

Tutorial DNSSEC ¹

David Robert Camargo de Campos
Rafael Dantas Justo
[<tutorial-dnssec@registro.br>](mailto:tutorial-dnssec@registro.br)

Registro.br

5 de março de 2008

¹ versão 1.3.8 (Revision: 4899)

A última versão deste tutorial pode ser encontrada em: <ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>

- Introduzir os conceitos de DNSSEC
- Apresentar um exemplo prático de DNSSEC utilizando BIND
- Incentivar a utilização de DNSSEC

1 DNS

- Conceitos
- Publicação
- Arquitetura
- Vulnerabilidades

2 DNSSEC

- Conceitos
- Resource Records
- Funcionamento
- Chaves
- DNS Vs DNSSEC

3 Implementação

- Softwares
- Configurações
- DNSSEC com BIND
- Testes de Validação
- Resumo Prático

4 Futuro

- Próximas Etapas
- Incentivo
- Referências

Parte I

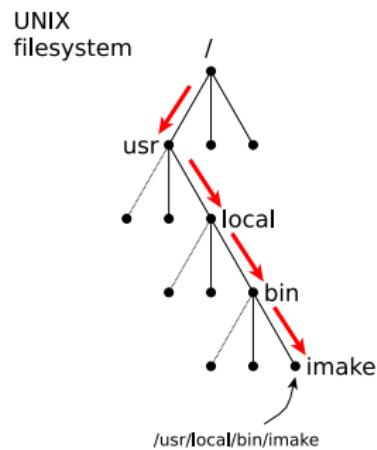
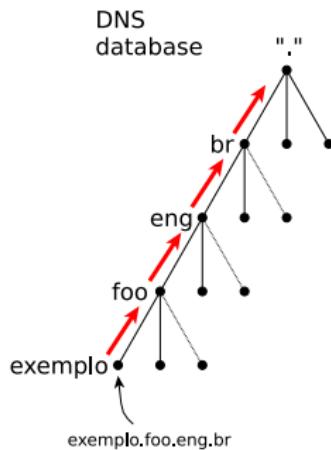
Conceitos de DNS e DNSSEC

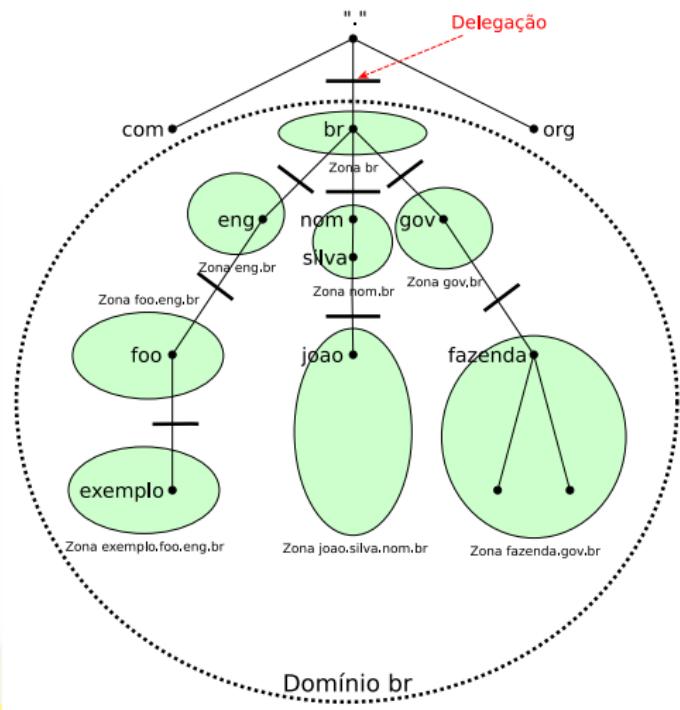


O Sistema de Nomes de Domínio é um banco de dados distribuído. Isso permite um controle local dos segmentos do banco de dados global, embora os dados em cada segmento estejam disponíveis em toda a rede através de um esquema cliente-servidor.

- Arquitetura hierárquica, dados dispostos em uma árvore invertida
- Distribuída eficientemente, sistema descentralizado e com cache
- O principal propósito é a resolução de nomes de domínio em endereços IP e vice-versa

exemplo.foo.eng.br	↔	200.160.10.251
www.cgi.br	↔	200.160.4.2
www регистрация br	↔	2001:12ff:0:2::3





Delegação

Indica uma transferência de responsabilidade na administração apartir daquele ponto na árvore DNS

- Reserva o direito da pessoa física ou jurídica sobre um determinado nome de endereço na Internet.
- Domínios não registrados não podem ser encontrados na Internet.

Sistema WEB

A interface WEB permite de maneira prática gerenciar os domínios de qualquer pessoa física ou jurídica.

- <http://registro.br/info/novo-registro.html>

EPP - Extensible Provisioning Protocol

É uma interface destinada somente a provedores de serviço previamente certificados pelo Registro.br.

- <http://registro.br/epp/>

O que é uma Publicação?

As modificações que são realizadas pela interface de provisionamento não são efetivadas imediatamente. A cada intervalo de tempo pré-determinado ocorre uma publicação DNS a qual atualiza o sistema DNS.



O que é uma Publicação?

As modificações que são realizadas pela interface de provisionamento não são efetivadas imediatamente. A cada intervalo de tempo pré-determinado ocorre uma publicação DNS a qual atualiza o sistema DNS.

As publicações DNS ocorrem a cada 30 minutos

- No caso do registro de um novo domínio ele já estará visível na Internet após a próxima publicação.
- No caso da alteração de dados de um domínio, após a próxima publicação, o domínio passará por um período de transição que poderá durar até 24 horas (tempo necessário para que o TTL do domínio expire e elimine o cache).

Os dados associados com os nomes de domínio estão contidos em **Resource Records** ou **RRs** (Registro de Recursos)

- São divididos em classes e tipos
- Atualmente existe uma grande variedade de tipos
- O conjunto de resource records com o mesmo nome de domínio, classe e tipo é denominado **RRset**

Alguns Tipos Comuns de Records

SOA Indica onde começa a *autoridade* a zona

NS Indica um *servidor de nomes* para a zona

A Mapeamento de nome a endereço (IPv4)

AAAA Mapeamento de nome a endereço (IPv6)

Exemplo de records de uma zona

```
foo.eng.br. IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (  
    1           ; serial  
    3600        ; refresh  
    3600        ; retry  
    3600        ; expire  
    900 )       ; TTL  
  
foo.eng.br.          IN NS ns1.foo.eng.br.  
foo.eng.br.          IN NS ns2.foo.eng.br.  
exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br  
exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br  
ns1.foo.eng.br.     IN A 200.160.3.97  
ns2.foo.eng.br.     IN A 200.160.10.251  
ns1.exemplo.foo.eng.br. IN A 200.160.3.97  
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
```

Servidor Recursivo

Ao receber requisições de resolução de nomes, faz requisições para os servidores autoritativos e conforme a resposta recebida dos mesmos continua a realizar requisições para outros servidores autoritativos até obter a resposta satisfatória

Servidor Autoritativo

Ao receber requisições de resolução de nome, responde um endereço caso possua, uma referência caso conheça o caminho da resolução ou uma negação caso não conheça



Exemplo de requisição de endereço

Supondo que o cache esta vazio ou sem informações de br, eng.br, foo.eng.br, exemplo.foo.eng.br

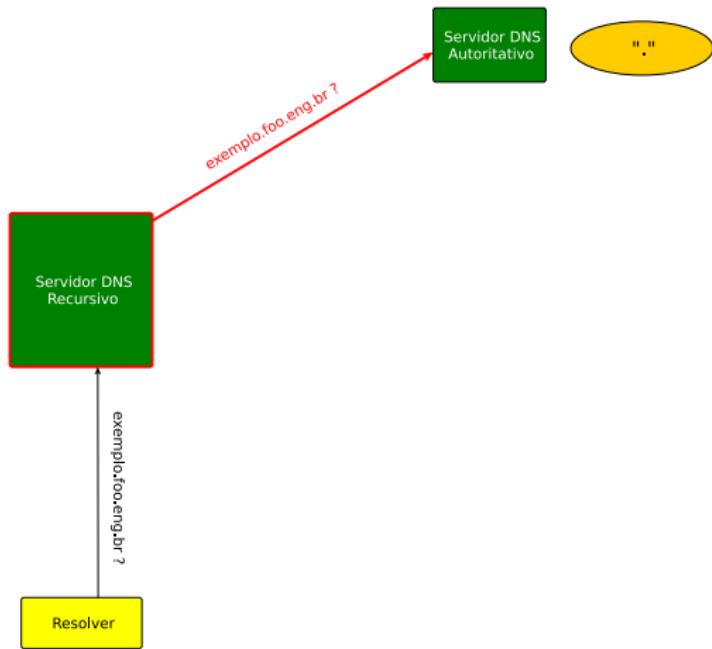
Resolver

Exemplo de requisição de endereço

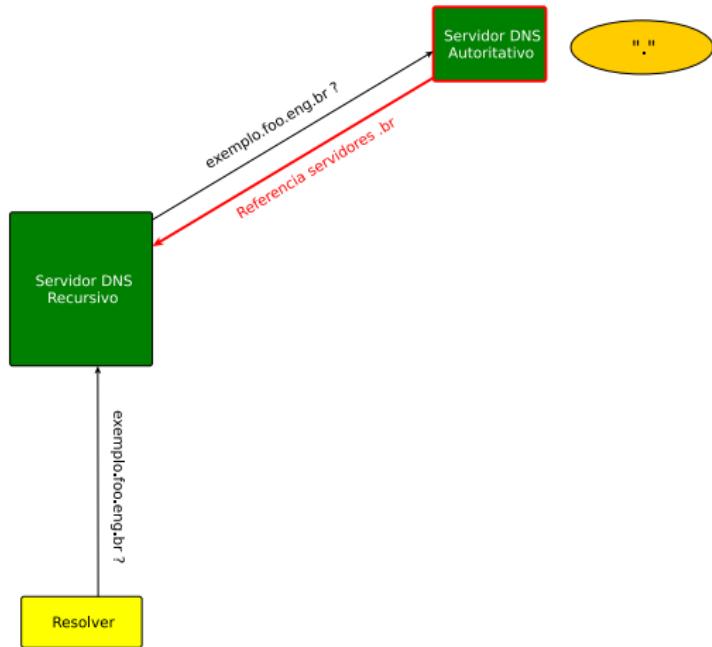
Supondo que o cache esta vazio ou sem informações de br, eng.br, foo.eng.br, exemplo.foo.eng.br



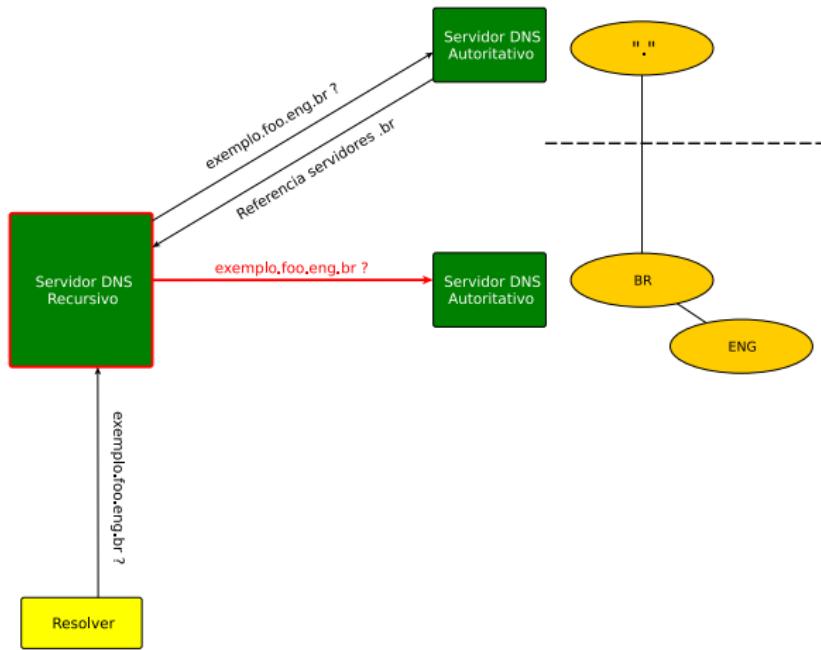
Exemplo de requisição de endereço



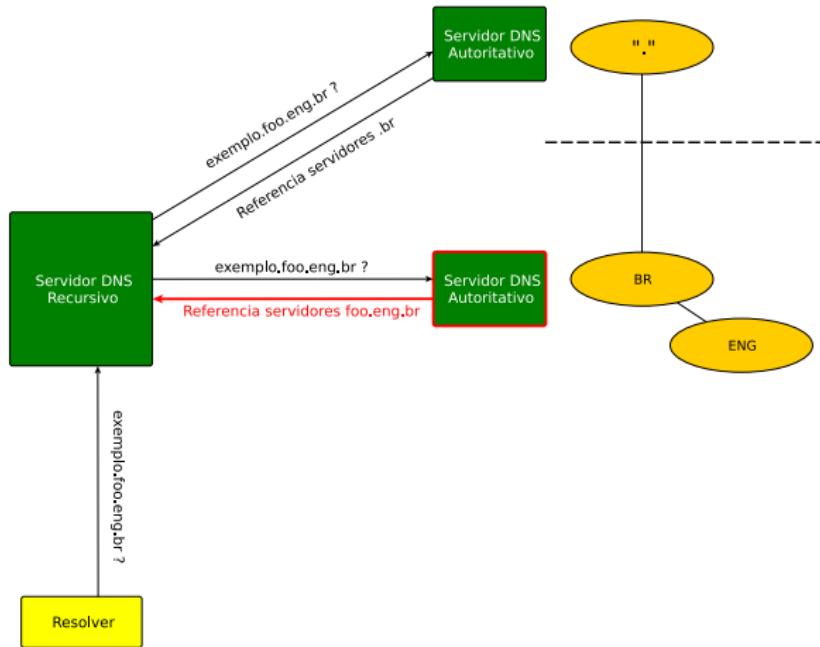
Exemplo de requisição de endereço



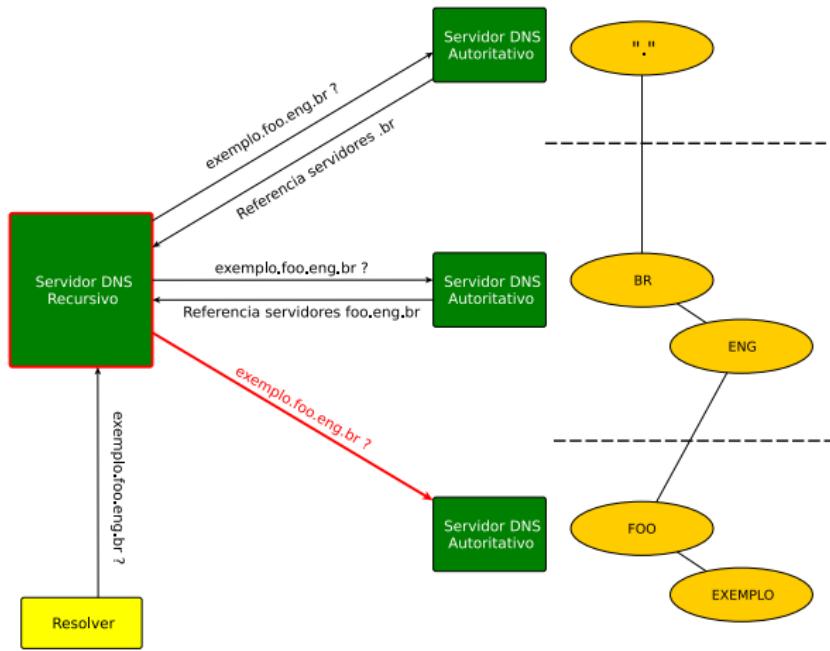
Exemplo de requisição de endereço



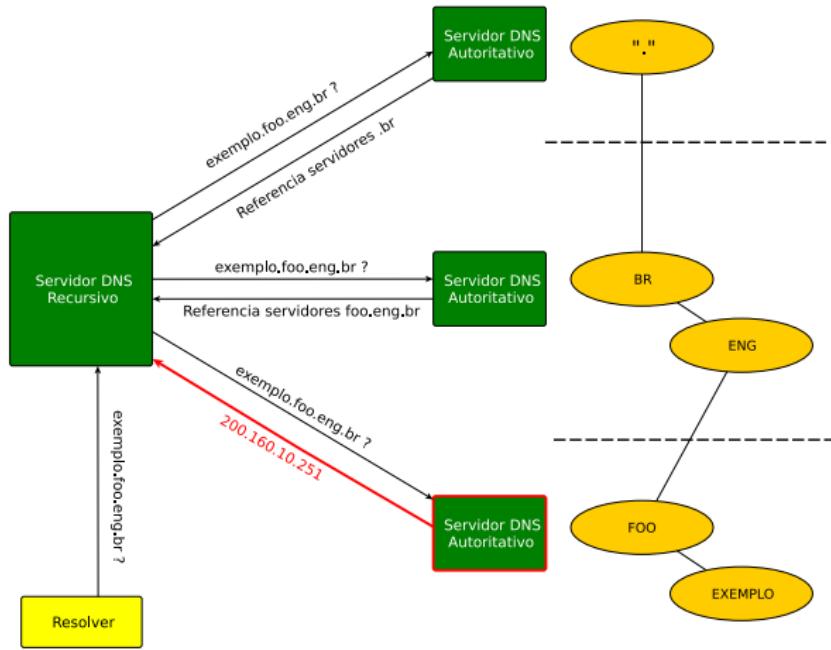
Exemplo de requisição de endereço



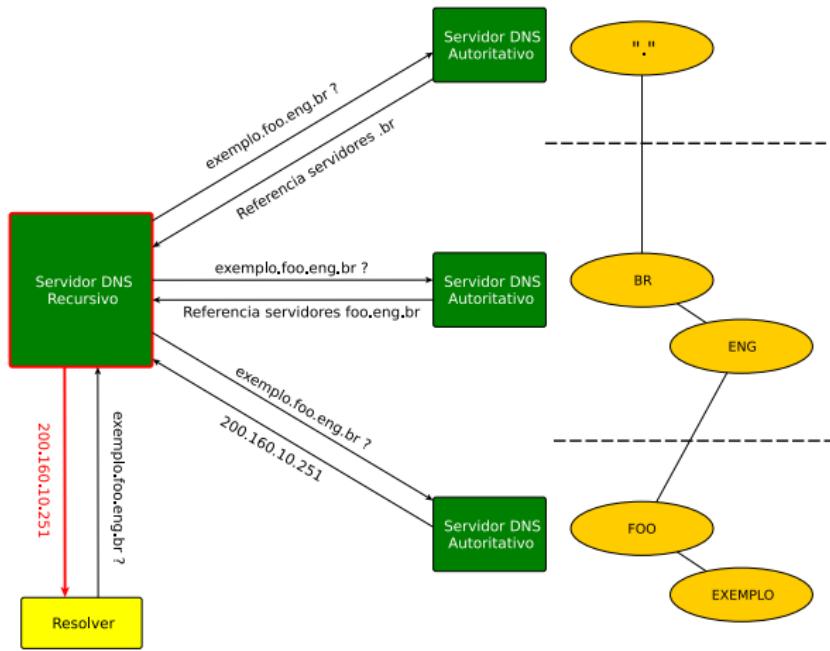
Exemplo de requisição de endereço



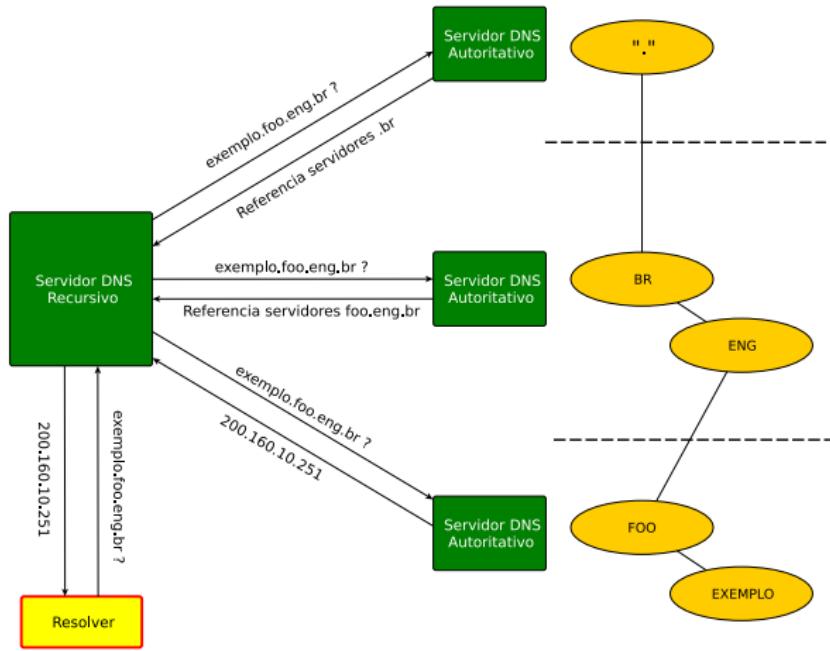
Exemplo de requisição de endereço

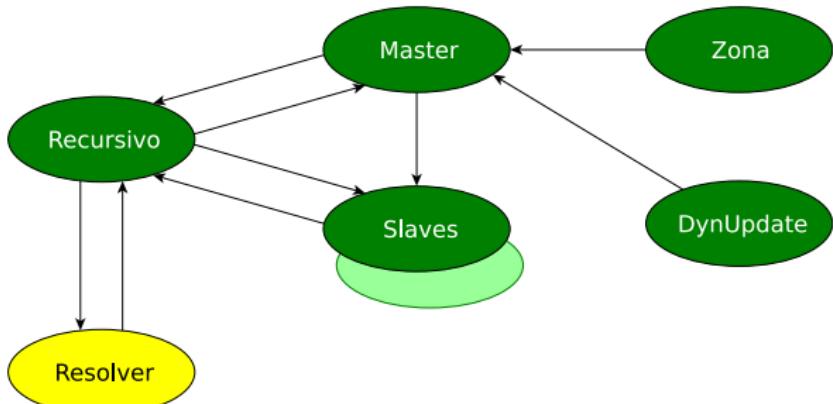


Exemplo de requisição de endereço

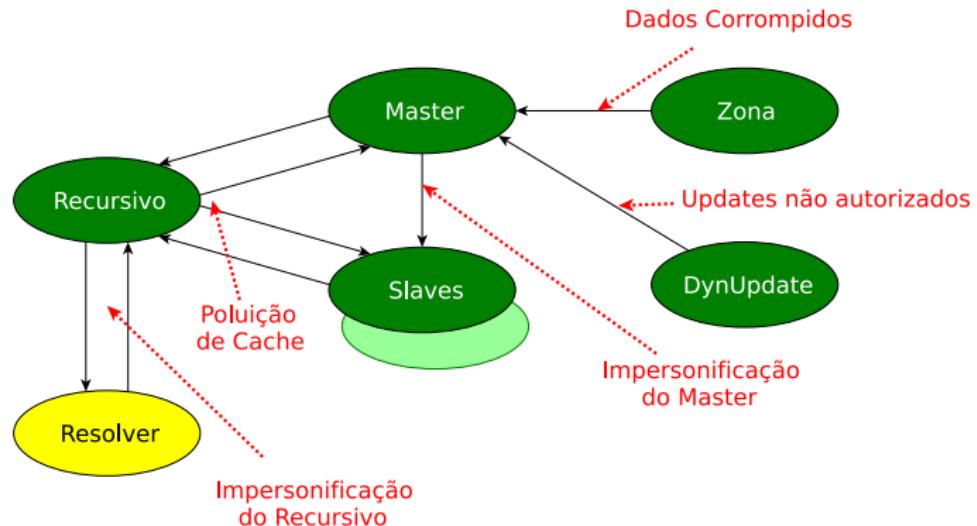


Exemplo de requisição de endereço

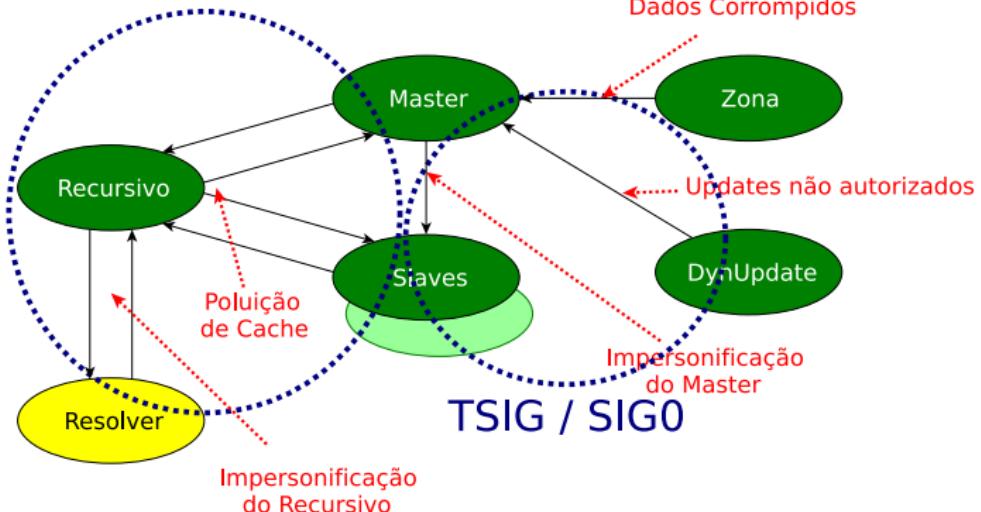




- 1 Resolver faz consultas no Recursivo
- 2 Recursivo faz consultas no Master ou Slave
- 3 Master tem a zona original (via arquivo ou Dynamic Update)
- 4 Slave recebe a zona do Master (AXFR ou IXFR)



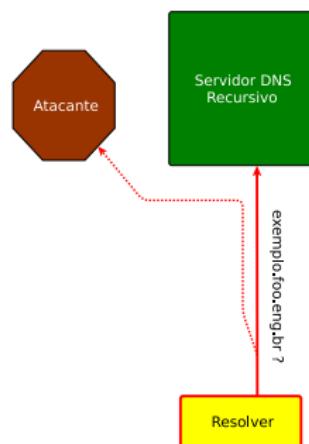
DNSSEC bis



Exemplo de Ataque

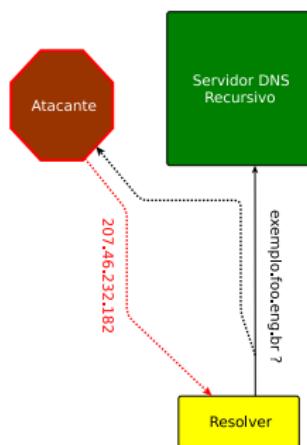
Resolver

Exemplo de Ataque



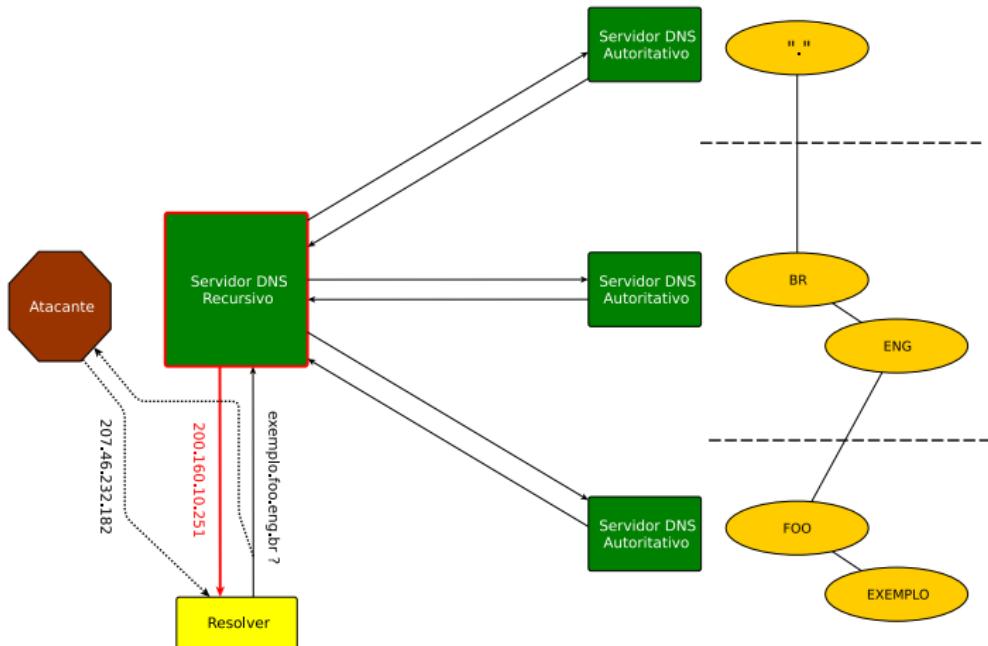
Exemplo de Ataque

O atacante responde mais rápido, spoofando endereço do recursivo



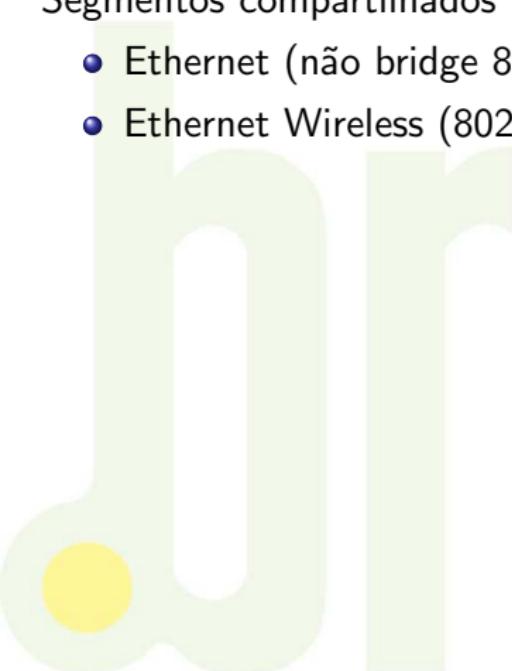
Exemplo de Ataque

O atacante responde mais rápido, spoofando endereço do recursivo



Segmentos compartilhados L2 ponto-multiponto

- Ethernet (não bridge 802.1d)
- Ethernet Wireless (802.11)



Segmentos compartilhados L2 ponto-multiponto

- Ethernet (não bridge 802.1d)
- Ethernet Wireless (802.11)

Atenção muito cuidado em conferências !

TSIG

Transaction Signatures – RFC 2845

- Autorização de AXFR (atualização total), IXFR (atualização das modificações) e Dynamic Updates (atualização imediata)
- Autenticação do servidor cache forwarder
- Tráfego assinado com a chave compartilhada



TSIG

Transaction Signatures – RFC 2845

- Autorização de AXFR (atualização total), IXFR (atualização das modificações) e Dynamic Updates (atualização imediata)
- Autenticação do servidor cache forwarder
- Tráfego assinado com a chave compartilhada

DNSSEC

- Provê segurança para a resolução de endereços
- Funciona como um caminho alternativo para a verificação de autenticidade
- Suas verificações ocorrem antes de diversas aplicações de segurança (SSL, SSH, PGP, etc...)

- Extensão da tecnologia DNS
(o que existia continua a funcionar)
- Possibilita maior segurança para o usuário na Internet
(corrigindo falhas do DNS)
- Atualmente em sua segunda versão denominada DNSSEC bis

O que garante?

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



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)



Avanço de DNSSEC no Mundo

World Wide DNSSEC Deployment

See also [DNSSEC Theory and World Wide Deployment](#) by Paul Wouters, November 21, 2007, [SecTor](#)



This map was created by Paul Wouters

fonte: <http://www.xelerance.com/dnssec/>

Quem pode utilizar DNSSEC?

Os registros que estiverem abaixo dos domínios indicados no site
<http://www регистрації.рф/info/dpn.html>



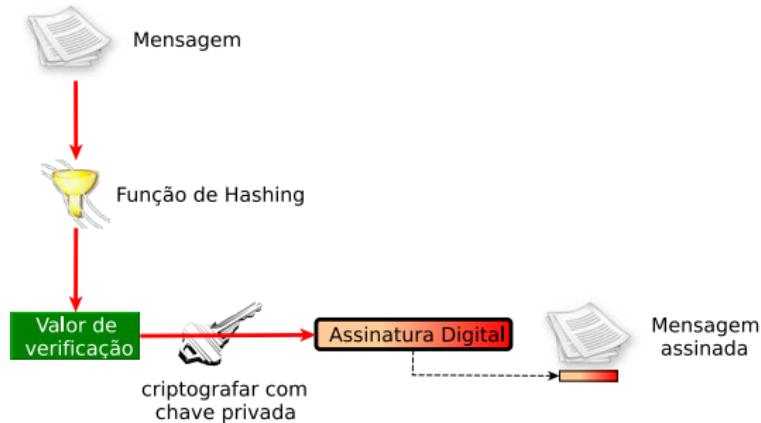
Quem pode utilizar DNSSEC?

Os registros que estiverem abaixo dos domínios indicados no site
<http://www регистра.бр/info/dpn.html>

Onde DNSSEC é Obrigatório?

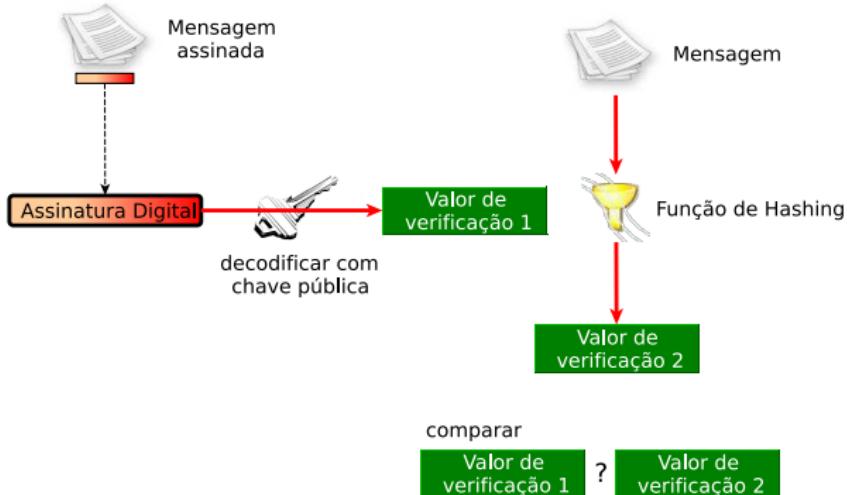
É obrigatório nos registros que estiverem diretamente abaixo dos domínios
.B.BR e .JUS.BR

Assinatura



DNSSEC utiliza o conceito de chaves assimétricas
– chave pública e chave privada

Verificação



DNSSEC utiliza o conceito de chaves assimétricas
– chave pública e chave privada

DNSKEY Chave pública

RRSIG Assinatura do RRset (somente registros com autoridade)

DS Delegation Signer (Ponteiro para a cadeia de confiança)

NSEC Aponta para o próximo nome e indica quais os tipos dos RRsets para o nome atual

É um resource record que armazena a chave pública da zona

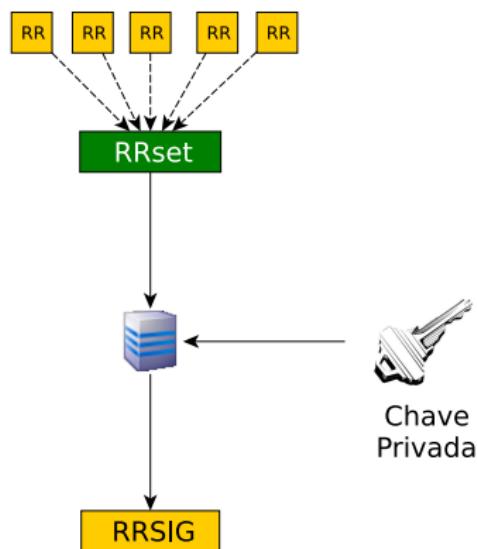
0	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	3	3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
/																					/
/																					/
/																					/

Exemplo

foo.eng.br.

```
900 IN DNSKEY 256 3 5 (
    AweAAeZPN2yMs9q6kgYjFUblEwjCnWwCpq+TGcJrD5ga
    XXAbP5MAqIkZ5J4TU1mmpL1A8gMfd/wUmBkVipXR8FK
    HRajBZSRfgeKnKaQtrxNZ32Ccts2F6Y1v9WaLxtiqebg
    OZtuJFpQr6pnIt/FoOI+I7BUsNrX28VTq4jXu/qTrmM/
) ; key id = 62745
```

- É um resource record que contém a assinatura de um RRset específico com uma determinada chave (DNSKEY)
- Possui uma validade inicial (inception) e final (expiration)



Exemplos de RRset:

```
foo.eng.br.      IN NS ns1.foo.eng.br.  
foo.eng.br.      IN NS ns2.foo.eng.br.
```

```
ns1.foo.eng.br.  IN A 200.160.3.97
```

```
ns2.foo.eng.br.  IN A 200.160.3.97
```

1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	3	3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
	Type Covered																		Algorithm	Labels	
	Original TTL																				
	Signature Expiration																				
	Signature Inception																				
	Key Tag																		/		
/	Signer's Name																		/		
/	Signature																		/		
/																			/		

Exemplo

foo.eng.br.

```
900 IN RRSIG SOA 5 3 900 20070617200428 (
    20070518200428 62745 foo.eng.br.
    g1EeCYyd/CCBfzH64y0RAQf90xYDsI4xuBNam+8DZQZ
    xeoSLQEEtwmp6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE
    1LLgLI+BLwdlz0t8MypcpL0aTm9rc7pP7UR5XLzU1k8D
    m6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCuja= )
```

É um hash do Record DNSKEY

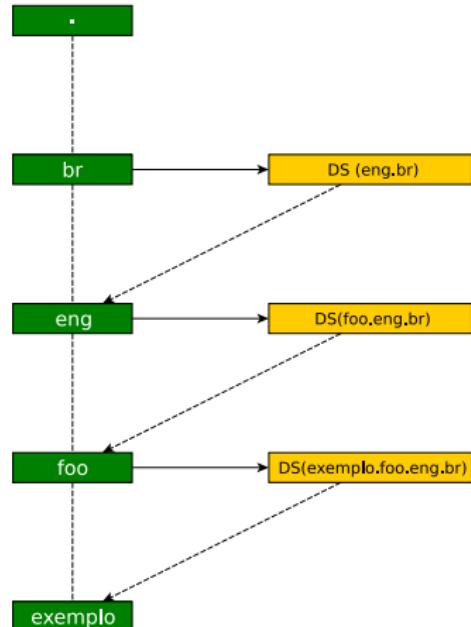
Serve para informar que existem uma cadeia de confiança entre um domínio e seus sub-domínios.

Indica:

- que a zona delegada está assinada
- qual a chave usada na zona delegada

A zona Pai tem autoridade pelo registro DS

- Os registros NS são apenas “hints” e não são autoritativos no Pai
- O record DS **não** deve aparecer no Filho



Cadeia de Confiança

O Record DS é um ponteiro para a cadeia de confiança, a qual garante a autenticidade das delegações de uma zona até um ponto de confiança – uma chave ancorada ou a utilização de DLV

1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	3	3		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	
	Key Tag											Algorithm		Digest Type								
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	
/											/											/
/	Digest										/											/
/											/											/
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	

Exemplo

foo.eng.br.

IN DS 817 5 1 EAEC29E4B0958D4D3DFD90CC70C6730AD5880DD3

É possível obter os DS da zona utilizando o sistema Whois.

Exemplo de DS pelo Whois

```
$ whois foo.eng.br
domain:      foo.eng.br
owner:       Frederico A. C. Neves
address:     Av. das Nacoes Unidas, 11541, 7 andar
address:     04578-000 - São Paulo - SP
country:     BR
owner-c:    FAN
admin-c:    FAN
tech-c:     FAN
billing-c:  FAN
nserver:    dixit.foo.eng.br 200.160.7.134
nsstat:     20070619 AA
nslastaa:   20070619
nserver:    sroot.dns.br
nsstat:     20070619 AA
nslastaa:   20070619
ds-record:  6928 RSA/SHA-1 CA7D9EE79CC37D8DC8011F33D330436DF76220D1
created:    20000103 #237812
expires:    20080103
changed:   20070604
status:     published
```

Permite autenticar uma resposta negativa

- Próximo nome seguro
- Indica os tipos de RRsets existentes
- Último registro da zona aponta para o primeiro (SOA)

1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	3	3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1

/	Next Domain Name																		/		

/	Type Bit Maps																		/		

Exemplo

foo.eng.br.

900 IN NSEC ns1.exemplo.foo.eng.br. NS SOA RRSIG NSEC DNSKEY

Prova de não existência, com pré-assinatura, sem a necessidade de chaves on-line para assinatura on-demand. Diminuindo a possibilidade de DOS.

• Respostas NXDOMAIN

- Um ou mais registros NSEC indicam que o nome ou a sintetização de um wildcard não existe

```
$ dig @200.160.10.251 zzz.foo.eng.br SOA +dnssec
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 18301
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
;; QUESTION SECTION:
;zzz.foo.eng.br.      IN  SOA
;; AUTHORITY SECTION:
foo.eng.br.          0    IN  SOA    ns1.foo.eng.br. hostmaster.foo.eng.br. 1 3600 3600 3600 900
foo.eng.br.          0    IN  RRSIG   SOA 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                           g1EeCYyd/CCBfzH64y0RAQf90xYDsI4xuBnaam+8DZQZxeoSLQEETwmp
                           6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE1LLgLI+BLwdlz0t8MypcpL0a
                           Tm9rc7pP7UR5XLzU1k8Dm6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCuja=
foo.eng.br.        900  IN  NSEC   ns1.exemplo.foo.eng.br. NS SOA RRSIG NSEC DNSKEY
foo.eng.br.        900  IN  RRSIG   NSEC 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                           0COCpFW5fR6MPhVBaUWfrP9pkIqVc+NDORi6PRwIX/p1dLmAT7NF5Rkc
                           9IfbAHZTxefoqTkqN/vPl1PqSxUzh0rl+atHblaH6yt79CTkmStota7C
                           SLYYXX5c7D93hRYJ2yk1COxQz6GG9SIp/U4qR4//TcQDHpqQ4bFs42ZsD4I=
ns2.foo.eng.br.  900  IN  NSEC   foo.eng.br. A RRSIG NSEC
ns2.foo.eng.br.  900  IN  RRSIG   NSEC 5 4 900 20070617200428 20070518200428 62745 foo.eng.br.
                           XVf7M09L4rVUD6uxa1P+EhQYohuimuwk1xzAemsn292esUhkkYz/BG7b
                           OT/L9fhzOEPYtYGFyMF4gZ1+mxwY31UmX6xVZZPYFJ7x5Kw2uTSD49FK
                           VsdUOLBCAHz088byAm8EwLe31+U0/q8RvPimAfpouoiivUDcuWtKxs0CzLyc=
```

- Resposta **NOERROR** + sem resposta (ANSWER = 0)
 - O registro NSEC prova que o tipo consultado não existe

```
$ dig @200.160.10.251 foo.eng.br TXT +dnssec
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60466
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; QUESTION SECTION:
;foo.eng.br.      IN  TXT
;; AUTHORITY SECTION:
foo.eng.br.    900   IN  SOA    ns1.foo.eng.br. hostmaster.foo.eng.br. 1 3600 3600 3600 900
foo.eng.br.    900   IN  RRSIG   SOA 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                           g1EeCYyd/CCBfzH64yORAQf90xYDsI4xuBNaam+8DZQZxeoSLQEETwmp
                           6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE1LLgLI+BLwdlz0t8MypcpL0a
                           Tm9rc7pP7UR5XLzU1k8Dm6ePW1bNkId7i0IPSghyoHM7tPvdL2GW51hCuja=
foo.eng.br.  900   IN  NSEC   ns1.exemplo.foo.eng.br. NS SOA RRSIG NSEC DNSKEY
foo.eng.br.    900   IN  RRSIG   NSEC 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                           OCOCpFW5fR6MPhVBaUWfrP9pkIqVc+NDORi6PRwIX/p1dLmAT7NF5Rkc
                           9IfbAHZTxefoqTKqN/vPl1PqSxUzh0rl+atHblaH6yt79CTkmStota7C
                           SLYYXX5c7D93hRYJ2y1C0xQz6GG9SIp/U4qR4//TcQDHpqQ4bFs42ZsD4I=
```

Record NSEC utilizado apenas para provar não existência. Não aparece em consultas “positivas”

```
$ dig @200.160.10.251 foo.eng.br SOA +dnssec +noadditional
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6372
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;foo.eng.br.      IN  SOA
;; ANSWER SECTION:
foo.eng.br.    900   IN  SOA    ns1.foo.eng.br. hostmaster.foo.eng.br. 1 3600 3600 3600 900
foo.eng.br.    900   IN  RRSIG   SOA 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                           g1EeCYyd/CCBfzH64yORAQf90xYDsI4xuBNaam+8DZQZxeoSLQEEtwmp
                           6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE1LLgLI+BLwdlz0t8MypcpL0a
                           Tm9rc7pP7UR5XLzU1k8Dm6ePW1bNkId7i0IPSghyoHM7tPvdL2GW51hCuJA=
;; AUTHORITY SECTION:
foo.eng.br.    900   IN  NS     ns2.foo.eng.br.
foo.eng.br.    900   IN  NS     ns1.foo.eng.br.
foo.eng.br.    900   IN  RRSIG   NS 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                           3iLm1ROC+UeqYk0xgQQQXkBzcKiKQRPwe+1JZlpjEzjU1UjOHU0Hefa
                           jXzMv7F1FMWYeU51Ybg49HFe67XQV1K54GeAFXWB7YS59yODLoNEBxQ1
                           9QEy6g/0OnLpuKTrST8qqd5Fc/eYqN/Ag3GnfcAviZgiQhhveGH9mJHWZyc=
```

- Autenticidade e Integridade são providas pela assinatura dos Resource Records Sets (RRset) com uma chave privada
- Zonas delegadas (filhas) assinam seus RRsets com a chave privada
 - Autenticidade da chave é verificada pela assinatura na zona pai do Record DS (hash da chave pública – DNSKEY – da zona filha)
- Chave pública é usada para verificar assinatura (RRSIGs) dos RRsets
- Autenticidade da não existência de um nome ou tipo provida por uma cadeia de nomes (NSEC) que aponta para o próximo nome em uma sequência canônica

- Não existem Certificados
(Certification Authority, Service Level Agreement, Certificate Revocation List)
- Chaves nunca expiram
- Assinaturas têm prazo de validade
(inception e expiration do RRSIG)
- Políticas das chaves são locais a zona

Sempre que utilizar um Servidor Recursivo com DNSSEC habilitado é necessário ancorar a chave pública.

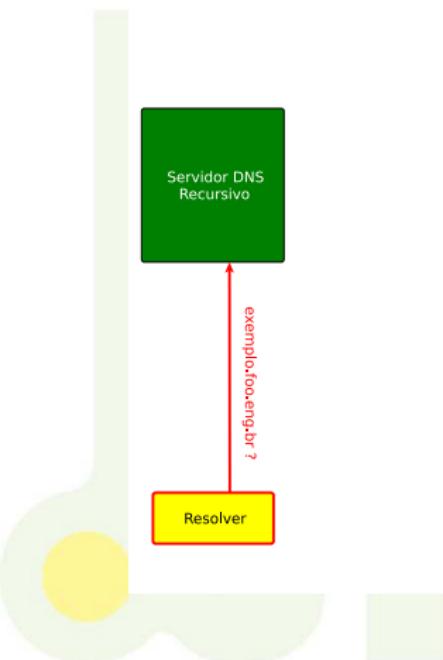
Isto serve para associar o inicio da cadeia de confiança a um ponto seguro.

Obtendo a chave a ser ancorada da zona “.br”

- .BR <https://registro.br/ksk/>

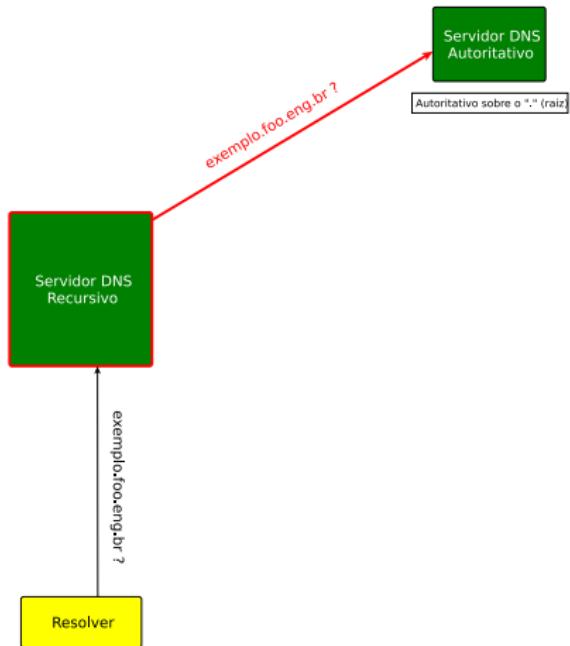
Exemplo

- O resolver recursivo já possui a chave pública da zona “.br” ancorada

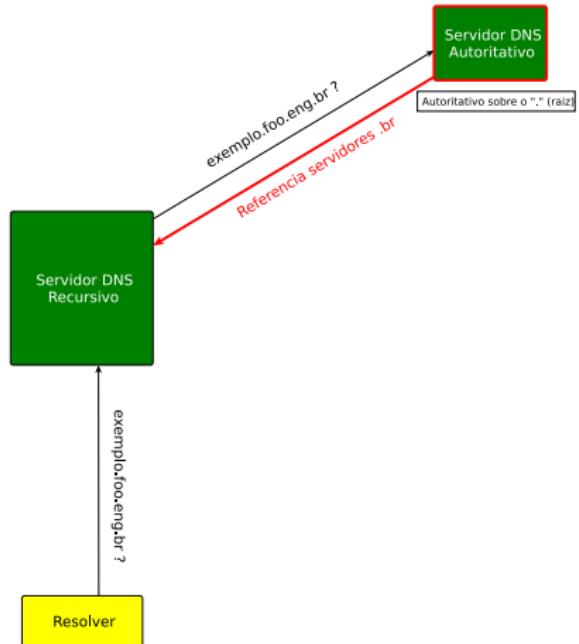


Exemplo

- Nesta simulação de resolução supomos que a raiz não está assinada.

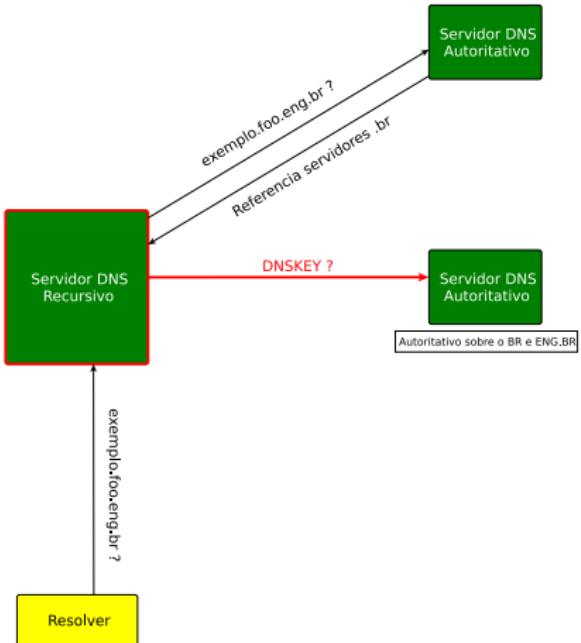


Exemplo



- Retorna sem resposta, mas com referência para os Records: NS do “.br” .

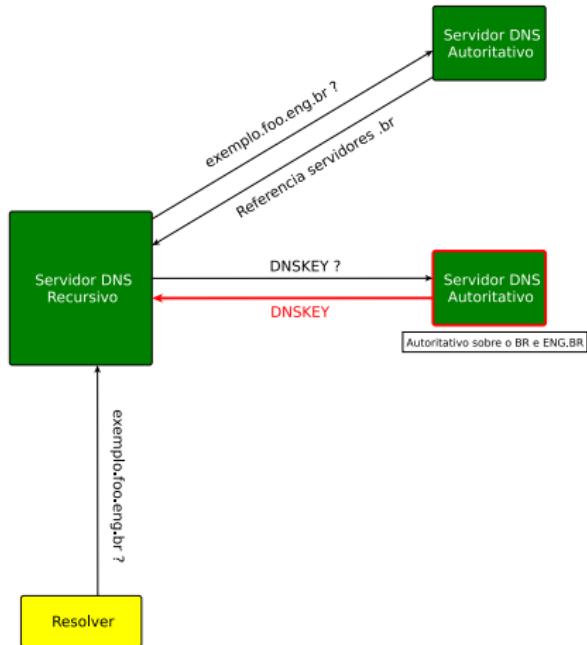
Exemplo



- O servidor recursivo requisita a DNSKEY ao verificar que o nome da zona é igual ao nome da zona que consta em sua trusted-key.

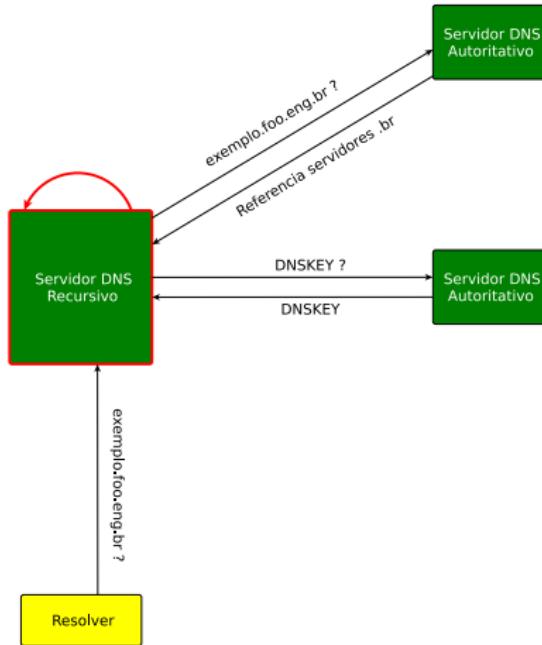
Exemplo

- O servidor DNS responde enviando DNSKEY e o RRSIG

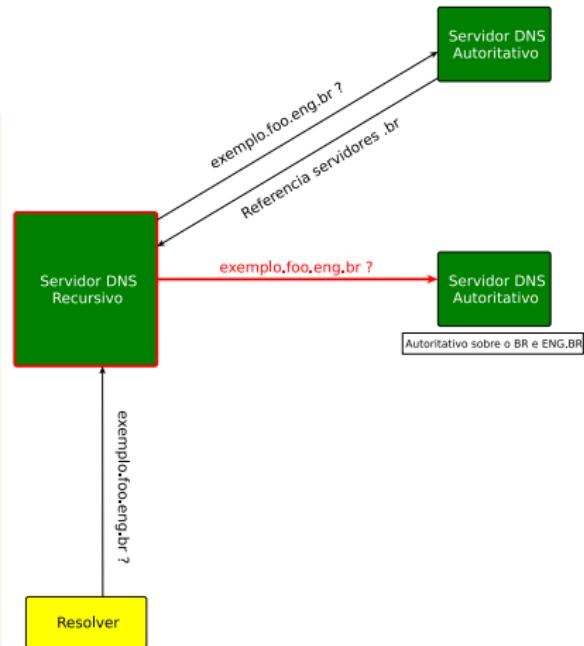


Exemplo

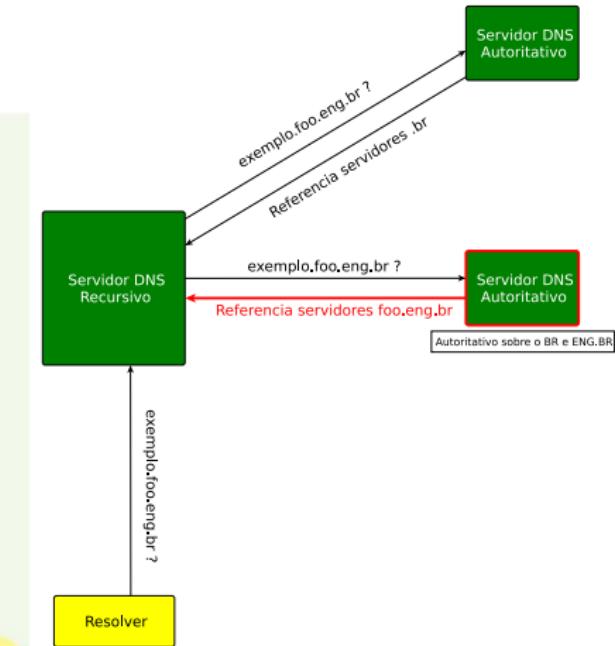
- Compara a trusted-key com a DNSKEY, caso for válida continua com as requisições



Exemplo



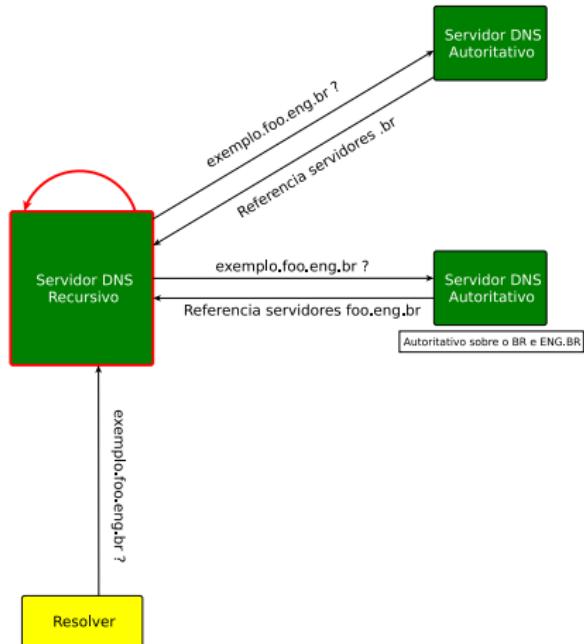
Exemplo



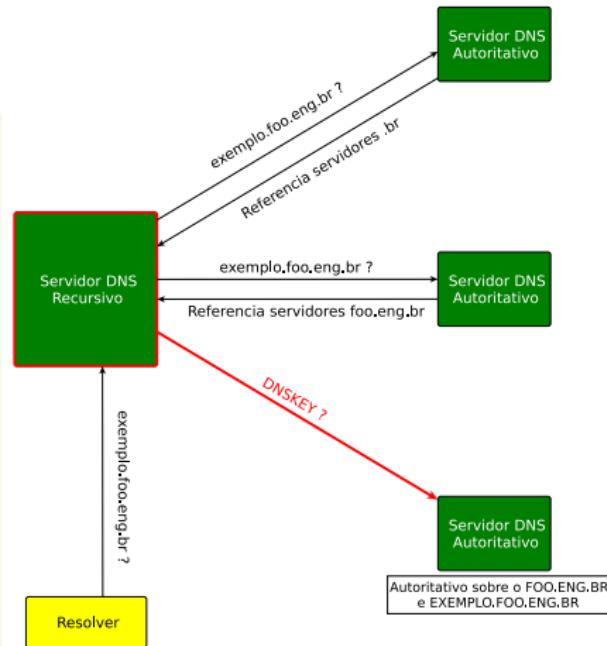
- Retorna sem resposta, mas com referência para os Records:
 - NS do “foo.eng.br”
- e com autoridade sobre os Records:
 - DS do “foo.eng.br”
 - RRSIG do Record DS

Exemplo

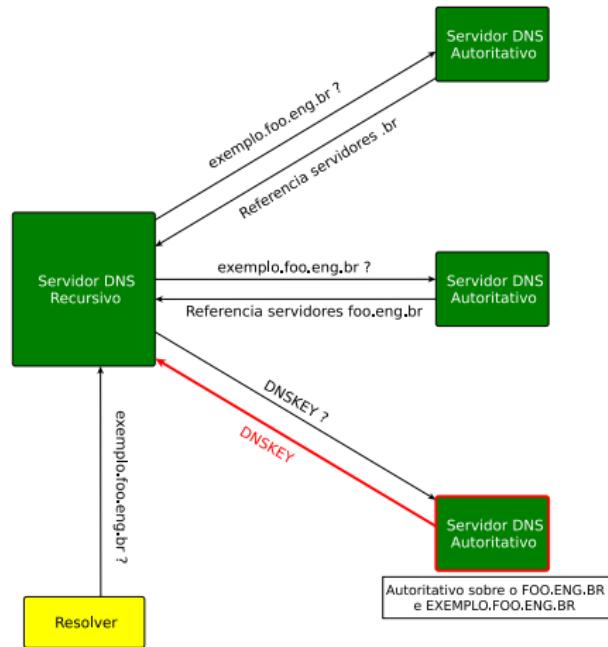
- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record DS



Exemplo

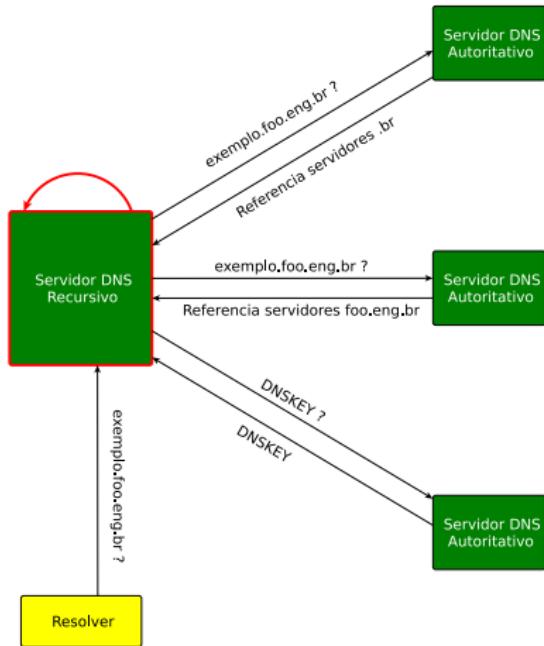


Exemplo

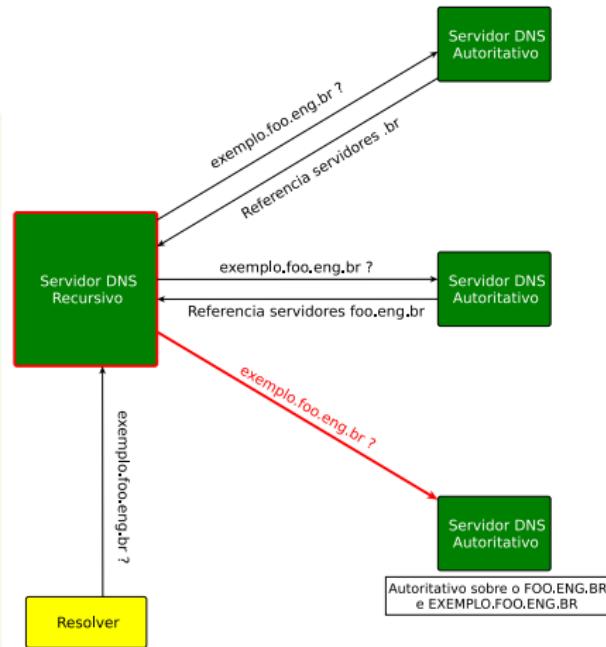


Exemplo

- O servidor DNS recursivo verifica através do DS e da DNSKEY, se este servidor DNS é válido.

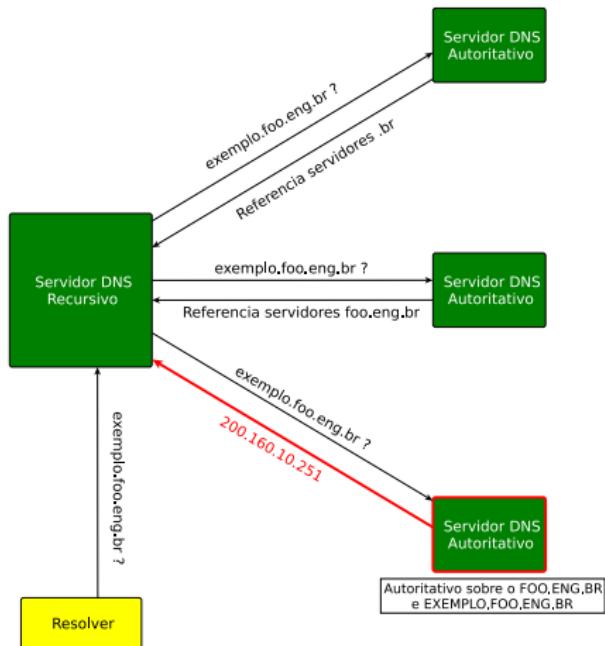


Exemplo



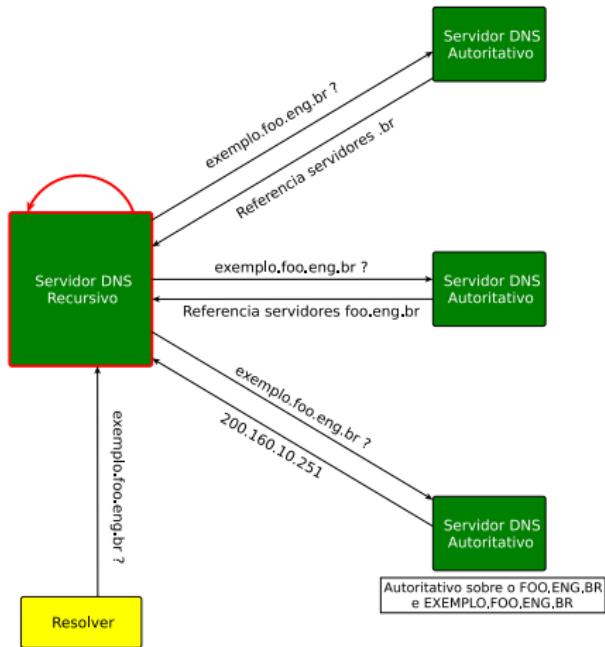
Exemplo

- Retorna o Record A e sua assinatura RRSIG.

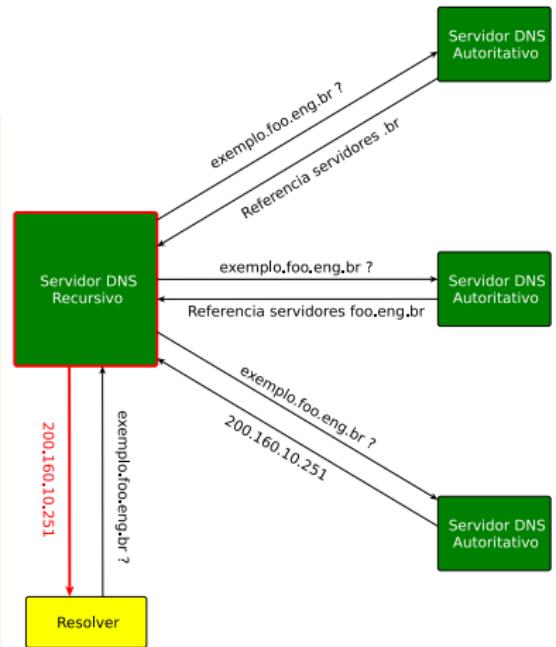


Exemplo

- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record A

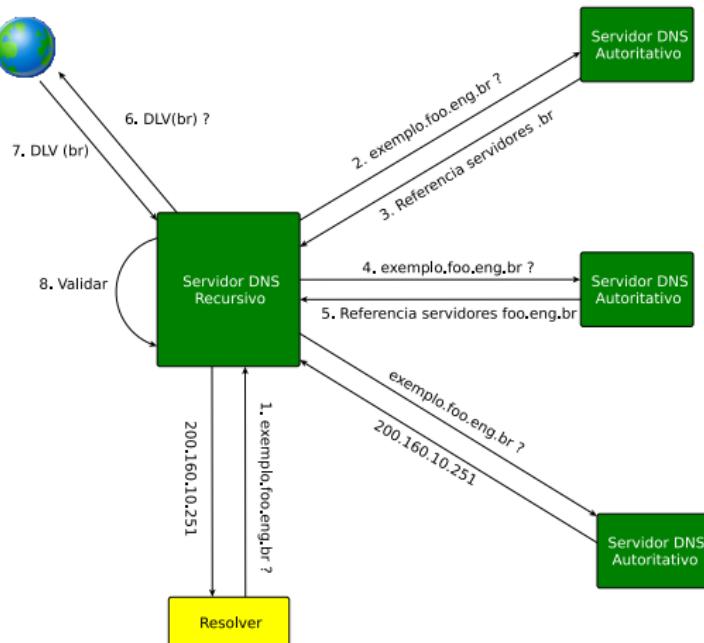


Exemplo



DLV – DNSSEC Lookaside Validation

Exemplo de chave não ancorada



- Permite que um domínio sem um pai assinado utilize DNSSEC



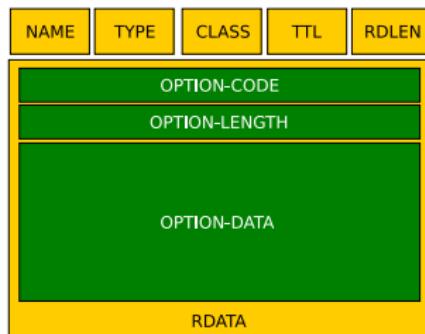
RFC 4431
The DNSSEC
Lookaside Validation
(DLV) DNS Resource
Record

Criado de forma a tornar mais flexíveis as limitações dos campos no protocolo DNS e possibilitar a análise de novos fatores na camada de transportes.

- Permite aos solicitadores informarem a capacidade máxima de seus pacotes UDP. Eliminando a limitação UDP DNS de 512 bytes.
- Aumenta a quantidade de flags e expande alguns campos já existentes no protocolo para permitir uma maior diversidade de valores
- É estruturado de forma a permitir o crescimento do protocolo
- Distingue quem suporta DNSSEC a partir da flag DO (DNSSEC OK, nova flag incluída nesta extensão)

Lembrete

É necessário que o transporte TCP também esteja habilitado no servidor.



NAME	“ ‘ . ’ ”
TYPE	“ ‘ OPT ’ ”
CLASS	Tamanho do pacote UDP
TTL	RCODE estendido e Flags
RDATA	Pares {Atributo, Valor}

Pseudo-RR OPT

- Armazena informações do EDNS0
- Não é armazenado em arquivo, sendo apenas utilizado no momento da comunicação entre os servidores

Configuração de Firewall

O firewall deve ser configurado para fazer a normalização de fragmentos de pacote UDP antes de checar as demais regras.

Caso isto não seja possível, uma alternativa é configurar o servidor recursivo para que solicite respostas UDP menores. Se estiver sendo utilizado Bind como servidor recursivo, isto pode ser feito a partir da versão 9.3.0 com as seguintes opções:

```
options {  
    edns-udp-size 1252; # Servidores recursivos  
    max-udp-size 1252; # Servidores recursivos e autoritativos  
};
```

1252 é apenas uma sugestão, este valor deve refletir as configurações de Firewall.

Recomendação

Firewalls e DNS, como e porque configurar corretamente
<ftp://ftp регистрация.br/pub/doc/dns-fw.pdf>

Por que existem dois tipos de chave?

- Permite substituir uma chave de uso frequente (ZSK) sem ter a necessidade de modificar o DS do parent (hash da KSK)
- Permite criar uma chave de tamanho menor para criar assinaturas menores

Key Signing Key (KSK)

As chaves utilizadas para assinar as chaves da zona, sendo, assina apenas os RRsets do tipo DNSKEY

Zone Signing Key (ZSK)

As chaves utilizadas para assinar RRsets da zona sobre o qual tem autoridade



Por que existem dois tipos de chave?

- Permite substituir uma chave de uso frequente (ZSK) sem ter a necessidade de modificar o DS do parent (hash da KSK)
- Permite criar uma chave de tamanho menor para criar assinaturas menores

Key Signing Key (KSK)

As chaves utilizadas para assinar as chaves da zona, sendo, assina apenas os RRsets do tipo DNSKEY

Zone Signing Key (ZSK)

As chaves utilizadas para assinar RRsets da zona sobre o qual tem autoridade

Lembrete

- O record DNSKEY pode armazenar tanto a chave pública de uma KSK quanto de uma ZSK
- O record RRSIG armazena a assinatura de um RRset realizada tanto por uma KSK quanto por uma ZSK

- Introduz um procedimento para mudanças periódicas das chaves KSK e ZSK
- Mantém a estrutura da zona e dos caches consistentes durante o período de mudança de chaves (aguarda os TTLs expirarem)

Cache

- Um cache DNS guarda localmente os resultados das requisições de resolução de nomes para utilização futura, evitando a repetição de pesquisas e aumentando drasticamente a velocidade de resposta
- O cache armazena as informações pelo período de tempo determinado no TTL (Tempo de Vida), que é um valor enviado junto a resposta de cada requisição

TTL

- Quanto maior for seu TTL, mais tempo a determinada informação ficará armazenada em CACHE, sendo interessante apenas para servidores que atualizam pouco sua zona
- Quanto menor for seu TTL, maior será o tráfego de rede, pois os servidores recursivos irão frequentemente requisitar novos dados, sendo interessante apenas para servidores que atualizam sua zona frequentemente

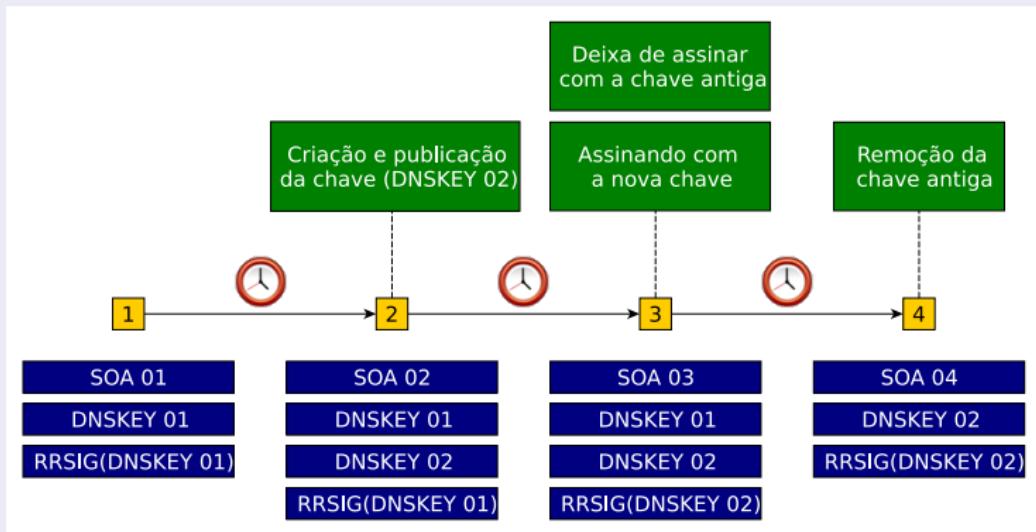
Exemplos de valores para o TTL

- 2 dias para os records do APEX (possuem o nome da zona)
- 6 horas para a record DNSKEY
- 1 dia para os demais records

OBS: O record NSEC possuirá o TTL determinado no record SOA (o record NSEC deve possuir um TTL baixo em razão do cache negativo)

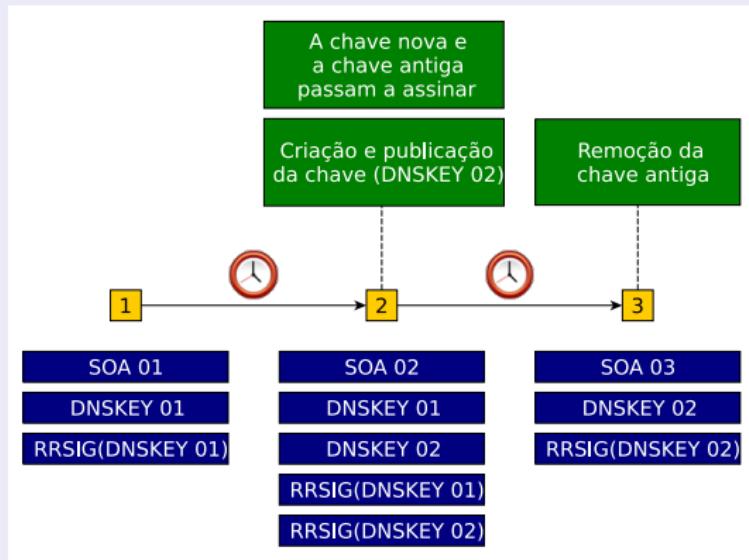
OBS2: O record RRSIG possuirá o mesmo TTL do record que assinou

Pre-Publish (utilizado na ZSK BR)



- 1 – 2 : A mudança da etapa 1 para a etapa 2 pode ser imediata
- 2 – 3 : Tempo de propagação para os servidores autoritativos + TTL do Key Set
- 3 – 4 : Tempo de propagação para os servidores autoritativos + TTL máximo da zona na versão antiga

Double Signing (utilizado na KSK BR)



- 1 – 2 : A mudança da etapa 1 para a etapa 2 pode ser imediata
- 2 – 3 : Tempo de propagação para os servidores autoritativos + TTL máximo da zona na versão antiga

Anúncios de Rollover do BR

Toda vez que ocorrer um processo de substituição da KSK da zona BR será enviado um aviso para as listas:

anuncios-dnssec <https://eng.registro.br/mailman/listinfo/anuncios-dnssec>

GTER <https://eng.registro.br/mailman/listinfo/gter>

GTS-L <https://eng.registro.br/mailman/listinfo/gts-l>

Política de rollover da KSK BR utilizada pelo Registro.br

Substituições programadas da KSK BR são feitas uma vez ao ano. KSKs são válidas por 14 meses e é utilizada a técnica de double-signing. Durante um período de 2 meses existirão duas KSK BR ativas.

– Informações mais atualizadas podem ser encontradas em:

<https://registro.br/info/dnssec-policy.html>

O Registro.br utiliza-se de 3 pares de chaves para assinatura em DNSSEC:

- ① **KSK BR:** Key Signing Key da zona BR. Sua chave privada é utilizada apenas para assinar o conjunto de chaves públicas da zona BR, ou seja, chaves públicas do KSK BR e ZSK BR.
- ② **ZSK BR:** Zone Signing Key da zona BR. Sua chave privada é utilizada para assinar registros da zona BR: conjunto de registros do apex da zona BR e conjunto de registros DS e NSEC.
- ③ **ZSK *.BR:** Zone Signing Key de algumas das zonas abaixo de BR. Sua chave privada é utilizada para assinar registros das zonas assinadas: conjunto de registros do apex destas zonas e conjunto de registros DS e NSEC.

Como o Registro.br tem autoridade sobre o BR e *.BR, não existe necessidade de KSK para *.BR.

O Registro.br utiliza-se de 3 pares de chaves para assinatura em DNSSEC:

- ① **KSK BR:** Key Signing Key da zona BR. Sua chave privada é utilizada apenas para assinar o conjunto de chaves públicas da zona BR, ou seja, chaves públicas do KSK BR e ZSK BR.
- ② **ZSK BR:** Zone Signing Key da zona BR. Sua chave privada é utilizada para assinar registros da zona BR: conjunto de registros do apex da zona BR e conjunto de registros DS e NSEC.
- ③ **ZSK *.BR:** Zone Signing Key de algumas das zonas abaixo de BR. Sua chave privada é utilizada para assinar registros das zonas assinadas: conjunto de registros do apex destas zonas e conjunto de registros DS e NSEC.

Como o Registro.br tem autoridade sobre o BR e *.BR, não existe necessidade de KSK para *.BR.

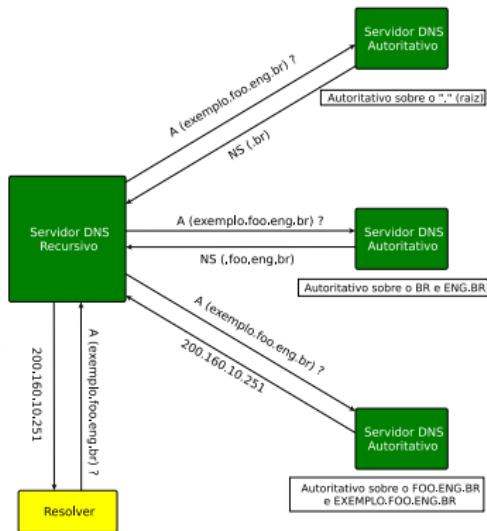
Validade das assinaturas

- Assinaturas geradas com KSKs BR têm validade de 4 meses.
- Assinaturas geradas com ZSKs têm validade de 7 dias.

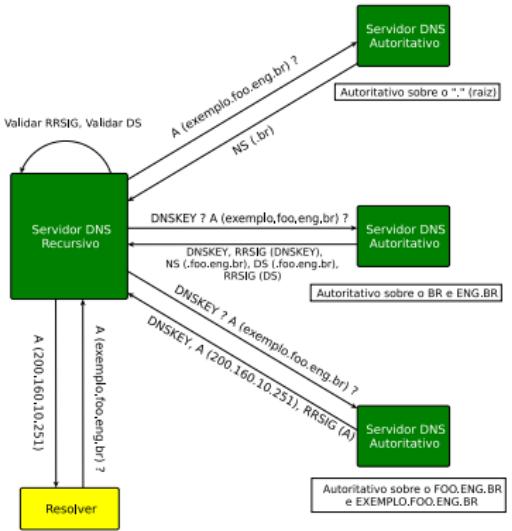
DNS Vs DNSSEC

Diferenças entre uma requisição DNS e uma requisição DNSSEC:

DNS



DNSSEC



8 Pacotes – X Bytes

12 Pacotes \pm 6X Bytes^a

^aDiferença proporcional ao tamanho da chave

Parte II

Utilizando DNSSEC na Prática



	Autoritativo	Recursivo	Caching	DNSSEC ^a	DNSSEC bis ^b	NSEC3 ^c	TSIG	IPv6
ANS	✓			✓	✓		✓	✓
BIND	✓	✓	✓	✓	✓		✓	✓
CNS		✓	✓	✓	✓		✓	✓
djbdns	✓	✓	✓					✓
IPControl	✓	✓	✓	✓	✓		✓	✓
IPM DNS	✓	✓	✓	✓	✓		✓	✓
MaraDNS	✓	✓	✓					?
Microsoft DNS	✓	✓	✓	✓			✓	✓
NSD	✓			✓	✓		✓	✓
PowerDNS	✓	✓	✓					✓
Unbound		✓	✓		✓	✓		✓
VitalQIP	✓	✓	✓	✓	✓		?	✓

^aVersão antiga do protocolo não suportada pelo Registro.br

^bVersão atual do protocolo

^cVersão aprimorada do protocolo DNSSEC também suportada pelo Registro.br

	BSD ^a	Solaris	Linux	Windows	MAC OS X
ANS	√	√	√	?	?
BIND	√	√	√	√	√
CNS	√	√	√	?	?
djbdns	√	√	√		√
IPControl		√	√	√	
IPM DNS	√	√	√		√
MaraDNS	√	√	√	√ ^b	√
Microsoft DNS				√	
NSD	√	√	√		√
PowerDNS	√	√	√	√	√ ^c
Unbound	√	√	√		√
VitalQIP		√	√	√	

^aSistema compatível com a norma POSIX assim como outros clones do Unix.

^bApenas nas versões mais recentes do sistema operacional

^cSoftware em versão Beta

	Criador	Código Aberto	Grátis
ANS	Nominum		
BIND	Internet System Consortium	✓	✓
CNS	Nominum	✓	
djbdns	Daniel J. Bernstein	✓	✓
IPControl	INS		
IPM DNS	EfficientIP		
MaraDNS	Sam Trenholme	✓	✓
Microsoft DNS	Microsoft		
NSD	NLnet Labs	✓	✓
Unbound	NLnet Labs	✓	✓
PowerDNS	PowerDNS.com / Bert Hubert	✓	✓
VitalQIP	Lucent Technologies		

DIG (Domain Information Groper)

Uma ferramenta para consultas sobre registros DNS

- para validação da cadeia de confiança é necessário compilar com a opção **sigchase** habilitada

DRILL

Uma ferramenta similar ao DIG com suporte nativo a DNSSEC

- até a versão 1.2.0 da Idns o DRILL não tinha suporte a validação de Records

CNAME

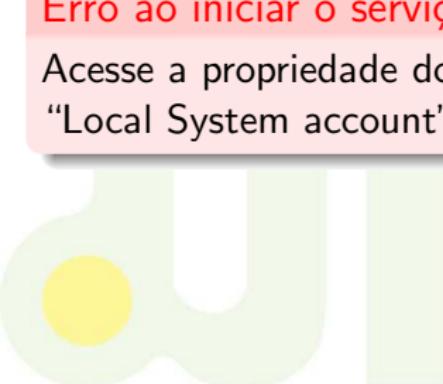


BIND no Windows

- Faça o download da última versão do BIND em <http://www.isc.org>
- Descompacte o arquivo ZIP e execute o programa BINDInstall.exe
- Após a instalação, acesse os Serviços (ferramentas administrativas) e inicie o serviço “ISC BIND”

Erro ao iniciar o serviço ISC BIND

Acesse a propriedade do serviço, e na aba “Log On” selecione a opção “Local System account”



BIND no Windows

O BIND no Windows funciona da mesma forma que no Linux, sendo que os arquivos ficam localizados em locais diferentes.

- Os arquivos de configuração estão localizados em c:\windows\system32\dns\etc
- Os executáveis (named, dig) estão localizados em c:\windows\system32\dns\bin

The image consists of three side-by-side screenshots of a Windows Command Prompt window. The first screenshot shows the configuration file named named.conf with options for a directory, port, and zone "foo.eng.br". The second screenshot shows the named process running with PID 28871114122149 and a query for "foo.eng.br.". The third screenshot shows the named process again with PID 28871114122149 and a query for "ns1.foo.eng.br.".

```
File Edit Search View Options Help
File Edit Search View Options Help
File Edit Search View Options Help
C:\Windows\system32\dns\etc\named.conf
options {
    directory "c:\windows\system32\dns\etc";
    port 53;
    listen-on { 127.0.0.1; };
    edns-udp-size 800; # Recursive
    max-udp-size 800; # Authoritative / Recursive
};

zone "foo.eng.br" {
    type master;
    file "c:\windows\system32\dns\etc\db.foo.signed";
};

C:\Windows\system32\dns\bin>dig foo.eng.br +dnssec
;; <> SIG 9.4.1-P1 <> foo.eng.br +dnssec
;; global options: printcmd
;; options: +nocmd +noverbose
;; +NODNSSEC<+ opcode: QUERY, status: NOERROR, id: 634
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
;;      flags: qr rd ra; QUERY: 0, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;foo.eng.br.           IN  A
;; ANSWER SECTION:
foo.eng.br.         900  IN  A   200.168.10.254
;; AUTHORITY SECTION:
foo.eng.br.         900  IN  NS  ns1.foo.eng.br.
;; ADDITIONAL SECTION:
ns1.foo.eng.br.     900  IN  A   200.168.10.254
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Oct 23 09:49:04 2007
;; MSG SIZE rcvd: 599
C:\Windows\system32\dns\bin>

C:\Windows\system32\dns\bin>dig db.foo
File Edit Search View Options Help
File Edit Search View Options Help
File Edit Search View Options Help
C:\Windows\system32\dns\etc\db.foo
ns1.foo.eng.br. 900 IN NS ns1.foo.eng.br.
ns1.foo.eng.br. 900 IN A 200.168.10.254
ns1.foo.eng.br. 900 IN A 200.168.10.251
include "foo.eng.br.+000+21822.key"
include "foo.eng.br.+000+63842.key"
Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Oct 23 09:49:04 2007
;; MSG SIZE rcvd: 599
C:\Windows\system32\dns\bin>
```

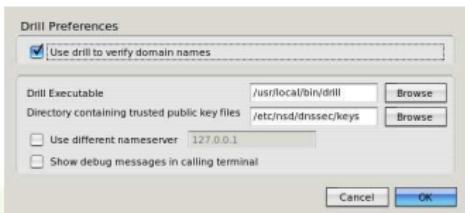
Drill Extension - Firefox Plugin

Plugin para o navegador Firefox que permite validar a cadeia de confiança caso o domínio esteja com DNSSEC habilitado

– http://www.nlnetlabs.nl/dnssec/drill_extension.html

The screenshot shows the official website of the Comitê Gestor da Internet no Brasil (NIC.br). The top navigation bar includes links to NIC.br, CETIC.br, Antispam.br, and PTT.br. The main content area features several sections: 'Destaque' (with a link to 'Pesquisa sobre o Uso das TICs no Brasil 2006'), 'Destaque' (with a link to 'Conheça o CETIC.br'), 'Indicadores' (with a link to '66,68% da população brasileira nunca usou a Internet.'), 'Notícias' (with articles about 'Crime virtual, castigo real?' and 'Internet neutra e sem amarras jurídicas.'), and 'Participe da campanha' (with a link to 'antispam.br'). On the right side, there are columns for 'Imprensa' (Press) and 'FAQ do CGI.br' (Frequently Asked Questions). A large sidebar on the right contains links to 'nic.br' (Núcleo de Informação e Coordenação), 'egi.br' (Comitê Gestor da Internet no Brasil), 'registro.br' (Registro de Domínios para a Internet no Brasil), 'cert.br' (Centro de Certificação e Verificação de Infraestrutura), and 'cetic.br' (Centro de Estudos sobre as Tecnologias da Informação e da Comunicação). At the bottom right, there is a red box highlighting the 'DNS SEC' logo and a red arrow pointing to the 'Valido - XHTML - CSS' and 'Valido - CSS' links.

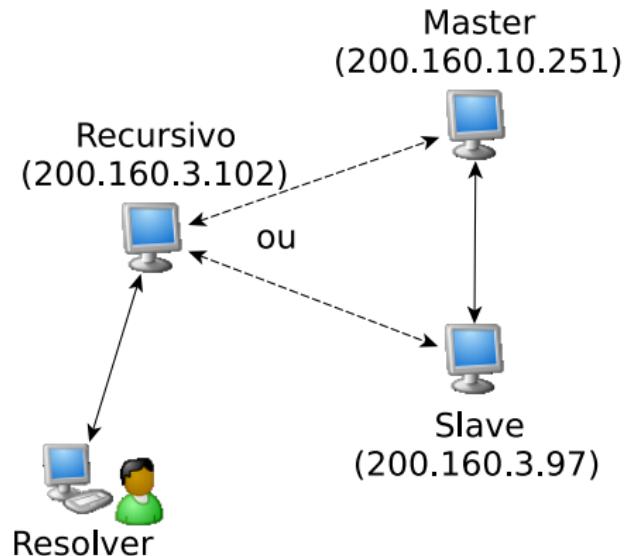
Após instalar o plugin, altere em suas configurações a localização das "trusted-keys" em seu computador.



No diretório das "trusted-keys", cada arquivo existente (o nome é indiferente) deve possuir uma chave no seguinte formato:

```
br. IN DNSKEY 257 3 5
AwEAAcmqkFULGgm1V1BbUYQEuCzSbEBYjAcNInY9gxftbTK+CSYwlGAfxl5hwx7kx0QAZ2ZMLrxD+sTQVC4StoAPPcUhFqEG0V+9G
I6SsD/fikQO IhxA s6INKkOP0kfBqotk6C5QbbVXcsML54/dtZYWi/Z7CaG2Hz93ouyUMQzIPohER+gkbFYq3ewDajqJKNsVm8caT
9/mkNw+CQHR+QNmWM=
```

- ① Configuração BIND
 - a Arquivo de zona
 - b named.conf
- ② Teste – Consulta de Record
- ③ Registro de domínio – atualização dos nameservers
- ④ Aguardar nova publicação
- ⑤ Configuração DNSSEC no BIND
 - a Geração da chave ZSK
 - b Geração da chave KSK
 - c Atualização do arquivo de zona
 - d Assinatura da zona
 - e Atualização do named.conf
- ⑥ Teste – Consulta de Record com DNSSEC
- ⑦ Atualização do Record DS no cadastro do domínio
- ⑧ Aguardando nova publicação
- ⑨ Teste – Validação da cadeia de confiança



Arquivo db.foo

```
foo.eng.br. IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
    1           ; serial
    3600        ; refresh
    3600        ; retry
    3600        ; expire
    900 )       ; TTL
foo.eng.br. IN NS ns1.foo.eng.br.
foo.eng.br. IN NS ns2.foo.eng.br.
exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br.
exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br.
ns1.foo.eng.br. IN A 200.160.3.97
ns2.foo.eng.br. IN A 200.160.10.251
ns1.exemplo.foo.eng.br. IN A 200.160.3.97
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
```

Arquivo db.exemplo.foo

```
exemplo.foo.eng.br. IN SOA ns.exemplo.foo.eng.br. hostmaster.exemplo.foo.eng.br. (
    1           ; serial
    3600        ; refresh
    3600        ; retry
    3600        ; expire
    900 )       ; TTL
exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br.
exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br.
ns1.exemplo.foo.eng.br. IN A 200.160.3.97
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
```

named.conf (master)

```
options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    dump-file "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";
    listen-on { 200.160.10.251; };
};

zone "foo.eng.br" {
    type master;
    file "/etc/namedb/db.foo";
    allow-transfer {
        200.160.3.97;
    };
};

zone "exemplo.foo.eng.br" {
    type master;
    file "/etc/namedb/db.exemplo.foo";
    allow-transfer {
        200.160.3.97;
    };
};
```

named.conf (slave)

```
options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    dump-file "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";
    listen-on { 200.160.3.97; };
};

zone "foo.eng.br" {
    type slave;
    file "/etc/namedb/db.foo";
    masters {
        200.160.10.251;
    };
};

zone "exemplo.foo.eng.br" {
    type slave;
    file "/etc/namedb/db.exemplo.foo";
    masters {
        200.160.10.251;
    };
};
```

Zona foo.eng.br

```
dig @200.160.10.251 foo.eng.br soa +noadditional +multiline
; <>> DiG 9.3.3 <>> @200.160.10.251 foo.eng.br soa +noadditional +multiline
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40573
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;foo.eng.br.           IN SOA
;; ANSWER SECTION:
foo.eng.br.          900 IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
                      1           ; serial
                      3600        ; refresh (1 hour)
                      3600        ; retry (1 hour)
                      3600        ; expire (1 hour)
                      900         ; TTL (15 minutes)
)
;; AUTHORITY SECTION:
foo.eng.br.          900 IN NS ns1.foo.eng.br.
foo.eng.br.          900 IN NS ns2.foo.eng.br.
;; Query time: 1 msec
;; SERVER: 200.160.10.251#53(200.160.10.251)
;; WHEN: Wed May 23 16:05:56 2007
;; MSG SIZE  rcvd: 143
```

Zona exemplo.foo.eng.br

```
dig @200.160.10.251 exemplo.foo.eng.br soa +noadditional +multiline
; <>> DiG 9.3.3 <>> @200.160.10.251 exemplo.foo.eng.br soa +noadditional +multiline
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63826
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;exemplo.foo.eng.br.      IN SOA
;; ANSWER SECTION:
exemplo.foo.eng.br.    900 IN SOA ns.exemplo.foo.eng.br. hostmaster.exemplo.foo.eng.br. (
                           1           ; serial
                           3600        ; refresh (1 hour)
                           3600        ; retry (1 hour)
                           3600        ; expire (1 hour)
                           900         ; TTL (15 minutes)
)
;; AUTHORITY SECTION:
exemplo.foo.eng.br.    900 IN NS ns2.exemplo.foo.eng.br.
exemplo.foo.eng.br.    900 IN NS ns1.exemplo.foo.eng.br.
;; Query time: 2 msec
;; SERVER: 200.160.10.251#53(200.160.10.251)
;; WHEN: Wed May 23 16:10:58 2007
;; MSG SIZE  rcvd: 154
```

Registro de domínios

registro.br

Registro de Domínios
para a Internet no Brasil

The screenshot shows the main dashboard of the registro.br domain registration system. At the top, there's a navigation bar with links like 'Elle', 'Edit', 'View', 'History', 'Bookmarks', 'Tools', and 'Help'. Below the navigation is a header bar with the text 'Núcleo de Informação e Coordenação do Ponto br' and a menu with links: 'Home', 'Registro', 'Info', 'FAQ', 'Pesquisas', 'Estatísticas', 'Mapa', and 'Contato'. A central callout box contains links: 'Alterar Cadastro do ID [RAJUS]', 'Fechar Sessão', 'Novos Domínios : Institucional [Profissional Liberal]', 'Pessoa Física', 'Sistema de IPs', 'Cancelar domínio', and 'Tickets Processados'. To the right, there's a sidebar titled 'Piloto EPP' with the 'registro.br' logo and the text 'Registro de Domínios para a Internet no Brasil'. On the far right, there's a timestamp 'Id: RAJUS 24/05/2007 17:57:12'. Below the main content area, there are two tables: one for 'Entidades' and another for 'Administrativo', 'Técnico', and 'Cobrança'.

Administrativo	Técnico	Cobrança

Entidades		

[n] Novo [o] Expirando [!] Expirado [x] Congelado

egi.br

nic.br

Registro de domínios

registro.br
Registro de Domínios
para a Internet no Brasil

File Edit View History Bookmarks Tools Help

Núcleo de Informação e Coordenação do Ponto br

Home Registro Info FAQ Pesquisas Estatísticas Mapa Contato

Tela Principal

Novo Domínio PL

Domínio eng.br ▾

Informações do Profissional Liberal

CPF **CHECAR**

Nome

CEP **CHECAR**

Endereço

Número Complemento

Cidade UF

DDD Tel. Ramal

Informações sobre os Contatos

Id Administrativo	RAJUS	PESQUISAR
Id Técnico	RAJUS	PESQUISAR
Id Cobrança	RAJUS	PESQUISAR

Piloto EPP
registro.br
Registro de Domínios
para a Internet no Brasil

Id: RAJUS
22/05/2007 10:53:43

nic
br

Delegações DNS

File Edit View History Bookmarks Tools Help

Delegações DNS

(Instruções para o preenchimento dos campos IP e IPv6. [Clique aqui.](#))

Servidor Master

Nome

Endereço IP

Endereço IPv6 (opcional)

Servidor Slave 1

Nome

Endereço IP

Endereço IPv6 (opcional)

Após estes procedimentos é necessário aguardar uma nova publicação

BIND: dnssec-keygen

Zona foo.eng.br:

```
dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE foo.eng.br
```

Zona exemplo.foo.eng.br:

```
dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE exemplo.foo.eng.br
```

Onde,

- -f : Define o tipo da chave
- -a : Algoritmo
- -b : Tamanho da chave (bits)
- -n : Especifica o tipo de dono da chave
- -r : Device de randomização

Em determinados ambientes, onde a geração de chaves demorar muito pode ser necessário especificar o device de randomização, como por exemplo: “-r /dev/urandom”

OBS1: Guardar o nome das chaves geradas relacionando qual é KSK e qual é ZSK para ser usado futuramente.

OBS2: Chaves geradas com dnssec-keygen não possuem passphrase.

Exemplo de Tamanho de chaves

- KSK BR: 1280 bits

BIND: dnssec-keygen

Zona foo.eng.br:

```
dnssec-keygen -a RSASHA1 -b 1024 -n ZONE foo.eng.br
```

Zona exemplo.foo.eng.br:

```
dnssec-keygen -a RSASHA1 -b 1024 -n ZONE exemplo.foo.eng.br
```

Onde,

- -a : Algoritmo
- -b : Tamanho da chave (bits)
- -n : Tipo de chave
- -r : Device de randomização

Em determinados ambientes, onde a geração de chaves demorar muito pode ser necessário especificar o device de randomização, como por exemplo: “-r /dev/urandom”

OBS1: Guardar o nome das chaves geradas relacionando qual é KSK e qual é ZSK para ser usado futuramente.

OBS2: Chaves geradas com dnssec-keygen não possuem passphrase.

Exemplo de Tamanho de chaves

- KSK BR: 1280 bits
- ZSK BR: 1152 bits
- ZSK *.BR: 1024 bits

Arquivo db.foo

```
foo.eng.br. IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
    2          ; serial
    3600       ; refresh
    3600       ; retry
    3600       ; expire
    900 )      ; TTL
foo.eng.br. IN NS ns1.foo.eng.br.
foo.eng.br. IN NS ns2.foo.eng.br.
exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br.
exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br.
ns1.foo.eng.br. IN A 200.160.3.97
ns2.foo.eng.br. IN A 200.160.10.251
ns1.exemplo.foo.eng.br. IN A 200.160.3.97
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
$include Kfoo.eng.br.+005+62745.key
$include Kfoo.eng.br.+005+00817.key
```

OBS

O serial deve ser incrementado todas as vezes em que o arquivo de zona for modificado

Arquivo db.exemplo.foo

```
 exemplo.foo.eng.br. IN SOA ns.exemplo.foo.eng.br.  
hostmaster.exemplo.foo.eng.br. (  
          2           ; serial  
        3600         ; refresh  
        3600         ; retry  
        3600         ; expire  
       900 )       ; TTL  
 exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br.  
 exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br.  
 ns1.exemplo.foo.eng.br. IN A 200.160.3.97  
 ns2.exemplo.foo.eng.br. IN A 200.160.10.251  
$include Kexemplo.foo.eng.br.+005+11970.key  
$include Kexemplo.foo.eng.br.+005+03112.key
```

OBS

O serial deve ser incrementado todas as vezes em que o arquivo de zona for modificado

Ao se assinar a zona são gerados os records RRSIG e NSEC que ficarão ordenados de forma canônica dentro do arquivo de zona

BIND: dnssec-signzone

Zona `foo.eng.br`:

```
$ dnssec-signzone -o foo.eng.br db.foo
```

Zona `exemplo.foo.eng.br`:

```
$ dnssec-signzone -o exemplo.foo.eng.br db.exemplo.foo
```

Onde,

- `-o` : Nome da zona
- `-e` : Data de expiração das assinaturas (formato AAAAMMDDHHMMSS) -
Se não informado é considerado 30 dias
- o último parâmetro se refere ao *arquivo de zona*

Geração de records DS

No momento em que se assina uma zona é gerado um arquivo contendo o Records DS que sera utilizado para as delegações.

– o arquivo gerado neste exemplo: `dsset-foo.eng.br`.

Inclusão do DS da delegação

O DS contido no arquivo dsset-exemplo.foo.eng.br. deverá ser adicionado no arquivo db.foo de forma a continuar a cadeia de confiança entre o domínio (foo.eng.br) e suas delegações (exemplo.foo.eng.br)

SHA1 exemplo.foo.eng.br. IN DS 3112 5 1 386B4390C5B30DB65D74EA8B660978077171948C

SHA256 exemplo.foo.eng.br. IN DS 3112 5 2 19602F6089F8877E037AA077B8376F30869E261EB55460F2A74E32AD1424F53A

```
foo.eng.br IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
    3           ; serial
    3600        ; refresh (1 hour)
    3600        ; retry (1 hour)
    3600        ; expire (1 hour)
    900         ; TTL (15 minutes)
)
NS ns1.foo.eng.br.
NS ns2.foo.eng.br.
...
exemplo.foo.eng.br. IN DS 3112 5 1 386B4390C5B30DB65D74EA8B660978077171948C
```

OBS

A zona foo.eng.br deve ser re-assinada após incluir o record DS na zona

Necessário atualizar no Master e no Slave

Habilitar a opção de DNSSEC

```
options {  
    directory "/etc/namedb";  
    pid-file "/var/run/named/pid";  
    dump-file "/var/dump/named_dump.db";  
    statistics-file "/var/stats/named.stats";  
    dnssec-enable yes; # somente BIND 9.3  
    listen-on { 200.160.3.97; };  
};
```



Necessário atualizar no Master

Alteração da referência para o arquivo de zona

```
zone "foo.eng.br" {  
    type master;  
    file "/etc/namedb/db.foo.signed";  
    allow-transfer {  
        200.160.3.97;  
    };  
};  
zone "exemplo.foo.eng.br" {  
    type master;  
    file "/etc/namedb/db.exemplo.foo.signed";  
    allow-transfer {  
        200.160.3.97;  
    };  
};
```

Obtendo a KSK a ser ancorada

- .BR <https://registro.br/ksk/>
- DLV <https://secure.isc.org/index.pl?/ops/dlv/index.php>

- ➊ Instalar o BIND, mantendo as configurações padrão
- ➋ No arquivo named.conf, definir “dnssec-enable yes” (somente BIND 9.3) e “dnssec-validation yes” (BIND 9.4 ou superior) nas opções
- ➌ Obtenha a chave pública KSK da zona br
- ➍ Inserir a chave pública no bloco denominado “trusted-keys” no arquivo named.conf

Exemplo de inclusão de uma “Trusted Key”

```
options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    dump-file "/var/dump/named.dump.db";
    statistics-file "/var/stats/named.stats";
    dnssec-enable yes; # somente BIND 9.3
    dnssec-validation yes; # BIND 9.4 ou superior
    listen-on { 200.160.3.102; };
};

trusted-keys {
    br.          257 3 5
        "AwEAAa290pX9aaNf053wZdk0GKmNCbLlbyCo1yNrwDiv
         fgyBcdI+cjtVvSEmzh6HoY+1QejKJDpbJF1/G9Zba/Aw
         rKCpahLFDz5SaZiP0sStuWg8UzWz8b5J5t2dlxsu6PeF
         dU08fkItt1FDEGCxsy3IR+eYJGdK0jowuDySoiQ8Uj/+_
         3ZHM4I4z2g0zEwb8uI3Jntmj5azop4B2o1WDNV1VdPJ1
         96TvMy5ImGsBkn03y3FUrQpynQn8M2x5pztuGE0g8KPZ
         Yp/VUp0VOHyqTjSPsM+mCT2x80xN5SghaMeby85u5fVs
         0Eks3T6fN27nFxrdnMvcnNlslwQvbxBWSwTNVeU=";
};

...
```

- ① Obtenha a chave pública do DLV em
<https://secure.isc.org/ops/dlv/dlv.isc.org.named.conf>
- ② Inclua a chave pública no bloco trusted-keys no arquivo named.conf
- ③ Habilite a opção “dnssec-lookaside . trust-anchor dlv.isc.org.;” no bloco options do arquivo named.conf

Exemplo de inclusão de uma chave DLV

```
options {  
    ...  
    dnssec-enable yes; # somente BIND 9.3  
    dnssec-validation yes; # BIND 9.4 ou superior  
    dnssec-lookaside . trust-anchor dlv.isc.org.;  
};  
trusted-keys {  
    ...  
    dlv.isc.org. 257 3 5  
        "AwEAAcPs1nnfJ4L5JdpZwfxER4FKf+hZMLsIhrLLZl721TrhPAySLykj  
        LBTA8SQHnZIumarRIskXnFRDRif3TcRPuo8mhkWlMv+JsihcK9KqHfL  
        sNEIRToWOnFctS/eoLiFQDl1zQUuSMMFt1fS3nDqSrf5l7H4omZsIkG9  
        zAAkTB1X";  
};  
...
```

Zona foo.eng.br

```
dig @200.160.10.251 foo.eng.br soa +dnssec +noadditional +multiline
;; ANSWER SECTION:
foo.eng.br.      900 IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
                  3           ; serial
                  3600        ; refresh (1 hour)
                  3600        ; retry (1 hour)
                  3600        ; expire (1 hour)
                  900         ; TTL (15 minutes)
)
foo.eng.br.      900 IN RRSIG SOA 5 3 900 20070617200428 (
                  20070518200428 62745 foo.eng.br.
                  g1EeCYyd/CCBfzH64y0RAQf90xYDsI4xuBNaam+8DZQZ
                  xeoSLQEETwmp6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE
                  1LLgLI+BLwdlz0t8MypcpL0aTm9rc7pP7UR5XLzU1k8D
                  m6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCuja= )
;; AUTHORITY SECTION:
foo.eng.br.      900 IN NS ns2.foo.eng.br.
foo.eng.br.      900 IN NS ns1.foo.eng.br.
foo.eng.br.      900 IN RRSIG NS 5 3 900 20070617200428 (
                  20070518200428 62745 foo.eng.br.
                  3iLm1ROC+UeqYk0xgQQQQXkBzcKiKQRPwe+1JZlpjEzj
                  U1UjOHUOHeFajXzMv7F1FMWYeU51Ybg49HFe67XQV1K5
                  4GeAFXWB7YS59y0DL0NEBxQl9QEY6g/00nLpuKTrST8q
                  qd5Fc/eYqN/Ag3GnfcAviZgiQhhveGH9mJHWZyc= )
```

Teste - Consulta de record com DNSSEC

Zona exemplo.foo.eng.br

```
dig @200.160.10.251 exemplo.foo.eng.br soa +dnssec +noadditional +multiline
;; ANSWER SECTION:
exemplo.foo.eng.br.    900 IN SOA ns.exemplo.foo.eng.br. hostmaster.exemplo.foo.eng.br. (
                          2           ; serial
                          3600        ; refresh (1 hour)
                          3600        ; retry (1 hour)
                          3600        ; expire (1 hour)
                          900         ; TTL (15 minutes)
)
exemplo.foo.eng.br.    900 IN RRSIG SOA 5 4 900 20070617184743 (
                          20070518184743 11970 exemplo.foo.eng.br.
                          QAPzSENr7i17xRkJ6vL1BunpSzDoVY+naC0wv9kRUB9s
                          yPqKx3RrKi/+u0sJYAUG3CDjFzggQ93yu7VFg6oIb0lD
                          cFV22vYbz5/ykx+LOHrgyszItPRH4Cf0SbQG1wXczPr2
                          FmeYj5AlwdcjqkTLCf0Ef/o0ylnp6x+2F/BSKiU= )
;; AUTHORITY SECTION:
exemplo.foo.eng.br.    900 IN NS ns1.exemplo.foo.eng.br.
exemplo.foo.eng.br.    900 IN NS ns2.exemplo.foo.eng.br.
exemplo.foo.eng.br.    900 IN RRSIG NS 5 4 900 20070617184743 (
                          20070518184743 11970 exemplo.foo.eng.br.
                          t7a3FEqAIW/roFQERDYyR+V6qT17erabiAtsLg0JQkw3
                          AEBQ9tS1dvdpZq29uIn2cpqbuj+DNPagubHO+C+tiTQ
                          o3IZj+sb8DNWb2zrTuo0YT96eCehX20Dq4tLliHpCcyyq
                          UANY/+KkJp+yAxgVRzByIfXFFHZwqysUYr+WI+I= )
```



Os campos abaixo devem ser preenchidos utilizando somente caracteres ASCII [a-zA-Z0-9-].

Domínio

camargo.eng.br

Servidor DNS (nome ou IP)

200.160.10.211

PESQUISAR **LIMPAR**

Records DS das chaves encontradas:

Key Tag **Algoritmo** **Digest DS**

51087 RSA/SHA1 5533CC7E64D1B412C273AFE5842DB5FA0C9361C2

egi.br

- Calcula o record DS a partir da DNSKEY
- Útil para validar um DS gerado por software de terceiros

Atualização do registro de domínios incluindo o DS

Apartir do arquivo dsset-foo.eng.br.

Records DS (preenchimento opcional)

Record DS 1

Key Tag

 Algoritmo RSA/SHA-1

foo.eng.br.

IN DS 817 5 1

EAEC29E4B0958D4D3DFD
90CC70C6730AD5880DD3

Record DS 2

2

Key Tag

 Algoritmo RSA/SHA-1

Digest

ENTRAR **LIMPAR**

O número após o Key Tag no Record se refere ao Algoritmo da chave (RFC 4034 - A.1)

- 3 DSA/SHA-1
- 5 RSA/SHA-1

Após estes procedimentos é necessário aguardar uma nova publicação

DIG - Sigchase

- O sigchase é uma opção no DIG que permite realizar uma verificação em toda a estrutura desde o ponto assinado até o domínio fornecido
- Útil na verificação da validade nas assinaturas e chaves das zonas
- Para utilizar DIG +sigchase, é necessário instalar a biblioteca de desenvolvimento do OPENSSL^a, compilar o BIND 9.4 com a variável de ambiente “STD_CDEFINES” definida com o valor “-DDIG_SIGCHASE=1” e rodar o comando “configure” com o parametro “–with-openssl”

^aNo Ubuntu o pacote se chama libssl-dev

Ancorando chave para o DIG +sigchase

- ① Obter a chave pública da KSK da “.br” fornecida pelo Registro.br
- ② Copiar a chave no arquivo /etc/trusted-key.key
não deixar nenhuma quebra de linha dentro da chave
não deixar nenhuma linha em branco após a chave

Teste - Validação da cadeia de confiança

Exemplo

```
dig @200.160.3.69 exemplo.foo.eng.br soa +sigchase +multiline
;; RRset to chase:
eng.br.          172800 IN SOA a.dns.br. hostmaster.registro.br. (
                  2007033785 ; serial
                  1800       ; refresh (30 minutes)
                  900        ; retry (15 minutes)
                  604800    ; expire (1 week)
                  900        ; TTL (15 minutes)
)
;; RRSIG of the RRset to chase:
eng.br.          172800 IN RRSIG SOA 5 2 172800 20070531204953 (
                  20070528174953 32986 eng.br.
                  ED6Xp/67/i6n7XhjEA4AmzmoWAPWgJLescK9UIu2bkqH
                  RKJS/gDa9voLjfDHnwjnHViq6aXt2AIi4Zj5T/I+5+mB
                  BDWEnuOpG9a4A7v4jAUTT78c5jlkRh2BvLw4QZdiEbuH
                  253Yq1xRUZCta37Qm4IKRgN40osNMRTfBy/BuXY= )
Launch a query to find a RRset of type DNSKEY for zone: eng.br.
;; DNSKEYset that signs the RRset to chase:
eng.br.          21600 IN DNSKEY 257 3 5 (
                  AWEAAbAgpvVTb3Pn70j7JDvfCZQLtyRDoJdo6G2mBeuM
                  fZXXx+Cj0qIhkZZ1zDTh3KyJ1Rb11WuD6+EEXey4LQm
                  qET3B7yUqrOCeSfCzHeeYYzYNRgIhKvinbWqJ21e5SMg
                  HxbASmezNm/rQmQHkYqLaDt9zw/rrwMSVyeH5DEEQc/P
) ; key id = 32986
```

Exemplo (Continuação)

```
;; RRSIG of the DNSKEYset that signs the RRset to chase:  
eng.br.          21600 IN RRSIG DNSKEY 5 2 21600 20070531204953 (  
                           20070528174953 32986 eng.br.  
                           nVf9AmuMrM WLpWl0R6I38pjXRkaE/9bYJrdvEAbSLPDD  
                           7kVyHexcis79EGp/GUgwG6/0towLvzW1y8PfqcbbgQhK  
                           5hjyH+ngKwBQUkGAjVw3Ysg19kJcKAfU042zhIe//xSY  
                           y3W+j87FmA67nwVyCqtz+cwmWPvsuqe60QwN1D8= )
```

Launch a query to find a RRset of type DS for zone: eng.br.

```
;; DSset of the DNSKEYset  
eng.br.          86400 IN DS 32986 5 1 (  
                           6E4CF7F759FD FE1F08E658AC505BC53BFD07915E )
```

```
;; RRSIG of the DSset of the DNSKEYset  
eng.br.          86400 IN RRSIG DS 5 2 86400 20070531204953 (   
                           20070528174953 60165 br.  
                           eT6fMTSGksBuags wjDfBI/YAegN+s6Xmfb3Awwe1AgrS  
                           dUFOvlcLU6pkvwgFROfDnj b7oU1kW2p3S5vEVuEu3LN8  
                           1YfswjmW7MMw68X44jY1xtsYkC5s00exxksrGCIRg+Vi  
                           Ah7fMy1EIIybaAjqILq/i00pqqueenJXjpI7iHVI= )
```

Exemplo (Continuação)

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING SOA RRset for eng.br. with DNSKEY:32986: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Now, we are going to validate this DNSKEY by the DS
;; OK a DS valids a DNSKEY in the RRset
;; Now verify that this DNSKEY validates the DNSKEY RRset
;; VERIFYING DNSKEY RRset for eng.br. with DNSKEY:32986: success
;; OK this DNSKEY (validated by the DS) validates the RRset of the DNSKEYs, thus the DNSKEY validates the
RRset
;; Now, we want to validate the DS : recursive call
Launch a query to find a RRset of type DNSKEY for zone: br.
;; DNSKEYset that signs the RRset to chase:
br.          21600 IN DNSKEY 257 3 5 (
    AwEAAaeACjj1oWq1bzK3eFIHyqKCMrJ+cCKbBpJ2X8Dx
    nu8PknEbsxgJaSXT5SeUphXGCTMgxYbwu6fefA7cS100
    zfkg9Mq3HMaxXgKCZdhy+GOL9xVFTD0hZm+8dUNG2LQG
    YCeqghu861S2GSoB6gCG5HN3p1R7K8gKSqj8JGsRp1Qu
    hPye+WGeY1Cnm5gm+ghz/3Jz1GA0mf3DSU8hI9j88tnp
    hMRqUpRbEJPZQYD01EJ19CCRF0/kKnZyYgB8gh1IHr10
    vRIhxN77ztjJi7PWgk6Jq/pL4eH6hcHwIs2JPR3m+pts
    nav7UlMt2kiFD4IN2rcdD+eoVLAzvzpvzeThC8M=
) ; key id = 1657
21600 IN DNSKEY 256 3 5 (
    AwEAAaeH0t8VKghhsM1W1ps0XLkS4xrYVfPUvx03av2tI
    sTSDxr5j23C+Zs4AwdxAO6WkuUs3ik8oI3kBTNq5fUVf
    jZkpoCkfGmxiviOoT3jejVRDHQeriCVRZAbry2JnAkVq
    2+c1ajc1Hr6/kn0z6hzv9p5JpLdfa454jBT7jh681j7L
) ; key id = 60165
```

Exemplo (Continuação)

```
; ; RRSIG of the DNSKEYset that signs the RRset to chase:  
br.          3600 IN RRSIG DNSKEY 5 1 21600 20070531204953 (   
                20070528174953 60165 br.  
                uF1LQOCYses5zHa0Ze33zwd6j1Kkkm74NJ6hyWky16Ic  
                TEZiJKucbHd9U+8K6zUxskrA77Vx6r0D0u7cmUSnxjDz  
                uPr2f2VJcTAW5nHrEk3u/8DU3gkyYdAIYu22KvGo+s4i  
                dEWssbiXOOQjvABDDXV3UyAJsNkakvIHAj0iEyA= )  
            3600 IN RRSIG DNSKEY 5 1 3600 20080101120000 (   
                20070101000000 1657 br.  
                f1kMiXop002+y1j5gxsbFKXgi1pB90t2Fmj7oXuJ5vBE  
                eb+1vy+qV03GbR29FIRMKbX7fWT7qCVISSN87bDNr/UJ  
                4hNRZ57q8tmX1S/1oSJjhqHcWYAgurFApiRsywLKUtws  
                ZpkEW69BNWVu4UVVqPIJdw1CcNy2MDVVKjzwXGaAp/Q  
                H2D+LM0sPpnRQFJua3rhynatsySJLvo1j3lw16oV1xDc  
                q7wAMTvklTck8LRfNy6SWEvC4m++uPdwWPLZvSMBGMYh  
                wMY91/1eVz7sWQ+ThCcpLt17niCdSiqyMIPczi0jLB0m  
                jD/D00zSscqp3UNdILCIqGo2mBjgLeARxQ== )
```

Launch a query to find a RRset of type DS for zone: br.

```
; ; NO ANSWERS: no more  
; ; WARNING There is no DS for the zone: br.  
; ; WE HAVE MATERIAL, WE NOW DO VALIDATION  
; ; VERIFYING DS RRset for eng.br. with DNSKEY:60165: success  
; ; OK We found DNSKEY (or more) to validate the RRset  
; ; Ok, find a Trusted Key in the DNSKEY RRset: 1657  
; ; VERIFYING DNSKEY RRset for br. with DNSKEY:1657: success  
; ; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS
```

- 1 Verificar a disponibilidade do domínio junto ao registro.br
- 2 Instalar BIND
- 3 Configurar um arquivo de zona no servidor Master
- 4 Configurar o arquivo named.conf no servidor Master
- 5 Configurar o arquivo named.conf no servidor Slave
- 6 Executar o BIND (named) no servidor Master
- 7 Executar o BIND (named) no servidor Slave
- 8 Registrar o domínio no Registro.br
- 9 Aguardar nova publicação
- 10 Realizar testes no servidor (DIG)

- 11 Criar chave KSK (dnssec-keygen) (slide 109)
- 12 Criar chave ZSK (dnssec-keygen) (slide 110)
- 13 Incluir as chaves geradas no arquivo de zona do servidor Master (slide 111)
- 14 Assinar a zona (dnssec-signzone) (slide 113)
- 15 Se existir delegações assinadas, incluir no arquivo de zona o DS de cada delegação e reassinar a mesma (slide 114)
- 16 Atualizar o named.conf do servidor Master de forma a utilizar o arquivo de zona .signed e habilitar DNSSEC-ENABLE (slide 116)
- 17 Atualizar o named.conf do servidor Slave habilitando DNSSEC-ENABLE (slide 115)
- 18 Restartar o BIND (named) no servidor Master
- 19 Restartar o BIND (named) no servidor Slave
- 20 Adicionar na interface de provisionamento o DS (localizado no arquivo dsset*) (slide 123)
- 21 Aguardar nova publicação

- 1 Instalar biblioteca de desenvolvimento do OpenSSL
- 2 Instalar BIND
- 3 Obter a trusted-key do site do Registro.br (slide 117)
- 4 Configurar o arquivo named.conf habilitando DNSSEC-ENABLE e DNSSEC-VALIDATION (slide 118)
- 5 Incluir a trusted-key no arquivo named.conf (slide 118)
- 6 Executar o BIND (named)

Recomendação

Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
<http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/>

- 1 Instalar BIND com sigchase
- 2 Obter a trusted-key do site do Registro.br (slide 117)
- 3 Incluir a trusted-key no arquivo /etc/trusted-key.key
- 4 Realizar testes no servidor (DIG +sigchase)

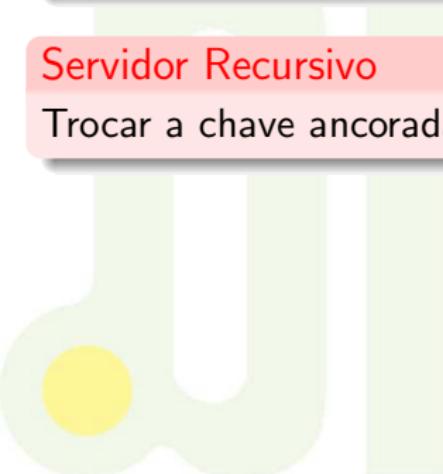
Servidor Autoritativo

Reassinar a zona antes das assinaturas expirarem

- ① Incrementar o serial (record SOA) do arquivo de zona original
- ② Reassinar a zona utilizando o comando dnssec-signzone

Servidor Recursivo

Trocar a chave ancorada quando ocorrer um rollover do BR



Parte III

Conclusão



Vulnerabilidades

- O Record NSEC é usado em DNSSEC para permitir a negação da existência
- De forma que para provar a inexistência, o NSEC aponta para o próximo nome existente na zona
- Esta prova de inexistência permite obter todo o conteúdo de uma zona com simples consultas de DNS

Varredura da Zona (Zone Walking)

- Até que este problema de varredura da zona esteja totalmente resolvido as zonas **.com.br** e **.org.br** não suportará DNSSEC



Possíveis Soluções

- Uma solução proposta pela RFC 4470 é a assinatura online dos records sempre que necessário. Porém, não é viável por exigir um processamento alto
- A IETF DNSEXT está trabalhando numa nova proposta denominada NSEC3 (draft-ietf-dnsext-nsec3)



NSEC3 - DNSSEC Hashed Authenticated Denial of Existence

- Soluciona o problema do “Zone Walking”
- Substitui o record NSEC pelo record NSEC3
- Faz um hash de todos os nomes da zona e ordena-os de forma canônica
- Ao invés de apontar para o próximo nome da zona, aponta para o próximo hash

Desvantagens com NSEC3

- Para toda requisição é preciso calcular o hash a cada prova de não existência

NSEC3 no Recursivo

- Atualmente apenas o servidor de nomes Unbound suporta a tecnologia NSEC3
 - Exemplo de configuração:

```
server:  
    verbosity: 2  
    interface: 192.168.0.1  
    interface: 127.0.0.1  
    access-control: 192.168.0.0/20 allow  
    chroot: '/usr/local/unbound/etc'  
    directory: '/usr/local/unbound/etc'  
    logfile: 'unbound.log'  
    pidfile: 'unbound.pid'  
    trust-anchor: 'br. DS 61207 5 1 637724A380ECE3426F5EBDCD6795AD4F729AB3E9'
```

Motivos para utilizar DNSSEC

- Impedir ataques do tipo “Man-in-The-Middle”
- Possibilitar um novo serviço de segurança pago aos seus clientes
- Assegurar-se de que seus dados estão chegando íntegros ao destino



-  [RFC 2671](#)
Extension Mechanisms for DNS (EDNS0)
-  [RFC 2845](#)
Secret Key Transaction Authentication for DNS (TSIG)
-  [RFC 4033](#)
DNS Security Introduction and Requirements (DNSSEC-bis)
-  [RFC 4034](#)
Resource Records for the DNS Security Extensions (DNSSEC-bis)
-  [RFC 4035](#)
Protocol Modifications for the DNS Security Extensions (DNSSEC-bis)
-  [RFC 4431](#)
The DNSSEC Lookaside Validation (DLV) DNS Resource Record
-  [RFC 4470](#)
Minimally Covering NSEC Records and DNSSEC On-line Signing
-  [RFC 4641](#)
DNSSEC Operational Practices
-  [Draft NSEC3 \(draft-ietf-dnsext-nsec3\)](#)
DNSSEC Hashed Authenticated Denial of Existence

- ▶ **DNSSEC.NET**
<http://www.dnssec.net>
- ▶ **Wikipédia - DNSSEC**
<http://pt.wikipedia.org/wiki/DNSSEC>
- ▶ **Wikipédia - Comparação entre softwares de servidores DNS**
http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software
- ▶ **Firewalls e DNS, como e porque configurar corretamente**
<ftp://ftp.registro.br/pub/doc/dns-fw.pdf>
- ▶ **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos**
<http://www.cert.br/docs/whitepapers/dns-recursivo-aberto>
- ▶ **FAQ - Registro.br (Perguntas Frequentes)**
<http://registro.br/faq>
- ▶ **A última versão deste tutorial pode ser encontrada em**
<ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>

Agradecimento em especial

- ▶ **DNSSEC – Olaf Kolkman (RIPE NCC/NLnet Labs)**
http://www.nlnetlabs.nl/dnssec_howto

Obrigado!

