Énoncé des pratiques du Système de noms de domaine (DNS) d'Amazon Registry Services, Inc. pour la Zone MOI

Version 0.2

Table des matières

1 INTRODRUCTION

Le présent document « Énoncé des pratiques des DNSSEC pour la Zone MOI » (DPS) décrit les politiques et pratiques d'Amazon Registry Services, Inc. concernant les opérations des DNSSEC de la zone MOI.

1.1 Présentation

L'objectif du DPS est de fournir des informations opérationnelles concernant le protocole DNSSEC pour la zone MOI gérée par Amazon Registry Services, Inc.. Le document suit le cadre du DPS proposé par le Groupe IETF de travail des Opérations du système de noms de domaine (DNSOP).

1.2 Nom de domaine et identification

Énoncé des pratiques du DNSSEC pour la Zone MOI (DPS MOI)
Version : 0.2
Disponible le : date de la délégation de zone de racine
En vigueur le : date de la délégation de zone de racine

1.3 Communauté et applicabilité

Les intervenants avec leurs rôles et responsabilités prévus concernant le Service DNSSEC MOI sont décrits ci-dessous.

1.3.1 Responsable de zone

Amazon Registry Services, Inc. est le responsable de zone MOI

1.3.2 Administrateur de zone

Neustar est l'administrateur de zone.

1.3.3 Opérateurs du serveur

Neustar est le seul opérateur du serveur.

1.3.4 Registre

Amazon Registry Services, Inc. est l'Opérateur du registre des enregistrements de noms de domaine MOI. Dans le cadre des services DNS, Amazon Registry Services, Inc. fournit des services DNSSEC à ses registraires qui fournissent à leur tour lesdits services à leurs déposants. Le registre signe la zone en utilisant une combinaison de clés ZSK et KSK. L'/Les enregistrement(s) DS des clés KSK est/sont enregistré(s) dans la zone racine qui permet ensuite au résolveur activé du DNSSEC de conserver une chaîne de confiance entre la racine et le registre MOI.

1.3.5 Registraire

Le Registre fournit des services pour les registraires du système d'enregistrement de noms de domaine MOI. Les registraires ont une relation commerciale contractuelle avec le Registre afin d'enregistrer et conserver des domaines pour leurs déposants. Les registraires fournissent des informations sur les domaines y compris les enregistrements DS dans la zone MOI.

1.3.6 Déposant

Le Déposant est le propriétaire du domaine MOI enregistré dans le Registre par le biais d'un Registraire MOI. Un Registraire ou un fournisseur DNS sélectionné par le Déposant est responsable de la fourniture des enregistrements DS pour le domaine enregistré. Grâce à la soumission de ces enregistrements au Registre, une chaîne de confiance du Registre à la sous-zone d'autorité du Déposant peut être établie.

1.3.7 Opérateur de la clé de signature de clé de la zone MOI

Neustar est l'Opérateur de la clé de signature de clé de la zone MOI. Neustar doit générer la Clé de signature de clé de la Zone MOI (KSK) et doit signer l'ensemble de clés MOI (MOIKeyset) pour l'utilisation de la KSK. Il doit également générer et stocker de manière sécurisée les clés privées et distribuer la partie publique de la KSK.

1.3.8 Opérateur de la clé de signature de zone de la Zone Racine

Neustar est l'Opérateur de la clé de signature de la zone MOI. Neustar doit générer la Clé de signature de zone de la Zone MOI (ZSK) et signer le Fichier de la zone MOI en utilisant la ZSK.

1.3.9 Partie utilisatrice

Les parties utilisatrices comprennent des résolveurs DNS, par exemple les navigateurs ou les hôtes qui peuvent résoudre des noms dans la zone, les fournisseurs DNS, les fournisseurs de services Internet (ISP) et tout utilisateur qui utilise ou répond aux services DNSSEC MOI pour la résolution sécurisée d'un nom en utilisant le protocole DNSSEC.

1.4 Administration des spécifications

1.4.1 Organisation de l'administration des spécifications

L'administrateur du DPS MOI est Amazon Registry Services, Inc.

1.4.2 Informations de contact

Neustar au nom d'Amazon Registry Services, Inc. à l'adresse Reg-support@neustar.biz

1.4.3 Procédures de modification des spécifications

Le contenu du DPS est examiné chaque année ou plus souvent si nécessaire. Les modifications sont réalisées dans le document existant ou publiées en tant que nouveau document. Toutes les modifications seront réalisées dans le répertoire décrit ci-dessous. Amazon Registry Services, Inc. se réserve le droit de publier les modifications sans notification.

2 PUBLICATIONS ET RÉPERTOIRES

2.1 Répertoire DPS

Le DPS est publié dans un répertoire présenté sur le site Internet d'Amazon Registry Services, Inc. sur NIC.MOI :

2.2 Publication des Clés de signature de clé

Les KSK sont publiées dans la zone racine. La chaîne de confiance peut être terminée en utilisant les clés de la racine en tant qu'ancres de confiance.

2.3 Contrôles d'accès sur les répertoires

Le DPS est accessible au public qui peut accéder et consulter le répertoire DPS. Toutes les demandes de modification doivent être soumises à Amazon Registry Services, Inc. en vue d'un examen. Les contrôles ont été réalisés pour éviter les modifications non autorisées du DPS.

3 EXIGENCES OPÉRATIONNELLES

3.1 Signification des Noms de domaine

Les noms de domaine sont accessibles au public en vue de l'enregistrement. Dans certains cas, le registre se réserve le droit de supprimer ou de refuser l'enregistrement si certaines politiques ne sont pas respectées.

3.2 Activation du DNSSEC pour la Zone enfant

La chaîne de confiance de la zone Moi à la Zone enfant est établie lorsque les enregistrements DS signés de la Zone enfant ont été publiés dans la zone MOI. Une fois que la chaîne de confiance est établie, la Zone enfant est le DNSSEC activé.

3.3 Identification et authentification du Responsable de la zone enfant

Le registre n'a pas de lien direct avec le Responsable de la zone enfant et par conséquent il n'identifie et n'authentifie pas le Responsable de la zone enfant.

3.4 Enregistrements des Signataires de délégation (DS)

Les registraires se connectent au registre pour fournir et gérer des données d'enregistrement de domaine, y compris les enregistrements DS, au nom de leurs déposants.

3.5 Méthode pour prouver la possession de la Clé privée

Le Registre ne valide pas la possession de la clé privée dans la zone d'autorité enfant.

3.6 Suppression des Enregistrements DS

Un Registraire peut à tout moment demander la suppression des enregistrements DS d'un domaine que le Registraire gère. À la réception d'une demande valable, le Registre supprimera le DS de la zone.

4 CONTRÔLES DES INSTALLATIONS, DE GESTION ET OPÉRATIONNELS

4.1 Contrôles physiques

Le Registre MOI est hébergé dans les installations du centre de données qui répondent ou dépassent les spécifications environnementales attendues d'une plateforme de missions importante.

4.1.1 Localisation et construction du site

Le Registre MOI et les services DNSSEC sont exploités à partir de plusieurs centres de données complètement redondants à Sterling, Virginie et Charlotte, Caroline du Nord, États-Unis. Les emplacements des installations fournissent une connectivité réseau diverse et une capacité de réseau appropriée nécessaires pour exploiter efficacement tous les aspects du Registre et se protéger contre les catastrophes naturelles et catastrophes causées par l'homme. Dans les deux centres de données, des clés cryptographiques sont stockées dans un Module de sécurité matériel (HSM) de niveau 3 FIPS 140-2.

4.1.2 Accès physique

Neustar opère à partir des centres de données très sécurisés pour fournir les niveaux de sécurité les plus élevés et la disponibilité des services. L'accès physique aux installations est contrôlé de près. Les mécanismes de sécurité physique comprennent des gardes de sécurité, des caméras de vidéo-surveillance TV à circuit fermé et des systèmes de détection d'intrusion. Le NOC (Centre des opérations de réseau) gère l'accès à tous les emplacements 24 heures sur 24.

L'accès au HSM nécessite au moins deux Clés, l'Administrateur et l'Auditeur de sécurité. Les sauvegardes de clés sont stockées sur les clés du Dispositif d'entrée PIN (PED) et bloquées dans un coffre-fort à combinaison résistant au feu pendant deux heures.

4.1.3 Énergie et air conditionné

Chaque centre de données opère à partir de plusieurs sources d'énergie, y compris des générateurs de secours et l'énergie d'une pile. Chaque installation possède plusieurs unités d'air conditionné pour contrôler la température et l'humidité.

4.1.4 Exposition à l'eau

Amazon Registry Services, Inc. et Neustar ont pris des mesures pour minimiser l'impact des dommages causés aux systèmes provenant de l'exposition à l'eau.

4.1.5 Prévention et protection contre les incendies

Amazon Registry Services, Inc. et Neustar ont pris des mesures pour prévenir et éteindre les incendies ou d'autres expositions préjudiciables aux flammes ou à la fumée. Tous les systèmes sont protégés par des systèmes anti-incendie automatisés.

4.1.6 Stockage des supports

Les procédures de stockage et de traitement des supports sont définies par la Politique relative à la protection des données de Neustar.

4.1.7 Élimination des déchets

La politique et la procédure de sécurité des informations de Neustar comprennent les directives concernant la suppression appropriée des matériaux obsolètes basée sur leur sensibilité. La procédure implique le dépôt d'informations papier obsolètes dans des poubelles à déchets spécialement indiquées dans les locaux de Neustar (soumises au déchiquetage). En outre, les données électroniques sont effacées efficacement ou les supports sont détruits physiquement. Les disques durs et les bandes de sauvegarde, qui ne sont plus nécessaires, sont soumis à la démagnétisation.

4.1.8 Sauvegarde hors site

Un logiciel de sauvegarde est installé et utilisé pour la sauvegarde de tous les systèmes importants et le support de sauvegarde est tourné vers un emplacement hors site régulièrement. De plus, toutes les sauvegardes de systèmes importants sont intégrées au processus établi pour des tests de restauration de sauvegarde semi-annuels conformément à la Politique de sauvegarde de Neustar.

4.2 Contrôles de procédures

4.2.1 Rôles confiés

Neustar possède un nombre limité de rôles de confiance/privilégiés dans la gestion et les opérations du DNSSEC. Les rôles sont les suivants :

Administrateur de clés

- Génération de clés et enregistrements DS
- Gestion des roulements de clés

Auditeur de sécurité

- Il supervise les audits de sécurité
- Il s'assure que les règles/procédures sont respectées

Responsable du DNSSEC

- Il participe à des conférences et à des ateliers communautaires
- Expert en technologie DNSSEC
- Coordinateur entre Neustar et les parties externes

4.2.2 Nombre de personnes requises par tâche

La cérémonie de signature de clés et l'activation du HSM requièrent au minimum deux Administrateurs de clés et un Auditeur de sécurité.

4.2.3 Identification et authentification pour chaque rôle

Seul le personnel autorisé peut obtenir un accès physique au centre de données dans lequel les systèmes DNSSEC MOI se trouvent. L'accès au système est uniquement accordé aux membres des rôles mentionnés ci-dessus.

4.2.4 Tâches qui requièrent la séparation des obligations

Les tâches qui requièrent la séparation des obligations comprennent la génération, la mise en œuvre et la suppression de clés.

4.3 Contrôles du personnel

4.3.1 Exigences en matière de compétences, d'expérience et d'autorisation

Seuls les employés peuvent se voir attribuer les rôles du DNSSEC décrits dans la section 4.2.1. L'expérience et les compétences sont évaluées au cas par cas mais en général des connaissances approfondies des opérations du DNS et des technologies associées à la sécurité sont requises.

4.3.2 Procédures de vérification des antécédents

Les vérifications des antécédents comprennent un examen des compétences du demandeur, des antécédents professionnels, références, formation et toutes autres données pertinentes concernant les responsabilités du poste.

4.3.3 Exigences en matière de formation

Le personnel reçoit une formation continue en matière d'opérations et de gestion du DNSSEC. La formation comprend mais n'est pas limitée aux règles et procédures spécifiques MOI et aux technologies associées. Le personnel participe activement aux ateliers et conférences du DNSSEC.

4.3.4 Fréquence et exigences en matière de reconversion

La reconversion est assurée si nécessaire et elle est réalisée au cas par cas.

4.3.5 Fréquence et séquence de rotation des postes

Non applicable au présent document.

4.3.6 Sanctions pour les actions non autorisées

Non applicable au présent document.

4.3.7 Exigences en matière de recrutement du personnel

Non applicable au présent document.

4.3.8 Documents fournis au personnel

Tous les membres du personnel qui participent aux activités liées au DNSSEC reçoivent des documents qui comportent les procédures opérationnelles, les règles et les politiques qui régissent le service.

4.4 Procédures d'enregistrement des audits

4.4.1 Types d'événements enregistrés

Le Registre MOI enregistre toutes les informations nécessaires concernant un événement (qui, quoi et quand) y compris :

- L'accès aux centres de données dans lesquels les services du DNSSEC se trouvent
- L'accès aux serveurs et au HSM

- Les modifications des fichiers et systèmes de fichiers
- Les opérations de clés :
  - Génération/suppression de clés et d'autres événements concernant le cycle de vie d'une clé
  - Génération d'enregistrements DS et publication dans la zone racine

4.4.2 Fréquence de traitement des journaux

Les journaux d'audit sont gérés à des intervalles de temps réguliers afin d'assurer l'intégrité opérationnelle du Service du DNSSEC MOI. Les événements anormaux sont signalés en vue de recherches supplémentaires à effectuer par l'Auditeur de sécurité du DNSSEC.

4.4.3 Durée de conservation des informations des journaux d'audit

Les journaux du registre sont conservés en ligne pendant au moins trois mois. Les journaux les plus anciens sont stockés et archivés pour une durée maximale de cinq ans.

4.4.4 Protection des journaux d'audit

L'accès aux journaux d'audit est uniquement possible pour le personnel autorisé afin de protéger les fichiers de la visualisation non autorisée, modification, suppression ou autre manipulation. Les journaux d'audit ne contiennent aucune information qui pourrait être utilisée dans le but de compromettre l'intégrité des clés privées.

4.4.5 Procédures de sauvegarde des journaux d'audit

Les journaux d'audit sont sauvegardés à des intervalles prédéfinis sur un système de stockage hors ligne. L'accès à ces archives peut uniquement être demandé et ils peuvent seulement être consultés par le personnel autorisé du DNSSEC.

4.4.6 Système de collecte de l'audit

Le Registre utilise des logiciels et des applications qui automatisent l'enregistrement d'événements essentiels dans des journaux d'audit. De même que l'enregistrement du niveau des systèmes, les journaux d'application sont enregistrés et stockés.

4.4.7 Notification à la personne ayant provoqué un événement

Non applicable au présent document.

4.4.8 Évaluations de la vulnérabilité

Des évaluations automatisées et manuelles des vulnérabilités sont réalisées en partie par la gestion des journaux d'audit. Le personnel du registre participe également et partage les informations relatives à la sécurité avec d'autres membres de la communauté.

4.5 Compromission et Reprise sur sinistre

4.5.1 Procédures de traitement des incidents et compromissions

Si un incident ou une compromission est détecté, la portée du problème est déterminée. En cas de clé compromise, un roulement de clé d'urgence est immédiatement lancé. Le Registre a des politiques de protection d'urgence pour les clés KSK et ZSK.

4.5.2 Ressources informatiques, logiciels et/ou données corrompus

Le Registre possède des systèmes de sauvegarde en cas de corruption de ressources, logiciels et/ou données. Selon la nature du problème, des mesures appropriées seront prises conformément au plan de restauration du Registre.

4.5.3 Procédures de compromission d'une clé privée d'entité

En cas de compromission de la KSK du Registre, les mesures suivantes seront prises :

- Générer et activer une nouvelle KSK ou activer la KSK précédente qui est déjà dans la zone du registre. Dans le cadre de l'activation, le DNSKEY sera annulé.
- Remplacer l'enregistrement DS de la clé compromise par le nouvel enregistrement DS dans la zone racine.
- Révoquer et ensuite supprimer la KSK compromise dans la zone du Registre dès que la suppression sera suffisamment sécurisée.

En cas de compromission de la ZSK du Registre, les mesures suivantes seront prises :

- Générer et activer une nouvelle ZSK ou activer la ZSK précédente qui est déjà dans la zone du registre. Dans le cadre de l'activation, toutes les signatures seront annulées.
- Supprimer la ZSK compromise de la zone du registre dès que ses signatures ont expiré.

4.5.4 Poursuite des activités et capacités de reprise sur sinistre des technologies de l'information (TI)

Le Registre conserve un site de sauvegarde/basculement entièrement opérationnel. En cas de sinistre, le site de basculement gérera les opérations DNSSEC.

4.6 Résiliation de l'entité

Dans le cas où le Registre est résilié, une transition ordonnée sera réalisée avec l'entière coopération du Registre.

5 CONTRÔLES DE SÉCURITÉ TECHNIQUES

5.1 Génération et installation de paires de clés

5.1.1 Génération de paires de clés

Les paires de clés KSK et ZSK sont générées au cours de la cérémonie de signature qui se produit une fois par an ou plus si nécessaire. En général, en raison des cycles de roulement de clé prévus, il y a assez de paires de clés générées au cours de la cérémonie pour permettre des mois d'opérations des services DNSSEC MOI. La génération de clés est réalisée par le personnel autorisé dans un Module de sécurité matériel de niveau 3 FIPS 140-2.

5.1.2 Remise des clés publiques

Les clés utilisées par le Registre, KSK et ZSK, sont disponibles dans le cadre de l'Ensemble d'enregistrements de ressources DNSKEY (RRset) du Registre. Elles ne sont distribuées par aucun autre moyen.

5.1.3 Génération des paramètres de clés publiques et vérification de la qualité

La validation des clés publiques est réalisée régulièrement.

5.1.4 Usages visés des clés

Les clés sont utilisées pour la génération de signatures dans la zone du Registre et elles ne sont utilisées pour aucune autre fin.

5.2 Protection des clés privées et contrôles techniques des modules cryptographiques

5.2.1 Normes et contrôles des modules cryptographiques

Les ZSK et KSK sont générées et stockées dans un Module de sécurité matériel de niveau 3 FIPS 140-2.

5.2.2 Contrôle à plusieurs des clés privées

Au cours de la génération de clés, au moins deux membres autorisés de l'Administrateur de clés DNSSEC doivent être présents.

5.2.3 Entièrcement des clés privées

Les clés privées de la zone MOI ne sont pas entièrcées.

5.2.4 Sauvegarde des clés privées

Les clés privées sont sauvegardes sur des cartes PCMCIA compatibles avec le module FIPS 140-2 et stockées hors site et dans un coffre-fort à combinaison résistant au feu pendant deux heures.

5.2.5 Stockage des clés privées sur un module cryptographique

Non applicable au présent document.

5.2.6 Archivage des clés privées

Les clés privées ne sont pas archivées à des fins de stockage sauf au niveau site de sauvegarde en cas de basculement.

5.2.7 Transfert des clés privées vers ou depuis un module cryptographique

Les ZSK et KSK générées dans le HSM sont transférées vers un site de sauvegarde sous forme cryptée.

5.2.8 Méthode d'activation des clés privées

Les clés privées sont activées par des Administrateurs de clés qui fournissent des PIN au module de sécurité matériel en la présence de l'Auditeur de sécurité.

5.2.9 Méthode de désactivation des clés privées

Les privées sont désactivées à l'arrêt du système.

5.2.10 Méthode de destruction des clés privées

Les KSK et ZSK privées sont supprimées du système de sorte qu'elles ne puissent plus être utilisées à nouveau.

5.3 Autres aspects de la gestion des paires de clés

5.3.1 Archivage des clés publiques

Les clés publiques obsolètes ne sont pas archivées.

5.3.2 Périodes d'utilisation des clés

Une KSK reste active dans la zone du Registre pendant environ un an plus la période de transition y compris la publication et la désactivation. En raison d'un grand nombre de signatures réalisées par la ZSK, la ZSK reste active pendant environ trois mois plus la période de transition y compris la publication et la désactivation. Le Registre peut modifier lesdites périodes si nécessaire.

5.4 Données d'activation

5.4.1 Génération et installation des données d'activation

L'activation du HSM nécessite un Administrateur de clés qui fournit un PIN à son dispositif d'entrée PIN en la présence de l'Auditeur de sécurité.

5.4.2 Protection des données d'activation

Les Administrateurs de clés sont responsables de la protection et de la sauvegarde de leur PIN et de leur PED. L'accès peut être révoqué ou modifié si nécessaire.

5.5 Contrôles de sécurité informatiques

Tous les composants du service DNSSEC possèdent différents groupes de membres de personnel autorisés qui ont accès à et peuvent réaliser certaines opérations. Cet accès et ces opérations sont enregistrés et écrits dans les journaux d'audit. Tous écarts par rapport aux règles ou toutes tentatives malveillantes sont suivis et enregistrés en vue de recherches complémentaires.

5.6 Contrôles de sécurité du réseau

Toutes les opérations du Service DNSSEC sont hébergées et réalisées dans les centres de données de Neustar. Ceux-ci sont des réseaux internes protégés par plusieurs niveaux de protection physique et de réseau. Les réseaux sont sécurisés conformément aux politiques de sécurité des réseaux et physique.

5.7 Horodatage

Tous les horodateurs utilisés par le Service DNSSEC se trouvent dans l'UTC et sont synchronisés en utilisant les serveurs du Protocole d'heure réseau (NTP).

5.8 Contrôles techniques du cycle de vie

5.8.1 Contrôles de développement du système

Tous les composants du Service DNSSEC respectent les directives strictes de développement avant le déploiement. Lesdites directives strictes assurent des résultats fiables, de haute qualité et reproductibles.

5.8.2 Contrôles de gestion de sécurité

Le Registre possède des mécanismes permettant de surveiller toutes modifications de logiciel sur ses serveurs et d'établir des rapports quotidiens à vérifier par le personnel autorisé.

5.8.3 Contrôles de sécurité du cycle de vie

Le Registre continue d'améliorer ses contrôles sur la base des retours et des meilleures pratiques de la communauté. Toutes modifications des logiciels ou des politiques et procédures de sécurité seront évaluées, testées et approuvées avant le déploiement.

6 SIGNATURE DE ZONE

6.1 Longueur et algorithmes de clés

Les KSK et ZSK du Registre sont RSASHA256. La KSK comprend 2 048 bites alors que la ZSK comprend 1 024 bits.

6.2 Déni d'existence authentifié

Le Registre utilise des enregistrements NSEC tels que spécifiés dans la RFC 4034 pour authentifier le déni d'existence.

6.3 Format de signature

Le format de signature des enregistrements dans la zone MOI est RSA.SHA-2 spécifié dans la RFC 5702.

6.4 Roulement de clé de signature de zone

La ZSK MOI fait l'objet d'un roulement de clé tous les trois mois.

6.5 Roulement de clé de signature de clé

La KSK MOI fait l'objet d'un roulement de clé tous les 12 mois.

6.6 Période de validité de la signature et fréquence de la nouvelle signature

Les signatures sont valables pendant 30 jours pour les signatures réalisées par la ZSK et la KSK. La nouvelle signature est réalisée environ sept jours avant l'expiration.

6.7 Vérification de l'ensemble de clés de signature de zone

La ZSK générée au cours de la cérémonie de signature respecte un ensemble de procédures bien établies. Les clés publiques générées ainsi que leurs métadonnées sont en outre vérifiées par un autre ensemble d'outils de validation automatisés.

6.8 Vérification des enregistrements de ressources

Le Registre réalise régulièrement une vérification en ligne de tous les enregistrements de ressources dans la zone. Il enregistre tous les enregistrements de ressources et valide toutes les signatures dans la zone.

6.9 TTL (Durée de vie) des Enregistrements de ressources

La TTL de DNSKEY, DS et de leur Signature d'enregistrement de ressources (RRSIG) correspondante est établie à 518400 (6 jours). Le TTL du NSEC et de leur RRSIG correspondante est de 86400 (1 jour). La TTL pourrait changer à l'avenir si nécessaire.

7 AUDIT DE CONFORMITÉ

Des audits sont réalisés en utilisant les journaux conservés et d'autres informations pertinentes pour s'assurer que les procédures appropriées ont été respectées à tout moment et que les procédures ont été réalisées avec précision.

7.1 Fréquence des audits de conformité des entités

Les audits sont réalisés par le Registre, ou dans le cas où les services techniques du registre proviennent d'un tiers, ledit fournisseur de services tiers au moins chaque année.

7.2 Identité et compétences de l'auditeur

Des audits de conformité sont réalisés par un cabinet de conseils de sécurité indépendant qui est compétent en matière d'audits de sécurité, outils de sécurité, DNS et DNSSEC.

7.3 Lien de l'auditeur avec le Tiers de confiance

L'auditeur en charge de la réalisation de l'audit sera externe au Registre et/ou au fournisseur de services du registre, le cas échéant.

7.4 Sujets abordés lors de l'audit

Le champ d'application de l'audit comprendra un examen des événements qui se sont produits au cours de la période de l'audit y compris les opérations de gestion des clés, les contrôles des infrastructures/administratifs, la gestion de la KSK et de la ZSK et du cycle de vie des signatures et la divulgation des pratiques.

7.5 Mesures prises à la suite d'une défaillance

Si une anomalie importante est constatée au cours de l'audit, le Registre et/ou le fournisseur de services externalisé du Registre, le cas échéant, en sera informé immédiatement et un plan d'action corrective sera créé et exécuté par les parties affectées.

7.6 Communication des résultats

Les résultats de chaque audit seront présentés dans un rapport écrit au Registre et ou au fournisseur de services externalisé, le cas échéant, au plus tard 30 jours après la réalisation de l'audit.

8 QUESTIONS JURIDIQUES

8.1 Frais

Aucun frais ne sera facturé pour l'acceptation, la signature et la publication des enregistrements de ressources du Signataire de délégation ou toute autre fonction associée au DNSSEC.

8.2 Responsabilité financière

Amazon Registry Services, Inc. rejette toute responsabilité financière pour l'utilisation inappropriée des signatures réalisées conformément au présent DPS.

8.3 Confidentialité des informations commerciales

8.3.1 Champ d'application des informations commerciales

Les enregistrements suivants seront tenues confidentiels et privés (Informations confidentielles/privées) :

- Clés et informations privées nécessaires pour récupérer lesdites clés privées
- Signatures des ensembles de clés à publier à l'avenir
- Enregistrements transactionnels (enregistrements complets et les pistes d'audit des transactions)
- Enregistrements des pistes d'audit créés ou conservés par Neustar
- Rapports d'audit créés par Neustar (dans la mesure où les rapports sont conservés) ou leurs auditeurs respectifs (qu'ils soient internes ou publics) jusqu'à ce que lesdits rapports soient rendus publics
- Planification d'urgence et plans de reprise après sinistre
- Mesures de sécurité contrôlant les opérations du matériel et des logiciels de Neustar et l'administration des clés DNS

8.3.2 Informations qui n'entrent pas dans le champ d'application des informations confidentielles

Les informations de la base de données des domaines exploités par Neustar telles que d'autres informations d'état des Clés publiques sont publiques.

8.3.3 Responsabilité de protéger les informations confidentielles

Non applicable.

8.4 Confidentialité des informations personnelles

8.4.1 Informations traitées comme privées

Non applicable.

8.4.2 Types d'informations non considérées comme privées

Non applicable.

8.4.3 Responsabilité de protéger les informations privées

Non applicable.

8.4.4 Divulgation conformément au Processus judiciaire ou administratif

Amazon Registry Services, Inc. sera autorisée à divulguer les Informations confidentielles/privées si, de bonne foi, Amazon Registry Services, Inc. estime que la divulgation est nécessaire dans le cadre d'un processus judiciaire, administratif ou de tout autre processus juridique au cours du processus de découverte lors d'une action civile ou administrative, telle que les assignations, interrogatoires, demandes d'admission et demandes d'établissement de documents.

8.5 Limitations de responsabilité

Amazon Registry Services, Inc. ne sera pas tenue pour responsable de toute perte financière ou toute perte découlant de dommages accessoires ou d'une défaillance, à la suite de l'exécution de ses obligations en vertu des présentes. Toute autre responsabilité, implicite ou explicite, est rejetée.

8.6 Durée et résiliation

8.6.1 Durée

Le DPS entre en vigueur à sa publication dans le répertoire d'Amazon Registry Services, Inc.. Les modifications du présent DPS entrent en vigueur à leur publication dans le répertoire d'Amazon Registry Services, Inc..

8.6.2 Résiliation

Le présent DPS tel que modifié de temps à autre restera en vigueur jusqu'à ce qu'il soit remplacé par une nouvelle version.

8.6.3 Dispositions relatives à la résolution des litiges

Les litiges entre les participants au DNSSEC seront réglés conformément aux dispositions figurant dans les accords applicables entre les parties.

8.6.4 Droit applicable/Juridiction

Le présent DPS sera régi par les lois et la juridiction de l'État de Washington aux États-Unis.