registro.br

Estado da implementação DNSSEC no .br

detalhes e os próximos passos

Frederico Neves <fneves@registro.br>

GTER25 - Salvador - 20080531

nic.br

Disponibilidade

- Início em 4/6/2007

  br

  blog.br

  eng.br

  eti.br

  gov.br

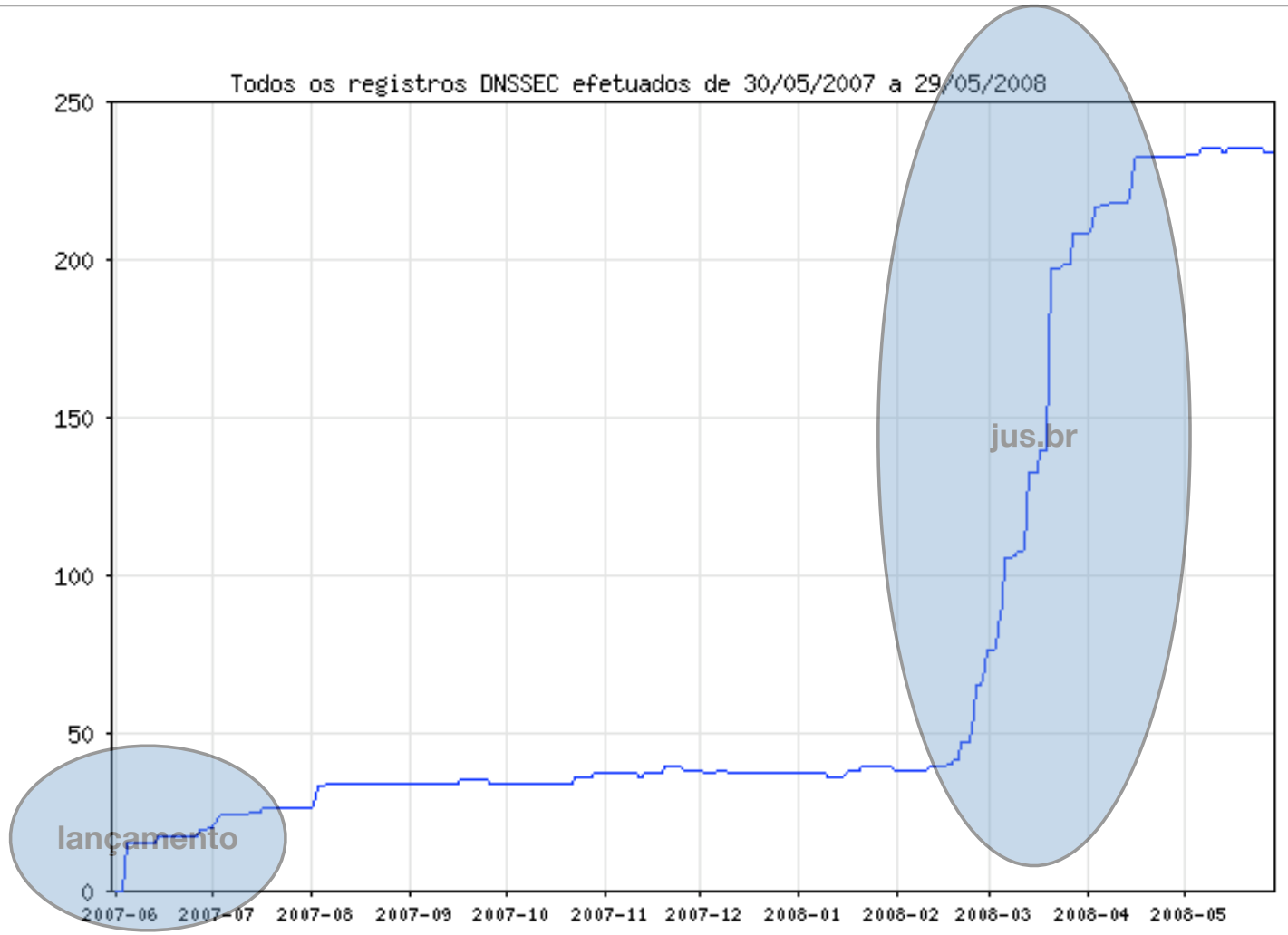
- No decorrer do ano fomos adicionando nova zonas

  http://registro.br/info/dpn.html

- Disponível atualmente em quase todos os domínios de segundo-nível
- Avisos de problemas com DNSSEC desde 17/4/2008

  Problema mais comum é a expiração de assinaturas

Crescimento



Disponibilidade de Software

- Bind 9.5.0 (recursivo e autoritativo)

  http://www.isc.org/index.pl?/sw/bind/index.php

- NSD 3.0.8 (autoritativo)

  http://www.nlnetlabs.nl/nsd/index.html

- Unbound 1.0.0 (recursivo com suporte para nsec3)

  http://unbound.net/

Política de Rollover KSK - Implicações TA

- Política atual efetua um Rollover do KSK a cada 12 meses
- Período do rollover dura 2 meses
- Em uma situação com disponibilidade de DNSSEC no parent este problema não existe

  Ao menos ele não é de sua responsabilidade

- A maior implicação é que os servidores recursivos que não atualizarem a âncora durante o período de 2 meses vão classificar os domínios a partir da remoção da chave antiga como “bogus” e retornarão SERVFAIL nas resoluções
- A solução de longo prazo é a adoção de um protocolo que faça a sinalização e a troca das chaves “in-band” (RFC5011)
- Enquanto não temos isto provavelmente uma chave de longa duração e uma chave backup já ancoradas parecem ser a melhor solução levando-se em conta um balanço entre a estabilidade e a segurança do sistema

  KSK em produção será armazenada em um HSM (FIPS 140-2 nível 4)

  KSK backup (smart card em local seguro)

nsec3 testbed - .sec3.br

- Domínio de Produção
- Registro gratuito através de todas interfaces de provisionamento

  web + EPP

  Informação do registro DS obrigatória (SHA1 ou SHA256)
- Servidor autoritativo separado - a.nsec3.dns.br

  NSD (svn 20080304)
- Sem opt-out
- Salt 10 bytes

  gerado randomicamente a cada publicação total ou em uma situação de colisão
- 2 Iterações na geração do hash

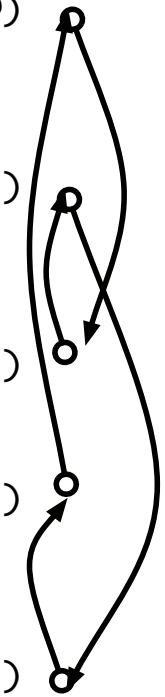
Prova de não existência - (NSEC x NSEC3)

NSEC

```
@ soa
@ nsec a rrtypes(@)

a ns
a ds
a nsec c rrtypes(a)

c ns
c ds
c nsec d rrtypes(c)

d ns
d nsec e rrtypes(d)

e ns
e ds
e nsec @ rrtypes(e)


On Co [@ a c d e]
```

NSEC3

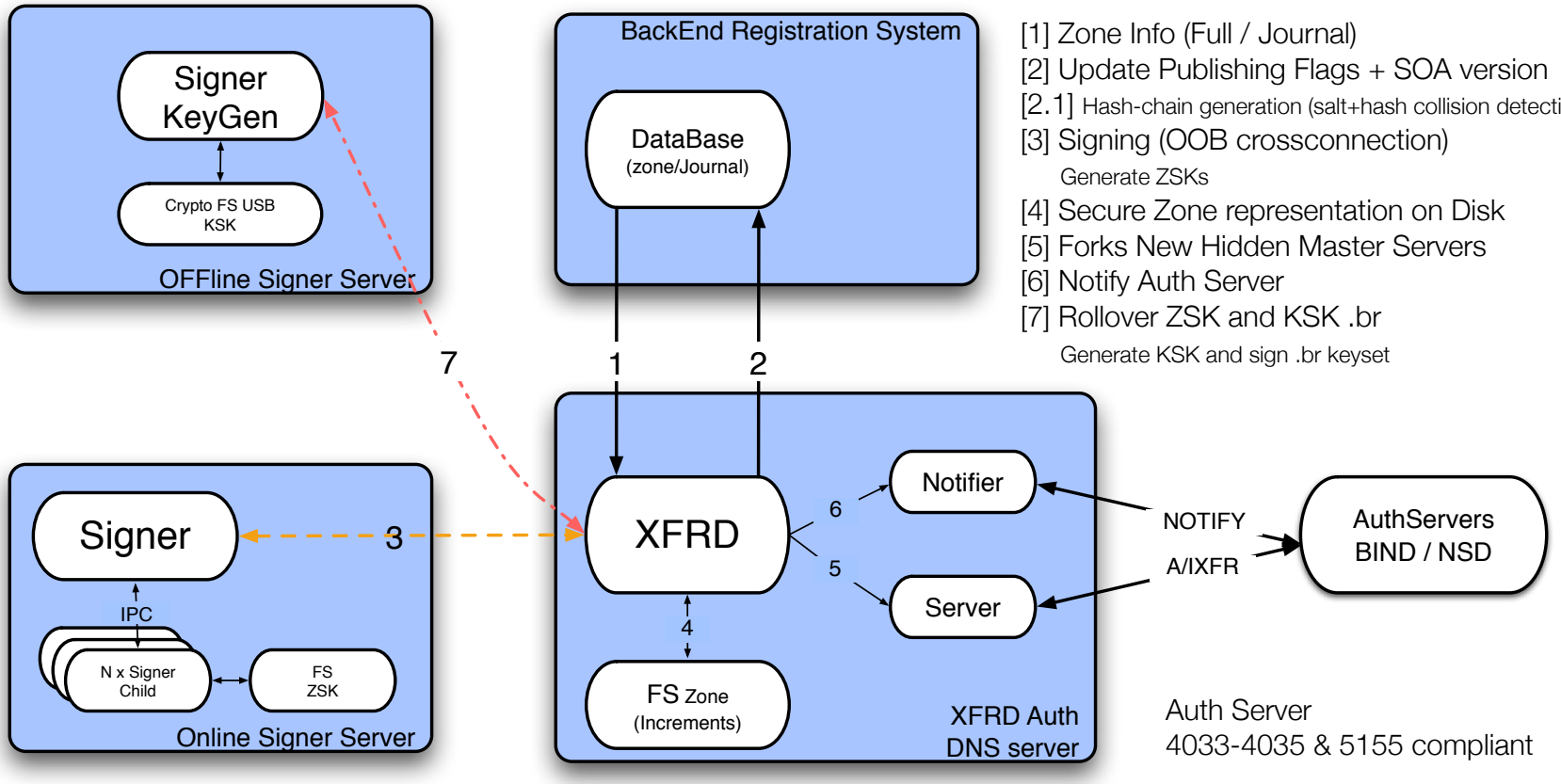
```
@ soa
h(@) nsec3 h(c) rrtypes(@)

a ns
a ds
h(a) nsec3 h(e) rrtypes(a)

c ns
c ds
h(c) nsec3 h(a) rrtypes(c)

d ns
h(d) nsec3 h(@) rrtypes(d)

e ns
e ds
e nsec3 h(d) rrtypes(e)


h(On) Co [@ c a e d]
```



Verificações da Implementação

- Testes automatizados
  - publicação total
  - zona vazia e suas variações
  - adição
  - remoção
  - validação da cadeia nsec/nsec3
- Usando Unbound + Drill Sigchase
- O resultado foi a descoberta de alguns erros da implementação

Arquitetura do XFRD 3.0.1



[1] Zone Info (Full / Journal)
[2] Update Publishing Flags + SOA version
[2.1] Hash-chain generation (salt+hash collision detection)
[3] Signing (OOB crossconnection)
Generate ZSKs
[4] Secure Zone representation on Disk
[5] Forks New Hidden Master Servers
[6] Notify Auth Server
[7] Rollover ZSK and KSK .br
Generate KSK and sign .br keyset

Auth Server
4033-4035 & 5155 compliant

sec3.br - Testem !

- É de graça
- Precisamos de voluntários (17 bravas almas)
- Está disponível desde 4/3/2008

  Instruções em:

  http://eng.registro.br/pipermail/gter/2008-March/016901.html
- Em casos de dúvidas/problemas

  lista do GTER

  dnssec@registro.br

Desafio sec3.br

- Enumere a zone a qualquer momento

  dica foo.sec3.br e outros nomes presentes em outras zonas assinadas no .br estão presentes nesta zona

- O primeiro que enviar uma prova ganha um registro de um domínio .com.br para o resto de sua vida :-)

Próximos passos

- .com.br e .org.br

  web + EPP

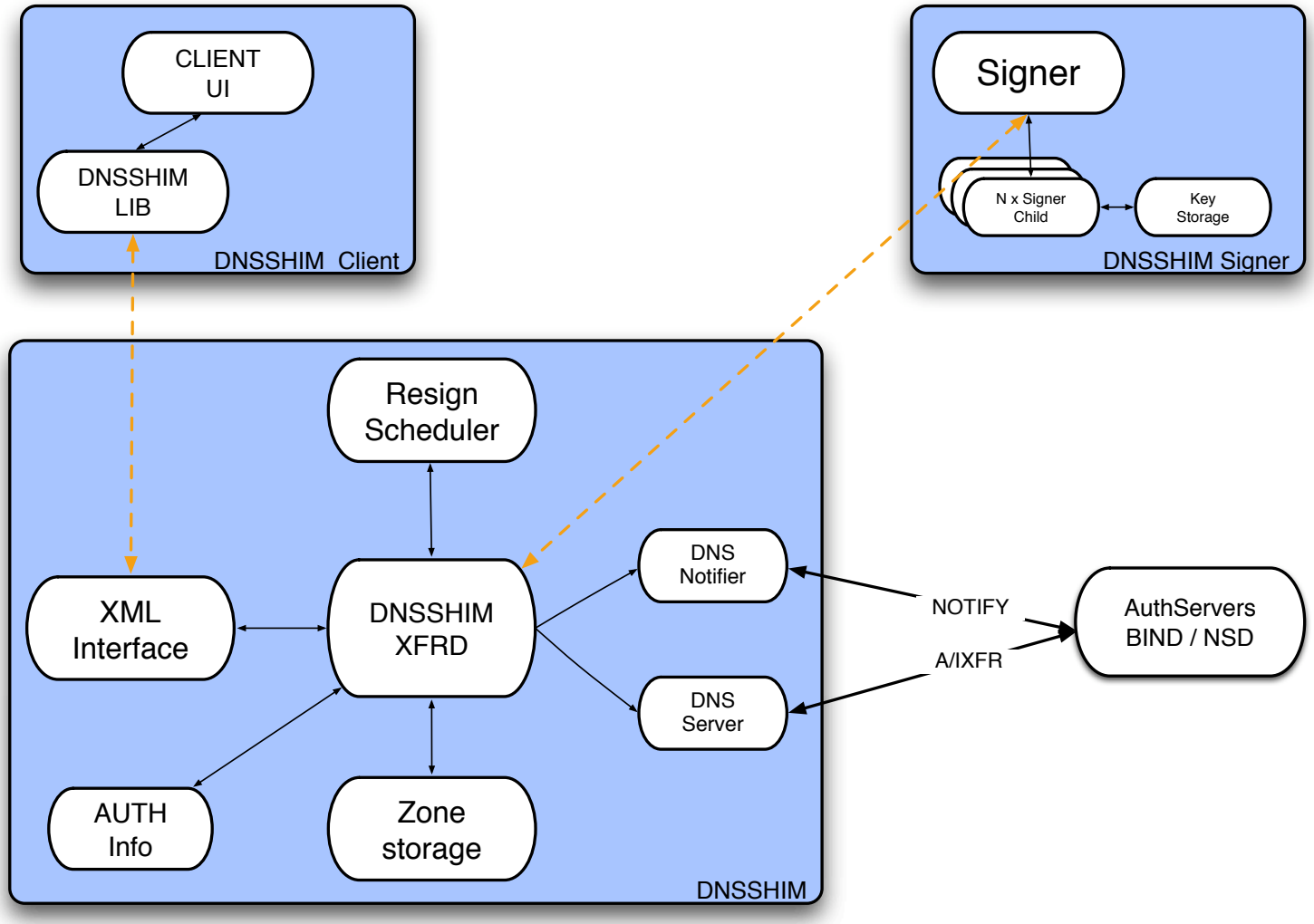
  DS opcional

- opt-out gap 100 nomes (redução da margem para replay attacks)
- Quando

  Tão logo tenhamos servidores autoritativos BIND e NSD estáveis com suporte a RFC 5155

- O testbed será encerrado 90 dias após a entrada em produção

Software para manutenção de zonas seguras



Perguntas ?

Obrigado !