registro.br

DNSSEC no .br

detalhes da implementação e os próximos passos

Frederico Neves <fneves@registro.br>

GTER23 - Belo Horizonte - 20070629

nic.br

Motivações

- Melhorar a segurança na resolução de nomes e consequentemente a confiança no sistema de nomes de domínio.

- Evitar DOS baseados na poluição de cache que impactam em praticamente todos os serviços existentes hoje na rede.

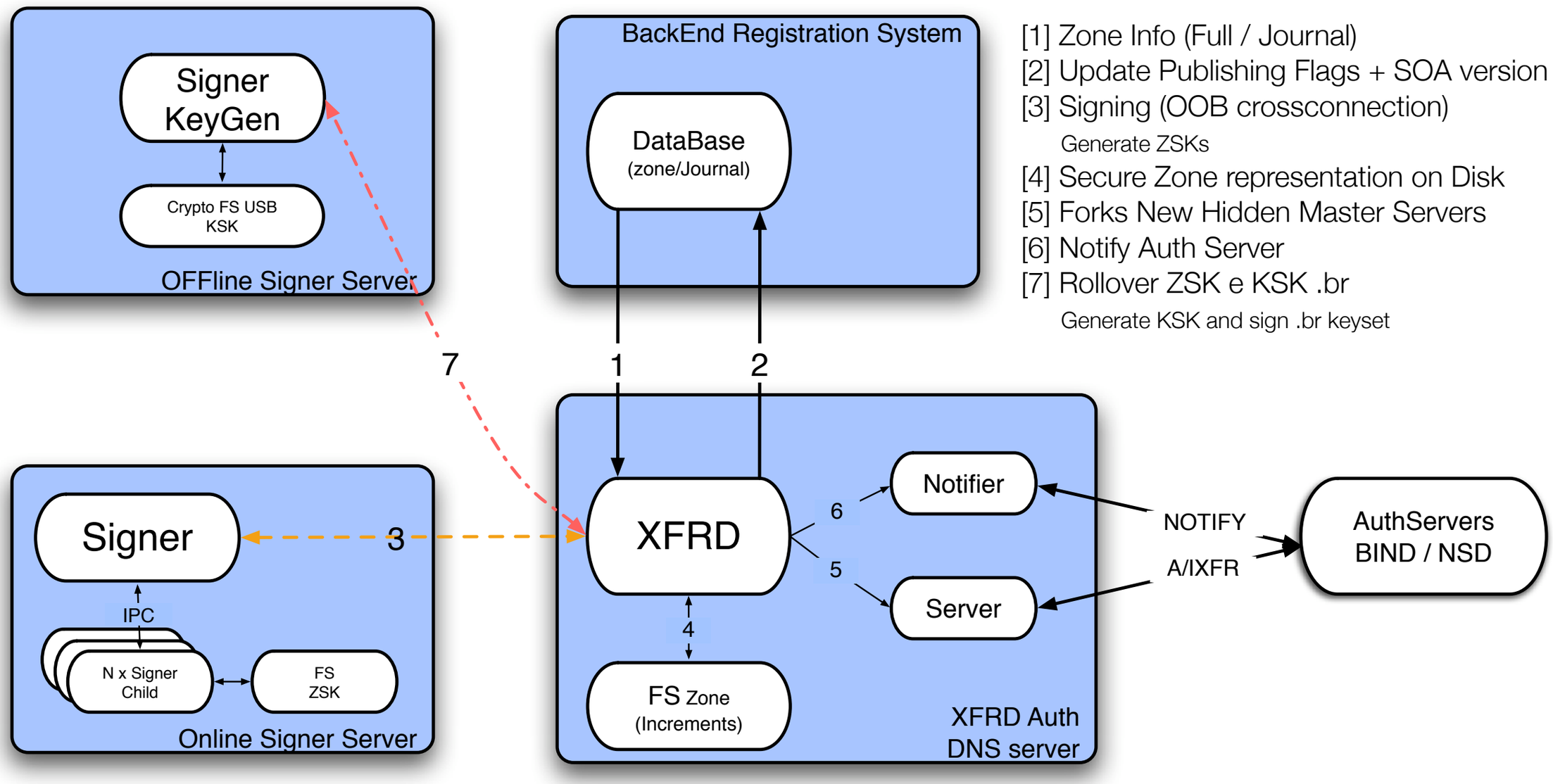
- Garantir a segurança no uso do DNS como meio de distribuição de políticas para outros protocolos (SPF, DKIM).

- Poder utilizar DNS como plataforma de distribuição genérica de chaves (PGP, PKI).

Mudanças no serviço de Registro

- Inicialmente oferta em 5 pequenas zonas de forma opcional.
  - .br .gov.br .blog.br .eng.br .eti.br
- Lançamento de domínios com uso obrigatório.
  - b.br - FEBRABAN
  - j.br - CNJ
- Disponível na interface web e EPP (RFC4310) com a adição de campos para a coleta do registro DS (Delegation Signer).
- Pequenas mudanças no serviço de publicação DNS.

Arquitetura do Sistema de publicação



[1] Zone Info (Full / Journal)
[2] Update Publishing Flags + SOA version
[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 e KSK .br
Generate KSK and sign .br keyset

Adoção e o papel dos vários Atores

- Inicialmente lenta devido a não disponibilidade inicial para todos as nossa extensões.
    - Anúncios somente na página do Registro.br, fóruns técnicos e press-release para a imprensa especializada.
- Via comunidade técnica nos foruns nacionais
- Provedores de acesso
    - Via CGI e pelo estímulo pelos domínios seguros em áreas específicas
- Detentores de domínio
    - Via prestadores de serviço EPP que podem se interessar em prover segurança agregando valor a seus produtos.
    - Na interface direta

Próximas fases

- Assinatura de todas as zonas pequenas (exceto .com.br e .org.br)
    - Este processo será feito gradativamente nos meses subsequentes terminando em outubro deste ano.
- Adoção do chamado DNSSEC-ter.
    - NSEC3 no lugar de NSEC como solução da prova da não existência de um nome ou tipo.
- Assinatura do .com.br e .org.br no final do ano.

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)
```

NSEC3

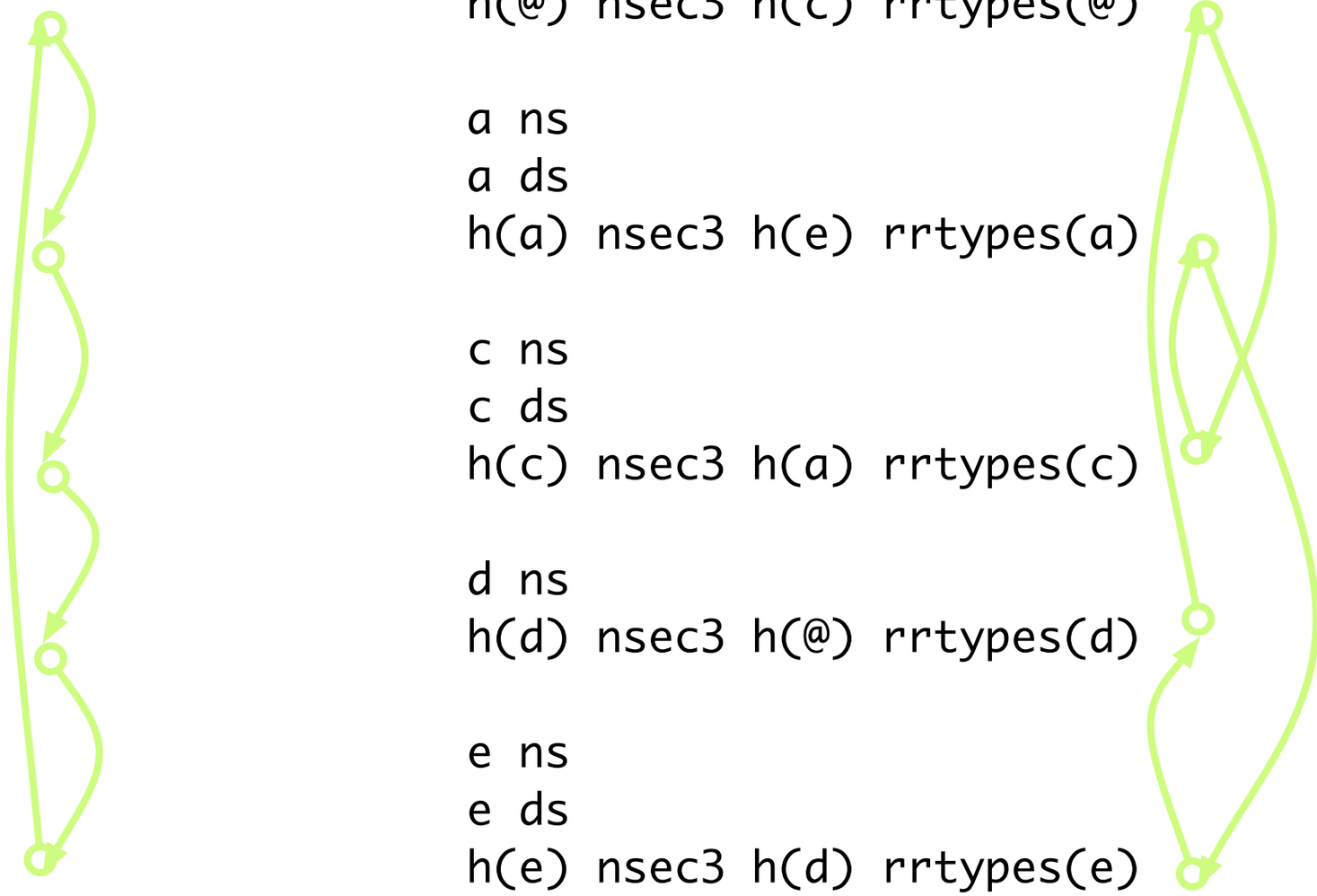
```
@ soa
h(@) nsec3 h(c) rrtypes(@)

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
h(e) nsec3 h(d) rrtypes(e)
```



On Co [@ a c d e]

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

Perguntas ?

Obrigado !