نشر امتدادات DNSSEC لنطاقات ccTLD

مكتب المسؤول الفني الأول في ICANN

يزيد أكانهو و بول موتشين
(Yazid Akanho & Paul Muchene)

OCTO-029
12 تشرين الثاني 2021

ICANN

قائمة المحتويات

هذه الوثيقة جزء من سلسلة وثائق مكتب كبير المسؤولين الفنيين (OCTO) في ICANN. يرجى الاطلاع على صفحة إصدارات مكتب المدير الفني المسؤول OCTO للاطلاع على قائمة الوثائق في سلسلة الإصدارات. إذا كانت لديكم أسئلة أو مقترحات حول أي مستند من هذه المستندات، فيرجى إرسالها إلى octo@icann.org.

تدعم هذه الوثيقة هدف ICANN الاستراتيجي المتمثل في تحسين مستوى المسؤولية المشتركة عن دعم أمن واستقرار نظام أسماء النطاقات (DNS) من خلال تعزيز تنسيق نظام اسم النطاق DNS بالشراكة مع أصحاب المصلحة المعنيين. يعد تعزيز أمن نظام أسماء النطاقات ونظام خادم الجذر (RSS) لنظام أسماء النطاقات جزءًا ضمن هدف ICANN الاستراتيجي.

1 مقدمة

زاد في السنوات الأخيرة تحول الأمن إلى قضية رئيسية بخصوص الإنترنت. فقد تم اقتراح وتطوير العديد من بروتوكولات الأمن المخصصة لنظام أسماء النطاقات (DNS)على مر السنين، وكانت الامتدادات الأمنية لنظام أسماء النطاقات (DNSSEC) واحدة من أهم البروتوكولات. حيث تساعد الامتدادات الأمنية لنظام أسماء النطاقات على تأمين استجابات نظام أسماء النطاقات عن طريق إضافة مصادقة منشأ البيانات وحماية سلامة البيانات.

أما منطقة جذر نظام أسماء النطاقات التي تديرها ICANN فقد تم توقيعها لأول مرة باستخدام الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC في يوليو/تموز 2010. وسوف تكون جميع نطاقات المستوى الأعلى العامة (gTLD) في وقت نشر هذا الدليل موقعة باستخدام الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC، ويرجع ذلك جزئيًا إلى الالتزامات التعاقدية المبرمة مع ICANN؛ ومن ناحية أخرى، تم توقيع حوالي 60% فقط من نطاقات المستوى الأعلى لرموز الدول (ccTLD). أحد الأسباب التي يمكن أن تفسر هذا التوجه على مستوى ccTLD هو قصر الرؤية من جانب مديري ccTLD حيال تأمين مناطقهم باستخدام DNSSEC.

لذلك نشر مكتب المسئول الفني الأول (OCTO) التابع لـ ICANN هذا الدليل لمساعدة مشغلي سجلات ccTLD على تولي زمام المسئولية الفعلية عن العملية التي يمكن أن تساعدهم على توقيع مناطقهم باستخدام الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC. علمًا بأن هذا الدليل لا يغطي الجانبَ الثاني من DNSSEC ألا وهو التحقق الذي يحدث بشكل أساسي على محللات DNS التكرارية الموجودة عادةً في مقرات مزودي خدمة الإنترنت (ISP)، أو في مشغلي السحابة العامة الكبيرة، أو في شبكات الشركات.

1.1 الجمهور المستهدف بهذه الوثيقة

يهدف هذا الدليل في المقام الأول إلى إعطاء مديري سجلات ccTLD والموظفين وأصحاب المصلحة وأمناء السجلات والمسجلين خاصة وأي شخص آخر نظرة عامة على الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC وكيف يمكن لأي سجل تنفيذها عند توقيع المنطقة. لا يتطرق هذا المستند إلى تفاصيل التكوين الفني؛ بل هو بمثابة دليل لفهم أساسي لبروتوكول DNSSEC والمتطلبات الأساسية واعتبارات النشر والاستخدام عند توقيع مناطق ccTLD.

حتى وإن كنت تقوم بالفعل بتشغيل نطاق TLD موقع ببروتوكول DNSSEC، يمكن لهذه الوثيقة أن تساعدك على تحديد العناصر التي يجب تحسينها، مثل أفضل الممارسات الخوارزمية الحالية أو التوثيق المناسب لخدمة DNS الشاملة. أما إذا كنت مشغل ccTLD، أو تدير مناطق قيد نطاق ccTLD موقع، فيمكن أن يساعدك هذا الدليل على الانطلاق. وعلى الرغم من أن جميع مشغلي gTLD وقعوا مناطقهم بالفعل، إلا أنه يمكنهم أيضًا جمع أفكار مختلفة حول أفضل الممارسات التشغيلية لبروتوكول DNSSEC الموضحة في هذا المستند واستخدامها معيارًا لزيادة مستوى الوعي ببروتوكول DNSSEC لفائدة أمناء سجلاتهم والمسجلين عندهم.

هناك عدد كبير من الوثائق التي تتناول الجوانب النظرية والتقنية والتشغيلية لـ DNSSEC، ويستشهد هذا الدليل بالعديد منها كمراجع. ولذلك، فإن القراء مدعوون لاستعراض هذه الوثائق المذكورة إذا كانوا يرغبون في تعميق معرفتهم أو فهمهم لأي من الجوانب الأخرى المتعلقة بـ DNSSEC.

2 امتدادات DNSSEC وقيمتها بالنسبة لنظام DNS

نظام أسماء النطاقات (DNS) عبارة عن نظام تسمية هرمي وموزع ولامركزي للإنترنت. فعلى غرار دليل الهاتف الذي يترجم الأسماء إلى أرقام هواتف، يساعد DNS على تحويل معلومات اسم النطاق إلى عناوين IP والعكس بالعكس. يعتبر DNS خدمة هامة على الإنترنت، ولكن لم يتم تصميمه في الأصل بآليات أمان قوية توفر تكاملاً ومصداقية لبياناته. فعلى مدار سنوات، تم اكتشاف عدد من نقاط الضعف التي تهدد موثوقية ومصداقية DNS، ويساعد DNSSEC في معالجة بعض منها.

لقد تم تعريف DNSSEC وتحديده بشكل أساسي في ثلاثة مستندات لمعايير الإنترنت، وهي: RFC 4033، *تعريف ومتطلبات أمان نظام أسماء النطاقات*؛ و RFC 4034، *سجلات الموارد لملحقات أمان نظام أسماء النطاقات*؛ إضافة إلى RFC 4035، *تعديلات بروتوكولية لملحقات أمان نظام أسماء النطاقات*. يستخدم DNSSEC تشفير المفتاح العام (بمعنى إنشاء أزواج المفاتيح العامة والخاصة) لإضافة مصادقة منشأ البيانات، وتكامل البيانات، والتوثيق، وقدرات الإنكار الموثق لوجود النطاقات إلى DNS. ويضيف على وجه التحديد التوقيعات الرقمية ومجموعة جديدة من أنواع سجلات الموارد وبيتات (علامات) عناوين الرسائل إلى DNS، والتي

يمكن استخدامها للتحقق من استجابات DNS من منطقة موقعة. ومن الجدير بالذكر أن DNSSEC لا تقوم بتشفير أي بيانات رسائل DNS وبالتالي فإنها لا توفر السرية.

وبمجرد توقيع النطاق باستخدام DNSSEC، يتم إنشاء التوقيعات الرقمية بواسطة مسؤول المنطقة باستخدام مفتاح خاص ويتم نشرها كسجل لتوقيع سجل الموارد (RRSIG) في ملف المنطقة كجزء من بيانات منطقة النطاق. وعندما يرسل محلل تكراري مزود بآليات الأمان، والمعروف أيضًا باسم محلل التحقق، استعلام DNS إلى خادم موثوق للنطاق الموقع، فإن استجابة DNS ستحتوي على سجل المورد بنص واضح أو بتنسيق غير مشفر والتوقيع الرقمي المرتبط به. ثم يستخدم المحلل التوقيع الرقمي الذي استلمه للتحقق من استجابة DNS هذه. لهذا الغرض، يطلب محلل التحقق أيضًا معلومات أخرى ذات صلة بامتدادات DNSSEC، مثل المفتاح العام الذي تم تخزينه في سجل DNSKEY ونشره مسؤول النطاق في بيانات المنطقة.

3 اشتراطات ومتطلبات نشر DNSSEC

3.1 توثيق النظام الحالي

نظرًا للدور الحاسم الذي يلعبه نظام أسماء النطاقات على الإنترنت والحاجة إلى منع انقطاع الخدمة في جميع الظروف، فمن المهم الحفاظ على وثائق حديثة تصف البنية التحتية لنظام أسماء النطاقات وعملياته. ومن ناحية أخرى، وتضيف امتدادات DNSSEC مستوى إضافيًا محددا من التعقيد إلى البنية التحتية والعمليات الخاصة بنظام أسماء النطاقات. لذلك، يعد الاحتفاظ بوثائق حديثة أمرًا بالغ الأهمية لضمان توفر صورة واضحة للنظام الحالي للرجوع إليها. يسمح هذا أيضًا بالاستمرارية التشغيلية في حالة تغير فريق العمل أو عمليات ترقية البنية التحتية.

ونوصي بأن تلخص الوثائق جانبين رئيسيين هما: سياسات الحوكمة الخاصة بنطاق ccTLD بالإضافة إلى الجوانب التشغيلية والفنية للخدمة.

علاوة على ذلك، يُنصح بأن يحتوي المستند على أقصى قدر ممكن من المعلومات، مع حذف أي بيانات حساسة أو سرية مثل أسماء المستخدمين وكلمات المرور التي يمكن استخدامها لشن هجمات ضد السجل.

يمكن أن تغطي جوانب الحوكمة في الوثيقة موضوعات مثل:

- النظرة العامة الشاملة لنطاق ccTLD وهيكله
- نموذج (نماذج) التسجيل: الثلاثي (السجل وأمين السجل والمسجل) أو الثنائي (السجل والمسجل فقط) أو نماذج أخرى
- جهات الاتصالات الفنية والإدارية لدى السجل
- الموارد البشرية والأدوار والمسؤوليات وجهات الاتصال بالأشخاص المشاركين في عملية صنع القرار الفني للسجل
- قائمة أمناء السجلات مع معلومات الاتصال الخاصة بهم

يمكن أن تغطي الجوانب الفنية والتشغيلية للوثيقة موضوعات مثل:

- عدد خوادم الأسماء الرسمية الأساسية والثانوية (NS) مع عناوين IP الخاصة بها، ومعلومات اتصال TLD (الهاتف وعناوين البريد الإلكتروني)، والبروتوكولات المستخدمة بين السجل وأمناء السجلات مثل بروتوكول التزويد المرن (EPP)، والبرامج والأجهزة المنفذة لوظائف التسجيل بما في ذلك، قاعدة بيانات التسجيل وبروتوكول الوصول إلى بيانات التسجيل (RDAP) و/أو خوادم WHOIS وغيرها من المعلومات التقنية الأخرى
- أن يكون وصول المستخدم وقائمة الامتيازات متاحان فقط وبشكل صارم لعدد محدود من الأشخاص المصرح لهم
- النسخ الاحتياطية وإجراءات الاستعادة
- الأمان: الوصول المادي وإدارة السجلات وضوابط الوصول وإدارة كلمات المرور وجدران الحماية وتكامل ملفات المنطقة وأمان نقل المنطقة على سبيل المثال لا الحصر.
- أنظمة المراقبة: الأجهزة والبرامج ومزامنة المنطقة (بين خوادم الاسم)
- استراتيجية الصيانة
- خطة استمرارية الأعمال والتعافي من الكوارث

3.2 تدقيق البنية التحتية الحالية

كما ذكرنا سابقًا، فإن نشر DNSSEC يضيف مستوى من التعقيد إلى البنية التحتية والعمليات الحالية لنظام أسماء النطاقات. لذلك، تتمثل الممارسة الجيدة والآمنة في إجراء تدقيق مقابل البنية التحتية للنظام الحالي والعمليات والإجراءات إما من خلال طرف خارجي أو داخلي ويتمتع بالمهارات والاستقلالية المطلوبة لتحديد وإعلان ما يتوصل إليه من نتائج وأي ثغرات. ومن الضروري إصلاح أي قصور في النظام الحالي قبل توقيع المنطقة أو بالتزامن معه. حيث يؤدي القيام بذلك إلى تقليل احتمالية عدم القدرة على إدارة الأمور بعد تنفيذ DNSSEC.

3.3 كتابة سياسة DNSSEC وبيانات الممارسة

3.3.1 ما هي سياسة DNSSEC وبيان ممارسات DNSSEC؟

هناك العديد من الاعتبارات التي يجب مراعاتها والمعلمات التي يجب تحديدها عند توقيع نطاق ما، مثل خوارزميات توقيع DNSSEC وأحجام المفاتيح وفترة صلاحية التوقيع ووتيرة تكرار تحديث التوقيع. ومن الممارسات الجيدة عند وجود منطقة بها عدد كبير من التفويضات إجراء توثيق كامل وتحديث مجموعات المعايير المطبقة على المنطقة والاستفادة منها بشكل عام. ولذلك تجب مراعاة مفهومين هنا:

- سياسة **الامتدادات الأمنية لنظام أسماء النطاقات (DP)**: تحدد متطلبات ومعايير الأمان التي سيتم تنفيذها لمنطقة موقعة باستخدام DNSSEC. تشكل سياسة الامتدادات الأمنية لنظام أسماء النطاقات (DP) أساسًا لتدقيق أو اعتماد أو تقييم أي كيان؛ كالسجل مثالاً. يمكن تقييم كل كيان مقابل سياسة DP واحدة أو أكثر يزعم تنفيذها. وباختصار، توضح سياسة DP ما يجب القيام به.
- **بيان تطبيق أو ممارسة الامتدادات الأمنية لنظام أسماء النطاقات** (أو DPS): هذه وثيقة إفصاح عن الممارسة التشغيلية التي يمكن أن تدعم أو تكون وثيقة تكميلية لسياسة DNSSEC (إن وجدت). وهي توضح - وعلى مستوى عالٍ - كيف يقوم مشغل المنطقة وشركاؤه في إدارة المنطقة إن وجدوا، بتنفيذ الإجراءات والضوابط اللازمة لتلبية متطلبات سياسة DP المعمول بها. وعلى العكس من سياسة DP، ينص بيان تطبيق الامتدادات الأمنية لنظام أسماء النطاقات DPS على ما يتم تنفيذه فعلياً.

حيث توفر سياسة DP مبادئ عامة بينما يقدم بيان تطبيق الامتدادات الأمنية لنظام أسماء النطاقات وصفًا للإجراءات والضوابط، مما يجعله أكثر تفصيلاً من سياسة DP. ومن ناحية أخرى، فإنه عادة ما يتم وضع السياسة من قبل السلطة المخولة بوضع السياسات (مثل مدير TLD أو الهيئة التنظيمية) وقد تكون قابلة للتطبيق على منطقة واحدة أو أكثر في التسلسل الهرمي لنظام أسماء النطاقات بينما تتم كتابة بيان التطبيق الخاص بمنطقة واحدة من قبل مشغل المنطقة الذي يصف كيف يفي بمتطلبات سياسة معينة أو مجموعة من السياسات.

على سبيل المثال، وفي السياق الذي تكون فيه كل من جهة الاتصال الإدارية وجهة الاتصال الفنية لنطاق ccTLD كيانات مختلفة، يمكن لجهة الاتصال الإدارية نشر سياسة تحدد المعايير والمتطلبات التي يجب اتباعها مع مطالبة جهة الاتصال الفنية أيضًا بنشر بيان تطبيق السياسة يوضح بالتفصيل الكيفية التي ستتم بها تلبية تلك المعايير والمتطلبات.

وعوضا عن ذلك، يجوز لمشغل أو مدير المنطقة الذي لا يخضع لأي سياسة خارجية نشر بيان ممارسة الامتدادات الأمنية لنظام أسماء النطاقات DPS.

ويعتبر نشر DPS أكثر صلة بالنسبة للكيانات التي تدير منطقة تحتوي على عدد كبير من التفويضات مثل نطاق مستوى أعلى TLD. ويساعد نشر بيان ممارسة أو تطبيق الامتدادات الأمنية لنظام أسماء النطاقات DPS على توفير مستوى من الشفافية يزيد من ثقة المجتمع بعمليات TLD ولكن كما ذكرنا سابقًا، يجب ألا يحتوي بيان DPS على معلومات تشغيلية حساسة.

RFC 6841، *إطار عمل لسياسات DNSSEC وبيانات تطبيق امتدادات DNSSEC*، هو مستند يوفر فهمًا عميقًا لقائمة شاملة من الموضوعات التي يجب على مشغل TLD مراعاتها عند تحديد كل من سياسة DP وبيان DPS على التوالي.

3.3.2 كيف تكتب سياسة DP وبيان DPS

تعد كتابة بيان DPS خطوة مهمة في رحلة توقيع أي نطاق من نطاقات ccTLD. ويمكن أن يكون بيان DPS قصيرًا وبسيطًا أو طويلاً ومعقدًا، ولكن يجب أن يساعد الناس على فهم إطار عمل عمليات DNSSEC وكيف يمكنهم الوثوق في عملية توقيع نطاق ccTLD.

الجدول التالي عبارة عن ملخص لمجموعة الأحكام التي تتكون من ثمانية مكونات تم توضيحها في وثيقة RFC 6841، والتي يمكن أخذها في الاعتبار عند صياغة سياسة DP أو بيان DPS. ليست كل المكونات في RFC 6841 إلزامية التنفيذ، وبالتالي فلك مطلق الحرية في اختيار تلك المكونات (الفرعية) المناسبة لاحتياجاتك.

العنوان	الوصف	المكونات الفرعية
مقدمة	يحدد ويقدم مجموعة الأحكام، ويشير إلى أنواع الكيانات والتطبيقات التي تستهدفها السياسة أو بيان تطبيق الامتدادات الأمنية.	• لمحة عامة • اسم الوثيقة وتحديد الهوية • المجتمع وقابلية التطبيق • إدارة المواصفات
النشر والمستودعات	يصف المتطلبات اللازمة لقيام أي كيان بنشر المعلومات المتعلقة بممارساته ومفاتيحه العامة والوضع الحالي لهذه المفاتيح جنبًا إلى جنب مع التفاصيل المتعلقة بالمستودعات التي يتم الاحتفاظ بالمعلومات فيها.	• المستودعات • نشر المفاتيح العمومية
متطلبات التشغيل	يصف المتطلبات التشغيلية عند تشغيل منطقة موقعة باستخدام DNSSEC.	• معنى أسماء النطاقات • تحديد ومصادقة مدير منطقة فرعية • تسجيل سجلات موارد سياسة DS • طرق إثبات حيازة وملكية مفتاح خاص • إزالة سجلات موارد سياسة DS
أنظمة وضوابط الموقع والإدارة والضوابط التشغيلية	يصف ضوابط الأمان غير الفنية، أي المادية والإجرائية والخاصة بفريق العمل من أجل أداء الوظائف ذات الصلة ببروتوكول DNSSEC بشكل آمن. وتشمل هذه الضوابط الوصول المادي وإدارة المفاتيح والتعافي من الكوارث والتدقيق والحفظ في الأرشيف. تعد ضوابط الأمان غير الفنية هذه ضرورية للثقة في تواقيع DNSSEC التي يتم انشائها.	• الضوابط المادية • الضوابط الإجرائية • ضوابط فريق العمل • إجراءات حفظ سجلات التدقيق • التعافي من حالات الاختراق والكوارث • إنهاء الكيان
ضوابط أمنية فنية	يحدد الإجراءات الأمنية المتخذة لإدارة مفاتيح التشفير وبيانات التنشيط، على سبيل المثال، أرقام PIN أو كلمات المرور أو مشاركات المفاتيح المحفوظة يدويًا ذات الصلة بعمليات DNSSEC.	• إنشاء زوج المفاتيح وتركيبه • حماية المفتاح الخاص والضوابط الهندسية لوحدة التشفير • بيانات التفعيل
توقيع المنطقة	يغطي جميع جوانب توقيع المنطقة، بما في ذلك مواصفات التشفير المحيطة بمفاتيح التوقيع ونظام التوقيع ومنهجية تبديل المفتاح وتوقيع المنطقة الفعلي. قد تعتمد المناطق التابعة والأطراف المعتمدة الأخرى على المعلومات الواردة في هذا القسم لفهم البيانات المتوقعة في المنطقة الموقعة وتحديد نمط سلوكها.	• أطوال المفاتيح وأنواعها والخوارزميات • إنكار الوجود الموثق • نسق التوقيع • تبديل المفتاح • عمر التوقيع ووتيرة إعادة التوقيع

تدقيق الامتثال	يصف كيفية إجراء عمليات التدقيق من قبل مشغل المنطقة وربما من قبل الكيانات المعنية الأخرى.	• وتيرة تدقيق امتثال الكيان • هوية/مؤهلات المدقق • الموضوعات التي يغطيها التدقيق • إجراءات ما بعد التدقيق
المسائل القانونية	يشير إلى الولاية القضائية أو المنطقة التي يتم تشغيل السجل فيها ويعطي إشارات إلى أي اتفاقيات سارية المفعول مرتبطة بها. يجوز لقسم الشؤون القانونية الإبلاغ عن أي تأثيرات محددة على حماية المعلومات الشخصية المحددة لهوية أصحابها.	• ذكر الاختصاص القضائي المعمول به • الالتزامات التعاقدية والامتثال للقوانين واللوائح الوطنية أو العابرة للحدود الوطنية أو الدولية • حماية البيانات والتعامل مع المعلومات الشخصية المحددة لهوية أصحابها

يمكن إضافة مكونات إضافية تحت إطار العمل هذا لمعالجة الاحتياجات الخاصة بنطاق ccTLD. توجد أمثلة لبيانات تطبيق امتدادات DNSSEC في الملحق "أ" المرفق بهذا الدليل.

3.3.3 اختيار خوارزميات التشفير للمنطقة

يتطور مجال التشفير بشكل مستمر. حيث تحل الخوارزميات الأحدث محل الخوارزميات الحالية متى ما يتبين أنها أقل أمانًا مما كان يعتقد سابقًا. لذلك، يتم تحديث متطلبات تنفيذ الخوارزمية وإرشادات الاستخدام بانتظام لتعكس الحقائق الجديدة.

كما يتطلب تنفيذ DNSSEC اختيار خوارزمية تشفير مناسبة. في وقت نشر هذا الدليل، تتناول وثيقة RFC 8624، *متطلبات تنفيذ الخوارزمية وإرشادات الاستخدام لـ DNSSEC*، كلاً من إرشادات تنفيذ الخوارزمية ومتطلبات معلمات التوقيع ذات الصلة ببروتوكول DNSSEC.

ويسرد الجدول التالي بعض التوصيات (غير المفصّلة) المستمدة من وثيقة RFC 8624. وقد يكون للمشغلين الفرديين متطلبات محددة وقد يرغبون بتعديلها وفقًا لذلك.

العنصر	**التوصية**
خوارزمية DNSKEY	توفر **الخوارزمية 13 (ECDSAP256SHA256)** قوة تشفير ويوصى بها حاليًا للاستخدام في عمليات نشر DNSSEC الجديدة نظرًا لقصر مفاتيحها وحجم التوقيع، مما ينتج عنه حزم DNS أصغر. ومع ذلك، يمكن أيضًا استخدام **الخوارزمية 8 (RSASHA256)** لأنها منتشرة على نطاق واسع كما أنها كانت الخوارزمية الافتراضية لعدة سنوات بسبب قوتها التشفيرية.
خوارزميات موقّع التفويض (DS)	تستخدم خوارزمية التجزئة الآمنة SHA-256 على نطاق واسع وهي عبارة عن خوارزمية تجزئة قوية، وبالتالي فهي موصى بها في عمليات النشر الجديدة والحالية لموقّع التفويض.
خوارزمية أمان DNSSEC (تتكون من خوارزمية التشفير وخوارزمية التجزئة)	التوصية الحالية هي الخوارزمية 13 (ECDSAP256SHA256). ويمكن أيضًا استخدام الخوارزمية 8 (RSASHA256) عوضا عن ذلك.
حجم مفتاح توقيع المنطقة (ZSK) ومفتاح التوقيع الرئيسي (KSK)	ستقوم الخوارزمية 13 (ECDSAP256SHA256) دائمًا بإنشاء مفاتيح ذات 256 بت.

	يمكن تعيين حجم مفتاح الخوارزمية 8 (RSASHA256) بين 2048 وبين 4096 بت.
فترة فاعلية مفتاح توقيع المنطقة ومفتاح التوقيع الرئيسي	لا توجد طريقة جيدة لتقدير احتياجات الفرد حيث يقوم المشغلون بضبط فترات الفاعلية الرئيسية بناءً على تجاربهم السابقة. ويستخدم العديد من المشغلين مفتاح ZSK لمدة من شهر إلى ثلاثة أشهر ومفتاح KSK لمدة تتراوح ما بين عام إلى خمس سنوات قبل إجراء عملية تبديله.
تخزين المفتاح الخاص	الأجهزة غير المتصلة بالإنترنت وغير المتصلة بالشبكة والآمنة ماديًا مثل وحدات أمان الأجهزة (HSM)

ملاحظة: ستعمل المفاتيح الأكبر حجمًا على زيادة أحجام سجلات RRSIG وDNSKEY وبالتالي ستزيد من فرصة زيادة تدفق حزمة DNS UDP. علاوة على ذلك، يزداد الوقت الذي يستغرقه التحقق من صحة وإنشاء توقيعات سجل الموارد (RRSIGs) مع المفاتيح الأكبر حجمًا، لذا تجنب زيادة أحجام المفاتيح بلا ضرورة.

3.3.4 إنكار وجود النطاق: NSEC أو NSEC3

إن إنكار الوجود أو إثبات عدم وجود شيء ما هو آلية تخبر المحلل أن اسم نطاق معين غير موجود (NXDOMAIN). وعلى النقيض من ذلك، يوجد اسم نطاق ولكنه لا يمتلك سجل المورد المحدد (NODATA) المطلوب. يستخدم الإنكار المصادق عليه للوجود عملية التشفير للتوقيع على استجابة سلبية. يتم تحقيق ذلك في DNSSEC باستخدام NSEC (أو Next Secure) أو NSEC3 (أو Next Secure v3)، على التوالي.

يستخدم NSEC لوصف الفاصل الزمني بين الأسماء. وهو يخبر المحلل بشكل غير مباشر بالأسماء غير الموجودة في منطقة من خلال تقديم الاسم قبله والاسم الذي يليه حسب الترتيب الأساسي. تشكل هذه الآلية المطبقة في NSEC الأساس وراء الرفض المصدق لوجود نطاق ما في DNSSEC وتواجه مشكلتين هما:

- أن سجلات NSEC عرضة للهجوم على محتويات المنطقة، وهذا الضعف يمكن أن يسمح للمهاجمين باجتياز جميع الأسماء في المنطقة المعنية. ولذلك فمن الممكن إعادة بناء المنطقة بأكملها، وبالتالي هزيمة أي محاولات لمنع عمليات نقل المنطقة إداريًا.

- المشكلة الثانية التي تواجه NSEC في منطقة مرتكزة على التفويض مثل نطاق المستوى الأعلى TLD، هي أن كل اسم في تلك المنطقة يحصل على سجل NSEC وRRSIG المرتبط به. وبمجرد التوقيع على المنطقة، يؤدي هذا إلى زيادة حجمها عكسياً. ويمكن أن تؤثر النفقات العامة الناتجة عن هذه الزيادة سلباً على أداء خوادم DNS الرسمية مثل تقييد موارد تخزين الأجهزة أو إطالة مدة إجراء عمليات نقل المعلومات في ملف المنطقة.

على العكس من ذلك، يخفف NSEC3 مشكلة الهجوم على محتويات المنطقة في NSEC، وذلك من خلال تجزئة أسماء النطاقات مع إمكانية تقويتها باستخدام ميزة salt. علاوة على ذلك، بفضل ميزة معينة تسمى "إلغاء الاشتراك"، لا تتطلب أسماء النطاقات غير الموقعة المفوضة في منطقة (التفويضات غير الآمنة) سجل NSEC3. وهذا يعني أنه عند تنشيط ميزة إلغاء الاشتراك في منطقة نطاق المستوى الأعلى TLD، فلا يمكن لـ NSEC3 إثبات أو نفي وجود النطاقات غير الموقعة المسجلة ضمن نطاق TLD هذا. ومع ذلك، فإن أحد المخاطر التي أظهرها NSEC3 هو أن استجابات DNS أكبر من استجابات NSEC تلك.

فليست هناك إجابة واحدة مناسبة عندما يتعلق الأمر بالاختيار بين NSEC وNSEC3. إذا فضل المرء استخدام NSEC3 لمنع الهجوم على محتويات المنطقة، فمن المستحسن عمومًا تنفيذ NSEC3 بدون تكرارات إضافية و'salt' فارغ. ومع ذلك، بالنسبة للمناطق الأصغر، فإنه لا يوصى باستخدام سجلات NSEC3 القائمة على إلغاء الاشتراك. وبالنسبة للمناطق الكبيرة جدًا والمتفرقة، والتي تكون فيها غالبية السجلات عبارة عن تفويضات غير آمنة، يمكن استخدام ميزة إلغاء الاشتراك بسجل NSEC3. بخلاف هذه الاعتبارات المذكورة أعلاه، فإنه من الأسهل استكشاف أخطاء NSEC وإصلاحها مما هو عليه الحال مع NSEC3.

3.4 مشاركة أمين السجل

يوصى بشدة إشراك أمناء السجلات في المراحل الأولية لتوقيع نطاق ccTLD. ليس فقط لأنهم الوسيط بين السجل والمسجلين، ولكن نشر امتدادات DNSSEC على مستوى ccTLD هو نقطة البداية لتأمين فضاء اسم ccTLD. وبمجرد توقيع ccTLD، يمكن لأصحاب نطاقات المستوى الثاني البدء بتأمين نطاقاتهم الخاصة. وسيتطلب ذلك من أمناء السجلات أن يكونوا قادرين على جمع وإرسال نوع جديد من السجلات من أصحاب نطاق المستوى الثاني أو مستوى لاحق إلى السجل. يسمى هذا النوع الجديد من السجلات مُوقِّع التفويض (DS).

ومن الناحية الفنية، فإن مُوقِّع التفويض عبارة عن تجزئة لمفتاح توقيع شفرة الدخول الأساسية (KSK) ويساعد على إنشاء سلسلة ثقة بين المنطقة الأم ومنطقة فرعية في فضاء الاسم لنظام DNS. يؤدي وجود سجل مُوقِّع التفويض في المنطقة الأم إلى إنشاء ارتباط آمن يجب على المهاجم الخارجي التغلب عليه لتزوير مادة أساسية في المنطقة الفرعية.

وعادةً ما يشارك نطاق ccTLD سجلَّ مُوقِّع التفويض الخاص به مع هيئة الإنترنت للأرقام المخصصة (IANA) للنشر في منطقة الجذر. ويشارك المسجلون والمسؤولون عن أسماء النطاقات ضمن نطاق ccTLD سجلات مُوقِّع التفويض الخاصة بهم مع نطاق ccTLD مباشرة أو عبر أمين السجل. ويؤدي أمناء السجلات دورين مهمين هنا:

- **توفير واجهة أو آلية آمنة وموثوقة لجمع سجلات مُوقِّع التفويض** من المسجلين؛ إذا كانت هذه الواجهة أو الآلية ليست موجودة بعد، فإن أمناء السجلات المستعدين لتقديم دعم DNSSEC للمسجلين لديهم يجب أن يعملوا في أقرب وقت ممكن على تنفيذها. ولا توجد طريقة موحدة لنقل سجل مُوقِّع التفويض بين العميل وأمين السجل. لأمناء السجلات المختلفين آليات مختلفة، بدءًا من واجهات الويب البسيطة إلى واجهات برمجة التطبيقات المختلفة.
- **دفع مُوقِّع التفويض إلى السجل**. يوصى بالحل التلقائي لنشر مُوقِّع التفويض في المنطقة الأصلية بدلاً من التدخل اليدوي. ففي نموذج السجل وأمين السجل، من الممكن استخدام امتدادات DNSSEC إلى بروتوكول التزويد المرن (EPP) لنقل مجموعات سجلات موارد مُوقِّع التفويض (مجموعات السجلات الآمنة) ومجموعات السجلات الآمنة لـ DNSKEY اختياريًا. وفي جميع الحالات، يجب إجراء الاختبارات بين مشغل ccTLD وأمناء السجلات للتأكد من أن المعاملات الجديدة ممكنة باستخدام البنية التحتية القائمة.

آلية أخرى تستخدمها المنطقة الفرعية في إدارة مُوقِّع التفويض تلقائيًا مع منطقتها الأم ألا وهي استخدام CDS (مُوقِّع التفويض الفرعي) أو مجموعة سجل موارد CDNSKEY (أو DNSKEY فرعي) إذا كان لدى المنطقة الأم سياسة قبول لهذه السجلات. ويمكن استخدامها في حالات الاستخدام الثلاث التالية:

- إصدار أولي لمُوقِّع التفويض
- تبديل المفتاح
- العودة إلى حالة عدم الأمان

وببساطة، فإن CDS/CDNSKEY عبارة عن تعليمات إلى المنطقة الأم لتعديل مجموعة السجلات الآمنة لمورد مُوقِّع التفويض في حالة اختلاف CDS/CDNSKEY ومُوقِّع التفويض. RFC 8078، *إدارة سجلات DS من المناطق الأم عبر CDS/CDNSKey* يشرح بالتفصيل الإدارة الآلية لسجلات مُوقِّع التفويض بين المنطقة الفرعية والمنطقة الأم.

وأخيرًا، فإن إشراك أمناء السجلات في وقت مبكر من العملية يسمح لهم أيضًا بالاستفادة من تدريبات DNSSEC والبرامج العملية التي تقدمها ICANN وشركاؤها داخل مجتمع الإنترنت.

4 الجدول الزمني

لا توجد جداول زمنية محددة لنشر DNSSEC. حيث يمكن أن تتراوح المدة من بضعة أسابيع إلى أشهر أو سنوات حسب عدة عوامل. ومع ذلك، ضع في اعتبارك الاقتراحات التالية لتجنب التأخيرات الطويلة:

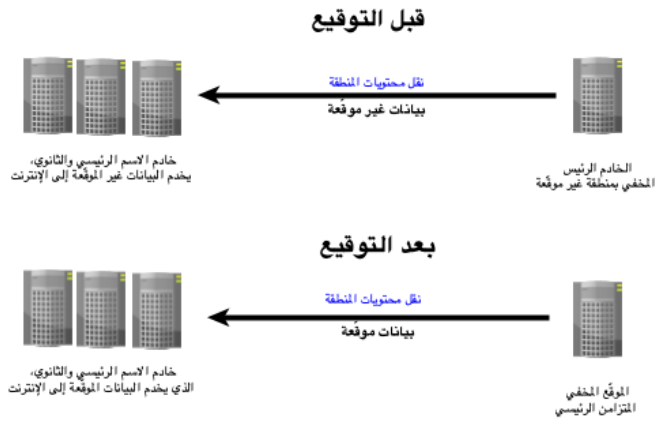
- حدد العملية في صورة مشروع بتاريخ بدء واضح وتاريخ انتهاء متوقع ومراحل تنفيذ يجب الوصول إليها. بالإضافة إلى ذلك، قم بتعيين مدير مشروع أو قائد تقني بالموارد المناسبة
- حدد وأدر وتعامل مع أصحاب المصلحة، بما في ذلك على سبيل المثال لا الحصر، المنظم (المنظمون) وأمناء السجلات والأطراف الفنية والإدارية والمقاولين ومشغل (مشغلو) الواجهة الخلفية أو أي طرف آخر. يجب أيضًا معالجة الاتصال بين مختلف أصحاب المصلحة في ccTLD
- تحديد وإدارة المخاطر بشكل صحيح

5 سيناريوهات نشر DNSSEC

سواء قررت إدارة المنطقة باستخدام الموارد والبنية التحتية الخاصة بك فقط أو من خلال التعاقد مع مقاول مثل مشغل الواجهة الخلفية، فمن المحتمل أن تتبع بنية النشر التقنية أحد السيناريوهين الرئيسيين الموصوفين هنا.

5.1 خادم أساسي للتوقيع المباشر (أساسي مخفي)

في سيناريو التكوين هذا، يقدّم خادم الاسم الأساسي المخفي -غير المعروف عادةً للإنترنت- المنطقة لمجموعة من الخوادم الموثوقة لنظام أسماء النطاقات، ويكون ذلك عادةً إلى خادم أساسي عام واحد وعدد من الخوادم الثانوية. لا يعد خادم الاسم الأساسي المخفي مطلبًا محددًا لـ DNSSEC، بل هو أفضل ممارسة لعملية DNS تقترح وجود خادم اسم رسمي خارج المجموعة ولا يمكن الوصول إليه وأنه غير معروف للجمهور، حيث يمكن إجراء جميع تحديثات المنطقة. يجب أن يقوم هذا الخادم أيضًا بتنفيذ إجراءات أمنية وتدقيق أكثر إحكامًا. ويشبه التركيب الهندسي الشكل أدناه:

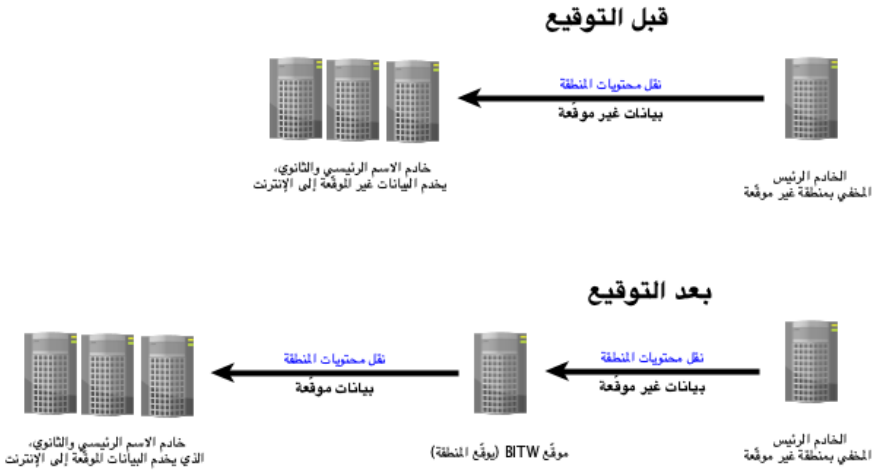


سيتم إعداد هذا الخادم الأساسي المخفي للتعرف على المفاتيح التي تم إنشاؤها، واستخدامها لإنشاء منطقة موقعة وتشغيلها، باتباع العملية التي يوفرها برنامج DNS الذي يتم تشغيله. وعند الانتهاء، سيتم نقل النسخة الموقعة من ملف المنطقة والاحتفاظ بها متزامنة مع جميع خوادم الأسماء الرسمية المرئية للعموم.

باستثناء تغييرات التكوين في خادم الاسم الأساسي المخفي، لا توجد تغييرات إضافية في التكوين أو البرنامج لإجراء هذه البنية.

5.2 التوقيع المتزامن الذي يطلق عليه توقيع "نتوءات في السلك" (BITW)

في سيناريو التكوين هذا، يتم إدخال خادم اسم جديد، المُوقّع، في البنية الحالية، ويتم وضعه بين الخادم الأساسي المخفي وخوادم الأسماء العامة التي تخدم المنطقة على الإنترنت. يعمل هذا الخادم الجديد كجهاز bump-in-the-wire (BITW). يأخذ ملف المنطقة غير الموقعة من الملف الأساسي المخفي، ويوقع البيانات ويرسل ملف المنطقة الموقّع لتوزيعه على خوادم الأسماء العامة للنطاق.



لتحقيق ذلك، يمكن النظر في الخطوات التالية:

1. يجب ألا يتم سرد الأساس المخفي في مجموعة RR الخاصة بخادم الأسماء (NS) للنطاق لتجنب الحصول على إجابات متضاربة، مثل الإجابات غير الموقعة من الإجابات الأولية المخفية والإجابات الموقعة من خوادم الأسماء الأخرى.
2. يجب تحديث تكوين الخادم الأساسي المخفي للسماح للموقِّع فقط بتنفيذ عملية نقل المنطقة.
3. يستخدم الموقّع ملف المنطقة غير الموقعة الذي تم استلامه من الخادم الأساسي المخفي ومفتاح خاص للتوقيع على سجلات الموارد. وفي النهاية، يوزع ملف المنطقة الموقعة على خوادم الأسماء الأولية والثانوية باستخدام آليات نقل المنطقة.
4. يجب أيضًا تحديث تكوين خوادم الأسماء وفقًا لذلك لتلقي نقل المنطقة فقط من الموقّع.

بغض النظر عن سيناريو النشر، يُنصح بالتحقق من المنطقة الموقعة قبل توزيعها على جميع الخوادم. يمكن إجراء تمرين التحقق هذا على اسم النطاق باستخدام أدوات عبر الإنترنت مثل تلك الموضحة في القسم 10 من هذا المستند. من الممارسات الجيدة أيضًا تشغيل العديد من الاستعلامات التي تبحث عن توقيعات سجل مورد DNSSEC وتواريخ انتهاء صلاحية التوقيع، من بين معلمات أخرى في كل منطقة من المناطق التي تتم إدارتها. قم بتضمين عمليات التشغيل التجريبية هذه كجزء من التحقق من صحة تنفيذك لها.

فلنقارن باختصار خطوات سلسلة إنتاج المنطقة بين DNS العادي والآخر مع خطوات DNSSEC:

- DNS عادي: إنشاء ← تحقق ← نشر ← مراقبة
- مع DNSSEC إنشاء ← تحقق ← تسجيل ← تحقق ← نشر ← مراقبة

6 توقيع نطاق TLD

يُوصى بشدة، كما هو الحال مع أي تغيير رئيسي آخر، بإجراء مرحلة اختبار عميق قبل التخطيط لدمج هذا في نظام الإنتاج. وهذا أكثر أهمية في حالة DNSSEC، لأنه يتم إدخال تغييرات جديدة في المنطقة. تقدم الخطوات الموضحة أدناه نظرة عامة شاملة على توقيع منطقة TLD، ولكن قد تحتاج إلى تعديلها بناءً على بيئتك والمتطلبات الخاصة بك.
في بعض الحالات، قد يكون التوقيع على ملف المنطقة كله مرة واحدة غير مناسب بالنسبة لنطاقات ccTLD الكبيرة؛ وسيكون من الأكثر أمانًا إنشاء نهج تدريجي لتوقيع المنطقة عوضا عن ذلك. قد تختار نطاقات ccTLD الأخرى أيضًا توقيع منطقة فرعية على وجه الاختبار أولاً، قبل إضافة سجل DS في المنطقة الأم. هذا اختبار تحضيري قبل التوقيع على منطقة ccTLD الفعلية.

على أي حال، ولإكمال عملية التوقيع بنجاح، سيكون من الحكمة المضي قدمًا بحذر من خلال اعتماد خطط نشر واختبار مناسبة مصحوبة بمنهجية تحقق صارمة.

1. نشر وتكوين بيئة اختبار DNSSEC. حسب نموذج النشر، يمكن أن يحتوي الاختبار على العناصر التالية:

- خادم توقيع تجريبي واحد، خادم أسماء (اختبار NS)، قادر على توقيع ملف منطقة. يجب أن يكون الخادم قادرًا إما على إنشاء مفاتيح التوقيع أو استلام المفاتيح التي تم إنشاؤها من خادم مختلف أو من وحدة أمان الأجهزة (HSM)، وتوقيع المنطقة وتوزيع ملف المنطقة الموقع بين وظائف أخرى.
- سيتلقى خادم اسم موثوق ثانوي تجريبي واحد المنطقة الموقعة ويخدمها.
- يجب تكوين محلل اختبار واحد لإجراء عمليات التحقق من DNSSEC محليًا بالنسبة للمنطقة الموقعة.

2. انسخ ملف المنطقة غير الموقعة من الخادم الأساسي المخفي إلى خادم التوقيع التجريبي. يمكن أتمتة توزيع ملف المنطقة غير الموقعة على نظام التوقيع التجريبي لاحقًا في مرحلة الاختبار.
3. إنشاء مفاتيح KSK وZSK. يوصى بإنشاء المفاتيح خارج نظام التوقيع. تخزين KSK على HSM خارج نطاق شبكة الإنترنت واستخدامه فقط للتوقيع على سجلات موارد DNSKEY.
4. توقيع المنطقة ونشرها على خادم (خوادم) الاسم الثانوي التجريبي.
5. إنشاء واستيراد DS كمفاتيح موثوقة في محلل الاختبار. لن يتم في أرض الواقع توزيع DS على المحلل التكراري حول العالم مباشرة بواسطة مسؤولي TLD؛ بل سيتم إرسالها إلى IANA لنشرها في منطقة الجذر. سيقوم أي محلل تكراري للتحقق من صحة البيانات حول العالم بإحضار DS المطابق لـ TLD هذا من منطقة الجذر.
6. إجراء بعض الاختبارات عن طريق إجراء اختبار قبول المستخدم (UAT) بناءً على حالات الاختبار المحددة. يجب أن تغطي الاختبارات موضوعات مثل استرداد المفاتيح والتوقيعات، والتحقق من انتهاء صلاحية التوقيعات، ووقت الاستجابة على الاستعلام، والحجم. إجراء تحقق DNSSEC إضافة إلى مهام أخرى.
7. إذا كانت عملية توقيع الاختبار مؤتمتة، فاحرص على مراقبة انتهاء صلاحية التوقيع والإنشاء التلقائي للتوقيعات الجديدة. وإذا لم يكن ذلك ممكناً، فيجب إجراء عمليات التبديل يدوياً إلى أن يصبح من الممكن إجراء عملية توقيع الاختبار تلقائيًا.
8. إجراء تبديل مفاتيح ZSK وKSK. إنشاء سياسة DS جديدة، بالنسبة إلى تبديل مفتاح KSK، ومحاكاة المشاركة مع المنطقة الأصلية عن طريق إضافتها إلى محلل الاختبار للتحقق المحلي من الصحة. اعتمادًا على معلمات التوقيت المختلفة مثل فترة فاعلية المفتاح في بيئة الاختبار، ستحتاج إلى إزالة DS القديم من المحلل التجريبي وKSK القديم من المنطقة لإكمال استبدال مفتاح KSK.
9. إجراء اختبارات جديدة بشكل متكرر وتهذيب الخطوات من 1 إلى 8.
10. بمجرد أن تثق بمنهجية الاختبار، ركز على البث المباشر واختيار البيئة المناسبة وسيناريو النشر الذي تختاره: BITW أو توقيع داخلي أساسي مخفي. قم بإجراء اختبار جديد لقبول المستخدم UAT للتأكد من أن جميع خوادم الأسماء المعتمدة للنطاق تخدم المنطقة وسجلات موارد DNSSEC المقابلة لها بشكل صحيح.
11. أخيرًا، انشر DS إلى منطقة الجذر باتباع إرشادات إدارة التفويض لنطاقات TLD على النحو المحدد من قبل IANA على https://www.iana.org/domains/root/manage. وبمجرد إضافة ccTLD إلى منطقة الجذر، فإنه يعلن للعالم أنه موقّع بامتدادات DNSSEC وأن أي محلل مدرك للأمان يجب أن يقوم بالتحقق من DNSSEC مقابل سجلات DNS التي تنشأ من تلك المنطقة. ويوصى بشدة باستخدام أداة مثل https://dnsviz.net/ (انظر القسم 10 لمزيد من التفاصيل) للتحقق من صحة سلسلة ثقة DNSSEC للمنطقة.
12. بمجرد توقيع ccTLD رسميًا، خطط لفتح الوصول لأمناء السجلات لنشر سجلات DS الخاصة بالمسجلين في السجل حتى تكون سلسلة الثقة فعالة.

7 تبديل المفتاح والخوارزمية

عندما يتم تأمين منطقة ما باستخدام DNSSEC، يجب أن يكون مدير المنطقة مستعدًا لاستبدال (أو "تبديل") المفاتيح المستخدمة لتأمين المنطقة، سواء تم ذلك بشكل دوري لأغراض أمنية أو لمخاوف تشغيلية أو في حالة الطوارئ. ولتنفيذ تبديل مفتاح أو خوارزمية، يجب إدخال مفاتيح جديدة وإلغاء المفاتيح القديمة من المنطقة. ومن الأهمية بمكان مراعاة كون البيانات المنشورة لمنطقة ما موجودة في ذاكرات التخزين المؤقت مختلفة لوحدات الحل. قد يؤدي تجاهل البيانات التي قد تكون في ذاكرات التخزين المؤقت إلى فقدان الخدمة بالنسبة للعملاء. خذ على سبيل المثال بيانات المنطقة الموقعة بمفتاح قديم، والتي يتم التحقق من صحتها بواسطة محلل لا يحتوي على مفتاح المنطقة القديم في ذاكرة التخزين المؤقت الخاصة به. في حال لم يعد المفتاح القديم موجودًا في المنطقة الحالية، فستفشل عملية التحقق وسيتم وضع علامة على بيانات المنطقة المقابلة على أنها زائفة.

من ناحية أخرى، فإن المحلل الذي يحاول التحقق من صحة البيانات التي تم توقيعها بمفتاح جديد، بينما لا يزال المفتاح القديم موجودًا في ذاكرة التخزين المؤقت لوحدة الحل، يؤدي أيضًا إلى وضع علامة على البيانات على أنها زائفة. توجد أنواع مختلفة من تقنيات تبديل المفاتيح والخوارزميات مثل تلك الموضحة في وثيقة RFC 6781 والممارسات التشغيلية لـ DNSSEC - الإصدار 2 بالإضافة إلى RFC 7583، وهيي اعتبارات توقيت تبديل مفتاح DNSSEC. ومن الأمثلة على هذه الأساليب: النشر المسبق و الاستبدال المزدوج لمفتاح ZSK RRSIG وdouble-KSK وdouble-DS وdouble-RRset على سبيل المثال لا الحصر.

في الحالة المحددة التي يكون فيها التبديل الطارئ للمفتاح مطلوبًا بسبب الاشتباه في تعرض زوج مفاتيح ZSK أو KSK للاختراق، فمن المستحسن أن يكون لديك بالفعل إجراء موثق.

7.1 تبديل مفتاح الدخول لمنطقة الجذر ZSK

أثناء تبديل ZSK، من الضروري التأكد من أن أي مدقق للتخزين المؤقت لديه حق الوصول إلى توقيع معين ولديه أيضا حق الوصول إلى ZSK الصالح المقابل. يوثق RFC 6781، تحت عنوان *ممارسات تشغيل DNSSEC، الإصدار 2* ثلاث طرق لإجراء تبديل مفتاح ZSK: النشر المسبق والتوقيع المزدوج وRRSIG المزدوج.

وسنصف في هذا المستند طريقة النشر المسبق فقط، حيث إنها تحافظ على المنطقة وأحجام الاستجابة عند الحد الأدنى أثناء عملية التبديل كلها. في هذه الطريقة، يتم إدخال ZSK الجديد في مجموعة DNSKEY RR وبعد انقضاء الوقت الكافي للتأكد من احتواء أي مجموعات DNSKEY RR المخزنة مؤقتًا على كل من المفتاحين. ثم يتم توقيع المنطقة باستخدام مفتاح ZSK الجديد وتتم إزالة التواقيع القديمة. وأخيرًا، عند انتهاء صلاحية جميع التواقيع التي تم إنشاؤها باستخدام ZSK القديم من ذاكرات التخزين المؤقت، تتم إزالة المفتاح القديم. تصف الخطوات أدناه العملية.

1. يتم إدخال ZSK A الجديد في المنطقة ويظهر في مجموعة DNSKEY RR، ولكن لن يتم استخدامه بعد لتوقيع السجلات في المنطقة. يقوم مفتاح KSK الحالي الفاعل بإقالة مجموعة DNSKEY RR، والتي يتم إعادة توقيعها بعد ذلك باستخدام KSKs النشطة حاليًا. في هذه المرحلة، يُقال أنه سيتم نشر ZSK الجديد.
2. بعد فترة زمنية معينة، يصبح ZSK A جاهزًا لتوقيع السجلات في المنطقة. تتوافق هذه الفترة مع تأخير انتشار المنطقة بالإضافة إلى وقت البقاء لسجلات DNSKEY في المنطقة. بمعنى آخر، هذا هو الحد الأقصى للوقت الذي تستغرقه سجلات DNSKEY الحالية لتنتهي صلاحيتها في ذاكرات التخزين المؤقت. ويصبح ZSK A مفعلاً ويبدأ بشكل فعال بتوقيع السجلات الخاصة بالمنطقة.
3. سيستمر ZSK A في التوقيع وتحديث السجلات للمنطقة حتى يحين وقت يلزم فيه نشر ZSK B جديد. يعتمد وقت نشر المفتاح B على وقت تنشيط المفتاح A وعمر ZSK المحدد للمنطقة في سياسة إدارة المفاتيح. ويستعد ZSK B ويمكن استخدامه لتوقيع السجلات، لكن ZSK A لا يزال فاعلاً.
4. عندما يتم الوصول إلى نهاية الفترة المحددة لـ ZSK للمفتاح A، يتم إيقافه. يصبح المفتاح B مُفعّلاً ويستخدم لتوقيع المنطقة. ومع ذلك، يجب الاحتفاظ بالمفتاح المنتهي الصلاحية في المنطقة لبعض الوقت (لـ "فترة تقاعد") للسماح بإنشاء RRSIG باستخدام هذا المفتاح لمواصلة التحقق من صحته من قبل المحللات. يتوافق الفاصل الزمني للتقاعد مع الوقت اللازم لإعادة توقيع جميع مجموعات RR الموجودة بالمفتاح B، بالإضافة إلى تأخير انتشار المنطقة، والحد الأقصى لـ TTL لجميع RRSIG الذي تم إنشاؤها باستخدام المفتاح القديم في المنطقة.
5. بعد فترة زمنية معينة، تختفي التواقيع التي تم إنشاؤها باستخدام المفتاح المتقاعد من ذاكرة التخزين المؤقت لوحدة الحل، ويُقال إن المفتاح القديم قد مات.
6. بمجرد أن يصبح المفتاح القديم ميتًا، يمكن إزالته من مجموعة DNSKEY RR، والتي يجب إعادة توقيعها باستخدام مفاتيح KSK للمنطقة الحالية. في هذه المرحلة، يتم الإعلان عن إزالة المفتاح A.
7. بعد مرور بعض الوقت، سيتم نشر مفتاح جديد، وستتكرر العملية برمتها.

7.2 تبديل مفتاح KSK

يكمن التحدي الرئيسي أثناء استبدال مفتاح KSK في ضمان وجود مفتاح KSK للمنطقة يوثق به في جميع الأوقات حتى أثناء عملية استبدال المفتاح. يوثق RFC 6781 أيضا، تحت عنوان *ممارسات تشغيل DNSSEC، الإصدار 2* ثلاث طرق لإجراء استبدال KSK: وهي KSK المزدوج وDS المزدوج وRRset المزدوج. تعد طريقة RRset المزدوج أكثرها كفاءة، حيث تنتشر سجلات DS الجديدة ومجموعات DNSKEY RR في آن واحد.

في هذه الطريقة، يتم نشر سجلات DNSKEY وDS الجديدة في نفس الوقت في المناطق المناسبة. وبمجرد انقضاء الوقت الكافي لانتهاء صلاحية مجموعتي DNSKEY ومجموعات RR لـ DS القديمتين من ذاكرات التخزين المؤقت، تتم إزالتهما من المناطق الخاصة بهما. يتم وصف خطوات التبديل على النحو التالي:

1. سجلات DS وDNSKEY موجودة في مناطقها الخاصة. KSK A المعني مُفعّل ويؤمّن المنطقة.
2. بمجرد اقتراب نهاية عمر KSK A الحالي، يتم إدخال KSK B جديد في المنطقة واستخدامه للتوقيع على مجموعة DNSKEY RR. يتم إرسال DS الخاص بـ KSK B إلى الأصل للنشر في المنطقة الأصلية.

3. يمكن للمنطقة الأم المضي قدمًا في التحقق من DS الجديد ثم نشره فيها.
4. بعد مرور فترة زمنية، يتم بالفعل نشر DS أو DNSKEY الجديد في ذاكرات التخزين المؤقت لمحللات التحقق من الصحة. وتتم في نفس الوقت إزالة ZSK A من المنطقة.
5. تتم لاحقًا إزالة سجلات DS وDNSKEY المرتبطة بـ ZSK A.
6. بعد فترة من الوقت، سيتم نشر مفتاح جديد، وستتكرر العملية برمتها.

8 اعتبارات أخرى للمناطق الموقعة

يجدر النظر في العناصر التالية استعدادًا لاستراتيجية نشر امتدادات DNSSEC:

- **تحديد برنامج تنمية القدرات**: تحديد ورش العمل والمشاركة فيها وكذلك الندوات عبر الإنترنت والتدريب العملي وأي أنشطة أخرى لبناء القدرات التي يمكن أن تساعد في زيادة المعرفة وتطوير مهارات جديدة في عمليات DNSSEC. تقدم المشاركة الفنية لـ ICANN مثل هذه التدريبات بما في ذلك ورش عمل DNSSEC، والتي تتم عادةً خلال اجتماعات ICANN.
  - مثل ICANN، يوفر مركز موارد بدء تشغيل الشبكة (NSRC)، ويوفر مجتمع الإنترنت وسجلات الإنترنت الإقليمية (RIRs) أيضًا أنشطة المشاركة المتعلقة بـ DNSSEC.
  - وأخيرًا، فمن شأن المشاركة في المنتديات والندوات عبر الإنترنت وورش العمل، التي يلتقي فيها المشغلون ذوو الخبرة والوافدون الجدد ويقدمون ويناقشون عمليات نشر DNSSEC الحالية والمستقبلية، أن يعزز بشكل كبير معرفتك بممارسات تشغيل DNSSEC.
- **اشترك في القوائم البريدية لـ NOG**: هذه منتديات جيدة يناقش فيها الأشخاص ويشاركون تجاربهم وخبراتهم الفنية بالإضافة إلى طلب الدعم والمساعدة في الأمور التقنية. إذن اعتبر أن هذا مجتمع يمكنه مساعدتك عند الحاجة.
- **إنشاء المفاتيح وإدارتها:** تقوم وحدات أمان الأجهزة (HSM) بتوفير وسيلة جيدة لإنشاء المفاتيح الخاصة وتخزينها. ومع ذلك، فإن تكاليف شراء وتأمين وصيانة وحدة أمن الأجهزة HSM تستحق أن تؤخذ في الاعتبار. وحسب ميزاتها، قد تختلف تكاليف HSM من مئات إلى آلاف الدولارات. يمكن أن تضيف وحدات HSM أيضًا نفقات التدريب، لأن تعلم أي جهاز جديد له تحدياته. ويعد استخدام وحدات HSM ممارسة جيدة ولكنه ليس الطريقة الوحيدة لإنشاء المفاتيح. هناك احتمال آخر يستحق النظر وهو إنشاء المفاتيح الخاصة وتخزينها واستخدامها في جهاز آمن ماديًا غير متصل بالشبكة وغير متصل بالإنترنت. وتوفر وثيقة RFC 6781 أيضا، تحت عنوان *ممارسات تشغيل DNSSEC، الإصدار 2* المزيد من التفاصيل حول إنشاء المفاتيح وإدارتها.
- **الاعتبارات الزمنية**: تقدم امتدادات DNSSEC فكرة الوقت المطلق في DNS. وتتمتع التوقيعات في DNSSEC بفترة صلاحية من تاريخ بدايتها إلى تاريخ انتهاء صلاحيتها، ويتم بعد ذلك تمييز التوقيع على أنه غير صالح وتعتبر البيانات الموقعة مزيفة. ومن الأهمية بمكان ضمان إدارة الوقت بشكل جيد بحيث يتم إنشاء التوقيعات تماشياً مع فترة الصلاحية الصحيحة. تخيل منطقة موقعة انتهت فترة صلاحية توقيعها؛ سيؤدي هذا إلى فشل التحقق من الصحة من جهة المحلل. وبالتالي، يوصى بشدة بتكوين خادم بروتوكول وقت الشبكة (NTP) من أجل الحفاظ على دقة الوقت. هناك أيضًا اعتبارات أخرى مثل الحد الأدنى والحد الأقصى لفترة فاعلية البيانات (TTL)، وفترة نشر التوقيع وفترة صلاحية التوقيع كما هو موضح في RFC 6781، *ممارسات تشغيل DNSSEC، الإصدار 2*.
- **متطلبات البرامج والأجهزة والشبكات**: يتم دعم تطبيقات امتدادات DNSSEC التجارية والمفتوحة المصدر حاليًا بما في ذلك نطاق اسم الإنترنت بيركلي (BIND) وPowerDNS وNLnet Labs Name Server Daemon (NSD) وKnot DNS على سبيل المثال لا الحصر. OpenDNSSEC هو حل توقيع يظل مستخدمًا على نطاق واسع لأنه يقوم بأتمتة عملية تتبع مفاتيح DNSSEC وتوقيع المناطق. إذا كنت تخطط لنشر DNSSEC على خادم موثوق، فستحتاج إلى إنشاء مفاتيح توقيع التشفير على النظام. ويعتمد مقدار الوقت المطلوب لإنشاء المفاتيح على مصدر العشوائية (الإنتروبيا) في النظام. وقد تستغرق أنظمة مثل الأجهزة الافتراضية ذات الإنتروبيا غير الكافية وقتًا أطول بكثير لإنشاء المفاتيح.
  - موارد الأجهزة مثل وحدة المعالجة المركزية وتخزين النظام والذاكرة هي أيضًا مجالات تستحق النظر فيها لتحسينات محتملة. وذلك لأن تمكين DNSSEC يزيد من تخزين النظام واستخدام الذاكرة وتحميل وحدة المعالجة المركزية جزئيًا بسبب إنشاء المفاتيح والتوقيع. دائمًا ما تكون المنطقة الموقعة مصحوبة بزيادة كبيرة في ملف المنطقة.
  - وفيما يتعلق بسياسات أمان الشبكة، تحقق من أن جدار الحماية وقواعد قائمة التحكم بالوصول ACL على سبيل المثال تسمح بحزم DNS UDP الكبيرة وDNS عبر TCP على المنفذ 53. ويجب، بالإضافة إلى ذلك، تنشيط آلية تبديل DNS (EDNS0) على كل من خوادم DNS وفي تكوين الشبكة، على التوالي.

9 إلغاء توقيع TLD عند اللزوم

إن الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC كغيرها من الأشياء في هذا العالم، لا تخلو من المشاكل. فعند إضافة المزيد من التعقيد إلى DNS، فإنه يزيد من احتمالية تعطل الأشياء أو حدوث خطأ ما. على سبيل المثال، قد يتم فقد أو اختراق مفتاح KSK أو ZSK أو كليهما. وقد يؤدي وجود خطأ غير متوقع في الأجهزة أو البرامج إلى منع توقيع المنطقة وتوزيعها، وبالتالي، التأثير على تقديم المنطقة بشكل صحيح.

في أسوأ السيناريوهات، قد تفضل إلغاء توقيع المنطقة لإصلاح أي مشكلات وأخطاء قبل التوقيع مرة أخرى. ومع ذلك، فإن إلغاء توقيع نطاق يستلزم تكلفة إعادته إلى حالة غير آمنة.

ويعرف العالم ما إذا كانت المنطقة موقعة أم غير موقعة من خلال وجود سجل DS في المنطقة الأصلية. لا يتم ضمان سلسلة الثقة في حالة عدم وجود سجل DS. ولذلك، فإن العودة إلى حالة غير موقعة تكون سهلة من الناحية الفنية مثل إزالة جميع سجلات DS من المنطقة الأصلية. أما في حالة ccTLD، فإن هذا يعني مطالبة IANA بإزالة سجل (سجلات) DS المقابل من منطقة الجذر.

يجب على مشغل TLD عند حل جميع المشكلات التفكير في إنشاء مفاتيح جديدة وإعادة توقيع المنطقة. يجب على المشغل علاوة على ذلك التأكد من أن المنطقة الموقعة حديثًا موزعة جيدًا ومتاحة في جميع خوادم الأسماء قبل نشر سجل DS جديد في منطقة الجذر. بمجرد أن يتم نشر DS بواسطة IANA، يدرك أطراف الإنترنت أن منطقة TLD قد تم التوقيع عليها مرة أخرى وأن أي محلل للتحقق سوف يتحقق من جميع سجلات الموارد التي تخدمها تلك المنطقة.

10 أدوات DNSSEC المفيدة

يمكن أن تكون الأدوات التالية مفيدة لاستكشاف مشكلات DNSSEC وإصلاحها.

10.1 مصحح أخطاء Verisign DNSSEC

يعد مصحح أخطاء DNSSEC، الموجود على https://dnssec-debugger.verisignlabs.com/، أداة قائمة على الويب، مما يساعد على ضمان أن "سلسلة الثقة" سليمة لاسم نطاق معين مُدعم بامتدادات DNSSEC. ويستعرض المصحح عملية التحقق خطوة بخطوة من اسم النطاق المحدد ويسلط الضوء على أي مشاكل ممكنة الحصول.

فيما يلي مثال لما قد تبدو عليه المخرجات

Domain Name: org

Analyzing DNSSEC problems for org

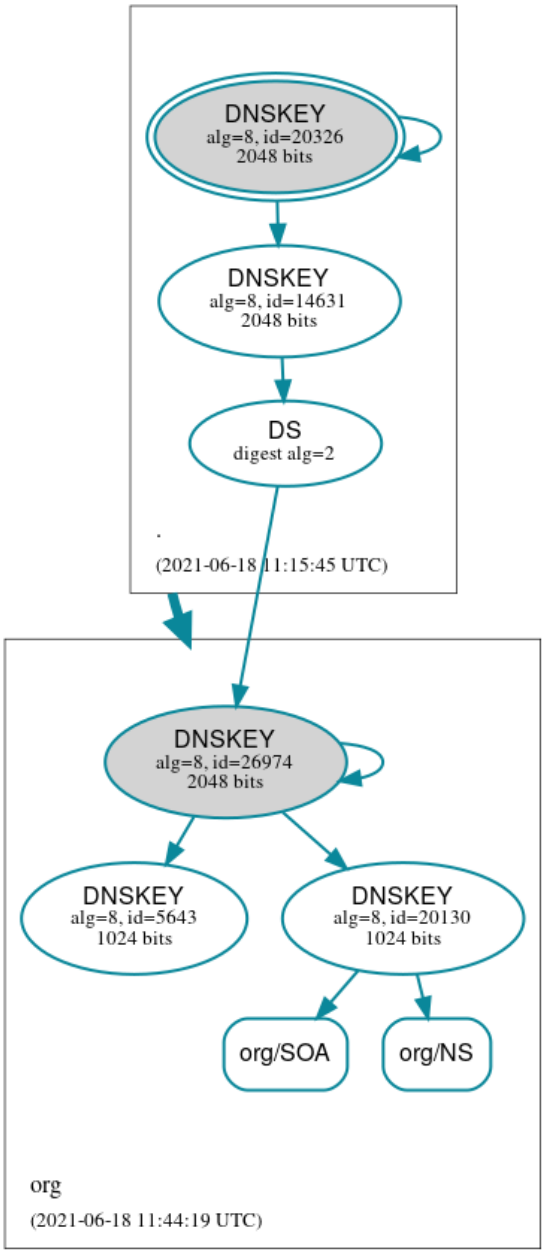
.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
org	Found 1 DS records for org in the . zone DS=26974/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=14631 and DNSKEY=14631 verifies the DS RRset Found 3 DNSKEY records for org DS=26974/SHA-256 verifies DNSKEY=26974/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=26974 and DNSKEY=26974/SEP verifies the DNSKEY RRset b2.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	c0.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	a0.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	a2.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	d0.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	b0.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

Want a second opinion? Test org at dnsviz.net.

DNSVIZ 10.2

إن DNSViz على الموقع (https://dnsviz.net) عبارة عن أداة لتصور حالة منطقة .DNS وهي توفر تحليلاً مرئيًا لسلسلة مصادقة DNSSEC لاسم النطاق ومسار الدقة الخاص به في فضاء اسم DNS. كما أنها تسرد أخطاء التكوين التي تكتشفتها الأداة.
تجد أدناه تصوراً لمنطقة نطاق ORG.:



11 الخاتمة

DNSSEC هي بروتوكول قوي يوفر مصداقية وسلامة بيانات DNS. يؤدي توقيع اسم النطاق باستخدام امتدادات DNSSEC إلى تغيير الكثير من الأشياء على المستوى التشغيلي من خلال تقديم مفاهيم ومهام جديدة لم تكن موجودة مع DNS العادي.

هذه الوثيقة هي دليل لمساعدة مشغلي سجل ccTLD وأي طرف آخر على فهم مقتضيات التوقيع على ccTLD. هناك الكثير من الأمور التي قد نتحدث عنها فيما يتعلق بـ DNSSEC، وقد غطت هذه الوثيقة بعض أهم جوانب النشر.

وكما هو الحال بالنسبة لأي حل أمني آخر، يُنصح باتباع العملية المناسبة والاستعداد لتجنب إفساد أمور أخرى. يجب على جميع الأطراف تقييم بيئتهم الخاصة والتهديدات ونقاط الضعف المرتبطة بها لتحديد مستوى المخاطر التي هم على استعداد لقبولها عند الاعتماد على DNSSEC لحماية منطقتهم والنطاقات الموجودة فيها.

وفي الأساس، تظل الجهود المنسقة والتعاون النشط من جميع أصحاب المصلحة عاملَين أساسيين للنشر الناجح لـ DNSSEC.

A- مثال على سياسات DNSSEC وبيانات تطبيق امتدادات DNSSEC

- إطار بيان سياسة وتطبيقات ZACR DNSSEC، الإصدار 001، سبتمبر/أيلول 2016، ZACR: https://www.registry.net.za/downloads/u/zacr-dps-signed.pdf
- بيان ممارسة DNSSEC.fr، الإصدار 1.2، يونيو/حزيران 2013، الجمعية الفرنسية للتعاون في مجال تسمية الإنترنت: https://www.afnic.fr/wp-media/uploads/2020/12/dps-english-fr.pdf
- بيان ممارسة CIRA DNSSEC لنطاق .CA، الإصدار 1.5، أغسطس/آب 2016، الهيئة الكندية لتسجيل الإنترنت: https://www.cira.ca/cira-dnssec-practice-statement-ca
- بيان ممارسة DNSSEC لمنطقة JP (أو JP DPS)، الإصدار 1.4، أكتوبر/تشرين الأول 2015، JPRS: https://jprs.jp/doc/dnssec/jp-dps-eng.v1.4.html
- بيان ممارسة DNSSEC من شركة VeriSign لمنطقة TLD/GTLD، الإصدار 1.8، ديسمبر/كانون الأول. 2019، شركة Verisign Inc.: https://www.verisign.com/assets/20191111_CTLD_VerisignDNSSECPracticeStatement_v1.8_finalized.pdf. يمكن العثور على قائمة المناطق التي ينطبق عليها هذا على: https://www.verisign.com/assets/20190430-Verisign-Operated-TLD-GTLD-Zones-v1.04-Converted.pdf

B- مثال على منطقة غير موقعة ومنطقة موقعة

1.B- منطقة غير موقعة

```
example.                  86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                2017072300 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                2419200    ; expire (4 weeks)
                300        ; minimum (5 minutes)
                )

example.                  86400  IN     NS     a.nic.dns.blablabla.
example.                  86400  IN     NS     b.nic.dns.blablabla.
example.                  86400  IN     NS     d.nic.dns.blablabla.
example.                  86400  IN     NS     e.nic.dns.blablabla.
example.                  86400  IN     NS     f.nic.dns.blablabla.
aaa.example.              86400  IN     NS     ns1.reg.zzzz.
aaa.example.              86400  IN     NS     ns2.reg.zzzz.
bbb.example.              86400  IN     NS     ns1.reg.zzzz.
bbb.example.              86400  IN     NS     ns2.reg.zzzz.
```

```
ccc.example.              86400  IN     NS     ns1.reg.zzzz.
ccc.example.              86400  IN     NS     ns2.reg.zzzz.
ddd.example.              86400  IN     NS     ns3-l2.nic.zzzz.
```

2.B- منطقة موقعة

```
example.                  86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                2017072305 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                2419200    ; expire (4 weeks)
                300        ; minimum (5 minutes)
                )

example.                  86400  IN     RRSIG  SOA 8 1 86400 20170724231821
20170618015310 660 example. nQ8H8StSRDoQgzwBNQ0k9+E1LGrV0tsCinoB6KxcyuHfGT4ehWsj5JI6
N01WpXqy/q1S/XlhqtjVoiti4zSOwIjFlSloug3W09eJnH9biwmb6U8B
JQoHf3edGvZtWNZdtcOKY1CFBI2ApceFn8KOYvT0qzpygOlF5lMrJvnO J5c=
example.                  86400  IN     NS     a.nic.dns.blablabla.
example.                  86400  IN     NS     b.nic.dns.blablabla.
example.                  86400  IN     NS     d.nic.dns.blablabla.
example.                  86400  IN     NS     e.nic.dns.blablabla.
example.                  86400  IN     NS     f.nic.dns.blablabla.
example.                  86400  IN     RRSIG  NS 8 1 86400 20170730192856
20170617025305 660 example. KNaF2jTPuCGq5FIzspbJL+TDBx/6z01E7+tkkzYRNh0xAKDnutcfb1It
D7XrNWPEbXsaafFyZ/M5DaDGzTzsVNm1h9h3md6o0vZNH07q8nmm+fYX
do8sx9aFxCgl9NsmG0cyrBbVnyrPKxDlAx69HJCh0kBb7PFKhr1hpnYY xGA=
example.                  86400  IN     DNSKEY 256 3 8
AwEAAasHjitdDurpevNLojD4Sp3609P+C9uOTR42DJel0NSSva/x38Ba
7gs0b4Q+tmKPI5cmxDhECiUfdzaRRA8vxPZK8x5LL/V1WZ5q6egFmH4x
eLxWaxlftFotev/T8kVe7jZUk7Hh3x7LPgGLajpjNNFELj42Xe6XBkkN 9FY1lQkB
example.                  86400  IN     DNSKEY 257 3 8
AwEAAY6HLDY5M5kjlrjVV9HQyWUkkrYZ2eB8KeJjUMN9qDM6FsA57pbS
5tmbGV1zxxqGon0pO7HYV06GZIgFOLBqDvgGsnKDQ5A2iktYNuSmTh+w
fd8ixgbYigtoBMBnNeqFozMK58c1yf7amui2cCOg9ibGZMpLQvjKOSyV
Jnlh0l8e3OE7Ul1GEa39XpVez2wkjImhsG0e7KAZPlFjEUpvwie8HEQV
jz3PK7Zr6SZVLLyet0rnN3prCHfvhNh6DycN/rt6/PopLvPQM8SaW+u8
zn6Z4S4AoTPTxKm5udzb7mWf7lT83PAbOvLu/WIRY6nqye+4SkJsrmjI xnLdk/Q54E8=
example.                  86400  IN     RRSIG  DNSKEY 8 1 86400 20170703000000
20170613000000 54322 example. B2riGYos+/q5RqXVBQKrrkVUuruDBH8ANNa8J6sMHUjf0MPZOuICd2kZ
PlAGMpZpp8LoaRoG2zaTVILZ8Vhi90FsyLsZVpPooAvmKlTFOrWoJoPo
XScLhb3ISRLOzKEnyLt5Ds3TxuabHLPlf8jpTXaHMFZCzYYtTJJQb+M3
BLeK+Lx4uCwU1pvxNkuR9StKa5tJquByIZCWZsSx5nKWPyrsGLtFJKrg
DXe8XlA8LxeER69OQgSZ1VXvK8Kd4p3wyvzUHCcsPYZzebxHXPqDrYB7
BU7eqsDUjCfThqbkC0Ju7koHROYRjGdoY/4f6nDOJEOICIFEgEDHJg2t w1nENQ==
example.                  0      IN     NSEC3PARAM 1 0 3 00FF
example.                  0      IN     RRSIG  NSEC3PARAM 8 1 0 20170716213640
20170606005304 660 example. a6Mp1NjW2/nnn+5i98AWzVrOX0yUvu/urP1cqY6zZjISReZOSLx6aorJ
lM9Nnx1fNVr2COtD71UVJI7kFUC5jVbmAitWdHHH/zyzK6WyyaN5Nsaf
cKW0Su8lLkctCHiqpKmuhOhnK1Dqmigx8YhyhPbN5nCzoST6lcnNjtV0 TwQ=
aaa.example.        86400  IN     NS     ns1.reg.zzzz.
aaa.example.        86400  IN     NS     ns2.reg.zzzz.
bbb.example.        86400  IN     NS     ns1.reg.zzzz.
bbb.example.        86400  IN     NS     ns2.reg.zzzz.
```

```
ccc.example.        86400  IN     NS     ns1.reg.zzzz.
ccc.example.        86400  IN     NS     ns2.reg.zzzz.
ddd.example.        86400  IN     NS     ns3-l2.nic.zzzz.
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN      NSEC3 1 1 3 00FF
464L7A368JEOCPKU9G34B9RQADEPKA14 NS DS RRSIG
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170703210235 20170602012306 660 example.
H+qdaHqnAgUa66VSKmMmfKWopeZQM0ridMUN2YN4rncHeWD8b0yA6O6N
hLF/ojpZoGrQN+G+p4SWJVb/pj2CkLk00E2AhloXXV0KaQIzUwPVNm7p
J9es7ohi5ErGtM1ClLpGggz05qNWboejbrXtS8TFdoTtn6Z2Omk4RNmj hG0=
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN      NSEC3 1 1 3 00FF
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA NS DS RRSIG
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170715005821 20170610062309 660 example.
dk6WScB3zmJYig0w8LxFXoc9vj1leqFRBlET4YAVVmeAwcGf0ixa41T+
pKKcMHbXDsw+PHYZHaRLmA9lEgs+4lJMdA3fRroNSXyV2usHMdFaKUoG
UZKehVGdgrBRx4vx+o4w1ztdumY6MsD0ART6IrhUbr+cvGHAlxNSviCI BbE=
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN      NSEC3 1 1 3 00FF
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7 NS SOA RRSIG DNSKEY NSEC3PARAM
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170706043605 20170604225320 660 example.
Ndq6p+Y8ztlgNN1vH12o5rxxh7QM8GLY3E1FPCX4h7N4RtnuoPpvEpsl
/K4XQ1p/8Uehe6Izg0BpvQ7A256/+UW3lkwlonR7UaOX/+gkEdxuxlC/
41nX5fI9G5QFrV7H8B7ezlVF/uLz4nXyH4mzz496x4iTMEoHfoAdMinL C7A=
example.                    86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. 2017072305 86400 14400 2592000 3600
```

C- قائمة مراجعة نشر DNSSEC

C.1- البدء والإعداد

- ❑ تحديد نشر DNSSEC كمشروع

إدارة العملية برمتها كمشروع بتاريخ بدء وتاريخ انتهاء مستهدف ومواد تسليم واضحة باستخدام نهج إدارة المشروع

- ❑ توثيق النظام الحالي.

وثيقة محدثة تصف النظام والعمليات المستخدمة

- ❑ تدقيق البنية التحتية الحالية

إصلاح أي أوجه قصور في النظام الحالي قبل نشر DNSSEC

- ❑ إشراك أصحاب المصلحة

إعداد فهمهم واستعدادهم لنشر DNSSEC

- ❑ تحديد واتباع خطة التدريب

زوّد موظفيك وأصحاب المصلحة بالمعرفة والمهارات اللازمة لنشر DNSSEC

C.2- النشر والمراقبة

- ❑ كتابة DP أو DPS

نشر إطار عمل عمليات DNSSEC المطبق في المنطقة

- ❑ كتابة خطة نشر DNSSEC

توثيق استراتيجية وخطوات النشر العالمية. يمكن تناول العديد من عناصر قائمة التحقق في هذا المستند.

- ❑ كتابة والتحقق من عمليات DNSSEC وإجراءات العمليات

  توثيق الإجراءات لمتطلباتك وبيئتك
- ❑ اختيار سيناريو نشر DNSSEC

  تحديد نموذج تنفيذ DNSSEC
- ❑ تحديد وشراء المواد والمعدات الجديدة

  اقتناء معدات ومواد جديدة
- ❑ حدد معلمات توقيع DNSSEC

  تعيين قيم لمجموعة من معلمات DNSSEC
- ❑ بناء منصة اختبار DNSSEC

  كتابة حالات الاختبار وتشغيلها والتحقق منها لتوقيع المنطقة لتكون على دراية بعمليات وعمليات DNSSEC
- ❑ التخطيط لبدء التنفيذ وإعداد إجراءات احتياطية

  إعداد وتوثيق بدء التشغيل في بيئة الإنتاج وكذلك إجراءات المراقبة وإجراءات الرجوع
- ❑ بدء التنفيذ والمراقبة

  تنفيذ ومراقبة توقيع DNSSEC في بيئة الإنتاج
- ❑ التخطيط لنشر DS للمسجلين

  تعزيز DNSSEC، والاستعداد لتلقي ومعالجة سجلات DS للنطاقات الفرعية
- ❑ نشر المسجلين DS

  الإعلان عن النطاقات الفرعية DS في منطقة ccTLD
- ❑ توثيق الدروس المستفادة

  تجميع الدروس والخبرات المستفادة في كل خطوة من العملية

D- قراءات إضافية

- انقطاعات DNSSEC الرئيسية وحالات فشل التحقق من الصحة، IANIX: https://ianix.com/pub/dnssec-outages.html
- *DNSSEC: طريق نشر الخوارزمية الطويل والوعر*، مركز معلومات شبكات آسيا والمحيط الهادئ، https://blog.apnic.net/2020/12/01/dnssec-the-long-and-bumpy-road-of-algorithm-deployment/
- إطار عمل تدقيق البنية التحتية لـ DNSSEC، مختبرات NLnet، https://nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf
- *معلومات DNSSEC الخاصة بالجذر*، هيئة الإنترنت للأرقام المخصصة، https://www.iana.org/dnssec
- *الأسئلة المتداولة حول الامتدادات الأمنية لنظام أسماء النطاقات*، SIDN، https://www.sidn.nl/en/faq/dnssec
- RFC 6781، *ممارسات تشغيل DNSSEC الإصدار 2*، https://www.rfc-editor.org/rfc/rfc6781.html

1. RFC 6841، *إطار عمل لسياسات DNSSEC وبيانات ممارسة الامتدادات الأمنية لنظام أسماء النطاقات*، https://www.rfc-editor.org/rfc/rfc6841.html
2. RFC 8078، *إدارة سجلات DS من النطاقات الأم عبر CDS/CDNSKey*، على https://www.rfc-editor.org/rfc/rfc8078.html

3. RFC 8624، *متطلبات تنفيذ الخوارزمية وإرشادات الاستخدام للامتدادات الأمنية لنظام أسماء النطاقات*، https://www.rfc-editor.org/rfc/rfc8624.html