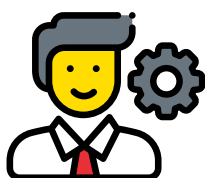
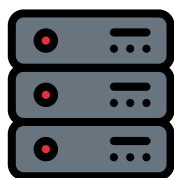


GUÍA DE IMPLANTACIÓN Y BUENAS PRÁCTICAS DE DNSSEC



www.incibe.es

INSTITUTO NACIONAL
DE CIBERSEGURIDAD

SPANISH NATIONAL
CYBERSECURITY INSTITUTE

 **incibe**__

INSTITUTO NACIONAL DE CIBERSEGURIDAD



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA
Y EMPRESA

Octubre 2018

INCIBE_GUIA_BUENAS_PRACTICAS_DNSSEC_2018_v1.1

La presente publicación pertenece a INCIBE (Instituto Nacional de Ciberseguridad) y está bajo una licencia Reconocimiento-No comercial 3.0 España de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- Reconocimiento. El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INCIBE o INCIBE-CERT como a su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE-CERT como titular de los derechos de autor. Texto completo de la licencia: <https://creativecommons.org/licenses/by-nc-sa/3.0/es/>

ÍNDICE

ÍNDICE	3
ÍNDICE DE FIGURAS	4
ÍNDICE DE TABLAS	5
1. Sobre esta guía	6
2. Introducción	7
2.1. DNSSEC: seguridad para el servicio DNS.....	7
2.2. Situación actual de DNSSEC	7
3. Elementos clave para la implantación de DNSSEC	9
3.1. Ámbito de aplicación del servicio DNSSEC	9
3.2. Alcance del servicio DNSSEC	10
3.3. Modelo de gestión del servicio DNS	11
3.3.1. Gestión externa del servicio DNS	11
3.3.2. Gestión propia del servicio DNS	14
3.4. Nivel de automatización esperado del servicio DNSSEC	14
3.5. Nivel de seguridad requerido para las claves	15
3.6. Requisitos y necesidades en los sistemas de información y comunicaciones	16
3.7. Valoración coste/beneficio.....	18
3.7.1. Resolver	18
3.7.2. Servidor DNS autoritativo.....	19
4. Recomendaciones de diseño	20
4.1. Políticas y procedimientos de seguridad y gestión de DNSSEC	20
4.1.1. Selección de los algoritmos de firma.....	22
4.1.2. Longitud de las claves criptográficas.....	26
4.1.3. Parámetros asociados a la validez de las firmas.....	28
4.1.4. Generación y almacenamiento de las claves criptográficas	33
4.1.5. Firmado y publicación de zonas DNS con autoridad	34
4.1.6. Selección del software del servidor de DNSSEC	38
4.1.7. Utilización y validación de registros DNSSEC	38
4.1.8. Mecanismo de renovación de las claves (<i>key rollover</i>).....	40
4.1.9. Generación de documentación para el despliegue de DNSSEC	44
4.2. Transferencia de una zona firmada a otro proveedor	46
4.3. Monitorización de DNSSEC.....	47
4.4. Resumen de las recomendaciones de diseño de DNSSEC.....	48
5. Migración y coexistencia de DNS y DNSSEC	50
5.1. Transición de DNS a DNSSEC.....	50
5.2. Recomendaciones de seguridad	50
5.2.1. Transición de zonas con autoridad de DNS a DNSSEC.....	50
5.2.2. Transición de <i>resolvers</i> de DNS a DNSSEC	51
6. Implantación	53
6.1. Servidores DNSSEC autoritativos	53
6.1.1. Activación de DNSSEC en el servidor DNS autoritativo	54
6.1.2. Selección de los algoritmos de firma y características criptográficas	54
6.1.3. Generación de las claves KSK y ZSK y firmado de la zona	54
6.1.4. Publicación de las claves	60
6.1.5. Proceso de firma de zonas DNS con autoridad.....	61
6.1.6. Establecimiento de cadenas de confianza	67

6.1.7. Comprobación del servicio DNSSEC	68
6.1.8. Transferencias de zona DNS con DNSSEC activo.....	70
6.1.9. Actualizaciones dinámicas en zonas DNS con DNSSEC activo.....	71
6.1.10. Notificaciones DNS con DNSSEC activo.....	73
6.2. Resolvers DNSSEC.....	74
6.2.1. Resolvers recursivos.....	74
6.2.2. Comprobación de la validación mediante DNSSEC	75
6.3. Despliegue de arquitecturas DNS <i>split-view</i> con DNSSEC.....	76
6.4. Resumen de las buenas prácticas en la implantación de DNSSEC.....	76
7. Operación.....	77
7.1. Servidores DNSSEC autoritativos	77
7.2. Recomendaciones del ciclo de vida de las claves en DNSSEC.....	77
7.2.1. Clave ZSK.....	78
7.2.2. Clave KSK	78
7.3. Alternativas de gestión y firmado de la zona	79
7.3.1. Esquema de gestión y renovación de las claves con BIND.....	80
7.4. Sustitución de los algoritmos de firma y características criptográficas.....	84
7.5. Proceso de refirmado de zonas DNS con autoridad	85
7.5.1. Refirmado manual.....	85
7.5.2. Refirmado automático	86
7.6. Resolvers DNSSEC.....	86
7.7. Monitorización del entorno	86
7.7.1. Detección de problemas	87
7.8. Procedimientos de emergencia	90
7.8.1. Renovación de claves ante una emergencia.....	90
7.8.2. Problemas de resolución de la zona	91
7.9. Resumen de las buenas prácticas en la operación de DNSSEC	93
8. Glosario de términos y acrónimos	95
9. Anexo: Registros CDS y CDNSKEY.....	98
10. Referencias	99

ÍNDICE DE FIGURAS

Figura 1 - Panel de control de un proveedor con parametrización de DNSSEC	13
Figura 2 - Panel de control de un proveedor sin parametrización DNSSEC	13
Figura 3 - Firmado digital	21
Figura 4 - Comando para obtener los números de algoritmo de los registros DS de la zona raíz..	24
Figura 5 - Comando para obtener los TLDs de nivel 1 con registro DS de tipo ECDSA.....	25
Figura 6 - Porcentaje de dominios para cada algoritmo de firma en la zona ".nl"	26
Figura 7 - Tiempos de validez de la firma de un registro en DNSSEC.....	29
Figura 8 - Ejemplo de cálculo del periodo de validez efectivo (lifetime) de un RRSIG.....	31
Figura 9 - Firmado online con servidor maestro primario (1) y con servidor maestro oculto (2)	36
Figura 10 - Ciclo de vida de una clave en DNSSEC.....	41
Figura 11 - Comandos BIND para generar las claves DNSSEC: ZSK y KSK	56
Figura 12 - Fichero con la clave pública ZSK ("key").....	58
Figura 13 - Comandos BIND para generar las claves DNSSEC en un HSM: ZSK y KSK.....	60
Figura 14 - Formato de los registros DNSKEY publicados en la zona	60
Figura 15 - Verificación mediante dnssec-verify del fichero de la zona firmada.....	62
Figura 16 - Opción para establecer los periodos de expiración y refresco.....	62
Figura 17 - named.conf: opciones para la gestión y el firmado manual de la zona.....	63
Figura 18 - Comando BIND para firmar una zona manualmente	63

Figura 19 - named.conf: referencia al fichero con el firmado manual de la zona	63
Figura 20 - named.conf: opciones para la gestión y el firmado automático de la zona.....	64
Figura 21 - Firmado de la zona mediante dnssec-signzone	64
Figura 22 - Opciones de configuración de firmado inline en named.conf (caso 1).....	66
Figura 23 - Opciones de configuración de firmado inline en named.conf (caso 2.1).....	66
Figura 24 - Opciones de configuración de firmado inline en named.conf (caso 2.2).....	66
Figura 25 - Firma inline de la zona con BIND en el servidor intermedio (caso 2.1)	67
Figura 26 - Comando named-checkzone para verificación de una zona firmada	67
Figura 27 - Generación del registro DS correspondiente a la clave KSK con BIND	68
Figura 28 - Generación del registro DS correspondiente a la clave KSK con PowerDNS	68
Figura 29 - Ejemplo de validación de un dominio mediante DNSSEC Analyzer (Verisign).....	69
Figura 30 - Ejemplo de consulta de registros DNSSEC de una zona mediante "dig"	70
Figura 31 - Creación de claves en DNSSEC para actualizaciones DNS dinámicas	72
Figura 32 - named.conf: clave (pública) secreta para actualizaciones DNS dinámicas	72
Figura 33 - Opciones de configuración de BIND para permitir actualizaciones DNS dinámicas	73
Figura 34 - Opción para activar la validación DNSSEC en un servidor DNS recursivo BIND con actualización automática del trust-anchor	74
Figura 35 - Ejemplo de validación de respuestas DNSSEC de una zona mediante "dig"	75
Figura 36 - Configuración del proceso de renovación de claves a través de dnssec-keymgr	83
Figura 37 - Comprobación de las claves usadas para la firma de una zona DNSSEC.....	87
Figura 38 - Ejemplo de error en el syslog por fallo de validación de la cadena de confianza	88
Figura 39 - Ejemplo de error en el syslog debido a firma expirada	89
Figura 40 - Ejemplo de error en el syslog debido a firma aún no válida.....	89
Figura 41 - Uso de "delv" para identificar fallos en DNSSEC	90
Figura 42 - Uso de NTAs en BIND: creación, listado y borrado	93

ÍNDICE DE TABLAS

Tabla 1 - Algoritmos criptográficos válidos para los registros asociados al proceso de firmado de zona en DNSSEC.....	23
Tabla 2 - Algoritmos de firma empleados en la zona raíz para los diferentes TLDs de primer nivel de DNSSEC.....	25
Tabla 3 - Propósito de los metadatos de tiempo de la clave en el ciclo de vida de DNSSEC	42
Tabla 4 - Recomendaciones criptográficas y de renovación para las claves DNSSEC	48
Tabla 5 - Recomendaciones de longitud y lifetime de las claves DNSSEC	49
Tabla 6 - BIND: generación de una clave ZSK de respaldo	80
Tabla 7 - BIND: generación de claves para gestión manual automatizada	81

1. SOBRE ESTA GUÍA

El objeto de la presente guía es proporcionar las recomendaciones técnicas generales necesarias para la correcta implantación de DNSSEC en una zona DNS ya operativa, profundizando en las estrategias y pasos a seguir para una correcta puesta en marcha de la solución.

La conveniencia de su elaboración surge de las conclusiones obtenidas en el "Estudio del estado de DNSSEC en España" publicado por INCIBE [Ref.- 1] en 2018, que mostró un bajo nivel de implantación del servicio DNSSEC en España, y pretende ofrecer unas pautas operativas que simplifiquen su despliegue, poniéndolo al alcance de cualquier organización que desee incorporarlo como una medida más de seguridad de su entorno tecnológico.

Para ello, se abordarán detalladamente una serie de áreas conceptuales, que irán desde el diseño hasta la implantación y posteriores tareas de gestión y operación de la zona con DNSSEC. Pese a que algunos elementos puedan parecer conceptualmente complejos, la guía pretende demostrar que la operativa de DNSSEC puede automatizarse enormemente en base a las herramientas existentes a día de hoy, simplificando todos los procesos.

El propósito no es realizar una configuración completa de DNSSEC para una plataforma concreta, una versión de sistema operativo específica o un software servidor DNS particular, sino detallar todos los elementos que deben abordarse durante la implementación, independientemente de la plataforma y el software empleado.

No obstante, dado que sí se aborda la implantación desde un punto de vista práctico, se ilustrará con ejemplos concretos las recomendaciones proporcionadas en aquellos apartados donde se considere necesario. Estos ejemplos tienen carácter didáctico, pero no están necesariamente adaptados a un escenario concreto o configuración particular.

Se ha seleccionado BIND como software DNS de referencia por su carácter gratuito, de código abierto, y que ofrece tanto procedimientos automáticos de gestión como mecanismos granulares que permiten ilustrar los distintos conceptos que se expondrán a lo largo de los diferentes apartados que conforman esta guía.

Las recomendaciones ofrecidas a lo largo de la presente guía deberían complementarse con las descritas en la "Guía de seguridad en servicios DNS" publicada por INCIBE [Ref.- 2], que proporciona mecanismos para incrementar la seguridad en el protocolo DNS.

De cara a la lectura de la presente guía y su formato, conviene saber que:

- Los términos anglosajones se presentan en *letra cursiva*, acompañados de sus equivalentes en castellano; éstos últimos se usarán a menos que no exista una equivalencia adecuada en lenguaje técnico.
- Los términos y expresiones en **letra negrita** corresponden a conceptos clave de DNSSEC que se desea resaltar en los apartados en que aparecen.
- Las referencias con formato "[Ref.- nn]" son enlaces a referencias bibliográficas relevantes en las que se puede consultar y ampliar la información proporcionada.
- Las referencias a pie de página corresponden a comentarios, referencias puntuales o aclaraciones sobre la información a la que acompañan.
- Los términos en fuente de letra `Courier` corresponden a comandos Unix/Linux y a sus parámetros específicos.

2. INTRODUCCIÓN

El protocolo DNS surgió en los orígenes de Internet para resolver la problemática de la escalabilidad de la traducción entre las direcciones IP manejadas por los elementos integrantes de la red y los nombres de servicios y sistemas manejados por los humanos, y no fue diseñado desde el punto de vista de la seguridad. Por este motivo, su implementación es extremadamente sensible a todo tipo de ataques, tanto dirigidos a los servidores como al protocolo, que han sido puestos de manifiesto a lo largo de los años en forma de incidentes de seguridad que han supuesto enormes pérdidas económicas y de prestigio para muchas organizaciones. Muchos de estos ataques se basan en técnicas de tipo "*Man-in-the-Middle* (MitM)", debido a que DNS se asienta sobre el protocolo de transporte UDP y a que no incorpora técnicas para verificar la autenticidad de la fuente de los mensajes ni la integridad de los mismos.

Una de las principales amenazas sobre el protocolo DNS consiste en que un atacante pueda contaminar la caché de un servidor de nombres recursivo (*recursive resolver*) falseando la dirección IP de un sitio web para redirigir al usuario a un servidor fraudulento controlado por dicho atacante, con el fin de obtener datos de acceso que puedan ser empleados posteriormente en el servicio legítimo con diversos fines. Este tipo de ataque, conocido como envenenamiento de caché DNS (*DNS cache poisoning*) se hizo especialmente popular a raíz de una investigación revelada por Dan Kaminsky en 2008 [Ref.- 3], en la que se detallaba un posible mecanismo para explotar la vulnerabilidad del protocolo de forma masiva.

2.1. DNSSEC: seguridad para el servicio DNS

DNSSEC, siglas de *Domain Name System Security Extensions* (extensiones de seguridad para el sistema de nombres de dominio), no surgió como un protocolo que reemplazase a DNS, sino como un conjunto de técnicas que permitiesen añadir autenticidad (garantía sobre el origen de los mensajes) e integridad (garantía de no alteración de los mensajes) al servicio de resolución de nombres existente, a través de un mecanismo de firmado basado en una cadena de confianza (originada en un *trust-anchor*). No es, por tanto, un protocolo en sí mismo, aunque a lo largo del presente estudio se podrá utilizar ese término por simplicidad. DNSSEC no proporciona mecanismos de cifrado.

Los orígenes de DNSSEC no son recientes, pues el primer RFC que lo aborda directamente es el 2065 [Ref.- 4], del año 1997, que fue evolucionando hasta dar lugar al RFC 4035 [Ref.- 5] y que sigue ampliándose en la actualidad, aunque fue la investigación de DNS *cache poisoning* de Dan Kaminsky la que alertó seriamente sobre la necesidad de su implantación.

Para obtener más detalles técnicos sobre la justificación y el propio diseño de DNSSEC, se recomienda la lectura del "Estudio del estado de DNSSEC en España" [Ref.- 1].

2.2. Situación actual de DNSSEC

Como reveló el "Estudio del estado de DNSSEC en España" [Ref.- 1], las condiciones tanto de infraestructura como técnicas existentes a día de hoy son propicias para el despliegue masivo de DNSSEC: el firmado de la zona raíz y de la mayor parte de los dominios de primer nivel (TLDs) está operativo desde hace años, muchos agentes registradores ya

ofrecen a sus clientes soporte para DNSSEC y el software que se requiere ya tiene un nivel de madurez suficiente.

Sin embargo, las estadísticas de implantación demuestran que solo un pequeño porcentaje de los dominios DNS están firmados con DNSSEC (en torno al 0,65% para ".com", al 0,9% para ".net" y al 0,84% para ".es").

Entre las razones subyacentes a estas cifras, se pueden encontrar el temor a incurrir en costes que no tengan un retorno de inversión directo, así como un desconocimiento a nivel técnico que dificulta la implantación y genera incertidumbre sobre las consecuencias de efectuar un despliegue fallido.

Evaluar las pérdidas que puede suponer un incidente de seguridad que podría haberse evitado con la puesta en marcha de DNSSEC no siempre es factible, especialmente porque las organizaciones afectadas no suelen revelar detalles, y las que aún no han sido objeto de uno, carecen de elementos cuantificables, de ahí que fijar un valor para la prevención, aun resultando necesario, no es habitual.

Sin embargo, se constata que el despliegue en países europeos como Holanda, Suecia y República Checa ha sido exitoso, con un amplio firmado de sus zonas de segundo nivel y una elevada tasa de validación de las transacciones DNSSEC en sus *resolvers*, lo cual pone de manifiesto la viabilidad técnica de la solución. Ello, unido a que los beneficios de DNSSEC desde el punto de vista de la seguridad son relevantes, debería redundar en una adopción más significativa por parte de la comunidad de Internet.

DNSSEC no es efectivo si no se implanta de manera global en todos los dominios y *resolvers*, de ahí que sea preciso concienciar a todos los agentes implicados (proveedores de servicios o ISPs, agentes registradores, propietarios de dominios y operadores de zona y de servidores caché recursivos) sobre su importancia y necesidad.

3. ELEMENTOS CLAVE PARA LA IMPLANTACIÓN DE DNSSEC

Como cualquier tecnología relativa a los Sistemas y Tecnologías de Información y Comunicaciones (STIC), DNSSEC lleva asociados ciertos elementos que deben conocerse con antelación a su puesta en marcha. DNSSEC no es una solución "out-of-the-box" que simplemente requiera instalar o actualizar un paquete de aplicaciones, sino que utiliza conceptos avanzados como claves y firmas criptográficas, el establecimiento de cadenas de confianza, la gestión de claves, etc. que deben conocerse en profundidad.

Adicionalmente, y dado que introduce elementos no presentes en el protocolo DNS, puede llevar asociada cierta inversión en hardware, infraestructura y personal técnico que se ha de cuantificar.

Además, se debe tener en cuenta que DNSSEC no es un servicio que parte de cero, sino que ha de construirse sobre la infraestructura del servicio de nombres DNS ya existente y operativo, minimizando la indisponibilidad de dicho servicio y sin afectar a su rendimiento.

El punto de partida del despliegue de DNSSEC para un dominio o zona pasa por asegurarse de que la zona padre está correctamente firmada y operativa desde el punto de vista de DNSSEC, y de evaluar las restricciones impuestas por el proveedor de servicios en caso de que se quiera externalizar el servicio DNSSEC.

El presente apartado hace referencia principalmente y de manera individual a una zona objetivo, la zona DNS sobre la que se desea desplegar DNSSEC, pero todas las recomendaciones facilitadas deben de ser extendidas y extrapoladas al conjunto total de zonas (en plural) de la organización.

Es importante reseñar que los mecanismos para el despliegue de DNSSEC, aun pudiendo parecer complejos, no lo son si se elabora un procedimiento exhaustivo y se ejecutan correctamente las acciones en él definidas.

Son varios los aspectos principales a determinar: por un lado, el ámbito, alcance y modelo de gestión; por otro, las necesidades de automatización de la gestión y el nivel de seguridad que se requiere para el entorno. Todos estos aspectos se detallan a continuación.

3.1. Ámbito de aplicación del servicio DNSSEC

Se recomienda hacer uso de DNSSEC desde los dos sentidos (cliente y servidor) asociados al proceso de resolución de nombres del servicio DNS, teniendo además en cuenta que el despliegue de ambos puede iniciarse simultáneamente o independientemente, pues no existen dependencias entre ellos:

- En el lado cliente DNS (*resolver*), de cara a asegurar que los clientes internos de la organización se conectan a los recursos legítimos, tanto corporativos como externos (ver apartado "3.2. Alcance del servicio DNSSEC"). La validación DNSSEC puede llevarse a cabo en cualquier punto de la red:
 - Directamente por parte de la aplicación que origina la consulta (cliente final).
 - En un *resolver* DNS instalado en el ordenador del cliente final como parte del sistema operativo o de una aplicación.
 - En el punto de conexión entre la red interna y la externa (*firewall, router...*).
 - En un *resolver* DNS centralizado y propio de la organización.

- En los *resolvers* DNS del proveedor de servicios de Internet (ISP).
- Referenciando *resolvers* DNS públicos como los de Google o Cloudflare [Ref.- 31].
- En los servidores caché recursivos, ya sean gestionados por el ISP o por la propia organización.

Los *resolvers* DNS que realizan las consultas al interior y/o exterior de la organización deben configurarse de forma que soliciten respuestas DNSSEC.

- En el lado servidor DNS, de cara a garantizar que los servidores autoritativos de la zona (de nuevo, interna y/o externa de la organización) proporcionan respuestas que cualquier *resolver* con soporte para DNSSEC podrá validar como íntegras y auténticas, permitiendo que los clientes se conecten a los servicios legítimos de la organización.

3.2. Alcance del servicio DNSSEC

El alcance del servicio DNSSEC corresponde a la decisión sobre si el despliegue de DNSSEC tendrá carácter privado, público, y/o ambos:

- **Privado:** servicios de resolución de nombres corporativos para las redes y recursos internos o privados a la organización.
- **Público:** servicios de resolución de nombres externos para las redes y recursos públicos, es decir, aquellos que ofrece la organización en Internet y que representan su presencia en Internet.

En la valoración de estos aspectos jugará un papel determinante el tamaño de la organización y la complejidad de su servicio de nombres actual. Entre otros aspectos, deberá considerarse el número de zonas definidas en la actualidad en el servicio DNS, y si se pretende implantar DNSSEC en todas ellas simultáneamente o de manera progresiva, así como el modelo existente de gestión de los dominios de las zonas (ver apartado "3.3. Modelo de gestión del servicio DNS").

Para organizaciones pequeñas en las que el servicio DNS no sea muy complejo, lo habitual será planificar el despliegue de DNSSEC de forma conjunta.

En organizaciones cuyo esquema de resolución de nombres sea más complejo, se recomienda optar por realizar el despliegue de forma progresiva, iniciándolo en los servicios más críticos desde el punto de vista de la seguridad y del negocio, para protegerlos lo antes posible. Sin embargo, según la criticidad de dichos servicios, podrá iniciarse el despliegue de DNSSEC mediante un piloto en el que esté involucrada una zona, privada o pública, de menor criticidad. Preferiblemente se recomienda comenzar con una zona privada, para minimizar el impacto en caso de posibles incidencias en el servicio, especialmente durante la fase inicial de pruebas.

3.3. Modelo de gestión del servicio DNS

A la hora de plantearse el despliegue de DNSSEC hay que partir del análisis del modelo actual de gestión del servicio de nombres (DNS), y determinar si se va a mantener este modelo o se va a optar por uno alternativo:

- **Gestión propia:** suele ser el caso de los dominios DNS internos o privados de la organización, ya sea mediante recursos y servidores DNS propios o a través de un servicio subcontratado. Sin embargo, también los dominios DNS públicos son autogestionados por muchas organizaciones, principalmente de mayor tamaño.
- **Gestión externa:** a través de un proveedor de servicios que soporta hospedaje o gestión del dominio en el servicio DNS. Es habitual para todo tipo de organizaciones, principalmente pequeñas y medianas, pero también para grandes organizaciones que cada vez más se unen a la tendencia en el uso de servicios "en la nube".

De cara al alta de un nuevo dominio para el que se desea habilitar DNSSEC, conviene elegir desde el inicio un agente registrador que posibilite el alta directamente con DNSSEC, independientemente del modelo de gestión a emplear. Además, para el caso de gestión externa, convendrá elegir un agente registrador que proporcione servicios de hospedaje o gestión del dominio con soporte para DNSSEC.

3.3.1. Gestión externa del servicio DNS

La externalización (o delegación¹) de la gestión del servicio DNS del dominio en un proveedor de servicios es la opción menos costosa en términos de recursos técnicos y económicos, pero, en función de las circunstancias, puede no resultar conveniente.

Se presentan dos escenarios:

- **El actual proveedor del servicio DNS ofrece DNSSEC como servicio:** en este caso, el primer paso será contactar con el proveedor para obtener los requisitos y los procedimientos establecidos por él para desplegar DNSSEC en el dominio.
- **El actual proveedor del servicio DNS no ofrece DNSSEC:** en este caso, el primer paso será identificar un proveedor con soporte para DNSSEC al que transferir potencialmente el dominio sin firmar, planificando las acciones operativas necesarias con el menor impacto posible. Aunque el traspaso en sí se realice inicialmente solo a nivel de DNS, se deberán tener en mente desde un principio las acciones asociadas al firmado de la zona.

La ausencia de soporte para DNSSEC por parte del proveedor del servicio DNS actual puede constituir en sí mismo un condicionante para evaluar si se cambia el modelo existente y se pasa a gestionar el servicio DNS con recursos propios.

El proceso de selección de un proveedor de servicios que soporte DNSSEC debe ser exhaustivo, por lo que, si la política de la organización conlleva requisitos específicos, como uso de registros NSEC3 frente a NSEC, algoritmos de firma de curva elíptica o custodia propia de las claves, será necesario obtener el listado de proveedores que los cumplen. Se

¹ En el caso del servicio DNS y DNSSEC se intentará evitar hacer uso del término delegación, frente a externalización, con el objetivo de que no sea confundido con el concepto de delegación de una zona o dominio, por parte de una zona padre hacia una zona hija, trasladando la responsabilidad y gestión de la misma a otra organización (o persona responsable).

recomienda contactar directamente con los posibles proveedores candidatos y confirmar con ellos el soporte de DNSSEC que ofrecen y su nivel de madurez.

También debe conocerse el mecanismo de carga de los registros DS en la zona padre. Para el ccTLD ".es", es el agente registrador (registrar o RAR) del dominio quien se encarga de trasladar los registros DS de la zona (junto a los registros NS) a Red.es, que es la entidad que actúa como registro (*registry* o RY) de la zona ".es".

En la referencia [Ref.- 52] se proporciona un enlace a la sección de "Actualidad y noticias" de dominios.es en la que se ofrece una lista de proveedores que ofrecen servicios de DNSSEC para el dominio ".es". También se puede consultar la lista de ICANN [Ref.- 53], pero teniendo presente que este listado puede haber sufrido variaciones desde su publicación y que debe tomarse como punto de partida y no como única referencia.

Es habitual que la generación de los registros DS correspondientes a una zona la lleve a cabo el operador que gestiona los servidores autoritativos para la zona, que puede ser el propio agente registrador (si también proporciona el servicio de hospedaje o gestión del dominio) u otro proveedor de servicios de gestión de DNS (que puede ser el proveedor de servicios empleado por la organización para el *hosting* de servidores web, correo electrónico, etc.).

Respecto al firmado de la zona en sí, el despliegue de DNSSEC es dependiente de los procesos establecidos por el proveedor, pudiendo darse distintas situaciones:

- **El proveedor no soporta firmado de zonas**, por lo que el responsable técnico de la organización propietaria del dominio debe realizar el proceso de firmado y subir la configuración a los servidores autoritativos hospedados en el proveedor. Posteriormente, el registro DS se enviará al agente registrador (sea o no el mismo que el proveedor de gestión del servicio DNS) para que lo traslade a los servidores DNS del dominio de nivel superior.
- **El proveedor soporta el firmado de zonas a través del interfaz de administración** del dominio, pudiendo admitir distintas configuraciones, como elegir el tamaño de las claves y el tipo de algoritmo de firmado, o proporcionar una configuración fija, que convendrá conocer de antemano.
- **El proveedor activa DNSSEC por defecto** nada más hacerse cargo de la gestión del dominio, sin requerir que el titular del mismo lo demande expresamente.

La "Figura 1" ilustra el panel de control de un proveedor de DNS que permite la gestión de DNSSEC y admite parametrización [Ref.- 32], mientras que la "Figura 2" muestra el panel de control de un proveedor que permite la gestión de DNSSEC sin parametrización [Ref.- 33]. Es importante destacar que ambos ejemplos se ofrecen a título ilustrativo, sin pretenderse en modo alguno que el lector tome estos proveedores como única referencia:

Zone Signing Keys		
Encryption Method	Key Expiration	Key Size
RSA/SHA-1	1 month from now	1,024 bit

Key Signing Keys		
Encryption Method	Key Expiration	Key Size
RSA/SHA-1	1 year from now	2,048 bit

Notifications

Contact


Send notifications

- When a key is created
- When a key expires
- Weeks before a key expires

[Add DNSSEC](#)

Figura 1 - Panel de control de un proveedor con parametrización de DNSSEC

[Informations générales](#) | [Zone DNS](#) | [Gestion DNS](#) | [Redirection](#) | [DynHost](#) | [GLUE](#) | [Taches récentes](#) | [Plus +](#)



Offre **gold**

Gestion des DNS **i** Configuration automatique

Protection contre le transfert **i**

Délégation Sécurisée - DNSSEC **i**

Service OWO (gratuit) **i**

Option DNS Anycast **i** DNS Anycast

Figura 2 - Panel de control de un proveedor sin parametrización DNSSEC

Si tras evaluar los servicios DNSSEC ofrecidos por el proveedor actual se considerase oportuno transferir la gestión de una zona ya firmada a otro proveedor por cualquier motivo, se deberán seguir las instrucciones descritas en el apartado "4.2. Transferencia de una zona firmada a otro proveedor".

Una vez seleccionado el proveedor, será preciso obtener de él los detalles operativos sobre cómo genera, custodia y despliega en la zona padre (por ejemplo, el dominio ".es") los registros DS asociados a la nueva zona que se desea firmar. En este sentido, se debe analizar cuidadosamente el acuerdo de servicios (SLA, *Service Level Agreement*) de forma que garantice la correcta operación de la zona DNSSEC, y que contemple la hipotética transferencia de la zona a otro proveedor en un futuro sin necesidad de que haya que dismantelar por completo el firmado de la misma.

El proceso de transferencia de una zona o dominio entre agentes registradores o proveedores de servicios es un trámite administrativo contemplado en el servicio DNS que no debería tener implicaciones específicas si aún no se ha desplegado DNSSEC.

La mayor parte de recomendaciones expuestas a lo largo de la presente guía solo son de aplicación en escenarios donde el modelo de gestión es propio, es decir, se emplean servidores autoritativos DNS propios de la organización, salvo mención expresa. En el caso de servidores DNS externalizados, también son de aplicación, pero la aplicación de las recomendaciones depende de la flexibilidad y granularidad proporcionada por el proveedor externo.

3.3.2. Gestión propia del servicio DNS

Aunque la gestión del servicio DNS se lleve a cabo como parte de los sistemas de información de la organización, la transferencia de los registros DS de una zona hija a la zona padre involucra necesariamente a las entidades responsables de esta última. Dependiendo del TLD, la transferencia de los registros DS puede llevarse a cabo a través del agente registrador del dominio (como es el caso del dominio o ccTLD ".es") o directamente con la entidad que actúa de registro.

Una vez conocido este mecanismo, habrá que contactar con la entidad responsable para conocer los requisitos técnicos que imponen y cuál es su política de actualizaciones de zona, dado que esta afecta directamente a los nuevos registros DS que entrarán en vigor cuando se renueve la clave KSK.

En el caso de los servidores del ccTLD ".es", las actualizaciones de zona se realizan cada 4 horas.

El segundo elemento clave a la hora de gestionar autónomamente el servicio de DNSSEC es la selección de la solución DNSSEC, en la cual influyen:

- Costes de implantación de la solución.
- Compatibilidad con el software DNS ya existente.
- Complejidad técnica.

3.4. Nivel de automatización esperado del servicio DNSSEC

DNSSEC conlleva procesos regulares y periódicos, algunos de los cuales llevan asociadas restricciones de tiempo, por lo cual se recomienda planificar mecanismos que ayuden a automatizar los procesos hasta donde permita el entorno tecnológico.

En función del nivel de automatización, del cual dependerá la elección del software DNSSEC a emplear, se puede establecer la siguiente clasificación para el entorno [Ref.-59]:

- **Bajo nivel de automatización**, son aquellos que presentan las siguientes características:
 - Intervención del usuario alta: la gestión de las operaciones de refirmado de la zona y renovación de claves se realiza principalmente de forma manual.
 - Escasa granularidad: el manejo de las claves (para su renovación o para el firmado de la zona) requiere de permisos de acceso elevados. Sin embargo, otros procesos de DNSSEC no requieren de acceso a las claves privadas. Si la granularidad es baja, una vulnerabilidad en el software de estos últimos procesos, que compartirían permisos elevados con los procesos más sensibles, podría comprometer las claves privadas.

- Conocimiento profundo de DNSSEC: si los procedimientos son manuales, el responsable técnico deberá conocer en detalle el protocolo para poder realizar una gestión correcta e identificar errores de forma eficiente.
- Dependencia de un interfaz gráfico de usuario: aunque la configuración pueda resultar aparentemente más sencilla empleando herramientas gráficas, las mismas requieren siempre de la intervención del usuario.
- **Alto nivel de automatización**, donde alternativamente se cumplen una serie de características más ambiciosas:
 - Escasa intervención del usuario: la puesta en marcha de buenas prácticas puede llevar a que la intervención del usuario se limite a supervisar el entorno y desplegar el proceso de renovación de las cadenas de confianza.
 - Conocimiento moderado de DNSSEC: aunque el nivel de automatización sea elevado y permita una gestión muy automatizada en el funcionamiento normal, las situaciones de emergencia requerirán un conocimiento razonable del protocolo para poder solventar el problema. Será crucial que la documentación del entorno sea muy clara, incluyendo procedimientos de escalada de un incidente ante eventuales problemas. En función del entorno, se puede optar por tener el conocimiento internamente o subcontratar las labores a expertos externos.
 - Arquitectura de alta disponibilidad: existencia de una zona de respaldo (o *backup*) que asuma el rol de firmante en caso de fallos de hardware o de la red, para evitar que las firmas puedan expirar si el periodo de indisponibilidad del servidor DNS primario se alarga. En este sentido, habrá que determinar los mecanismos de intercambio de claves o, si se opta por no transferirlas, planificar un refirmado completo de la zona a través de un par de claves distintas.

3.5. Nivel de seguridad requerido para las claves

DNSSEC se fundamenta en la definición y mantenimiento de cadenas de confianza, lo cual depende irreversiblemente de la seguridad de las claves privadas implicadas en el proceso.

Más allá de la robustez de los algoritmos empleados y de la longitud de las claves, hay que valorar detenidamente cómo se llevará a cabo la gestión de las claves privadas, que guarda a su vez relación con el nivel de automatización de su mantenimiento.

En virtud del nivel de automatización y de seguridad de las claves, se puede establecer la siguiente clasificación para el entorno DNSSEC [Ref.- 59]:

- **Gestión de las claves con un nivel de seguridad bajo o medio**, agrupándose bajo este criterio los entornos que cumplen:
 - Manejo de claves manual: se introduce el riesgo de error humano.
 - Permisos a nivel de sistema no controlados: las claves privadas deben tener los mínimos permisos de lectura de forma que solo el proceso responsable de la firma pueda acceder a ellas. En ocasiones, el software DNSSEC utiliza permisos a nivel de usuario y grupo, lo cual debe controlarse minuciosamente o hacer uso de entornos `chroot` (en Unix/Linux).
 - Servidor firmante visible: en general, la recomendación para proteger las claves es que la firma de la zona se lleve a cabo en un sistema

independiente (un servidor oculto que pueda transferir la zona firmada a los servidores DNS más expuestos que ofrecen el servicio). Sin embargo, algunas soluciones para la automatización de procesos DNSSEC no permiten esta configuración.

- **Gestión de las claves con un nivel de seguridad alto**, donde, en general, se liga esta clasificación al uso de módulos HSM (*Hardware Security Module*). Sin embargo, hay otros elementos que también se deben tener en cuenta:
 - Plataforma de sistema operativo segura: el servidor DNSSEC está bastionado y ofrece las máximas medidas para que los datos DNS sin firmar no puedan ser alterados antes del proceso de firma.
 - Servidor firmante oculto: la exposición vía Internet (o vía las redes internas de la organización) del sistema en el que se realiza el proceso de firma puede comprometer la gestión de claves de DNSSEC. Asegurar que el servidor DNS con las claves privadas de DNSSEC está oculto es una recomendación que minimiza este riesgo.

A pesar de que en ocasiones no se cuente con los medios técnicos más sofisticados para asegurar las claves, siempre hay buenas prácticas que permiten mitigar los riesgos:

- Elegir una solución DNSSEC que, de forma automática, controle la generación de las claves y el firmado con el mismo modelo de permisos usuario/grupo, de forma que los permisos sean mínimos y, si no es el caso, alerte de la situación.
- Elegir una solución DNSSEC que alerte de cuándo las claves ya no son necesarias y verifique si se han eliminado correctamente.
- Elegir *appliances* DNS (mediante soluciones comerciales especializadas que combinan software y hardware) con un nivel de bastionado elevado, que mitiguen los accesos por parte de personal no autorizado.

3.6. Requisitos y necesidades en los sistemas de información y comunicaciones

El punto de partida de cara a la correcta implantación de DNSSEC es examinar el tipo de infraestructura actual asociada a los sistemas de información y comunicaciones de la organización. DNSSEC requiere más capacidad de procesamiento y no está soportado por todas las implementaciones de los servidores DNS de la industria, además de generar un tráfico hasta 2,5 veces (de media) superior a DNS.

En algunos casos, el dimensionamiento actual de los servidores y de los equipos de red puede ser ya suficiente para absorber la mayor demanda de recursos de DNSSEC, pero, en otros casos, puede ser necesario dotar a la organización de cierto equipamiento, tanto hardware como software.

Además, algunos elementos técnicos asociados a DNSSEC pueden requerir la utilización de recursos adicionales:

- **DNSSEC introduce el concepto de "tiempo absoluto" en el esquema de resolución de nombres**, al contrario que el servicio DNS, donde el tiempo solo es relativo y basado en el TTL (*Time To Live*) de los registros. En DNSSEC, la firma de una zona tiene un período de validez (ver apartado "4.1.3. Parámetros asociados a la validez de las firmas"), marcado por los campos "inception" (comienzo) y "expiration" (caducidad) de los registros RRSIG (firmados con la clave ZSK). Antes de que se llegue a la fecha declarada en "expiration" se deberá renovar la clave ZSK y publicar los nuevos registros RRSIG actualizados (firmados con la nueva clave ZSK) en el fichero de zona del servidor DNS autoritativo. Además, de cara al servicio DNSSEC, los *resolvers* y los servidores DNS autoritativos deben estar sincronizados en tiempo para evitar que los registros sean considerados inválidos por parte del *resolver* por un problema de referencia horaria. Por tanto, DNSSEC es muy sensible a las referencias de tiempo y, si un atacante consigue alterar la hora del *resolver*, puede hacer que este dé por expirada la firma de un registro que aún sigue vigente (ataque de Denegación de Servicio, DoS).

Además del periodo de validez de la firma de los diferentes registros DNS que se obtiene de los registros RRSIG, también se mantiene la referencia temporal o TTL original del registro estándar (RR) del que se partió, asociada al servicio DNS, de forma que el registro se considera válido en DNSSEC si se cumplen ambas condiciones, es decir, hasta que expire el TTL y mientras la firma esté vigente; de esas dos condiciones, la que se incumpla primero será la que dé lugar a que el registro se marque como inválido (*bogus*). Por tanto, sincronizar los servidores de nombres primarios y secundarios a nivel de referencias de tiempo, así como los *resolvers* DNS, es fundamental para el correcto funcionamiento del servicio DNSSEC (por ejemplo, a través del protocolo NTP, *Network Time Protocol*).

- **Problema de inconsistencias durante el tiempo de transferencia o propagación de la zona en DNSSEC**: debido al esquema de replicación de la información de una zona entre un servidor DNS primario y los servidores DNS secundarios, que se emplea para garantizar la disponibilidad del servicio y una eficiente distribución de la carga, puede ocurrir que las actualizaciones de los registros, que tienen lugar únicamente en el servidor primario y solo se propagan a los secundarios durante la operación de transferencia de zona, no estén sincronizadas durante el tiempo en el que se está realizando dicha transferencia. Esto puede dar lugar a diferencias entre los estados de un servidor primario y sus servidores secundarios, y un *resolver* podrá obtener potencialmente distintas respuestas a una misma consulta según a qué servidor se dirija. Se recomienda emplear notificaciones (NOTIFY) y transferencias de zona incrementales (IXFR), frente a transferencias de zonas absolutas, completas o autoritativas (AXFR) para minimizar este problema.

De cara a asegurar la validación, es preciso que el hardware del servidor DNS caché soporte la carga computacional extra asociada a la validación necesaria en DNSSEC, aunque, con el hardware moderno existente hoy en día, incluso un servidor DNS caché que ejecute dentro de una máquina virtual podrá asumir dicha carga. Adicionalmente, se debe asegurar que la infraestructura de red soporta:

- **DNS sobre TCP**: el uso de DNSSEC provoca que los paquetes DNS (especialmente las respuestas DNSSEC) superen el máximo tamaño de una trama DNS sobre UDP (512 bytes), en cuyo caso el servidor DNS caché empleará el

mecanismo de DNS conocido como "*TCP fallback*" o "*fallback to TCP*", para llevar a cabo la misma consulta empleando TCP en lugar de UDP. Aunque la ampliación de DNS mediante *Extended DNS* (EDNS o EDNS0), descrita a continuación, está orientada en este sentido, se recomienda asegurarse de que los *firewalls* y otros dispositivos de red y seguridad perimetrales no bloqueen el tráfico DNS sobre TCP y soportan el cambio de UDP a TCP, potencialmente utilizado más comúnmente en el servicio DNSSEC.

- **Tamaño de trama UDP superior a 512 bytes:** en el servicio DNS, la mayoría de los mensajes tienen un tamaño inferior a 512 bytes y son transmitidos mediante UDP. Sin embargo, las firmas asociadas a DNSSEC incrementan el tamaño de las respuestas, con tamaños de hasta 4.000 bytes. DNSSEC utiliza la extensión EDNS0 (*Extended DNS*, mencionada en el punto anterior) del protocolo DNS, que permite el uso de tramas UDP mayores de 512 bytes, antes de tener que cambiar a TCP. Los *firewalls* y otros dispositivos de red y seguridad perimetrales deben de poder admitir dichas tramas sin descartarlas, es decir, han de estar optimizados frente a mensajes UDP de más tamaño, así como no rechazar tramas UDP fragmentadas.

3.7. Valoración coste/beneficio

Los criterios de coste/beneficio de la solución DNSSEC dependen principalmente del ámbito de aplicación y del modelo de servicio. En el "Informe del estado de DNSSEC en España" publicado por INCIBE [Ref.- 1] se analizan los distintos aspectos implicados en estos criterios en detalle.

De forma resumida, se puede considerar que, con un modelo de gestión de DNSSEC basado en un proveedor externo, el coste de despliegue únicamente será el que el proveedor aplique al servicio (que, en algunos casos, puede incluso no suponer ningún coste extra).

Desde el punto de vista del registro del dominio, existen ya diversos agentes registradores que gestionan el alta del mismo con DNSSEC, sin costes asociados.

En el caso de un modelo de gestión de DNSSEC propio, se distinguirán los criterios de coste/beneficio entre los aplicables en el *resolver* y en el servidor DNS autoritativo.

Además de sopesar el coste/beneficio propio individualmente, se debe tener en mente que la implantación de DNSSEC a nivel global contribuye a la seguridad de toda la comunidad de Internet.

3.7.1. Resolver

El coste se puede considerar de entre bajo a muy bajo, pues no requiere inversión en software (existen soluciones de código abierto estandarizadas que soportan DNSSEC) y tampoco en hardware (considerando que la organización ya dispone de servidores con prestaciones estándar). El coste se deberá fundamentalmente a:

- **Recursos humanos:** inversión en tiempo y dedicación por parte del departamento de administración de sistemas. La implantación de DNSSEC no debería llevar más

de una a dos semanas² (aunque, lógicamente, dependerá del número de servidores DNS y de usuarios finales).

- **Adquisición de equipos de red** si los actuales no están bien dimensionados, especialmente para acomodar el mayor tamaño de los paquetes de DNSSEC (ver apartado "3.6. Requisitos y necesidades en los sistemas de información y comunicaciones").

El beneficio de DNSSEC en el *resolver* es directo, pues elimina el riesgo de ataques de suplantación desde Internet para aquellos servicios pertenecientes a dominios securizados con DNSSEC. Obviamente, el riesgo seguirá existiendo para todos los servicios que sigan dependiendo del servicio DNS tradicional.

3.7.2. Servidor DNS autoritativo

La inversión en software, al igual que en el lado del *resolver* y por las mismas razones, debería ser baja.

Respecto al hardware, si se cuenta con servidores con prestaciones estándar, a día de hoy tampoco debería ser preciso adquirir nuevos sistemas. Sí es conveniente evaluar la adquisición de módulos HSM para proteger y automatizar la gestión de las claves.

La principal inversión puede venir de los recursos humanos necesarios, pues DNSSEC precisa de conocimientos técnicos que quizá requieran formación para los administradores del servicio DNS (dependiendo de su experiencia actual). En cuanto a las tareas de administración, si bien el despliegue requerirá de una buena planificación, el mantenimiento y la operación pueden automatizarse de forma que no supongan una carga excesiva adicional a la existente para el servicio DNS.

Respecto al beneficio, este está estrechamente ligado a la imagen de la organización en Internet, y también dependerá del riesgo que suponga sufrir un ataque de envenenamiento de caché o de DNS *spoofing* que afecte a los servicios ofrecidos por la organización. Este riesgo deberá ser evaluado junto a la existencia de otras medidas de seguridad implantadas en protocolos y servicios de nivel superior como, por ejemplo, el uso generalizado /o en exclusiva) de HTTPS (frente a HTTP).

² https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_Deploying_DNSSEC_v20.pdf

4. RECOMENDACIONES DE DISEÑO

En este apartado se proporcionan las recomendaciones relativas al diseño necesario para abordar el despliegue de DNSSEC desde cero, es decir, partiendo de la existencia de una zona DNS que actualmente no ha implementado ningún elemento propio de DNSSEC.

A día de hoy, el software disponible para desplegar DNSSEC tiene suficiente nivel de madurez, por lo que la clave para el éxito del despliegue radica en definir correctamente las políticas de implantación, gestión y operación siguiendo los procedimientos disponibles tanto para garantizar la seguridad como la estabilidad del entorno.

A continuación, se proporcionan las recomendaciones de diseño de cada uno de los distintos elementos que conforman un entorno DNSSEC.

Se recomienda la lectura del RFC 6781 [Ref.- 25], que presenta multitud de consideraciones relativas que influirán en la elección de los distintos elementos disponibles en DNSSEC.

4.1. Políticas y procedimientos de seguridad y gestión de DNSSEC

Como cualquier otro elemento sensible de un sistema informático, la infraestructura del servicio de nombres debe protegerse desde un punto de vista:

- **Físico:** ubicarlo en un entorno controlado, a salvo de condiciones ambientales adversas, con controles de acceso físico, detección de intrusos y una política adecuada de copias de seguridad y de recuperación ante desastres.
- **Lógico:** acceso restringido mediante contraseñas robustas, uso de segundo factor de autenticación, política de actualizaciones (de seguridad) controlada, separación de roles de administración, principio de mínimos privilegios, etc.

Pero además, dado que DNSSEC proporciona integridad y autenticidad para las respuestas proporcionadas por los servidores de nombres autoritativos ante una consulta DNS, en base a un esquema de firma criptográfica en el que se apoyan todas las operaciones de validación, la definición de los aspectos criptográficos requerirá de especial atención.

El proceso de firmado y verificación de una firma criptográfica sigue el esquema descrito en la "Figura 3" [Ref.- 11]:

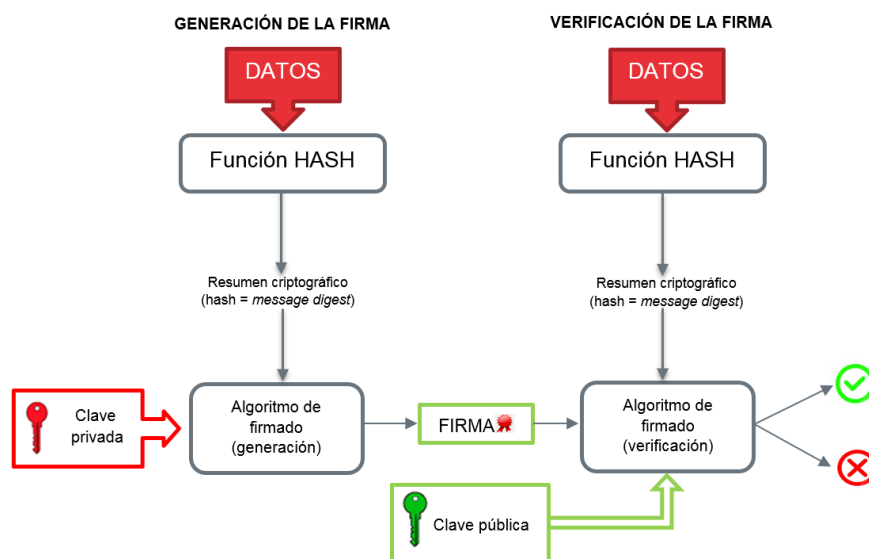


Figura 3 - Firmado digital

En un esquema de firma intervienen dos elementos principales, para los cuales se enumeran los requisitos propios de DNSSEC [Ref.- 21]:

■ **Sistema de gestión de claves:**

- Debe soportar separación de claves (KSK y ZSK).
- Debe soportar la renovación de claves tal como se describe en el RFC 6781 [Ref.- 25].
- Si no se utilizan dispositivos HSM, las claves deben protegerse criptográficamente cuando se almacenen en memoria persistente.
- Debe soportar procesos de renovación de claves de zona automáticos y planificados mediante la publicación anticipada de claves según describe el RFC 6781 [Ref.- 25].

■ **Sistema de firmado:**

- La implementación de DNSSEC debe cumplir con los RFCs 4033 [Ref.- 22], 4034 [Ref.- 7] y 4035 [Ref.- 5] y sus actualizaciones.
- Debe soportar RSA con SHA1, SHA256 y SHA512 según el RFC 5702 [Ref.- 19]³.
- Debe soportar NSEC3 tal como define el RFC 5155 [Ref.- 23]. Adicionalmente, debe soportar el cambio de los parámetros NSEC3 (NSEC3PARAM) sin que para ello sea necesario revertir el firmado de la zona.
- Debe soportar los registros DS publicados con SHA256 según el RFC 4509 [Ref.- 24].
- El sistema de firmado debe permitir configurar el periodo de refresco de las firmas (registros RRSIG), así como su periodo de validez.

³ Por simplificar, para todas las referencias a los algoritmos criptográficos de *hashing* se hace uso de la nomenclatura SHA1, en lugar de SHA-1 (con guión), salvo en las configuraciones del protocolo DNS donde sea necesario el uso del guion.

Adicionalmente, se recomienda que el sistema de firmado soporte:

- ECDSA P-256/SHA256 y ECDSA P-384/SHA384 como describe el RFC 6605 [Ref.- 13].
- El firmado con dos o más algoritmos de firma simultáneamente como, por ejemplo, RSA y ECDSA.
- La transición de NSEC a NSEC3 sin revertir el firmado de la zona.
- El cambio de algoritmo de firma (y, por tanto, de generación de claves) sin revertir el firmado de la zona.

4.1.1. Selección de los algoritmos de firma

Los registros asociados a firmas criptográficas en DNS incluyen un identificador de 8 bits que representa el algoritmo empleado en su generación. Existen tres registros de este tipo en DNSSEC: DNSKEY, RRSIG, DS; adicionalmente, existen otros tres registros asociados a las firmas (KEY, SIG, y CERT) utilizados en otros estándares de DNS, que también incluyen el identificador de su algoritmo [Ref.- 6].

El RFC 4034 [Ref.- 7] definió inicialmente los algoritmos válidos para el firmado de zona en DNSSEC. Posteriormente, en el RFC 5155 [Ref.- 23], se incluyó "RSASHA1-NSEC3-SHA1" para soportar el uso de NSEC3 con RSA/SHA1. En el RFC 6944 [Ref.- 10] se actualizaron los requisitos mínimos (y recomendaciones) para dichos algoritmos, añadiéndose el uso de RSA/SHA256 y RSA/SHA512 y de ECDSA. A fecha de elaboración de la presente guía, los algoritmos disponibles para firmado en DNSSEC son⁴:

Valor	Algoritmo	Mnemónico	Firmado de zona	RFC
0	reservado	-	-	4034 4398 8078
1	RSA/MD5 (obsoleto)	RSAMD5	No	3110 4034
2	Diffie-Hellman	DH	No	2539
3	DSA/SHA-1	DSA	Sí	2536 3755
5	RSA/SHA-1 (obligatorio)	RSASHA1	Sí	3110 4034
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1	Sí	5155
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1	Sí	5155
8	RSA/SHA-256	RSASHA256	Sí	5702
10	RSA/SHA-512	RSASHA512	Sí	5702
12	GOST R 34.10-2001	ECC-GOST	Sí	5933
13	ECDSA Curve P-256 / SHA-256	ECDSAP256SHA256	Sí	6605
14	ECDSA Curve P-384 / SHA-384	ECDSAP384SHA384	Sí	6605
15	Ed25519	ED25519	Sí	8080
16	Ed448	ED448	Sí	8080
253	privado	PRIVATEDNS	Sí	4034
254	privado	PRIVATEOID	Sí	4034
17 122	sin asignar			

⁴ Las actualizaciones en los números de algoritmo están disponibles en <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml>

123 252	reservado			
255	reservado			

Tabla 1 - Algoritmos criptográficos válidos para los registros asociados al proceso de firmado de zona en DNSSEC

Es obligatorio implementar como mínimo RSA/SHA1.

La generación de firmas digitales mediante el algoritmo RSA está especificada en el estándar PKCS#1 [Ref.- 12], y se basa en la exponenciación del producto de números primos.

Por su parte, el estándar que recoge el uso de algoritmos de firma (DSA, *Digital Signature Algorithm*) basados en curva elíptica (ECDSA) para DNSSEC es el RFC 6605 [Ref.- 13].

Las claves utilizadas en los algoritmos de firma RSA requieren de mayor longitud en bits para alcanzar un nivel de seguridad equivalente al que se consigue con claves de los algoritmos de firma ECDSA de menor longitud.

Según se describe en el RFC 6605 [Ref.- 13], la fortaleza de una clave ECDSA con una curva elíptica P-256, es decir de 256 bits, es equivalente a la de RSA de 3.072 bits, y se estima que el coste computacional para generar una firma ECDSA comparable en fortaleza a una firma RSA es unas 10 veces inferior [Ref.- 15]. Sin embargo, pese a que la mayoría de las distribuciones software DNSSEC actuales soportan ECDSA tanto para firma como para validación, medidas tomadas en la práctica en un estudio en 2015 de la Universidad de Twente en Holanda muestran que solo en torno al 80% de los *resolvers* reconocían las firmas ECDSA [Ref.- 16]. Este aspecto también se analiza en profundidad en un estudio realizado por APNIC en 2014 basado en mediciones reales [Ref.- 29]. Por otra parte, según el mismo estudio, aunque la creación de la firma ECDSA es considerablemente más rápida que la de RSA, la validación de una firma equivalente es en torno a 6 veces y media más lenta que la de RSA (por ejemplo, para claves de 1.024 bits).

Adicionalmente, de cara a la selección de los algoritmos criptográficos, hay que tener en cuenta que, en la actualidad, no todos los agentes registradores y operadores de dominios TLD soportan ECDSA, por lo que es necesario consultar al propio agente registrador (u operador) para ver si da esta opción o se limita a RSA. En términos generales, y en función de los datos obtenidos a fecha de elaboración de la presente guía, se considera que la **opción más conservadora** de cara a la elección del **algoritmo de firma** es **RSA**.

Por otra parte, dado que lo que en realidad se firma no son los propios *resource records* (RRs) sino un hash criptográfico que se calcula a partir de los RRsets, o conjuntos en los que dichos RRs se agrupan en DNSSEC, el algoritmo de *hashing* que se escoja debe ser robusto para no comprometer la firma. En la actualidad, el algoritmo MD5 no se considera suficientemente robusto, de ahí que al menos se recomiende como mínimo SHA1. Pese a ello, recientes estudios ponen también en cuestión la robustez de SHA1 en base a las capacidades de cómputo actuales y a otras debilidades del propio algoritmo. Por tanto, y aunque el uso de SHA1 ha sido durante años muy generalizado en DNSSEC, la recomendación de cara a DNSSEC actual es elegir un **hash** de tipo **SHA256**.

Otro elemento que interviene en la selección de los algoritmos criptográficos es si la zona debe protegerse contra el denominado ataque de "enumeración de zona" (*zone enumeration* o *zone walking*) subyacente a la implementación de NSEC como mecanismo para gestionar en DNSSEC los escenarios de recursos inexistentes en DNS. Este ataque, consistente en poder obtener los nombres de todos los recursos de la zona a través de

consultas deliberadas sobre registros no existentes, se resuelve sustituyendo los registros NSEC por registros NSEC3. El problema de enumeración de zona no tiene por qué ser tal para todos los dominios y, en esos casos, no compensa sustituir NSEC por NSEC3 por la carga adicional que supone, especialmente para zonas pequeñas. Sin embargo, puede haber ocasiones en las que sea necesario protegerse de él (por ejemplo, puede darse el caso de que exista alguna regulación al respecto en determinadas organizaciones, o que algún acuerdo de confidencialidad lo exija). En ese caso, debe seleccionarse un algoritmo de firma que disponga de soporte para NSEC3.

El algoritmo de firma empleado para los registros KEY, SIG, DNSKEY, RRSIG, DS y CERT se identifica en la trama DNS (registro RDATA) a través de un número de 8 bits [Ref.- 6], tal como se ha descrito anteriormente, aunque no todos los números son válidos para todos los tipos de registros (RRs).

Así, para los mecanismos de seguridad de transacciones (registros SIG(0) y TSIG), se pueden emplear solo los algoritmos definidos inicialmente en los RFCs 2845 y 2931 [Ref.- 8] [Ref.- 9], respectivamente. Por su parte, los registros de tipo DNSKEY para claves RSA/SHA256 se almacenan con un número de algoritmo igual a 8. Los registros de tipo DNSKEY para claves RSA/SHA512 se almacenan con número de algoritmo igual a 10.

Cuando se hace uso como algoritmo de firma de RSA/SHA256 o RSA/SHA512, tal como describe el RFC 5702 [Ref.- 19], el valor del campo firma de los registros RRSIG sigue un esquema de firma de tipo RSASSA-PKCS1-v1_5 (de la especificación PKCS #1 v2.1). Los valores para los campos RDATA que preceden a la firma están definidos en el RFC 4034 [Ref.- 7]. El valor del campo firma se calcula obteniendo el *hash* correspondiente y con el siguiente formato:

- $hash = SHA-XYZ(data)$ (donde XYZ puede ser 256 o 512, según el algoritmo de *hashing* a emplear, y *data* tiene el formato especificado por el RFC 4034 para el RRSet que se desea firmar).
- $signature = (00 | 01 | FF^* | 00 | prefix | hash) ** e \pmod n$ (donde se lleva a cabo la concatenación, "|", de diferentes valores hexadecimales fijos, y *e* y *n* son, respectivamente, el exponente privado y el módulo público de la clave de firma RSA. El valor "FF" debe repetirse tantas veces como sea necesario para que el tamaño de los datos a firmar, entre paréntesis, coincida con la longitud del módulo *n*).

A modo de ejemplo, se proporciona una tabla que muestra los algoritmos utilizados en los registros DS de la zona raíz en el momento de elaboración de la presente guía (correspondientes a los TLDs de primer nivel, tanto ccTLDs como gTLDs). Para obtener los datos de esta tabla, se ha empleado el siguiente comando:

```
$ curl -s http://www.internic.net/domain/root.zone | awk '$4 == "DS"
{ print $6}' | sort -n | uniq -c
 164 5
  519 7
2206 8
   40 10
```

Figura 4 - Comando para obtener los números de algoritmo de los registros DS de la zona raíz

En la columna situada más a la derecha, se encuentra el identificador del tipo de algoritmo de firma según el RFC 4034 [Ref.- 7], o posteriores. La columna de la izquierda muestra el número de registros DS que se han generado en base a cada algoritmo de firma:

Algoritmo	Número de registros DS firmados
5 (RSA/SHA 1)	164
7 (RSASHA1 NSEC3 SHA1)	519
8 (RSA/SHA 256)	2.206
10 (RSA/SHA 512)	40

Tabla 2 - Algoritmos de firma empleados en la zona raíz para los diferentes TLDs de primer nivel de DNSSEC

Concretamente, la zona ".es" está firmada con el algoritmo 8 (RSA/SHA-256), tal como se describe en la declaración de políticas y procedimientos [Ref.- 34], el más común de los algoritmos de firma de los TLDs de primer nivel.

Como se puede apreciar, no existen DS en la zona raíz firmados con el algoritmo 13, que corresponde a ECDSA Curve P-256 con SHA256. Durante el proceso de revisión de la presente guía, se confirmó la existencia de un TLD de primer nivel en la zona raíz firmada con ECDSA y correspondiente a ".cz" (República Checa⁵), a fecha 2 de julio de 2018:

```
$ curl -s http://www.internic.net/domain/root.zone | awk '$4 == "DS"
{ print $1 " " $6 }' | awk '$2 == "13" { print $1 }'
CZ.
```

Figura 5 - Comando para obtener los TLDs de nivel 1 con registro DS de tipo ECDSA

Complementariamente, en el estudio realizado por CloudFlare [Ref.- 15] sobre los sitios web de "Alexa One Million", se concluye que, de los en torno a 15.600 dominios que soportan DNSSEC, solo 23 zonas estaban firmadas con ECDSA.

El registro holandés (zona ".nl") ofrece diversas estadísticas relativas al uso de DNSSEC en su zona⁶, entre ellas, los algoritmos de firma empleados en los dominios; se constata que los algoritmos RSA (7 y 8) suman el 99% para los dominios ".nl" con DNSSEC.

⁵ <http://www.dns.cz>

⁶ <https://stats.sidnlabs.nl/en/dnssec.html>

Used algorithms (i)

Most popular DNSSEC algorithms uses by .nl domains,

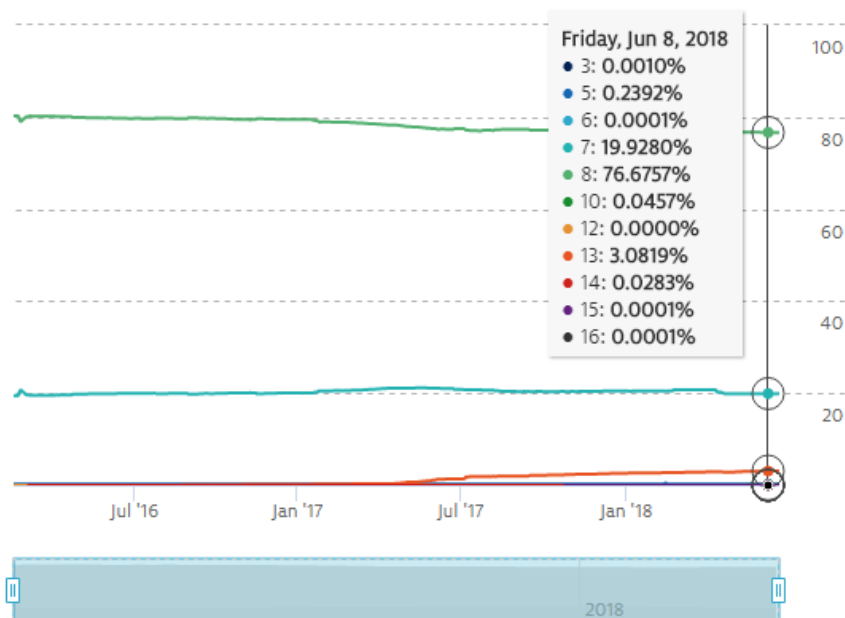


Figura 6 - Porcentaje de dominios para cada algoritmo de firma en la zona ".nl"

4.1.1.1. Uso de NSEC3 vs NSEC

Las respuestas negativas, o de recursos inexistentes, en DNSSEC pueden presentar un tamaño considerable. NSEC es más sencillo de implementar y genera menos tráfico que NSEC3 por ser sus paquetes de respuesta de menor tamaño, además de que su carga computacional es menor.

Por tanto, para dominios con un número de nombres reducido, o para aquellos que no estén afectados por acuerdos de confidencialidad, en general se recomienda utilizar NSEC.

Adicionalmente, NSEC3 requiere de un esquema de firma en tiempo real.

En caso de tenerse que emplear NSEC3, en base al RFC 5155 [Ref.- 23] se recomienda, entre otros, que la generación del hash criptográfico emplee una semilla de 64 bits con un periodo de validez del registro NSEC3 igual al establecido para las firmas (registros RRSIG), y no superar los límites máximos de iteraciones del algoritmo de *hash* establecidos en función de la longitud de las claves (con referencia a claves RSA y hashes SHA-1).

4.1.2. Longitud de las claves criptográficas

Los criterios a la hora de elegir la longitud de las claves criptográficas empleadas en DNSSEC tienen que buscar el equilibrio entre:

- **La seguridad:** a mayor tamaño de clave, más robusta es y más difícil resulta romper la misma. En este aspecto influye notoriamente el tipo de algoritmo de firma, ya que, como se indicó en el apartado anterior, los algoritmos de tipo ECDSA requieren de una longitud de clave menor que los de tipo RSA para obtener un nivel de fortaleza similar.

- **El rendimiento:** a mayor tamaño de clave, se incrementa la carga computacional, no solo en la generación de las claves, firmado de la zona y operaciones de validación, sino también en el tamaño de cada firma, que incrementará el tamaño de las respuestas DNS que se transmitirán por el tráfico de red.
- **El tiempo de vida de la clave:** para aquellas claves cuyo tiempo de vida sea corto, es asumible una longitud de clave menor que para aquellas destinadas a renovarse con menor frecuencia (al estar expuestas, y tener que ser protegidas, durante más tiempo).
- **El tipo de custodia y exposición que tendrá la clave:** si se utiliza un HSM o se realiza un firmado *offline* de la zona, en cuyo caso las claves privadas no estarán potencialmente accesibles desde el exterior, la clave puede ser de menor tamaño.
- **Los requisitos operacionales de la renovación:** si son muy costosos, se deberá elegir una clave de mayor tamaño para espaciar más las renovaciones en el tiempo.

Aunque desde el punto de vista del protocolo no se exige disponer de dos pares de claves con roles de firma separados, sino que se podría hacer que la KSK sirviera también para firmar la zona, salvo que existan razones justificadas se recomienda la separación en dos pares de claves para independizar la gestión y que:

- La clave de firma de zona (ZSK) sea de menor longitud pero se renueve más frecuentemente.
- La clave de firma de claves (KSK) tenga mayor longitud y se renueve cada más tiempo.

En la web KeyLength.com de BlueKrypt [Ref.- 14] se dispone de una serie de datos obtenidos de diferentes estándares y evaluaciones, en forma de tablas, en las que, en función del tipo de algoritmo criptográfico (de cifrado simétrico, asimétrico, firma, o tipo de hash utilizado) y de la longitud de la clave, se puede determinar el nivel de protección (medido en años a partir del año de generación) de una clave. Estas tablas se pueden tomar como referencia fiable para seleccionar los parámetros relativos a las claves, tanto ZSK como KSK.

Para DNSSEC, teniendo en cuenta que el tamaño de la clave debe estar en función del algoritmo de firma elegido y el tiempo de vida de la clave, se puede concluir que:

1. La **longitud de las claves ZSK**, considerando RSA/SHA1 o RSA/SHA256, es decir **RSA** como algoritmo de firma y SHA1 o SHA256 como algoritmo de hash, se recomienda que sea de **1.024 bits**, y que su tiempo de vida oscile entre **1 y 4 meses** [Ref.- 18]. La renovación de la ZSK puede automatizarse. En caso de utilizarse **ECDSA**, sería suficiente con emplear P-256 (**256 bits**). Sin embargo, dado que, como se indicó en el anterior apartado, puede ocurrir que el agente registrador o el operador de dominio (en caso de dominios gestionados por un proveedor) no soporten ECDSA, se recomienda verificar primero la viabilidad de uso de los diferentes algoritmos de firma antes de plantearse la utilización de ECDSA como opción adecuada.
2. La **longitud de las claves KSK** para **RSA**, considerando un periodo de validez de **entre 1 y 2 años**, se recomienda que sea de **2.048 bits**. La KSK es más compleja de renovar, y requiere intervención manual de cara a actualizar los registros DS en la zona padre.

A modo de ejemplo, la clave ZSK de la zona raíz utilizó RSA de 1.024 bits hasta octubre de 2016 [Ref.- 17] [Ref.- 20], fecha a partir de la cual se cambió a RSA de 2.048 bits (que

es la misma longitud que se emplea para la KSK). Unos 60 TLDs utilizan ya RSA de 2.048 bit para sus claves ZSK. No es el caso de la zona ".es", que emplea RSA/SHA256 con una clave ZSK de 1.024 bits [Ref.- 34].

Es importante destacar que, si una zona se divide en varias subzonas, puede optarse por emplear la misma ZSK para todas ellas o diferentes claves para cada subzona, sin que ello comprometa necesariamente la seguridad (especialmente si todas las zonas son gestionadas por el mismo servidor DNS). De cara a la gestión de claves, sin embargo, sí resulta más eficaz el uso de una única clave.

En escenarios de *Split DNS*, para los que las respuestas a una consulta pueden ser diferentes en función de cuál sea el origen de la misma (por ejemplo, una dirección IP privada o pública), puede ser recomendable independizar mediante el uso de diferentes claves los espacios de nombres o incluso dejar sin firmar ciertas subzonas delegadas.

Aunque la renovación anticipada de las claves no tendría por qué producirse salvo en caso de sospecha de haber sido comprometidas, siguiendo las buenas prácticas de seguridad, se recomienda su renovación anticipada como mecanismo de mitigación de posibles ataques.

4.1.3. Parámetros asociados a la validez de las firmas

La validez de las firmas es el elemento fundamental para el correcto funcionamiento de DNSSEC, pero es muy sensible a diversas cuestiones relativas al propio comportamiento del protocolo y a los agentes involucrados.

Uno de los ataques a nivel de seguridad que afectan al diseño del protocolo DNS es el de ataques de repetición o *replay attacks*. En el servicio DNS tradicional, los servidores caché recursivos mantienen en memoria un registro mientras su TTL (que suele ser de minutos, horas o días; un valor utilizado de manera estándar es 86.400 segundos, es decir, 24 horas) está vigente, y no consultan de nuevo al servidor DNS autoritativo si les llega una nueva petición asociada a un registro cacheado (al estar asociado a un TTL aún válido).

Si un servicio asociado a un recurso, y por tanto a un registro DNS concreto, ha sido comprometido y el administrador del servicio DNS ha eliminado o modificado el registro correspondiente para que apunte a una nueva dirección IP, puede ocurrir que sigan existiendo servidores caché recursivos que respondan con la antigua dirección IP.

Los ataques de repetición no se solucionan con DNSSEC. Si se da el caso de que un RRset en el servidor DNS autoritativo se modifica antes de que su firma expire, el RRset antiguo y su correspondiente RRSIG serán sustituidos por unos nuevos, pero los *resolvers* (servidores caché recursivos) pueden mantener aún una copia del antiguo registro con la firma antigua que seguirá siendo válida hasta que expire el TTL de dicho RRset (o hasta que expire su firma), momento tras el cual descartarán el registro. Cuando reciban una nueva petición, lo consultarán de nuevo, y en ese momento obtendrán la nueva versión del RRset y del RRSIG asociado.

Sin embargo, si un atacante consigue realizar un ataque de repetición sobre esa nueva petición o consulta DNS, es decir, hace creer al *resolver* que su respuesta viene del servidor DNS autoritativo, y envía el registro DNSSEC antiguo que aún tiene una firma con un período de validez vigente, el atacante puede impedir que el nuevo registro se actualice en el *resolver* y forzará a que el cliente final siga obteniendo el RRset antiguo.

Este escenario es especialmente crítico si el motivo de haber modificado el RRset en el servidor DNS autoritativo es que se haya cambiado la dirección IP de un servidor debido, por ejemplo, a un ataque de tipo DDoS o por haber sido comprometido. Con el ataque de repetición en marcha, el atacante podría conseguir que el *resolver* siguiese disponiendo del antiguo registro (apuntando a la dirección IP antigua) hasta que expire su firma (lo cual puede llevar días o semanas). El efecto es que los clientes seguirían tratando de acceder al servicio con la dirección IP que ya no es válida, no está disponible (DDoS) o ha sido comprometida.

Teniendo en cuenta que se recomienda que la clave empleada para firmar la zona (ZSK) se renueve entre uno y cuatro meses (y como mínimo 30 días), un incidente de seguridad que afectase a un registro firmado nada más renovarse la clave podría llevar a que este sea utilizado de manera maliciosa durante al menos un mes.

Se define como "RRset vulnerable" aquel registro que ha sido cambiado en el servidor DNS autoritativo pero cuya firma para el antiguo RRset aún no ha expirado.

Para disminuir este periodo de vulnerabilidad, se establece que las firmas de los registros de una zona se actualicen periódicamente cada cierto tiempo (que lógicamente, debería ser menor al periodo de renovación de la clave ZSK), siempre buscando el compromiso entre la seguridad, la practicidad y aplicabilidad del procedimiento vinculado al proceso de firmado de la zona.

El registro RRSIG (firma) asociado a un RRset contiene un valor de inicio y otro de fin de validez de la firma, definidos de forma que, por un lado, se disponga de un margen suficiente para su renovación o refirmado y, por otro, para minimizar el periodo de validez de la firma (frente a los escenarios de ataques de repetición previamente descritos). Por tanto, si el periodo de validez de la firma de los registros RRSet es de 15 días, su periodo de vulnerabilidad se reducirá a un máximo de 15 días.

El siguiente diagrama ("Figura 7") [Ref.- 25] [Ref.- 49] ilustra lo parámetros de tiempo para una firma:

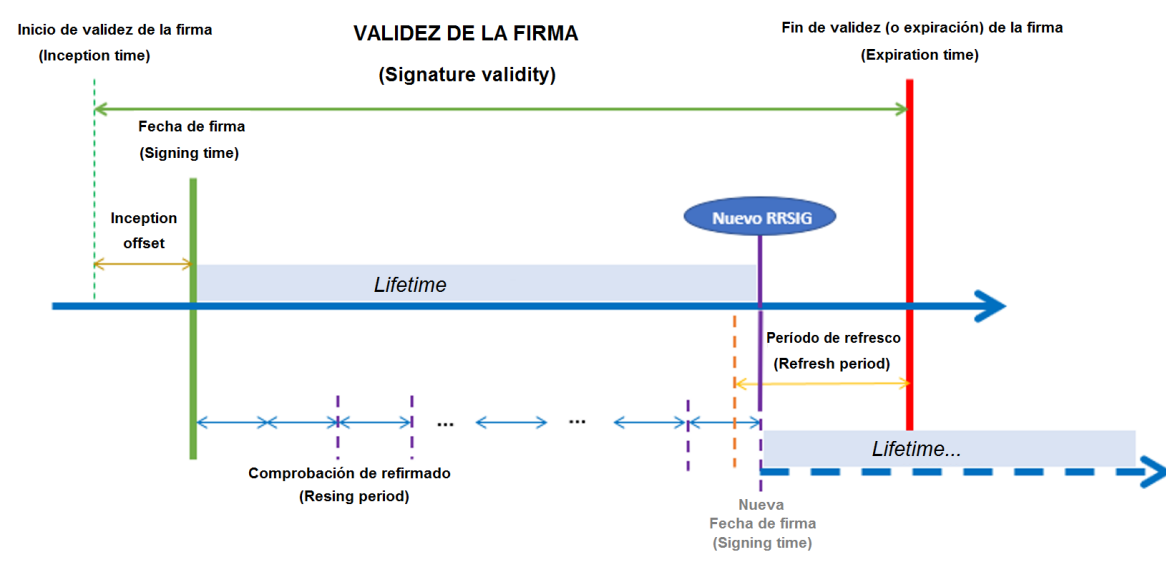


Figura 7 - Tiempos de validez de la firma de un registro en DNSSEC

- **Inception time** (fecha de inicio de validez de la firma): periodo inicial desde el que la firma se considera válida para un registro.

Suele ser anterior a la fecha de firma para evitar inconsistencias con la sincronización de tiempos entre *resolvers* y servidores DNS (esta diferencia entre ambos tiempos se denomina *inception offset*). Por ejemplo, en el caso de BIND, el *inception offset* tiene un valor fijo de 1 hora [Ref.- 48].

- **Signing time** (fecha de firma): fecha concreta de generación de la firma de un registro (RRset), es decir, de creación del registro RRSIG asociado.
- **Expiration time** (fecha de fin de validez, o expiración, de la firma): fecha a partir de la cual la firma de un registro se considera caducada y, por tanto, el RRSIG asociado es inválido.
- **Signature validity o RRSIG validity** (período de validez de la firma): determina el periodo temporal (habitualmente medido en días) en el que los registros (RRsets y RRSIGs) asociados a una firma serán válidos.

Este es el periodo de validez de la firma estimado y/o teórico en función de todos los parámetros empleados inicialmente para generar la firma (e incluidos en el registro RRSIG). Sin embargo, como se describirá posteriormente, el objetivo del servidor DNS es refirmar el registro (RRset asociado) antes de la fecha de expiración de la firma.

- **Refresh period** (período de refresco): define con qué antelación, al menos, respecto a la fecha de expiración de la firma se deben refirmar (o refrescar las firmas de) los registros (RRset), generando nuevos registros RRSIG, empleándose para ello la clave ZSK actualmente activa en la zona para el proceso de firmado.

Este periodo define realmente el periodo mínimo de refirmado (o refresco) en el que se desea sustituir los registros RRSIG actuales por unos nuevos, con anterioridad a que los actuales expiren. Es un valor aproximado, ya que el proceso de refirmado se producirá dentro del periodo de refresco, cuando se lleve a cabo la siguiente comprobación de refirmado (en función del periodo de comprobación de refirmado).

- **Resign (o re-sign) period** (periodo de comprobación de refirmado): es un intervalo de tiempo en el que el servidor DNS autoritativo va comprobando si es preciso refirmar algún registro, es decir, regenerar alguna firma correspondiente a registros cuya firma va a expirar próximamente (se encuentran dentro del periodo de refresco).

Este no es realmente el periodo de refirmado efectivo, es decir, en el que se produce el refirmado de los registros (pese a su nombre en inglés), sino el periodo de comprobación empleado por el servidor DNS para ver si ese proceso de refirmado es necesario (por lo que podría denominarse "resign (o re-sign) check period").

En base a estos parámetros de tiempo, se puede derivar el siguiente parámetro de manera artificial, pero que permite conocer el periodo de refirmado o publicación de un RRSIG:

- **Lifetime** (período de refirmado, regeneración o publicación de los registros RRSIG⁷): es la diferencia entre el período de validez de la firma (*signature validity*) y el periodo de refresco (*refresh period*), y determina el tiempo en el que la firma de un registro (RRset) no será sustituida y, en consecuencia, su RRSIG se considerará vigente. Este parámetro define por tanto el periodo tras el cual las firmas serán refrescadas, refirmándose los registros RRset y generándose nuevos registros

⁷ Debido a que en DNSSEC no existe la posibilidad de revocar un registro RRSIG previamente generado, éste será válido hasta la fecha de expiración de la firma. El periodo de refirmado también podría considerarse como el periodo de publicación de un registro RRSIG, entendiendo como tal el periodo hasta que se lleva a cabo el proceso de refirmado del RRset correspondiente y el anterior es realmente sustituido por un nuevo registro RRSIG en la zona.

RRSIG, que serán publicados en la zona sustituyendo a los registros RRSIG previos. Por ejemplo:

```
Lifetime = signature validity - refresh period

Período de validez de la firma (signature validity) = 15 días
Periodo de refresco (refresh period)                = 5 días
Periodo de refirmado de un RRSIG                    = 15 - 5 = 10 días

Por tanto, los RRSIG deberán refirmarse (aprox.) cada 10 días.
```

Figura 8 - Ejemplo de cálculo del periodo de validez efectivo (lifetime) de un RRSIG

Por tanto, los RRSet son refirmados cada cierto tiempo, por ejemplo, cada 10 días, disponiendo de un margen para evitar o solucionar problemas antes de que expire la firma.

El mínimo periodo de validez de la firma (*signature validity*) debe permitir disponer de tiempo suficiente para solucionar un problema de configuración de la firma antes de que la misma expire, y el registro pueda ser considerado *bogus*. Por tanto, debe ser al menos de unos días. Por ejemplo, el periodo mínimo de validez para los registros DS (considerados los más críticos, al estar asociados a la clave KSK) debe ser mayor de 2 días [Ref.- 25], especialmente si los administradores de la zona no están disponibles durante el fin de semana. Debe tenerse en cuenta que este periodo de validez de los registros DS está definido en realidad por la política de firmado de la zona padre.

Normalmente, el mínimo periodo de validez de la firma (*signature validity*) se define seleccionando en primer lugar el periodo de refresco (*refresh period*), normalmente varios días, y posteriormente el periodo de comprobación de refirmado (*resign period*), de forma que la diferencia entre ambos establezca el tiempo suficiente disponible en el peor de los casos para resolver problemas operacionales en el proceso de firmado, al ser este el tiempo restante antes de la fecha de expiración de la firma.

El máximo periodo de validez de la firma (*signature validity*) debe establecer por cuánto tiempo la zona acepta ser vulnerable frente a ataques de repetición. Existen consideraciones especiales para ciertos registros, como por ejemplo los registros DS en caso de ataques sobre la clave KSK, ya que en este caso también es necesario tener en cuenta aspectos operativos asociados a los procedimientos de refirmado y publicación de la zona padre, por lo que el valor máximo suele estar entre una semana y varios meses.

Según el RFC 6781 [Ref.- 25], dónde se describen de manera detallada las razones para los valores sugeridos habitualmente, teniendo en cuenta aspectos de rendimiento para evitar picos de carga innecesarios en los servidores DNS autoritativos al vencer simultáneamente el TTL o la firma de múltiples registros de la zona, se recomienda que:

- El valor máximo del TTL de la zona⁸ sea inferior al periodo de validez de la firma (*signature validity*). Si fuera superior, podría haber registros en cachés cuya firma ya no es válida.
- El periodo de refresco sea al menos el equivalente al valor máximo del TTL de la zona antes del fin del periodo de validez de la firma. Es decir, entre el final del *lifetime* y la fecha de expiración de la firma debe haber al menos un TTL. Se intenta

⁸ El TTL es definido globalmente en el registro SOA de la zona.

evitar así el refirmado de la zona al final del periodo de validez ya que además los registros podrían expirar en las cachés debido a su TTL.

- El valor mínimo del TTL de la zona permita la obtención de todos los registros involucrados en la comprobación de la cadena de confianza. Se han identificado problemas a este respecto con TTLs muy reducidos de entre 5 y 10 minutos.
- El periodo mínimo de validez de la firma (*signature validity*) debe ser al menos de unos días (más de 2 días para acomodar contingencias durante el fin de semana, tal como se ha descrito previamente).
- Se recomienda que el plazo de expiración de los registros SOA de la zona (*expire*), sea entre $\frac{1}{3}$ y $\frac{1}{4}$ del periodo de validez de la firma (*signature validity*), con el objetivo de identificar problemas de transferencia de zona antes de que caduquen las firmas.
- El periodo máximo de validez de la firma (*signature validity*) para registros DNSKEY no debe ser mayor de una semana⁹, con el objetivo de minimizar el impacto si las claves (ZSK o KSK) son comprometidas.
- El periodo de comprobación de refirmado (*resign period*) debe ser menor que el periodo de refresco (*refresh period*) para permitir el refirmado de los registros a tiempo, antes de que expiren.

Adicionalmente, existe la posibilidad de establecer en el proceso de firma un tiempo de desviación (*jitter time*) para que el periodo de validez de la firma (*signature time*) varíe ligeramente, de forma que no todas las firmas asociadas a todos los registros de la zona expiren a la vez (no reflejado en la figura y descripciones previas por simplicidad). Este parámetro es especialmente relevante en zonas DNSSEC de gran tamaño.

Se recomienda evaluar, en función del entorno, el valor idóneo para los valores de todos los parámetros de validez de la firma. Por ejemplo, el periodo de validez de la firma (*signature validity*) podría estar en torno 15 días; por su parte, el periodo de refresco debe ser al menos de 2 días, y normalmente es de varios días, por ejemplo 5 días, por lo que el periodo de validez efectivo de un registro firmado (*lifetime*) sería aproximadamente de 10 días, tras el cual se refirmará el RRSet y se generará un nuevo RRSIG.

Por otro lado, el periodo de validez de la firma de distintos tipos de registros (RRsets) puede ser diferente, en función de su criticidad e impacto, por ejemplo, en ataques de repetición. También se deben tener en cuenta ataques de repetición negando que existen datos, es decir, dónde el atacante dispone de un registro previo, junto a su firma, que indican que un recurso no existe, aunque este haya sido añadido posteriormente. En este caso se debe ajustar adecuadamente el periodo de validez de la firma de los registros NSEC y NSEC3.

Los parámetros de tiempo de validez de las firmas empleados por defecto en BIND están descritos, a modo de referencia, en el apartado "6.1.5.2. Firmado automático".

En resumen, para evitar ataques de repetición posibles durante todo el periodo de validez de la clave ZSK para una zona, DNSSEC introduce mayor granularidad en la vigencia de los registros firmados a través del periodo de validez de la firma, reduciendo el periodo de vulnerabilidad de un "RRset vulnerable". El resto de parámetros de tiempo asociados a la validez de las firmas son empleados por el servidor DNS para simplificar y facilitar la planificación del proceso de firmado, y de manera conservadora, evitar escenarios indeseados tanto desde el punto de vista de sobrecarga del servidor como de problemas a la hora de realizar el proceso de refirmado (antes de que expire la firma).

⁹ https://www.stigviewer.com/stig/microsoft_windows_2012_server_domain_name_system/2016-06-30/finding/V-58589

4.1.4. Generación y almacenamiento de las claves criptográficas

De cara a la generación de las claves criptográficas, se recomienda tener en cuenta los siguientes elementos:

- Parámetros relativos al uso de las claves:
 - Definir la política de tiempo de validez de las firmas (*lifetime*) de las claves (ver apartado "4.1.3. Parámetros asociados a la validez de las firmas"). Este elemento tiene relación directa con el siguiente.
 - Prever la política de renovación de las claves, de forma que se permita tanto la renovación planificada como la renovación de emergencia: se recomienda generar un segundo par de claves (tanto KSK como ZSK) con parámetros de tiempo relativos (en función de la planificación de renovación de claves establecida) a las claves que se están empleando en el proceso de firma actual.
- Parámetros relativos a la generación física de las claves: el hardware en el que se generen (y almacenen; ver siguientes puntos) debe ser seguro. Entre las alternativas disponibles, están:
 - Utilizar un HSM (*Hardware Security Module*), o módulo de seguridad hardware, es decir, un dispositivo hardware criptográfico que genera, almacena, permite hacer uso de, y protege, las claves, ya que no permite su extracción fuera del HSM. Es la alternativa más costosa desde el punto de vista económico, pero permite que la clave privada nunca abandone el dispositivo en el que se generó.
 - Emplear un equipo informático desconectado de la red y custodiado de forma segura.
 - El generador de números aleatorios (RNG, *Random Number Generator*) debe ser robusto, basado en estándares (como FIPS) y, preferiblemente, integrado en el hardware, frente a uno basado en funciones de librerías software potencialmente inseguras como "rand()". En la actualidad, se dispone de dispositivos hardware muy económicos que se pueden emplear con este fin. Si no fuese posible emplear un componente hardware, se deberá verificar que se selecciona un generador software que garantice un nivel de entropía suficientemente alto [Ref.- 30].

De cara a los mecanismos de custodia o almacenamiento de las claves criptográficas, se recomienda:

- Mantener las claves privadas inaccesibles a través de la red si es posible, ya sea mediante un HSM o en un sistema desconectado de la red.
 - Para la clave de firma de claves (KSK), que se emplea únicamente para firmar los registros DNSKEY de la zona y generar el registro DS para su inclusión en la zona padre, el firmado puede hacerse (y se recomienda que se haga) *offline*.
No se aconseja trasladar la clave privada KSK a ningún otro dispositivo diferente al que la generó y hace uso de ella, más allá de aquel que se emplee como respaldo o *backup*. Es importante tener en cuenta que, cuando se renueve la ZSK, el nuevo RRSet de tipo DNSKEY tendrá también que ser firmado con la KSK. En este punto, será necesario disponer de esta

última en el servidor donde se realice la operación de firma de los registros DNSKEY.

- Para la clave de firma de la zona (ZSK):
 - Si el firmado del fichero correspondiente a la zona se va a realizar en modo *offline* (ver apartado "4.1.5. Firmado y publicación de zonas DNS con autoridad"), lo más recomendable es no extraer las claves del lugar en el que fueron generadas, y crear una copia de seguridad que se custodie en un sitio seguro tanto desde el punto de vista físico como lógico.
 - En caso de que el firmado se realice en modo *online*, las claves deberán ser trasladadas al servidor DNS autoritativo de la zona, empleando un medio lo más seguro posible y estableciendo un protocolo de transporte adecuado. Idealmente, en este escenario las claves deberían permanecer en un módulo HSM conectado a dicho servidor, o por lo menos, disponer de una configuración que permita delegar en un componente fiable del sistema (*trusted component*) las operaciones criptográficas.

4.1.5. Firmado y publicación de zonas DNS con autoridad

En este apartado se proporcionan las recomendaciones de diseño referentes al proceso de firma y publicación de zonas DNS con autoridad en DNSSEC, que consta de dos fases:

- Firmado de la zona: consiste en generar las firmas criptográficas de los registros DNS (RRsets) pertenecientes a la zona, que se publican como registros RRSIG. En el proceso de firma se identifican dos operaciones diferenciadas:
 - Firmado completo: consiste en firmar todos los registros de la zona. Debe realizarse cuando se firme la zona por primera vez, así como para restaurar el estado del firmado en caso de una emergencia que haya requerido suprimir temporalmente la operativa de DNSSEC, o (según el modo de operación del servidor DNS) al renovar las claves.
 - Mantenimiento de la zona firmada: una vez realizado el proceso de firmado inicial, debe decidirse qué política se empleará para los cambios de la zona (supresión, modificación o adición de registros, o renovación de claves). Las opciones son:
 - Refirmado completo de la zona: esta opción solo es viable para entornos muy estables y con un reducido número de registros. Permite que las claves se custodien de forma aislada respecto al servidor DNS autoritativo, pero implican una gestión manual.
 - Firmado incremental: corresponde al proceso de firmado de los cambios que se producen en la zona ya firmada. Los nuevos registros o los cambios en los registros se firman automáticamente, y los RRSIG correspondientes a los registros eliminados se suprimen. Estos cambios se propagan a los servidores DNS secundarios mediante los mecanismos de transferencia de zona o notificaciones DNS del entorno, que son independientes del uso de DNSSEC. Las versiones actuales de las soluciones DNSSEC ofrecen mecanismos consolidados para firmado incremental en tiempo real de los registros, por lo que este será el modo de firma

recomendado tras la implantación, ya que permite su automatización.

- Establecimiento de la cadena de confianza para la zona: corresponde al proceso de generación del registro DS asociado a la clave pública KSK y su transferencia a la zona padre.

4.1.5.1. Firmado inicial, mantenimiento y publicación de la zona

Este proceso es muy dependiente del modelo de gestión del dominio DNSSEC. Si la gestión está externalizada en un proveedor de servicios externo, conviene conocer en detalle las opciones que el proveedor ofrece para poder seleccionar la más conveniente. Por tanto, este apartado aborda únicamente el modelo de gestión propia.

El proceso de firmado inicial, aunque pueda considerarse una operación independiente, está estrechamente relacionado con el mantenimiento y operación de la zona firmada una vez está en producción, aunque se pueden combinar diversas alternativas.

Desde el punto de vista de dónde se realiza el proceso de firmado, existen dos posibilidades [Ref.- 35]¹⁰:

- **Firmado *offline*** (sin conexión a la red): todas las operaciones de firma se realizan en un sistema externo al servidor DNS que ofrece el servicio, y los registros firmados se transfieren posteriormente y de manera manual al servidor DNS autoritativo primario (este distribuirá la zona firmada al resto de servidores autoritativos secundarios o esclavos mediante las transferencias de zona). Este esquema se denomina habitualmente "*stand alone signer*", y permite que la clave privada de la ZSK no salga del sistema en el que se generó, si es el mismo que aquel en el que se lleva a cabo la operación de firmado de la zona. Se puede emplear este esquema en zonas estáticas o que varían muy poco. También es una opción para el firmado inicial de zonas muy grandes, en las que las operaciones criptográficas consumirán muchos recursos, por lo que es preferible generar las firmas fuera de línea y transferirlas después a los servidores DNS de producción.
- **Firmado *online*** (con conexión a la red): las operaciones de firma se realizan en un servidor que pertenece a la arquitectura y al servicio DNS. Es la opción recomendada para el mantenimiento de zonas muy grandes, que cambian mucho, y necesaria para zonas dinámicas y aquellas donde se requiere utilizar NSEC3. Aunque puede haber más configuraciones posibles, normalmente suele implementarse según dos esquemas (ver "Figura 9"):

¹⁰ Las opciones de arquitectura del servicio DNSSEC planteadas pretenden ofrecer diferentes soluciones para distintos escenarios básicos de uso, pudiendo existir otras combinaciones en función del entorno, que deben evaluarse en cada caso.

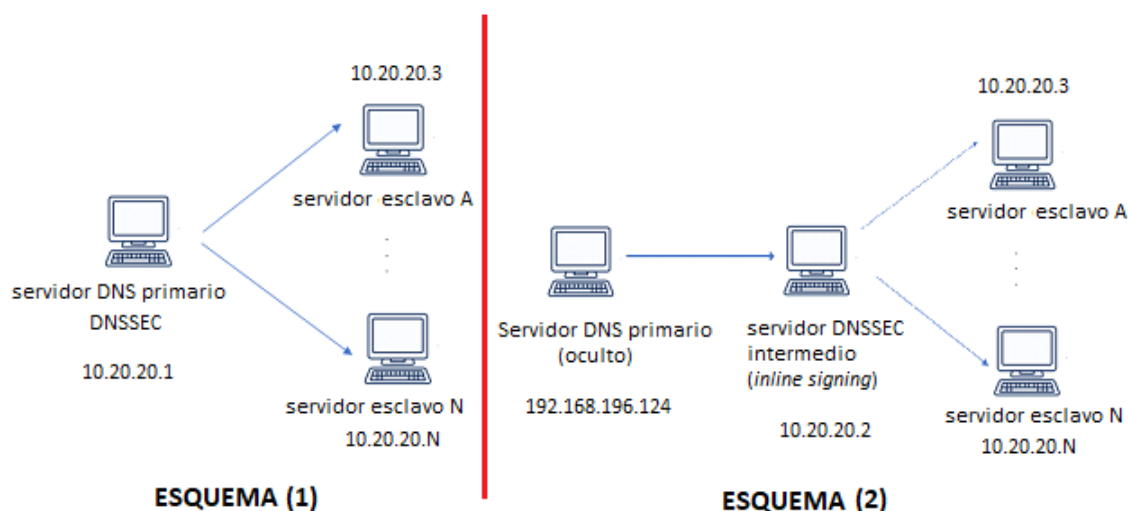


Figura 9 - Firmado online con servidor maestro primario (1) y con servidor maestro oculto (2)

- (1) El servidor maestro primario sirve directamente la zona DNSSEC y firma los registros en tiempo real. Esta opción no es la recomendada desde el punto de vista de seguridad, ya que implica que el material criptográfico se encuentra en sistemas que son accesibles directamente desde Internet (o desde las redes internas o externas a las que dan servicio), pero puede requerirse en configuraciones especiales, como en el escenario de DDNS (*Dynamic DNS* o *Dynamic Updates*); ver apartado "6.1.9. Actualizaciones dinámicas en zonas DNS con DNSSEC activo".
- (2) Un servidor maestro primario oculto o escondido (*hidden*) no accesible desde Internet (o desde las redes internas o externas a las que da servicio) sirve la zona a un servidor intermedio ("Bump in the Wire" [Ref.- 74]), accesible desde los servidores esclavos o secundarios (que, a su vez, sí son accesibles públicamente). Dentro de este escenario, se distinguen dos posibilidades:
 - (2.1) El servidor primario oculto gestiona la zona sin firmar, y la transfiere al servidor intermedio (expuesto a las redes) para su firma. Este a su vez transfiere la zona firmada a los servidores esclavos. Es la configuración más simple de cara a la puesta en marcha y a su posterior mantenimiento, pues permite que el servidor primario no tenga por qué tener habilitado DNSSEC, ni que el software utilizado como servidor DNS sea el mismo que el empleado para DNSSEC en el servidor intermedio y esclavos. Sin embargo, requiere que las claves privadas de firma estén en un sistema accesible desde el exterior, el servidor intermedio.
 - (2.2) Un servidor primario oculto dedicado gestiona la zona y realiza las operaciones de firma, custodiando el material criptográfico, y transfiriendo posteriormente la zona firmada al servidor DNS intermedio. Este a su vez transfiere la zona firmada a los servidores esclavos. Es la opción más recomendada desde el punto de vista de seguridad, porque no expone las claves privadas de firma en los sistemas que ofrecen el servicio DNS. En este escenario se debe

prestar especial atención a que la transferencia de zona entre el servidor oculto y el intermedio se realice de forma segura sobre una conexión cifrada para evitar que los registros puedan ser modificados.

Por otro lado, se debe tener en cuenta que el firmado inicial puede ser *offline* aunque el mantenimiento de la zona firmada se realice posteriormente de forma *online*.

También es preciso tener en mente el modelo de renovación de las claves, ya que, en función del software servidor de DNSSEC elegido, las opciones de configuración empleadas en el firmado de zona pueden variar.

De cara a facilitar y permitir la automatización de la renovación de la clave de zona (ZSK) tras la implantación de DNSSEC, se recomienda tener como mínimo dos claves de firmado de zona, de forma que una de ellas sea la activa y la otra (futura clave ZSK) se publique con antelación (antes de llevar a cabo su sustitución o renovación completa), controlando bien los tiempos que marcan la validez de las firmas de los registros DNSSEC.

4.1.5.2. Establecimiento de la cadena de confianza para la zona

El establecimiento de la cadena de confianza para la zona DNSSEC corresponde a la operación mediante la cual el registro DS (*Delegation Signer*) correspondiente a la clave KSK, a través de las siguientes acciones:

- Se genera en la zona hija.
- Se transfiere a la zona padre.
- Se firma en la zona padre.
- Se propaga a todos los servidores DNS autoritativos de dicha zona padre, haciendo que esté disponible para cualquier *resolver* que lo solicite.

La operativa vendrá marcada por los procesos del agente registrador (*registrar*) o del operador de la zona padre, ya sea esta externa (por ejemplo, en el caso de TLDs de nivel 1) o interna (en caso de subdominios dentro de una zona propiedad de la organización).

En el caso del dominio ".es", es necesario proporcionar a Red.es (por mediación del agente registrador con el que se dio de alta el dominio) el registro DS, sin que Red.es realice ningún tipo de comprobación técnica sobre su validez, según se menciona en el apartado "Segundo.- Custodia y generación de las claves necesarias para el uso del DNSSEC " del documento oficial [Ref.- 57]. En el caso de otros operadores de TLDs, se solicita el registro DNSKEY correspondiente a la KSK, y es el propio operador del dominio el que calcula el registro DS según sus estándares y requisitos (tipo de hash, semilla, etc.).

Por tanto, según el caso, el administrador del TLD de nivel superior podrá:

- Generar él mismo el registro DS a partir de la clave pública KSK (registro DNSKEY) proporcionada por el propietario de la zona.
- Solicitar el registro DS al propietario de la zona.

En cualquiera de los dos casos, tras la publicación del registro DS en la zona padre, deberán llevarse a cabo las oportunas verificaciones para confirmar que el registro DS ha sido correctamente publicado en la zona de nivel superior.

Cuando la gestión de la zona DNS está delegada en un proveedor diferente al agente registrador de la zona, será necesario contactar con ambos para conocer los mecanismos de generación y publicación del registro DS. Lo habitual es que el operador del dominio

proporcione los registros DS que se han de transferir al agente registrador para su carga en el operador de la zona padre.

4.1.6. Selección del software del servidor de DNSSEC

En general, se recomienda elegir un software para el servidor de DNSSEC que simplifique lo más posible su integración con el resto del entorno DNS actual. Por tanto, siempre que sea posible, se aconseja emplear el mismo software que se esté utilizando en la actualidad en el entorno de producción.

Para determinar si esa opción es posible o si será necesario migrar a otro tipo de servidor DNS, hay que determinar las opciones que, según el entorno, son exigibles al software del servidor DNSSEC como, por ejemplo, la facilidad para automatizar la gestión de claves, la simplicidad de configuración inicial, o las capacidades de auditoría del entorno.

En función de los elementos planteados en el apartado "3. Elementos clave para la implantación de DNSSEC", algunos de los criterios para la selección del software son:

- Qué tipos de almacenamiento soporta para las claves privadas.
- Soporte para un esquema de firmado de zona en un servidor oculto.
- Modelo de permisos a nivel de sistema operativo para las claves y los ficheros de zona.
- Capacidad de firmado y refirmado automático de zona sin intervención del administrador.
- Automatización del proceso de renovación de claves.
- Soporte para registros NSEC3 (si el entorno lo requiere).
- Estrategia ante fallos como, por ejemplo, disponibilidad de mecanismos de transferencia segura de las claves al sistema de *backup*, o procedimientos para revocar una clave ZSK y, especialmente, KSK comprometida.

En los inicios de DNSSEC, era preciso firmar las zonas con anterioridad a su despliegue y posteriormente cargarlas en un servidor autoritativo con capacidades de DNSSEC. Con el paso de los años, las implementaciones han ganado en madurez y permiten mayor flexibilidad de cara al despliegue, por lo que en la mayor parte de los casos se podrá recurrir al servidor empleado actualmente en el entorno DNS tradicional.

4.1.7. Utilización y validación de registros DNSSEC

A través del firmado de la zona, se generan las firmas criptográficas que utilizarán los *resolvers* DNSSEC para verificar los registros que el servidor DNS autoritativo de la zona publica hacia los clientes DNS, como RRSIG y DNSKEY.

Dentro de los *resolvers*, se distinguen:

- **Servidores DNS (caché) recursivos:** centralizan las consultas DNS de modo que reciben peticiones de resolución por parte de diversos clientes finales y las gestionan de forma recursiva con los servidores autoritativos correspondientes, manteniendo opcionalmente una caché con las respuestas DNS.
- **Stub resolvers:** los *resolvers* implementados en el cliente final. Aunque lo habitual es que las consultas se cursen a través de un servidor DNS recursivo, puede haber escenarios donde una aplicación o un usuario final realicen el proceso de resolución de nombres directamente.

Los **resolvers** deben estar configurados para validar de manera exhaustiva y estricta todas y cada una de las **consultas DNSSEC** que realizan, indicando sus capacidades DNSSEC mediante el bit "DO" o "AD" en sus consultas, y verificando la firma y validez de todas las respuestas recibidas.

Se recomienda **activar las capacidades de DNSSEC** también en los **stub resolvers**, para que indiquen en sus consultas que están interesados en hacer uso de DNSSEC activando el bit "DO" o "AD" en sus consultas. De lo contrario, si un *stub resolver* pregunta por una zona que está firmada en DNSSEC y hay algún problema en el proceso de validación, el servidor caché recursivo podría devolver un error de DNS estándar. Si se prioriza el uso de DNSSEC, recibirá el error específico y verificado por DNSSEC que indica que la validación ha fallado.

Para que un servidor autoritativo de la zona que implementa DNSSEC sirva los registros firmados, el *resolver* que origine la consulta debe informar de que desea validación mediante DNSSEC, lo cual se configura en el propio *resolver* mediante las opciones correspondientes.

Un *resolver* configurado correctamente y operativo será capaz de:

- Resolver nombres de dominios firmados con DNSSEC y correctamente validados (flag AD o DO).
- Rechazar recursos o dominios DNS que, habiendo sido firmados con DNSSEC, no se pueden validar correctamente.
- Permitir la resolución de dominios no firmados (sin soporte para DNSSEC) empleando el servicio DNS tradicional.

De cara a elegir el software que actuará como *resolver* recursivo, hay que tener en cuenta unos requisitos funcionales mínimos [Ref.- 21]¹¹:

- La validación debe cumplir con los RFCs 4033 [Ref.- 22], 4034 [Ref.- 7] y 4035 [Ref.- 5] y sus actualizaciones.
- La validación debe soportar RSA/SHA1 como describe el RFC 3110 [Ref.- 26], y RSA/SHA256 o RSA/SHA512 según el RFC 5702 [Ref.- 19].
- Debe soportar NSEC3 y DNSSEC *Opt-In* tal como se define en el RFC 5155 [Ref.- 23].
- Debe soportar registros DS con SHA256 según el RFC 4509 [Ref.- 27].

Adicionalmente, se recomienda que la validación soporte la actualización automática de las cadenas de confianza según se describe en el RFC 5011 [Ref.- 28] y la desactivación temporal de la validación para todo o parte del espacio de nombres.

Para que los *resolvers* DNSSEC puedan reconstruir la cadena de confianza completa desde la zona raíz, y a través de las zonas padre e hija, deben tener acceso a la clave KSK de la zona raíz. Esta clave se puede configurar de dos formas:

- **Configuración manual de los anclajes de confianza de la zona raíz**, incluyendo su actualización manual cuando se renueven. Requiere su obtención de la web de IANA y su comparación con un fichero independiente también proporcionado por IANA [Ref.- 37].

¹¹ Los RFCs citados pueden eventualmente haber sido complementados o actualizados con otros más recientes, por lo que se recomienda consultar la documentación de cada RFC en cuestión.

- **Actualización automática de los anclajes de confianza de la zona raíz**, mediante un software que soporte actualizaciones automáticas del *trust-anchor* a través del protocolo “*Automated Updates of DNS Security (DNSSEC) Trust Anchors*” definido en el RFC 5011 [Ref.- 28]. Según este RFC, la clave KSK actualmente vigente firma un RRset que contiene la nueva clave KSK, a fin de que los registros que se firmen con esta última sean reconocidos y la clave KSK se añada como *trust anchor*. Esta nueva clave KSK no pasa a ser de confianza mientras que no transcurra el denominado “*hold-down time*” (período de 30 días durante el cual el RRset de la nueva clave KSK se publica continuamente mediante la clave KSK antigua).

La mayor parte de los *resolvers* recursivos soportan ambos tipos de configuración, manual y automática, entre ellos BIND versión 9 [Ref.- 38], Unbound [Ref.- 39] y Knot DNS [Ref.- 40].

En caso de operar el servidor DNS autoritativo de una zona, se recomienda prestar especial atención a los procesos de renovación de la clave KSK de la zona raíz [Ref.- 41], a fin de conocer con antelación cualquier información relevante en torno a ellos.

Asimismo, es preciso mantener actualizado el software del servidor DNS recursivo, para que incluya la última versión de la clave KSK, y evitar fallos (o *bugs*) y solucionar vulnerabilidades de seguridad existentes en versiones previas.

Por último, se recomienda contrastar periódicamente el *trust-anchor* empleado por el *resolver* con el publicado por ICANN para la zona raíz, a fin de ratificar que no ha sido alterado de forma ilegítima.

4.1.8. Mecanismo de renovación de las claves (*key rollover*)

Aunque no existe ninguna restricción que afecte a la validez de las claves en DNSSEC y, por tanto, no se impone ninguna obligación respecto a su renovación, las buenas prácticas del protocolo recomiendan que las claves se renueven de manera periódica para evitar que la clave privada pueda ser obtenida (con suficiente tiempo) o minimizar el impacto si la clave privada resulta comprometida.

El objetivo principal de la política de renovación de claves es garantizar la consistencia de las respuestas proporcionadas a los *resolvers*, evitando que se produzcan situaciones de denegación de servicio en DNSSEC. Para ello, los cambios en los estados asociados al ciclo de vida de las claves (ilustrados en la “Figura 10”) se realizarán de forma que nunca se devuelvan ni firmas (RRSIG) expiradas ni firmas asociadas a claves que ya no estén disponibles.

Por ello, un punto importante a tener en cuenta es evitar cambiar el valor de los TTLs durante el proceso de renovación de las claves.

La renovación de las claves en DNSSEC debe producirse en dos situaciones:

- En caso de que las claves sean comprometidas, ya que DNSSEC no define ningún mecanismo de revocación [Ref.- 76]: debe disponerse de claves alternativas que puedan sustituir a las actuales en caso de emergencia (ver RFC 5011 [Ref.- 28]).
- Cuando la clave está próxima a su expiración, con la antelación suficiente como para que las firmas de los registros de DNS se actualicen y que los *resolvers* puedan validarlas correctamente.

Además, debe tenerse en cuenta que, desde el punto de vista criptográfico, hay elementos que se almacenan en servidores DNS distintos:

- Las claves de firma se gestionan en el propio entorno del servicio DNS de la zona.
- El registro DS, asociado a la clave KSK, se almacena en el servidor DNS de la zona padre para garantizar la cadena de confianza.

Por tanto, si bien es posible renovar de manera autónoma la clave de firma de la zona (ZSK), no es posible renovar la clave de firma de claves (KSK) sin actualizar su correspondiente registro DS en los servidores DNS autoritativos de la zona padre. Cualquier problema en la sincronización entre la clave KSK y su registro DS, o entre ambas claves KSK y ZSK (ya que la clave ZSK está firmada por la clave KSK), podría dejar la zona inoperativa desde el punto de vista de la resolución de nombres de DNSSEC.

El IETF publicó en octubre de 2015 el RFC 7583 [Ref.- 43], en el que se establecen las recomendaciones para definir adecuadamente los procesos y periodos temporales de renovación de las claves.

La "Figura 10" ilustra el ciclo de vida de las claves [Ref.- 18], mientras que la "Tabla 3" [Ref.- 74] muestra a qué escenario dentro de dicho ciclo de vida corresponden los metadatos de tiempo de una clave (descritos en detalle en el apartado "6.1.3.1. Generación de las claves en el sistema operativo"):

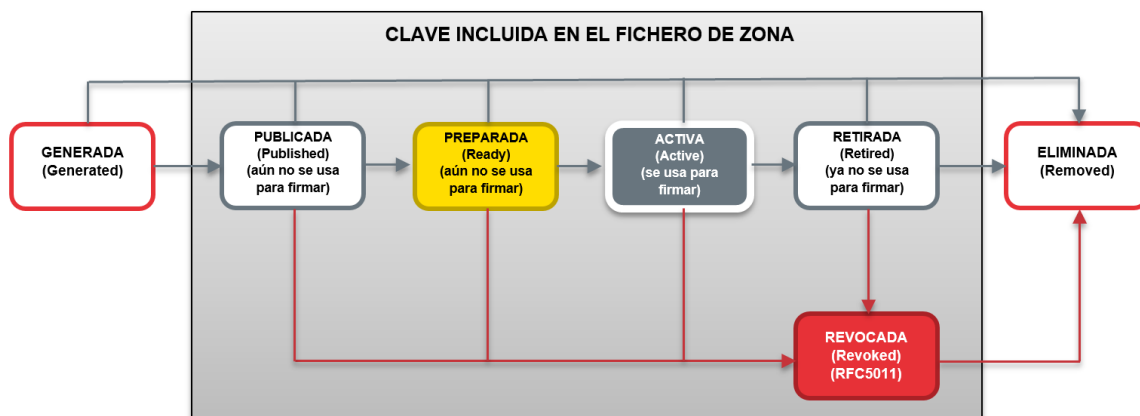


Figura 10 - Ciclo de vida de una clave en DNSSEC

ESTADO	¿Presente en el fichero de la zona?	¿Usada para firmar la zona?	Propósito
Generada	No	No	Generación de la clave
Publicada	Sí	No	Publicación de la clave en la zona
Preparada	Sí	No	Activación futura de la clave planificada
Activa	Sí	Sí	Fecha de activación de la clave para firmar registros
Revocada	Sí	Sí	La clave será retirada próximamente de la zona
Retirada	Sí	No	Clave retirada o inactiva, no empleada para firmar
Eliminada	No	No	Clave eliminada de la zona

Tabla 3 - Propósito de los metadatos de tiempo de la clave en el ciclo de vida de DNSSEC

La transición de un estado al siguiente depende de:

- El período de validez de los registros en la zona (TTL y periodo de validez de la firma).
- El tiempo requerido para transferir la zona a los servidores DNS autoritativos secundarios.
- Los parámetros asociados a la sincronización horaria de los servidores DNS.

4.1.8.1. Renovación de la ZSK

Para la renovación de la clave ZSK se consideran habitualmente dos técnicas distintas (ver RFC 6781 [Ref.- 25]):

- **Publicación anticipada** (*pre-publication o pre-publish ZSK rollover*): consiste en incluir el nuevo registro DNSKEY correspondiente a la nueva clave ZSK en el RRSet actual, junto al registro DNSKEY de la clave ZSK que aún está vigente, hasta tener la seguridad de que todos los *resolvers* tienen la nueva clave (junto a la clave antigua) en caché (evento marcado por el TTL del RRSet de tipo DNSKEY). En ese momento las firmas creadas con la clave antigua pueden ser reemplazadas por las firmas generadas con la clave nueva. Durante el proceso de refirmado (completo u *online*), no importa con qué clave se ha firmado el registro RRSIG obtenido por un *resolver*, ya que ambas claves son válidas. Una vez la zona contiene solo firmas creadas con la nueva clave, se debe esperar a que los registros RRSIG creados con la clave antigua expiren en la caché de todos los *resolvers* (en función del TTL de cada RRSIG), y en ese momento se estará en disposición de eliminar de los registros DNSKEY la clave antigua (ya que no quedarán firmas creadas con esta en ningún *resolver*). Este método es el más complejo, aunque el más óptimo en cuanto al tamaño de la zona y de las respuestas DNSSEC, ya que se debe introducir la nueva clave, aproximadamente en el periodo correspondiente a un TTL, tiempo durante el que

se deben firmar los registros, y aproximadamente en el periodo correspondiente a otro TTL, proceder a eliminar la clave antigua.

- **Doble firma** (*double-signature ZSK rollover*): la nueva clave ZSK se introduce en la zona y se emplea también para firmar los RRsets de todos los recursos, generando nuevos registros RRSIG. Los nuevos y los antiguos RRSIG se sirven a los *resolvers* durante el período de renovación para que exista certeza de que uno de los dos será validado correctamente.

Este método es el más sencillo y el más rápido, pues en el periodo correspondiente a aproximadamente un TTL los *resolvers* dispondrían de las dos copias (tanto los DNSKEYs y los RRSIGs que van a expirar como sus reemplazos), y se podrán eliminar de la zona la clave antigua y sus firmas. Sin embargo, para zonas muy grandes, puede resultar una sobrecarga importante en el tamaño de la zona y de las respuestas DNSSEC, ya que se duplican tanto los registros DNSKEY como, especialmente, las firmas o registros RRSIG de todos los recursos (o RRsets) de la zona.

El proceso de renovación de la ZSK depende también de si la zona se refirma completamente o si los nuevos registros y las actualizaciones se firman incrementalmente en función de su periodo de validez; ver apartado "4.1.5. Firmado y publicación de zonas DNS con autoridad".

NOTA: Existe un tercer mecanismo de renovación de la clave ZSK, definido en el RFC 7583 [Ref.- 43], denominado doble RRSIG (double-RRSIG). El método de doble firma descrito en realidad corresponde a doble firma y doble clave, ya que se publican por duplicado tanto las claves como las firmas. Una variante asociada a este tercer método sería publicar únicamente por duplicado las firmas, pero sin publicar la clave aún. Sin embargo, el mismo queda fuera del alcance de la presente guía, ya que presenta los inconvenientes de los dos métodos anteriores, por lo que es poco probable que se utilice en escenarios reales en producción.

4.1.8.2. Renovación de la KSK

Se recomienda iniciar el proceso de renovación de la clave KSK al menos un mes antes de la fecha prevista de entrada en vigor de la nueva clave.

En el caso de la clave KSK es menos relevante que un resolver no disponga de acceso a la firma creada con una clave KSK válida, ya que la KSK solo se usa para una firma, la del RRset de tipo DNSKEY, y tanto el registro como la firma se transmiten juntos. Lo fundamental en este caso es que la KSK sea de confianza.

Aunque se dispone de dos métodos para la renovación de la clave KSK, la elección de uno u otro método dependerá de los procesos impuestos por la zona padre (ver RFC 6781 [Ref.- 25]):

- **Doble firma o doble KSK** (*double signature KSK rollover o double-KSK*): es el esquema más sencillo, al requerir solo una interacción con la zona padre, pero incrementa el tamaño del RRset de tipo DNSKEY durante el proceso de renovación.
 - Generación de la nueva clave KSK pública, que se añade al RRSet de tipo DNSKEY de la zona.
 - Generación de la correspondiente firma del nuevo RRSet de tipo DNSKEY (por tanto, habrá dos registros RRSIG para el RRSet de tipo DNSKEY, uno firmado con la clave actual y otro firmado con la nueva clave KSK).
 - Notificación a la zona padre del inicio del proceso de renovación:

- Cuando la nueva firma (nuevo registro RRSIG) se propague, y el antiguo registro RRSIG expire de la caché de los *resolvers*, se solicitará a la zona padre que publique el nuevo registro DS (el antiguo ya no será necesario, por lo que se puede cambiar uno por el otro).
- Transcurrido aproximadamente el periodo correspondiente a un TTL del registro DS actual, publicado y definido en la zona padre, la zona hija podrá eliminar el registro DNSKEY de la clave KSK antigua, reduciendo así el tamaño del RRSet asociado a las claves.
- **Doble DS (Double DS):** este suele ser el esquema preferido por los administradores de los TLDs de nivel 1, se mantiene el tamaño del RRset de tipo DNSKEY al mínimo, pero se requieren dos interacciones con la zona padre.
 - Adaptación de los parámetros de tiempo de inactivación y borrado de la antigua clave KSK.
 - Generación de la nueva clave KSK en base a los parámetros de tiempo de su clave predecesora.
 - Generación del registro DS correspondiente a la nueva clave KSK y envío a la zona padre.
 - Publicación por parte de la zona padre del registro DS antiguo y del nuevo, cada uno asociado a un registro DNSKEY diferente (el correspondiente a la clave KSK antigua y a la nueva).
 - Cuando el cambio se propaga a las cachés, la zona hija sustituye el registro DNSKEY antiguo por el nuevo (cambiando efectivamente la clave KSK).
 - Aproximadamente tras el periodo correspondiente a un TTL del registro DNSKEY de la clave KSK antigua, es decir, cuando este expire en las cachés de los *resolvers*, se notificará a la zona padre para que elimine el antiguo registro DS.

Todos los procesos de renovación de claves deben poder realizarse de forma automatizada (aunque planificada), una vez que sus reemplazos estén en estado *preparado*.

Se recomienda que existan dos KSKs y dos ZSKs en todo momento en una zona en estado operativo, a fin de simplificar y asegurar la transición durante la renovación. Una de ellas será la activa y la otra se publicará con antelación, controlando bien los tiempos que marcan la validez de las firmas de los registros de DNSSEC (ver "Figura 7").

NOTA: Al igual que para la ZSK, existe un tercer mecanismo de renovación de la clave KSK, definido en el RFC 7583 [Ref.- 43], denominado doble RRset (double-RRset). Sin embargo, el mismo queda fuera del alcance de la presente guía, ya que presenta los inconvenientes de los dos métodos anteriores, por lo que es poco probable que se utilice en escenarios reales en producción.

4.1.9. Generación de documentación para el despliegue de DNSSEC

Dado que el despliegue de DNSSEC conlleva acciones más allá de la mera configuración del software de DNS, es fundamental elaborar documentación detallada tanto para planificar el despliegue como para simplificar los procedimientos operativos tras la implantación. Se distinguen dos tipos de documentación:

- Documentación de políticas y procedimientos, que incluya las políticas DNSSEC adoptadas y un resumen de procedimientos que describan los controles utilizados para garantizar la fiabilidad del sistema.

- Documentación técnica para el despliegue de DNSSEC en la zona y para la operación de la zona una vez operativa desde el punto de vista de DNSSEC y del software de DNS empleado.

ICANN publicó en el año 2013 el RFC 6841 [Ref.- 42] para orientar a los operadores del servicio DNS sobre los aspectos fundamentales de cara a la elaboración de la documentación denominada "Declaración de políticas y procedimientos para implantar DNSSEC" en una zona determinada; el concepto "*DNSSEC Policy*" (DP), definido en dicho RFC, identifica los requisitos que debe cumplir un sistema para garantizar un determinado nivel de seguridad, que deberá demostrarse a través de auditorías; el término "*DNSSEC Practice Statement*" (DPS) identifica los procedimientos y controles implementados en la gestión de una zona.

La DP permite establecer elementos operativos comunes a varias zonas de la jerarquía. Sin embargo, el DPS aplica a una única organización o una única zona, y especifica los medios por los que el responsable de la entidad cumple los requisitos definidos en la política.

El documento correspondiente a esta "Declaración de políticas y procedimientos para implantación de DNSSEC" debe contener los siguientes apartados:

- Control documental, incluyendo fecha de redacción, autor, revisor y registro de las diferentes versiones y control de cambios.
- Introducción, incluyendo la definición de los términos que se vayan a emplear a lo largo del documento, los datos administrativos de la organización y el mecanismo para solicitar cambios en los procedimientos detallados en el documento.
- Repositorio seguro: referencia a la localización de las claves ZSK y KSK y a otros elementos de DNSSEC que tienen carácter confidencial.
- Requerimientos operacionales: incluyendo los procedimientos de renovación y eliminación de registros DS.
- Infraestructura: protección de los sistemas ante riesgos intrínsecos a su condición física (como fallos de corriente, protección contra incendios o inundaciones, etc.).
- Auditorías: sistema de registro de eventos, copia de seguridad de *logs*, etc.
- Definición de los procedimientos ante emergencias e incidentes de seguridad.
- Controles técnicos de seguridad:
 - Generación de las claves (incluyendo sus parámetros).
 - Distribución de la clave pública KSK.
 - Protección de las claves privadas ZSK y KSK (elemento criptográfico, respaldo de la clave, activación y desactivación).
 - Período de uso de las claves ZSK y KSK.
 - Sincronización de tiempos entre los servidores del entorno DNSSEC.
- Firmado de la zona:
 - Tipo de claves, algoritmos criptográficos empleados y periodo de validez.
 - Formato de la firma.
 - Renovación de las claves ZSK y KSK.
 - Frecuencia de refirmado de la zona.
 - TTL de los registros DNSKEY.

A modo de ejemplo, se recomienda consultar el documento "Declaración de Políticas y Procedimientos para DNSSEC de la zona .ES", elaborado por Red.es [Ref.- 34].

Respecto a la documentación técnica asociada al despliegue de DNSSEC, habrá de incluir:

- Identificación de los algoritmos de firma.
- Identificación del tipo de claves criptográficas, el algoritmo de hash empleado y el tipo de semilla (por ejemplo, para registros DS o NSEC3).
- El software empleado para la generación de las claves, especificando la versión concreta.
- El software empleado tanto para los servidores DNS autoritativos como para los *resolvers*, especificando las versiones concretas.
- El mecanismo utilizado para la generación de las claves.
- El procedimiento utilizado para firmar la zona, especificando si se realizará en modo *online* o en modo *offline*.
- El procedimiento utilizado para generar la cadena de confianza y la transferencia del registro DS a la zona padre, incluyendo las acciones para verificar su disponibilidad y operatividad.
- El mecanismo de transferencia de zona a los servidores DNS secundarios.
- Los procesos mediante los cuales se llevarán a cabo las actualizaciones de registros de la zona.
- Los mecanismos de renovación de claves.

4.2. Transferencia de una zona firmada a otro proveedor

La decisión de transferir la gestión de una zona firmada con DNSSEC a otro proveedor requiere una planificación concienzuda, que pasa por contactar con ambos operadores para acordar la secuencia de pasos, los tiempos y los requisitos necesarios.

A continuación, se presenta una lista de comprobación que convendrá revisar y cotejar con los agentes implicados. Esta lista se ha obtenido a partir de la presentación de la reunión de ICANN número 37, celebrada en 2010 [Ref.- 58], pero cuyas recomendaciones siguen vigentes, y ha sido cotejada con el RFC 6781 [Ref.- 25], que tiene categoría informativa.

Por simplicidad, se denominará AO (antiguo operador) al que dejará de operar la zona, NO (nuevo operador) a quien se hará cargo de la zona, R (*registry*) al operador del TLD de nivel superior y P (propietario) al responsable del dominio.

1. P solicita a NO que se encargue de la operación de la zona. NO contacta con AO para cooperar en la transmisión de los ficheros de la zona y acuerdan un periodo de transición. La transferencia de la zona deberá incluir los registros DNSKEY de la zona.
2. AO no deberá realizar ningún proceso de renovación de claves ZSK o KSK durante este periodo.
3. NO incorporará la ZSK proporcionada por AO y firmará con ella la zona para regenerar los registros RRSIG y NSEC.
4. NO generará una nueva clave ZSK (y sus correspondientes registros DNSKEY), que será añadida a los servidores de AO.
5. Tras completar los pasos 3 y 4, los RRsets de tipo DNSKEY de AO y NO contendrán tanto la clave ZSK de AO como la de NO.
6. NO generará un nuevo registro DS para la zona, asegurándose de que el antiguo registro DS de AO permanece aún en la zona padre.

7. P solicitará a R (a través del agente registrador) la publicación del nuevo registro DS generado por NO.
8. Se debe esperar a que el TTL más largo expire de entre los siguientes: TTL del registro NS de la zona en AO, TTL del registro NS en la zona padre (en la mayor parte de los casos, este será el TTL mayor), TTL del registro DS de la zona en AO.
9. AO apuntará los registros NS de la zona hacia los servidores de NO.
10. P solicitará a R (a través del agente registrador) que los registros NS en la zona padre apunten a los servidores de NO.
11. Se debe esperar a que todos los registros NS de la zona en los servidores de AO expiren (en base al mayor TTL de los registros NS de la zona), a fin de que los nuevos registros NS de NO sean visibles globalmente.
12. Detener el servicio DNSSEC en AO. Si esta acción se realizase antes de este momento, se producirían fallos importantes de resolución. Si esta acción se demora, algunos *resolvers* podrían seguir tratando de resolver vía AO, en lugar de NO, y no detectar el cambio.
13. Comprobar que la resolución vía DNSSEC está operativa en NO.
14. P solicitará a R (a través del agente registrador) la eliminación de los registros DS correspondientes a AO en la zona padre.
15. Eliminar la clave ZSK de los servidores de AO.

Si, además de la gestión del dominio, se deseara delegar en NO el registro del mismo (en caso de que NO también ejerza como agente registrador), se debe primero proceder al cambio en la gestión del dominio y, posteriormente, cambiar el agente registrador.

En caso de que no exista cooperación entre los agentes implicados, la opción más sencilla pasa por inhabilitar DNSSEC para la zona durante el tiempo que dure el cambio:

1. P solicitará a R (a través del agente registrador) la eliminación del registro DS gestionado por AO.
2. P solicitará a R (a través del agente registrador) que apunte los registros NS de la zona a los servidores de NO.
3. Una vez el cambio se haya propagado de forma exitosa, NO firmará la zona y generará el nuevo registro DS.
4. P solicitará a R (a través del agente registrador) la publicación del nuevo registro DS gestionado por NO.

4.3. Monitorización de DNSSEC

Los principales requisitos de una herramienta de monitorización para DNSSEC son:

- Debe comprobar que las firmas se actualizan según la política definida y la configuración que aplique.
- Debe comprobar que los servidores de nombres responden con autenticación positiva a los registros SOA, NS y DNSKEY.

- Debe comprobar que los servidores de nombres responden de forma correcta y autenticada a las situaciones de denegación de existencia (NSEC/NSEC3).
- Debe comprobar que las transferencias de zona se realizan correctamente en todos los servidores de nombres autoritativos.
- Debe comprobar que todos los servidores de nombres se sincronizan correctamente a nivel de fecha y hora.

4.4. Resumen de las recomendaciones de diseño de DNSSEC

A continuación, se proporciona una tabla resumen con las diferentes recomendaciones de diseño para DNSSEC detalladas a lo largo del presente capítulo:

- Algoritmos de firma, tamaño de clave y periodo de renovación recomendados para las claves ZSK y KSK:

Tipo de clave	Algoritmo de firma	Tamaño de clave	Renovación
KSK	RSA-SHA256	2.048 bits	1 – 2 años
	ECDSA con curva P-256 o P-384	f = 224 – 255 bits	
ZSK	RSA-SHA256	1.024 bits	1 – 3 meses
	ECDSA con curva P-256 o P-384	f = 224 – 255 bits	1 – 2 años

Tabla 4 - Recomendaciones criptográficas y de renovación para las claves DNSSEC

NOTA: El rango del parámetro "f" (224-255) en el tamaño de clave de la tabla superior para firmas con curva elíptica (ECDSA) especifica el tamaño de "n", siendo "n" el orden del punto base G. "f" es considerado comúnmente como el tamaño de la clave¹² [Ref.- 75].

- Uso de NSEC3 vs NSEC: se recomienda el uso de NSEC3 únicamente cuando exista un SLA o en caso de que la enumeración de zona pueda resultar crítica.
- Parámetros de tiempo para la validez de la firma, relacionados con el firmado de la zona (definen la validez de los registros RRSIG y su regeneración):
 - Los múltiples detalles y recomendaciones para los diferentes parámetros de tiempo están disponibles en el apartado "4.1.3. Parámetros asociados a la validez de las firmas".
- Generación y custodia de las claves:
 - En un módulo HSM.
 - En un servidor no accesible desde la red (si lo permite la actual arquitectura DNS).
- Firmado inicial de la zona:
 - Se recomienda realizar el firmado inicial de la zona de modo que las claves privadas no sean accesibles desde el exterior. Las alternativas son:
 - En modo *offline* (no accesible desde la red).

¹² <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>

- En modo *online*, usando un servidor oculto que realiza el proceso de firmado y transfiere la zona firmada a los servidores autoritativos, siendo accesible solo desde ellos.
- Mecanismo de renovación de claves:
 - Definir un procedimiento que permita realizar la renovación de las claves de forma manual para casos de emergencia.
 - Disponer de un procedimiento de renovación de claves automático.
 - Esquema de pre-publicación de la nueva clave para la clave ZSK.
 - Esquema de doble firma para la renovación de la clave KSK.
 - Generación de un segundo par de claves de cada tipo (ZSK y KSK) que simplifique la renovación futura de ambas.
- Validación de registros DNSSEC:
 - Selección del software DNS para el *resolver* que permita configuración manual del *trust-anchor* y también soporte actualizaciones automáticas del mismo.
- Establecer un mecanismo de monitorización del entorno DNSSEC que asegure que este funciona según lo esperado.
- Generación de documentación del despliegue de DNSSEC:
 - Documento de políticas y procedimientos.
 - Documentación técnica para el despliegue y la operación.

La "Tabla 5" resume las recomendaciones de longitud y *lifetime* asociadas a las claves ZSK y KSK en función del algoritmo de firma seleccionado:

Algoritmo de firma / hash	Longitud KSK (bits)	Longitud ZSK (bits)	Lifetime ZSK (días)	Lifetime KSK (días)
RSA/SHA256	2.048	1.024	32	367
ECDSA P 256/SHA256	256	256	32	367
RSASHA1 NSEC3/SHA1	2.048	1.024	32	367

Tabla 5 - Recomendaciones de longitud y lifetime de las claves DNSSEC

5. MIGRACIÓN Y COEXISTENCIA DE DNS Y DNSSEC

Durante el tiempo desde que se inicia el despliegue de DNSSEC y hasta que los mecanismos de comprobación del despliegue demuestren que la zona está completamente operativa y los *resolvers* son capaces de validar correctamente las consultas DNSSEC, es preciso asegurar que no se devolverán errores que puedan ocasionar una denegación de servicio en el servicio DNS.

5.1. Transición de DNS a DNSSEC

La transición de DNS a DNSSEC implica el establecimiento de nuevas relaciones con el operador del registro encargado del TLD de nivel superior (zona padre) del que cuelga la zona. Esta relación, que en DNS se limitaba a publicar los registros NS correspondientes, se amplía debido a la necesidad de incluir la nueva zona en la cadena de confianza de DNSSEC a través de la inclusión del registro DS en la zona padre, y a tener en cuenta los procedimientos implantados por esta de cara a la renovación de la clave KSK.

Más allá de esto, dado que DNSSEC fue diseñado para poder coexistir con DNS, la existencia de subdominios (o subzonas) delegadas que implementen DNSSEC con otros que no lo hagan dentro de una misma zona no debe plantear ningún problema.

En general, para minimizar la dificultad de la transición, se recomienda utilizar para DNSSEC el mismo software que en el entorno DNS tradicional, tanto para el servidor como para el cliente, ya que ello:

- Aprovecha el conocimiento actual de los administradores acerca del entorno empleado para el servicio DNS.
- Simplifica y agiliza la detección y corrección de posibles fallos.
- No requiere trasladar la configuración actual de la arquitectura DNS a un nuevo entorno.

Es importante que el despliegue de DNSSEC se notifique a los usuarios, a quienes se debe proporcionar instrucciones para que informen sobre cualquier mensaje de alerta o aviso que puedan recibir, y que ofrezca una pequeña guía con los códigos de los mensajes que pueden informar de irregularidades serias (como denegaciones de servicio por operativa incorrecta del servidor DNS caché desde el punto de vista de DNSSEC, o alertas reales que se puedan asociar a un fallo de validación debido al compromiso de un dominio firmado).

5.2. Recomendaciones de seguridad

De nuevo, la transición del servicio DNS a DNSSEC se puede orientar desde dos puntos de vista: el servidor DNS con autoridad sobre la zona DNSSEC, y el *resolver* con capacidades de validación de las transacciones DNS mediante DNSSEC (foco del presente apartado).

5.2.1. Transición de zonas con autoridad de DNS a DNSSEC

Debido a que la presente guía se centra en todos y cada uno de sus apartados en ofrecer recomendaciones y buenas prácticas para hacer uso de DNSSEC en una zona, asumiendo

en todo momento que en la zona ya se dispone del servicio DNS tradicional, no se profundizará más en detalle en dicha transición en el presente apartado.

5.2.2. Transición de *resolvers* de DNS a DNSSEC

Normalmente, la mayor parte de las organizaciones utilizan para la resolución de nombres servidores DNS caché recursivos, lo cual permite que el cliente final no deba realizar consultas iterativas directamente y descargar a su vez de trabajo a los servidores DNS autoritativos. Sin embargo, estos servidores caché suelen ser el principal objetivo de ataques de envenenamiento de caché, ya que, desde el punto de vista de un atacante, generalmente no suele compensar dirigir su ataque a un único sistema final frente al sistema centralizado que proporciona respuestas DNS a todos los demás clientes.

Hay que destacar el hecho de que la validación DNSSEC solo será exitosa si todos los servidores caché recursivos definidos para un grupo o conjunto de clientes la emplean correctamente, pues en caso de que uno solo no lo haga, no se podrá asegurar que se eviten los riesgos derivados de la no utilización de DNSSEC.

Las versiones recientes de los principales paquetes de software DNS que implementan servidores caché recursivos soportan DNSSEC. Es importante asegurarse de que se dispone de la última versión de software, tanto para garantizar que el *trust-anchor* raíz que traen (habitualmente) precompilado los servidores DNS es el vigente, como para minimizar los fallos de seguridad debidos a problemas y vulnerabilidades conocidas ya resueltas.

Se recomienda obtener una copia del *trust-anchor* de la zona raíz [Ref.- 37] a través de un enlace HTTPS seguro, y validarlo con la copia disponible en el software DNS del servidor, igual que se sugirió en el apartado "4.1.7. Utilización y validación de registros DNSSEC".

Se recomienda instalar y configurar el software con soporte para DNSSEC en algún servidor DNS de prueba y realizar en él las verificaciones necesarias antes de realizar el despliegue en el servidor DNS de producción. Durante la fase de pruebas, se elegirá un grupo de sistemas finales o clientes en los que se configurará el *resolver* de modo que solicite las consultas de resolución de nombres mediante DNSSEC.

Además de realizar el proceso de validación, los servidores DNS caché clasifican internamente los RRsets que reciben como respuesta a una consulta, y comunican los resultados a los clientes finales, en base a tres estados [Ref.- 75]:

- **Seguros:** cuando la verificación de la firma ha sido exitosa. Estos registros se mantendrán en caché según su TTL y siempre que no se exceda el periodo de validez de la firma. Las respuestas proporcionadas por el *resolver* llevan el flag AD (*Authenticated Data*) activo.
- **Inseguros** (respuestas de zonas sin soporte de DNSSEC): cuando no se ha podido realizar la validación de la respuesta, al no recibirse registros propios de DNSSEC en la respuesta, y no esperar recibirlos, como en el caso de subzonas sin soporte para DNSSEC debido a la no existencia del registro DS del dominio en la zona padre. En función de la política (o nivel de permisividad) definida en el cliente final, podrá ocurrir que no se confíe en el registro y que la resolución falle, o que este se dé por bueno. Las respuestas proporcionadas por el *resolver* no llevan el *flag* AD activo.
- **Bogus** (falso): cuando la verificación de la firma ha fallado (la respuesta no coincide con la firma del registro RRSIG o el RRSIG ha expirado). En función de cómo este

configurado, el *resolver* caché podrá desechar dicha respuesta o incluirla en una caché especial denominada BAD caché. En las respuestas proporcionadas por el *resolver*, el *flag AD* no estará activo.

Para que un *resolver* final con soporte para DNSSEC pueda transmitir al servidor DNS caché que quiere que le envíe los registros *bogus*, incluirá el bit CD (*Checking Disabled*) en la cabecera del mensaje DNS. Si no lo incluye, el servidor caché devolverá un error.

Desde el punto de vista de seguridad, se debe evitar confiar en los registros *bogus*. Sin embargo, en ocasiones este escenario se puede presentar como consecuencia de una renovación de las claves no exitosa. Por tanto, será precisa la intervención manual del administrador en caso de que la resolución DNSSEC para una zona falle, afectando a todos sus registros, a fin de determinar si se trata de una zona comprometida debido a un incidente de seguridad o de una renovación de clave fallida.

Adicionalmente, en el período inicial de despliegue de DNSSEC, se puede recurrir a mecanismos NTA (*Negative Trust Anchors*; ver apartado "7.8.2.1. Negative Trust Anchors (NTA)") para evitar fallos de validación intermedios.

6. IMPLANTACIÓN

A lo largo del presente apartado se proporcionarán recomendaciones para completar los pasos necesarios para llevar a cabo la implantación de DNSSEC. El alcance de la presente guía no incluye detalles ni sobre la instalación del software DNSSEC para una plataforma concreta, ni sobre la configuración completa de una zona DNS.

Se proporcionan ejemplos de configuración, la mayor parte de ellos basados en BIND, con el objetivo de ilustrar las distintas fases asociadas al despliegue e implantación de DNSSEC de forma granular.

La última versión de BIND a fecha de elaboración de la presente guía es la 9.12, y es la versión que ha sido empleada para los ejemplos mostrados (sobre Linux/Debian), tanto para servidores DNS autoritativos como para *resolvers*. La utilización de las herramientas y utilidades asociadas a BIND, así como las opciones y parámetros disponibles, pueden variar significativamente entre versiones.

6.1. Servidores DNSSEC autoritativos

Algunas de las soluciones más extendidas (pero no las únicas) que ofrecen soporte para DNSSEC de forma estable son:

- BIND [Ref.- 38]: es un estándar de facto para servidores DNS autoritativos en el mundo Unix/Linux, de código abierto y que ofrece también capacidades de *resolver*.
- Windows 2012/2016 DNS Server: ofrece un interfaz gráfico de configuración para la administración del servidor DNS nativo en entornos Microsoft Windows.
- PowerDNS [Ref.- 55]: dispone de capacidades de servidor DNS autoritativo de código abierto, con soporte para múltiples *backends* y bases de datos. Ofrece también capacidades de *resolver*, dentro de sus distintos modos de operación [Ref.- 56]. PowerDNS trata normalmente las firmas y las claves como entidades diferentes, almacenándolas en tablas distintas dentro de la misma base de datos.
- Knot-DNS [Ref.- 40]: ofrece un servidor DNS autoritativo de código abierto con capacidades para la gestión automatizada de claves, incluyendo su renovación.
- Unbound [Ref.- 39]: servidor DNS de código abierto que ofrece capacidades de servidor autoritativo y de *resolver*.

Adicionalmente, se sugiere la evaluación del proyecto OpenDNSSEC [Ref.- 46], un proyecto de código abierto desarrollado conjuntamente en base a una cooperación internacional entre varios organismos (incluido ICANN) para simplificar el despliegue de DNSSEC en una zona, incluyendo las tareas de firmado de zona, publicación de la zona en un servidor DNS autoritativo y el mantenimiento de las claves de DNSSEC. No se trata de un software para servidores DNS, sino que es una herramienta de gestión cuyo objetivo es simplificar el despliegue de DNSSEC en su conjunto, sin tener que entrar en los diferentes detalles técnicos. Para ello, proporciona una serie de utilidades que permiten firmar una zona, obtener el registro DS para publicarlo en la zona padre, o migrar una zona DNSSEC ya existente a OpenDNSSEC. Todas estas opciones se describen de forma sencilla en la documentación oficial [Ref.- 47], por lo que quedan fuera del alcance de la presente guía.

6.1.1. Activación de DNSSEC en el servidor DNS autoritativo

El proceso de activación de DNSSEC en el servidor DNS autoritativo es habitualmente sencillo. Por ejemplo, para indicar a BIND que debe proporcionar los diferentes registros DNSSEC de la zona en sus respuestas cuando reciba una petición DNSSEC, se debe añadir opción "dnssec-enable yes;" en el fichero "*named.conf*"¹³, e incluso, en las últimas versiones de BIND, esta está ya activa por defecto.

6.1.2. Selección de los algoritmos de firma y características criptográficas

En el apartado "4. Recomendaciones de diseño" se indicó que los algoritmos de firma de curva elíptica proporcionan más robustez que los de tipo RSA con un menor tamaño de clave y producen firmas más cortas, pero que aún existe un porcentaje de *resolvers* que no soportan ECDSA y no todos los agentes registradores lo ofrecen como opción. Por otra parte, RSA es el algoritmo más extendido entre los TLDs de primer nivel. Sin embargo, dado que estas condiciones pueden cambiar en un futuro próximo, se proporcionarán ambas alternativas de implementación.

Para las zonas que requieran implementar NSEC3, se utilizará como algoritmo de firma RSA (RSASHA1-NSEC3/SHA1).

6.1.3. Generación de las claves KSK y ZSK y firmado de la zona

Una vez determinados los parámetros asociados al ciclo de vida de una clave y la política de renovación, se procederá a generar los dos pares de claves (pública y privada; en adelante, dos claves) que se usarán para el firmado de la zona, ZSK y KSK. Ambas claves se publicarán y activarán inmediatamente. Adicionalmente, siguiendo las recomendaciones de diseño, se generará un segundo conjunto de claves de respaldo que se publicarán inmediatamente, pero no se activarán hasta el plazo que se indique en la política de claves. De este modo, BIND añadirá los registros DNSKEY asociados a estas dos claves de respaldo al fichero de zona, pero no los empleará para firmar hasta que llegue el momento.

A continuación, se proporcionan las pautas generales de configuración de ambos escenarios, pero se recomienda consultar el manual de administración de BIND 9 [Ref.-48] para obtener los detalles concretos para cada plataforma.

BIND 9 permite la generación y el almacenamiento de las claves tanto en un equipo Unix/Linux (sea o no el que actúa como servidor DNS autoritativo de la zona) como en un dispositivo HSM.

Para generar las claves es preciso asegurarse de que se dispone de un generador de números aleatorios que presente un nivel de entropía suficiente. Si no es posible recurrir a un dispositivo hardware especializado, se puede utilizar el pseudo-generador de números aleatorios de Unix/Linux, preferiblemente `/dev/random`. No obstante, como los servidores DNS no suelen ser máquinas con dispositivos de entrada/salida ampliamente utilizados, se puede optar también por instalar algún componente software que, basado en elementos como el tiempo de ejecución de determinado código en un procesador y otras actividades aleatorias, incrementen el nivel de entropía de `/dev/random`.

¹³ A lo largo de la presente guía, el fichero de configuración de BIND será referenciado como "*named.conf*" (por ejemplo, disponible bajo `/etc/bind/named.conf`), independientemente de que los parámetros de configuración puedan añadirse a este fichero, al fichero "*named.conf.options*", o a cualquier otro fichero de configuración específico de la zona.

6.1.3.1. Generación de las claves en el sistema operativo

BIND 9 proporciona una utilidad denominada "dnssec-keygen" que simplifica la generación de claves para su uso en DNSSEC, según se define en los RFCs 2535 y 4034 [Ref.- 7]. Los argumentos dependen de la versión concreta de BIND, por lo que debe consultarse la documentación específica de cada versión. En la versión 9.12 de BIND, entre otros, los argumentos principales de esta utilidad son:

- -a <algoritmo de firma>: opción empleada para especificar el algoritmo de firma a utilizar y generar las claves adecuadas (ej. RSA, ECDSA...).
- -b <tamaño de clave>: especifica el tamaño de la clave en bits; no es necesario para algoritmos ECDSA.
- -3: esta opción comprueba que el algoritmo de firma seleccionado es compatible con el uso de NSEC3.
- -fk: opción empleada para generar la clave KSK.
- -r <dispositivo_random>: opción que permite proporcionar como parámetro un fichero que contenga datos aleatorios. Si se omite, utiliza "/dev/random" como dispositivo por defecto.
- -l: opción para indicar un TTL propio para el registro DNSKEY de la clave a generar. Si no se especifica, se empleará el TTL del registro SOA.

GENERACIÓN DE LAS CLAVES ZSK (para el firmado de la zona):

Creación del directorio en el que se desea que se almacenen las claves. El path o referencia a este directorio se debe añadir en el fichero "named.conf" dentro de la sección "key-directory". Para el ejemplo utilizado a continuación, se considera que las claves se generan en "/etc/bind/keys".

Generación de la clave ZSK para una zona denominada "ejemplo.es":

```
$ cd /etc/bind/keys
$ dnssec-keygen -a [RSASHA256 | NSEC3RSASHA1 | ECDSAP256SHA256] -b 1024
ejemplo.es
Generating key pair.....+++++ ..+++++
Kejemplo.es.+008+64698
```

El algoritmo de firma que se facilita como parámetro ("-a") será uno de los indicados entre corchetes, según el que se considere más idóneo para la zona.

Como resultado, en el directorio "/etc/bind/keys" se generarán estos ficheros¹⁴:

```
$ ls -xla
total 16
-rw-r--r-- 1 root bind 429 Jun 11 06:38 Kejemplo.es.+008+43530.key
-rw----- 1 root bind 1012 Jun 11 06:38 Kejemplo.es.+008+43530.private
```

Generación de la clave ZSK de respaldo para la zona, de forma que su publicación sea inmediata ("-P now"), pero no se activará hasta el periodo marcado por la opción "-A +<periodo_hasta_activación>":

¹⁴ Tras la generación de los dos ficheros de clave se debe verificar que ambos (".key" y ".private") pertenecen al grupo "bind" (empleado por BIND) y que BIND dispone de permisos de lectura sobre ambos y sobre el directorio que almacena las claves.

```
$ dnssec-keygen -a [RSASHA256 | NSEC3RSASHA1 | ECDSAP256SHA256] -b 1024
-P now -A +<periodo_hasta_activación> -r /dev/random ejemplo.es
```

GENERACIÓN DE LAS CLAVES KSK (para el firmado de las claves):

Generación de la clave KSK para una zona denominada "ejemplo.es":

```
$ dnssec-keygen -a [RSASHA256 | NSEC3RSASHA1 | ECDSAP256SHA256] -b 2048
-fk ejemplo.es
Generating key pair.....+++
.....+++
Kejemplo.es.+008+0346
```

Generación de la clave KSK de respaldo para la zona:

```
$ dnssec-keygen -a [RSASHA256 | NSEC3RSASHA1 | ECDSAP256SHA256] -b 2048
-P now -A +<periodo_hasta_activación> -r /dev/random -fk ejemplo.es
```

Tras generar las dos claves para el firmado inicial, ZSK y KSK, sin considerar las claves de respaldo, dentro del directorio de creación (en este caso, "/etc/bind/keys"), se dispondrá de 4 ficheros, dos para la clave ZSK y otros dos para la clave ZSK. De cada par, un fichero corresponde a la clave pública (.key) y otro a la clave privada (.private)¹⁵:

```
$ ls -xla
total 24
-rw-r--r-- 1 root bind 602 Jun 11 06:39 Kejemplo.es.+008+03436.key
-rw----- 1 root bind 1776 Jun 11 06:39 Kejemplo.es.+008+03436.private
-rw-r--r-- 1 root bind 429 Jun 11 06:38 Kejemplo.es.+008+43530.key
-rw----- 1 root bind 1012 Jun 11 06:38 Kejemplo.es.+008+43530.private
```

Figura 11 - Comandos BIND para generar las claves DNSSEC: ZSK y KSK

El nombre de los ficheros generados emplea la siguiente nomenclatura:

```
K<nombre de la clave o zona>.<código del algoritmo de firma>
+<identificador o huella de la clave>.<key || .private>
```

El fichero con extensión ".key" tiene el formato del registro DNSKEY que se publicará en la zona y que contiene (entre otros parámetros, como por ejemplo el algoritmo de firma empleado) la clave pública. El fichero con extensión ".private" corresponde a la clave privada y contiene adicionalmente los parámetros específicos del algoritmo de firma. Es importante que este fichero no disponga de permisos de lectura genéricos.

Además del material criptográfico, el fichero correspondiente a la clave pública (".key") contiene varias líneas con comentarios (precedidas de ";") que representan metadatos de tiempo (fecha y hora) utilizados por el servidor DNS localmente para definir el ciclo de vida de las claves según el modelo descrito en la "Figura 10" [Ref.- 74]:

¹⁵ No se consideran para este ejemplo las claves de respaldo, con el objetivo de simplificar el listado de ficheros.

- **Generada o Creada** (*Generated o Created*): paso inicial de creación o generación de la clave. Los metadatos de tiempo para este estado reflejan el momento en el que la clave fue generada.
- **Publicada** (*Publish o Published*): la clave ha sido publicada en la zona (mediante los registros DNSKEY asociados), aunque todavía no se emplea para firmar ningún registro. Habitualmente, la nueva clave se publica para posteriormente renovar una clave antigua, por lo que también sirve de mecanismo de notificación a los *resolvers* para indicar que se va a introducir una nueva clave en la zona próximamente. Los metadatos de tiempo para este estado reflejan la fecha que establece cuando la clave será publicada en la zona.
- **Preparada** (*Ready*): la clave está publicada en la zona y su activación ha sido planificada en una fecha futura; todavía no es empleada para firmar ningún registro (no existen metadatos de tiempo específicos para este estado).
- **Activa** (*Activate*): la clave ha sido activada en la zona, es decir, está incluida en la zona y es empleada para firmar los registros DNSSEC. Los metadatos de tiempo para este estado reflejan la fecha en que la clave entrará en el estado activo.
- **Revocada** (*Revoked*): la clave ha sido revocada de la zona mediante el flag REVOKE. Mientras, la clave se incluirá en la zona y será empleada para firmar los registros DNSSEC (si los metadatos de la clave tienen una fecha "Publicada" válida), permitiendo indicarle a los *resolvers* que próximamente la clave será retirada de la zona. Los metadatos de tiempo para este estado reflejan la fecha en que la clave será revocada.
- **Retirada o Inactiva** (*Inactive o Retired*): la clave ha pasado al estado inactivo en la zona, es decir, aunque todavía será incluida en la zona, ya no será empleada para firmar ningún registro. Los metadatos de tiempo para este estado reflejan la fecha en que la clave pasará a estar inactiva en la zona, es decir, fijan la fecha de expiración o retirada de la clave.
- **Eliminada** (*Removed, Delete o Unpublished*): la clave ha sido eliminada de la zona, finalizándose la publicación de la misma (aunque siga existiendo en el sistema de ficheros o en el repositorio de claves del servidor DNS). Los metadatos de tiempo para este estado reflejan la fecha en que la clave será eliminada de la zona.

Esta información de tiempos asociada a las claves está disponible a través de seis parámetros en los metadatos de los ficheros de claves, y corresponden a las fases indicadas en inglés entre paréntesis previamente (salvo para la fase "Preparada"). Asimismo, la información de tiempos se puede alterar mediante parámetros de la utilidad "dnssec-keygen" (o "dnssec-settime"). Los parámetros admiten tanto una fecha absoluta como una desviación (*offset*) calculada a partir de la fecha actual del sistema. Las referencias temporales se pueden expresar en formato "AAAAMMDD" y "AAAAMMDDHHMMSS". Por su parte, el *offset* puede ser a futuro ("+") o desde el pasado ("-"), y llevar sufijos "y" (año definido como 365 días con días de 24 horas), "mo" (mes definido como 30 días de 24 horas), "w" (semana), "d" (día), "h" (hora) y "mi" (minuto).

Los parámetros de tiempo de la utilidad "dnssec-keygen" son [Ref.- 50]:

- -P: (Publicada) fija la fecha en que la clave se publicará en la zona. Después de dicha fecha, la clave se incluirá en la zona, pero no se usará para firmarla. Si no se

emplea este parámetro en la utilidad de BIND, se toma por defecto el momento actual de generación de la clave.

- -A: (Activa) fija la fecha en que la clave será activada en la zona. Después de esa fecha, la clave se incluirá en la zona y se usará para firmar los registros. Si no se emplea este parámetro en la utilidad de BIND, se toma por defecto el momento actual de generación de la clave.
- -R: (Revocada) fija la fecha de revocación de la clave. Pasada esa fecha, la clave se marcará como revocada (*flag* REVOKE), pero si la fecha de publicación es válida, todavía se incluirá en la zona y se usará para firmar los registros.
- -I: (Inactiva o Retirada) fija la fecha en que la clave será retirada. Pasada esa fecha, la clave se incluirá en la zona, pero no se usará ya para firmar los registros.
- -D: (Borrada) fija la fecha en que la clave será borrada. Pasada esa fecha, la clave no se incluirá en el fichero de zona.

Si no se especifica ninguno de estos parámetros, los ficheros de clave solo tendrán por defecto los campos "Created", "Publish" y "Activate", todos referenciando la fecha de creación de la clave. Esto es suficiente para el funcionamiento de DNSSEC, puesto que los registros DNSKEY y DS no llevan asociada información de tiempo (únicamente el TTL si se define uno propio para ellas en lugar del existente por defecto en el SOA de la zona).

```
$ cat Kejemplo.es.+008+43530.key
; This is a zone-signing key, keyid 43530, for ejemplo.es.
; Created: 20180611103832 (Mon Jun 11 06:38:32 2018)
; Publish: 20180611103832 (Mon Jun 11 06:38:32 2018)
; Activate: 20180611103832 (Mon Jun 11 06:38:32 2018)

ejemplo.es. IN DNSKEY 256 3 8
AwEAAAdDPz6W/5mQ/2VdHL8QVtMw5D/3EI0rWscrBWA8Ya/eBnDsOWcvp
5NjGMTJFHLmaLnPujywqEeSXlSnUURX15BTZKsn9a4/AvEqrFIAYtnH
LL+jr6zPnzONyKAqL8PiF5Ti7D6GPlCVirkwFFv8dAHoTSCLFomfSyTX Q16e3udX
```

Figura 12 - Fichero con la clave pública ZSK (".key")

Los metadatos de tiempo de una clave ya existente se pueden alterar mediante la utilidad "dnssec-settime" (el cambio afecta a ambos ficheros del par de claves, ".key" y ".private") [Ref.- 51]. El fichero ".key" contendrá una descripción de los metadatos en formato legible.

Una vez generadas las claves, se puede proceder al firmado de la zona.

6.1.3.2. Generación de las claves en un dispositivo HSM

BIND 9 proporciona una serie de herramientas que permiten el uso de un dispositivo hardware HSM para la generación y almacenamiento de las claves.

Para utilizar el esquema PKCS#11 basado en OpenSSL, el primer paso es definir la variable de entorno LD_LIBRARY_PATH de modo que incluya las librerías de OpenSSL y PKCS#11, para que el demonio *named* las use en lugar de las librerías PKCS#11 nativas:

```
$ export LD_LIBRARY_PATH=/opt/pkcs11/usr/lib:${LD_LIBRARY_PATH}
```

Adicionalmente, puede ser preciso añadir alguna otra variable de entorno en función del dispositivo HSM que se utilice. Para ello, se debe consultar la documentación propia del fabricante del dispositivo.

Para la generación de las claves se debe emplear la utilidad "pkcs11-keygen" que, entre otros, recibe como parámetros:

- -a <clase del algoritmo de firma>: soporta RSA, DSA, DH, ECC y ECX. "RSA" corresponde a RSASHA1-NSEC3/SHA1 y es el algoritmo por defecto. Por su parte, "ECC" corresponde a ECDSA P-256/SHA256. También se puede especificar una etiqueta de algoritmo según el formato de DNSSEC, por lo que "-a RSASHA256" generaría las claves con RSA/SHA256.
- -b <tamaño de clave>: especifica el tamaño de la clave en bits.
- -l <etiqueta>: permite definir una etiqueta para identificar la clave generada en el HSM.
- -p <PIN>: permite introducir un código o PIN para proteger la clave privada en el HSM. Si no se especifica este parámetro en línea de comandos, la utilidad lo solicitará durante la ejecución del proceso de generación de la clave.

GENERACIÓN DE LAS CLAVES ZSK (para el firmado de la zona) EN UN HSM:

Generación de la clave ZSK en el módulo HSM. En el ejemplo, se almacenará la clave ZSK en el módulo HSM con la etiqueta "zsk-ejemplo":

```
$ pkcs11-keygen -a [RSA | ECC] -b 1024 -l zsk-ejemplo  
Enter Pin:
```

El algoritmo de firma que se facilita como parámetro ("-a") será uno de los indicados entre corchetes, según el que se considere más idóneo para la zona.

Creación de los ficheros correspondientes al par de claves pública y privada de la ZSK que usará BIND 9 a través del HSM. Se basa en la invocación de la utilidad "dnssec-keyfromlabel", donde es necesario especifica la zona DNS, la cual creará dos ficheros de claves a partir de las claves almacenadas en el HSM, una con extensión ".key" (pública) y otra con extensión ".private" (privada). Sin embargo, ambos ficheros contienen solo datos asociados a la clave pública, junto a un identificador para la clave privada que se mantiene en el HSM, ya que el firmado (y cualquier otra operación criptográfica con dicha clave) tiene lugar dentro de él:

```
$ dnssec-keyfromlabel -l zsk-ejemplo ejemplo.es
```

Como resultado, en el directorio de las claves se generarán los siguientes ficheros:

```
$ ls -xla  
total 16  
-rw-r--r-- 1 root bind 429 Jun 7 06:45 Kejemplo.es.+008+43698.key  
-rw----- 1 root bind 1012 Jun 7 06:45 Kejemplo.es.+008+43698.private
```

GENERACIÓN DE LAS CLAVES KSK (para el firmado de las claves) EN UN HSM:

Los pasos para la generación de la clave KSK son similares a los correspondientes a la clave ZSK, salvo que el tamaño de clave se fijará en 2.048 bits para el comando "pkcs11-keygen" y que la utilidad "dnssec-keyfromlabel" llevará como parámetro "-f KSK" para indicar que esta clave es la KSK:

```
$ pkcs11-keygen -a [RSA | ECC] -b 2048 -l ksk-ejemplo  
Enter Pin:
```

El resultado de la generación de las claves dentro del HSM se puede comprobar a través de la herramienta "pkcs11-list":

```
$ pkcs11-list
Enter Pin:
object[2]: handle 2 class 2 label[12] 'zsk_ejemplo' id[0]
object[3]: handle 3 class 2 label[12] 'ksk_ejemplo' id[0]
```

Creación de los ficheros correspondientes al par de claves pública y privada de la KSK que usará BIND 9 a través del HSM:

```
$ dnssec-keyfromlabel -l ksk-ejemplo -f KSK ejemplo.es
```

Figura 13 - Comandos BIND para generar las claves DNSSEC en un HSM: ZSK y KSK

Al igual que en el caso de generación de claves en el sistema operativo, se aconseja generar los respectivos pares de claves de respaldo.

Las claves generadas según el formato de clave privada se pueden importar en PowerDNS mediante la utilidad "pdnsutil":

```
# pdnsutil import-zone-key <zona> <fichero_de_clave_privada> [ksk || zsk]
```

6.1.4. Publicación de las claves

El concepto de publicación de las claves en DNSSEC hace referencia a la creación de los registros DNSKEY asociados a las claves públicas ZSK y KSK y su publicación en la zona.

El formato de estos registros en el fichero de configuración de la zona presenta el siguiente formato:

```
<zona> <TTL> <CLASE> <Tipo RR> <flags> <protocolo> <algoritmo> <clave>
ejemplo.es. 86400 IN DNSKEY 256 3 5 ( WqTkFmynfzW4kyBv015MUG2DeIQ3
Cbl+BBZH4b/0PY1kxkmvHjcZc8no
ASdj3lGajIQKY+TpPS0I8=eP35S7
WqTkF7H6RfoRqXQeogmMHfpftf6z
Mv1LyFR3Kiolza6ZEzOJBOztyvhjL
742iU/TpPSEDhm2SNKLi jfUppn1U
aNvv4w== )
```

Figura 14 - Formato de los registros DNSKEY publicados en la zona

- El campo <protocolo> tendrá siempre el valor "3", correspondiente a DNSSEC.
- El campo <algoritmo> contiene el identificador del tipo de algoritmo de firma empleado según el RFC 4034 [Ref.- 7]. En el ejemplo, el algoritmo de firma empleado es RSA/SHA-1 (tipo 5).
- El campo <flags>, de dos bytes de longitud, permite identificar si la clave es la ZSK o la KSK: los bits [0-6] y [8-14] están reservados y siempre tienen valor 0. El bit 7 indica que el registro es una clave, y el bit 15 (denominado SEP, *Secure Entry Point*) tiene valor 1 cuando corresponde a la clave KSK (y valor 0 para la clave ZSK), para informar de que puede usarse como parte de la cadena de confianza. Por tanto, un valor de 256 indica que el registro corresponde a la clave ZSK y un valor de 257 indica que corresponde a la clave KSK.

- El campo `<clave>` contiene la clave pública propiamente, codificada en base 64.

El tipo de almacenamiento de las claves (fichero, base de datos, etc.) dependerá del servidor DNS concreto.

La publicación de las claves en BIND se realiza durante el proceso de firma, pero opcionalmente se pueden incluir manualmente los registros DNSKEY en el fichero de configuración de la zona sin firmar, incluso antes de llevar a cabo dicho proceso.

6.1.5. Proceso de firma de zonas DNS con autoridad

El soporte para DNSSEC fue uno de los objetivos clave que se persiguieron en el desarrollo de BIND 9, de forma que se proporcionasen utilidades para efectuar el firmado de una zona y su posterior mantenimiento. Estas utilidades van evolucionando con cada nueva versión de BIND 9. Entre las principales características, la versión 9.7.2 de BIND, introdujo el concepto de "*smart signing*", destinado a simplificar tanto el firmado inicial, como la gestión de las claves.

La funcionalidad "*smart signing*" introdujo varias opciones y comandos, entre los que destacan:

- `dnssec-keygen`: para la generación de claves.
- `dnssec-signzone`: para el firmado de la zona de forma sencilla.
- `dnssec-dsfromkey`: para obtener el registro DS directamente de la clave KSK asociada.

BIND 9.7 introdujo además capacidades para gestión automática de las claves del dominio DNSSEC (*Auto-DNSSEC*), mediante la directiva "`auto-dnssec`" de la zona, que puede tomar como valores posibles [Ref.- 74]:

- `off`: la gestión de las claves se realizará manualmente (opción por defecto).
- `allow`: permite que las claves sean actualizadas y la zona sea refirmada por completo cuando se invoque el comando "`rndc sign <nombre de zona>`".
- `maintain`: indica a BIND que debe realizar las operaciones de mantenimiento del entorno DNSSEC de forma **automática**, ajustando la gestión planificada de las claves de la zona en función de los metadatos incluidos en las claves. Se recomienda utilizar esta opción, debido a que simplifica enormemente la posterior operación, ya que BIND periódicamente (por defecto, cada hora) identifica la presencia de nuevas claves, retira claves antiguas, y gestiona los registros DNSKEY en función de estas tareas de gestión.

Además, BIND 9.7 incorporó las siguientes opciones relacionadas con DNSSEC:

- `key-directory`: especifica el directorio donde se encuentran las claves DNSSEC.
- `dnssec-secure-to-insecure`: permite convertir un dominio (o zona) firmado en uno sin firmar de forma sencilla, revirtiendo la configuración de DNSSEC a DNS.
- `sig-validity-interval`: permite definir el periodo de validez de una firma.

La aplicación de las modificaciones de cualquier parámetro del fichero "`named.conf`" (y del resto de ficheros de configuración de BIND) se puede llevar a cabo mediante dos métodos:

- Reiniciando el demonio `named`.
- Ejecutando el comando "`rndc reload`". Este comando, además de recargar la configuración, recargará todas las zonas.

El firmado de la zona puede ser **manual** o **automático**, y ambas opciones, con el objetivo de ejemplificarlas, se describirán a continuación.

Como resultado del proceso de firma, se generará un fichero de zona firmado (en el ejemplo utilizado, será "ejemplo.es.db.signed"), que contendrá:

- Los registros DNSKEY asociados a las claves DNSSEC.
- Un registro RRSIG para cada RRSet de la zona que contiene la firma del RRSet correspondiente.
- Una cadena de registros NSEC firmados (o NSEC3 si se utilizó un algoritmo compatible con él).

Tras firmar la zona, conviene verificar el fichero de zona generado, incluida la cadena de registros NSEC, para lo cual se dispone de la utilidad "dnssec-verify", que recibe como parámetros el nombre de la zona y el fichero firmado de la misma:

```
$ dnssec-verify -o ejemplo.es ejemplo.es.db.signed
```

Figura 15 - Verificación mediante dnssec-verify del fichero de la zona firmada

En la práctica, el periodo de refresco (*refresh period*) establece el tiempo o periodo de validez de una firma (*lifetime*), y se recomienda que este valor sea superior (al menos en un día) al valor de expiración de la zona (o periodo de expiración, *expiration time*), para solventar el problema que surgiría en caso de que un servidor secundario no pudiese transferir la zona desde el servidor primario por cualquier causa (ver apartado "4.1.3. Parámetros asociados a la validez de las firmas" para obtener todos los detalles sobre la validez de una firma).

BIND permite establecer los periodos de validez (desde la generación de la firma hasta la fecha de expiración) y refresco de los registros firmados, para que puedan ser diferentes a los establecidos por defecto, mediante la opción "sig-validity-interval". Continuando con el ejemplo del apartado "4.1.3. Parámetros asociados a la validez de las firmas", el siguiente ejemplo especifica un periodo de validez de 15 días y un periodo de refresco de 5 días:

```
# periodo de validez (15 días) y periodo de refresco (5 días)  
sig-validity-interval 15 5;
```

Figura 16 - Opción para establecer los periodos de expiración y refresco

De cara al proceso de firmado, BIND consulta el flag SEP (descrito anteriormente, y en el RFC 4035 [Ref.- 5]) de las claves para determinar cuál se empleará para firmar los registros de la zona (ZSK) y cuál para firmar el RRSet de tipo DNSKEY (KSK).

6.1.5.1. Firmado manual

Para llevar a cabo el proceso de firmado manual de la zona DNSSEC se recomienda:

- 1) Añadir las opciones de configuración apropiadas para el entorno DNSSEC al fichero "named.conf":

```
options {  
    # directorio de claves:  
    key-directory "<path_al_directorio_de_claves>";  
    dnssec-enable yes;  
    auto-dnssec [off || allow];  
};
```

Figura 17 - named.conf: opciones para la gestión y el firmado manual de la zona

- 2) Editar el fichero de configuración de la zona y añadir los registros DNSKEY correspondientes a las claves públicas ZSK y KSK según el formato definido en el RFC 4034 [Ref.- 7].
- 3) Firmar la zona mediante el comando "dnssec-signzone" y las claves ZSK y KSK (cuyas opciones están detalladas en el siguiente apartado):

```
$ dnssec-signzone -o <zona> -f <fichero_zona.db.signed>  
<fichero_zona.db> <ZSK>.key <KSK>.key
```

Figura 18 - Comando BIND para firmar una zona manualmente

- 4) Actualizar la sección correspondiente a la zona en el fichero de configuración "named.conf" para que incluya la referencia al fichero firmado (extensión ".db.signed"):

```
zone "ejemplo.es" IN {  
    type master;  
    file "/etc/bind/master/ejemplo.es.db.signed";  
};
```

Figura 19 - named.conf: referencia al fichero con el firmado manual de la zona

- 5) Indicar a *named* que debe releer y aplicar la nueva configuración mediante "rndc reload".
- 6) Repetir los pasos 3 y 5 cada vez que se hagan modificaciones en la zona.

6.1.5.2. Firmado automático

BIND 9.9 introdujo la funcionalidad *inline signing* (ver apartado "6.1.5.3. Utilización de *inline signing* en escenarios de firma *online*"), mediante la cual *named* crea una versión interna de la zona que se firma en tiempo real en memoria y que es la que se sirve de cara a las consultas DNS, manteniendo intacta en el sistema de ficheros la versión de la zona sin firmar, que no es servida directamente. Las modificaciones de la zona se realizan sobre el fichero sin firmar, lo que simplifica su administración.

Esta funcionalidad se habilita definiendo el parámetro "inline-signing yes" en el fichero de configuración de *named*.

La opción de *inline signing* suele ir ligada a la gestión de la zona DNSSEC de forma automática (directiva "auto-dnssec maintain"), aunque conceptualmente no representen lo mismo.

Para llevar a cabo el proceso de firmado automático de la zona DNSSEC mediante *inline signing* se recomienda:

- 1) Añadir las opciones de configuración apropiadas para el entorno DNSSEC al fichero "named.conf":

```
options {  
    # directorio de claves:  
    key-directory "<path_al_directorio_de_claves>";  
    dnssec-enable yes;  
    auto-dnssec maintain;  
    inline-signing yes;  
};
```

Figura 20 - named.conf: opciones para la gestión y el firmado automático de la zona

- 2) Firmado de la zona con la opción de "smart signing" ("dnssec-signzone -S"), que examina el repositorio de claves y, cuando encuentra un fichero que corresponda a la zona indicada:
 - a. Genera e incluye los registros DNSKEY correspondientes en el fichero de zona.
 - b. Examina los metadatos de tiempo asociados a las claves y, en función de ellos, determina cómo usar la clave ZSK respecto al proceso de firma, asociándole un estado (creada, publicada, activa, revocada, inactiva o eliminada).

```
$ dnssec-signzone -S -K /etc/bind/keys/ -g -a -r /dev/random -o  
ejemplo.es -f ejemplo.es.db.signed ejemplo.es.db
```

Figura 21 - Firmado de la zona mediante dnssec-signzone

Durante la generación del fichero de zona se comprobará que al menos existe una KSK autofirmada y que todos los registros se han firmado.

Los principales parámetros que soporta la utilidad "dnssec-signzone"¹⁶ son:

- -o <zona>: nombre de la zona a firmar.
- -f <fichero de la zona>: referencia al fichero de la zona firmado que será generado como resultado del proceso de firma.
- -K <directorio>: directorio con el repositorio de claves.

Adicionalmente, se puede especificar:

- -g: genera los registros DS para las zonas hija a partir de los ficheros correspondientes.
- -3 <semilla>: semilla empleada para los hashes de los registros NSEC3.
- -s <YYYYMMDDHHMMSS>: inicio (s = start) del periodo de validez de la firma para los registros RRSIG.
- -e <YYYYMMDDHHMMSS>: fin (e = end) del periodo de validez de la firma para los registros RRSIG.
- -T <ttd>: TTL para el registro DNSKEY que se importa en la zona desde el repositorio de claves (si no se especifica, se tomará el TTL que se haya definido por defecto en el registro SOA de la zona).
- -H <iteraciones>: número de iteraciones para los hashes de los registros NSEC3 (10 por defecto).

¹⁶ Se recomienda instalar la última versión de BIND disponible y consultar las opciones concretas del comando en cuestión: <https://ftp.isc.org/isc/bind9/cur/9.12/doc/arm/man.dnssec-signzone.html>.

- `-x`: el uso de esta opción hará que el RRSet de tipo DNSKEY se firme solo con la clave KSK (omitiendo las firmas de la clave ZSK), lo que permite disminuir ligeramente el tamaño del fichero de la zona firmada.
- `-a`: esta opción verifica o valida todas las firmas (registros RRSIG) generadas en el proceso de firma de la zona.
- `-i <intervalo>`: esta opción, acompañada del fichero que identifica una zona previamente firmada, determina que se debe reevaluar el refirmado de los registros de la zona. Su valor corresponde al periodo de refresco (ver apartado "4.1.3. Parámetros asociados a la validez de las firmas"). El parámetro "`<intervalo>`" define (en segundos) un periodo a contar desde el momento actual. Al analizar la zona, si la fecha expiración de un RRSIG es posterior al intervalo, se mantiene; en caso contrario, se considera que va a expirar pronto y se refirma. El intervalo por defecto es " $\frac{1}{4} * (\text{fecha de inicio} - \text{fecha de fin})$ " de la firma, es decir, " $\frac{1}{4} * (\text{período de validez de la firma})$ ". Cuando no se especifican parámetros de inicio y fin de la firma, "`dnssec-signzone`" generará por defecto firmas válidas durante 30 días, por lo que el intervalo de refirmado antes de la expiración es de 7,5 días, reemplazándose todos los RRSIG que van a caducar antes de 7,5 días.

- 3) Indicar a *named* que debe volver a leer y aplicar la nueva configuración mediante "`rndc reload <zona>`"¹⁷. Tras ello, BIND se encargará de mantener la zona firmada, tanto para los nuevos registros como para la gestión y renovación de las claves.

La opción de *inline signing* no requiere modificar el parámetro "`file`" en el fichero de configuración "`named.conf`" para que referencie al fichero firmado ("`<zona>.signed`").

Cuando se usa el esquema de *inline signing*, BIND refrescará las firmas en función del periodo de refresco. Este aspecto debe tenerse en cuenta durante los procesos de renovación de las claves, para garantizar que todas las firmas de la zona se han generado con la nueva clave ZSK.

BIND *inline signing* es similar al denominado *front signing* de PowerDNS. Si se utiliza como servidor DNS PowerDNS, el firmado de una zona sin firmar se lleva a cabo mediante el siguiente comando, que se encargará de realizar todos los pasos de despliegue de DNSSEC para la zona:

```
# pdnsutil secure-zone <zona>
```

PowerDNS permite además servir zonas firmadas tras haber importado dichas zonas a su base de datos mediante la utilidad "`pdnsutil set-presigned <zona>`".

6.1.5.3. Utilización de *inline signing* en escenarios de firma *online*

A continuación, se proporcionan detalles sobre cómo emplear el modo *inline signing* para implementar los modelos de firmado *online* descritos en el apartado "4.1.5.1. Firmado inicial, mantenimiento y publicación de la zona".

¹⁷ Si se utilizan zonas dinámicas, el comando "`rndc reload <zona>`" no funcionará. Es preciso congelar las actualizaciones dinámicas mediante "`rndc freeze <zona>`" previamente y retomarlas tras la recarga mediante "`rndc thaw <zona>`": <https://unix.stackexchange.com/questions/132171/how-can-i-add-records-to-the-zone-file-without-restarting-the-named-service>.

Las opciones de configuración de "named.conf" para los servidores DNS encargados de la gestión de la zona en DNSSEC en cada escenario serían (ver "Figura 9"):

- Para el caso (1), en el que servidor DNS primario es quien servirá directamente la zona DNSSEC:

```
zone "ejemplo.es" {  
    type master;  
    file "/etc/bind/master/ejemplo.es.db";  
    allow-transfer { localhost; 10.20.20.3; ...; 10.20.20.N; };  
    auto-dnssec maintain;  
    inline-signing yes;  
};
```

Figura 22 - Opciones de configuración de firmado inline en named.conf (caso 1)

- Para el caso (2), el servidor DNS primario oculto deberá ser configurado para permitir transferencias de zona únicamente desde el nuevo servidor DNS intermedio, que servirá la zona DNSSEC al resto de servidores DNS secundarios o esclavos:

- Para el caso (2.1), en el que el servidor primario oculto gestiona la zona sin firmar, la configuración DNSSEC para el nuevo servidor intermedio, que servirá la zona firmada al resto de servidores DNS esclavos, es:

```
zone "ejemplo.es" {  
    type slave;  
    masters { 192.168.196.124; }; #servidor primario oculto  
    file "<...>";  
    allow-transfer { localhost; 10.20.20.3; ...; 10.20.20.N; };  
    auto-dnssec maintain;  
    inline-signing yes;  
};
```

Figura 23 - Opciones de configuración de firmado inline en named.conf (caso 2.1)

- El caso (2.2) para el servidor primario oculto es equivalente al caso (1), pero la transferencia de la zona ya firmada se llevaría a cabo únicamente entre el servidor primario oculto y el servidor intermedio. La configuración DNSSEC para el servidor primario oculto:

```
zone "ejemplo.es" {  
    type master;  
    file "/etc/bind/master/ejemplo.es.db";  
    allow-transfer { localhost; 10.20.20.2; }; # servidor intermedio  
    auto-dnssec maintain;  
    inline-signing yes;  
};
```

Figura 24 - Opciones de configuración de firmado inline en named.conf (caso 2.2)

El comando "rndc reconfig" generará la versión firmada de la nueva zona, sin alterar la zona original:

- Bajo el directorio "master" para los casos (1) y (2.2).
- Bajo el directorio "slave" para el caso (2.1): en este caso, cuando se recargue la configuración en el servidor DNS intermedio, *named* transferirá una copia de la zona sin firmar desde el servidor DNS primario oculto y generará una versión firmada de la zona en el directorio indicado:

```
$ /usr/sbin/rndc reconfig
$ cd /etc/bind/slave/
$ ls
ejemplo.es.db  ejemplo.es.db.signed  ejemplo.es.db.jnl
```

Figura 25 - Firma inline de la zona con BIND en el servidor intermedio (caso 2.1)

Una vez se hayan realizado las pruebas necesarias y se constate que el nuevo servidor intermedio funciona correctamente, tanto a nivel de DNSSEC como incorporando las modificaciones que se puedan realizar en la zona por parte del servidor primario, se procederá a apuntar al servidor intermedio desde los servidores secundarios ya existentes.

NOTA: El mecanismo de firmado *inline* provoca que BIND incremente el número de serie de la zona firmada cuando renueve las firmas, por lo que el formato empleado para este valor podría tener que revisarse.

Para verificar los datos de la zona firmada, se puede utilizar el comando:

```
$ named-checkzone -D -f raw ejemplo.es ejemplo.es.db.signed
```

Figura 26 - Comando named-checkzone para verificación de una zona firmada

6.1.6. Establecimiento de cadenas de confianza

La cadena de confianza en DNSSEC para una zona se habilita cuando el registro DS calculado a partir de la clave KSK de la zona hija se da de alta en la zona padre, quien lo firma como parte de los registros de su zona y lo publica (junto a la firma o registro RRSIG) en sus servidores DNS autoritativos. A partir de ese momento, el registro DS se servirá a los *resolvers* que así lo soliciten.

El formato utilizado para cargar en la zona padre el registro DS vendrá marcado por el administrador de la zona o, en el caso de los TLDs de primer nivel, por el agente registrador.

Para generar el registro DS, es preciso partir del registro DNSKEY asociado a la clave pública KSK, que tiene activo el *flag* SEP descrito en el apartado "6.1.4. Publicación de las claves".

La versión de BIND empleada suministra la herramienta "*dnssec-dsfromkey*", que permite generar el registro DS siguiendo las normas definidas en los RFCs 3685 y 4509 [Ref.- 24]. Las opciones soportadas por dicha herramienta se pueden consultar en la página del manual. La utilidad admite como algoritmos de *hashing* SHA1, SHA256, SHA384 y GOST.

```
$ cd /etc/bind/keys
$ dnssec-dsfromkey Kejemplo.es.+008+03436.key
ejemplo.es. IN DS 3436 8 1 3E09AC00B45631723A0DFC91AD2712046E7C6011
ejemplo.es. IN DS 3436 8 2
583AC696F0B8E38FD1D53A28B69B38934C6E89289534A563FACBC86A0451A1A4
```

Figura 27 - Generación del registro DS correspondiente a la clave KSK con BIND

Como se puede apreciar, el hash obtenido para el algoritmo 2 es más largo que el del algoritmo 1 (SHA1), porque corresponde a SHA256, y es el que se recomienda transferir a la zona padre.

La salida del comando representa el registro DS que se debe cargar en la zona padre siguiendo los procesos del agente registrador empleado para dar de alta el dominio.

En caso de utilizarse PowerDNS, el comando para generar el registro DS sería:

```
$ pdnssec show-zone ejemplo.es

DS = ejemplo.es IN DS 3436 8 1 3e09ac00b45631723a0dfc91ad2712046e7c6011
; ( SHA1 digest )

DS = ejemplo.es IN DS 3436 8 2
583ac696f0b8e38fd1d53a28b69b38934c6e89289534a563facbc86a0451a1a4
; ( SHA256 digest )
```

Figura 28 - Generación del registro DS correspondiente a la clave KSK con PowerDNS

Una vez generado el registro DS, se transferirá su contenido al responsable de la administración de la zona padre o TLD de nivel superior.

Como alternativa para simplificar y automatizar la gestión de los registros DS (asociada a la renovación de la clave KSK) se propuso un mecanismo que se describe en el apartado "9. Anexo: Registros CDS y CDNSKEY".

6.1.6.1. Cadena de confianza entre subdominios de una misma zona

Para incluir el registro DS generado para una zona hija en una zona padre que se encuentra dentro de la propia organización, basta con incluir el registro en el fichero de configuración de la zona padre (como parte de la zona DNSSEC), incrementar el número de serie de la zona (*serial*) y recargar la configuración para que el nuevo registro se firme con la clave ZSK de la zona padre. Si la administración del dominio de nivel superior se lleva a cabo por otro departamento de la organización, deberá coordinarse su publicación con sus responsables.

6.1.7. Comprobación del servicio DNSSEC



La comprobación del correcto despliegue y funcionamiento de DNSSEC debe realizarse inmediatamente después de su puesta en producción en los servidores DNS autoritativos.

Actualmente, existen diversos mecanismos para analizar el estado de una zona DNSSEC, algunos de los cuales se ilustran a continuación:

- Utilidad de Verisign Labs "DNSSEC Analyzer" [Ref.- 36]:

Analyzing DNSSEC problems for gob.es

.	<ul style="list-style-type: none"> ✔ Found 4 DNSKEY records for . ✔ DS-19036/SHA-256 verifies DNSKEY-19036/SEP ✔ DS-20326/SHA-256 verifies DNSKEY-20326/SEP ✔ Found 1 RRSIGs over DNSKEY RRset ✔ RRSIG-19036 and DNSKEY-19036/SEP verifies the DNSKEY RRset
es	<ul style="list-style-type: none"> ✔ Found 4 DS records for es in the . zone ✔ DS-29450/SHA-1 has algorithm RSASHA256 ✔ DS-29450/SHA-256 has algorithm RSASHA256 ✔ DS-44290/SHA-1 has algorithm RSASHA256 ✔ DS-44290/SHA-256 has algorithm RSASHA256 ✔ Found 1 RRSIGs over DS RRset ✔ RRSIG-39570 and DNSKEY-39570 verifies the DS RRset ✔ Found 2 DNSKEY records for es ✔ DS-29450/SHA-1 verifies DNSKEY-29450/SEP ✔ Found 1 RRSIGs over DNSKEY RRset ✔ RRSIG-29450 and DNSKEY-29450/SEP verifies the DNSKEY RRset
gob.es	<ul style="list-style-type: none"> ✔ Found 4 DS records for gob.es in the es zone ✔ DS-38356/SHA-1 has algorithm RSASHA256 ✔ DS-33722/SHA-256 has algorithm RSASHA256 ✔ DS-33722/SHA-1 has algorithm RSASHA256 ✔ DS-38356/SHA-256 has algorithm RSASHA256 ✔ Found 1 RRSIGs over DS RRset ✔ RRSIG-33001 and DNSKEY-33001 verifies the DS RRset ✔ Found 2 DNSKEY records for gob.es ✔ DS-38356/SHA-1 verifies DNSKEY-38356/SEP ✔ Found 1 RRSIGs over DNSKEY RRset ✔ RRSIG-38356 and DNSKEY-38356/SEP verifies the DNSKEY RRset ✔ Found 1 RRSIGs over SOA RRset ✔ RRSIG-20781 and DNSKEY-20781 verifies the SOA RRset

Move your mouse over any  or  symbols for remediation hints.

Want a second opinion? Test gob.es at dnsviz.net.

Figura 29 - Ejemplo de validación de un dominio mediante DNSSEC Analyzer (Verisign)

- Empleando un *resolver* configurado para validar las consultas DNS mediante DNSSEC, se puede emplear la utilidad "dig" para consultar los datos relativos a la zona:

Si se devuelven (al menos) dos registros DNSKEY, la zona dispone probablemente de una clave KSK (257) y de una clave ZSK (256). Ejemplo:

```
$ dig +multiline <zona> dnskey
```

```
$ dig +multiline es dnskey
```

```
...
```

```
es.      22503 IN DNSKEY      257 3 8 (
        AwEAAcmsgzTAPZlvShLsW5KN25uAmuUjSXwkMKQR0Qp+
        oVQMLapa0GDjBJKeEUb/N2CLv7xse/qnI5oxalOQY2vh
        pmtufgo5cDHcvlS1PkT7IxvEsKmjbjxxUWohkv3FPKWo
```

```

Y0j+YAQ+ob9ihv7D5XaXxaYaS2s34cSQKUbJVAOzVZED
xeeCY+K7ZBfGWbW3UCUgFDYbYL4xWkx1mHMcuD1aO+U8D
Z10ex73Tr7qSMNaocBh4lOVamvDEQ07hQepPJSiRNjjP
vWUL2OQQlMlVliOBkme4bLITo01csKFUgWpZCcMt1cF7
1eC6LGeyhmk1CF7Ma20I93CVOum7cZuS6+bDANs=
) ; KSK; alg = RSASHA256 ; key id = 29450
es.      22503 IN DNSKEY      256 3 8 (
AwEAAAdwH1R2SM4iIwbMOI6tVsts3ohLlWWuBFhXCJoOm
UzrcT3Tp3hC+QVn0shqsgv4Af9ZpmbVZpEjEUAFLiuff
nzTW0pMLwiryXUrRDzmvja6dF5QzrX2n5Pqgj6VD4ndW
YKDyO6mYzPnjDUuAwMausLJjBQ3MooIy2BfG2TGyRO6v
) ; ZSK; alg = RSASHA256 ; key id = 33001

Obtención de los registros DS publicados en la zona padre, que deberán coincidir con
los generados por la zona hija (relacionados por el identificador de clave). Ejemplo:

$ dig [+trace] DS <zona> [+short]

$ dig DS es
...
es.      5      IN      DS      44290 8 2
562EF35E7065588A7178A4BD0155C8527F029C82AA455DD359C84908 B2A7FE17
es.      5      IN      DS      29450 8 2
8BEC32A2C9CFE42E393BAF81FFE71B521D3E940612A4590B4763ADC5 39E4B563
es.      5      IN      DS      29450 8 1
417BEAFB46ABF3430B75C5C29AEF785D476B60E1
es.      5      IN      DS      44290 8 1
7711F564D55B41C8CE7DFAF4DD323C5B271F86CD

$ dig DS es +short
29450 8 1 417BEAFB46ABF3430B75C5C29AEF785D476B60E1
44290 8 1 7711F564D55B41C8CE7DFAF4DD323C5B271F86CD
44290 8 2 562EF35E7065588A7178A4BD0155C8527F029C82AA455DD359C84908
B2A7FE17
29450 8 2 8BEC32A2C9CFE42E393BAF81FFE71B521D3E940612A4590B4763ADC5
39E4B563

NOTA: El parámetro "+trace" hace que las consultas generadas por "dig" sean iterativas
en lugar de recursivas, funcionamiento por defecto de "dig", que también puede ser
modificado con la opción "+norecurse".

```

Figura 30 - Ejemplo de consulta de registros DNSSEC de una zona mediante "dig"

6.1.8. Transferencias de zona DNS con DNSSEC activo

DNSSEC no ofrece mecanismos para proteger las operaciones de transferencia de zona mediante las cuales se sincronizan los datos del servicio DNS entre los diferentes servidores autoritativos, primarios y secundarios. Para ello, se puede emplear el estándar TSIG (*Transaction Signature protocol*) definido originalmente en el RFC 2845 [Ref.- 8], "Secret Key Transaction Authentication for DNS (TSIG)", y actualizado posteriormente por el RFC 3645 [Ref.- 60], "Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)", que proporciona los medios para identificar y autenticar a los extremos de una conexión DNS.

La autenticación de la transacción se realiza calculando un HMAC (*keyed-Hash Message Authentication Code* o *Hash-based Message Authentication Code*), que permite obtener un código de autenticación en base a una *función hash criptográfica* en combinación con una

clave secreta, compartida entre los dos extremos de la comunicación. El mensaje a transferir se envía junto al HMAC, de forma que el destinatario podrá verificarlo, obteniendo el *hash* a partir del mensaje recibido y de la clave previamente compartida y, si coincide con el que acompaña al mensaje, lo dará por válido.

En el caso de DNS, el HMAC se calcula a partir de la trama DNS completa empleando como clave una cadena de caracteres aleatoria conocida por los servidores DNS autoritativos implicados en la transferencia de zona, y se transmite como un registro (RR) de tipo TSIG que se concatena con la trama DNS.

De cara a la distribución de las zonas firmadas con DNSSEC, se establecen las siguientes recomendaciones:

- Las transferencias de zona deberían protegerse frente a ataques de modificación y truncado mediante TSIG.
- Las transferencias de zona deberían autenticarse a través de un algoritmo de tipo HMAC o GSS-TSIG.

La configuración de TSIG y GSS-TSIG, totalmente independientes de la gestión y proceso de firma de la zona en DNSSEC, quedan fuera del alcance de la presente guía.

Los intervalos de refresco para el SOA (*SOA refresh*) y de reintento (*SOA retry*) establecen cada cuanto un servidor DNS autoritativo secundario consulta la existencia de actualizaciones de zona en el servidor DNS autoritativo primario. Se recomienda que el intervalo de refresco para el SOA (*SOA refresh*) en DNSSEC sea de entre 1 y 4 horas, con un valor de reintento (*SOA retry*) de entre 15 y 60 minutos [Ref.- 54].

6.1.9. Actualizaciones dinámicas en zonas DNS con DNSSEC activo

El concepto de "*Dynamic Updates*" (actualizaciones dinámicas) en DNS permite a un administrador autorizado de la zona añadir o eliminar datos o registros DNS a través de un mensaje con un formato especial, sin requerir modificar los ficheros de la zona. Se definió inicialmente en el RFC 1035, y se complementó en el RFC 2136 [Ref.- 61]. Las actualizaciones dinámicas involucran el uso de una clave secreta, conocida por los dos extremos de la comunicación, pero son independientes del uso de DNSSEC en el entorno.

Entre sus aplicaciones se encuentran las redes locales donde el direccionamiento IP se asigna dinámicamente a través del protocolo DHCP, por lo que el servidor DHCP debe ser capaz de actualizar la zona DNS para informar de los cambios.

La complejidad conceptual de este mecanismo en DNSSEC radica en que las zonas deben firmarse según se lleve a cabo el proceso de actualización de asignación dinámica de direcciones IP. Sin embargo, las versiones más recientes de los servidores DNSSEC, incluido BIND, soportan firmado en tiempo real de la zona, incluyendo el firmado de registros procedentes de actualizaciones dinámicas, haciéndolo transparente para el usuario.

El inconveniente de este escenario es que, cuando las actualizaciones dinámicas proceden de un sistema conectado a Internet (o más concretamente, a las redes internas o externas a las que da servicio), para que se pueda realizar el firmado de la zona en tiempo real, será preciso que el servidor DNS autoritativo que custodia la clave ZSK esté accesible desde el sistema o cliente que envía las actualizaciones (por ejemplo, el servidor DHCP), y, por tanto, potencialmente vulnerable a ataques desde estas redes que podrían comprometer la clave privada ZSK.

Una posible solución defensiva para este escenario (si no se quiere asumir el riesgo descrito anteriormente) es delegar las actualizaciones dinámicas a una subzona (o subdominio) que cuelgue de la zona DNSSEC principal, la cual se firmará con claves DNSSEC independientes de las de la zona padre. El registro DS de esta zona hija se firmará en la zona padre para establecer la cadena de confianza.

La configuración detallada de DNSSEC para zonas dinámicas queda fuera del alcance de la presente guía, aunque se describirán a continuación las opciones principales disponibles que atañen al firmado de la zona DNSSEC.

Para que las actualizaciones de la zona sean seguras, es necesario que el servidor DNS autoritativo y el cliente que va a realizar las actualizaciones dinámicas compartan una clave secreta, que se genera en el servidor DNS a través del siguiente procedimiento:

- Ejecución del comando "dnssec-keygen", indicando como algoritmo un HMAC. En el ejemplo que ilustra la figura "Figura 31", se utiliza un hash HMAC-SHA256:

```
$ cd /etc/bind/keys
$ dnssec-keygen -a HMAC-SHA256 -b 256 -n HOST dynamicupdates.ejemplo.es

$ ls -xla Kdynamicupdates.ejemplo.es.+163+09285*
-rw----- 1 root bind  89 Jun  7 10:00
Kdynamicupdates.ejemplo.es.+163+09285.key
-rw----- 1 root bind 188 Jun  7 10:00
Kdynamicupdates.ejemplo.es.+163+09285.private

$ cat Kdynamicupdates.ejemplo.es.+163+09285.key
dynamicupdates.ejemplo.es. IN KEY 512 3 163
ik4fsR8D1C5HWvCozEChCxiysg7GgVyA5XxZ0abnSCg=

$ cat Kdynamicupdates.ejemplo.es.+163+09285.private
Private-key-format: v1.3
Algorithm: 163 (HMAC_SHA256)
Key: ik4fsR8D1C5HWvCozEChCxiysg7GgVyA5XxZ0abnSCg=
Bits: AAA=
Created: 20180607140041
Publish: 20180607140041
Activate: 20180607140041
```

Figura 31 - Creación de claves en DNSSEC para actualizaciones DNS dinámicas

- Como ilustra la "Figura 31", se crean dos ficheros, uno que corresponde a la clave pública (.key) y otro que corresponde a la clave privada (.private). En esta última, el campo "Key" es en realidad la clave pública obtenida del fichero ".key".
- La clave anterior se añadirá al fichero "named.conf" dentro de la sección global:

```
key dynamicupdates.ejemplo.es. {
    algorithm HMAC-SHA256;
    secret "ik4fsR8D1C5HWvCozEChCxiysg7GgVyA5XxZ0abnSCg=";
};
```

Figura 32 - named.conf: clave (pública) secreta para actualizaciones DNS dinámicas

- En la sección correspondiente a la zona del fichero "named.conf", incluir las siguientes directivas:

- `auto-dnssec maintain`: para permitir el refirmado de la zona de forma automática.
- `allow-update {<clave>}`: donde "`<clave>`" referencia al fichero que incluye la clave pública secreta.
- `key-directory "<directorio_de_claves_de_firma>"`: referencia al directorio en el que se encuentran los ficheros de clave asociados al secreto que comparten los extremos implicados en las actualizaciones dinámicas.

```
zone "ejemplo.es" {  
    ...  
    auto-dnssec maintain;  
    allow-update {key Kdynamicupdates.ejemplo.es.+157+35073.key};  
    key-directory "/etc/bind/keys";  
    ...  
};
```

Figura 33 - Opciones de configuración de BIND para permitir actualizaciones DNS dinámicas

- Congelación de las actualizaciones dinámicas mediante el comando "`rndc freeze <zona>`", ya que BIND no permite modificaciones y el firmado de la zona mientras esta se está actualizando. Durante ese periodo, *named* creará un fichero *journal* (con extensión ".jnl") que contendrá las actualizaciones que hayan tenido lugar. Los contenidos de este fichero se pueden consultar mediante el comando:

```
$ named-journalprint ejemplo.es.db.jnl
```
- Firma de la zona DNS dinámica, cuando la zona se firma por primera vez, mediante la invocación del comando "`rndc reload <zona>`", para que BIND relea la configuración.
- Descongelación de la zona tras la recarga mediante el comando "`rndc thaw <zona>`" para volver a permitir las actualizaciones dinámicas y aplicar y firmar las actualizaciones las que se hayan recibido durante el proceso de firma inicial.

6.1.10. Notificaciones DNS con DNSSEC activo

El mecanismo "DNS NOTIFY", definido en el RFC 1966 [Ref.- 62], permite a los servidores DNS maestros primarios notificar a sus servidores secundarios o esclavos sobre los cambios en una zona, lo cual hará que el servidor secundario contacte con el servidor primario para comprobar la versión más reciente de la zona y, si no se corresponde con la suya, iniciar una operación de transferencia de zona.

Este mecanismo de notificaciones no se ve alterado por el uso de DNSSEC, ya que no afecta a los registros en el servidor DNS primario, pero, al igual que sucede con las actualizaciones dinámicas y las transferencias de zona (descritas previamente para entornos DNSSEC en los apartados "6.1.9. Actualizaciones dinámicas en zonas DNS con DNSSEC activo" y "6.1.8. Transferencias de zona DNS con DNSSEC activo" respectivamente), se recomienda protegerlas mediante TSIG.

Se recomienda en DNSSEC que el servidor DNS primario envíe mensajes NOTIFY cuando haya actualizaciones de la zona para reducir el número de comprobaciones SOA por parte de los servidores DNS autoritativos secundarios [Ref.- 54].

6.2. Resolvers DNSSEC

En la presente guía se ha utilizado BIND [Ref.- 38] como software DNS *resolver* para los ejemplos prácticos, disponible con licencia de código abierto (*open-source*) en cualquier distribución Unix/Linux.

6.2.1. Resolvers recursivos

Las versiones más recientes de los *resolvers* en BIND ya realizan validación DNSSEC por defecto. No obstante, las opciones que habilitan la validación DNSSEC son "dnssec-enable yes" y "dnssec-validation", que puede tomar los siguientes valores:

- "auto": indica que *named* utilizará como *trust-anchor* las claves incluidas por defecto en el fichero "bind.keys". La renovación de estas claves será detectada y aplicada gracias al método introducido en BIND 9.7 denominado "*Managed-Keys*" (claves gestionadas), que implementa el RFC 5011 [Ref.- 28]:

```
dnssec-validation auto;
```

Figura 34 - Opción para activar la validación DNSSEC en un servidor DNS recursivo BIND con actualización automática del trust-anchor

El fichero "bind.keys" incluirá una versión inicial precompilada del *trust-anchor*, en la que se definirá la directiva "managed-keys {...}".

Este mecanismo es el recomendado para asegurar que BIND actualiza el anclaje inicial de la cadena de confianza cuando se renueve la clave KSK de la zona raíz.

- "yes": indica que *named* no utilice como *trust-anchor* las claves incluidas por defecto en el fichero "bind.keys", sino que el administrador tendrá que declarar manualmente cuál es el anclaje de confianza. Para ello, deberá incluir las referencias en la directiva "trusted-keys {...}", que guarda la copia de los registros DNSKEY de las zonas que se emplean como *trust-anchor*.

Es importante destacar que las claves definidas como "trusted-keys {...}" se consideran siempre de confianza, mientras que las incluidas como "managed-keys {...}" solo lo son de confianza desde el arranque de BIND hasta que se inicia el proceso "*Managed-Keys*" y las claves de la zona raíz son descargadas.

Para que el cambio de configuración tenga efecto, es preciso, bien reiniciar *named*, bien invocar el comando "rndc reconfig" para recargar la nueva configuración.

Adicionalmente, puede ser necesario incluir en el servidor DNS recursivo la opción:

```
dnssec-lookaside auto;
```

Esta directiva le indica a *named* que utilice el servicio o registro DLV (*DNS Look-aside Validation*) del ISC (Internet System Consortium), el cual surgió para permitir que una zona DNSSEC pudiera existir aunque su zona padre no estuviera firmada mediante una extensión del protocolo DNSSECbis. Así, en lugar de establecerse una cadena de confianza continua y jerárquica, desde la zona raíz, se permitía la existencia de islas DNSSEC (zonas firmadas cuyo padre no lo está).

La existencia del registro DLV tenía sentido cuando el despliegue de DNSSEC no era generalizado en los TLDs de nivel superior. Afortunadamente, la mayor parte de los gTLDs y ccTLDs están firmados a día de hoy, por lo que el ISC ha anunciado la suspensión del servicio DLV [Ref.- 63].

El impedimento para eliminar definitivamente el registro DLV se debe a que aún existen en Internet multitud de *resolvers* que pueden seguir operando con base a él, por lo que existe el riesgo de que dichos *resolvers* fallen en su resolución.

6.2.2. Comprobación de la validación mediante DNSSEC

La comprobación de la correcta validación mediante DNSSEC debe realizarse inmediatamente después de la puesta en producción del *resolver* DNSSEC.

Actualmente, existen diversas utilidades para comprobar si un *resolver* está realizando la validación mediante DNSSEC correctamente:

- La utilidad "dig", mediante la opción "+dnssec" (complementariamente se puede usar la opción "+multiline"), sobre un dominio firmado devolverá la cabecera de la respuesta con el flag AD (y/o DO) activo, indicando que la respuesta se ha autenticado y validado mediante DNSSEC por parte del *resolver*:

```
$ dig @<resolver DNSSEC> +dnssec [+multiline] <zona>

$ dig @1.1.1.1 +dnssec es
; <<>> DiG 9.10.6 <<>> @1.1.1.1 +dnssec es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 24489
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1452
;; QUESTION SECTION:
;es.          IN      A

;; AUTHORITY SECTION:
es.          86400   IN      SOA   ns1.nic.es. hostmaster.nic.es.
2018060105 7200 7200 2592000 86400
es.          86400   IN      RRSIG  SOA  8 1 86400 20180620113148
20180601162022 33001 es.
bj2geKPxKhD3vytopxBGTsY/VzmNRcC9ecqC7UutWkhAnOMb6Ch...UvNB HDU=

a7allreacafms5sprtffofn2pk7t7igu.es. 86400 IN NSEC3 1 1 5
17BC055A09B13088 A7CG2552100KQG9OUCB0H6QI9035AK30 NS SOA RRSIG DNSKEY
NSEC3PARAM
a7allreacafms5sprtffofn2pk7t7igu.es. 86400 IN RRSIG NSEC3 8 2 86400
20180620045536 20180601082340 33001 es.
SvmXDXqKYze3CjqFjF7SuKcYtVIaC1PYi5bQnA55qo+4UKo2c/z...CS99 dm4=
...
```

Figura 35 - Ejemplo de validación de respuestas DNSSEC de una zona mediante "dig"

- Existen múltiples recursos y servicios web que ofrecen servicios de comprobación y validación de DNSSEC, enumerados en el apartado "7.7.1.1. Herramientas de verificación".

6.3. Despliegue de arquitecturas DNS *split-view* con DNSSEC

Una configuración o arquitectura de tipo *split-view* (*split* o *split-horizon*) en DNS permite ofrecer distintas respuestas ante una consulta en función del origen de la misma. Un escenario típico de uso consiste en disponer de una vista del servicio DNS, o de una zona concreta, para los usuarios de la red interna y otra diferente para el resto de usuarios de Internet (o clientes DNS externos).

Para combinar este esquema con DNSSEC, normalmente se emplean claves distintas para cada vista. Sin embargo, este elemento supone un problema para BIND, quien utiliza el nombre de la zona como referencia para nombrar muchas de las salidas de sus herramientas (por ejemplo, "dnssec-keygen"). De cara a simplificar la gestión de DNSSEC en este tipo de escenarios, se recomienda el uso de "dnssec-tools.org" [Ref.- 64].

6.4. Resumen de las buenas prácticas en la implantación de DNSSEC

- Utilizar herramientas que simplifiquen la generación de claves: `dnssec-keygen`.
- Establecer los parámetros de tiempo asociados a las claves de la zona: `dnssec-settime`.
- Generar las claves ZSK y KSK en un dispositivo HSM.
- Generar dos claves, tanto para la KSK como para la ZSK, que permitan preparar el proceso de renovación de claves: una clave será la activa y la otra la de respaldo.
- Utilizar herramientas que simplifiquen el firmado de la zona: `dnssec-signzone`.
- Determinar con antelación el mecanismo de inclusión de la zona en la cadena de confianza: generación y publicación del registro DS (`dnssec-dsfromkey`).
- Planificar la operación de firma de manera que permita la gestión automática de la zona:
 - `inline-signing yes;`
 - `auto-dnssec maintain;`
- Proteger con TSIG las operaciones de transferencia de zona entre los servidores DNS autoritativos primarios y secundarios.
- Configuración de la validación *resolver* DNSSEC:
 - `dnssec-enable yes;`
 - `dnssec-validation auto;`
- Comprobación de la validación DNSSEC en el *resolver*: "`dig +dnssec +multiline <...>`".

7. OPERACIÓN

La operación del entorno DNSSEC se ha simplificado enormemente con las últimas versiones de las soluciones disponibles en el mercado. A día de hoy, es factible tener un entorno operativo con escaso mantenimiento, en el que la mayor parte de las actividades relacionadas con el servicio DNSSEC estén automatizadas.

Sin embargo, conviene tener una base de conocimiento técnico sobre la teoría y los procesos asociados al protocolo y servicio DNSSEC, a fin de poder establecer las mejores opciones de mantenimiento y poder reaccionar ante situaciones inesperadas.

A lo largo del presente apartado se presentarán los eventos relevantes y las buenas prácticas en la operación, mantenimiento y administración del dominio DNSSEC una vez el despliegue inicial se haya completado con éxito.

7.1. Servidores DNSSEC autoritativos

De cara a asegurar el correcto funcionamiento de los servidores DNSSEC autoritativos, se recomienda:

- Consultar periódicamente la web del proveedor de software del servidor DNS, a fin de tenerlo actualizado no solo de cara a los errores y *bugs* resueltos, sino también a las vulnerabilidades de seguridad solucionadas y a las nuevas mejoras introducidas. La mayor parte de servidores DNSSEC introducen nuevas opciones y herramientas que simplifican la gestión del entorno. Por ejemplo, en el caso de BIND, consultar las novedades en el blog oficial de ISC [Ref.- 65].
- Suscribirse a canales a través de los que se difundan detalles sobre la detección de nuevas amenazas, noticias sobre ataques, vulnerabilidades encontradas, etc.
- Evaluar las nuevas herramientas y servicios disponibles públicamente que simplifican la gestión del dominio en DNSSEC.

7.2. Recomendaciones del ciclo de vida de las claves en DNSSEC

Se recomienda la lectura detallada del RFC 7583 [Ref.- 43], publicado en 2015, en el que se establecen las recomendaciones para definir adecuadamente los procesos de renovación de las claves de DNSSEC y los periodos de tiempo que afectan al ciclo de vida de estas claves, complementando las buenas prácticas generales del RFC 6781 [Ref.- 25].

Los intervalos de renovación deben marcarse teniendo en cuenta el nivel de seguridad existente para la custodia de las claves, ya que una clave poco o nada expuesta es menos vulnerable que la que está potencialmente accesible desde el exterior constantemente.

La renovación de las claves es el proceso más delicado de DNSSEC, y los plazos definidos irán en consonancia con los parámetros asociados al ciclo de vida de las claves.

Los riesgos potenciales de una renovación de clave incorrecta son:

- Si la antigua clave ZSK a sustituir se elimina demasiado pronto de la zona, los *resolvers* pueden dar por inválidas las respuestas DNSSEC, por corresponder la firma (RRSIG) a una clave que ya no está disponible.
- Respecto a la clave KSK, se puede sufrir una situación denominada "*DNS darkness*", en la cual el dominio estará totalmente inaccesible, si existe

desincronización entre el registro DS en la zona padre y la clave KSK de la zona hija.

- Si la clave KSK a renovar actúa como *trust-anchor* (se utiliza para firmar registros DS de zonas hijas), una renovación incorrecta romperá la cadena de confianza, y dejará a todas las zonas hijas y a sus subdominios asociados en estado *bogus* (ver apartado "5.2.2. Transición de *resolvers* de DNS a DNSSEC").

De cara a planificar los procesos de renovación, conviene tratar de automatizar la renovación de las claves (siempre con supervisión por parte del administrador) para evitar errores de planificación y/o errores humanos.

A continuación, se proporciona un esquema que permitiría asegurar la consistencia del proceso de renovación de claves en DNSSEC.

7.2.1. Clave ZSK

Las recomendaciones para los tiempos de renovación de la clave ZSK, empleando el método de pre-publicación de la misma, y teniendo en cuenta las implicaciones tanto desde el punto de vista de los *resolvers* como de los servidores DNS autoritativos secundarios, son [Ref.- 49]:

- Mínimo periodo de renovación:
 - Pre-publicación de la nueva ZSK:
TTL (RRSet DNSKEY) + periodo de transferencia de la zona
 - Fin de la publicación de la antigua ZSK:
***lifetime*¹⁸ (firmas) + TTL máximo de la zona + periodo de transferencia de la zona**
- Periodo conservador de renovación:
 - Pre-publicación de la nueva ZSK:
Período de expiración del SOA + periodo transferencia de la zona
 - Fin de la publicación de la antigua ZSK:
***lifetime* (firmas) + periodo expiración del SOA + periodo transferencia de la zona**

7.2.2. Clave KSK

Dado que la renovación de la clave KSK conlleva una interacción con agentes externos, como la zona padre, en lugar de fijar los parámetros del ciclo de vida de la clave KSK solo en función de los parámetros de tiempo y de los TTLs definidos en la zona, se recomienda establecer plazos conservadores (por ejemplo, de un mes previo al inicio de la renovación

¹⁸ El parámetro "*lifetime* (firmas)" corresponde al parámetro "*lifetime*" descrito en el apartado "4.1.3. Parámetros asociados a la validez de las firmas", que se calcula como la diferencia entre el periodo de validez de la firma menos el período de refresco.

y un mes posterior a su fin). Un esquema conservador para la renovación de la clave KSK consistiría en:

- Un mes antes de la fecha prevista de renovación:
 - Ajustar los metadatos de tiempo de la actual clave KSK para establecer la fecha de retirada (apuntando al día planificado para la renovación) y fecha de eliminación (un mes posterior a la renovación).
 - Generar la nueva clave KSK y su registro DS en base a los metadatos de la clave a renovar. Si la nueva clave KSK ya existiese, simplemente será necesario actualizar sus metadatos de tiempo.
 - Publicar la nueva clave KSK en el registro DNSKEY.
 - Transferir el registro DS a la zona padre.
 - Posteriormente, confirmar que el nuevo registro DS ha sido publicado correctamente.
- El día de la renovación:
 - Activar la nueva clave KSK para que se utilice en el proceso de firma (del registro DNSKEY), dejando de firmar con la clave KSK antigua.
- Un mes después de la renovación:
 - Eliminar la antigua clave KSK del registro DNSKEY de la zona.
 - Eliminar el antiguo registro DS de la zona padre.

7.3. Alternativas de gestión y firmado de la zona

La mayor parte de soluciones DNSSEC soporta tres modos de gestión de las claves y del proceso de firmado de la zona:

- Gestión manual: todas las operaciones de generación de claves, firmado de zona y gestión de las claves y del proceso de firmado se lleva a cabo por parte del administrador del servicio DNSSEC. Dentro de este esquema, hay dos posibilidades:
 - Todas las tareas las realiza manualmente el administrador.
 - El administrador diseña las tareas de generación de claves y asignación de parámetros de tiempo, pero incluye las respectivas actividades en tareas automatizadas (por ejemplo, mediante "`cron`").
- Gestión manual automatizada (manual de las claves y automática de la zona): el servidor DNSSEC mantiene las firmas y renueva las claves de firmado en base a los parámetros de tiempo definidos. Es el administrador quien crea las claves y determina y configura estos parámetros manualmente.
- Gestión automática de la zona: el servidor DNSSEC se encarga tanto del firmado automático de la zona como de la gestión de las claves, incluyendo su renovación, sin intervención (o intervención mínima) del administrador. Existen soluciones (por ejemplo, Knot), que permiten la renovación automática de la KSK, para lo cual comprueban periódicamente la existencia de registros DS en la zona padre y, cuando confirman su existencia, llevan a cabo las tareas de supresión de la clave KSK antigua.

Como se ha mencionado en diversos apartados de esta guía, una buena práctica de gestión de claves es disponer de dos claves de cada tipo (una KSK y otra ZSK):

- Una de ellas será la clave activa, y se usará para los procesos de firmado la zona.
- La otra será la clave de respaldo, pero no se utilizará para firmar la zona. Su parte privada deberá mantenerse fuera de los servidores DNS autoritativos de la zona para que no exista riesgo de compromiso.
 - Si se incluye la clave de respaldo en el RRSet de tipo DNSKEY, los *resolvers* tendrán en caché ambas copias, lo que acelera la transición de una a otra de cara a su futura renovación.
 - Incluso aunque no se incluya esta en el RRSet de tipo DNSKEY, disponer de la segunda clave ya creada simplifica la renovación ante una emergencia.

Si se desea que la clave de respaldo se emplee en los procesos de renovación, tanto automáticos como manuales, se asignarán los metadatos de tiempo definidos para el ciclo de vida definido del entorno a ambas claves, activa y de respaldo.

Ejemplo de generación de una clave ZSK de respaldo en BIND

Para generar una segunda clave ZSK de respaldo que se publique inmediatamente en la zona y se active dentro de 6 semanas, se debe hacer uso del siguiente comando:

```
$ dnssec-keygen -a [algoritmo] -P now -A +6w -r /dev/random <zona>
```

Con las opciones marcadas en negrita, la nueva clave se publicará inmediatamente ("-P now"), pero no se empleará aún para firmar la zona.

Si se desea que esta clave sea además la que se emplee para la renovación futura de la clave ZSK, se puede generar sin las opciones de tiempos marcadas en negrita, y establecer posteriormente los valores para los metadatos de tiempo de la clave a emplear mediante el comando "dnssec-settime", como se ilustra en el apartado "6.1.3.1. Generación de las claves en el sistema operativo".

Tabla 6 - BIND: generación de una clave ZSK de respaldo

7.3.1. Esquema de gestión y renovación de las claves con BIND

Un aspecto importante a tener en cuenta es que, antes de realizar cambios en las claves en una zona dinámica, es recomendable congelar las actualizaciones siguiendo la operativa propia del entorno DNS. Finalizado el proceso, se procederá a descongelar la zona.

La gestión de las claves se simplifica mediante la utilidad "dnssec-settime", que permite fijar los parámetros asociados al ciclo de vida de una clave descritos en la "Figura 10", tomando como base los valores de la clave que se indica como predecesora. De esta forma, BIND realizará de forma transparente para el usuario los procesos asociados a cada etapa.

- **Renovación manual:** conlleva los siguientes pasos:
 - Generación, publicación y activación de la clave de reemplazo mediante "dnssec-keygen -P now -A now". Si ya existiera una clave de respaldo generada previamente, bastaría con modificar los parámetros de tiempo para su activación inmediata mediante "dnssec-settime -P now -A now".
 - Inactivación de la clave actual para que la zona deje de firmarse con ella. Marcarla como eliminada con, al menos, unos días de margen para que las

cachés de los *resolvers* ya no contengan registros firmados con ella:
"dnssec-settime -I now -D <fecha>".

- Aplicar los cambios en BIND: "rndc loadkeys <zona>".
 - Tras un tiempo prudencial, definido a partir del borrado de la clave del entorno DNSSEC, se pueden borrar del sistema de ficheros los archivos correspondientes a las claves antiguas.
- **Renovación manual automatizada:** consiste en la inclusión de los comandos asociados al proceso de renovación de claves en tareas planificadas (por ejemplo, mediante la ejecución de scripts en "cron" planificados para ejecutarse con la periodicidad necesaria):
- La utilidad "dnssec-settime" permite fijar los parámetros asociados al ciclo de vida de una clave descritos en la "Figura 10" tomando como base los valores de la clave que se indica como predecesora; así, BIND realizará de forma transparente para el usuario los procesos asociados a cada etapa.
 - La herramienta "dnssec-keygen" incluye la opción "-s <clave_predecesora> -i <intervalo>", que permite crear una clave lista para suceder a la actual y que se pre-publicará en el intervalo especificado.
 - La fecha de activación de esta nueva clave se fijará con respecto a la fecha de inactivación de la clave de referencia (opción "-s <ZSK_antigua.key>" de la utilidad "dnssec-settime"), y, opcionalmente, se puede prepublicar antes para que los *resolvers* la vayan conociendo y teniendo en caché (opción "-i <intervalo>").
 - Fijar las fechas de retirada y eliminación de la actual clave ZSK (a renovar): opciones "-I" y "-D" del comando "dnssec-settime".
 - Aplicar los cambios en BIND: "rndc loadkeys <zona>".
 - El script deberá definir el directorio del cual leer las claves, de forma que BIND pueda acceder a ellas y realizar las acciones correspondientes.

ZSK:

```
$ cd /etc/bind/keys/ejemplo.es
$ dnssec-settime -I 20180701 -D 20180801 Kejemplo.es.+008+15844
./Kejemplo.es.+008+15844.key
./Kejemplo.es.+008+15844.private
$ dnssec-keygen -i +15d -S Kejemplo.es.+008+15844
Generating key pair..+++++ .....+++++
Kejemplo.es.+008+51423
```

KSK:

```
$ cd /etc/bind/keys/ejemplo.es
$ dnssec-settime -I 20180901 -D 20181001 Kejemplo.es.+008+0733
./Kejemplo.es.+008+0733.key
./Kejemplo.es.+008+0733.private

$ dnssec-keygen -i +30d -S Kejemplo.es.+008+0733
Generating key pair..+++++ .....+++++
Kejemplo.es.+008+17459

$ dnssec-dsfromkey -a RSASHA256 Kejemplo.es.+008+17459.key
```

Tabla 7 - BIND: generación de claves para gestión manual automatizada

- **Renovación automática:** mediante la técnica "*smart signing*" (ver apartado "6.1.5.2. Firmado automático"), el proceso *named* realizará automáticamente la renovación de las claves y los procesos de refirmado de la zona que aseguren que las firmas no expiren.
 - Habilitar la opción de configuración "`auto-dnssec: maintain`".
 - Generar la clave sustituta con los parámetros del ciclo de vida adecuados mediante "`dnssec-keygen`".
 - Modificar la clave antigua para que expire en el momento adecuado mediante "`dnssec-settime`".
 - Recargar la configuración en BIND mediante "`rndc reconfig`".

A partir de ese momento, BIND se encargará de la gestión automática de las claves.

Para la **renovación de la clave KSK**, si bien es posible automatizar parte del proceso, las dependencias existentes con la zona padre hacen recomendable que se coordinen ciertas acciones de forma manual, aunque asistidas por las utilidades ofrecidas por el software DNS. En el caso de BIND y utilizando el modelo de "Doble DS" (ver apartado "4.1.8. Mecanismo de renovación de las claves (*key rollover*)"):

- Mediante la herramienta "`dnssec-settime`", se ajustarán los parámetros de tiempo:
 - Sobre la clave nueva, si por cualquier causa, se desea variar los metadatos de tiempo de la clave que se generó para la renovación.
 - Sobre la clave antigua, para establecer la fecha de inactivación y de eliminación.
- Generar la nueva clave con la opción "-s" del comando "`dnssec-keygen`", que creará una clave sucesora para la clave antigua.
- La herramienta "`dnssec-dsfromkey`" permitirá obtener el futuro registro DS a partir de la nueva clave KSK.
- Se procederá a realizar el proceso de "doble firma" para la clave KSK descrito en el apartado "4.1.8. Mecanismo de renovación de las claves (*key rollover*)".

Se recomienda adicionalmente confirmar con la zona padre el mecanismo de actualización de los registros DS, para verificar los TTLs vigentes y por si hubiese otras novedades importantes a tener en cuenta.

NOTA: La renovación de la clave KSK se ha detallado según el esquema usado por BIND porque permite ilustrar los diversos pasos que deben llevarse a cabo. Servidores como PowerDNS incluyen mecanismos que permiten realizar este proceso de manera más intuitiva. Un ejemplo ilustrativo se proporciona en "<https://doc.powerdns.com/authoritative/guides/kskroll.html>".

7.3.1.1. `dnssec-keymgr`: automatización completa de la gestión de claves

Complementando la función "`auto-dnssec maintain`" para la gestión automática de la zona, BIND 9.11 introdujo la herramienta "`dnssec-keymgr`" [Ref.- 66].

Esta herramienta combina los comandos "`dnssec-keygen`" y "`dnssec-settime`" y, en base a unas políticas definidas en su fichero de configuración (por defecto, "`/etc/dnssec-policy.conf`") y a los metadatos de tiempo propios de las claves, automatiza casi completamente los procesos de renovación de claves.

El fichero de políticas (que puede tener tanto ámbito global como ámbito de zona) permite definir:

- `algorithm-policy [algoritmo] {}`: dentro de la política para el algoritmo criptográfico especificado, se puede fijar la longitud de ambas claves, ZSK y KSK:
 - `key-size zsk <...>;`
 - `key-size ksk <...>;`
- `policy [nombre] {}`: define la política con el nombre especificado, y dentro de ella admite (entre otros):
 - algoritmo de firma para esa política.
 - `roll-period [zsk || ksk]`: periodo de renovación de las claves (*rollover*).
 - `pre-publish [zsk || ksk] <plazo>`: periodo de publicación anticipada de las claves.
 - `post-publish [zsk || ksk] <plazo>`: fin del periodo de publicación de las claves.
 - `coverage <plazo>`: marca la duración, o periodo, durante la cual se desea asegurar que la clave es correcta.
- `zone <nombre_zona> {}`:
 - `policy <nombre>`: declara la política (con el nombre especificado anteriormente) que se aplicará a esa zona.
 - Si se desea alterar algún parámetro de los definidos por defecto en esa política, se puede incluir la directiva referente al parámetro con el nuevo valor deseado.

Una vez configuradas las políticas para una zona, la invocación del comando "`dnssec-keymgr`" examinará las claves existentes en el directorio especificado ("-K"), y comparará los metadatos de estas con las políticas que sean de aplicación. Si algún parámetro de la clave no es correcto, se corregirá para adaptarlo a la política.

Ejemplo de uso:

```
$ dnssec-keymgr -K /etc/bind/keys/ -r /dev/random <zona>
```

Figura 36 - Configuración del proceso de renovación de claves a través de `dnssec-keymgr`

Es importante destacar que el uso de políticas no es exclusivo de BIND. Por ejemplo, Knot también las emplea como método para automatizar la gestión de claves, y permite realizar una gestión totalmente automática de la zona [Ref.- 49].

Para poder asegurar que la renovación de la clave ZSK se ha completado, existen dos opciones:

- Monitorizar la propagación de la zona y seguir avanzando en el proceso de renovación y configuración solo si todos los servidores de nombres se han actualizado: se debe evitar que algún servidor DNS secundario no haya podido actualizar la zona pero siga proporcionando firmas con la clave ZSK antigua hasta que expire el TTL de la zona. En este caso, un *resolver* podría obtener la nueva ZSK de un servidor secundario actualizado, pero podría tener firmas correspondientes a la antigua ZSK proporcionadas por el servidor secundario desactualizado.
- Para simplificar el proceso, se puede simplemente adelantar los tiempos de pre-publicación de la nueva clave ZSK y los de fin de la publicación de la antigua para permitir que el TTL de la zona expire entre tanto, lo cual aseguraría consistencia en los *resolvers*.

El mecanismo de publicación anticipada para la ZSK está especialmente indicado para zonas DNSSEC de gran tamaño.

7.4. Sustitución de los algoritmos de firma y características criptográficas

La sustitución de los algoritmos de firma en DNSSEC, una vez la zona está firmada y operativa, no es trivial. Esto se debe a que existe software DNS de validación (*resolvers*) que asume que el algoritmo reflejado en el registro DS es utilizado para firmar todos los registros de la zona y, por tanto, no diferencia entre los registros firmados con la clave ZSK y los firmados con la clave KSK [Ref.- 77]. Así, mientras el antiguo registro DS esté presente en la zona padre, puede ocurrir que algunos *resolvers* fallen tras el cambio del algoritmo de firma.

Para evitar esta situación, si se desea cambiar el algoritmo de firma o sus características criptográficas, lo más recomendable es renovar la clave KSK y la clave ZSK al mismo tiempo.

Para simplificar el proceso, se recomienda que el cambio de algoritmo se realice en el servidor DNS autoritativo.

A continuación, se sugiere un posible procedimiento basado en los mecanismos de BIND según el esquema de "Doble DS" [Ref.- 74]:

- Generar los registros DNSKEY en base al nuevo algoritmo de firma.
- Incluir la nueva clave KSK y la nueva clave ZSK en la zona: en el caso de BIND, copiar los ficheros "K*" en el directorio empleado como repositorio de claves para *named*, con los permisos Unix/Linux apropiados.
- Firmar la zona con la nueva clave ZSK según el procedimiento marcado por la organización. En el caso de BIND, se distinguen dos situaciones, descritas en el apartado "6.1.5. Proceso de firma de zonas DNS con autoridad":
 - Zonas con gestión manual: los registros DNSKEY asociados a las nuevas claves se deben incluir en el fichero de configuración de la zona, y luego proceder al refirmado manual de la misma:
 - Si se hace uso de *inline signing* (ver apartado "6.1.5.2. Firmado automático"), se puede ejecutar el comando `nsupdate [update] add`¹⁹ para incluir el registro DNSKEY de las nuevas claves. Este comando efectúa operaciones de actualización dinámicas (*Dynamic DNS Updates*) según el RFC 2136.
 - En caso contrario, los nuevos registros DNSKEY se añadirán editando el fichero de configuración de la zona.
 - Zonas con gestión automática (opción "auto-dnssec: maintain"): *named* automáticamente firmará la zona con las nuevas claves en función de los metadatos de tiempo que contengan cuando transcurra el intervalo "dnssec-loadkeys-interval" o se ejecute el comando `rndc loadkeys`.

¹⁹ El comando "nsupdate" sólo es de aplicación en el caso de un servidor DNS autoritativo configurado como maestro.

- Publicar el nuevo registro DS en la zona padre y en cualquier otro repositorio de cadenas de confianza donde se haya incluido previamente la clave antigua (tipo DLV).
- Esperar el máximo TTL para los registros DS de la zona padre para asegurar que futuras consultas recuperarán el nuevo registro DS con el nuevo algoritmo de firma.
- Transcurrido dicho TTL, eliminar el registro DS correspondiente al antiguo algoritmo de firma y retirar la antigua clave KSK, clave ZSK y firmas asociadas de la zona.
- Esperar otro TTL más para que los antiguos registros DS desaparezcan de las cachés de los *resolvers*.
- Eliminar los registros DNSKEY correspondientes al algoritmo de firma antiguo de la zona. En el caso de BIND:
 - Para zonas de gestión automática: *named* se encargará de esta tarea. Si se desea iniciarlo manualmente, se puede utilizar la herramienta "`dnssec-settime -D <date/offset>`" con un valor relativo al pasado.
 - Para zonas de gestión manual: los antiguos registros DNSKEY y sus firmas deben ser eliminados del fichero de configuración de la zona:
 - Con *inline signing*, el comando "`nsupdate [update] [delete]`" provocará que se borren tanto los registros DNSKEY de las antiguas claves, como los correspondientes registros RRSIG.
 - En caso contrario, el administrador deberá eliminar los registros DNSKEY manualmente y volver a firmar la zona para que se eliminen todas las firmas realizadas con las claves antiguas.
- Eliminar los ficheros correspondientes a las claves empleadas por el antiguo algoritmo de firma del directorio de claves una vez verificado que los antiguos registros DNSKEY y sus RRSIGs correspondientes al algoritmo de firma que ha sido reemplazado se han eliminado.

7.5. Proceso de refirmado de zonas DNS con autoridad

Se dispone de dos alternativas para llevar a cabo el proceso de refirmado de zonas DNS con autoridad: manual y automático.

7.5.1. Refirmado manual

El refirmado de una zona estática que se gestiona manualmente se puede automatizar parcialmente mediante tareas "`cron`" en entornos Unix/Linux. Esto se debe a que la utilidad "`dnssec-signzone`" puede recibir como parámetro un fichero de zona ya firmado, y solo actualizará las firmas que hayan cambiado (añadiendo, borrando o actualizando los registros, según corresponda).

Si se utiliza la opción "`-i <intervalo_de_refresco>`" y se referencia el fichero de zona firmado, solo los registros cuya validez expire durante ese intervalo se refirmarán.

Según lo anterior, se puede ejecutar una tarea "`cron`" a diario para mantener la zona actualizada. Si la zona es muy grande, la opción "`-j`" (jitter) permitirá que la validez de los registros no venza simultáneamente en todos ellos, para distribuir en el tiempo el proceso de refirmado.

7.5.2. Refirmado automático

Si se usa la directiva `"inline-signing"` conjuntamente con `"autodnssec maintain"`, BIND se encargará de refirmar la zona según sea necesario, no requiriéndose acción alguna por parte del administrador.

7.6. Resolvers DNSSEC

Desde el punto de vista de los *resolvers*, la principal tarea administrativa consistirá en asegurar la actualización de los *trust-anchors* configurados para el *resolver* cuando éstos se renueven:

- Si el *resolver* está configurado para actualizar los anclajes de la cadena de confianza de forma manual, como ocurre en BIND si se emplea la opción `"dnssec-validation yes"`, la labor se reducirá a verificar periódicamente que los *trust-anchors* declarados en la directiva `"trusted-keys {...}"` son los auténticos, siguen siendo válidos y no han sido comprometidos.

Para el anclaje de la zona raíz, conviene descargar el *trust-anchor* de la web de IANA mediante una conexión segura HTTPS y de confianza, y compararlo con el configurado en el *resolver*. Si se emplean otros *trust-anchor*, el proceso será similar.

- Si el *resolver* emplea un método de actualización automática de los anclajes (como el *"Managed-Keys"* de BIND descrito en el apartado "6.2.1. Resolvers recursivos", también convendrá comparar de vez en cuando, por prudencia, las claves declaradas como `"managed-keys {...}"` en el fichero `"bind.keys"` con las obtenidas de los correspondientes sitios oficiales.

En ambos escenarios, siempre es preciso estar atento a los procesos de renovación de las claves KSK de la zona raíz, y de cualquier otra para la que se haya definido un anclaje de confianza específico.

Adicionalmente, dado que durante la validación de DNSSEC el *resolver*, además de la cadena de confianza, verifica el periodo de validez de la firma del registro, es preciso que la fecha y hora del *resolver* sean siempre correctas.

Otro elemento importante es revisar la política de actuación del *resolver* ante errores de DNSSEC, aunque no todos los *resolvers* ofrecen la misma granularidad. Así, por ejemplo, BIND solo permite habilitar/deshabilitar la validación, mientras que Knot define tres modos (estricto, normal y permisivo) [Ref.- 67].

7.7. Monitorización del entorno

Los elementos principales a monitorizar en el entorno DNSSEC son:

- **Fecha y hora** de los servidores DNS autoritativos para una zona. Además de comprobar el funcionamiento de NTP, hay que comprobar la hora del sistema, para evitar problemas en caso de que el servidor NTP no esté accesible para alguno de los servidores autoritativos, o de desajustes de la zona horaria (*timezone*).
- **Períodos de expiración de las claves:** el proyecto "Nagios" [Ref.- 68], que sirve para monitorizar redes y sistemas, incluye desde la versión 3.2.3 de su Core, monitorización para DNSSEC a través de un *plug-in*.
- **Consistencia del dominio:** se trata de determinar la corrección de las cadenas de confianza, la validez de las claves empleadas, etc. Actualmente, existen diversas

herramientas y aplicaciones web que permiten comprobar el estado de un dominio DNSSEC:

- <http://dnsviz.net>: recibe el nombre de un dominio y elabora el árbol de validación, incluyendo los registros DNSKEY.
 - <http://www.zonecheck.fr>: ofrece información general del dominio, incluyendo la conectividad, la consistencia y el estado de DNSSEC.
 - <https://zonemaster.iis.se>: equivalente al anterior.
 - <https://dnssec-analyzer.verisignlabs.com>: herramienta de Verisign Labs [Ref.- 36] mencionada en el apartado "6.1.7. Comprobación del servicio DNSSEC".
 - <https://en.internet.nl>: utilidad para la verificación de múltiples propiedades de un dominio, publicada por el gobierno holandés.
- **Comprobación del estado actual de una zona:** se puede emplear el siguiente comando de BIND, que mostrará los identificadores de las claves empleadas para la firma de una zona DNSSEC:

```
$ rndc signing -list ejemplo.es
Done signing with key 43530/RSASHA256
Done signing with key 0346/RSASHA256
```

Figura 37 - Comprobación de las claves usadas para la firma de una zona DNSSEC

- **Verificación de las transferencias de zona** entre servidores primarios y secundarios a través del "serial", para detectar si ha existido algún problema en el intercambio de la zona en alguno de los servidores DNS autoritativos.

7.7.1. Detección de problemas

Un problema en DNSSEC puede estar tanto en la parte servidora o autoritativa, como en el lado del *resolver*, aunque la mayor parte de errores se manifiestan en estos últimos, por lo que, en ocasiones, pueden resultar difíciles de identificar e, incluso, de detectar en el lado del servidor DNS autoritativo.

Por ello, un elemento importante en la monitorización del entorno DNSSEC es utilizar un servidor recursivo propio para realizar validaciones de prueba. Si la organización no dispone de uno propio, se puede recurrir a un *open resolver*.

Por su parte, los operadores de los *resolvers* recursivos desempeñan un importante papel en la detección de problemas, siendo deseable que informen de ellos a los propietarios de los dominios afectados, especialmente si se sospecha que el fallo tiene origen en un compromiso o incidente de seguridad en el dominio.

No obstante, antes de pensar en el posible compromiso del dominio, conviene descartar errores de administración y configuración, especialmente si se han producido cambios recientemente que afecten a las claves (como operaciones de renovación de claves, de refirmado de la zona o actualizaciones en la zona padre).

7.7.1.1. Herramientas de verificación

Los errores de validación de DNSSEC ocasionados en un *resolver* recursivo se trasladarán al cliente final como un mensaje SERVFAIL, pero dicho mensaje puede deberse a varias causas.

Antes de concluir que el fallo tiene origen en una configuración incorrecta de la zona DNSSEC consultada, hay que descartar que el fallo no esté en el lado del propio *resolver*. Para ello, se puede:

- Determinar si el dominio ha funcionado con normalidad habitualmente y ha dejado de hacerlo recientemente.
- Determinar si el dominio falla también desde un *resolver* ajeno al propio, preferiblemente con una versión de software distinta y actualizada.
- Emplear herramientas como "dig" para determinar si la respuesta obtenida desde el servidor autoritativo es consistentemente diferente de la obtenida a través de los *resolvers*, en cuyo caso se puede sospechar de un posible incidente de seguridad.

Para tratar de averiguar qué sucede, se puede recurrir a diversas herramientas:

- 1) Analizar el **syslog** del *resolver* en busca de mensajes significativos, en combinación con la herramienta "dig":

- error (insecurity proof failed) resolving
- named[6703]: error (no valid RRSIG) resolving
- named[6703]: error (broken trust chain) resolving
- verify failed due to bad signature (keyid=19036): RRSIG has expired
- verify failed due to bad signature (keyid=19036): RRSIG validity period has not begun

El mensaje proporcionará posibles pistas para encontrar la fuente del error:

- El error "broken trust chain" indica un problema debido a la cadena de confianza. En este caso se podría ejecutar:
 - Comando "dig @<dirección del resolver> <zona> DS" para obtener los registros DS de la zona.
 - Comando "dig @<dirección del resolver> <zona> DNSKEY +cd +multi +dnssec" para obtener los registros DNSKEY de la zona.
 - Comparando los identificadores de las claves ("*key id*") de ambas salidas, se verá si existe concordancia entre el registro DS que tiene la zona padre y el registro DNSKEY que publica la zona hija.

La siguiente figura ilustra este escenario en él se ve que el "key id" que publica la zona padre para el registro DS de la zona hija no coincide con el "key id" de la clave KSK de la zona hija, sino con el de la clave ZSK: todo apunta a un error del administrador en la generación del registro DS. Si el "key id" del registro DS publicado por la zona padre no coincidiese con ninguna de las dos claves (ZSK o KSK), cabría la posibilidad de un ataque que hubiese podido alterar alguno de los servidores, potencialmente el de la zona padre.

```
$ dig @1.1.1.1 ejemplo.es. DS
...
ejemplo.es. 22341 IN DS 31524 8 2 583AC...1A1A4

$ dig @1.1.1.1 ejemplo.es. DNSKEY +dnssec +cd +multi
...
ejemplo.es. 121 IN DNSKEY 257 ... ; KSK; ... key id = 30436
ejemplo.es. 121 IN DNSKEY 256 ... ; ZSK; ... key id = 31524
```

Figura 38 - Ejemplo de error en el syslog por fallo de validación de la cadena de confianza

- El error "verify failed due to bad signature" apunta a un problema con las firmas, es decir, el registro RRSIG. Cada RRSIG contiene dos referencias de tiempo (*timestamps*): fecha de inicio de validez de la firma y fecha de expiración de la firma. Si la fecha y hora en el *resolver* no se encuentran dentro de ese intervalo, se producirá un error de ese tipo, por lo que el primer paso será verificar en el *resolver* la referencia horaria en UTC con el comando "date -u" y ver si es correcta. Dentro de esta categoría de error, los errores más habituales son:
 - "RRSIG has expired for <recurso>": ejecutando el comando "dig @<dirección del resolver> <recurso> +cd +multi +dnssec", se comprobará:
 - Si existe una firma para el recurso: buscar el registro RRSIG.
 - Si la firma ha expirado: la fecha de expiración es la primera del registro RRSIG, tal como muestra el siguiente ejemplo:

```
$ date -u
Mon Jul 2 23:23:12 UTC 2018

$ dig @1.1.1.1 ww1.ejemplo.es.+cd +multi +dnssec
ww1.ejemplo.es.      4200 IN RRSIG CNAME 5 3 4200 (
                    20180629120654 20180605120654
```

Figura 39 - Ejemplo de error en el syslog debido a firma expirada

- "RRSIG validity period has not begun <recurso>": ejecutando el comando "dig @<dirección del resolver> <recurso> +cd +multi +dnssec", se comprobará:
 - Si existe una firma para el recurso: buscar el registro RRSIG.
 - Si la fecha de inicio de validez de la firma aún no ha comenzado: la fecha de inicio de validez es la segunda fecha del registro RRSIG, tal como muestra el siguiente ejemplo:

```
$ date -u
Mon Jul 2 23:23:12 UTC 2018

$ dig @1.1.1.1 ww2.ejemplo.es.+cd +multi +dnssec
ww2.ejemplo.es.      4200 IN RRSIG CNAME 5 3 4200 (
                    20180729120654 20180705120654
```

Figura 40 - Ejemplo de error en el syslog debido a firma aún no válida

- 2) Habilitar el mecanismo de "debug" del *resolver*: se recomienda no hacerlo inicialmente en el servidor recursivo de producción, ya que esto puede aumentar la carga del mismo, sino emplear preferiblemente un *resolver* de pruebas.
- 3) Utilizar "delv" (*Domain Entity Lookup & Validation*), utilidad similar a "dig" pero específicamente orientada a DNSSEC²⁰:

²⁰ <https://ftp.isc.org/isc/bind9/cur/9.12/doc/arm/man.delv.html>

```
$ delv @<dirección del resolver> <recurso> +rtrace +multiline
```

Figura 41 - Uso de "delv" para identificar fallos en DNSSEC

- 4) Utilizar sitios web que ofrecen recursos y servicios para comprobar la validación de DNSSEC a través de una página web. Algunos de los servicios disponibles son²¹:
- <http://www.dnssec-failed.org>: servicio configurado expresamente para que los servidores que validan DNSSEC fallen y devuelvan un error de estado "SERVFAIL" ante la ejecución del comando:

```
$ dig @<resolver> dnssec-failed.org A +dnssec
```
 - Abriendo desde un navegador el enlace "<https://www.dnssec-tools.org>" o "<http://www.dnssec-deployment.org>", se obtendrá un mensaje informando de si se está realizando validación DNSSEC o no.
 - Otros servicios alternativos:
 - <http://www.rhybar.cz>
 - <http://en.conn.internet.nl/connection>
 - <http://dnssec.vs.uni-due.de>
 - <http://www.dnssec-validator.cz>
- 5) Si se sospecha que el error no está originado en la parte servidora DNSSEC, sino en el *resolver*, se puede recurrir a *resolvers* públicos que diversas entidades ponen a disposición de la comunidad como, por ejemplo, los DNS-OARC²². Se puede contrastar las salidas de los comandos "dig" utilizando dichos servidores con las ofrecidas por el *resolver* propio, y tratar de ver dónde radica el problema.

7.8. Procedimientos de emergencia

Una emergencia en el entorno DNSSEC puede deberse a diversas causas:

- Alguna de las claves ha sido comprometida: en este caso, se debe definir un mecanismo y procedimiento de revocación y renovación de claves, dado que el protocolo no define un mecanismo estándar [Ref.- 76].
Debido a que técnicamente las firmas en DNSSEC tienen validez hasta su tiempo o periodo de expiración, no es posible revocar los registros firmados una vez han sido generados (ver apartado "4.1.3. Parámetros asociados a la validez de las firmas").
- Un problema en la zona padre impide la verificación de las cadenas de confianza, por lo que la zona hija es inaccesible:
 - Registro DS incorrecto (por haber expirado la validez o por un error en la configuración o renovación).
 - Problemas con la validación o generación de las firmas de la zona padre.

7.8.1. Renovación de claves ante una emergencia

Las medidas de cara a minimizar el impacto ante una situación de emergencia dependen principalmente del riesgo asociado a que las claves se vean comprometidas. Así, por

²¹ <http://www.internetsociety.org/deploy360/resources/dnssec-test-sites/>

²² <https://www.dns-oarc.net/oarc/services/odvr>

ejemplo, si se almacenan en un módulo HSM o la zona se firma de forma *offline*, el riesgo de compromiso es tan reducido que quizá asumir el coste de las medidas de mitigación del impacto no compense.

En caso de que exista un riesgo alto de que las claves sean comprometidas, o que la consecuencia del posible compromiso sea significativa, se recomienda (ver RFC 7583 [Ref.- 43]):

- Disponer de dos claves de reemplazo en estado "Ready" (preparadas):
 - Para la clave ZSK, esto es posible con el esquema de pre-publicación de la futura nueva clave. Si, por las características de la zona, la clave privada está expuesta y existe mayor riesgo de compromiso, se puede optar por disponer de un RRSet de tipo DNSKEY en *stand-by* de forma que se pueda usar tan pronto la clave de reemplazo se active.
 - Para la clave KSK, con el método de "Doble KSK" (que requiere que la clave de respaldo se introduzca en el RRSet de tipo DNSKEY), si además se usa también para firmar el registro DNSKEY, la renovación solo requeriría introducir el nuevo registro DS en la zona padre. Con el método de "Doble DS", como la zona padre ya dispone del registro DS de *standby*, solo sería preciso activar la clave y empezar a usarla para firmar el RRSet de tipo DNSKEY.
- Reducir el TTL del RRSet de tipo DNSKEY para que el periodo de compromiso sea más pequeño.
- Reducir el periodo de validez de la firma del RRSet de tipo DNSKEY, se recomienda que no sea mayor de una semana, para que el periodo de compromiso sea más pequeño (ver apartado "4.1.3. Parámetros asociados a la validez de las firmas").
- Revocar la clave comprometida tan pronto sea posible. El procedimiento recomendado es:
 - Generar una nueva clave para su reemplazo.
 - Marcar la clave actual como "REVOKED".
 - Firmar la zona con ambas claves (revocada y nueva) para que, cuando los *resolvers* examinen el RRSet de tipo DNSKEY, no vuelvan a aceptar la clave revocada para verificar las firmas, pero puedan validar la respuesta con la nueva clave.
 - Eliminar la clave de la zona transcurrido el máximo TTL de la zona.

El comando `"dnssec-revoke {fichero_de_claves}"` de BIND leerá el fichero de claves especificado, activará el bit "REVOKED" en la clave y generará una nueva clave (un par de ficheros de claves pública y privada) con nuevo "key id" a partir de la clave revocada.

Tras eliminar la clave comprometida de la zona, se recomienda verificar que efectivamente la misma ha sido eliminada del RRSet de tipo DNSKEY, de forma que la misma no pueda ser considerada como válida en operaciones de firma futuras.

7.8.2. Problemas de resolución de la zona

Un problema de resolución que afecte a toda la zona en DNSSEC puede deberse a dos factores principales:

- Un fallo de seguridad (como el compromiso de las claves).
- Un fallo de configuración, entre otros:

- Una definición incorrecta de los parámetros de tiempo de la clave de firma de zona, (ZSK) que puede provocar que las firmas expiren antes de lo esperado.
- Una renovación fallida de las propias claves, como el borrado de las antiguas antes de que se hayan propagado los cambios a todos los agentes.
- Una definición incorrecta de los parámetros de tiempo de las firmas de la zona (registros RRSIG) que puede provocar que las firmas expiren antes de lo esperado.
- No disponer de los *trust-anchors* correctos, bien por compromiso en el propio entorno, bien por haber sido renovados sin que la zona DNSSEC haya incorporado los nuevos.
- Problemas con los registros DS en la zona padre, que impidan la validación de la cadena de confianza hacia la zona hoja.
- Diferencias en el comportamiento de los *resolvers*.

En el caso de un problema de validación debido al compromiso de la zona padre, podría llegar a ser necesario planificar la conversión de una zona DNSSEC firmada a una zona DNS estándar no firmada.

BIND ofrece la directiva `"dnssec-secure-to-insecure yes"`, que permite convertir una zona firmada (DNSSEC) en una zona no firmada (DNS). Si se está realizando la gestión automática de la zona, será necesario cambiar el parámetro `"auto-dnssec"` del valor `"maintain"` al valor `"allow"` y llevar a cabo la aplicación de la nueva configuración mediante `"rndc reload"`.

Para evitar tener que acometer una medida tan drástica, existe un mecanismo denominado "Negative Trust Anchors", que se describe a continuación.

7.8.2.1. Negative Trust Anchors (NTA)

En el RFC 7646 [Ref.- 73] de septiembre de 2015 se propuso el concepto de "*Negative Trust Anchor*" (NTA) como el opuesto al de un *trust-anchor*. Es decir, si el *trust-anchor* establece el punto de arranque de una cadena de confianza en DNSSEC, el NTA establece el fin de la cadena de confianza o validación de forma que, al topar con uno, el *resolver* tratará las respuestas recibidas como si la zona hija no estuviera firmada (es decir, no hiciera uso de DNSSEC), y no incorporará el *flag AD* en sus respuestas a los clientes.

Este mecanismo opera del lado del *resolver*, y mediante los NTAs no pretende deshacerse de los errores de validación de DNSSEC para evitarlos sin más, sino disponer de un mecanismo **temporal** para un escenario en el que un dominio está inaccesible por un problema de configuración, situación que se debe haber constatado previamente (descartando que el motivo es un compromiso o incidente de seguridad). En caso contrario, podría ocurrir que la zona haya sido comprometida y, al aceptar los NTAs, se estaría permitiendo que el atacante controlase la zona desde el punto de vista del servicio DNS. Por tanto, los operadores de *resolvers* que hayan activado un NTA deben comprobar periódicamente si la zona afectada ya opera normalmente con DNSSEC para desactivar el NTA. Idealmente, esto debe comprobarse para todos los servidores DNS autoritativos de dicha zona.

Antes de establecer un NTA, se debe comprobar que la validación del dominio no se ha roto intencionadamente y circunstancialmente (por ejemplo, durante la realización de unas pruebas).

El mecanismo de NTA también es útil durante el despliegue inicial de DNSSEC, a fin de poder realizar pruebas antes de la puesta en producción.

Por ejemplo, BIND 9.11 incorporó el parámetro "nta" a su comando "rndc" para añadir un NTA a una zona. La opción "-1" establece la duración en segundos (por defecto) del NTA. Para eliminar el NTA, se emplea la opción "-r <zona>":

```
$ rndc nta -1 60 ejemplo.es
Negative trust anchor added: ejemplo.es/_default, expires 14-June-2018
13:49:09.000

$ rndc nta -dump
ejemplo.es: expiry 14-June-2018 13:49:09.000

$ rndc nta -r ejemplo.es
```

Figura 42 - Uso de NTAs en BIND: creación, listado y borrado

7.9. Resumen de las buenas prácticas en la operación de DNSSEC

A continuación, se proporciona un resumen de las recomendaciones de cara a la operación de la zona en DNSSEC:

- Ciclo de vida y gestión de las claves:
 - Establecer los parámetros de tiempo de renovación de las claves en función de las necesidades del entorno, incluyendo el intervalo de renovación, mecanismos de publicación y eliminación de las claves reemplazadas de forma que la zona no quede en un estado *bogus*.
 - El periodo de renovación habitual de la clave ZSK es de entre 1 y 4 meses, mientras que el de la clave KSK es de entre 1 y 2 años.
 - Los plazos conservadores de renovación de claves serán de al menos 1 mes para la KSK. Para la ZSK, dependerá de diversos factores asociados al servicio DNSSEC y los parámetros de tiempo configurados actualmente.
 - Para la clave ZSK, se recomienda el método de pre-publicación.
 - Para la clave KSK, se recomienda el método de "Doble DS" para minimizar la cantidad y el tamaño de los datos firmados.
 - Disponer de conjunto adicional de claves de respaldo para simplificar la renovación de las claves actuales.
 - Evaluar el valor de expiración del SOA y de los TTLs que afectan a la zona, tanto de cara al tiempo de propagación de los nuevos registros a través del sistema de nombres entre los servidores DNS autoritativos, como de cara al tiempo de validez de los registros, durante el cual todavía serán válidos en los servidores de caché que pudieran haber almacenado registros de la zona.
 - Se recomienda, siempre que sea posible, recurrir a la gestión automática de la zona en DNSSEC.
- Refirmado de la zona:
 - Siempre que sea posible, recurrir a mecanismos de refirmado automático como, por ejemplo, *inline signing* en BIND.
- Resolvers DNSSEC:

- Recurrir a la gestión automática de los *trust-anchors* en los resolvers DNSSEC.
- Cotejar periódicamente los *trust-anchors* configurados en los *resolvers* con los publicados oficialmente por las entidades responsables.
- Monitorización del entorno:
 - Verificar las referencias horarias: fecha y hora.
 - Revisión de los períodos de expiración de las claves.
 - Comprobar la consistencia del dominio mediante herramientas de análisis de DNSSEC.
 - Supervisar la correcta operativa de las transferencias de zona entre los servidores DNS autoritativos primarios y secundarios.
 - Establecer mecanismos de detección de problemas, mediante herramientas locales y también mediante servicios disponibles en recursos públicos.
- Establecer un procedimiento de emergencia que minimice el impacto de los fallos, compromisos y posibles incidentes de seguridad.

8. GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

Agente registrador (*Registrar*): Entidad intermediaria entre el propietario de un dominio (*Registrant*) y el organismo registrador del TLD de primer nivel correspondiente (*Registry* o *Registro*). Gestiona el alta del dominio (tanto DNS como DNSSEC).

Anclaje de confianza (*Trust-anchor*): Elemento común (o raíz) del que parte la cadena de confianza, en el cual confían necesariamente todos los agentes implicados en la validación de dicha cadena.

Apex: El *apex* de una zona es el punto más alto de entrada a esa zona en la jerarquía DNS, por ejemplo, "incibe.es" para la zona "incibe.es" de INCIBE.

AXFR: Transferencia de zona autoritativa completa (operación de DNS).

Cadena de confianza: Mecanismo por el cual un agente confía en otro en base a la verificación de firmas criptográficas desde un punto o elemento de confianza común para ambos.

ccTLD: *country code Top Level Domain*. Dominio de primer o más alto nivel en la jerarquía de DNS que representa a un país concreto, como por ejemplo ".es", ".fr" o ".pt".

Claves de DNSSEC:

ZSK: *Zone Signing Key*. Clave de firmado de zona en DNSSEC.

KSK: *Key Signing Key*. Clave de firmado de (otras) claves (por ejemplo, la ZSK) en DNSSEC.

DHCP: *Dynamic Host Configuration Protocol*. Protocolo de gestión y configuración de red para la asignación de direcciones IP dinámicamente, junto a otros parámetros de configuración como, por ejemplo, los servidores DNS o *gateway* por defecto.

DNS: *Domain Name System*. Protocolo empleado para la resolución de nombres y direcciones IP en Internet.

DNS *cache poisoning*: Ataque de envenenamiento de caché DNS.

DNS *spoofing*: Ataque de suplantación de las peticiones y/o respuestas DNS.

DNSSEC: *Domain Name System Security Extensions* (extensiones de seguridad para el sistema de nombres de dominio). Conjunto de técnicas que añaden autenticidad e integridad al servicio DNS.

DDoS: *Distributed Denial of Service*. Ataque de denegación de servicio distribuido.

DoS: *Denial of Service*. Ataque de denegación de servicio.

DSA: *Digital Signature Algorithm*. Algoritmo de firma criptográfica basado en clave pública.

ECDSA: *Elliptic Curve Digital Signature Algorithm*. Algoritmo de firma criptográfica basado en curvas elípticas.

EDNS (o EDNS0): *Extended DNS*, ampliación del protocolo DNS para la gestión de paquetes DNS de mayor tamaño al estándar de una trama DNS sobre UDP (512 bytes).

GSS-TSIG: *Generic Security Service for TSIG* o *Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS*. Evolución del protocolo TSIG (ver TSIG).

gTLD: *generic Top Level Domain*. Dominio de primer o más alto nivel genérico en la jerarquía de DNS, como por ejemplo ".com", ".net" o ".org".

Hold-down time: Período de 30 días durante el cual el RRset de la nueva KSK se publica continuamente por la KSK antigua.

HMAC: *keyed-Hash Message Authentication Code* o *Hash-based Message Authentication Code*. Código de autenticación generado en base a un algoritmo de *hash* y una clave secreta.

HSM: *Hardware Security Module*. Módulo hardware empleado para el almacenamiento y gestión de material y claves criptográficas.

IANA: *Internet Assigned Numbers Authority*. Organismo internacional encargado, entre otros, de la gestión de los servidores DNS de los dominios de primer nivel (TLDs) del servicio DNS.

ICANN: *Internet Corporation for Assigned Names and Numbers*. Organismo internacional encargado, entre otros, de la gestión de los dominios genéricos de primero más alto nivel (gTLDs) del servicio DNS, y de los servidores DNS raíz.

ISP: *Internet Service Provider*. Proveedor de servicios de Internet.

IXFR: Transferencia de zona incremental (operación de DNS).

MitM: *Man in the Middle*, ataques de hombre en el medio basados en la interceptación del tráfico del usuario o servidor víctima.

NOTIFY: Operación de DNS mediante la cual el servidor autoritativo primario (o maestro) de una zona informa a los servidores secundarios (o esclavos) de un cambio en la zona.

NTA: *Negative Trust Anchors*. Concepto opuesto al de un *trust-anchor*. El *trust-anchor* establece el punto de arranque de una cadena de confianza, mientras que el NTA establece el fin de la cadena de confianza o validación en DNSSEC.

NTP: *Network Time Protocol*. Protocolo de red para la sincronización de tiempos y referencias horarias.

PRNG: Pseudo Random Number Generator. Generador de números pseudo-aleatorios.

Resolver: Cliente DNS encargado de trasladar las consultas sobre recursos de red al servicio de nombres. Puede ser tanto un cliente final (*stub resolver*) como un servidor DNS recursivo (*recursive resolver*).

Registro (*Registry*): Entidad responsable de la gestión y operación de los TLDs de primer nivel, ya sean ccTLDs o gTLDs.

Red.es: Registro a nivel de DNS, u organismo responsable, del ccTLD para España, ".es".

Registros de DNSSEC:

CDNSKEY: *Child DNSKEY*. Registro correspondiente a una copia del registro DNSKEY del servidor DNS hijo.

CDS: Child DS. Registro correspondiente a una copia del registro DS del servidor DNS hijo.

DS: *Delegation Signer*. Registro que contiene la referencia a una zona delegada, junto a una referencia al hash criptográfico del registro DNSKEY de la clave KSK de la zona delegada.

DNSKEY: *DNS Key*. Registro que contiene la clave ZSK (Zone Signing Key) y la clave KSK (Key Signing Key) de la zona.

RRSIG: *Resource Record SIGNature*. Registro que contiene la firma criptográfica empleada para autenticar los de registros de DNSSEC (RRsets).

NSEC: *Next SECure*. Registro que permite probar la negación de existencia (denial of existence) de un registro DNS, es decir, demostrar que el registro DNS asociado al recurso solicitado no existe.

NSEC3: *Next SECure versión 3*. La versión 3 del registro NSEC introduce mejoras respecto a NSEC.

RNG: *Random Number Generator*. Generador de números aleatorios.

RR: *Resource Record*. Registro con información de resolución de nombres de un recurso en el servicio DNS.

RRset: *Resource Record set*. Conjunto de registros con información de resolución de nombres de un mismo tipo de recurso en el servicio DNSSEC.

RSA: *Rivest-Shamir-Adleman*. Algoritmo de firma criptográfica (entre otros usos) basado en clave pública.

SEP: *Secure Entry Point*. Bit empleado en los registros DNSKEY de DNSSEC para indicar si el registro corresponde a una clave KSK (1) o a una clave ZSK (0). El término de punto de entrada segura en DNSSEC (o Secure Entry Point) refleja el punto de entrada a una zona con soporte para DNSSEC (de ahí la referencia a segura), identificado en el proceso de delegación de DNSSEC entre una zona padre y una zona hija por los registros DS.

SLA: *Service Level Agreement*. Acuerdo de nivel de servicios, que especifica los requisitos del servicio a proporcionar, como por ejemplo el nivel de confidencialidad o la disponibilidad requerida (ej. 99,99%).

STIC: Sistemas y tecnologías de información y comunicaciones.

Stub resolver: En la terminología de DNS y DNSSEC, un "stub resolver" es el cliente DNS final que se comunica habitualmente con un servidor DNS *resolver*, que también actúa como cliente DNS frente a los servidores DNS autoritativos.

TLD: *Top Level Domain*. Dominio de primer o más alto nivel en la jerarquía de DNS, genérico (gTLD) o por país (ccTLD), como por ejemplo ".com" o ".es".

TSIG: *Transaction SIGNature protocol* o Secret Key Transaction Authentication for DNS. Protocolo que proporciona los medios para identificar y autenticar a los extremos de una conexión DNS, por ejemplo, una transferencia de zona.

TTL: *Time To Live*. Periodo de validez de un elemento del servicio DNS (registro, clave, etc.) desde la fecha de su creación.

Trust-anchor: Ver "Anclaje de confianza".

9. ANEXO: REGISTROS CDS Y CDNSKEY

Debido a la complejidad de renovar la clave KSK causada por la necesidad de coordinación entre la zona padre y la zona hija, en septiembre de 2014 se propuso el RFC 7344 [Ref.- 71], el cual se actualizó mediante el RFC 8078 [Ref.- 71] en marzo de 2017.

En estas especificaciones se propone un método que permita a los operadores de dominios de las zonas hijas renovar las claves KSK empleando mecanismos propios de DNS. Algunos operadores de dominio y agentes registradores, como CloudFlare [Ref.- 72], están impulsando la iniciativa ante el beneficio que supondría para el entorno DNSSEC.

Para ello, se crean dos nuevos registros con el siguiente propósito:

- **CDS (Child DS):** registro correspondiente a una copia del registro DS del servidor DNS hijo, listo para ser transferido al servidor DNS padre. Se emplea en las solicitudes de actualización de los registros DS por parte de una zona hija en la zona padre. Si los dos registros CDS y CDNSKEY están disponibles en la zona hijo, el registro CDS tiene preferencia.
- **CDNSKEY (Child DNSKEY):** registro correspondiente a una copia del registro DNSKEY del servidor DNS hijo, listo para ser transferido al servidor DNS padre. Se emplea en las solicitudes de actualización de los registros DS (hash calculado a partir del registro DNSKEY) por parte de una zona hija en la zona padre.

Ambos registros forman un RRSet que expresa el contenido que la zona hija desea que se publique en la zona padre en relación al RRSet de los registros DS cuando desee efectuar un cambio en el registro DS, asociado a un cambio en la clave KSK. Es decir, la publicación de un RRSet CDS/CDNSKEY indica a la zona padre que debe reemplazar el registro DS que almacena para la zona hija y el formato final deseado para él, dejando a criterio de la zona padre las operaciones necesarias en sus sistemas para formalizar y completar este cambio.

Estos registros no influyen en la cadena de validación de DNSSEC, es decir, no afectan a los *resolvers*.

El uso de estos nuevos registros es opcional, tanto para la zona padre como para la zona hija. Si la zona padre soporta su uso, el cambio en el RRSet formado por ambos registros se puede detectar en la zona padre de dos formas:

- **Polling (sondeo):** la zona padre ejecuta una comprobación periódica de todas las zonas hijas para los que guarda un registro DS.
- **Pushing (notificación):** la zona hija notifica a la zona padre de la modificación de su registro CDS/CDNSKEY.

Dado que aún no existe un estándar de facto, cada software DNS servidor puede utilizar soluciones diferentes. Por ejemplo, PowerDNS ofrece un mecanismo específico²³.

Por su parte, BIND incluyó en su versión 9.11 el uso de ambos registros²⁴, añadiendo además las opciones "SYNC Publish" y "SYNC Delete" a los comandos "dnssec-keygen" y "dnssec-settime" para gestionar la publicación y eliminación de los registros CDS y CDNSKEY durante la gestión de las claves.

²³ <https://doc.powerdns.com/authoritative/guides/kskrollcdnskey.html>

²⁴ <https://www.isc.org/downloads/bind/bind-9-11-new-features/>

10. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

Referencia	Título, autor, fecha y enlace web
[Ref.- 1]	"Estudio del estado de DNSSEC en España". INCIBE-CERT. INCIBE (Instituto Nacional de Ciberseguridad de España). 4 de octubre de 2018. URL: https://www.incibe-cert.es/guias-y-estudios/estudios/estudio-del-estado-dnssec-espana
[Ref.- 2]	"Guía de seguridad en servicios DNS". CERTSI. INCIBE (Instituto Nacional de Ciberseguridad de España). 9 de abril de 2014. URL: https://www.certs.es/blog/guia-dns URL: https://www.certs.es/sites/default/files/contenidos/guias/doc/guia_de_seguridad_en_servicios_dns.pdf
[Ref.- 3]	"CVE-2008-1447: DNS Cache Poisoning Issue ("Kaminsky bug)". ISC Knowledge Base. July 2008. URL: https://kb.isc.org/article/AA-00924 URL: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html URL: https://www.kb.cert.org/vuls/id/800113
[Ref.- 4]	"RFC 2065: Domain Name System Security Extensions". IETF. January 1997. URL: https://tools.ietf.org/html/rfc2065
[Ref.- 5]	"RFC 4035: Protocol Modifications for the DNS Security Extensions". IETF. March 2005. URL: https://tools.ietf.org/html/rfc4035
[Ref.- 6]	"Domain Name System Security (DNSSEC) Algorithm Numbers". IANA. October 2017. URL: https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml
[Ref.- 7]	"RFC 4034: Resource Records for the DNS Security Extensions". IETF. Marzo 2005. URL: https://tools.ietf.org/html/rfc4034
[Ref.- 8]	"RFC 2845: Secret Key Transaction Authentication for DNS (TSIG)". IETF. May 2000. URL: https://tools.ietf.org/html/rfc2845
[Ref.- 9]	"RFC 2931: DNS Request and Transaction Signatures (SIG(0)s)". IETF. September 2010. URL: https://tools.ietf.org/html/rfc2931
[Ref.- 10]	"RFC 6944: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status". IETF. April 2013. URL: https://tools.ietf.org/html/rfc6944
[Ref.- 11]	"Digital Signature Standard (DSS)". NIST. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[Ref.- 12]	"RFC 8017: PKCS #1: RSA Cryptography Specifications Version 2.2". IETF. November 2016. URL: https://tools.ietf.org/html/rfc8017
[Ref.- 13]	"RFC 6605: Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC". IETF. April 2012. URL: https://tools.ietf.org/html/rfc6605
[Ref.- 14]	"KeyLength.com: Cryptographic Key Length Recommendations". BlueKrypt. URL: https://www.keylength.com/en/3/ (ejemplo, ECRYPT)
[Ref.- 15]	"ECDSA: The missing piece of DNSSEC". CloudFlare. URL: https://www.cloudflare.com/dns/dnssec/ecdsa-and-dnssec/
[Ref.- 16]	"Making the Case for Elliptic Curves in DNSSEC". Roland van Rijswijk-Deij et al. October 2015. URL: http://www.sigcomm.org/sites/default/files/ccr/papers/2015/October/0000000-0000002.pdf
[Ref.- 17]	"Increasing the Zone Signing Key Size for the Root Zone". Verisign. June 2016. URL: https://www.nanog.org/sites/default/files/Wessels02.pdf
[Ref.- 18]	"Cryptographic sanity: Key sizes". SURF. Agosto 2010. URL: https://blog.surf.nl/en/cryptographic-sanity-key-sizes/ "Good practices guide for deploying DNSSEC". ENISA. 2010. URL: https://www.enisa.europa.eu/publications/gpgdnssec
[Ref.- 19]	"RFC 5702: Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC". IETF. October 2009. URL: https://tools.ietf.org/html/rfc5702
[Ref.- 20]	"Increasing the Strength of the Zone Signing Key for the Root Zone". Verisign. May 2016. URL: https://blog.verisign.com/security/increasing-the-strength-of-the-zone-signing-key-for-the-root-zone/
[Ref.- 21]	"Recommendations for DNSSEC deployment at municipal administrations and similar organisations". Kirei AB. 2014. URL: https://www.iis.se/docs/Recommendations_for_DNSSEC_deployment.pdf

Referencia	Título, autor, fecha y enlace web
[Ref.- 22]	"RFC 4033: DNS Security Introduction and Requirements". IETF. March 2005. URL: https://tools.ietf.org/html/rfc4033
[Ref.- 23]	"RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence". March 2008. URL: https://tools.ietf.org/html/rfc5155
[Ref.- 24]	"RFC 4509: Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)". IETF. May 2006. URL: https://tools.ietf.org/html/rfc4509
[Ref.- 25]	"RFC 6781: DNSSEC Operational Practices, Version 2". IETF. December 2012. URL: https://tools.ietf.org/html/rfc6781
[Ref.- 26]	"RFC 3110: RSA/SHA-1 SIGs and RSA KEYS in the Domain Name System (DNS)". IETF. May 2001. URL: https://tools.ietf.org/html/rfc3110
[Ref.- 27]	"RFC 4509: Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)". IETF. May 2006. URL: https://tools.ietf.org/html/rfc4509
[Ref.- 28]	"RFC 5011: Automated Updates of DNS Security (DNSSEC) Trust Anchors". IETF. September 2007. URL: https://tools.ietf.org/html/rfc5011
[Ref.- 29]	"ECDSA and DNSSEC". APNIC. October 2014. URL: https://blog.apnic.net/2014/10/23/ecdsa-and-dnssec/
[Ref.- 30]	"Random Numbers". OpenSSL. URL: https://wiki.openssl.org/index.php/Random_Numbers
[Ref.- 31]	"Google Public DNS". Google. URL: https://developers.google.com/speed/public-dns/docs/using "Announcing 1.1.1.1": Cloudflare. URL: https://blog.cloudflare.com/announcing-1111/
[Ref.- 32]	"Setting up DNSSEC". Oracle + Dyn. URL: https://help.dyn.com/setting-up-dnssec/
[Ref.- 33]	"Proteja su dominio con DNSSEC". OVH. URL: https://docs.ovh.com/es/domains/proteja_su_dominio_con_dnssec/
[Ref.- 34]	"Declaración de Políticas y Procedimientos para DNSSEC en la zona ".ES"". Red.es. Junio 2014. URL: http://www.dominios.es/dominios/sites/dominios/files/files/Declaraci%C3%B3n%20de%20Pol%C3%ADticas%20y%20Procedimientos%20para%20DNSSEC%20en%20la%20zona%20%20ES.pdf
[Ref.- 35]	"DNSSEC Complexities and Considerations - Key Management". CloudFlare. URL: https://www.cloudflare.com/dns/dnssec/dnssec-complexities-and-considerations/
[Ref.- 36]	"DNSSEC analyser". Verisign Labs. URL: https://dnssec-analyzer.verisignlabs.com
[Ref.- 37]	"Trust Anchors and Keys ". IANA. URL: https://www.iana.org/dnssec/files "root zone trust anchor file". IANA. URL: https://data.iana.org/root-anchors/root-anchors.xml "root zone detached signature file". IANA. URL: https://data.iana.org/root-anchors/root-anchors.p7s
[Ref.- 38]	"BIND". ISC, Internet System Consortium. URL: https://www.isc.org/downloads/bind/
[Ref.- 39]	"Unbound". NLNETLABS. URL: https://www.nlnetlabs.nl/projects/unbound/about/
[Ref.- 40]	"Knot DNS". CZ.NIC. URL: www.knot-dns.cz
[Ref.- 41]	"Root Zone KSK Rollover". URL: https://www.icann.org/resources/pages/ksk-rollover
[Ref.- 42]	"RFC 6841: A Framework for DNSSEC Policies and DNSSEC Practice Statements". ICANN. January 2013. URL: https://tools.ietf.org/html/rfc6841
[Ref.- 43]	"RFC 7583: DNSSEC Key Rollover Timing Considerations". IETF. October 2015. URL: https://tools.ietf.org/html/rfc7583
[Ref.- 44]	"Deploying DNSSEC: Validation on recursive caching name servers". Surf Net (Roland van Rijswijk - Deij). August 2012. URL: https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_Deploying_DNSSEC_v20.pdf

Referencia	Título, autor, fecha y enlace web
[Ref.- 45]	"Observations from the DNSSEC Deployment". Osterweil, Eric & Massey, Dan & Zhang, Lixia. (2007). 1 - 6. 10.1109/NPSEC.2007.4371619. URL: https://www.researchgate.net/publication/4286260_Observations_from_the_DNSSEC_Deployment
[Ref.- 46]	"OpenDNSSEC". Roland M. van Rijswijk – Deij et al. URL: https://www.opendnssec.org/
[Ref.- 47]	"OpenDNSSEC Initial Deployment Guide". W. Matthijs Mekking. November 2014. URL: https://www.opendnssec.org/wp-content/uploads/2009/06/opendnssec-start-guide.pdf "OpenDNSSEC 2.X Documentation". URL: https://wiki.opendnssec.org/display/DOCS20
[Ref.- 48]	"BIND 9 Administrator Reference Manual". ISC, Internet System Consortium. 2018. URL: https://ftp.isc.org/isc/bind9/cur/9.12/doc/arm/Bv9ARM.html
[Ref.- 49]	"DNSSEC signing your domain with BIND inline signing". Switch Security Blog. November 2014. URL: https://securityblog.switch.ch/2014/11/13/dnssec-signing-your-domain-with-bind-inline-signing/
[Ref.- 50]	"dnssec-keygen: DNSSEC key generation tool Manual Pages". ISC, Internet System Consortium. URL: https://ftp.isc.org/isc/bind9/cur/9.12/doc/arm/man.dnssec-keygen.html
[Ref.- 51]	"dnssec-settime: Manual Pages". ISC, Internet System Consortium. URL: https://ftp.isc.org/isc/bind9/cur/9.12/doc/arm/man.dnssec-settime.html
[Ref.- 52]	"Trece Agentes Registradores ya han implantado el protocolo de seguridad DNSSEC para dominios ".es"". Actualidad y noticias de dominios.es. Octubre 2015. URL: http://www.dominios.es/dominios/es/actualidad-y-noticias/comunicados/trece-agentes-registradores-ya-han-implantado-el-protocolo-de
[Ref.- 53]	"Registrars that support end user DNSSEC management, including entry of DS records". ICANN. April 2017. URL: https://www.icann.org/resources/pages/deployment-2012-02-25-en
[Ref.- 54]	"DNS Zone File Time Value Recommendations". Daniel Stirnimann (Switch Security Blog). February 2014. URL: https://securityblog.switch.ch/2014/02/06/zone-file-recommendations/
[Ref.- 55]	"PowerDNS". An OX Company. URL: https://www.powerdns.com
[Ref.- 56]	"DNSSEC Modes of Operation". PowerDNS docs. URL: https://doc.powerdns.com/authoritative/dnssec/modes-of-operation.html
[Ref.- 57]	"Instrucción mediante la que se regula la implantación del servicio de protocolo de seguridad DNSSEC para los nombres de dominio ".ES"". Red.es. Junio 2014. URL: http://www.dominios.es/dominios/sites/dominios/files/files/INSTRUCCION%20DNSSEC%20(firmada).pdf
[Ref.- 58]	"DNS/DNSSEC and Domain Transfers: Are they compatible?" Olafur Gudmundsson & Steve Crocker. Shinkuro inc. March 2010. URL: https://archive.icann.org/en/meetings/nairobi2010/bitcache/DNS_DNSSEC%20and%20Domain%20Transfers_%20Are%20They%20Compatible--vid=9321&disposition=attachment&op=download.pdf
[Ref.- 59]	"Choosing a DNNSEC Solution". Zytrax.open. 2006. URL: http://www.zytrax.com/books/dns/info/choose-dnssec.html
[Ref.- 60]	"RFC 3645: Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)". IETF. October 2003. URL: https://tools.ietf.org/html/rfc3645
[Ref.- 61]	"RFC 1035: Domain Names - Implementation and Specification". IETF. November 1987. URL: https://tools.ietf.org/html/rfc1035 "RFC 2136: Dynamic Updates in the Domain Name System (DNS UPDATE)". IETF. April 2017. URL: https://tools.ietf.org/html/rfc2136
[Ref.- 62]	"RFC 1996: A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)". IETF. August 1996. URL: https://tools.ietf.org/html/rfc1996
[Ref.- 63]	"ISC's DNSSEC Look-aside Validation Registry". ISC, Internet System Consortium. October 2017. URL: https://www.isc.org/downloads/bind/dlv/
[Ref.- 64]	"DNSSEC-Tools with Split-View Zones". URL: https://www.dnssec-tools.org URL: https://www.dnssec-tools.org/wiki/index.php?title=DNSSEC-Tools_with_Split-View_Zones

Referencia	Título, autor, fecha y enlace web
[Ref.- 65]	"ISC Blog: BIND". ISC, Internet System Consortium. URL: https://www.isc.org/blogs/category/bind/
[Ref.- 66]	"dnssec-keymgr: Manual pages". ISC, Internet System Consortium. URL: https://ftp.isc.org/isc/bind/9.11.0/doc/arm/man.dnssec-keymgr.html
[Ref.- 67]	"Knot DNS Resolver". URL: http://knot-resolver.readthedocs.io/en/stable/daemon.html#enabling-dnssec
[Ref.- 68]	"Nagios Open Source". URL: www.nagios.org URL: https://www.dnssec-tools.org/wiki/index.php?title=Nagios
[Ref.- 69]	"Automatic DNSSEC signing". Knot Documentation. URL: https://www.knot-dns.cz/docs/2.6/html/configuration.html#automatic-dnssec-signing
[Ref.- 70]	"Automatic KSK management". Knot Documentation. URL: https://www.knot-dns.cz/docs/2.6/html/configuration.html#automatic-ksk-management
[Ref.- 71]	"RFC 7344: Automating DNSSEC Delegation Trust Maintenance". IETF. September 2014. URL: https://tools.ietf.org/html/rfc7344 "RFC 8078: Managing DS Records from the Parent via CDS/CDNSKEY". IETF. March 2017. URL: https://tools.ietf.org/html/rfc8078
[Ref.- 72]	"CloudFlare Wants To Update DNS Registration Model To Automate DNSSEC". Internet Society Blog. February 2015. URL: https://www.internetsociety.org/blog/2015/02/cloudflare-wants-to-update-dns-registration-model-to-automate-dnssec/
[Ref.- 73]	"RFC 7646: Definition and Use of DNSSEC Negative Trust Anchors". IETF. September 2015. URL: https://tools.ietf.org/html/rfc7646
[Ref.- 74]	"BIND DNSSEC Guide". ISC, Internet System Consortium. 2017. URL: https://ftp.isc.org/isc/dnssec-guide/html/dnssec-guide.html URL: https://ftp.isc.org/isc/dnssec-guide/dnssec-guide.pdf
[Ref.- 75]	"Secure Domain Name System (DNS) Deployment Guide". SP800-81-2. NIST. September 2013. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf
[Ref.- 76]	"Key revocation system for DNSSEC". Gilles Guette. Universidad de Rennes. URL: https://pdfs.semanticscholar.org/146c/2eadaf72e91d066a8a13bcf8096591b00f66.pdf
[Ref.- 77]	"DNSSEC Algorithm Roll-over". Anand Buddhdev. Ripe NCC. November 2015. URL: https://labs.ripe.net/Members/anandb/dnssec-algorithm-roll-over



INSTITUTO NACIONAL DE CIBERSEGURIDAD