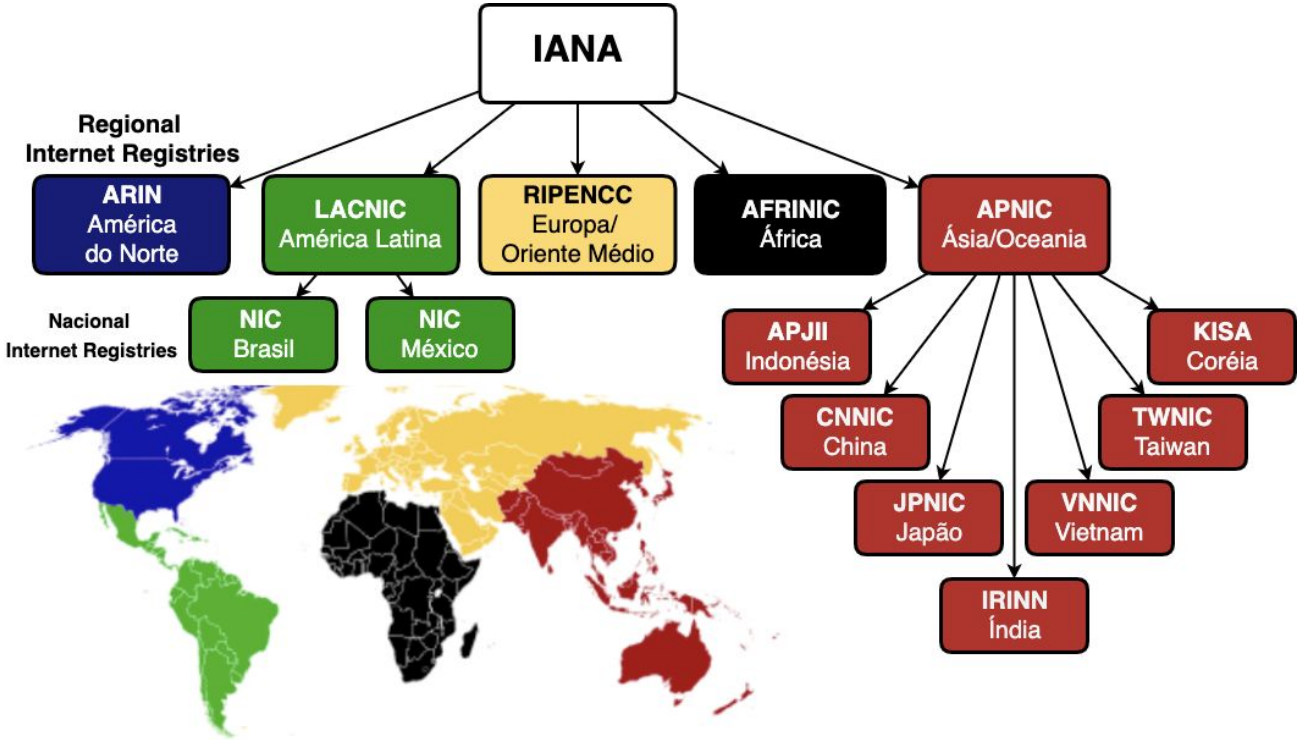
# Parte III
# RPKI: certificação de recursos

# Certificação de Recursos

RPKI: Certificar as alocações de IPs e ASNs

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

# Distribuição de recursos numéricos



# Cadeia de certificação do RPKI

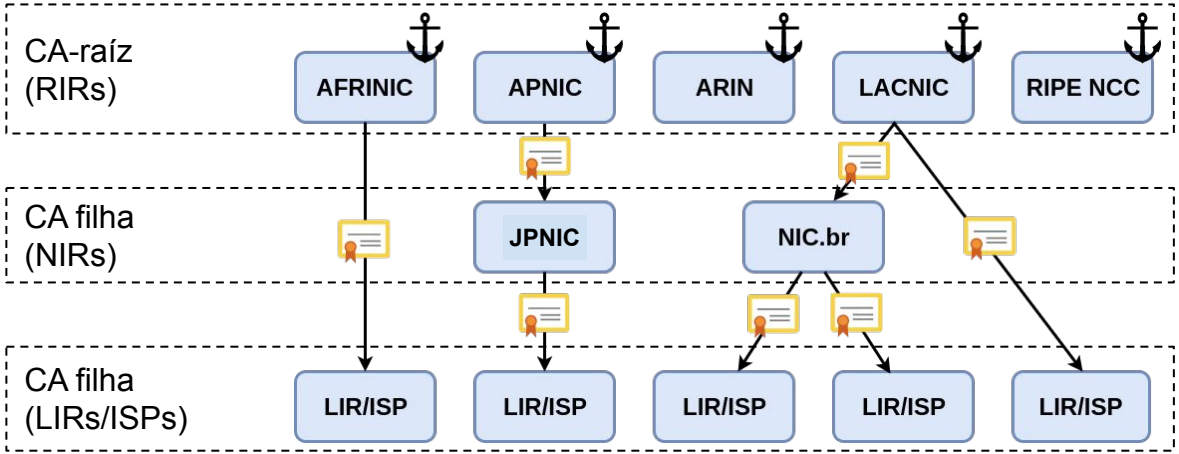
Cada RIR pode ser uma fonte autoritativa para a alocação de recursos

- Delegação de endereços IPs (IPv4 e IPv6)
- Delegação de ASNs

Funcionam como CA do par IPs-ASN e da chave pública do AS

# Cadeia de certificação do RPKI

- RIRs
  - *Trust Anchor*
    - Confiabilidade implicita
    - Certificados auto-assinados
  - 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

# 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 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**

| | |
|---|---|
| Prefixo | <IP>/<prefixo> |
| ASN | XXXX |
| Prefixo Max | /<prefixo> |
| Tempo de validade | TTTT |
| 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

- Alocações no ROA devem vir da organização responsável pelos recursos (CA)
- Armazenados em repositórios públicos confiáveis

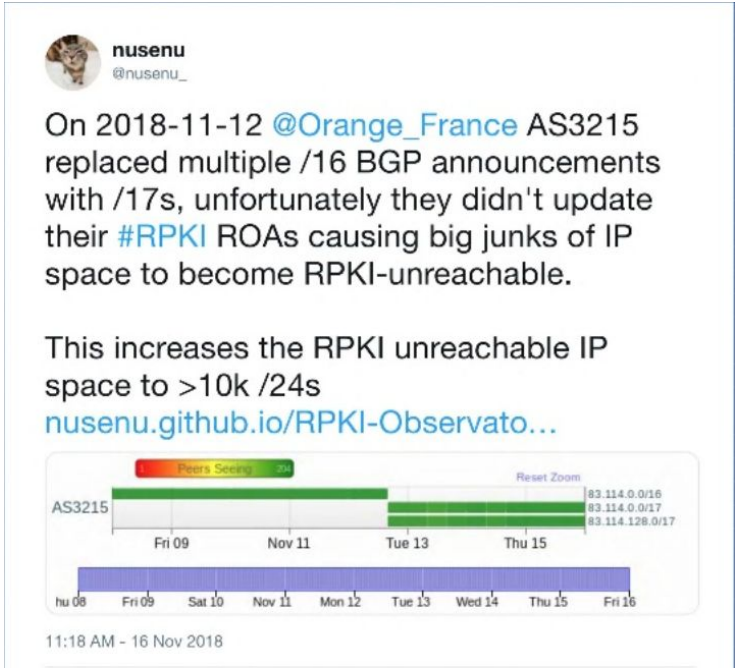
# ROAs

- 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!

# Manutenção é essencial!

**Não esqueça do RPKI!**

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



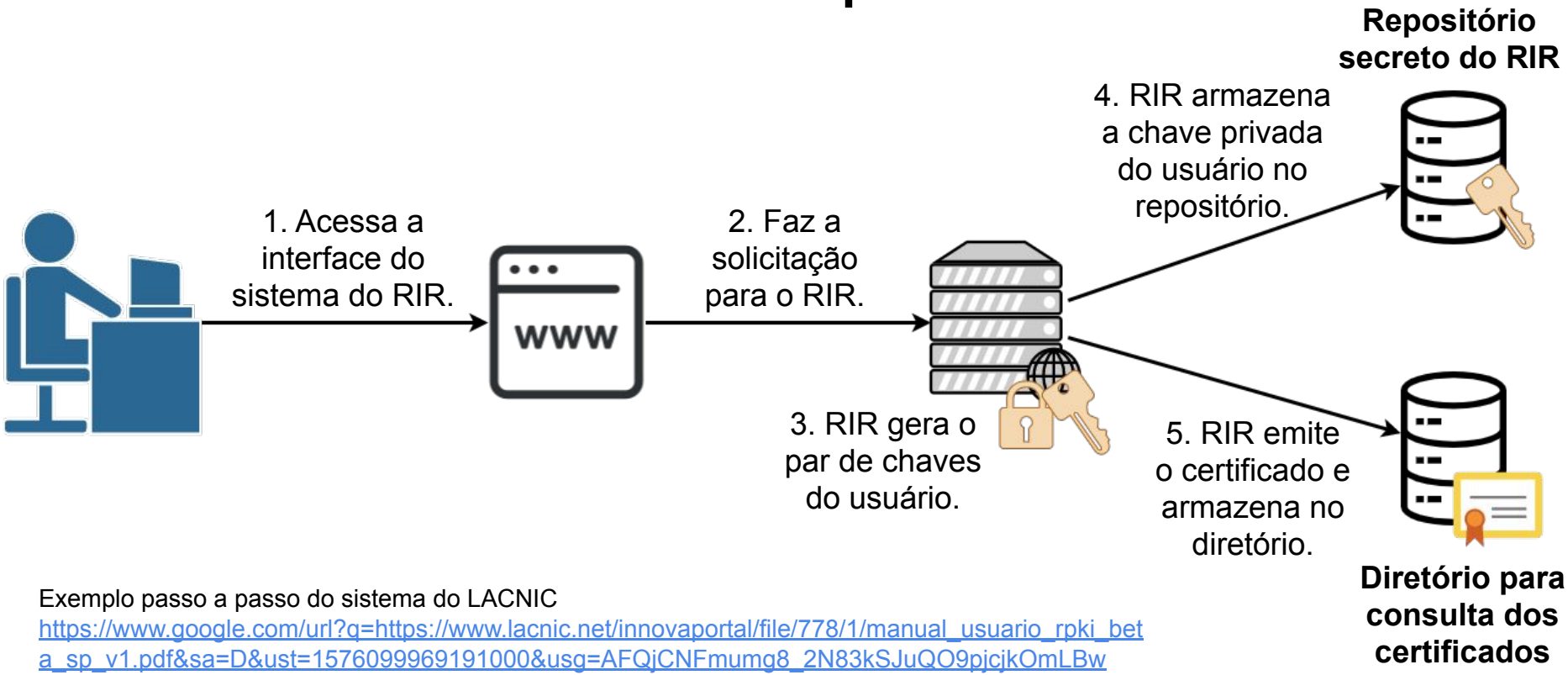
# Modos de operação no RPKI

- 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

# 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**
  - rpkid - Dragon Research Labs

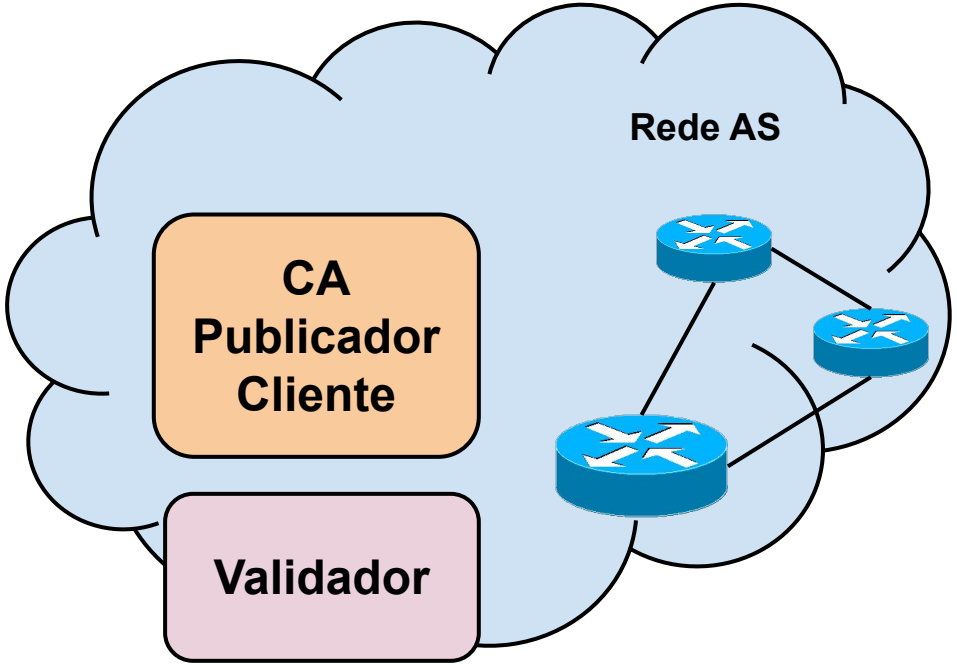
- **Servidor de publicação**
  - Próprio (alta disponibilidade) ou de **terceiros** (NIC.br)

# Componentes principais para adotar o RPKI

- Autoridade Certificadora (CA)
- Servidores de publicação (repositórios)
- *Relying Party* (RP) / Validador
- Roteadores com suporte RPKI

# RPKI


RIR/NIR
Autoridades Certificadoras
ROAs
Manifesto
CRLs
Repositório RPKI
Certificação
de recursos e publicação


Rede AS
CA
Publicador
Cliente
Validador

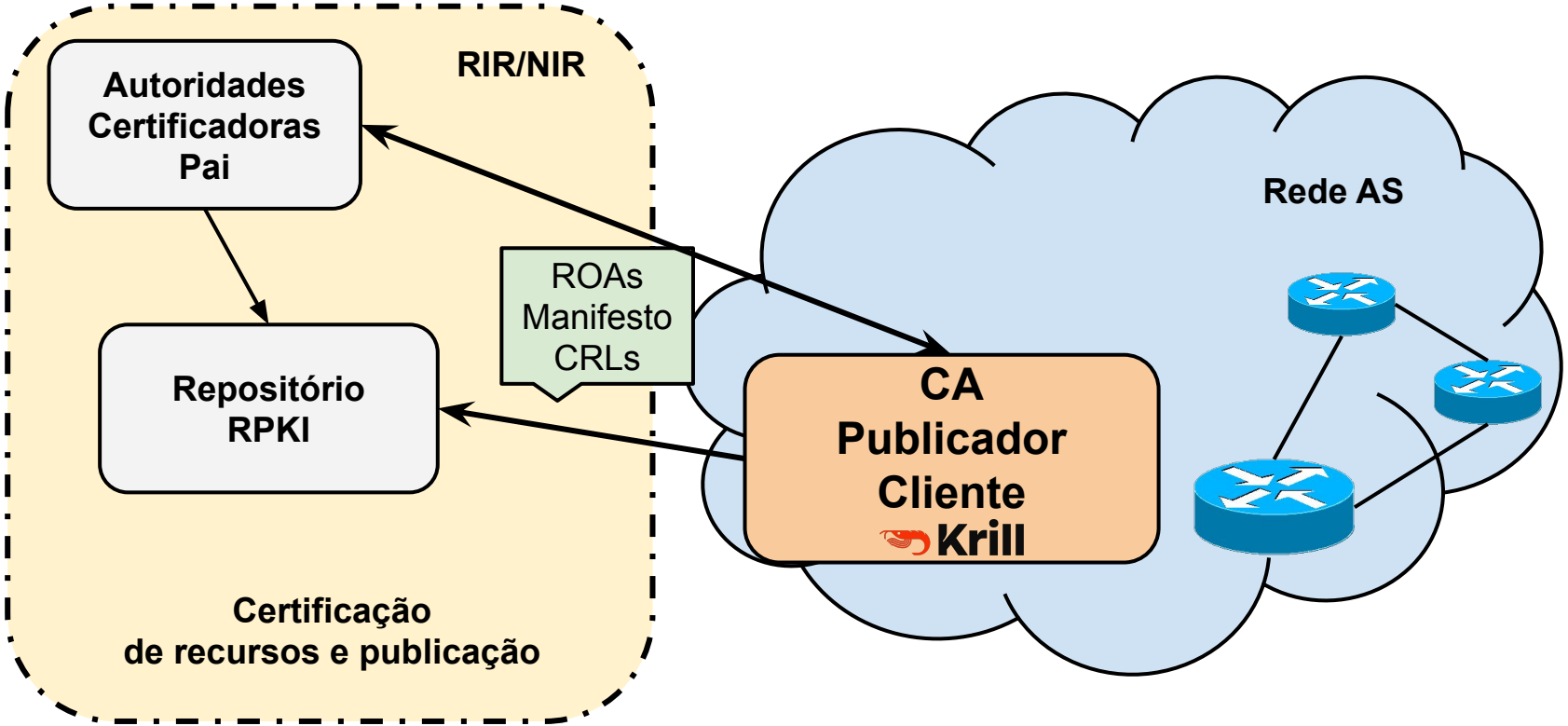
# Papel da Organização no RPKI

- Certificar recursos
  - São CA dos próprios recursos
  - Geram e assinam ROAs
  - Disponibilizam certificados e ROAs em um repositório público

# Papel da Organização no RPKI

- Validar o originador do prefixo no BGP
  - Verificam a validade dos objetos assinados
  - Enviam validações para os roteadores
  - Configuram roteadores para utilizar RPKI
  - Utilizam os dados do RPKI para decisões de roteamento
    - Filtros
    - *Communities*

# RPKI: Recapitulando

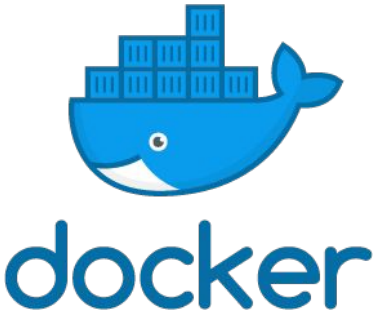


# O que é o Krill?

- Software *open source*
  - Criação, gerenciamento, publicação de CAs e ROAs
- Possui repositório próprio, mas permite a utilização de repositório de terceiros
- Atualmente, funciona apenas por linha de comando
  - Em breve terá interface gráfica para usuário

# Instalação do Krill

- Duas opções




OU

OpenSSL
Cryptography and SSL/TLS Toolkit

+

Rust

+

**C toolchain**

Fonte: https://rpki.readthedocs.io/en/latest/krill/installation.html

# Subindo o servidor Krill

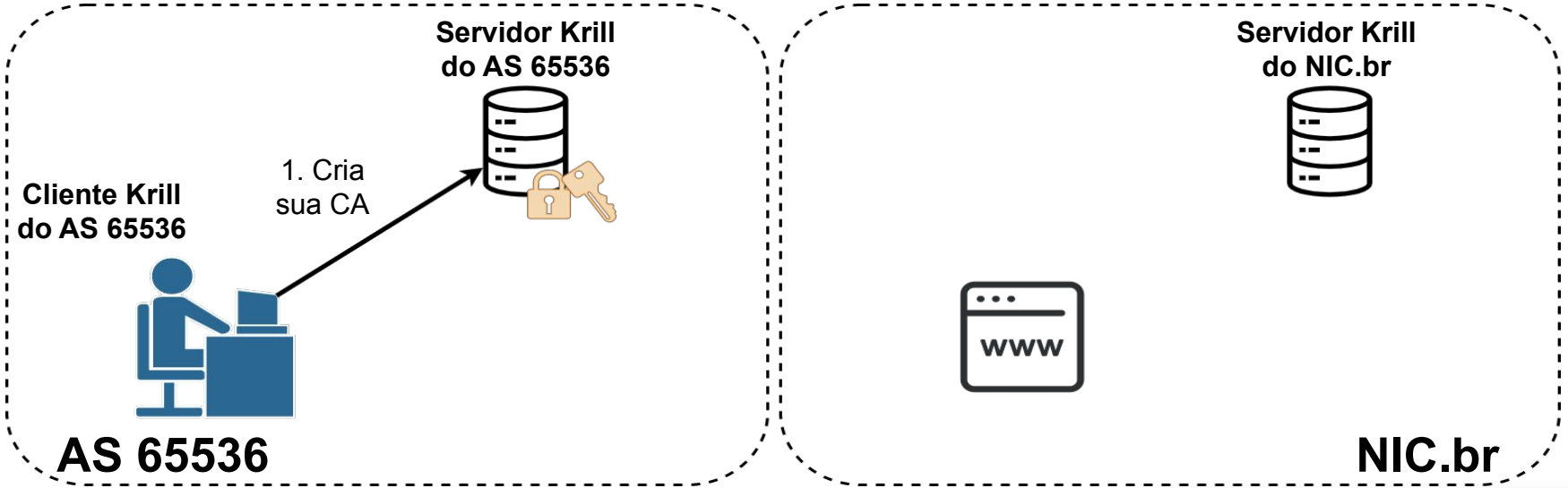
Passo inicial

```
$ krill -c krill.conf
```

# Cadastrando uma CA com Krill

1. Criar CA do AS 65536 pelo cliente Krill do AS 65536

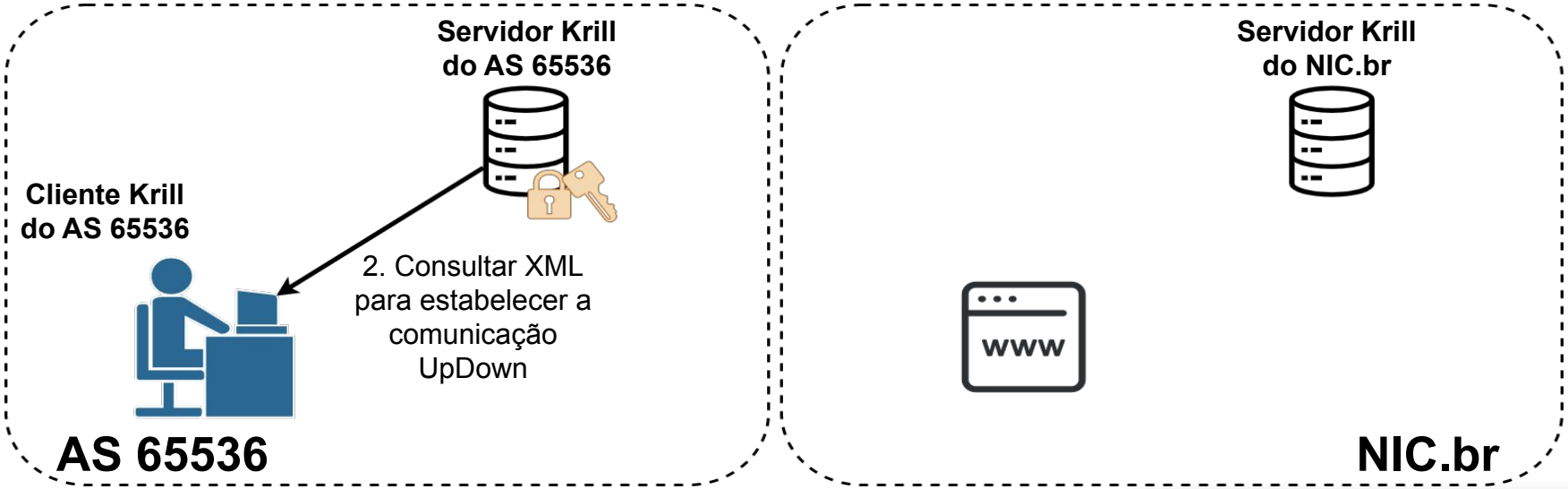
```
$ krillc add --server <URL> --token <senha> --ca <nome>
```



# Cadastrando uma CA com Krill

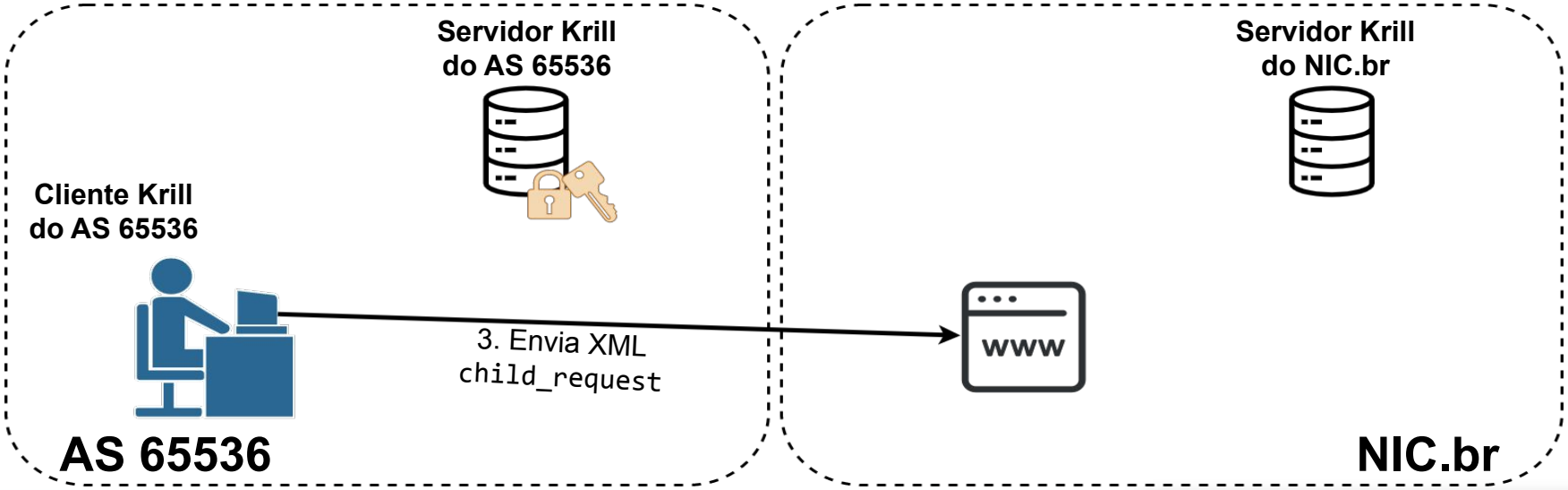
2. Consultar XML `child_request` para estabelecer a comunicação UpDown entre o AS 65536 e o NIC.br

```
$ krillc parents myid --server <URL> --token <senha> --ca <nome>
```



# Cadastrando uma CA com Krill

3. Enviar XML `child_request` para o sistema do NIC.br



# Cadastrando uma CA com Krill

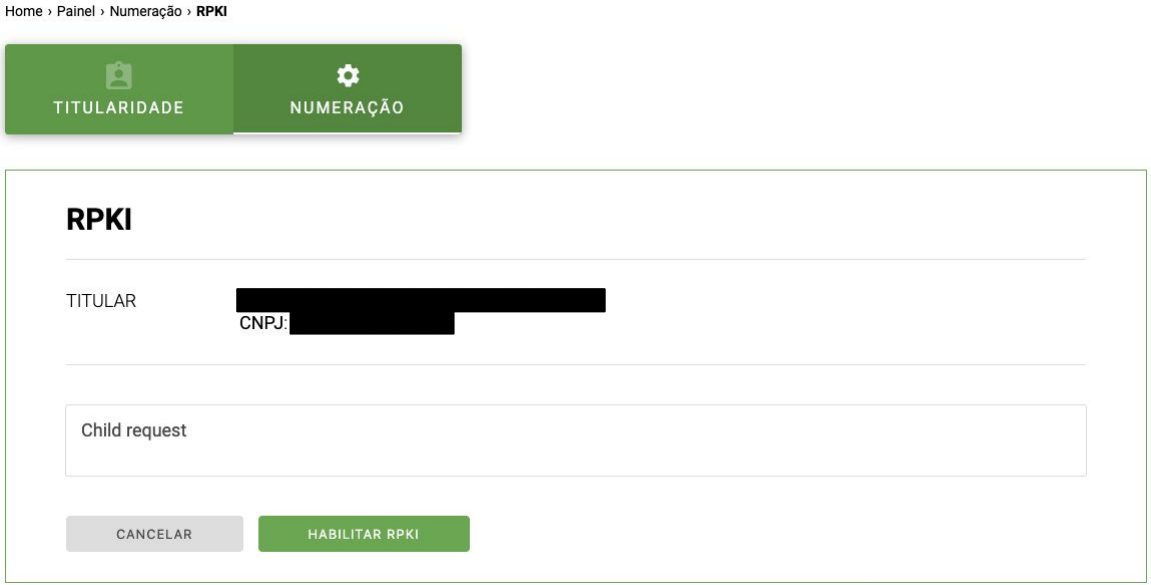
3. Enviar XML `child_request` para o sistema do NIC.br
   3.1. Login no sistema do Registro.br > Titularidade

# Cadastrando uma CA com Krill

3. Enviar XML `child_request` para o sistema do NIC.br
   3.2. Titularidade > RPKI

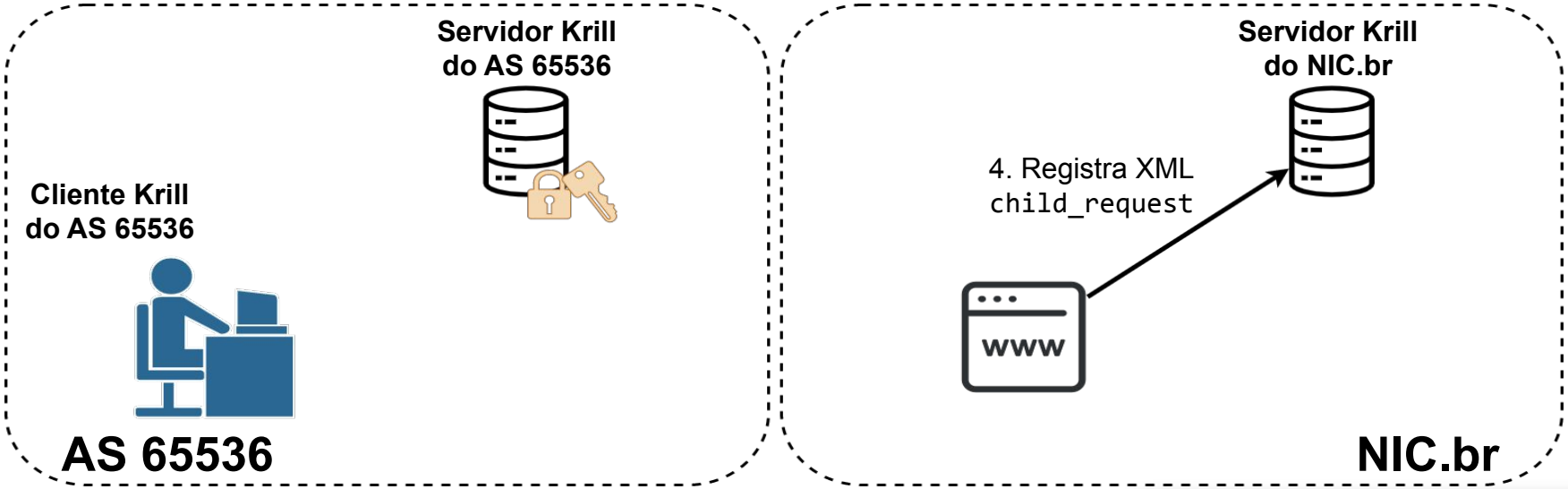
# Cadastrando uma CA com Krill

3. Enviar XML `child_request` para o sistema do NIC.br
   3.3. RPKI > enviar o `child_request`



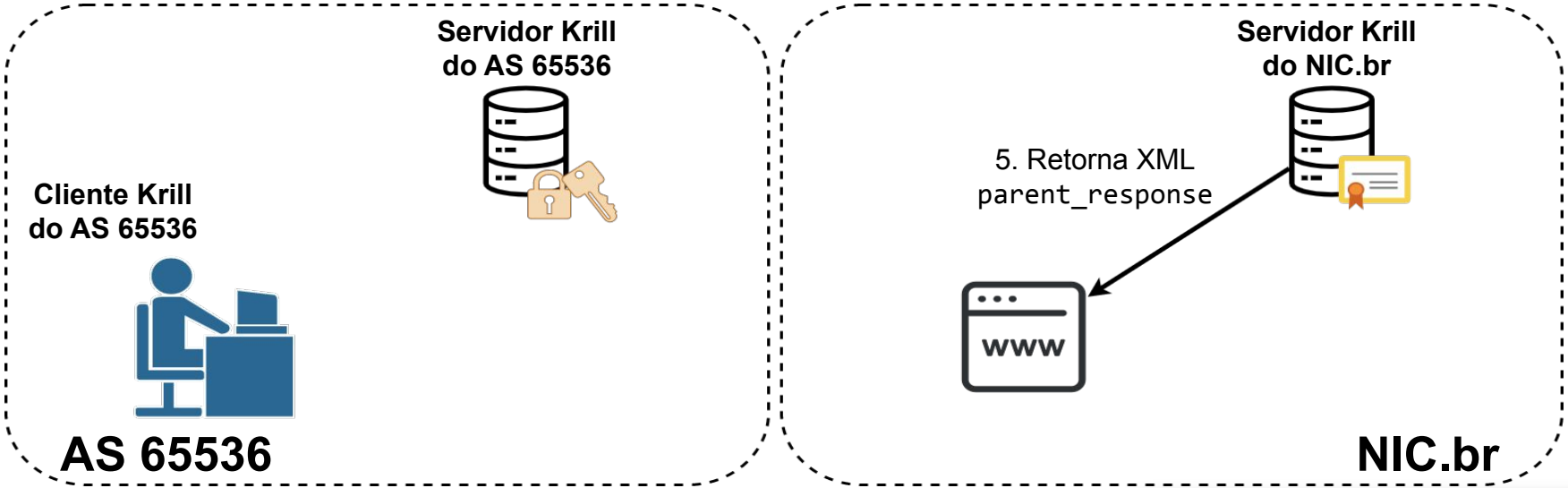
# Cadastrando uma CA com Krill

4. Servidor Krill do NIC.br registra XML `child_request` do AS 65536



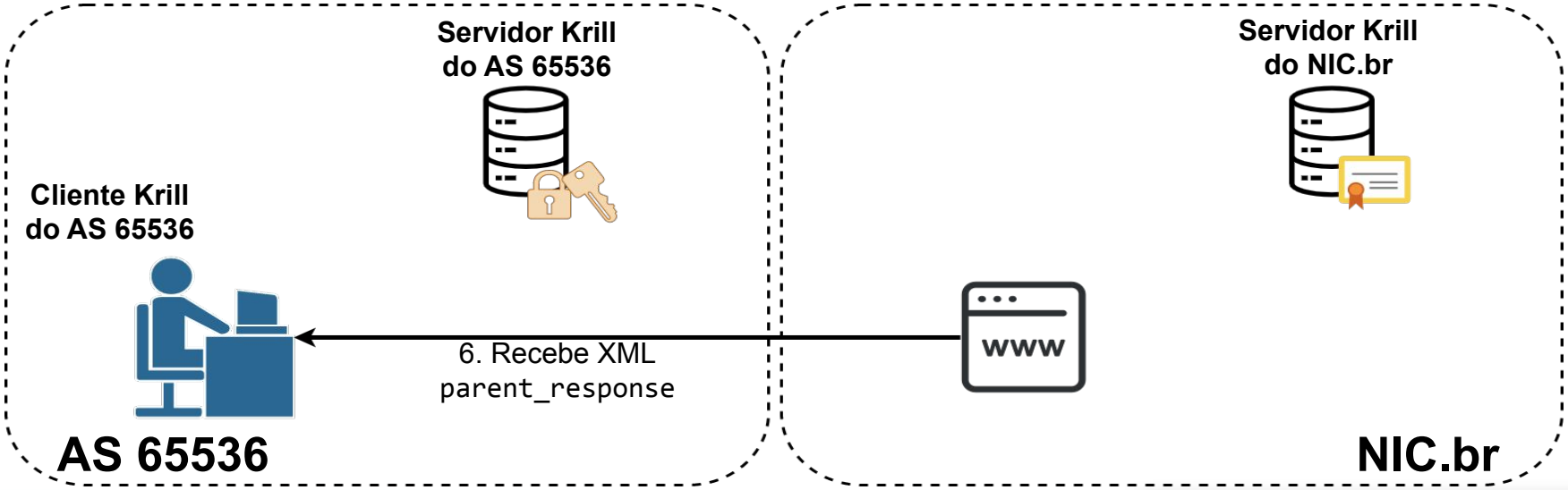
# Cadastrando uma CA com Krill

5. Retorna XML `parent_response` do AS 65536



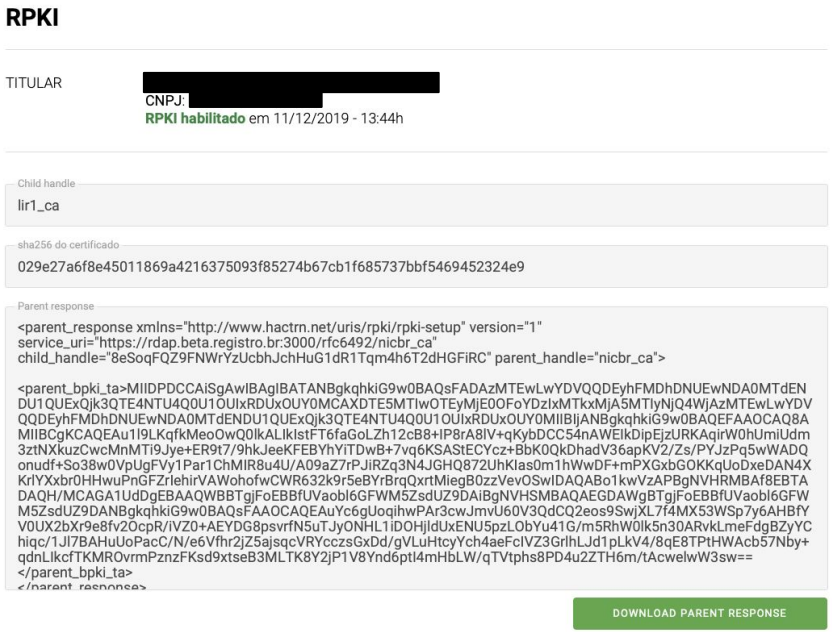
# Cadastrando uma CA com Krill

6. AS 65536 recebe XML `parent_response`



# Cadastrando uma CA com Krill

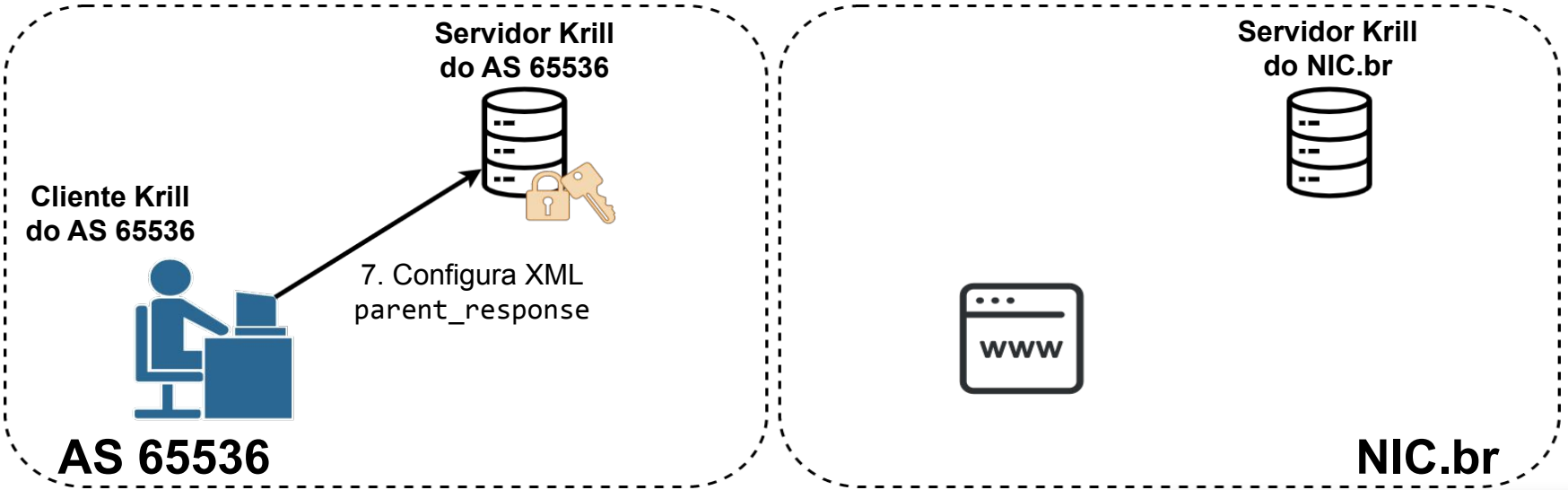
6. AS 65536 recebe XML `parent_response`



# Cadastrando uma CA com Krill

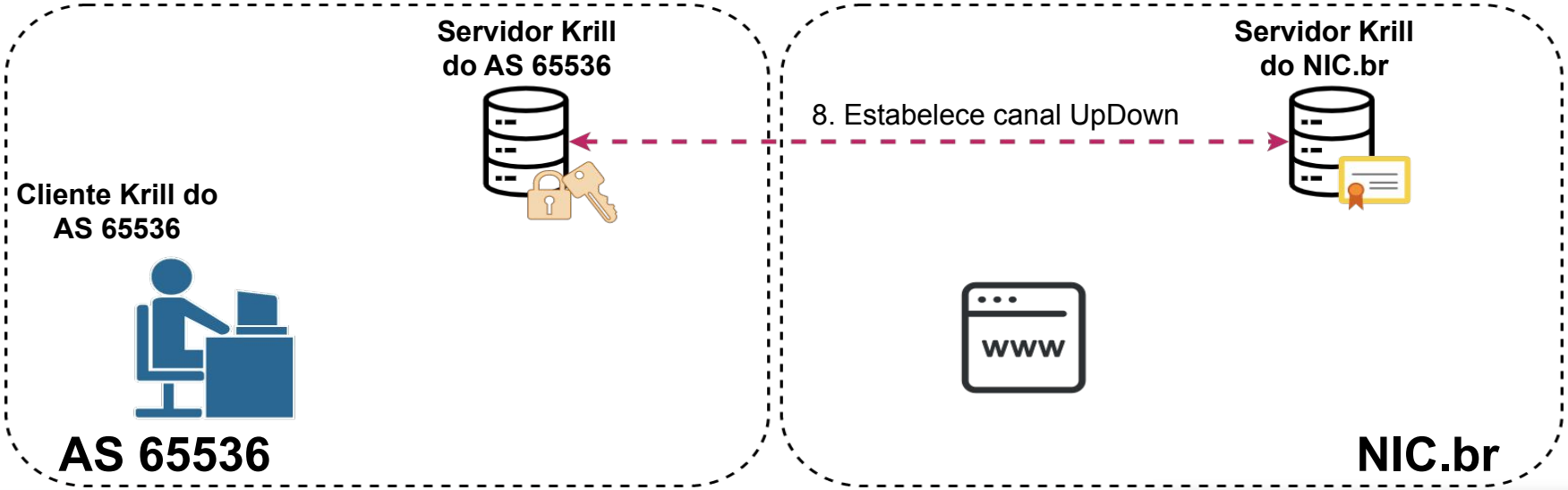
7. AS 65536 configura XML `parent_response` no seu Servidor Krill

```
$ krillc parents add --server <URL> --token <senha> --ca <nome>
    --parent <nome> --rfc8183 <arquivo XML>
```



# Cadastrando uma CA com Krill

8. Sincroniza Servidor Krill do AS 65536 com o Servidor Krill do NIC.br, criando o canal de comunicação UpDown para a troca de informações das CAs



# Criação de ROAs no Krill

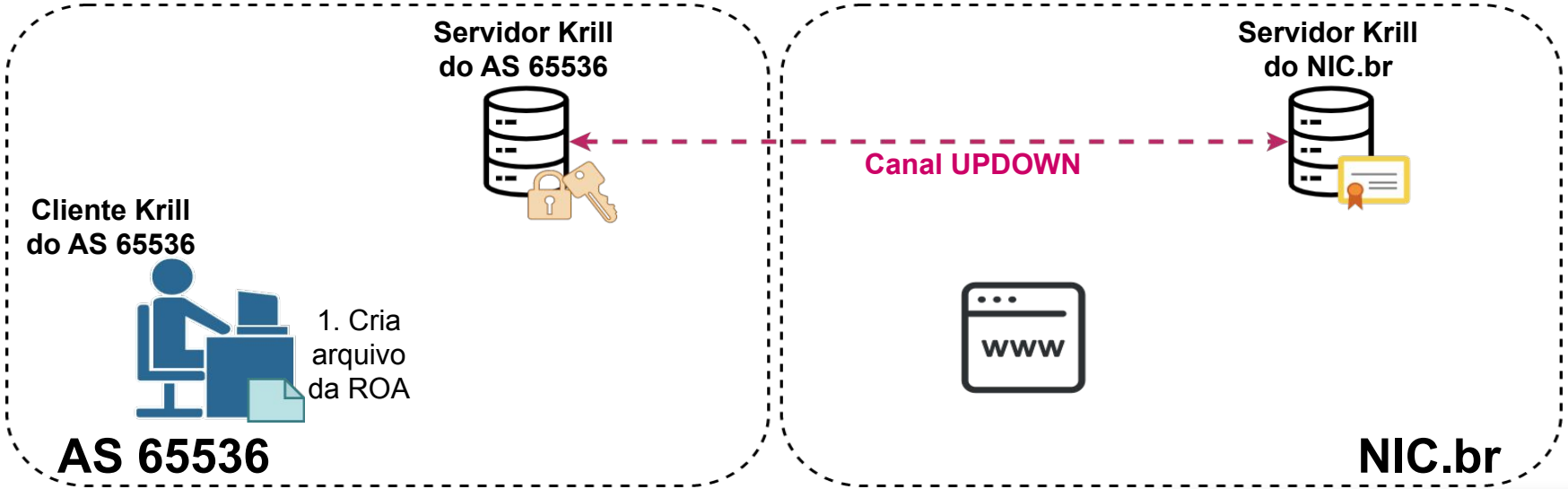
1. Criar arquivo texto de modificação das ROAs de um ASN ou mais

```
# Some comment
  # Indented comment

A: Y.Y.Y.Y/24 => XXXX
A: W:W:W::/48 => XXXX
A: Y.Y.Y.Y/16-20 => XXXX   # Add prefix with max length
R: Y.Y.Y.Y/24 => XXXX      # Remove existing authorization
```

Fonte: https://rpki.readthedocs.io/en/latest/krill/manage-cas.html#roas

# Criação de ROAs no Krill

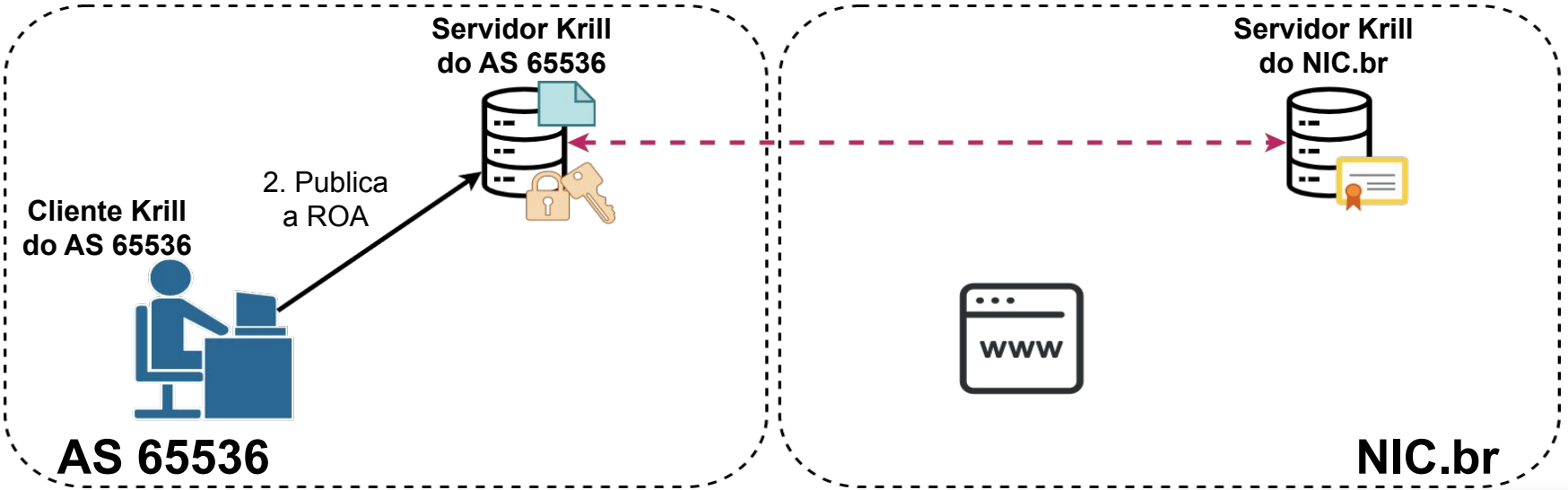
1. Criar arquivo texto de modificação das ROAs de um ASN ou mais



# Criação de ROAs no Krill

## 2. Publica a ROA no servidor Krill local do ASN 65536

```
$ krillc roas update --server <URL> --token <senha> --ca <nome>
      --delta <arquivo TXT>
```

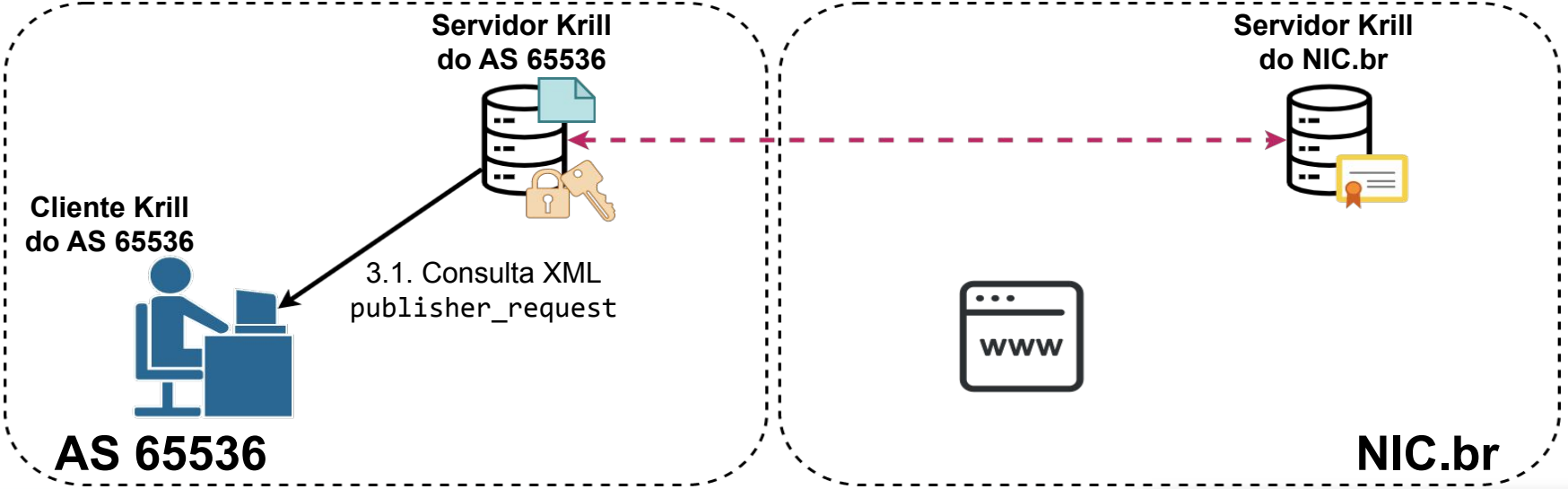


# Criação de ROAs no Krill

3. (Opcional) Publica a ROA no servidor Krill remoto do NIC.br

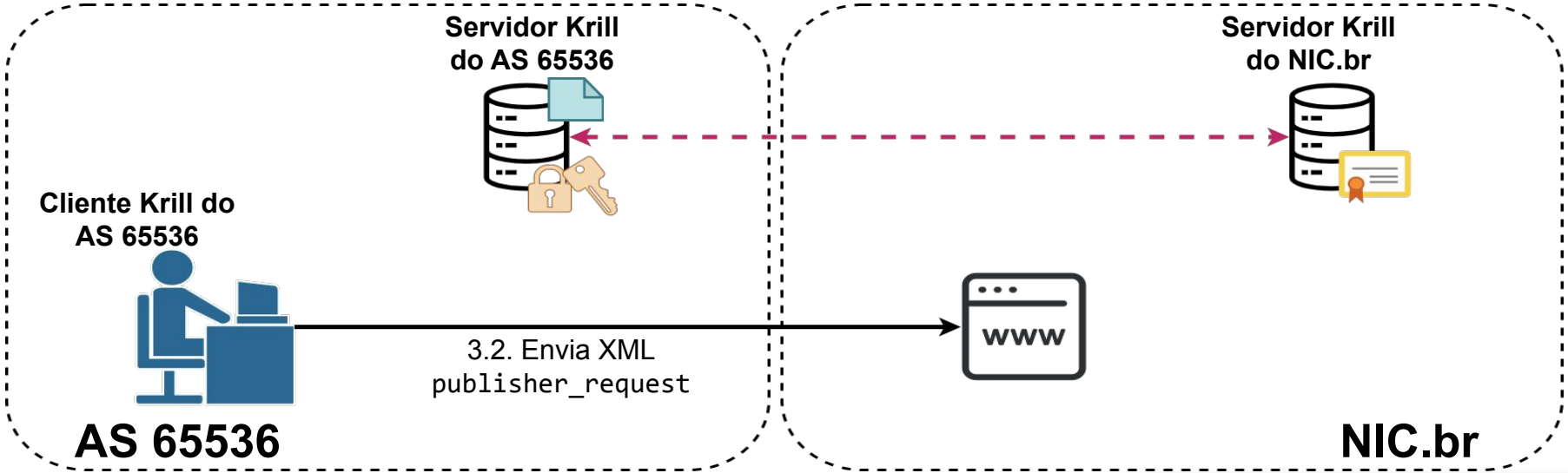
3.1. Consultar o XML `publisher_request`

```
$ krillc repo request --server <URL> --token <senha> --ca <nome>
```



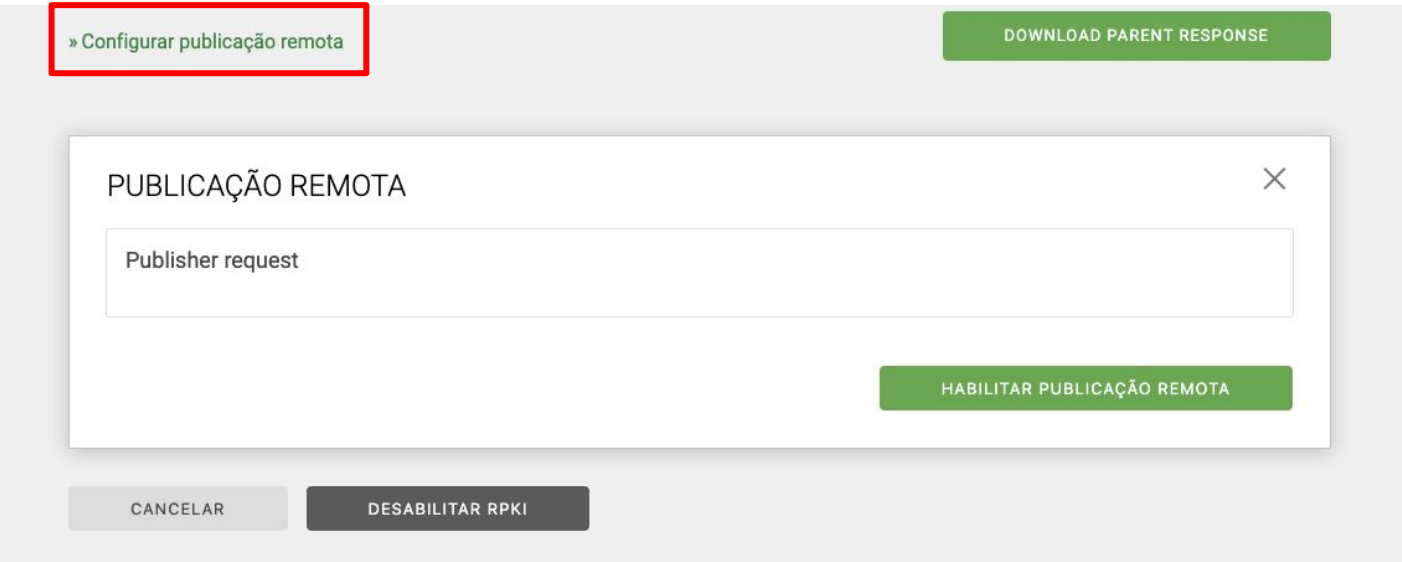
# Criação de ROAs no Krill

## 3.2. Envia do XML `publisher_request` para o sistema do NIC.br



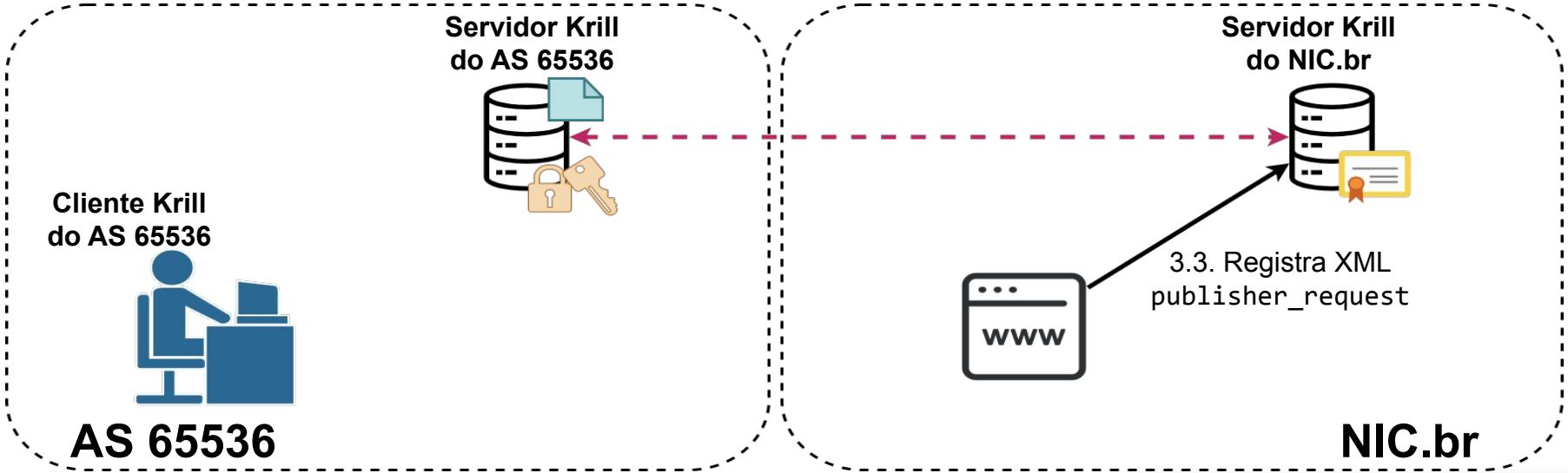
# Criação de ROAs no Krill

## 3.2. Envia do XML `publisher_request` para o sistema do NIC.br



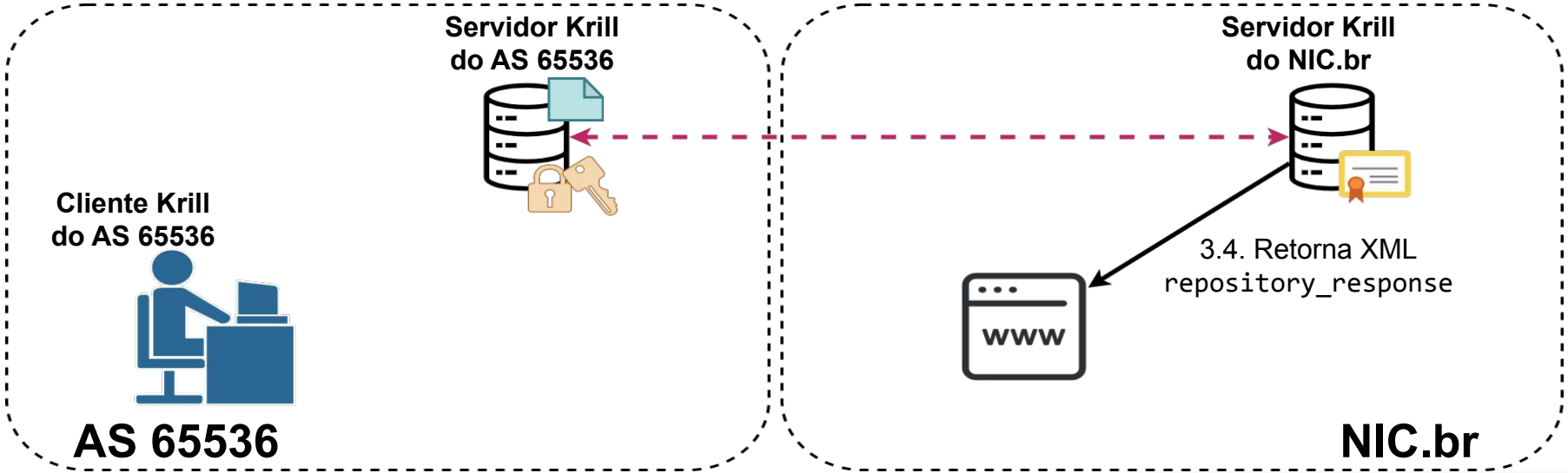
# Criação de ROAs no Krill

## 3.3. Servidor Krill do NIC.br registra XML `publisher_request` do AS 65536



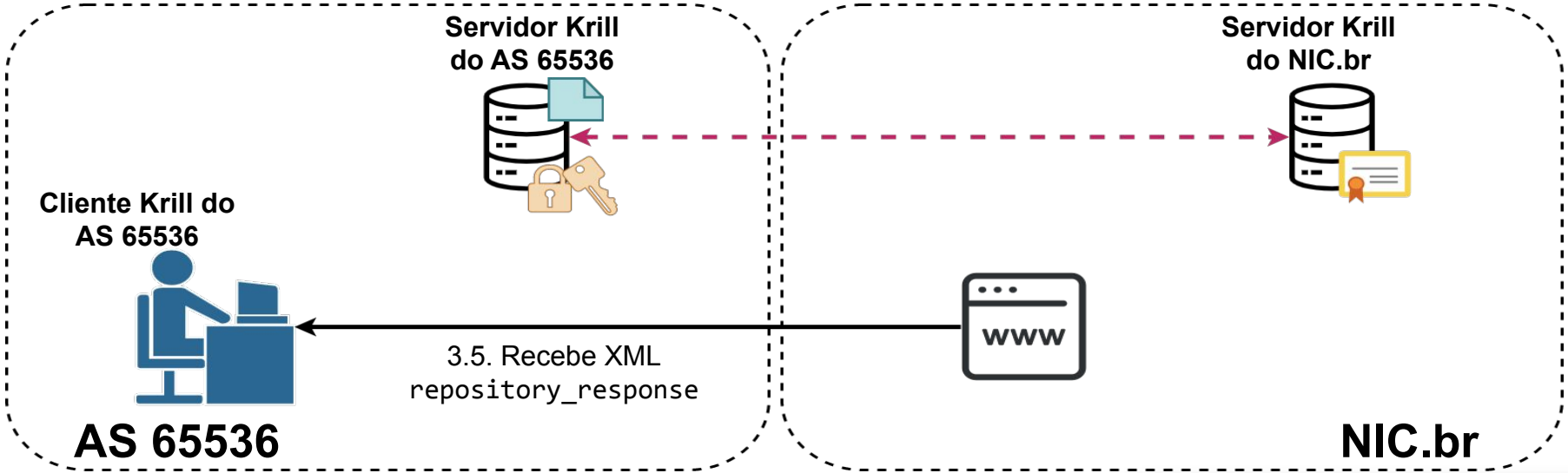
# Criação de ROAs no Krill

## 3.4. Retorna XML `repository_response`



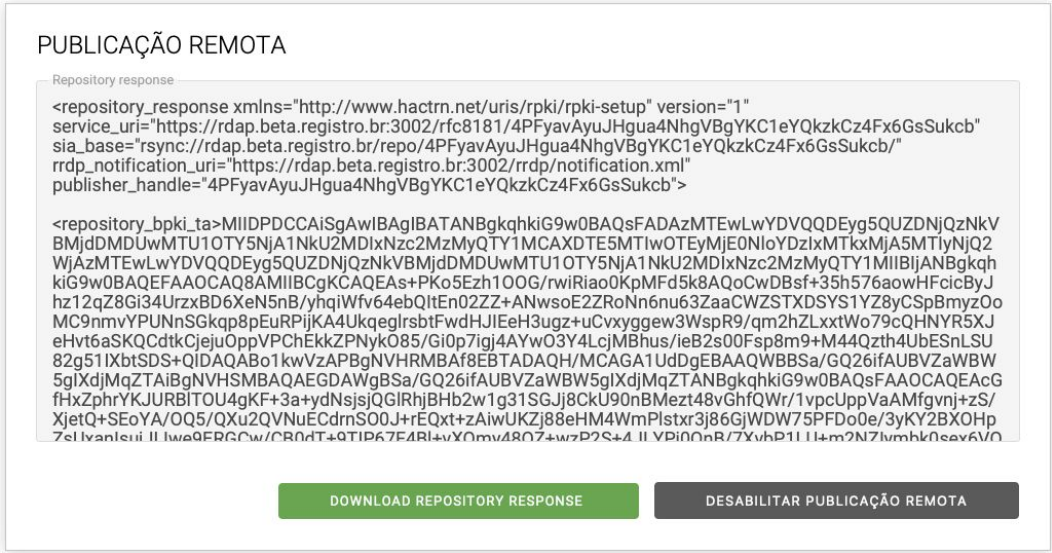
# Criação de ROAs no Krill

## 3.5. Recebe o XML `repository_response`



# Criação de ROAs no Krill

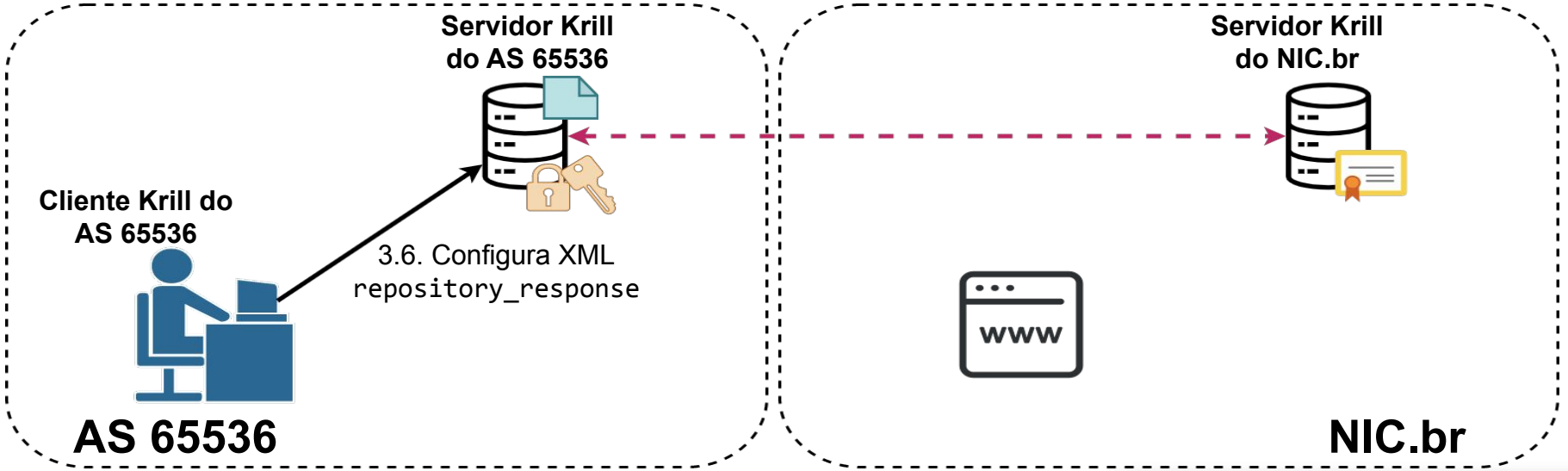
## 3.5. Recebe o XML `repository_response`



# Criação de ROAs no Krill

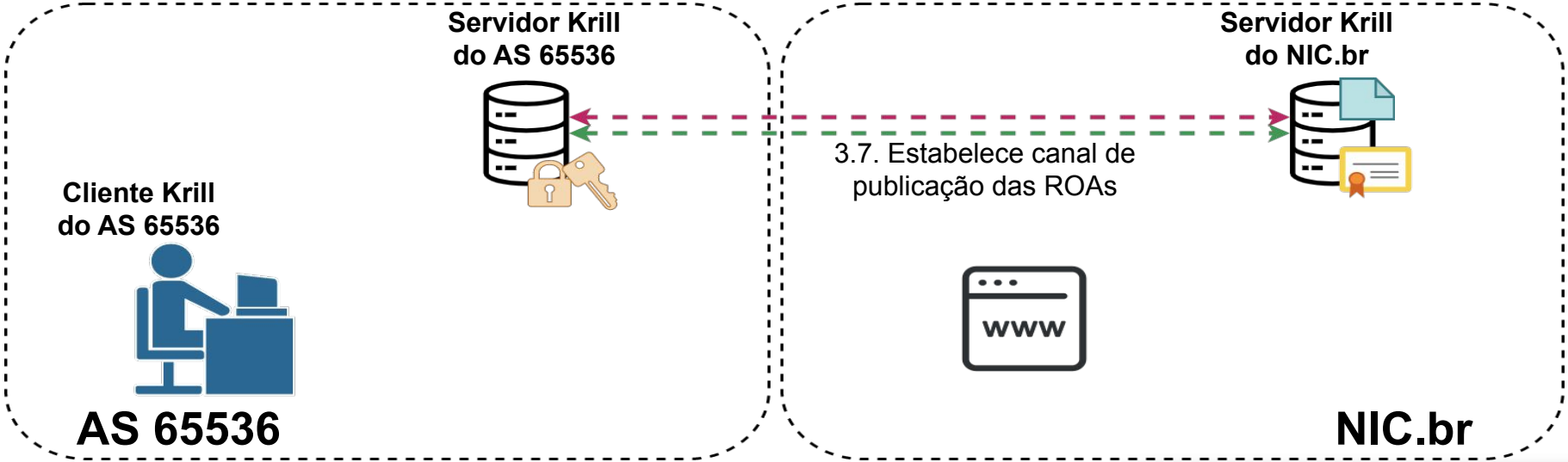
3.6. Configura o XML `repository_response` no Krill do ASN 65536

```
$ krillc repo update rfc8183 <arquivo xml> --server <URL>
     --token <senha> --ca <nome>
```



# Criação de ROAs no Krill

3.7. Sincroniza Servidor Krill do AS 65536 com o Servidor Krill do NIC.br, criando o canal de publicação das ROAs do AS 65536



# Como verificar existencia de ROAs

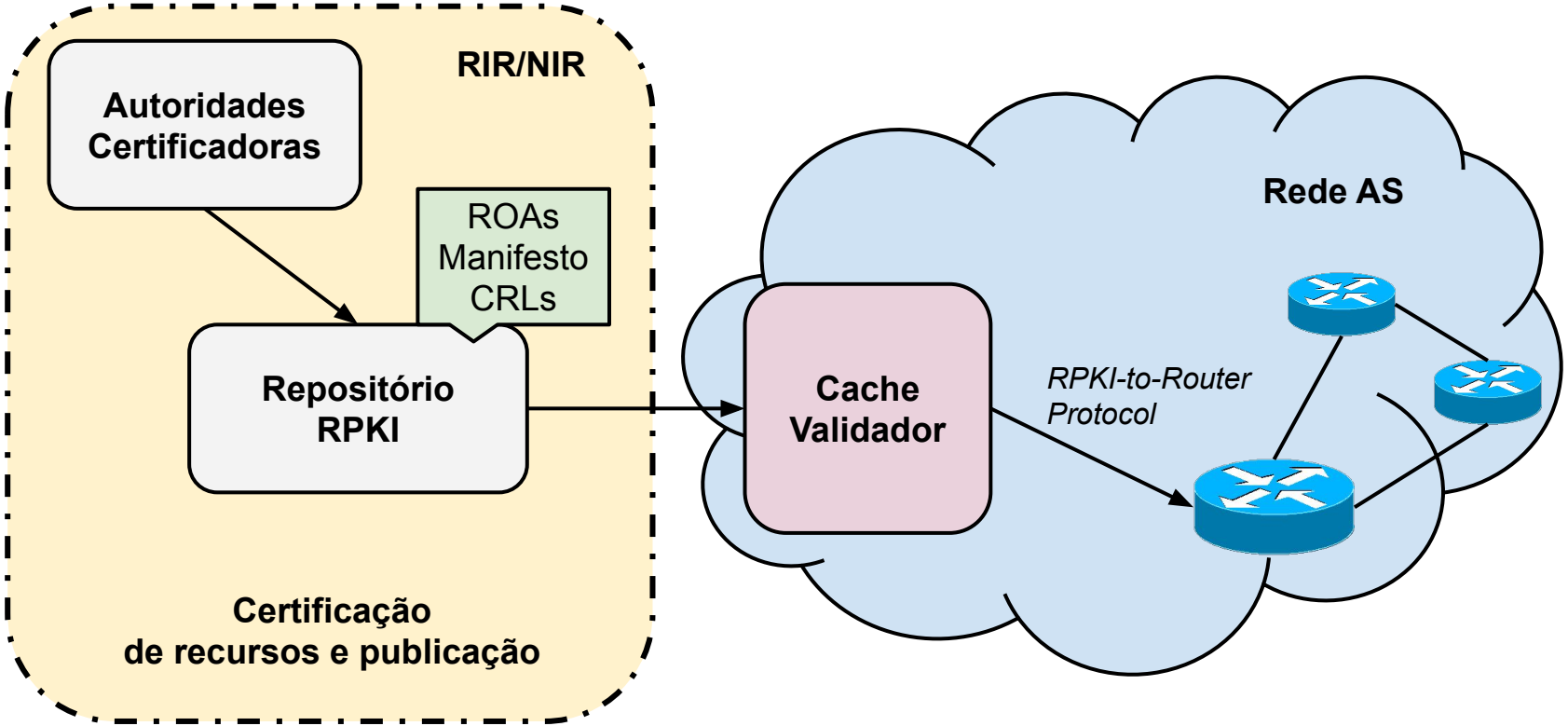
```
$ whois -h whois.bgpmon.net 200.160.0.0

Prefix:              200.160.0.0/20
Prefix description:  Registro.BR Network
Country code:        BR
Origin AS:           22548
Origin AS Name:      N?cleo de Inf. e Coord. do Ponto BR - NIC., BR
RPKI status:         ROA validation successful
First seen:          2011-10-19
Last seen:           2019-12-11
Seen by #peers:      66
```

# Visualizando uma ROA

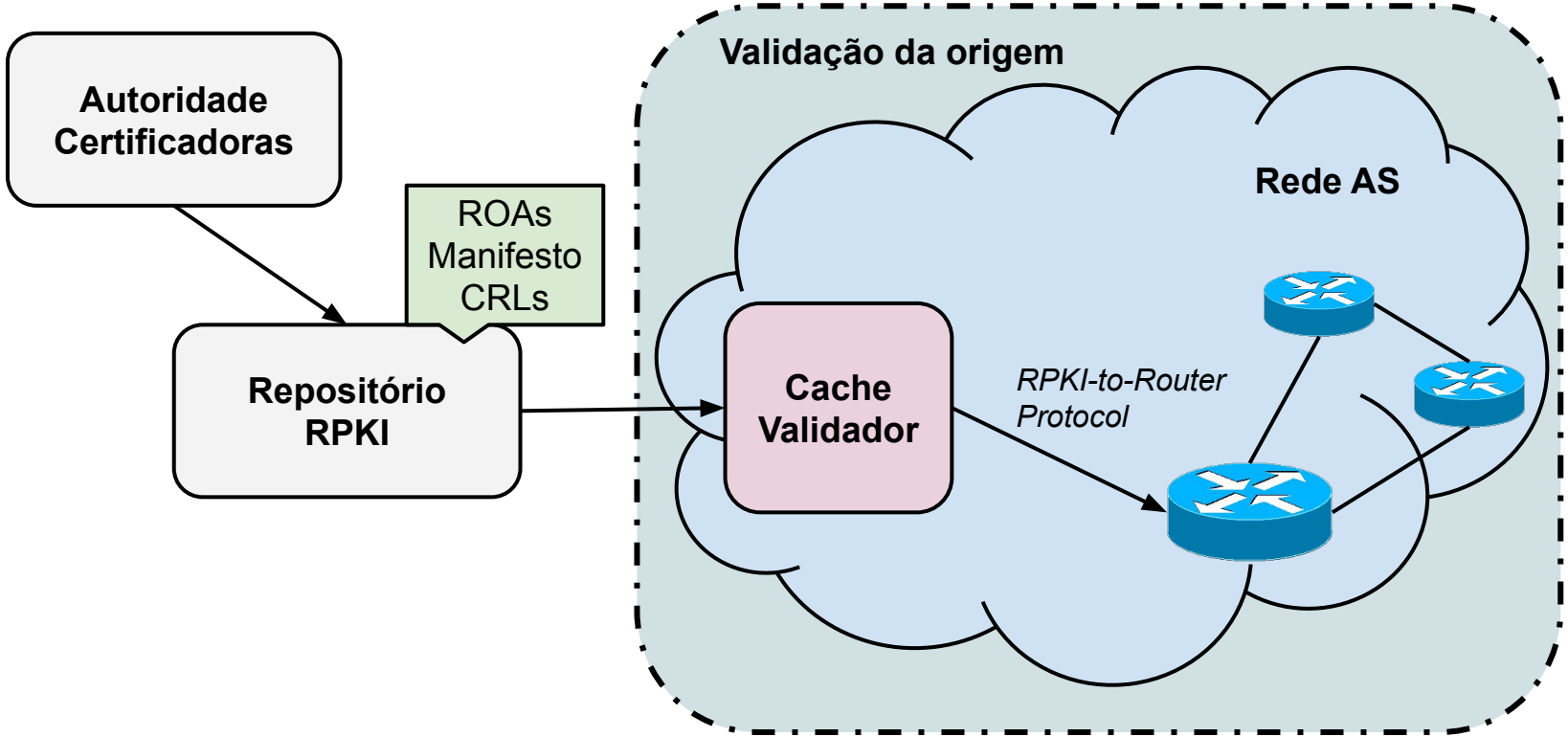
```
$ whois -h whois.bgpmon.net " --roa 22548 200.160.0.0/22"
0 - Valid
------------------------
ROA Details
------------------------
Origin ASN:       AS22548
Not valid Before: 2019-12-12 17:20:05
Not valid After:  2020-12-12 17:25:05  Expires in
1y14h24m2.60000000149012s
Trust Anchor:     rpki-repo.registro.br
Prefixes:         200.160.0.0/20 (max length /24)
```

# Parte IV
# RPKI: validação na origem

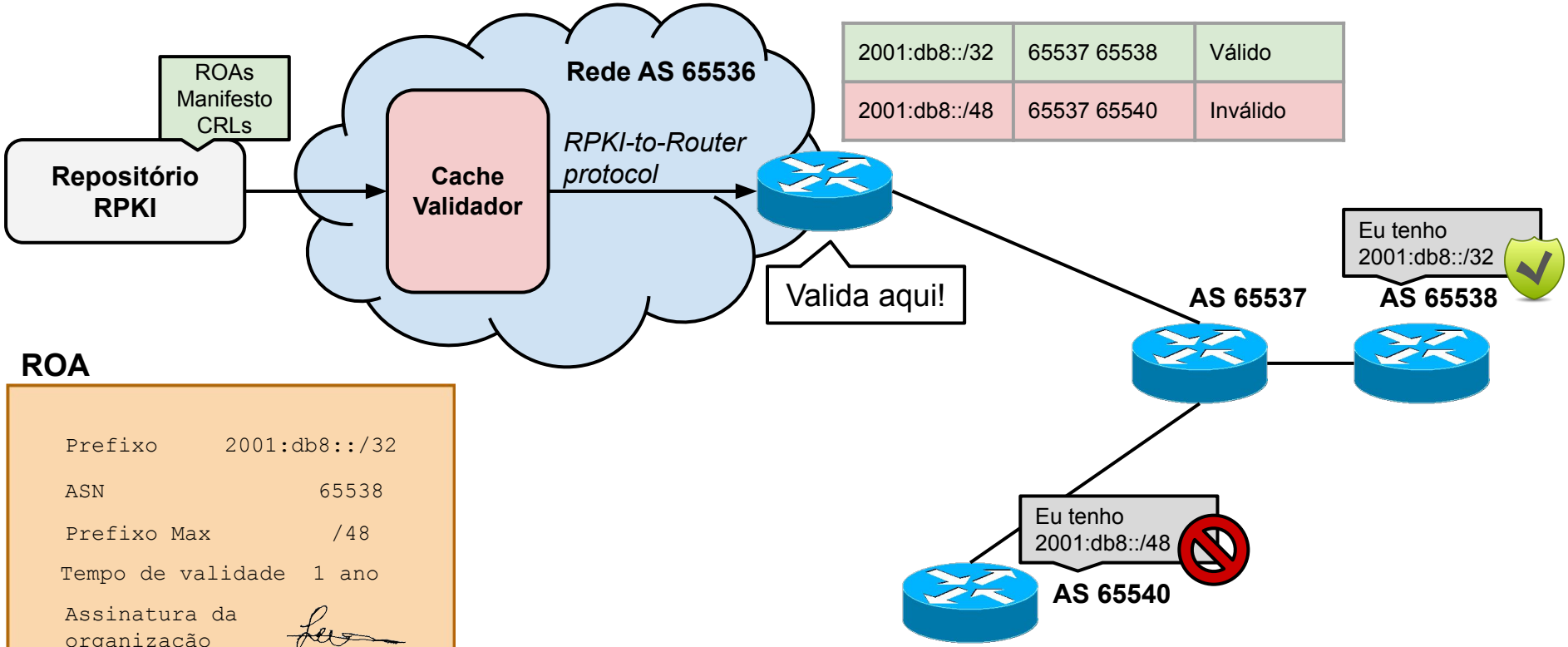
# RPKI: Recapitulando



# RPKI: Validação da origem



# RPKI: Validação da origem



# 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

# Validador

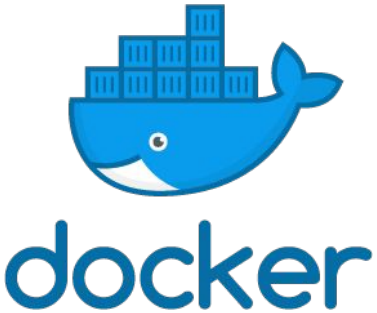
- Conexão com repositórios confiáveis (RIPE, LACNIC,...)
  - Rsync ou RPKI Repository Delta Protocol (RRDP)
- Cache
  - Atualizações periódicas
- Validação
  - Verificação das assinaturas dos ROAs e certificados
  - Geração de *Verified ROA Payloads* (VRP)
- Envia VRPs para o roteador usando o protocolo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

# Validador

- Existem vários softwares disponíveis:
  - **Routinator**
  - Dragon Research toolkit
  - RIPE validator
  - RTRlib (bird, FRR, Quagga...)
  - OctoRPKI & GoRTR (Cloudflare)

# ROUTINATOR

- Instalação: duas opções




OU


+


+

**C toolchain**

Fonte: https://rpki.readthedocs.io/en/latest/routinator/installation.html

# ROUTINATOR

- *Trust Anchor Locator* (TAL) já vem incorporados
  - Localizador para os 5 RIRs
    - ARIN necessário aceitar o termo de uso

```
routinator init
Before we can install the ARIN TAL, you must have read
and agree to the ARIN Relying Party Agreement (RPA).
It is available at

https://www.arin.net/resources/manage/rpki/rpa.pdf

If you agree to the RPA, please run the command
again with the --accept-arin-rpa option.
```

```
routinator init --accept-arin-rpa
```

# ROUTINATOR

- Verificando a base baixada

```
# routinator vrps
```

- Filtrar por AS

```
# routinator vrps --format csv --filter-asn <ASN>
# routinator vrps --format json --filter-asn <ASN>
```

# ROUTINATOR

- Filtrando por prefixos

```
# routinator vrps --format csv --filter-prefix <IP>/<prefixo>
# routinator vrps --format json --filter-prefix <IP>/<prefixo>
```

- Validar prefixo

```
# routinator validate --asn <ASN> --prefix <IP>/<prefixo>
# routinator validate --json --asn <ASN> --prefix <IP>/<prefixo>
```

# ROUTINATOR

- Executando o Routinator como servidor
  - HTTP

```
routinator server --http <IPv4>:<porta> --http [<IPv6>]:<porta>
```

  - RTR

```
routinator server --rtr <IPv4>:<porta> --rtr [<IPv6>]:<porta>
```

Fonte: https://rpki.readthedocs.io/en/latest/routinator/daemon.html

# 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.

# 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

# Roteador

Exemplo:

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

| | | |
|---|---|---|
| Válida | 65536 | 10.10.0.0/16 |
| Inválida | 65536 | 10.0.10.0/24 |
| Desconhecido | 65540 | 10.0.0.0/8 |

# Roteador

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

# Configurando o roteador

- **Juniper**
  - Conexão com validador

```
# set routing-options validation group group-name
session address port port-number
```

# Configurando o roteador

- **Juniper**

```
# set policy-options community origin-validation-state-invalid
members 0x4300:0.0.0.0:2
# set policy-options community origin-validation-state-unknown
members 0x4300:0.0.0.0:1
# set policy-options community origin-validation-state-valid
members 0x4300:0.0.0.0:0
```

# Configurando o roteador

- **Juniper**

```
# set policy-options policy-statement validation term
valid from protocol bgp
# set policy-options policy-statement validation term
valid from validation-database valid
# set policy-options policy-statement validation term
valid then community add origin-validation-state-valid
# set policy-options policy-statement validation term
valid then accept
```

# Configurando o roteador

- **Juniper**

```
# set policy-options policy-statement validation term
invalid from protocol bgp
# set policy-options policy-statement validation term
invalid from validation-database invalid
# set policy-options policy-statement validation term
invalid then community add origin-validation-state-invalid
# set policy-options policy-statement validation term
invalid then accept
```

# Configurando o roteador

- **Juniper**

```
# set policy-options policy-statement validation term
unknown from protocol bgp
# set policy-options policy-statement validation term
unknown then validation-state unknown
# set policy-options policy-statement validation term
unknown then community add origin-validation-state-unknown
# set policy-options policy-statement validation term
unknown then accept
```

# Configurando o roteador

- **Juniper**

```
# set protocols bgp import validation
```

  - Para verificar

```
# show route protocol bgp
# show validation database
```

# Resumindo

## Certificação de recursos

- RIRs são Autoridades Certificadoras
  - Criam certificados digitais para recursos de numeração (IPs e ASNs), emitem para ASNs
  - ASNs usam o certificado para criar declarações
    - ROA
      - Autoriza um ASN a originar prefixos de uma organização no BGP
      - Prefixo máximo do anúncio

Adaptado de: https://archive.nanog.org/sites/default/files/RPKI%20-%20NANOG63.pdf

# Resumindo

## Validação na Origem

- ASNs validam e comparam ROAs com informações recebidas no BGP
  - Aplicam filtros de acordo com o resultado
    - Válido
    - Inválido
    - Desconhecido

Adaptado de: https://archive.nanog.org/sites/default/files/RPKI%20-%20NANOG63.pdf

# Obrigado!!!

Equipe de cursos do CEPTRO.br (Eduardo Barasal Morales, Tiago Jun Nakamura, Tuany Oguro tabosa, Andrea Erina Komo e Fernanda Vitoria Santos Machado)

@ cursosceptro@nic.br @ hostmaster@registro.br

**São Paulo, dezembro de 2019**

nic.br cgi.br

www.nic.br | www.cgi.br