Minicurso Tópicos em Segurança da Informação
Parte 3 - DNSSEC

I Workshop de Tecnologia de Redes do POP-BA
Ponto de Presença da RNP na Bahia

Italo Valcy <italo@pop-ba.rnp.br>

20 e 21 de setembro de 2010

Licença de uso e atribuição

Todo o material aqui disponível pode, posteriormente, ser utilizado sobre os termos da:

Creative Commons License:
Atribuição - Uso não comercial - Permanência da Licença

http://creativecommons.org/licenses/by-nc-sa/3.0/

Agenda

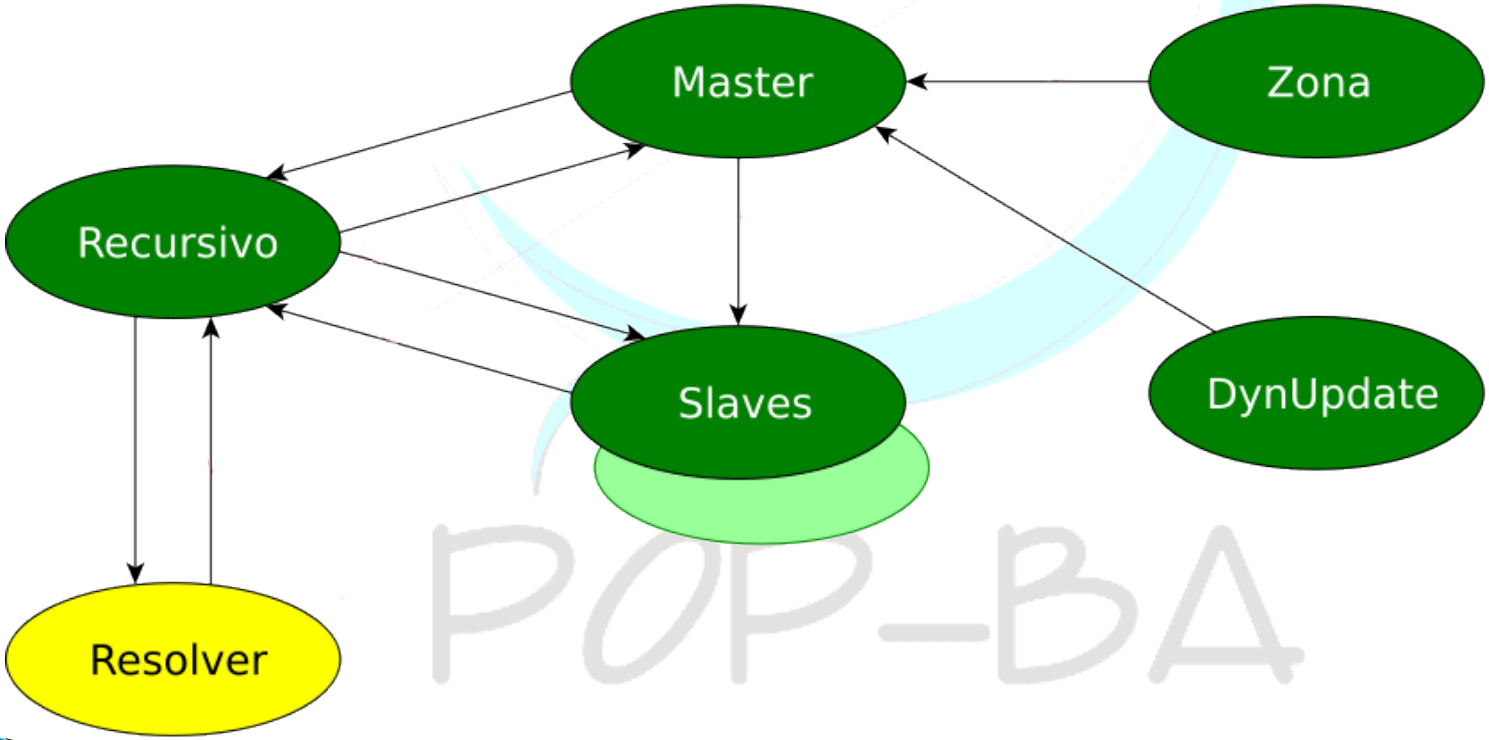
- Revisão sobre DNS e seus problemas
- Conceitos básicos do DNSSEC
- DNSSEC/Bahia/Brazil
- Prática de DNSSEC no recursivo
- Conclusões

Conceitos

- Tipos de servidores DNS
  - ***Autoritativo*** – contém os dados para a zona e responde a todo o mundo sobre essa zona.
  - ***Recursivo*** – recebe requisições dos clientes e consulta servidores externos
- ***Resource Record*** (RR) – registros de dados do DNS (RFC 1035 §3.2.1). Campos mais importantes: Nome, Classe, Tipo, Dado.
  - ***RRset***: RRs que têm o mesmo Nome, Classe e Tipo.

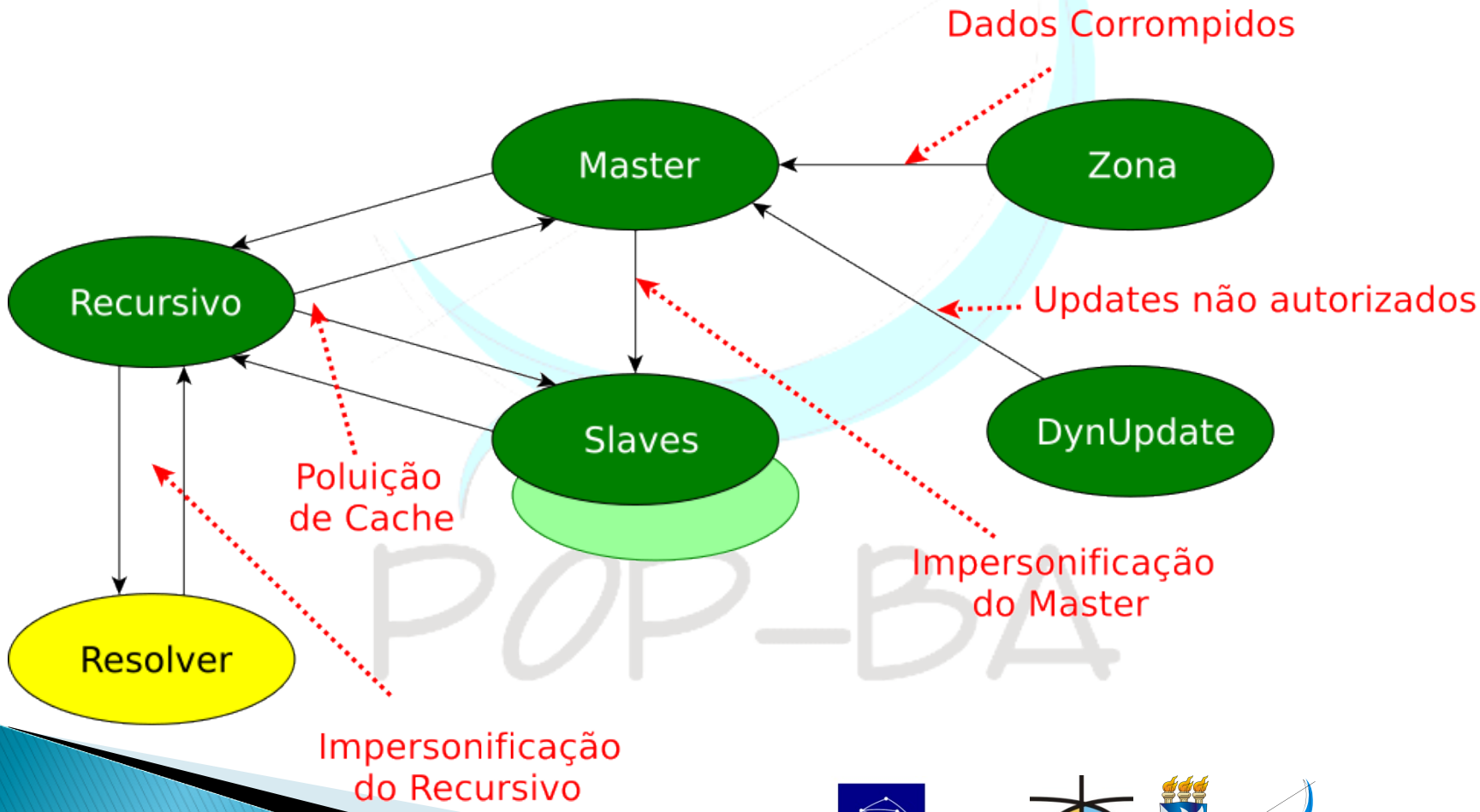
DNS – Revisão

- Fluxo de dados



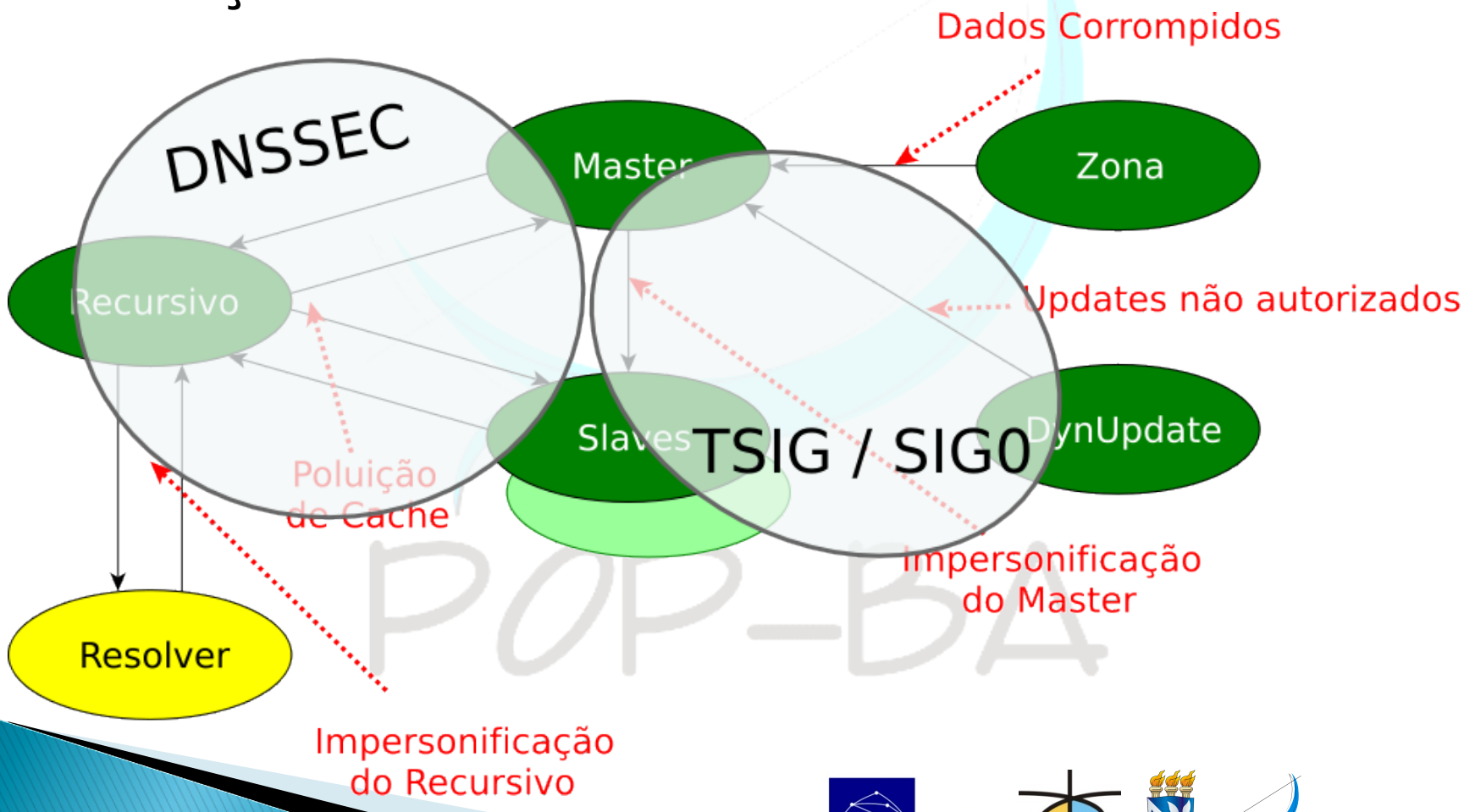
DNS – Revisão

- Vulnerabilidades



DNS – Revisão

- Soluções



Como resolver esses problemas?

DNSSEC

- Extensão do protocolo DNS para adicionar mecanismos de segurança
- Permite que se possa **verificar** as informações recebidas, invés de "*confiar*" em sua validade
- Suas verificações ocorrem antes de diversas aplicações de segurança (SSL, SSH, etc.)

DNSSEC

O que **garante**?

- Origem (Autenticidade)
- Integridade
- A não existência de um nome ou tipo

O que **não** garante?

- Confidencialidade
- Proteção contra ataques de negação de serviço (DoS)

DNSSEC – visão geral

- Utiliza o conceito de chave assimétrica
- Inclusão de quatro novos RRs
  - RRSIG
  - DNSKEY
  - NSEC
  - DS
- Assim como outras técnicas de segurança (ex: SPF), você precisa **implantar DNSSEC** em sua zona e **validar as respostas** no recursivo.

DNSSEC – visão geral

- Assinar os registros:
  - RRSIG
- Divulgar a chave pública:
  - DNSKEY
- Garantir a não existência de um registro/tipo
  - NSEC/NSEC3
- Criar o canal de confiança (*chain of trust*)
  - DS

Como funciona DNSSEC

Uso de criptografia assimétrica (DNSKEY)

- DNSSEC usa criptografia assimétrica para verificar autenticidade e integridade dos dados (assinatura digital)
- Chaves públicas armazenadas nos registros ***DNSKEY***

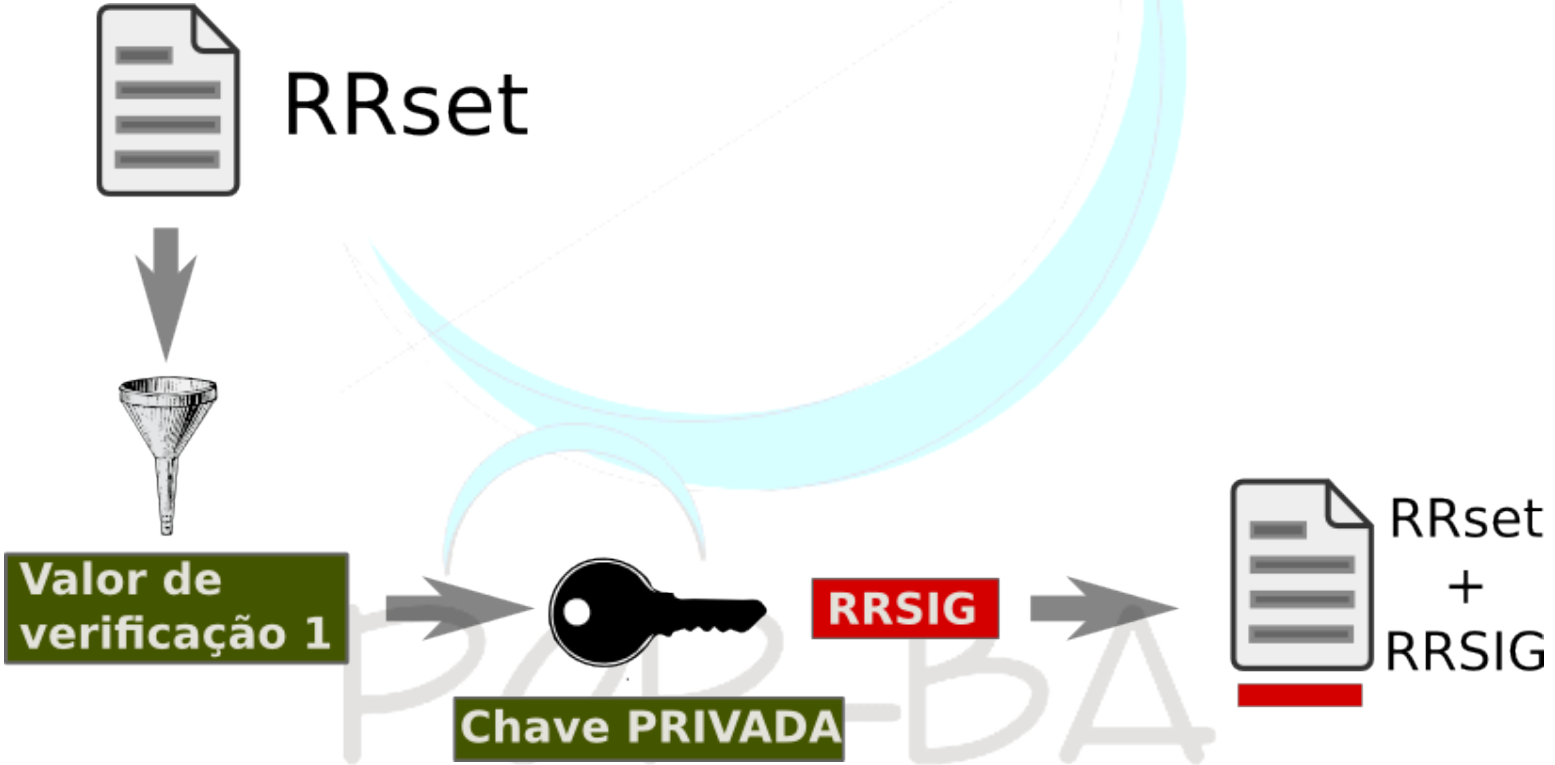
```
pop-ba.rnp.br.   IN   DNSKEY   257 3 5 zWDdbb6c4e23ffd428636071294
pop-ba.rnp.br.   IN   DNSKEY   256 3 5 QGd060ca2fc88f11b73a877e2cf
```

Assinatura dos registros (RRSIG)

- Usamos a chave privada para assinar os RRsets
- A assinatura gera um novo registro: ***RRSIG***
  - Assinatura digital: ***cifra(hash(RRset))***
- O processo de assinatura da zona é feito *off-line*

Assinatura dos registros (RRSIG)

- Na assinatura



Assinatura dos registros (RRSIG)

- Inicialmente

```
a.pop-ba.rnp.br.    IN    A    192.168.10.2
b.pop-ba.rnp.br.    IN    A    10.1.0.30
                    IN    A    10.1.0.40
```

Assinatura dos registros (RRSIG)

- Inicialmente

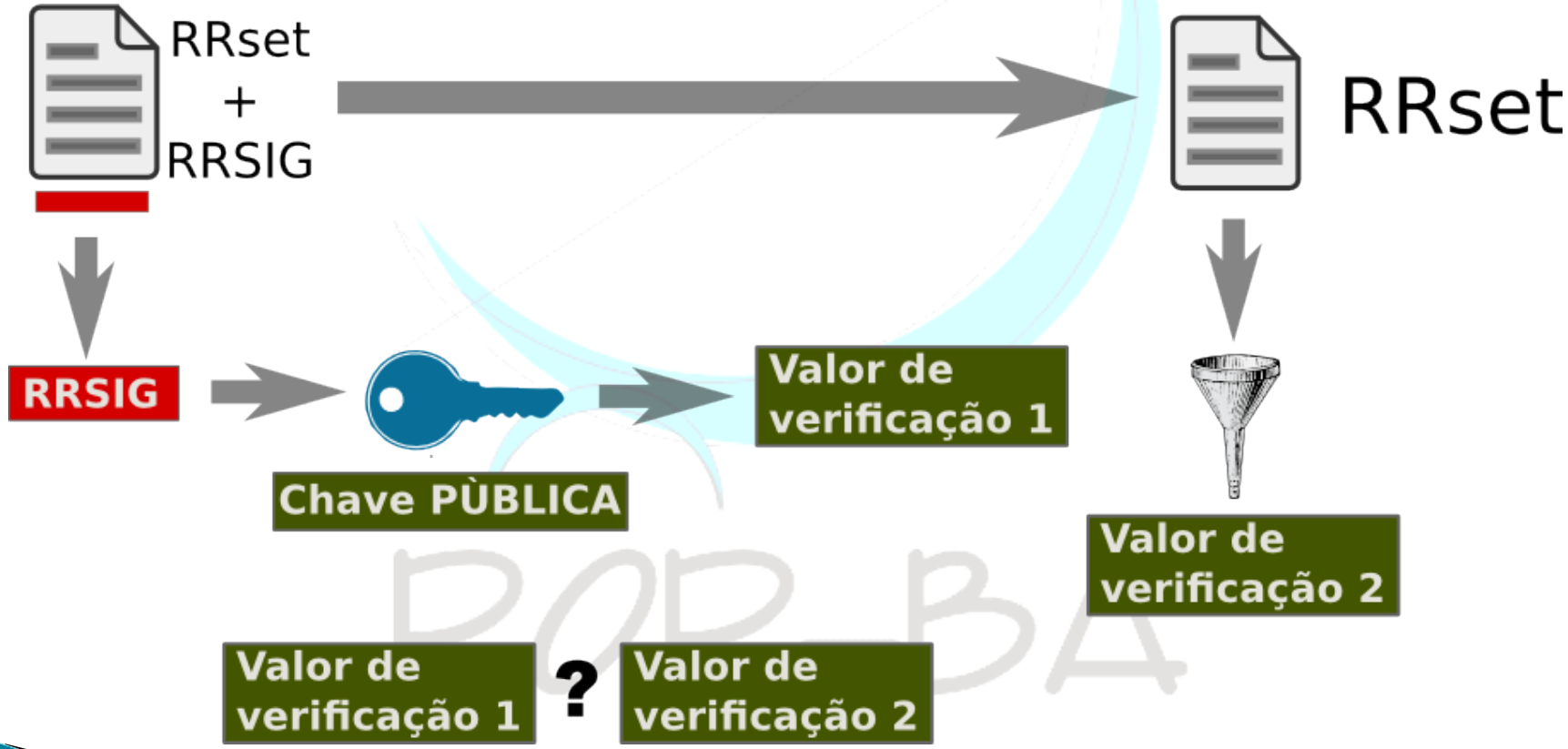
```
a.pop-ba.rnp.br.    IN    A    192.168.10.2
b.pop-ba.rnp.br.    IN    A    10.1.0.30
                    IN    A    10.1.0.40
```

- Depois de assinados

```
a.pop-ba.rnp.br.   IN  A          192.168.10.2
a.pop-ba.rnp.br.   IN  RRSIG  A   eZlH2hCUP8MzTY8fveAueLD86Kl/X4JjCxI
b.pop-ba.rnp.br.   IN  A          10.1.0.30
                   IN  A          10.1.0.40
b.pop-ba.rnp.br.   IN  RRSIG  A   DJTlGVd5ss2iB+gXQg44tykd8Hat3wVsRrB
```

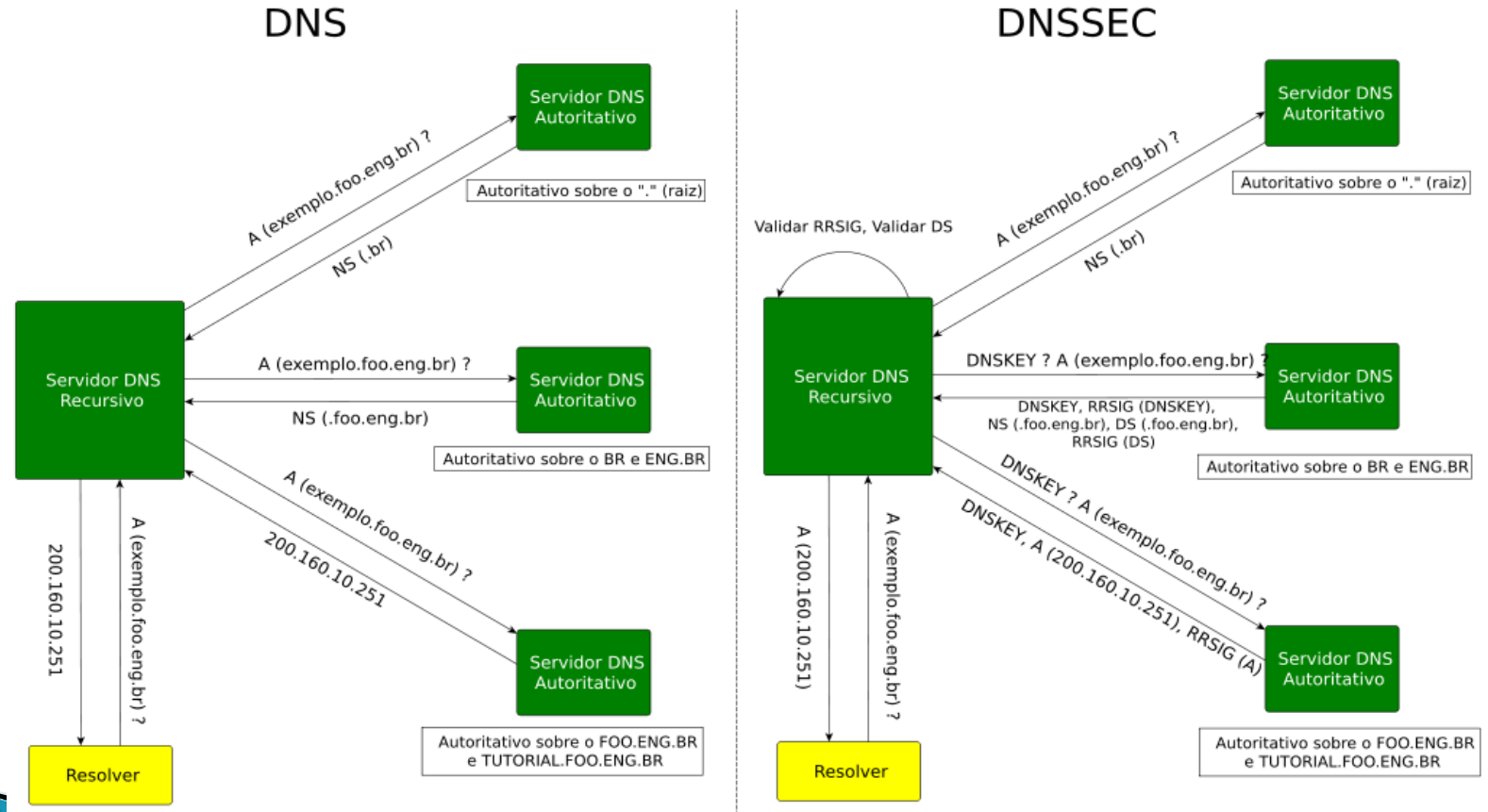
Assinatura dos registros (RRSIG)

- Como funciona a consulta no recursivo?



Assinatura dos registros (RRSIG)

- Como funciona a consulta no recursivo?



Fonte: Tutorial DNSSEC – Registro.br

Garantia de não-existência (NSEC)

- Porém, uma vez que a assinatura não é gerada em tempo real, como um servidor poderá assinar a resposta a uma consulta para o qual ele não conhece (*NXDOMAIN*)?
- Daí, surge o registro ***NSEC*** (Next SECure)
- A ideia é garantir a ***não existência*** de um registro

Garantia de não-existência (NSEC)

- O NSEC armazena informações sobre o próximo nome da zona, que agora passa a ser ordenada.
- Cada registro mantém um ***apontador*** (NSEC) para o próximo registro; o último ***aponta*** para o primeiro.

Garantia de não-existência (NSEC)

- Inicialmente

```
a.pop-ba.rnp.br.
b.pop-ba.rnp.br.
d.pop-ba.rnp.br.
```

Garantia de não-existência (NSEC)

- Inicialmente

```
a.pop-ba.rnp.br.
b.pop-ba.rnp.br.
d.pop-ba.rnp.br.
```

- Após assinar a zona

```
a.pop-ba.rnp.br
a.pop-ba.rnp.br NSEC b.pop-ba.rnp.br

b.pop-ba.rnp.br
b.pop-ba.rnp.br NSEC d.pop-ba.rnp.br

d.pop-ba.rnp.br
d.pop-ba.rnp.br NSEC a.pop-ba.rnp.br
```

Garantia de não-existência (NSEC)

- Do ponto de vista do cliente:
  - Consulta por ***c.pop-ba.rnp.br***
  - Recebe ***b.pop-ba.rnp.br NSEC d.pop-ba.rnp.br***
    - Assinado!
  - Ora, o cliente deve ser ***inteligente*** o suficiente para verificar que ***não existe c.pop-ba.rnp.br***

- Isso é chamado de ***garantia de não existência***

Cadeia de confiança (DS)

- Como garantir o canal de confiança na delegação de zonas?

- O registro ***DS*** armazena um hash do *DNSKEY* da zona que será delegada.
- No processo de consulta recursiva o cliente requisita o ***DS*** da zona parent e verifica com o *DNSKEY* da zona que foi delegada.

DNSSEC/Bahia/Brasil

DNSSEC

- Como está sua implantação no Brasil?
  - Obrigatório para JUS.BR
  - Registro.br tem incentivado bastante
  - PoP-BA é o segundo PoP do Brasil a implantar
    - Início dos trabalhos para implantação nos clientes (campanha DNSSEC-Ready)
- Mais informações:
  - http://cert.pop-ba.rnp.br

Prática de DNSSEC no recursivo

DNSSEC no recursivo

- Tutorial para implantação de DNSSEC no servidor recursivo
  - https://cert.pop-ba.rnp.br/DNSSEC_TutorialRecursivo
- Testando DNSSEC com o DIG
  - https://cert.pop-ba.rnp.br/DNSSEC_TesteDIG
- Documentação completa
  - https://cert.pop-ba.rnp.br/DocDNSSEC

Conclusões

Conclusões

- Novamente, excesso de confiança na Internet.
- Ataques no DNS não são fáceis de explorar, mas têm um impacto grande quando bem sucedidos (difícil de detectar)
- DNSSEC não soluciona todos os problemas, mas os principais.
  - Obviamente, tem-se um custo por isso.
- POP-BA / CERT.Bahia fornece todo o apoio aos clientes para implantação

Dúvidas?