Certificados Digitais para Endereços IPs

Ricardo Patara
LACNIC

Resumo

- Estrutura de Certificados de Chaves Públicas (PKI - Public Key Infrastructure)
- Autorização/direito de uso de um recurso (*não é autenticação*)
- Extensão crítica contendo listagem de recursos Internet (RFC 3779)

Motivação

- Proteção do sistema de rotas interdomínio
  - Caso Youtube.
  - Mais recentemente, sequestro de rotas "imperceptível"
- Tempos interessantes com esgotamento de estoque IPv4 não alocado.

Motivação

- Estrutura hierárquica PKI pode ser "mapeada" facilmente com hierarquia de distribuição de Recursos Internet
- Uso de estrutura já conhecida e bem desenvolvida (PKI, X.509)

Introdução

- Termos utilizados
  - CA: Certification Authority
  - Subject
  - RE: Relaying Party
  - TA: Trust Anchor

Introdução

- PKI, estrutura hierárquica de CAs
- Cadeia de verificação/certificação
  - “Percorre” todos CAs até um TA
  - Certificado dado como válido, caso assim o seja em toda a cadeia (não está em nenhuma CRL, não expirou, extensões criticas “compreendidas”)

Introdução

- Exemplo mais comum: Certificados para HTTPS (SSL)
- Relaying Parties: browsers
- TA: Entidades Certificadoras mais conhecidas
- Cadeia de verificação, em geral, um nível

Introdução

- Arquitetura para Certificação de recursos:
  - uma estrutura PKI (Resource PKI)
  - objetos assinados digitalmente
  - repositório de informações distribuído

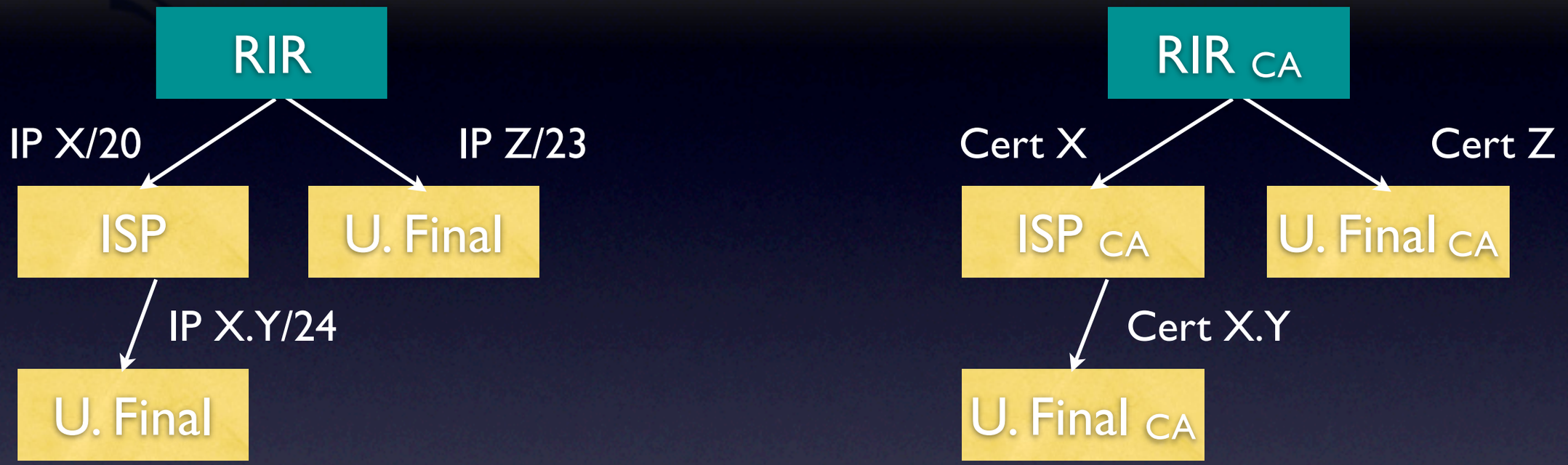
Introdução

- Principal objetivo:
  - Mecanismos para atestar que uma entidade é legitimo "detentor" do ***direto de uso*** de um IP e/ou ASN
  - Mecanismos para explicitamente autorizar o anuncio de IPs com origem em um ASN. (Ex. construção de filtros de rotas)

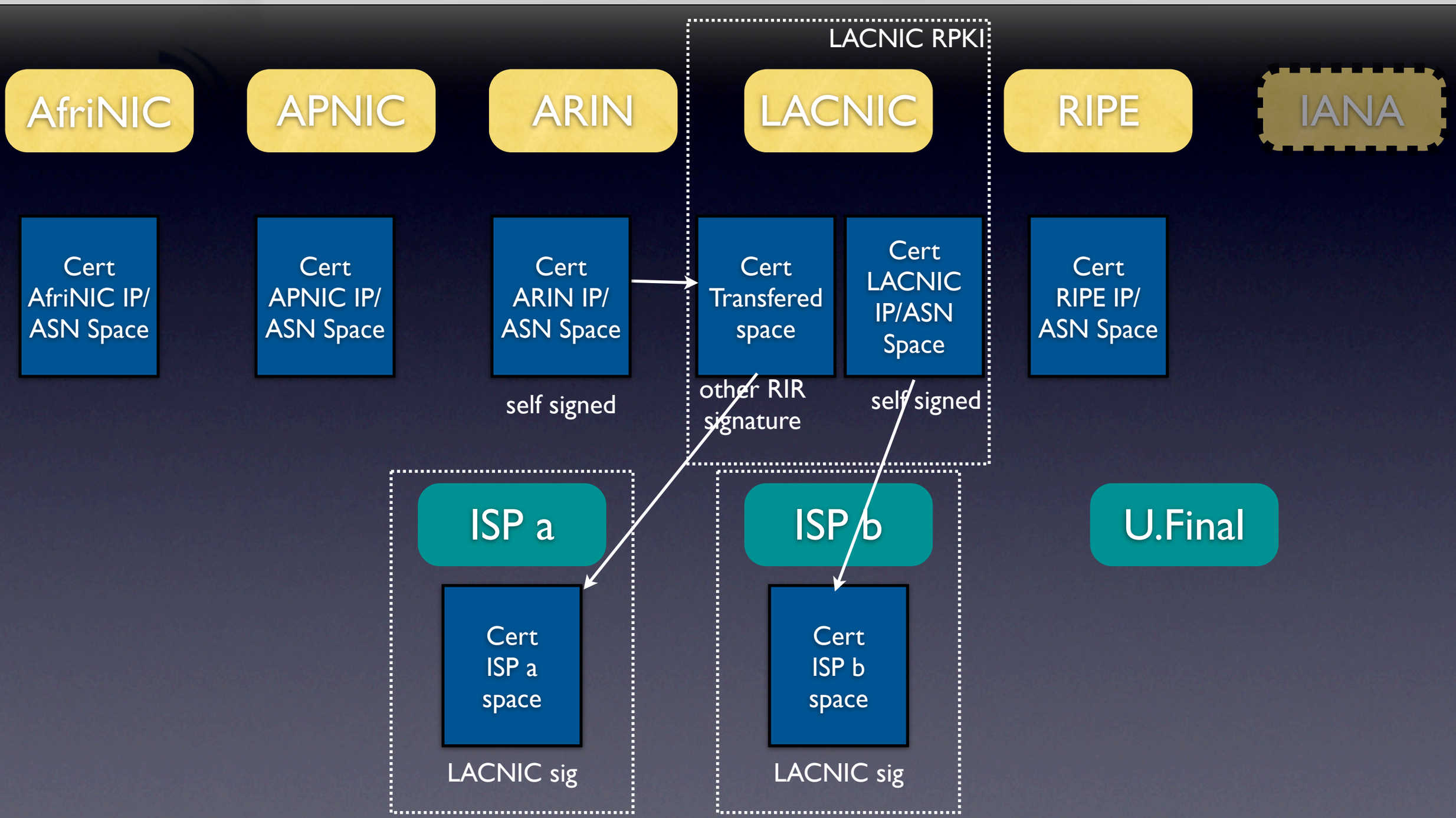
Certificado

X.509	
Issuer:	
Subject:	
SIA:	AIA:
Not valid before/ after	
....	
Critical Extention RFC 3779	

Hierarquia


RIR
IP X/20
IP Z/23
ISP
U. Final
IP X.Y/24
U. Final
RIR CA
Cert X
Cert Z
ISP CA
U. Final CA
Cert X.Y
U. Final CA

Hierarquia


LACNIC RPKI
AfriNIC
APNIC
ARIN
LACNIC
RIPE
IANA
Cert AfriNIC IP/ ASN Space
Cert APNIC IP/ ASN Space
Cert ARIN IP/ ASN Space
Cert Transfered space
Cert LACNIC IP/ASN Space
Cert RIPE IP/ ASN Space
self signed
other RIR signature
self signed
ISP a
ISP b
U.Final
Cert ISP a space
Cert ISP b space
LACNIC sig
LACNIC sig

Certificação

- Maioria certificados com “bit” CA ativo
  - Chave privada referente a parte pública contida nesse tipo de certificado somente “assina” outros certificados
- Exceto certificados “EE” (End Entity)
  - Chave privada pode “assinar” outros objetos

Certificação

- Cada entidade que faça ou receba alocação é uma entidade Certificadora (certificado com bit CA)
- RIRs emitem certificados para seus "membros" (ISP, U.final, NIRs). Hospedarão PKI de seus membros.
- ISPs, NIRs emitem certificados para seus clientes e membros
- ISPs, U.Finais emitem certificados "EE"

Certificação

- Certificados emitidos pelos RIRs ao seus membros
- “Subject”, sem valor significativo externamente
- “Issuer”, nome do RIR

Verificação

- Verificação de certificados (cadeia de certificação)
  - Executado pelo "Relaying Party"
    - Dado um certificado, verificar sua assinatura, período de validade, extensões
    - CRL e certificado do "Issuer"
    - Repetir até chegar a um "TA"

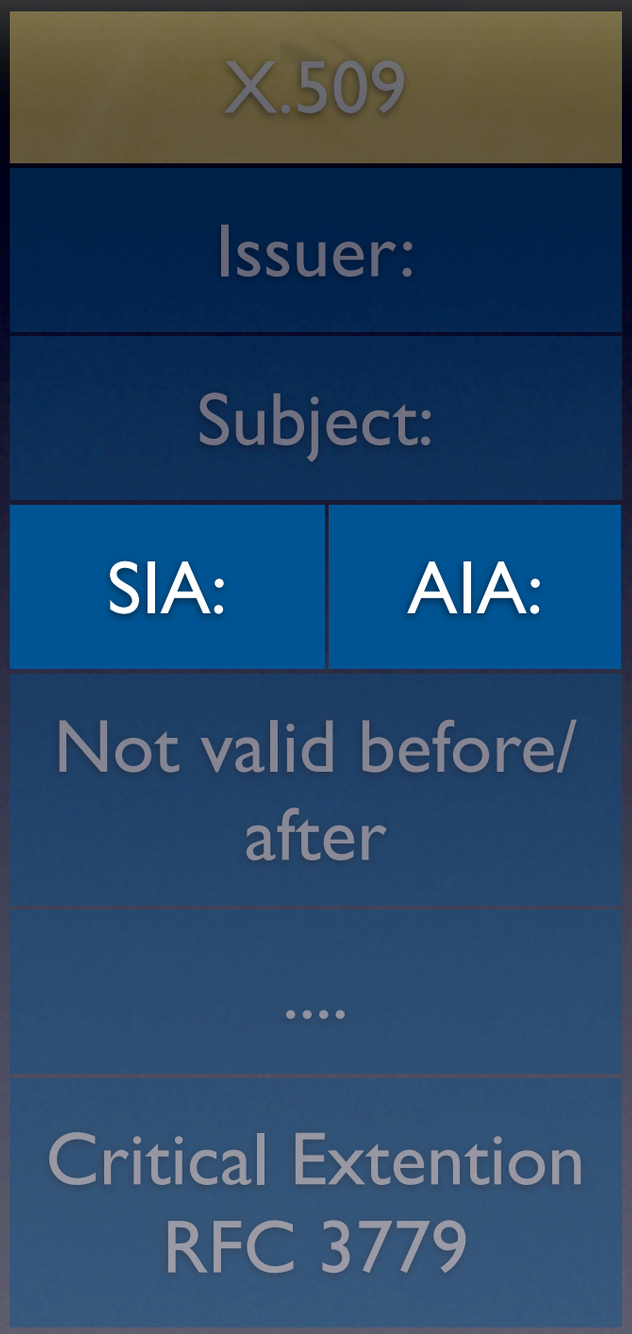
Verificação

- Nessa arquitetura RPKI:
  - RIRs = TAs default
  - TA decisão de "RP". Portanto, pode ter outro conjunto
  - Cadeia pode ter aprox. 6 a 10 níveis

Repositório

- Acesso Público
- Estrutura hierárquica
- Cada nível contem certificados, CRL, objetos “assinados” por um CA
  - Nível 0 RIR. Nivel 1 ISP, seus certificados, CRLs e objetos assinados com esse certificado

Repositório



- SIA (Subject Information Access)
  - URL que aponta para repositório contento objetos desse "Subject" CA
- AIA (Authority Information Access)
  - URL que aponta para repositório contento objetos da entidade CA que assinou esse certificado

ROA

- Route Origin Authorization
- Formato CMS (Crypto Message Syntax)
- Indica autorização para um ASN originar rotas para blocos IP.
  - Contém: ASN, bloco IP, maxlength
- Assinado por "entidade" com direito de uso para esse bloco IP.

ROA

- Certificado EE, sem "bit" CA é criado para esse fim
- Um para cada objeto. Não se necessita portanto armazenar chave privada
- Revocar esse EE, revoca-se objeto por ele assinado

Outros objetos

- Certificados EE serão criados para "assinarem" outros objetos:
  - Manifest
  - BOAs
  - etc.

Resumo

- RIR aloca bloco IP e emite certificado. Publica informação em repositório
- Entidade receptora, emite outros certificados EE. Publica em repositório
- Gera ROA. Publica em repositório

Resumo

- Outras entidades podem construir filtros com base em ROAs publicadas em cada um dos repositórios:
  - Coleta todas ROAs e certificados.
  - Valida certificados
  - Valida ROAs.

Referencias

- SIDR IETF Working Group:
  - http://www.ietf.org/html.charters/sidr-charter.html
- Drafts sobre arquitetura, "profile" dos certificados, repositórios, manifestos, ROA, CP, CPS...

Duvidas?

Obrigado!