

Documento Auxiliar Implementação DNSSEC



11.06.2010
v0.4

Este documento tem como objectivo guiar na implementação de DNSSEC quer ao nível das ferramentas utilizadas como da configuração do sistema e do DNS.

Os procedimentos demonstrados tem por base a utilização de um ambiente Unix, apesar das ferramentas aqui mencionadas também se encontrarem disponíveis para Windows.

Antes de iniciar o processo de assinatura de uma zona deverá garantir que tem instaladas as ferramentas necessárias para o fazer, nomeadamente, versões recentes e sem vulnerabilidades de OpenSSL e BIND.

I - Instalação ou actualização de ferramentas:

- 1) Instalar uma versão do OpenSSL actualizada e sem bibliotecas partilhadas;
- 2) Instalar uma versão do BIND actualizada e com suporte OpenSSL;
- 3) Verificar se o BIND ficou correctamente instalado.

II - Processo de assinatura de uma zona

- 1) Configurar uma zona DNS num servidor de nomes primário;
- 2) Editar as configurações de forma a incluir as opções de DNSSEC;
- 3) Realizar sempre uma cópia de segurança da última zona correctamente configurada;
- 4) Reiniciar o serviço para actualizar a informação no servidor de nomes;
- 5) Gerar os pares de chaves a utilizar, pelo menos duas, uma chave para assinar a zona (ZSK) e uma chave que assina a chave que assina a zona (KSK);
- 6) Incluir as chaves públicas geradas no ficheiro de zona;
- 7) Assinar a zona com as chaves (KSK e ZSK);
- 8) Verificar se a zona assinada ficou correctamente configurada;
- 9) Alterar as configurações de forma a reflectir o novo nome da zona assinada;
- 10) Reiniciar o serviço para actualizar a informação no servidor de nomes;
- 11) Verificar se existe resposta do servidor de nomes e se esta vem com informação DNSSEC;
- 12) Se o seu domínio se encontra activo numa hierarquia sob .pt, que não a hierarquia dnssec.pt, então deverá submeter a informação do resource record DS directamente no sistema de gestão online de domínios .pt efectuando login como responsável técnico do domínio;
- 13) Se está a utilizar um domínio de teste sob a hierarquia dnssec.pt deverá enviar a informação dos resource record DS e NS (servidores de nomes) para dev@dnssec.pt para que estes sejam inseridos e assinados na zona dnssec.pt criando assim a cadeia de confiança pretendida;
- 14) Para configurar um servidor de nomes recursivo (resolver) com um trusted-anchor de modo a efectuar validação DNSSEC de domínios assinados.



I - Instalação ou actualização de ferramentas

Este tópico tem como objectivo auxiliar na instalação ou actualização de ferramentas com suporte a DNSSEC. Os procedimentos demonstrados tem por base a utilização de um ambiente Unix, mas as ferramenta aqui mencionadas também se encontram disponíveis para Windows.

- 1) Instalar uma versão do OpenSSL actualizada e sem bibliotecas partilhadas. Para mais informação consulte <http://www.openssl.org/>:

```
# wget http://www.openssl.org/source/openssl-1.0.0a.tar.gz
```

Após a transferência do ficheiro deve-se extrair o mesmo (`tar -zxvf openssl-1.0.0a.tar.gz`), entrar na respectiva pasta e correr as seguintes configurações:

```
# ./config --prefix=/usr/  
# make  
# make test  
# make install
```

- 2) Instalar uma versão do BIND actualizada e com suporte OpenSSL, para mais informação consulte <https://www.isc.org/>:

```
# wget http://ftp.isc.org/isc/bind9/9.7.0-P2/bind-9.7.0-P2.tar.gz
```

Após a transferência do ficheiro deve-se extrair o mesmo (`tar -zxvf bind-9.7.0-P2.tar.gz`), entrar na respectiva pasta e correr as seguintes configurações:

```
# ./configure --with-openssl  
# make  
# make test  
# make install
```

- 3) Após instalar o BIND verificar se a configuração ficou correcta e que a versão instalada é a que está como predefinida na máquina:

```
# named -V  
  
BIND 9.7.0-P2 built with '--with-openssl'
```

II - Processo de assinatura de uma zona

Este tópico serve como referência nas várias etapas de configuração de um domínio com DNSSEC. Os procedimentos aqui exemplificados foram realizados num ambiente Unix com a ferramenta BIND, mas esta ferramenta também se encontra disponível para Windows.

Antes de iniciar este processo deverá garantir que tem instaladas as ferramentas necessárias, nomeadamente, versões recentes e sem vulnerabilidades de OpenSSL e BIND.

- 1) Configurar uma zona dns sob dnssec.pt num servidor de nomes primário, supondo que o nome da zona é “zonateste.dnssec.pt” e nome do ficheiro da zona será “db.zonateste.dnssec.pt”:

Exemplo do conteúdo do ficheiro “db.zonateste.dnssec.pt”:

```
$origin zonateste.dnssec.pt.
$TTL 14400          ; 4 hours
@      IN      SOA      ns01.zonateste.pt. hostmaster (
                        2009012101      ; serial
                        14400           ; refresh (6 hours)
                        7200            ; retry (2 hours)
                        604800          ; expire (30 days)
                        14400           ; minimum (4 hours)
                        )
                        IN      NS      ns01.zonateste.pt.
                        IN      NS      ns02.zonateste.pt.
                        IN      A      127.0.0.1
```

- 2) Editar o ficheiro “named.conf” acrescentando opções de DNSSEC, a zona “zonateste.dnssec.pt”:

Normalmente em /etc/named.conf e verifique que versão BIND tem instalada com “named -v”:

```
options{
    dnssec-enable yes; //A partir da versão BIND 9+ (ou superior)
}
...

zone "zonateste.dnssec.pt" {
    type master;
    file "db.zonateste.dnssec.pt"; //Normalmente em /var/named/
};
...
```

- 3) Após confirmar se a “zonateste.dnssec.pt” foi correctamente configurada poderá realizar uma cópia de segurança da mesma (útil associar o número de série da zona ao nome da cópia):

Comando para confirmar se as configurações da zona e do “named.conf” estão correctas:

```
# named-checkconf -z
```

Exemplo do resultado da correcta configuração da zona “zonateste.dnssec.pt” no “named.conf”:

```
zone zonateste.dnssec.pt /IN: loaded serial 2009012101
```

```
[UNIX]:# cp db.zonateste.dnssec.pt db.zonateste.dnssec.pt.2009012101  
[WINDOWS]: copy db.zonateste.dnssec.pt db.zonateste.dnssec.pt.2009012101
```

4) Reiniciar ou Iniciar o named

Para reiniciar no caso de já estar a correr e consoante a localização do ficheiro named.pid:

```
[UNIX]:# kill -HUP $(cat /var/named/named.pid)  
[WINDOWS]: Control Panel -> Administrative Tools -> Services -> ISC BIND ->  
Restart Service
```

Para iniciar no caso de ainda não estar a correr:

```
[UNIX]:# named  
[WINDOWS]: Control Panel -> Administrative Tools -> Services -> ISC BIND ->  
Start Service
```

- 5) Gerar as chaves para a “zonateste.dnssec.pt”. É necessário escolher as dimensões e algoritmo de geração, recomendamos que utilize para a ZSK dimensão 1024 e para a KSK dimensão 2048, para o algoritmo recomendamos que se utilize o NSEC3RSASHA1 (disponível na versão BIND 9.6 ou superior) pois evita a enumeração da zona. Uma vez que poderá não ter uma versão BIND tão recente utilize o algoritmo RSASHA1:

Para mais informações:

```
# man dnssec-keygen ou http://www.manpagez.com/man/8/dnssec-keygen/
```

Geração da chave ZSK – Zone Signing Key:

```
# dnssec-keygen -a NSEC3RSASHA1 -b 1024 -n ZONE zonateste.dnssec.pt  
//BIND 9.6+
```

ou

```
# dnssec-keygen -a RSASHA1 -b 1024 -n ZONE zonateste.dnssec.pt
```

Exemplo do resultado da geração da chave ZSK:

```
Kzonateste.dnssec.pt.+007+31277
```

ou

```
Kzonateste.dnssec.pt.+005+31277
```

-a algoritmo (para NSEC3 deverá ser NSEC3RSASHA1 evita “zone walking”);
-b tamanho da chave (pode variar consoante o algoritmo utilizado mas para RSAMD5/RSASHA1 tem de estar entre 512 e 2048 bits.);
-n tipo de nome, deverá ser ZONE no caso de ser a chave para uma zona DNSSEC (KEY/DNSKEY);

Geração da chave KSK – Key Signing Key:

```
# dnssec-keygen -f KSK -a NSEC3RSASHA1 -b 2048 -n ZONE zonateste.dnssec.pt
```

```
//BIND 9.6+
```

ou

```
# dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE zonateste.dnssec.pt
```

Exemplo do resultado da geração da chave KSK:

```
Kzonateste.dnssec.pt.+007+38193
```

ou

```
Kzonateste.dnssec.pt.+005+38193
```

```
-f activa a flag KSK (Key Signing Key) DNSKEY;  
-a algoritmo (para NSEC3 deverá ser NSEC3RSASHA1);  
-b tamanho da chave (pode variar consoante o algoritmo utilizado);  
-n tipo de nome, deverá ser ZONE no caso de ser a chave para uma zona DNSSEC  
(KEY/DNSKEY);
```

- 6) Incluir ambas chaves públicas geradas (ZSK e KSK com extensão .key) no final do ficheiro de zona “db.zonateste.dnssec.pt” e não esquecer de actualizar o número de série:

Exemplo, alterar número de série de “2009012101” para “2009012102”:

```
$origin zonateste.dnssec.pt.  
$TTL 14400 ; 4 hours  
@ IN SOA ns01.zonateste.pt. hostmaster (  
2009012101 ; serial  
14400 ; refresh (6 hours)  
7200 ; retry (2 hours)  
604800 ; expire (30 days)  
14400 ; minimum (4 hours)  
)  
IN NS ns01.zonateste.pt.  
IN NS ns02.zonateste.pt.  
IN A 127.0.0.1  
$include Kzonateste.dnssec.pt.+007+31277.key ; ZSK inserida a 20090121  
$include Kzonateste.dnssec.pt.+007+38193.key ; KSK inserida a 20090121
```

- 7) Assinar a “zonateste.dnssec.pt” com as chaves (KSK e ZSK) sem as extensões das mesmas:

Para mais informações:

```
# man dnssec-signzone ou http://www.manpagez.com/man/8/dnssec-signzone/
```

Assinatura da zona “zonateste.dnssec.pt” que será válida por 30 dias a contar a partir do processo de assinatura :

```
# dnssec-signzone -k Kzonateste.dnssec.pt.+007+38193 -o zonateste.dnssec.pt  
-t -3 - -A db.zonateste.dnssec.pt Kzonateste.dnssec.pt.+007+31277  
//BIND 9.6+
```

ou

```
# dnssec-signzone -k Kzonateste.dnssec.pt.+005+38193 -o zonateste.dnssec.pt  
-t db.zonateste.dnssec.pt Kzonateste.dnssec.pt.+005+31277
```

```
-e end-time, especifica a data e hora em que os Resource Records RRSIG gerados irão expirar, deve-se indicar um tempo absoluto no formato
```

YYYYMMDDHHMMSS (-e 20091231173000 assinatura válida até 31 de Dezembro de 2009 pelas 17h30m00s). Se não for especificado o end-time será configurado por defeito a 30 dias a contar a partir do processo de assinatura, recomendamos que mantenha o formato por defeito para efectuar pelo menos uma manutenção mensal à zona;

-k indica que é uma KSK seguido de Kzonateste.dnssec.pt.+007+38193;

-o nome original da zona, neste exemplo é zonateste.dnssec.pt;

-t para incluir resultado das estatísticas após assinatura;

-3 salt (gera a cadeia NSEC3 com o respectivo hex encoded salt, pode ser utilizado um - (dash) para indicar que não é necessário utilizar salt na geração da cadeia NSEC3;

-A Quando é gerada uma cadeia NSEC3 configura a flag OPTOUT em todos os Resource Records NSEC3 e não são gerados RRs NSEC3 para delegações não seguras, isto é, que não se encontrem assinadas;

db.zonateste.dnssec.pt nome do ficheiro de zona;

Kdnssec.pt.+007+31277 especifica que chave deve ser utilizada para assinar a zona (ZSK);

Resultado após da assinatura:

```
zonateste.dnssec.pt.signed
Signatures generated:      9
Signatures retained:      0
Signatures dropped:       0
Signatures successfully verified: 0
Signatures unsuccessfully verified: 0
Runtime in seconds:       0.013
Signatures per second:    681.766
```

8) Verificar se a zona assinada “zonateste.dnssec.pt.signed” ficou correctamente configurada:

Comando para confirmar se as configurações da zona estão correctas:

```
# named-checkzone zonateste.dnssec.pt db.zonateste.dnssec.pt.signed
```

Exemplo do resultado da zona correctamente configurada e assinada:

```
zone zonateste.dnssec.pt/IN: loaded serial 2009012102 (signed)
```

9) Alterar no ficheiro de configuração “named.conf” o nome do ficheiro da zona para o novo nome que contém a zona “zonateste.dnssec.pt” já assinada:

Alterar no named.conf de “db.zonateste.dnssec.pt” para “db.zonateste.dnssec.pt.signed”:

```
zone "zonateste.dnssec.pt" {
    type master;
    file "db.zonateste.dnssec.pt.signed";
};
```

10) Reiniciar ou Iniciar o named

Para reiniciar no caso de já estar a correr e consoante a localização do ficheiro named.pid:

```
[UNIX]:# kill -HUP $(cat /var/named/named.pid)
[WINDOWS]: Control Panel -> Administrative Tools -> Services -> ISC BIND ->
Restart Service
```

Para iniciar no caso de ainda não estar a correr:

```
[UNIX]:# named  
[WINDOWS]: Control Panel -> Administrative Tools -> Services -> ISC BIND ->  
Start Service
```

11) Verificar se existe resposta do servidor de nomes e se esta vem com informação DNSSEC:

```
# dig @localhost zonateste.dnssec.pt SOA +dnssec +multiline
```

Exemplo do resultado da correcta configuração da zona “zonateste.dnssec.pt” com um RRSIG associado ao RR pedido, indicando que este se encontra correctamente assinado:

```
zonateste.dnssec.pt.      14400 IN SOA ns01.zonateste.pt. hostmaster (
                          2009012102 ; serial
                          14400      ; refresh (4 hours)
                          7200      ; retry (2 hours)
                          604800    ; expire (1 week)
                          14400      ; minimum (4 hours)
                          )
zonateste.dnssec.pt.      14400 IN RRSIG SOA 7 2 14400 20091214123000 (
                          20091001135720 40652 dnssec.pt.
                          V/aTWiVDi1XKGPEJNijkMYsq//DVX503HVFwhyYYdYqT
                          bjj5vfWG9A/jQNx23trajFXEPXfogykbzahjfkPQ0NJV
                          65VhHkLSd6BJeTh7LpmWQKg2YYXyAfIRB/GsFI0aTkQk
                          GZhHvtqoe9W5DUUpCZgp1iIQ9wpAIajXrxUkC0Zo= )
```

12) Se o seu domínio se encontra activo numa hierarquia sob .pt, que não a hierarquia dnssec.pt, então deverá submeter a informação do resource record DS directamente no sistema de gestão online de domínios .pt efectuando login como responsável técnico do domínio:

Aceder a <https://online.dns.pt/> como responsável técnico do domínio em causa:

- No “Resumo do Estado dos domínios” seleccionar o link “Active”;
- Na lista do domínios apresentada seleccionar o link do número de processo correspondente ao domínio que pretendemos;
- Depois de entrar na “Ficha de Processo” do domínio seleccionar a opção DNSSEC que se encontra na lista de “Opções RT” (Responsável Técnico);
- Deverá adicionar novo resource record DS preenchendo todos os dados solicitados e realizar submeter no final;
- Após ter inserido correctamente o novo resource record DS e este se encontrar na tabela de chaves deverá seleccioná-lo e “Activar” para que o mesmo seja incluído na zona .pt.

Para saber os dados correctos do DS que vai inserir deverá verificar o conteúdo do ficheiro “dsset-zonateste.dnssec.pt” que foi gerado automaticamente quando a “zonateste.dnssec.pt” foi assinada:

[UNIX]: cat dsset-zonateste.dnssec.pt.
[WINDOWS]: type dsset-zonateste.dnssec.pt.

Conteúdo do ficheiro “dsset-zonateste.dnssec.pt” que deverá utilizar:

```
zonateste.dnssec.pt. IN DS 38193 7 1 E8014F32288DF46357097FDA3FF24907F9E2F4D1
```

Gestão de Domínios Online

Processo	Domínio	Hierarquia	Estado	Data Submissão	Facturado até	ET	EG	RA	RT
396741	saramonteiro	.nome.pt	ACTIVE	03/12/2009		S	N	N	S

Consulta: [Ficha de Processo](#)

Opções ET: [Remover Domínio](#) | [Senha p/ alteração EG](#) | [Assumir a Gestão](#) |

Opções RT: [Alterações técnicas](#) | [Pedido de Avaliação](#) | [DNSSEC](#) |

DNSSEC

A tabela que se segue contém informação relativa às chaves associadas ao seu domínio no âmbito da assinatura de domínios por DNSSEC.

Para publicar novas chaves, remover chaves anteriormente publicadas ou modificar o estado de chaves referentes à sua zona deverá efectuar aqui as respectivas alterações:

Key Tag	Algoritmo	Tipo	Resumo	Activa	Desde	
28824	7: RSA/SHA-1 (NSEC3)	1	4C15DE1F351C204E31B8D1CE2972E147D05A29C1	Sim	27/01/2010 16:14	<input type="checkbox"/>

Alterações: [Activar](#) [Desactivar](#) [Eliminar](#)

Adicionar novo:

Key Tag	<input type="text"/>
Algoritmo da Chave	...
Tipo de Resumo	...
Resumo	<input type="text"/>
<input type="button" value="Submeter"/>	

- 13) Enviar o resource record DS e os NS (servidores de nomes) para dev@dnssec.pt para que estes sejam inseridos e assinados na zona dnssec.pt criando assim uma cadeia de confiança:

Para descobrir o DS deverá verificar o conteúdo do ficheiro “dsset-zonateste.dnssec.pt” que foi gerado automaticamente quando a “zonateste.dnssec.pt” foi assinada:

[UNIX]: cat dsset-zonateste.dnssec.pt.
[WINDOWS]: type dsset-zonateste.dnssec.pt.

Conteúdo do ficheiro “dsset-zonateste.dnssec.pt”:

```
zonateste.dnssec.pt. IN DS 38193 7 1 E8014F32288DF46357097FDA3FF24907F9E2F4D1
zonateste.dnssec.pt. IN DS 38193 7 2
40E94A1B262E4396A3C8A2FBDA0B35D2BA76C4C23DDB1EEDBAD90B1C 458C5B3F
```

Enviar para dev@dnssec.pt os NS e o DS gerado por SHA-1 (neste caso é o que aparece primeiro):

```
zonateste.dnssec.pt. IN DS 38193 7 1 E8014F32288DF46357097FDA3FF24907F9E2F4D1
zonateste.dnssec.pt. IN NS ns1.teste.pt.
IN NS ns2.teste.pt.
```

- 14) Para configurar um servidor de nomes recursivo (resolver) com um trusted-anchor de modo a efectuar validação DNSSEC de domínios assinados:

Como boa prática para se efectuar validação DNSSEC a mesma deverá ser realizada num servidor de nomes recursivo não autoritário, principalmente por duas razões:

- 1) Não é lógico que o servidor de nomes faça validação de “si próprio”;
- 2) Garantir que os domínios delegados nesse servidor de nomes autoritário não se encontrem vulneráveis a ataques do tipo negação do serviço. Infelizmente muitas entidades e instituições de modo a economizarem recursos têm esta tipologia, felizmente com DNSSEC os riscos de vulnerabilidade são menores mas presentes:

Para configurar um servidor de nomes recursivo, como no caso dos ISPs, para que seja realizada validação DNSSEC sempre que ocorre a resolução de nomes de domínio assinados é necessário acrescentar as seguintes opções no “named.conf”:

- Editar o ficheiro “named.conf” que normalmente se encontra em /etc/named.conf;
- Verificar a versão BIND que se encontra instalada na máquina, para saber se é compatível com as opções pretendidas, utilizando o comando “named -v” ou “named -V”;
- Acrescentar as opções de validação DNSSEC e definir qual o trusted-key em que pretendem confiar para verificar a veracidade das assinaturas DNSSEC (o trusted-key do .pt encontra-se disponível em www.dnssec.pt em “Chave Pública” e o de dnssec.pt em “Registar Agora”).

```
options{
dnssec-enable yes; //A partir da versão BIND 9+ (ou superior)
dnssec-validation yes; //BIND 9.4+
}
zone "zonatestes.dnssec.pt" {
    type master;
    file "db.zonatestes.dnssec.pt"; //Normalmente em /var/named/
};

...

trusted-keys {
dnssec.pt. 257 3 7 "AwEAAam09sDJMrgDSNcda9x08a5vti3K81YbLoWAcZ5VqjQsxtRUCvhe
JMwEkKmok+83kC8BntYwldfmmDpMVlLHvI5h80OGc2Imth/VaIt1do5v
XbYMwKCQHbOW6Gq+EFto0ZLJkpxSRowF8rLvZ61ePVQacarbgUXTuPz7
jbai0TRPnnE3XPiAKVd4r+duUDlBjmf4MDS+oS4hyh0CIna/RGAIDj+q
4JlBTlugRUQJzIQR153U13+WaPfaGb10AyTddUDQZ5M9BgkqbaihZ14Y
zIImTi8JYhJUXy3KhWGPjBqfpC5XzQvzQVv5Rps7twtnJdrW6DUPP2t6 4FzEV5J/tRM=";
};
```

Num mundo perfeito os servidores recursivos e *resolvers* terão apenas que confiar nas chaves do “.” (root) que irá ser disponibilizado em breve (anunciado para Julho de 2010), a validação é assim feita através de um ponto de confiança e enquanto a root não for assinada é possível validar através de outros pontos de confiança, como por exemplo do DLV do ISC, do ITAR da IANA ou directamente de TLDs que já se encontrem assinados como é o caso do .pt, .br, .se entre outros.

```
trusted-keys {
dlv.isc.org. 257 3 5 "BEAAAAPHMu/5onzrEE7z1egmhg/WPO0+ju
oZrW3euWEn4MxDCE1+1Ly2brhQv5rN32RKtMzX6Mj70jdzeND4XknW58
dnJNPCxn8+jAGl2FZLK8t+1uq4W+nnA3qO2+DL+k6BD4mewMLbIYFwe0
PG73Te9fZ2kJb56dhgMde5ymX4BI/oQ+cAK50/xvJv00FrF8kw6ucMTw
FlgPe+jnGxPPEmHate/URkY62ZfkLoBAADLHQ9Irs2tryAe7mbBZVcOw
IeU/Rw/mRx/vwwMCTgNboMQKtUdvNXDrYJDSHZws3xiRXF1Rf+a19UmZ
fSav/4NWLKjHzpT59k/VStTDN0YUuWrBNh";
};
```

Quando todas as máquinas passarem a validar DNSSEC e todos os domínios se encontrarem assinados é necessário realizar, de forma consciente, uma manutenção das assinaturas digitais para que as mesmas nunca expirem, pois caso tal aconteça os domínios em causa ficarão inacessíveis ao “mundo”, isto é, com se tivessem “desaparecido” e obtêm-se resultados DNS com respostas de SERVFAIL ou REFUSED.