Infraestructura de clave pública para certificación de recursos (*RPKI*)

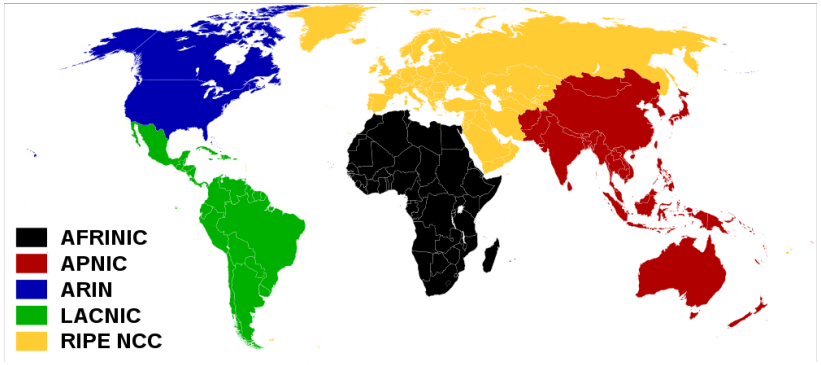
Carlos M. Martínez – Darío Gómez

Agenda

- Alocação e administração dos recursos da Internet
  - Relação entre registos e usuários dos recursos
- Roteamento na Internet
- Seqüestro de rotas
- Certificação de recursos
- ROAs
- Referências

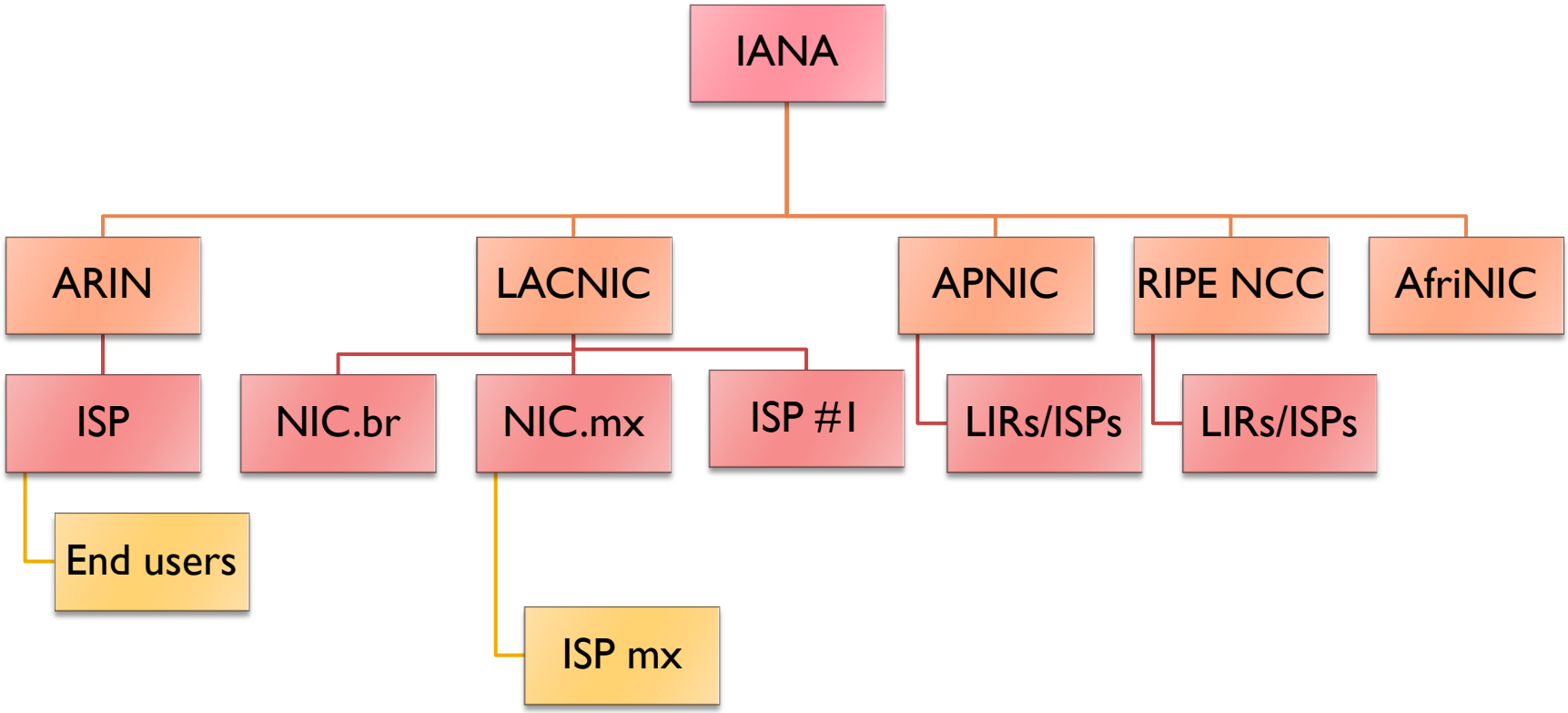
Alocação e administração dos recursos da Internet

- Recursos
  - Endereços IPv4
  - Endereços IPv6
  - Sistemas Autônomos
    - 16 y 32 bits



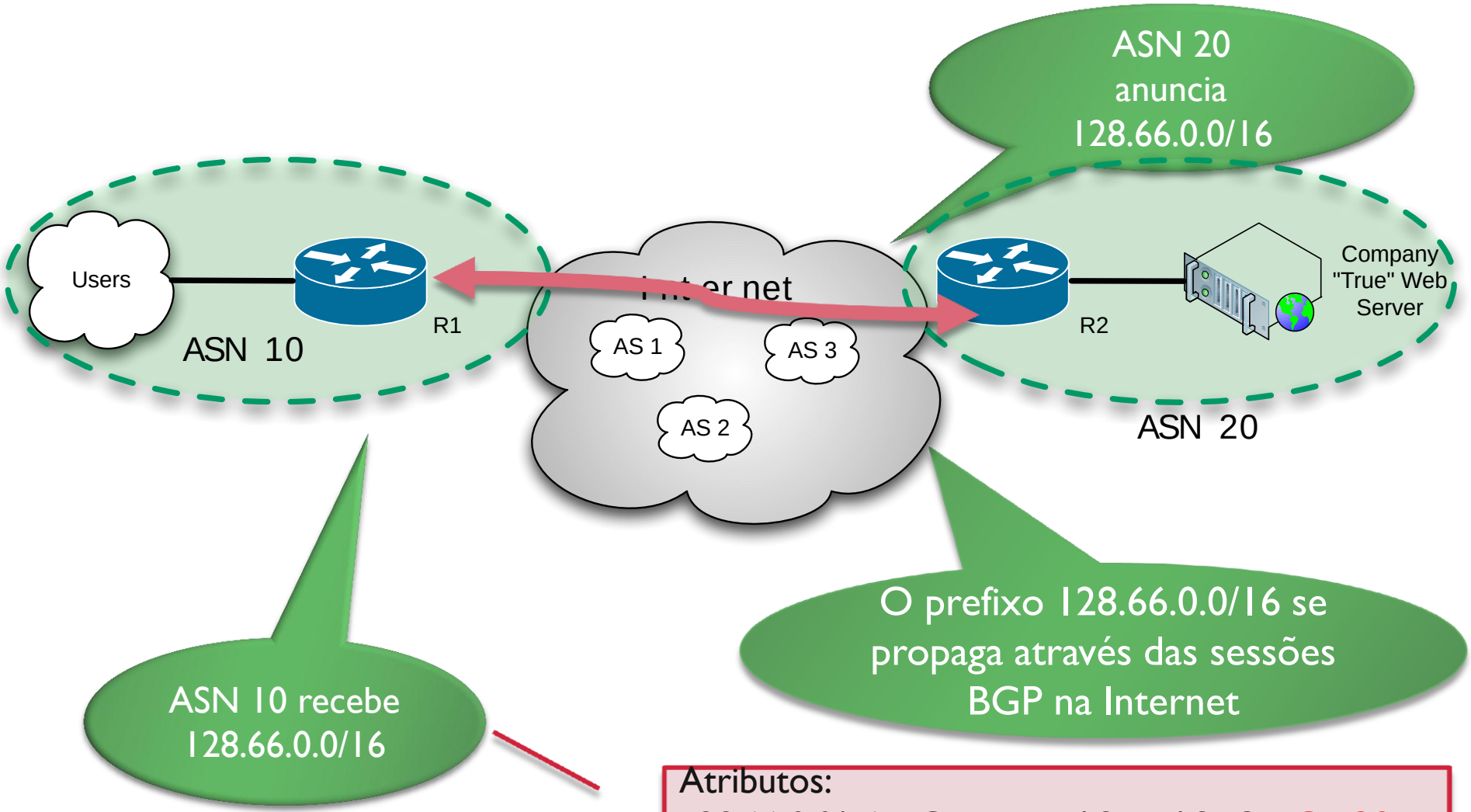
- Documento fundacional: RFC 2050
  - "*IP Registry Allocation Guidelines*"
- Cada RIR é **fonte autoritativa de informações da relação "usuario" <-> "recurso"**
  - Cada RIR opera sua banco de dados de registo

Alocação e administração dos recursos da Internet (i)



- Cada RIR é **fonte autoritativa de informações da relação "usuario" <-> "recurso"**

Roteamento na Internet em um slide

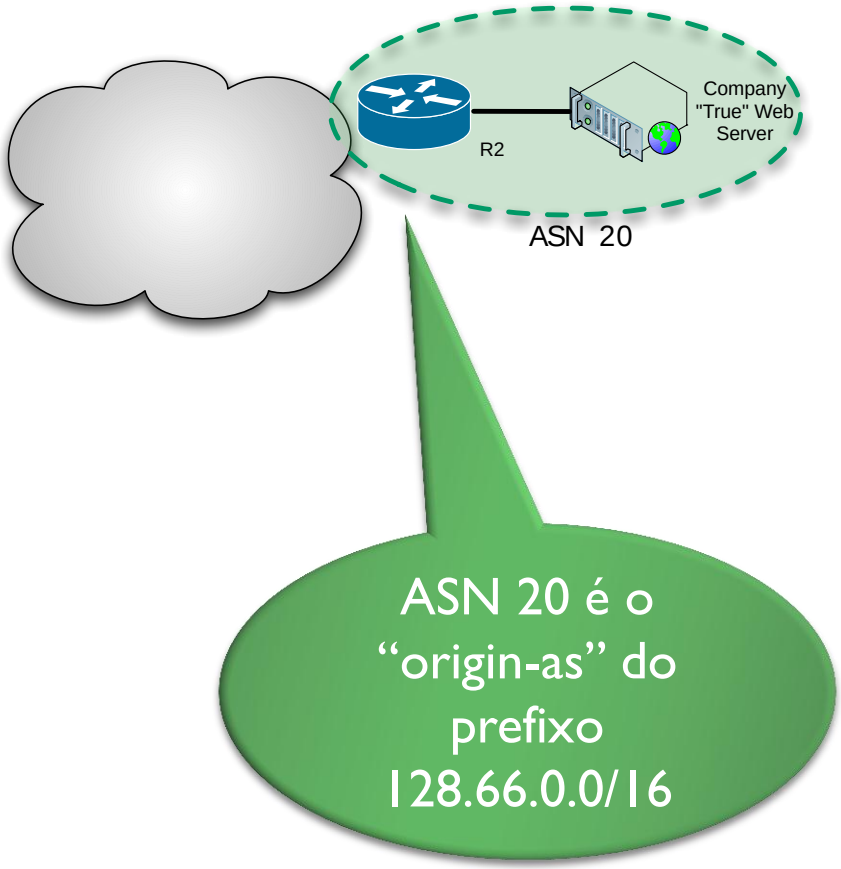


Atributos:
128.66.0.0/16 **AS_PATH** ASN1 ASN3 **ASN20**

Roteamento na Internet (ii)

- BGP escolhe rotas de acordo com um **algoritmo de decisão** e os valores dos **atributos**

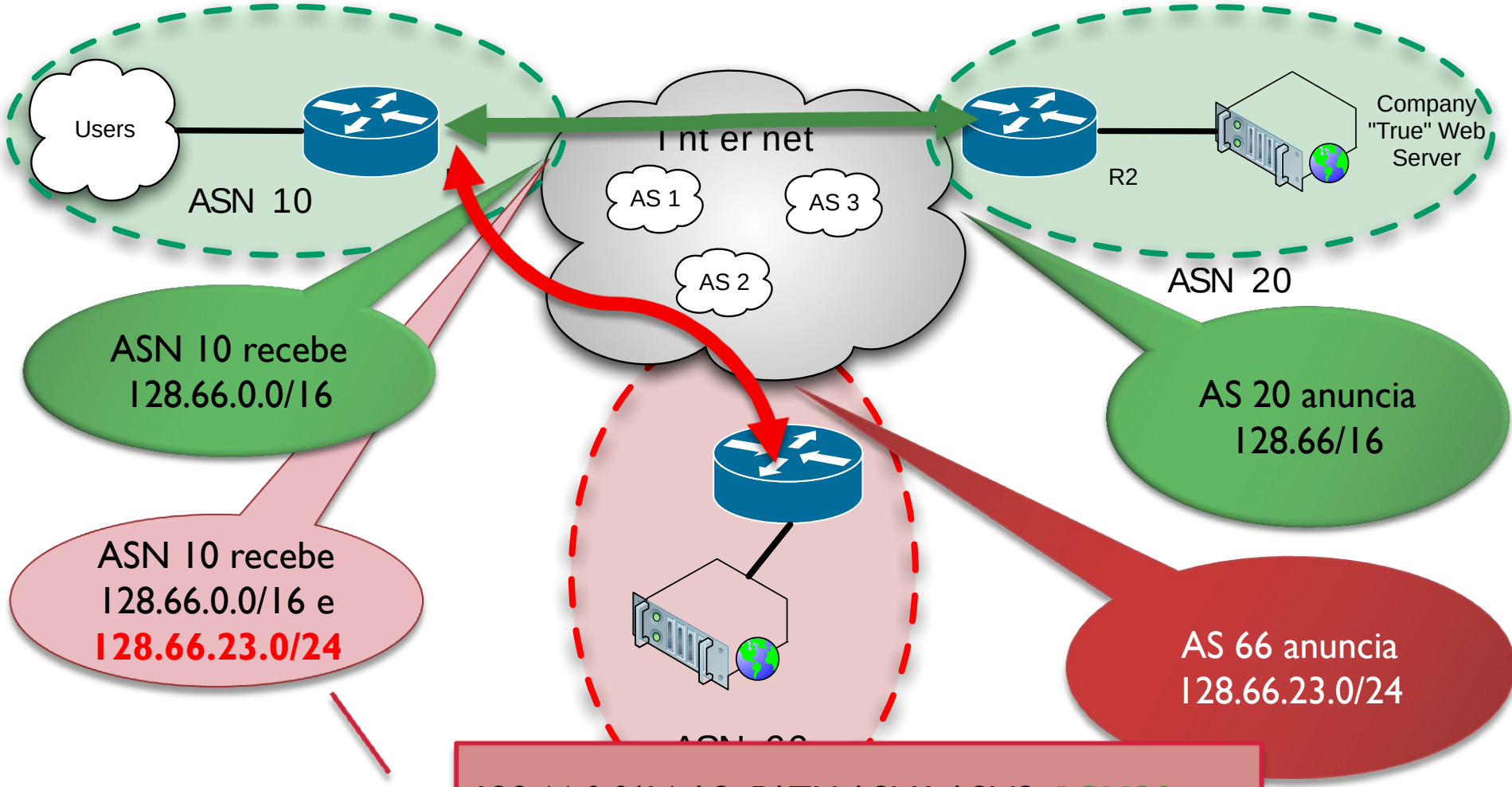
- AS_PATH e AS de origem
  - AS_PATH é a lista de sistemas autônomos percorridos por um UPDATE
  - Inclui o AS que origina o anúncio ("origin-as")



Seqüestro de rotas

- Quando um participante no roteamento na Internet anuncia um prefixo que não tem autorização para anunciar se produz um "seqüestro de rota" (*route hijacking)*
- Malicioso ou causado por erros operacionais
- Casos mais conhecidos:
  - Pakistan Telecom vs. You Tube (2008)
  - China Telecom (2010)
  - Google no Leste Europeu (vários AS, 2010)
  - **Casos em nossa região (janeiro/fevereiro de 2011)**

Seqüestro de rotas (ii)



Resource PKI (i)

- Objetivos:
  - Emitir certificações digitais de autorização de uso dos recursos
  - Prover uma técnica para validar a autoridade associada a um anúncio BGP e validar a "**origem de uma rota**"
- O emissor da informação de rota "**assina**" a informação de "AS de origem"
- Para a validação dos certificados e informação de roteamento se utilizam:
  - As propriedades do cifrado de chave pública (certificados)
  - As propriedades dos blocos CIDR

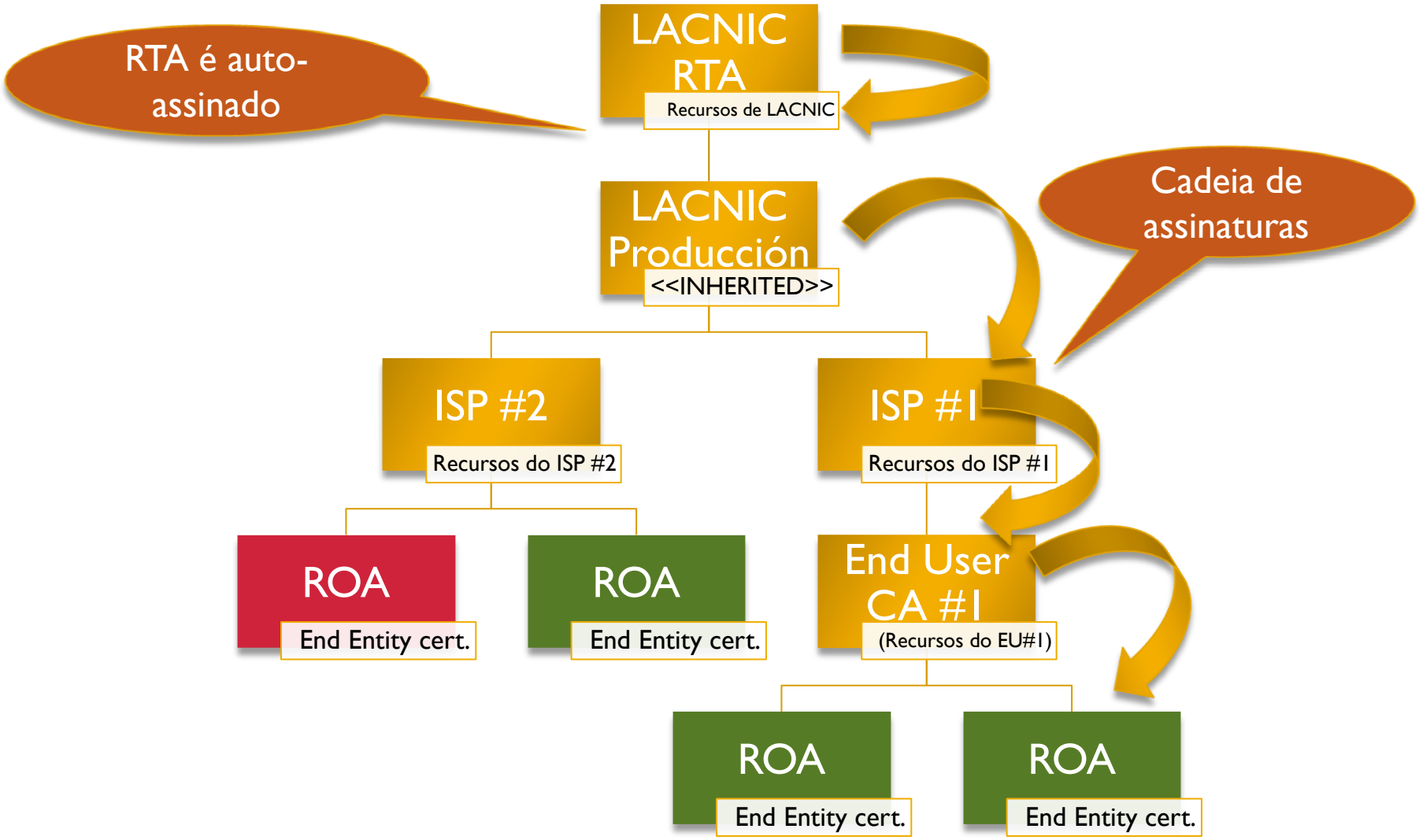
Resource PKI (ii)

- Certificação de recursos
  - Uso de certificados X.509 v3
  - Uso de extensões RFC 3779 permitem representar em certificados recursos de Internet (endereços v4/v6, ASNs)
  - Mecanismo de **validação de prefixos**
- Esforço de estandardização:
  - SIDR working group no IETF
- Esforço de implementação
  - RIRs

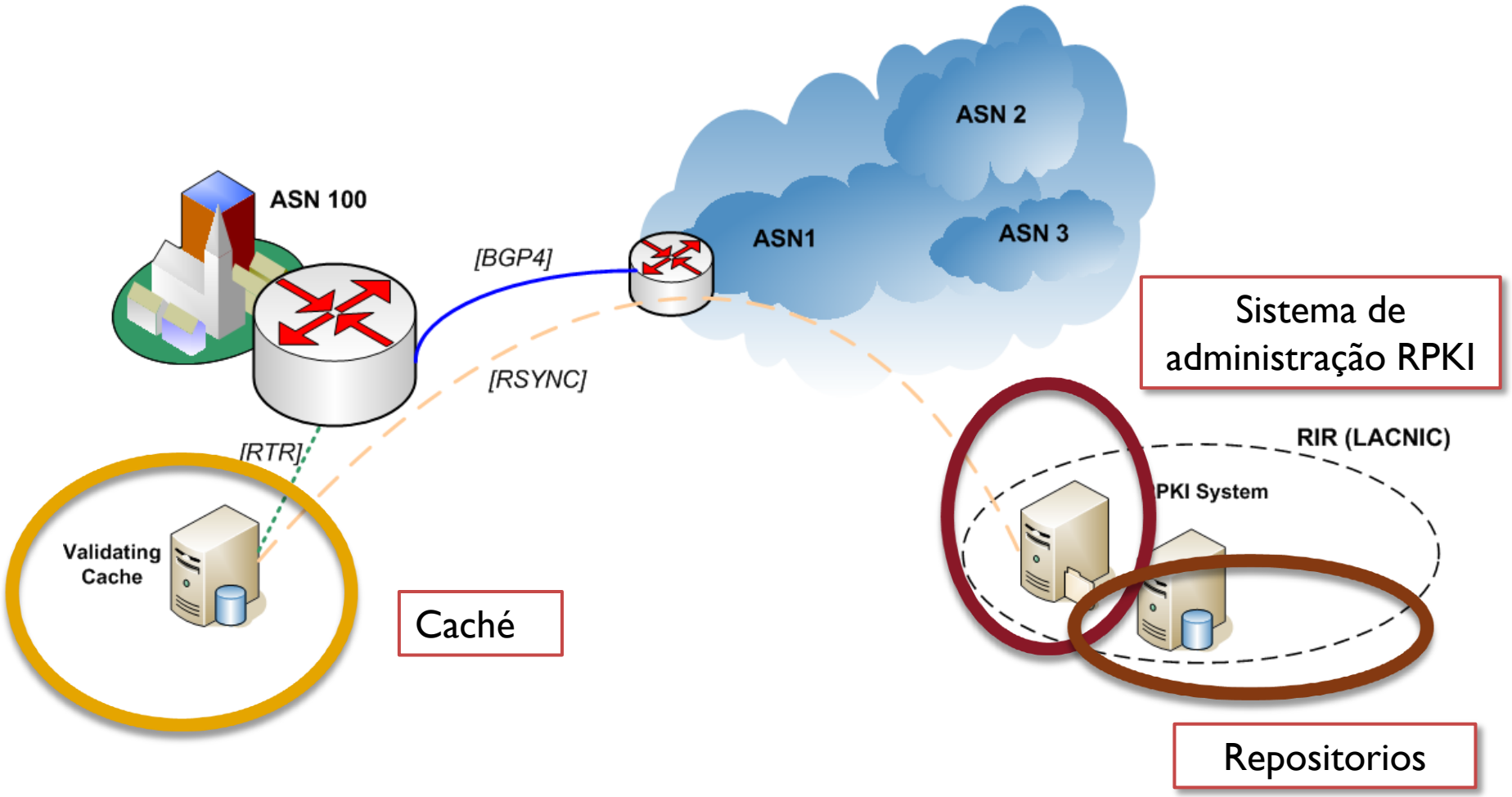
Certificados X.509 v3 com extensões RFC 3779

- Seção "IP Delegation"
  - Valor especial "INHERITED"
- Seção "AS Delegation"
  - Valor especial "INHERITED"
- Processo de validação
  - Se validam as **cadeias de assinaturas**
  - É validada a inclusão de recursos (CIDR) de filhos para pais

Estrutura da RPKI



Resource PKI (iii)



Route Origin Authorizations: ROAs (i)

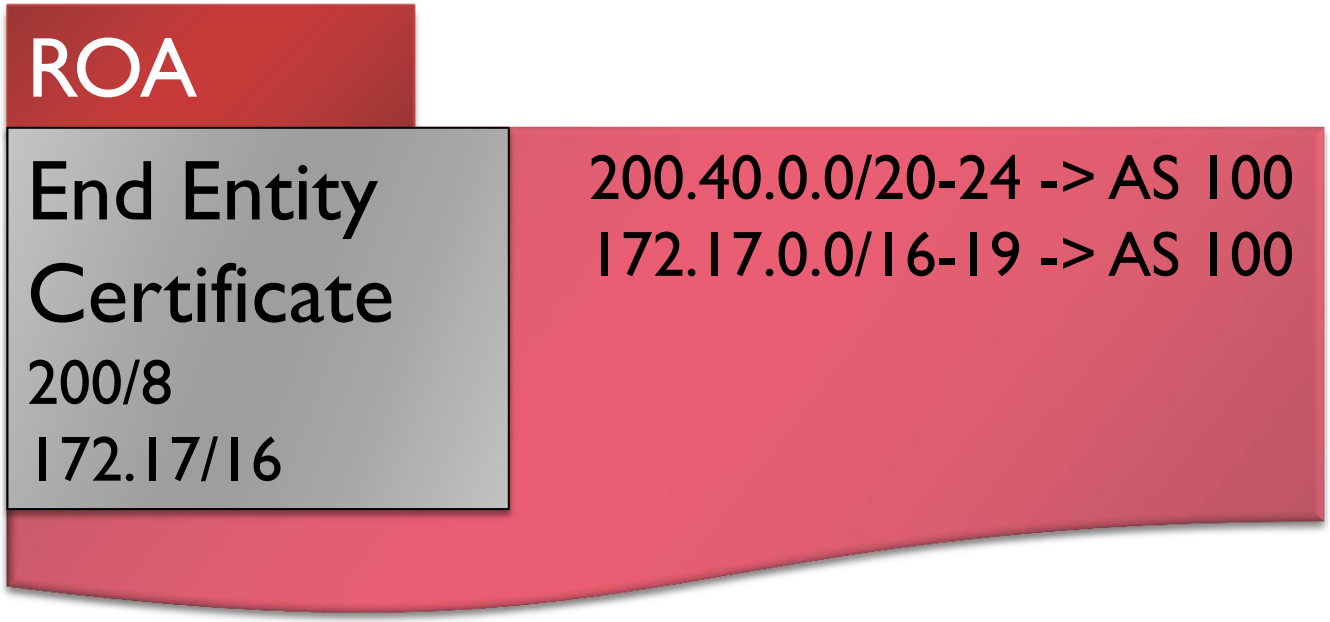
- Um ROA (simplificado) contém esta informação:

Prefijo	Largo_Máximo	AS Origen	Valido_Desde	Valido_Hasta
200.40.0.0/17	20	6057	2011-01-02	2012-01-01
200.3.12.0/22	24	28000	2011-01-07	2012-01-06

- Este ROA afirma que:
  - *"O prefixo 200.40.0.0/17 será anunciado pelo sistema autônomo 6057 e poderá ser fraccionado em prefixos de até 20 bits de longo. Isto será valido desde o 2 de janeiro de 2011 até o 1 de janeiro de 2012"*
- Além disso
  - O ROA contém o material criptográfico que permite **verificar** a validade desta informação contra a RPKI

ROAs (iii)

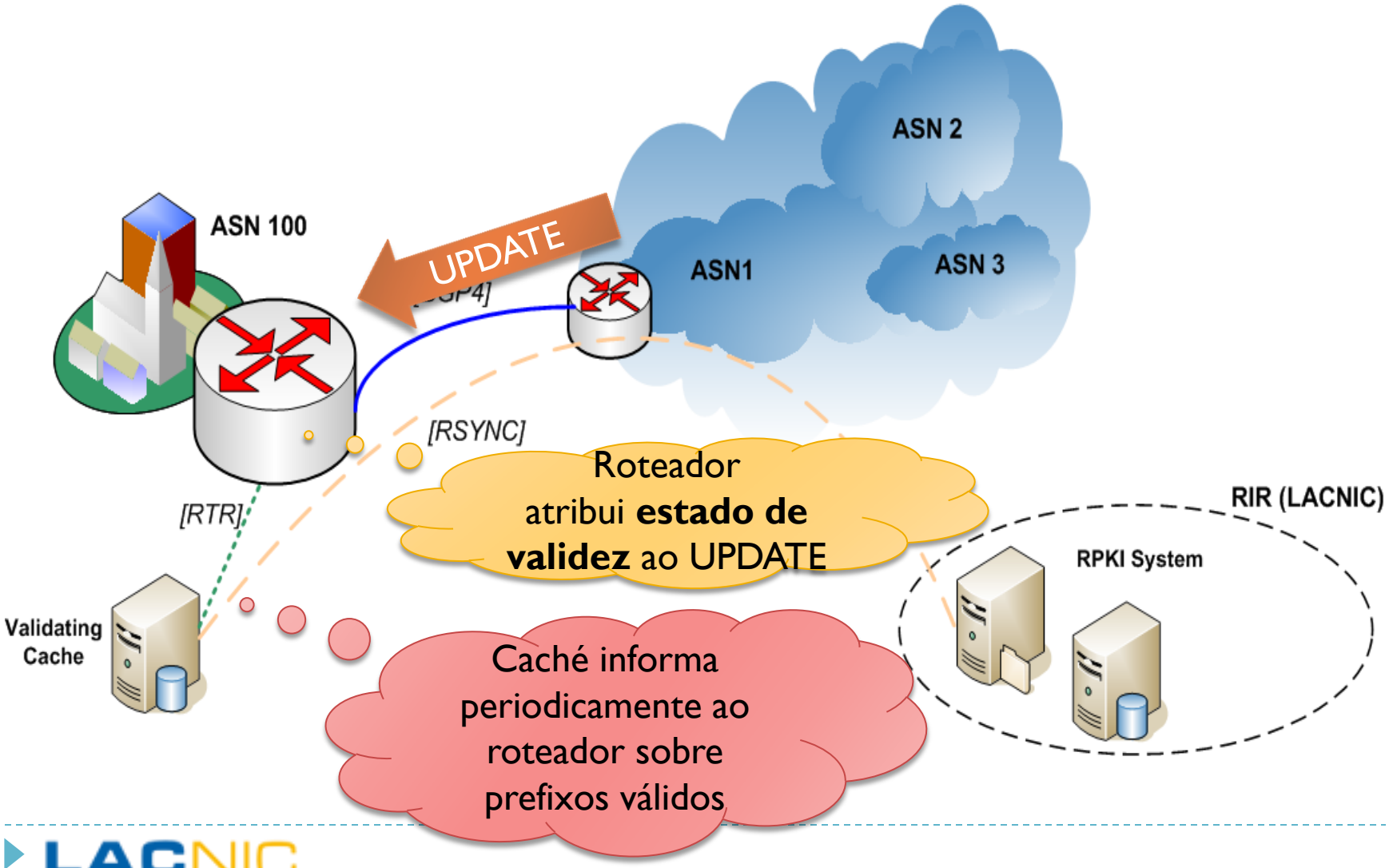
- Os ROA contêm
  - Um certificado End Entity com recursos
  - Uma lista de "route origin attestations"



ROAs (iii) - Validação

- O processo de validação dos ROAs envolve:
  - A validação criptográfica dos certificados end entity (EE) que estão conteúdos dentro de cada ROA
    - Certificado de recursos da organização
    - Certificado de recursos do RIR
  - A validação CIDR dos recursos listados no EE respeito dos recursos listados no certificado emissor
    - Inclusão nos recursos listados no EE
    - Inclusão nos recursos do certificado da organização
  - A verificação de que os prefixos listados nos "route origin attestations" estão incluídos nos prefixos listados nos certificados end entity de cada ROA

RPKI em funcionamento



Interação com BGP

- O roteador cria uma tabela com as informações que recebem do caché
- Essa tabela contém
  - Prefixo
  - Longo mínimo
  - Longo máximo
  - AS de origem
- Com base em um conjunto de regras é atribuído para cada prefixo um **estado de validade**
  - {VALID, INVALID, NOT_FOUND}

Interação com BGP (ii)

UPDATE 200.0.0.0/9
ORIGIN-AS 20

VALID

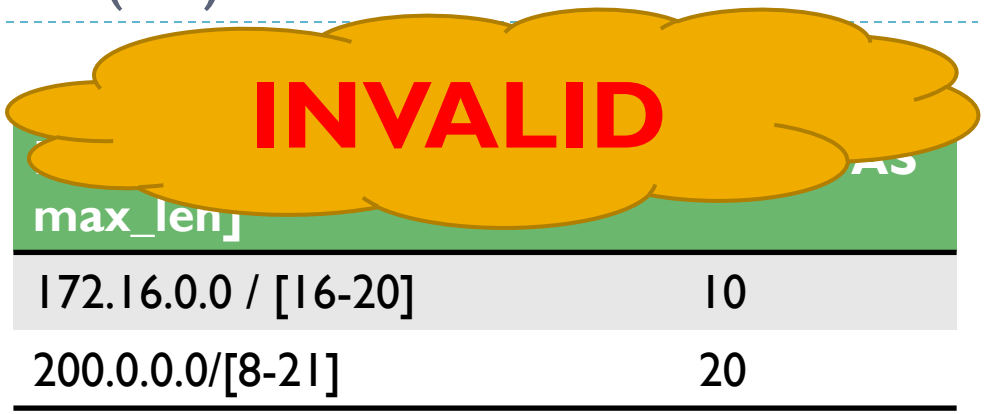
max_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Se o "UPDATE pfx" **não** encontra nenhuma entrada que o tenha incluso no banco de dados -> "**not found**"
- Se o "UPDATE pfx" encontra pelo menos uma entrada que o tenha incluso no banco de dados e também o AS de origem do "UPDATE pfx" coincide com um deles -> "**valid**"
- No caso anterior, se não coincide nenhum AS de origem -> "**invalid**"

Interação com BGP (iii)

UPDATE 200.0.0.0/9

ORIGIN-AS 66



- Se o "UPDATE pfx" **não** encontra nenhuma entrada que o tenha incluso no banco de dados -> "**not found**"
- Se o "UPDATE pfx" encontra pelo menos uma entrada que o tenha incluso no banco de dados e também o AS de origem do "UPDATE pfx" coincide com um deles -> "**valid**"
- No caso anterior, se não coincide nenhum AS de origem -> "**invalid**"

Estado atual de RPKI na LACNIC

- RPKI em modo "hosted" está em produção desde o 1-1-2011
  - http://rpki.lacnic.net
- Quem pode utilizá-lo?
  - Todos os membros de LACNIC através de seus contatos técnicos e administrativos
- Que funcionalidades estão disponíveis?
  - Criação do certificado de recursos
  - Criação, modificação e revogação de ROAs
- Onde se encontra o repositório da LACNIC?
  - rsync://repository.lacnic.net/rpki/

Referências

- RPKI LACNIC: http://rpki.lacnic.net
- Estatísticas RPKI: http://www.labs.lacnic.net/~rpki
- RPKI Demo:
  - Acesso: http://rpkidemo.labs.lacnic.net
  - Documento de uso: http://www.labs.lacnic.net/drupal/acceso-al-demo-rpki
- IETF SIDR Working Group: http://tools.ietf.org/wg/sidr/
- RIPE Repository Validator:
  - http://labs.ripe.net/Members/agowland/ripe-ncc-validator-for-resource-certification

Obrigado pela atenção!

Carlos M. Martínez (carlos@lacnic.net)
Darío Gómez (dario@lacnic.net)