RFC 6841 : A Framework for DNSSEC Policies and DNSSEC Practice Statements

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 janvier 2013

Date de publication du RFC : Janvier 2013

https://www.bortzmeyer.org/6841.html

Comme pour toutes les techniques de sécurité informatique, DNSSEC n'est efficace que si son déploiement s'accompagne de bonnes pratiques de sécurité. Il ne suffit pas de générer une clé et de signer la zone ! Pour prendre un exemple caricatural, si on signe sa zone DNS avec DNSSEC, mais que la partie privée de la clé est stockée, en mode 644 (lecture pour tous), sur un serveur sur lequel tous les employés du registre, les stagiaires et les consultants ont un compte, alors DNSSEC n'apportera guère de sécurité. Il est donc nécessaire de prendre certaines précautions. Un **DPS** ("*DNSSEC Policies and DNSSEC Practice Statement*") est un document qui liste les politiques et les pratiques d'un utilisateur de DNSSEC, y compris ces précautions.

Il a deux usages principaux. L'un est plutôt externe, communiquer au reste du monde, notamment aux utilisateurs du nom de domaine en question, les pratiques du registre, pour que ces utilisateurs, le régulateur, les autorités de cyber-sécurité (comme l'ANSSI en France) et les autres parties prenantes puissent se faire une idée du niveau de sécurité de DNSSEC dans cette zone. Et le deuxième usage est plus interne, documenter des choix effectués. Si un DPS peut n'être vu que comme un exercice bureaucratique de plus, il peut aussi être une utile "*check-list*" pour s'assurer qu'on maîtrise bien tous les composants de la chaîne de sécurité et qu'on n'a rien oublié dans sa réflexion.

Ce RFC fait la liste de tout ce que peut contenir un DPS, de manière à guider les auteurs de tels documents. Par contre, il ne dit pas quels sont les bons choix (en partie parce que ceux-ci dépendent des caractéristiques particulières de la zone signée), cela sera « vous devez indiquer si vous utilisez NSEC ou NSEC3 », pas « NSEC3 est meilleur que NSEC ». Ce RFC s'inspire d'un document équivalent fait pour X.509, le RFC 3647 [1] mais ne le copie pas, DNSSEC étant très différent de X.509.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3647.txt

En pratique, ce RFC sera sans doute surtout utilisé par les gérants de TLD mais il peut être utile à d'autres, notamment les zones les plus critiques, ou tout simplement ceux qui veulent améliorer leur sécurité (au prix d'un certain travail).

D'abord, une distinction entre **politique DNSSEC** ("*DNSSEC policy*") et **déclaration de pratiques DNSSEC** ("*DNSSEC Practice Statement*") en section 3 du RFC. La première est de plus haut niveau, plus générale, elle exprime le cahier des charges, ce qu'on veut atteindre comme objectif. Si une évaluation de la sécurité d'une zone est faite, par rapport à certaines menaces, c'est par rapport à cette politique DNSSEC. (La politique DNSSEC la plus simple est « on ne signe pas avec DNSSEC » mais elle est typiquement insuffisante face aux menaces d'aujourd'hui.) La seconde, la déclaration de pratiques DNSSEC, est plus concrète, décrivant les mécanismes qu'on déploie pour s'approcher de cet objectif. Si la politique DNSSEC dit ce qu'il faut faire, la déclaration de pratiques DNSSEC dit ce qui est fait. Attention, une déclaration de pratiques DNSSEC est typiquement un document public et on déclare donc ce qui est utile au public, et pas ce qui est confidentiel.

On notera que les deux documents peuvent être écrits par deux acteurs différents. On peut imaginer, par exemple, un régulateur écrivant la politique DNSSEC (les objectifs de sécurité) et le registre qui a obtenu la délégation de la zone écrivant la déclaration de pratiques DNSSEC (ce qu'il va faire pour atteindre ces objectifs).

La déclaration de pratiques étant plus concrète, elle est aussi plus détaillée et, typiquement, bien plus longue que la politique DNSSEC.

Si vous voulez voir des exemples de DPS existantes (je vais en citer plusieurs, à titre d'exemple), l'ISOC maintient une bonne liste <http://www.internetsociety.org/deploy360/resources/dnssec-practice-statements/>. Ce sont plutôt des déclarations de pratiques que des politiques. On y trouve surtout des TLD (j'ai utilisé pour les exemples la DPS <http://www.afnic.fr/fr/ressources/documents-de-reference/politiques-de-registre/dps.html> de `.FR` et celle <https://www.sidn.nl/en/about-nl/dnssec> de `.NL`) mais aussi des domaines comme `in-addr.arpa` (DPS du RIPE-NCC en ligne sur leur site <http://www.ripe.net/data-tools/dns/dnssec/dnssec-policy-and-practice-statement>) ou bien sûr comme la racine <https://www.iana.org/dnssec/icann-dps.txt>. Notons qu'elles ne sont pas forcément en anglais. Celle de `.CL` a deux versions mais celle en espagnol est la seule à faire autorité.

Alors, justement, que peut-on mettre dans ces documents ? La section 4 fait la liste des points qu'il peut être souhaitable de couvrir. Je ne vais pas les répéter ici, consultez le RFC 6841 si vous voulez tout savoir. Parmi les points qu'on peut noter, l'importance d'identifier dans le document à qui il s'adresse (section 4.1.3) : au gouvernement, au régulateur, aux gérants des serveurs récursifs, aux titulaires de noms de domaine, à tous à la fois ?

Un sujet de discussion dans la communauté DNSSEC a toujours été la publication des clés. DNSSEC reposant sur l'architecture arborescente du DNS, il n'y a en théorie besoin de publier qu'une seule clé, celle de la racine. Toutefois, on peut avoir de bonnes raisons de publier la clé d'un sous-domaine, par exemple pour être indépendant de la racine, ou bien parce qu'on a une relation plus forte avec le gérant de la zone qu'avec celui de la racine. Pour prendre un exemple imaginaire, on pourrait voir `gouv.fr` signé et chaque ministère mettre la clé de `gouv.fr` dans ses résolveurs, de manière à ce que la communication au sein du gouvernement français ne dépende pas du tout d'une organisation extérieure. Dans un cas comme celui-ci, la section 4.2.2 rappelle qu'il faut inclure dans ses documents publics les mécanismes de publication, et notamment la méthode que doivent utiliser les gérants de résolveurs validant pour s'assurer de l'authenticité des clés (récupération sur un serveur HTTPS, signature des clés avec PGP, etc). D'autres informations importantes peuvent être ajoutées comme la fréquence de renouvellement des clés et la technique qui sera utilisée pour prévenir d'un tel renouvellement. Par exemple, le `.CL`

utilise une liste de diffusion « *"NIC Chile mantendr[Caractère Unicode non montré [2]] una lista de correo electr[Caractère Unicode non montré]nico, de suscripci[Caractère Unicode non montré]n p[Caractère Unicode non montré]blica, donde se anunciar[Caractère Unicode non montré]n con anticipaci[Caractère Unicode non montré]n los inicios y términos de los rollovers de KSK : anuncios-dnssec@listas.nic.cl"* ».

À titre d'exemple, voyez la publication des clés de la racine <https://data.iana.org/root-anchors/> et sa documentation <https://data.iana.org/root-anchors/draft-icann-dnssec-trust-anchor.html>, ou bien celle de .FR <https://www.afnic.fr/fr/certificats/> ou du RIPE-NCC <http://www.ripe.net/data-tools/dnssec-keys/>. Au contraire, les clés de .UK ne font pas l'objet d'une publication (à part dans le DNS).

La déclaration de pratiques doit exposer comment sont délégués les enregistrements DS. DNSSEC ne servirait à rien si, par exemple, on pouvait ajouter ou modifier une DS via un canal non-sécurisé. De même, un registre peut avoir des méthodes pour tester que la DS soumise l'a bien été par le gérant de la zone (par exemple, Zonecheck <http://www.zonecheck.fr/>, depuis la version 3 <https://www.bortzmeyer.org/zonecheck-3-0.html>, peut vérifier que la zone est bien signée avec une clé correspondant à la DS indiquée). Ces méthodes sont alors décrites dans ce document. Enfin, le document peut indiquer comment on retire une DS de la zone (certains registres peuvent le faire dès qu'un problème technique est signalé, rendant alors la zone non sécurisée, mais, au moins, utilisable). Par exemple, .FR dit « Un enregistrement DS peut-être supprimé par une demande du bureau d'enregistrement via EPP ou un formulaire web sécurisé par TLS. » mais a aussi une possibilité de suppression par le titulaire « Un Titulaire d'un nom de domaine sous une extension géré par l'Afnic qui se trouve incapable de joindre le bureau d'enregistrement correspondant à ce nom, pourra utiliser une procédure exceptionnelle de suppression de DS, similaire à la procédure de demande d'urgence du auth_info. ».

La sécurité n'est pas l'affaire que de technique. Les sections 4.4 et 4.5 rappelent qu'il y a aussi toute une organisation nécessaire et qu'elle aussi doit être décrite dans la document : accès physique aux locaux (si vous utilisez des empreintes rétiniennes, c'est là qu'il faut en parler, idem pour les autres mesures "*high-tech*" prises pour assurer la sécurité du système, bref tous les gadgets James Bond utilisés dans le registre), procédures à suivre pour les opérations, etc. Par exemple, il est fréquent que les opérations de sécurité (comme le démarrage du processus de signature) reposent sur un schéma « M parmi N ». Cela veut dire que N personnes sont habilitées à effectuer les opérations et que M d'entre elles (avec M [Caractère Unicode non montré] N) doivent être présentes. La déclaration de pratiques DNSSEC est l'endroit où on donne les valeurs de M et de N (section 4.4.2).

Et comment décide-t-on que ces personnes sont « qualifiées » ? La section 4.4.3 dit que cela doit être marqué noir sur blanc : qualifications requises, enquêtes effectuées, sanctions prévues contre les employés qui violent les procédures, etc. La racine va assez loin dans l'examen de ses employés « "*Check of credit/financial records to the extent allowed by national laws for the individual's country of residence*" ». .FR dit « Le recrutement interne ou externe est effectué par la fonction RH de l'Afnic, qui vérifie les antécédents et les qualifications des candidats, prend en compte : Le curriculum vitae des candidats, Emplois précédents, Références, Les diplômes obtenus. Pour être admissible à l'un des rôles de confiance, ces contrôles ne peuvent pas révéler un critère d'incapacité. » Et .NL s'appuie sur les mécanismes de certification du pays « *"All persons that fulfill a role in the DNSSEC ceremony must have a "Certificate of Good Conduct" ("Verklaring omtrent Gedrag") issued by the Dutch government."* ».

C'est aussi à cet endroit qu'on devrait indiquer si les manœuvres de sécurité sont effectuées uniquement par les employés du registre ou bien peuvent l'être par le stagiaire envoyé par une SSII. Ainsi, .NL précise « *"No person outside of the specified Trusted Roles (4.2.1) can get access to the signer systems.If*

2. Car trop difficile à faire afficher par LaTeX

necessary, tasks can be performed with the guidance of an external contractor. At no time is the contractor allowed to be the person performing the tasks on the system." » alors que la racine est plus ouverte « "*In limited circumstances, independent contractors or consultants may be used to fill Trusted Roles. Any such contractor or consultant is held to the same functional and security criteria that apply to any ICANN employees in a comparable role. Independent contractors and consultants who have not completed or passed the background check procedures specified in DPS section 4.3 are permitted access to ICANN's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.*" ».

Une part du travail d'évaluation des risques concerne évidemment les PCA et PRA, en section 4.4.5.

Au passage, la section 4.4.1 concernait les risques physiques. Aux Pays-Bas, comme leur nom l'indique, le risque principal est l'inondation, ce qui explique cette mention dans le DPS du RIPE-NCC : « "*Additionally, we have a back-up site outside of Amsterdam at around 30 metres above sea level.*" » et, dans le DPS de `.NL` : « "*Several sites are located above sea level.*" ».

Les audits, pour vérifier si le système correspond réellement à ce qui est décrit dans la déclaration de pratiques DNSSEC, font l'objet de la section 4.7. Un avis personnel : comme toujours en sécurité, ils peuvent être traités comme un moyen concret de déterminer le vrai niveau de sécurité, ou bien simplement comme une série de processus, style ISO 27001, ayant peu de liens avec la réalité (« "*process over result*" »).

La génération des clés cryptographiques doit être particulièrement soignée (c'est souvent le point faible des processus cryptographiques). Chez les registres importants, elle fait en général l'objet de cérémonies solennelles, avec des auditeurs qui notent gravement toutes les étapes dans un gros livre, et deux caméras qui enregistrent le tout. La déclaration de pratiques DNSSEC doit indiquer comment se fait cette génération (sur un serveur Unix connecté à l'Internet ? au sein d'un HSM ?) et quelles précautions sont prises (la salle où se fait la génération est-elle une cage de Faraday, pour empêcher les attaques Tempest ?) Rappelez-vous, comme pour le reste de ce RFC, que ce RFC 6841 dit juste quels sont les points à couvrir, il ne prend pas position sur, par exemple, la question de savoir si un HSM vaut la peine ou pas. Le RFC dit juste « décrivez le système qui générera les clés ». La réponse « le responsable écrit à la main une série de chiffres sortis de sa tête, et qui lui semble cool et aléatoire » est acceptable, car elle permettra aux auditeurs de se faire une idée de la sécurité du système.

Une fois la clé générée, il faut garder en sécurité la partie privée (section 4.5.2). La mettre dans un fichier en mode 0644 (lecture pour tous) sur un serveur Web public (cf. section 4.5.6) est certainement une très mauvaise idée. Mais, ensuite, il y a plusieurs choix possibles, le choix dépendant en partie des moyens financiers du registre. Un fichier en mode 0600 (lisible uniquement par le propriétaire), propriété de root, sur une machine Unix bien gérée (cf. section 4.5.5), semble assez sûr mais il y a des risques : si un attaquant vole la machine physique, il met le disque dans une autre machine et il peut tout lire. Voilà pourquoi il existe des boîtiers assurant une certaine protection contre le vol physique. La norme FIPS-140 décrit leurs différents niveaux. Il faut noter que ce n'est qu'à partir du niveau 4 que le boîtier est "*tamper-zeroize*", c'est-à-dire qu'il garantit l'effacement des clés en cas d'ouverture non autorisée (« coupe le fil bleu »). Les HSM des niveaux 2 et 3 ne garantissent que la résistance à l'ouverture (qui n'est jamais infinie) ou le "*tamper-evident*" (si quelqu'un a ouvert le boîtier, cela se verra). Il faut donc prêter attention, pas juste à l'étiquette FIPS-140 mais aussi au niveau exact. Et, naturellement, comme toute technique de sécurité, il faut une évaluation globale, pour s'assurer de la cohérence du système. Il ne serait pas très utile d'avoir un HSM FIPS-140 niveau 4 si la base de données du registre permettait à n'importe qui d'écrire n'importe quoi dedans. Le RIPE-NCC dit « "*Systems used for signing the zones are FIPS 140-2 Level 2-certified*" » alors que la racine met la barre plus haut « "*For RZ KSK generation and RZ KSK private component operations and storage, ICANN uses hardware security modules that are validated at FIPS 140-2 level 4 overall.*" ». Même chose pour `.FR` : « Le Système utilise un module de Sécurité matérielle (HSM) conforme aux exigences du standard FIPS 140-2 Niveau 4 ». Le `.CL` ne fait pas référence à FIPS-140

mais dit « *"La "m[Caractère Unicode non montré]quina firmadora off-line" se encuentra en una caja fuerte bajo control directo de NIC Chile, y los Ministros de Fe conocer[Caractère Unicode non montré]n la clave para abrirla. Cuando no esté en uso, la "m[Caractère Unicode non montré]quina firmadora off-line" se mantendr[Caractère Unicode non montré] en una bolsa sellada para asegurar que no ha sido intervenida.*" ».

Autres questions sur la gestion de la partie privée : y a-t-il un séquestre ? Des sauvegardes (si on n'en fait pas, on minimise les risques de copie non autorisée mais on risque d'être très embêté en cas de destruction accidentelle de la clé) ? Et, si oui, on veut bien des détails. Pour `.FR`, la DPS annonce « L[Caractère Unicode non montré]Afnic n'a pas recours à l'entiercement des clés » et « Les clés créées sont : recopiées en format chiffré sur les cartes de sauvegarde (SMK) spécifiques au HSM exploité par l'Afnic. [...] Les clés sont sauvegardées de façon sûre et synchronisée après chaque génération de clé. ».

L'activation de la clé privée, pour commencer les signatures, dépend souvent de choses que possèdent les personnes autorisées. Il faut donc écrire noir sur blanc ce que sont ces choses : une carte à puce ? Un PIN ? Une partie de la clé privée (pour les cas où elle est divisée) ? Plusieurs choses ?

Enfin, la journalisation correcte des événements nécessite un estampillage temporel correct et la section 4.5.7 rappelle qu'il faut penser à décrire comment on obtient l'heure et avec quel niveau de sécurité <`http://seenthis.net/messages/98491`>. Le RIPE-NCC affirme « *"The signer systems securely sychronise their system clocks with a trusted time source inside our network*" ». Tout aussi vague, la racine dit « *"The ceremony administrator will manually set the signer system clock and the wall clock to current UTC time drawn from a reliable time source."* ». Et `.NL` : « *"The registry utilizes its default NTP-policy for timestamping. Time stamps are conducted using UTC and are standardized for all log information and validity time for signatures."* ». Bien sûr, aucune de ces trois déclarations n'est précise. Mais, bon, c'est une question difficile quand on rédige une DPS : trop de détails, et on risque de se lier les mains et de ne plus être à jour rapidement. Pas assez, et la déclaration ne sert pas à grand'chose.

Tout aussi technique, la section 4.6 concerne le processus de signature de la zone : quel algorithme de cryptographie utiliser (aujourd'hui, c'est RSA pour l'écrasante majorité des zones DNSSEC mais d'autres sont possibles, voir par exemple les RFC 6605 et RFC 5933), quelle longueur pour les clés, quel TTL pour les enregistrements, etc. On dit aussi ici si on utilise NSEC ou NSEC3 (RFC 5155) pour prouver la non-existence d'un nom. `.NL` annonce ses TTL ainsi « *"DNSKEY : 7200 seconds \ NSEC3 : equal to minumum[sic] field of SOA record (RFC5155) \ RRSIG : equal tot[sic] TTL of RRset covered, 7200 in practice*" » et la longueur « *"RSA algorithms with a key length of 2048 bits are currently used for KSK and 1024 bits for ZSK."* ». La racine dit « *"DNSKEY 48 hours \ NSEC same as SOA minimum (24 hours) \ RRSIG same as the covered RR (varies)*" ».

Un gros morceau de cette section est le problème récurrent du remplacement des clés <`https://www.bortzmeyer.org/remplacement-cles.html`>. Le sujet est sensible mais, en tout cas, il faut documenter les choix effectués.

Et, comme la sécurité n'est pas une question purement technique, que les registres peuvent avoir des obligations contractuelles, il faut aussi penser aux risques légaux et (section 4.8) documenter quelle est la loi qui s'applique au registre et ses éventuelles obligations contractuelles. La racine dit « *"This DPS shall be governed by the laws of the State of California*" » (problème classique de gouvernance Internet, la racine, ressource mondiale, est contrôlée par un seul État). Par contre, la DPS de `.JP` (dans sa traduction anglaise non officielle) « *"When operating JP DNSSEC Service, the Registry follows the laws of Japan and the rules defined by the Registry (No English translation is available)."* ». Et celle de `.FR` dit « La Loi française s'applique au présent document ».

La section 5 est simplement une suggestion de plan pour la rédaction d'une déclaration de pratiques DNSSEC. La plupart des déclarations que j'ai lues reprennent ce plan tel quel (certes, le RFC vient juste

de paraître, mais il est issu d'"*Internet-Drafts*" bien plus anciens, le processus de publication ayant été très lent). Une étude faite au sein du CENTR en février 2011 a montré notamment que, sur les 19 registres répondants, 17 connaissait cet "*Internet-Draft*" et 13 l'avaient utilisé comme "*check-list*" pour écrire leur propre DPS.

Merci à Florian Maury pour sa relecture (ce qui ne veut pas dire qu'il est d'accord avec moi sur tout.)