DNSSEC história e standard

Frederico A C Neves
<fneves@registro.br>

História

- Nov 1993 - Design team
- Jan 1997 - 1° std - RFC2065
- Mar 1999 - 2 ° std - RFC2535
  - 2000 - NO x NXT
  - 2001 - OPT-IN
- 2°sem. 2004 - 3° std
  - draft-ietf-dnsext-dnssec-intro-12
  - draft-ietf-dnsext-dnssec-protocol-8
  - draft-ietf-dnsext-dnssec-records-10

Futuro do WG

- Promovendo documentos no std-track
  - TSIG, IXFR, Notify, Dynamic Update etc...

- Requisitos para a comprovação de não existência (NSEC II III)
  - Draft-ietf-dnsext-signed-nonexistence-requirements-00

Adoção DNSSECbis “Já”

Tundo indica que sim

- ccTLDs
  NL, SE
- RIRs

Sem informação pública

- GTLDs
- Outros ccTLDs

Principais reclamações (xxTLDs)

- Consumo de recursos

  (6-8x > em casos de delegation-only)

- Publicidade da zona - NSEC Walking

Suporte Servidores (DNSSECbis)

NSD 2.1.x (auth-only, compile-time opt)

BIND 9.3.0 (compile-time opt, runtime opt)

Standard

DNSSEC garante somente origem e integridade de um RRset

Não existe confidencialidade (muito pelo contrário)

Standard

Novos RR

- **DNSKEY**

  chave publica para o dominio em questão

  Flag, protocolo, algoritimo, chave (base64)

- **RRSIG**

  assinatura do RRSET (somente registros com autoridade)

  Type, algoritimo, # labels (syntetic detection), sig exp e incep, sig name, assinatura

- **NSEC**

  próximo registro seguro e RRsets para o nome atual

- **DS**

  delegation Signer (cadeia de confiança)

  Keyid, algoritimo, digest type, digest (sha1)

DNSSEC história e standard