



Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

DNSSEC

Declaração de Política e Procedimentos



Serviço de Registo de Domínios .PT

Julho de 2009

Índice

1. INTRODUÇÃO.....	6
1.1. ACERCA DO DNS .PT	6
1.2. ÂMBITO	7
1.3. CERTIFICAÇÃO E AUDITORIA.....	8
1.4. IDENTIFICAÇÃO DO DOCUMENTO	9
2. PARTICIPANTES NOS PROCEDIMENTOS DNSSEC DE .PT.....	10
2.1. PÚBLICO ALVO	10
2.2. INTERVENIENTES	10
2.2.1. FCCN / DNS .PT	10
2.2.2. TITULAR DO DOMÍNIO.....	11
2.2.3. ENTIDADE GESTORA	11
2.2.4. RESPONSÁVEL TÉCNICO	11
3. ÁREA DE RESPONSABILIDADE DO DNS .PT	12
3.1. ASSINATURA DA ZONA .PT	12
3.2. DELEGAÇÕES SEGURAS DE SUBDOMÍNIOS DA ZONA .PT	12
4. MEDIDAS DE SEGURANÇA NA GESTÃO E ARMAZENAMENTO DAS CHAVES	13
4.1. RESPONSABILIDADE DOS TÉCNICOS INTERVENIENTES	13
4.2. SEGURANÇA FÍSICA.....	13
5. GESTÃO E ARMAZENAMENTO DE CHAVES DA ZONA .PT.....	15
5.1. AMBIENTE TÉCNICO PARA A GERAÇÃO DE CHAVES.....	15
5.2. GERAÇÃO E ARMAZENAMENTO DAS CHAVES.....	15
5.2.1. ZSK – ZONE SIGNING KEY.....	15
5.2.2. KSK – KEY SIGNING KEY.....	16
5.3. TROCA DE CHAVES.....	17
5.3.1. ROTAÇÃO PROGRAMADA – ZSK.....	17
5.3.2. ROTAÇÃO PROGRAMADA – KSK.....	17
5.3.3. SUBSTITUIÇÃO DE CHAVES.....	18
5.3.4. PUBLICAÇÃO DE CHAVES DA ZONA .PT.....	19
6. ASSINATURA DA ZONA .PT	20
7. GESTÃO DAS CHAVES PARA SUBDOMÍNIOS	21
8. VERIFICAÇÃO DA RELAÇÃO ENTRE A CHAVE E O TITULAR DO DOMÍNIO	22
9. CONFORMIDADE LEGAL E ALTERAÇÕES.....	23
9.1. CONFORMIDADE LEGAL.....	23
9.2. ALTERAÇÕES A ESTE DOCUMENTO	23

Índice de Tabelas

TABELA 1 – VERSÃO DO DOCUMENTO	9
TABELA 2 – ROTAÇÃO PROGRAMADA DA ZSK.....	16
TABELA 3 – ROTAÇÃO PROGRAMADA DA KSK.....	17
TABELA 4 – SUBSTITUIÇÃO DE CHAVES	18
TABELA 5 – PROCEDIMENTO DE ASSINATURA DA ZONA .PT	20

Índice de Figuras

FIGURA 1 - CICLO DE VIDA DA CHAVE ZSK	17
FIGURA 2 - CICLO DE VIDA DA CHAVE KSK.....	18
FIGURA 3 – PROCESSO DE ASSINATURA DA ZONA .PT	20

Lista de Acrónimos e Abreviaturas

CCTLD	– Country Code Top Level Domain
DNS	– Domain Name System
DNSSEC	– Domain Name System Security Extensions
DS	– Delegation Signer
FCCN	– Fundação para a Computação Científica Nacional
FIPS	– Federal Information Processing Standard
HSM	– Hardware Security Module
IANA	– Internet Assigned Numbers Authority
ICANN	– Internet Corporation for Assigned Names and Numbers
ISC	– Internet Systems Consortium
ISP	– Internet Service Provider
KSK	– Key Signing Key
PKCS	– Public Key Cryptography Standards
TLD	– Top Level Domain
ZSK	– Zone Signing Key

1. Introdução

Existem cerca de mil milhões de utilizadores da Internet, o que equivale a uma taxa de penetração global de 15,4% (*Fonte: Marktest, 2008*).

Portugal apresenta um nível de penetração da Internet em lugares de topo mundial, com cerca de 4 milhões de utilizadores. Em 2009, sete em cada dez utilizadores portugueses acedem diariamente à Internet.

A Internet é hoje o meio que maior influência exerce na tomada de decisão dos consumidores que a utilizam cada vez mais para acessos a plataformas de comércio electrónico, home banking (visitas e operações em sites da Banca), ou seja, acessos que necessitam ter acrescidas preocupações de segurança.

Este documento contém a política e procedimentos de manuseamento de chaves utilizados pelo Serviço de Registo de Domínios .PT no âmbito do projecto DNSSEC (Domain Name System Security Extensions).

Neste contexto, o Serviço de Registo de Domínios .PT, de agora em diante referido como DNS .PT, cumprindo o seu importante papel de Registry do domínio de topo de Portugal (.PT), e com vista a garantir a autenticidade e integridade das consultas DNS efectuadas sobre domínios em .PT decidiu implementar as extensões de segurança ao protocolo DNS denominadas por DNSSEC.

Neste documento descrevem-se os intervenientes e respectivas áreas de responsabilidade, assim como os procedimentos e esquemas operacionais, relativos à implementação de DNSSEC pelo DNS .PT. Este documento pretende ser uma referência no cálculo do nível de confiança que o projecto DNSSEC do DNS .PT confere às várias entidades intervenientes nos processos descritos.

1.1. Acerca do DNS .PT

O DNS .PT, é uma unidade orgânica da FCCN – Fundação para a Computação Científica Nacional. Cabe à FCCN, no âmbito da delegação efectuada pela IANA – Internet Assigned Numbers Authority (RFC 1032, 1033, 1034 e 1591) a responsabilidade pela gestão, registo e manutenção de domínios sob o TLD (Top Level Domain) .pt, domínio de topo correspondente a Portugal.

O DNS .PT constitui um pilar fundamental da Comunidade Internet Portuguesa e tem como missão prestar um serviço de qualidade à mesma, garantindo uma correcta gestão técnica e administrativa do espaço de nomes sob .pt.

Desde que foi registado o primeiro domínio em .pt um longo caminho tem sido percorrido quer no número de nomes de domínio registados, evidência do crescimento da Internet em .pt, quer na importância crescente que a segurança do serviço tem vindo a assumir nas suas mais variadas vertentes. O nome de domínio constituiu um direito. O direito ao nome de domínio é um direito de uso exclusivo por parte do seu titular. O direito constitui-se pelo registo e permite ao seu titular ser identificado e distinguido dos demais no universo Internet. Ser titular de um nome de domínio é uma verdadeira mais valia e indispensável para qualquer projecto, serviço, empresa ou produto.

Para mais informações sobre o registo e gestão de nomes de domínio sob .pt, consulte o sítio de Internet em <http://www.dns.pt>.

1.2. Âmbito

O Domain Name System (DNS), criado em 1984, é uma das ferramentas fundamentais para o funcionamento da Internet que efectua a resolução de nomes de domínios em endereços IP (sejam eles em IPV4 ou IPV6) e vice-versa.

Este Sistema garante dois objectivos essenciais:

- A possibilidade que dá ao ser humano de se abstrair de endereços de rede (endereços IP) cuja memorização é complexa, ao mesmo tempo que permite alterações desses endereços IP sem que o utilizador tenha que conhecer essa alteração para continuar a usar um serviço;
- A garantia que as máquinas e os seus nomes sejam geridos de forma hierárquica e distribuída com o Root Server mundial no topo da hierarquia e com a informação distribuída por milhares de servidores de nomes existentes na Internet, pressuposto do seu sucesso enquanto rede global – não sendo necessário contactar uma entidade central sempre que se efectue uma alteração ou uma adição de novos dispositivos na Internet.

Este sistema que garante a disponibilidade e sucesso da Internet faz-se acompanhar porém, de algumas vulnerabilidades sempre que um utilizador pretende aceder a um serviço da Internet, nomeadamente a falta de confiança na autenticidade do site (aceder a um site forjado que erroneamente se apresenta como o original) e a falta de integridade dos dados transmitidos (corrupção dos dados enviados e recebidos pelos utilizadores sem conhecimento dos mesmos).

Com o crescimento da Internet e do número de utilizadores, as ameaças de segurança e a consciencialização dessa realidade têm vindo a ocupar um lugar de destaque nas preocupações por parte das entidades responsáveis por esta matéria. Por conseguinte a procura de soluções que garantam um ambiente mais seguro no serviço e na rede é uma preocupação mundial por parte dos especialistas.

Nesta sequência, em termos globais, foram criadas as condições necessárias para a adopção de mecanismos de segurança em torno do DNS. Como medida central identificou-se o DNSSEC – um conjunto de extensões de segurança adicionadas ao protocolo DNS que permitem a verificação da autenticidade e da integridade das respostas DNS e com o qual se pretende evitar a exploração das vulnerabilidades já referidas.

Na sequência dos desenvolvimentos internacionais, acompanhados de perto pelo DNS .PT e com o objectivo de obviar a eventuais tentativas de intrusão ou perturbações na correcta operação do DNS foram implementadas as normas DNSSEC com suporte NSEC3, integrando as respectivas extensões de segurança ao protocolo DNS no serviço de registo de domínios sob a designação .pt, prestado pelo DNS .PT, com vista a alcançar melhorias de segurança a nível da rede nacional e contribuindo, na sua medida, para uma Internet mais segura a nível global.

As extensões DNSSEC são baseadas em tecnologia de criptografia de chaves assimétricas, sendo utilizados dois tipos de chaves criptográficas: Zone Signing Key (ZSK) e Key Signing Key (KSK). Estas chaves serão posteriormente descritas em maior detalhe.

O suporte NSEC3 surgiu como complemento às extensões DNSSEC e tem como objectivo único não permitir o recurso a técnicas de “Zone Walking”, utilizadas abusivamente e com fins ilícitos para reconstruir a topologia e a infra-estrutura lógica de rede de uma organização.

1.3. Certificação e Auditoria

O procedimento de manuseamento de chaves adoptado será transposto para o do Sistema de Gestão da Qualidade do DNS que, no âmbito e no respeito da certificação ISO 9001:2000, será submetido a auditorias internas e de terceira parte com vista a determinar a conformidade das disposições planeadas e os requisitos da norma.

A adopção do DNSSEC no DNS.PT constitui ainda um pilar determinante na decisão sobre a eventual certificação ISO/IEC 27001 a qual consolida um conjunto das melhores práticas da gestão da segurança da informação assente em três pilares fundamentais, que têm vindo a ser as grandes preocupações do DNS.PT: confidencialidade, disponibilidade e integridade.

1.4. Identificação do documento

Este documento de Declaração de Política e Procedimentos DNSSEC é identificado pelos seguintes dados:

Versão do Documento:	0.7
Estado do Documento:	Aprovado
Data de Revisão:	8 de Julho de 2009
Número do Documento:	2009-07-08-0.7
Localização:	http://www.dnssec.pt/

Tabela 1 – Versão do Documento

2. Participantes nos Procedimentos DNSSEC de .pt

O DNS .PT assume a responsabilidade por este documento sendo a entidade emissora do mesmo, bem como a responsável pela implementação do DNSSEC no country code Top Level Domain (ccTLD) de .pt.

O DNS .PT é, ainda, a entidade competente para determinar a adequação e actualização dos procedimentos necessários a uma correcta política de segurança DNSSEC.

2.1. Público Alvo

Este documento descreve a política e procedimentos da operação das extensões de segurança DNSSEC no .pt, sendo o seu público alvo todos os administradores de zona com intenção de usar DNSSEC.

Este documento é relevante para:

- Titulares de nomes de domínio;
- Registrars (Agentes de Registo) que intervêm como gestores de nomes de domínio;
- Responsáveis técnicos que operam e administram tecnicamente os nomes de domínio;
- Operadores de Internet (ISP's – Internet Service Providers) que fornecem serviços DNS;
- Para os utilizadores de Internet que utilizam directa ou indirectamente os dados da zona .pt.

Assume-se que os destinatários são conhecedores dos conceitos: DNS, criptografia e infra-estruturas de chaves assimétricas assim como das extensões DNSSEC ao protocolo DNS mencionadas nos RFC 4033, 4034, 4035, 5155 e NSEC3 no RFC 5155.

Caso pretendam aprofundar os conhecimentos nas matérias acima referidas, recomenda-se a leitura atenta das definições constantes na página de Internet <http://www.dnssec.pt>.

2.2. Intervenientes

2.2.1. FCCN / DNS .PT

A Fundação para a Computação Científica Nacional - FCCN, é uma instituição privada sem fins lucrativos a quem incumbe a responsabilidade pela gestão, registo e manutenção de domínios de .pt. no âmbito da delegação efectuada pela IANA - Internet Assigned Numbers Authority (RFC 1032-4 e 1591).

2.2.2. Titular do Domínio

Pessoa singular ou colectiva que assume a titularidade do domínio/subdomínio. Compete-lhe a escolha do nome do domínio/subdomínio assumindo integralmente a responsabilidade pela mesma. O titular pode indicar uma entidade para gerir o respectivo processo de registo/manutenção, ou optar por assumir, ele próprio, essas tarefas. No caso de se tratar de pessoa colectiva, deve ainda indicar o nome completo de uma pessoa singular a contactar em caso de necessidade. Cabe ao titular proceder a todas as alterações aos dados fornecidos assim como à remoção do domínio/subdomínio.

2.2.3. Entidade Gestora

Responsável pela gestão do processo de registo/manutenção do domínio/subdomínio, tendo, em simultâneo, a responsabilidade administrativa e técnica deste. Nessa medida deverá fornecer o nome completo de uma pessoa a contactar em caso de necessidade, bem como os dados relativos às pessoas responsáveis pelas questões administrativas e técnicas. Como tal, é da sua exclusiva responsabilidade garantir que os dados dos responsáveis administrativo e técnico estão actualizados, não tendo a FCCN qualquer tipo de responsabilidade por dificuldades de contacto resultantes da não actualização destes dados. A entidade gestora poderá ser uma entidade com estatuto de agente de registo (registrar) junto da FCCN, conforme lista disponível em <http://www.dns.pt>.

2.2.4. Responsável Técnico

Representante da entidade gestora indicado para o tratamento das questões de índole técnica. Cabe-lhe a administração técnica dos nomes dentro do domínio/subdomínio, responsabilizando-se pelo comportamento das máquinas e servidores do mesmo. Deverá ter conhecimentos técnicos, disponibilidade para receber e avaliar relatórios sobre problemas e, se for o caso, tomar as acções necessárias para os resolver. O responsável técnico será devidamente notificado dos problemas de natureza técnica que decorram do processo de registo/manutenção do domínio/subdomínio. Deverá ser possível contactar o responsável técnico através contacto de email indicado para o efeito.

3. Área de responsabilidade do DNS .PT

3.1. Assinatura da zona .pt

O DNS .PT é responsável pela gestão dos nomes de domínios delegados na zona .pt, ou seja, é a entidade a quem incumbe a gestão, registo e alteração das delegações associadas a um nome de domínio do ccTLD de .pt.

A zona .pt é assinada regularmente, por chaves que são geradas e manuseadas pelo DNS .PT. O processo de assinatura decorre automaticamente no seguimento do processo de geração do ficheiro de zona.

3.2. Delegações seguras de subdomínios da zona .pt

O resumo da chave pública da KSK de cada subdomínio é assinado regularmente pelo DNS .PT com a ZSK activa da zona .pt. Os algoritmos utilizados para gerar resumos são primeiramente SHA-1 e SHA-256. Outros algoritmos poderão vir a ser utilizados. O resumo assinado é publicado na zona .pt em forma de resource record do tipo DS (Delegation Signer).

As chaves correspondentes aos subdomínios da zona .pt devem ser criadas pelo titular desse domínio que as identifica como sendo dele ou por um terceiro a quem foi delegada a responsabilidade de administração dos dados da chave da zona, como acontece com o Responsável Técnico e /ou Entidades Registrars.

O DNS .PT só assina resource records DS correspondentes a subdomínios da zona .pt.

As zonas abaixo de .pt são responsáveis pela gestão dos respectivos subdomínios efectuando delegações, alterações e assinaturas dos mesmos.

Uma cadeia de segurança é estabelecida a partir do momento que a entidade gestora responsável por um determinado subdomínio adere ao DNSSEC, isto é, quando o resource record DS do domínio respectivo, foi devidamente transmitido ao DNS .PT, e a delegação do mesmo se encontra devidamente publicada e assinada, na zona de .pt.

4. Medidas de Segurança na gestão e armazenamento das Chaves

No quadro da operação do DNSSEC a protecção das chaves KSK e ZSK é uma prioridade garantida pela adopção das melhores práticas internacionais e, sempre que possível, dos standards.

De entre as medidas implementadas destacam-se a utilização de equipamento certificado com a norma FIPS 140-2 de nível 4 e a criação de um ambiente isolado para gestão e armazenagem da chave KSK.

4.1. Responsabilidade dos Técnicos intervenientes

A intervenção humana no processo de geração de chaves e de assinatura da zona .pt é efectuada por colaboradores designados pelo Conselho Executivo da FCCN para exercer estas funções, com os conhecimentos e as capacidades técnicas e humanas comprovadas e com garantias de total isenção e confidencialidade.

Todas as operações de manuseamento de chaves são obrigatoriamente realizadas conjuntamente por um mínimo de dois colaboradores.

4.2. Segurança Física

O processo de geração das chaves é, obrigatoriamente, efectuado directamente num módulo criptográfico em hardware designado HSM (Hardware Security Module), existindo sempre, pelo menos, uma cópia de segurança numa entidade externa devidamente certificada conforme a norma de Qualidade ISO 9001 para a prestação de serviços de transporte, guarda e tratamento de valores, especializada na salvaguarda de informação sensível e privada. Desta forma todas as cópias de segurança possuem o mesmo nível de segurança que a chave original.

O HSM adoptado possui características específicas para a função de gestão de chaves, tais como, a certificação em consonância com a norma FIPS 140-2, a destruição automática das chaves em resposta a uma exposição adulterada das mesmas, entre outras certificações e características. A FIPS 140-2 é uma norma estabelecida pelo Governo Norte-Americano que contém os requisitos essenciais de segurança que os produtos tecnológicos com informação sensível e secreta devem respeitar.

Prevê-se a existência de três níveis de segurança física com diferentes mecanismos de controlo de acessos:

1º nível: Acesso condicionado a colaboradores devidamente autorizados e registo individual de entradas e saídas. As instalações e respectivos acessos garantem um nível de segurança necessário e adequado, incluindo segurança física, detecção contra intrusão e videovigilância, As instalações dispõem de

sistemas de alimentação ininterrupta com a potência suficiente para manter autonomamente a rede eléctrica durante longos períodos de falta de corrente e para proteger os equipamentos face a flutuações eléctricas que os possam danificar. As instalações possuem ainda condições de segurança contra a exposição a água, incêndios e outro tipo de cataclismos.

2º nível: Controlo de acessos restrito a colaboradores designados para o exercício das funções técnicas do DNS.PT, com recurso a um token de segurança distinto daquele que é usado para acesso ao 1º nível. Esta zona de segurança contém o hardware de suporte ao DNS.PT e inclui protecção anti-roubo.

3º nível: Controlo de acessos restrito a colaboradores designados para o exercício de funções de gestão do DNSSEC.

As instalações remotas que possuem as cópias de segurança das chaves são geograficamente separadas e as condições de segurança são idênticas ou superiores às existentes no local principal do DNS .PT.

5. Gestão e armazenamento de chaves da zona .pt

A geração dos pares de chaves é processada de acordo com os requisitos e algoritmos definidos nesta política.

5.1. Ambiente técnico para a geração de chaves

As chaves ZSK e KSK do DNS .PT são geradas por um HSM utilizando a ferramenta dnssec-keygen incluída no ISC (Internet Systems Consortium) BIND¹ a partir da versão 9.6.

As chaves ZSK e KSK são administradas por meio de PKCS #11 (Public Key Cryptography Standards) entre uma máquina dedicada e o HSM. Este último para além da geração e de armazenamento de chaves, providencia ainda rapidez no processamento criptográfico evitando assim a sobrecarga computacional dos servidores.

5.2. Geração e armazenamento das chaves

Esta secção descreve os procedimentos usados para geração e armazenamento de chaves.

5.2.1. ZSK – Zone Signing Key

A ZSK, como o nome indica, é a chave utilizada para assinar zonas DNS, especificamente a zona .pt. Este processo ocorre sempre que se efectua uma actualização ou geração de um novo ficheiro de zona. Esta chave, como anteriormente mencionado é gerada pelo HSM e armazenada pelo próprio. Para além da versão original da chave que se encontrará armazenada no HSM é efectuada uma cópia de backup da ZSK para um token de segurança (dispositivo electrónico seguro que armazena as chaves e que possui suporte para vários algoritmos de criptografia) permitindo a existência, por razões de segurança, de uma cópia de reserva da chave (no HSM e no token seguro e encriptado).

O token de segurança com a cópia de reserva da chave KSK fica à responsabilidade da entidade externa referida no ponto 4. pela qual o token é transportado para local seguro.

Para a geração da ZSK é utilizado o algoritmo RSASHA1 para NSEC3 com dimensão de 1024 bits.

A substituição programada da ZSK ocorre em respeito pelo procedimento descrito na Tabela 2.

¹ <http://www.isc.org>

Procedimento: Rotação Programada da ZSK

Intervenientes: A intervenção humana no processo de geração da chave ZSK da zona .pt é efectuada por dois colaboradores autorizados.

Passos:

- ⇒ A ZSK é gerada no HSM (**ZSK 2**);
- ⇒ Na geração de zona seguinte após a geração da nova chave passa a ser utilizada esta chave para assinar a zona removendo qualquer referência à ZSK (**ZSK 1**) utilizada anteriormente.
- ⇒ A chave é armazenada no HSM;
- ⇒ É efectuada uma cópia de segurança num token seguro;
- ⇒ É realizada a entrega do token seguro com a cópia da ZSK (**ZSK 2**) à entidade externa responsável pela salvaguarda da mesma.

Tabela 2 – Rotação Programada da ZSK

5.2.2. KSK – Key Signing Key

A chave KSK é aposta a um resource record do tipo DNSKEY e é utilizada para assinar o conjunto de resource records DNSKEY que possuem a informação de todas as chaves contidas na zona, designadamente a ZSK.

Uma vez que a KSK assina menos dados da zona, o seu tempo de vida de utilização pode ser mais extenso até à criação de uma nova chave. Esta é constituída por um par de chaves assimétricas a parte pública da chave é aquela que é publicada e comunicada pelos utilizadores da Internet, estabelecendo desta forma uma cadeia de confiança entre as várias hierarquias presentes no DNS.

A chave KSK para além de armazenada no HSM é ainda salvaguardada num token de segurança permitindo, tal como efectuado no caso da ZSK a existência de uma cópia de reserva da chave (no HSM e no token seguro e encriptado).

O token de segurança com a cópia de reserva da chave KSK fica à responsabilidade da entidade externa referida no ponto 4. pela qual o token é transportado para local seguro.

Para a geração da KSK é utilizado o algoritmo RSASHA1 para NSEC3 com dimensão de 1280 bits.

A substituição programada da KSK ocorre uma vez por ano, tal como se observa no procedimento da Tabela 3.

Procedimento: Rotação Programada da KSK

Intervenientes: A intervenção humana no processo de geração da chave KSK da zona .pt é efectuada por dois colaboradores autorizados.

Passos:

- ⇒ É gerada no HSM uma nova KSK (**KSK 2**);
- ⇒ Na geração de zona seguinte a ocorrer após a geração da nova chave passa a ser utilizada esta nova chave para assinar a zona para além da KSK vigente (**KSK 1**).
- ⇒ A chave é armazenada no HSM;
- ⇒ É efectuada uma cópia de segurança num token seguro;
- ⇒ É realizada a entrega do token seguro com a cópia da KSK à entidade externa responsável pela salvaguarda da mesma;
- ⇒ Passados 6 meses de utilização desta nova chave é realizada uma actualização onde é removida da zona a chave que se encontrava anteriormente em vigor (**KSK 1**) e todas as referências da mesma, passando a haver apenas uma chave KSK (**KSK 2**) na zona .pt .

Tabela 3 – Rotação Programada da KSK

5.3. Troca de chaves

5.3.1. Rotação Programada – ZSK

Trimestralmente, como se observa na Figura 1, e em consonância com o procedimento descrito na Tabela 2, ocorre a Rotação Programada da ZSK:

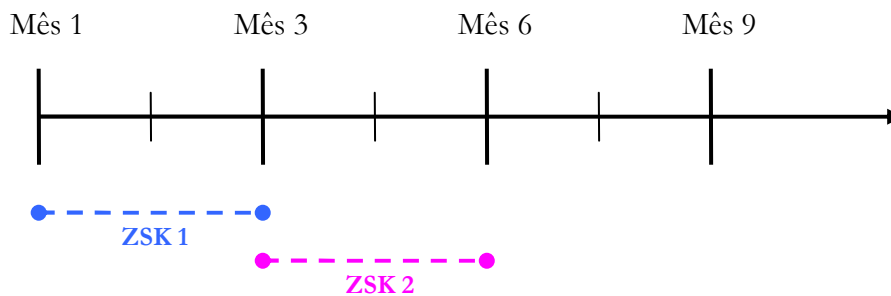


Figura 1 - Ciclo de Vida da chave ZSK

5.3.2. Rotação Programada – KSK

As KSK são validadas de 18 meses em 18 meses. Isto significa que existem chaves cuja data de

expiração se sobrepõe por 6 meses como se observa na Figura 2 e respeitando o procedimento descrito na Tabela 3:

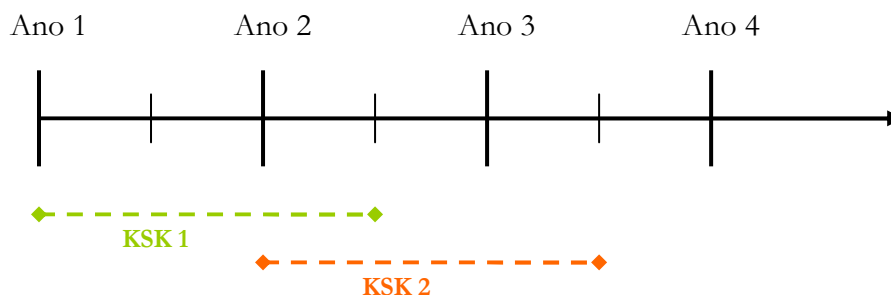


Figura 2 - Ciclo de Vida da chave KSK

5.3.3. Substituição de chaves

A substituição de emergência de uma chave ZSK e KSK poderá ser necessária se a componente chave privada ficar comprometida. Uma chave comprometida significa que o DNS .PT não garante o controlo da chave privada por perda, furto, cópia, reconstrução por criptografia (análise criptográfica, procura exaustiva) ou outro método não mencionado.

Se pelo menos uma das chaves da zona .pt ficar comprometida, a sua utilização será, de imediato, descontinuada. Uma nova ZSK ou KSK é imediatamente gerada e publicada com a máxima brevidade.

Procedimento: Substituição de Chaves

Intervenientes: A intervenção humana no processo de geração da chave ZSK da zona .pt é efectuada por dois colaboradores autorizados.

Passos:

- ⇒ Geração da nova chave que se encontra actualmente comprometida (ZSK ou KSK);
- ⇒ É realizada uma geração de zona forçada onde é efectuada a utilização da nova chave para assinar a zona.
- ⇒ A chave é armazenada no HSM;
- ⇒ É realizada uma cópia de segurança num token seguro;
- ⇒ É realizada a entrega do token seguro com a cópia da chave à entidade externa responsável pela salvaguarda da mesma.

Tabela 4 – Substituição de Chaves

5.3.4. Publicação de chaves da zona .pt

Toda a informação com respeito à actualização e substituição das chaves da zona .pt é comunicada via mailing list pelo endereço de email info@dnssec.pt.

É da responsabilidade das partes interessadas subscrever este canal de comunicação para garantir que possuem sempre a informação actualizada. A informação é ainda publicada e actualizada na página de Internet em <http://www.dnssec.pt>. Esta página manterá um histórico de todas as trocas de chave efectuadas.

Enquanto a zona raíz (. ou root) não for assinada será necessário submeter a informação da chave pública do .pt num repositório de chaves seguro e de confiança. Este tipo de repositório designa-se de TAR (Trust Anchor Repository) que consiste na partilha de informação de chaves por forma a realizar-se verificação DNSSEC entre os domínios de topo.

Para além do ITAR (Interim Trust Anchor Repository) gerido pela IANA ainda em versão beta outro tipo de TAR é o DLV (DNSSEC Look-aside Validation), cujo responsável pela gestão é o ISC, mais informação poderá ser consultada em <https://itar.iana.org/> e <https://dlv.isc.org/>, respectivamente.

6. Assinatura da zona .pt

O processo de assinatura da zona .pt é efectuado com base ZSK e encontra-se integrado com o processo normal de geração de zona:

Procedimento: Geração e assinatura da zona .pt

Intervenientes: Este processo não exige intervenção humana sendo gerado de forma automática.

Passos:

- ⇒ O ficheiro de zona é gerado de acordo com a informação de zona contida na base de dados;
- ⇒ O ficheiro de zona gerado é transferido para a máquina responsável por administrar a zona;
- ⇒ Nesta máquina é efectuada a validação do ficheiro de zona e este é transferido para a máquina responsável por assinar a mesma.
- ⇒ A máquina responsável por assinar a zona utiliza a chave ZSK activa assinando a zona;
- ⇒ A zona já assinada é copiada novamente para a máquina de administração da mesma;
- ⇒ Após a validação do ficheiro já assinado a nova zona é enviada para o servidor de nomes primário de .pt que por sua vez efectua a distribuição da zona pelos restantes servidores de nomes secundários.

Tabela 5 – Procedimento de assinatura da zona .pt

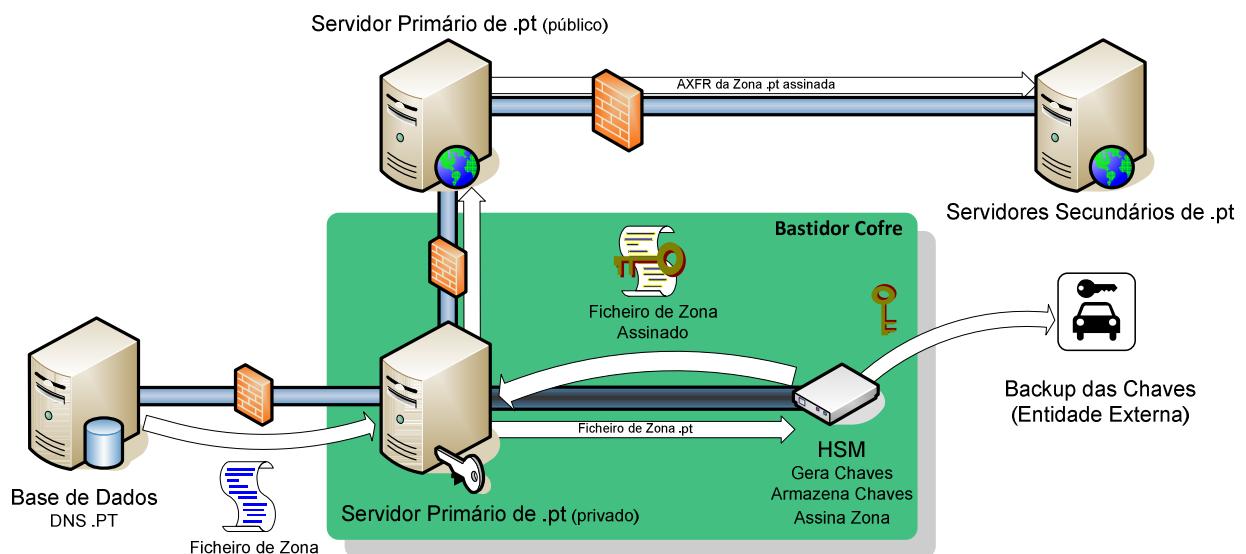


Figura 3 – Processo de assinatura da zona .pt

7. Gestão das chaves para subdomínios

O DNS .PT não assume qualquer responsabilidade pela gestão e mecanismos de segurança relacionados com a gestão das chaves utilizadas nas respectivas zonas dos domínios delegados na zona .pt, isto é, nos subdomínios que não são da sua titularidade.

A entidade titular de cada domínio delegado na zona .pt assume a responsabilidade pela geração de chaves e publicação das mesmas no DNS bem como pela sua gestão de forma segura, aconselhando-se a utilização das boas práticas referidas neste documento para a zona .PT. O titular pode delegar a responsabilidade de administração dos dados da chave da zona a terceiros, como acontece com o papel do Responsável Técnico e/ou Entidade Gestora, podendo esta ser ou não, uma Entidade Registrar.

Se a chave de um subdomínio é divulgada, importa que o resumo da sua chave pública e que consta na zona .pt seja actualizado. A actualização é efectuada através da publicação do novo resource record DS de acordo com os procedimentos vigentes no DNS .PT à data.

8. Verificação da relação entre a chave e o titular do domínio

O DNS .PT utiliza o seguinte procedimento de verificação da ligação entre uma chave pública e o titular de um nome de domínio.

1. A entidade gestora em representação do titular subscreve um contrato disponível on-line em <http://www.dnssec.pt> com o DNS .PT relativo ao projecto DNSSEC de .pt para um determinado domínio e especifica quem é contacto técnico para esse domínio incluindo a informação de contacto do mesmo.
2. A entidade gestora deve verificar se a informação especificada no acordo corresponde à informação que se encontra no sistema DNS .PT de gestão online.
3. O contacto técnico acede ao interface de gestão online do DNS .PT no qual administra o resource record DS para o nome de domínio em questão.
4. Com a adesão ao DNSSEC, o titular de um nome de domínio pode fazer disso publicidade nos serviços que utiliza com base no mesmo (sitio, correio electrónico, etc).

9. Conformidade legal e alterações

9.1. Conformidade legal

É responsabilidade do DNS .PT zelar pelo cumprimento de disposições legais ou normas internacionais sobre esta matérias.

9.2. Alterações a este documento

É responsabilidade do DNS .PT realizar e aprovar mudanças nesta política de procedimentos de acordo com as melhores práticas internacionais nesta matéria.

Sempre que tal acontecer este documento terá uma nova versão e será devidamente publicado na página de Internet <http://www.dnssec.pt>.