DPS .fr

Politique de signature des domaines Afnic et conditions de mise en œuvre

(Version 1.2 - 11/06/2013)

afnic

Gestion du document

Identification du document

Responsable du doument
Responsable de la sécurité

Titre	DPS .fr
Référence du document	DPS-FR-01
Version	V1.2
Dernière mise-à-jour	Juin 2013

Classification de sécurité		**Nom du fichier**
Public	X	dps-fr.pdf
Sensible/Interne	☐	
Réservé/Diffusion restreinte	☐	
Stratégique/Critique	☐	

Approuvé par

Date	**Nom**	**Fonction**
Janvier 2012	Alain Caristan	CSO
11 juin 2013	Philippe Renaut	CTO

Révisions

Version	Author	Date	Révision
V1	Alain Caristan, David Barou	Mars 2012	Création
V1.2	Alain Caristan, David Barou	Juin 2013	Mise-à-jour vers la RFC_6841, janvier 2013

Sommaire

DPS .fr

Politique de signature des domaines Afnic et conditions de mise en œuvre

1. Introduction

Ce document décrit l'ensemble des politiques, procédures et outils mis en œuvre pour signer la zone .fr, grâce aux extensions de sécurité du DNS (DNSSEC).

Le DNS n'intégrait pas originellement de mécanisme de sécurité. Différentes vulnérabilités découvertes au fils des années ont menacé le fonctionnement et la confiance dans ce système.

Les extensions de sécurité du DNS, répondent à ces vulnérabilités en mettant en œuvre des mécanismes de signature cryptographique pour garantir l'intégrité et l'authenticité des enregistrements DNS.

Ce document fournit les éléments permettant à l'ensemble des utilisateurs de la zone .fr, d'évaluer le niveau de sécurité de la chaîne de confiance sur .fr Il présente également les procédures et infrastructures mises en œuvre pour la sécurité du registre.

1.1. Aperçu

Les extensions de sécurité du DNS (DNSSEC) est un ensemble de spécifications de l'IETF pour ajouter l'authentification de l'origine et l'intégrité des données au Domain Name System. DNSSEC fournit un moyen pour les logiciels de valider que les données du DNS n'ont pas été altérées ou modifiées pendant le transport Internet. Cela se fait en intégrant la clé publique cryptée dans la hiérarchie DNS pour former une chaîne de confiance provenant de la zone racine.

Huit éléments principaux sont décrits dans ce document :

1. Introduction
2. Publication et référentiel
3. Besoins opérationnels
4. Contrôle des accès, opérations et de gestion
5. Contrôles techniques de sécurité
6. Signature de zone
7. Audit de conformité
8. Dispositions légales

1.2. Nom et identification du document

Titre du document : DPS .fr
Version : v1.2

Création : 01/01/2012
Mise à jour : 11/06/2013

1.3. Parties concernées et condition d'application

Les rôles et délégations suivantes ont été identifiés.
La relation entre le Registre et le bureau d'enregistrement est notifiée dans le dossier d'accréditation qui peut être retrouvé dans son intégralité à l'adresse suivante :
http://www.afnic.fr/fr/produits-et-services/le-fr/devenir-bureau-d-enregistrement/

1.3.1. Registre

L'Afnic Association Française pour le Nommage Internet en Coopération, est responsable de la gestion de la zone .fr. Cela signifie que l'Afnic administre, ajoute, modifie et supprime des données pointant des noms de domaine vers des zones faisant autorité sous .fr. Cela signifie aussi que l'Afnic administre et fait évoluer l'infrastructure technique assurant performance et résilience à la zone .fr à son niveau.
De la même manière, l'Afnic, gère les clés permettant de signer cryptographiquement les enregistrements de la zone .fr, selon les modalités et les procédures décrites ci-dessous.
L'Afnic s'engage à signer régulièrement avec sa ZSK le résumé cryptographique des KSKs des délégations signées sous .fr.

1.3.2. Les bureaux d'enregistrement

Le bureau d'enregistrement est le tiers responsable de l'administration et de la gestion des noms de domaine au nom du titulaire. Le bureau d'enregistrement gère l'enregistrement, la maintenance et la gestion des noms de domaine d'un titulaire. Il est responsable de l'identification de ces titulaires.
Il est aussi responsable de l'ajout, suppression et mise à jour des empruntes de clés publiques « DS » pour *Delegation Signer*, à la demande du titulaire ou du contact technique du nom de domaine correspondant.

1.3.3. Le titulaire et contacts du nom de domaine

Un nom de domaine est créé par le titulaire, qui définit un contact technique responsable de l'administration de la zone. Lorsqu'ils administrent leur zone eux même, les contacts désignés pour un nom de domaine ont la capacité de transmettre les empreintes de KSK et d'assurer la gestion leurs publications grâce aux interfaces de leur bureau d'enregistrement, s'ils administrent leur zone.

1.3.4. Les relais

Parties qui participent au déploiement de DNSSEC d'un bout à l'autre de la chaîne de résolution, tels que la validation des signatures par les résolveurs et autres applications. Ces parties sont impliquées dans le déploiement de

DNSSEC et les mises à jour des clés. Ces parties doivent se tenir informer de toute mise à jour de l'Afnic sur ses zones si la clé de .fr est utilisée comme trust anchor. Sinon ils doivent se tenir informer de toute mise à jour des clés de la racine du DNS.

1.3.5. Auditeur

L'auditeur est l'entité qui audite aussi bien le service DNSSEC proprement dit et la façon dont l'Afnic l'opère.

1.3.6. Conditions d'application

Chaque titulaire est chargé de déterminer le niveau pertinent de sécurité dont il a besoin pour les noms de domaine dont les TLDs sont gérés par l'Afnic. Ce DPS est exclusivement applicable, au niveau des extensions Afnic et décrit les procédures, les contrôles de sécurité, ainsi que les pratiques applicable pour l'utilisation et la gestion des clés et des signatures pour les extensions gérées par l'Afnic.

En s'appuyant sur ce DPS les différentes tierces parties peuvent déterminer le niveau de confiance qu'ils attribuent aux extensions gérés par l'Afnic et en déduire leur propre niveau de risque.

1.4. Spécification de l'Administration

Ce DPS est mis à jour le cas échéant, comme lors d'une modification importante du système ou des procédures ayant un impact significatif sur le contenu de ce document.

1.4.1. Organisation en charge de l'administration

Afnic

1.4.2. Contacts

Autorité de Gestion des Politiques DNSSEC :

Immeuble International
13 avenue de la gare
Hall A2 - 7ème étage
Montigny le Bretonneux

Contact information
Afnic
support@afnic.fr

1.4.3. Procédures de modifications des spécifications

Le DPS de l'Afnic est révisé sur une base annuelle ou en cas de force majeure. Cette révision est effectuée par le Responsable du DPS du .fr (voir 4.2.1).
Les modifications au DPS sont faites soit sous la forme d'amendements au document existant soit par la publication d'une nouvelle version du document.
Le DPS et ses amendements sont publiés à l'adresse :
https://www.afnic.fr/fr/ressources/documents-de-reference/politiques-de-registre/

Seule la version la plus récente du DPS est applicable.

2. Publication et référentiel

2.1. Publications sur le site de l'Afnic

L'Afnic publie les informations importantes sur DNSSEC pour chacune de ses extensions à l'adresse **https://www.afnic.fr/fr/certificats/**
La version électronique officielle du DPS est celle publiée à :
https://www.afnic.fr/fr/ressources/documents-de-reference/politiques-de-registre/
Les notifications concernant DNSSEC sont poussées sur :
https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-operationnelles/
https://twitter.com/Afnic_Op

2.2.Publications de la clé qui signe les clés (KSK)

L'Afnic publie ses KSK sous la forme d'une DNSKEY et DS
La DNSKEY à utiliser en trust anchor est publiée sur le site de l'Afnic à l'adresse
https://www.afnic.fr/fr/certificats/
La DS est publiée auprès de IANA dans la racine du DNS.

3. Besoins opérationnels

3.1. Les noms de domaine

Le nom de domaine est un identifiant unique, qui est associé à des services tels que le web, l'hébergement ou encore l'email. Les demandes d'enregistrement sous .fr sont conformes à une politique de nommage élaborée avec l'opérateur de registre.

Le guide de procédures pour l'enregistrement des noms de domaines est disponible ici :
http://www.afnic.fr/fr/ressources/documents-de-reference/documents-techniques

3.2. L'activation des DNSSEC pour les zones filles

DNSSEC est activé pour un nom de domaine par au moins la publication d'un DS record dans la zone .fr, ce qui permet de créer une chaîne de confiance avec la zone fille. C'est le bureau d'enregistrement qui a la responsabilité de transmettre le DS, l'Afnic suppose que l'enregistrement DS qui lui est fourni est correcte.

3.3. Identification et authentification du gestionnaire pour les zones filles

Il est de la responsabilité du Bureau d'enregistrement de bien identifier et authentifier le titulaire grâce à un mécanisme approprié et en conformité avec les contrats qui le lient avec son client et l'Afnic.

3.4. Enregistrement des empreintes de clés (DS)

L'Afnic accepte les demandes de publication de DS via l'interface EPP et un formulaire web sécurisé par TLS. Pour EPP, les enregistrements doivent être validés et transmis suivant le format indiqué dans le RFC 5910 (*Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)*).
6 enregistrements DS peuvent être publiés au maximum.

3.5. Méthode pour prouver la possession de la clé privée

Le registre utilise le test ZoneCheck pour vérifier la correspondance de la clé et la bonne configuration de la zone. Le bureau d'enregistrement reste chargé de mener les contrôles qui sont et qu'il juge nécessaire pour assurer le bon fonctionnement des noms de domaine dont il a la responsabilité des enregistrements.

3.6. Suppression d'un enregistrement DS

Un enregistrement DS peut-être supprimé par une demande du bureau d'enregistrement via EPP ou un formulaire web sécurisé par TLS. La suppression de tous les enregistrements DS permet de désactiver DNSSEC pour une zone.

3.6.1. La capacité de suppression d'un enregistrement DS

Seul le bureau d'enregistrement peut passer les commandes de suppression des DS à la demande de son client.

3.6.2. Procédure de suppression

Le Titulaire demande au Bureau d'Enregistrement d'enlever le(s) enregistrement(s) DS de la zone .fr.
Le Bureau d'Enregistrement exécute la demande de retrait en appliquant les procédures définies par l'Afnic.

Pour répondre à la demande de suppression du Bureau d'Enregistrement, l'Afnic supprime l'enregistrement DS de la zone .fr.
Le temps nécessaire à la suppression d'un enregistrement DS de la zone .fr après avoir reçu la demande de suppression du greffe dépend de la mise à jour du DNS programmée par l'Afnic. Le délai maximum de mise à jour est de 10 minutes.

3.6.3. Procédure d'urgence pour un 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.

4. Contrôle des accès, opérations et de gestion

4.1. Contrôle physique

L'Afnic a mis en place des contrôles de sécurité physique pour satisfaire aux exigences spécifiées dans le présent DPS.

- Double sécurité d'accès au site avec gardiennage permanent et chemin de ronde.

  Une double vérification de l'identité et de l'autorisation d'accès de chaque intervenant sur le site est effectuée à l'accueil, puis au poste de sécurité, avec une présence 24/24 assurée.
  Un système d'accès par badge individuel et un système de reconnaissance biométrique tri dimensionnel complètent ce dispositif en limitant l'accès aux zones autorisées et en permettant une « traçabilité » des personnes sur le site. Trois check points sont installés entre l'entrée du site et l'espace client.

  De plus, la sûreté des locaux est assurée par un système CCTV doublé de caméras infrarouges en extérieur. Un nombre important de caméras filment et enregistrent numériquement les locaux et l'extérieur des bâtiments.
  Une batterie de moniteurs de contrôle enregistrent et conservent les données filmées sur une période allant jusqu'à 6 mois.

- Infrastructure résiliente offrant de larges espaces et une charge au sol jusqu'à 2 tonnes.

- Site multi bâtiments reliés entre eux par des tunnels en béton.

4.1.1. Emplacement et consrtuction

L'Afnic a mis en place un data-center géographiquement éloigné de son siège. Ce site répond aux normes Tier3 qui garantissent une haute sécurité et une haute disponibilité des systèmes hébergés. Tous les composants systèmes sont protégés dans un périmètre physique avec un contrôle d'accès et système d'alarme.
Le plan de continuité d'activité de l'Afnic répond aux bonnes pratiques, en termes de sécurité physique, alimentation, environnementales, incendie et protection de l'eau.

4.1.2. Accès physique

L'accès physique à l'environnement sécurisé est limité au personnel autorisé. L'entrée est contrôlée en permanence.
Sur le site du Datacenter, l'Afnic dispose d'une salle privée dont elle contrôle l'accès par des badges.

4.1.3. Puissance et climatisation

La puissance est fournie aux installations opérationnelles à travers plusieurs sources distinctes. Dans le cas de pannes de courant, la puissance est fournies par les systèmes d'alimentation de secours du data center (Tier 3 de Uptime Institure (basé sur la norme ANSI : ANSI/TIA-924)). Ils ont la capacité de fournir de l'alimentation pendant 72 heures.

Note :

- tier 1
  - Composé d'un seul circuit électrique pour l'énergie et pour la distribution de refroidissement
  - Sans composants redondants
  - offre un taux de disponibilité de 99,671%
- Tier 2
  - Composé d'un seul circuit électrique pour l'énergie et pour la distribution de refroidissement
  - Avec des composants redondants
  - Offre un taux de disponibilité de 99,741%
- Tier 3
  - Composé de plusieurs circuit électrique pour l'énergie et pour la distribution de refroidissement, mais seulement un circuit est actif
  - A des composants redondants
  - Offre un taux de disponibilité de 99,982%

4.1.4. Protection contre l'eau

Le site est en zone non inondable. Les installations sont protégées des inondations grâce :

- Un système de détection d'eau en faux plancher et sur tous les équipements.
- Une architecture de drainage (pompes de drainage et relevage dans les galeries en sous-sol)

4.1.5. Protection incendie

Le site répond aux normes de sécurité industrielles :

- Un système de sécurité incendie de catégorie A
- Un système d'extinction par Azote
- Application des règles R7/R13/R4
- Maintenance de la norme NFS 940
- Formation régulière des équipes
- Moyens d'accueil et d'intervention pompiers

4.1.6. Stockage des données

Le stockage est fait suivant la politique de stockage de l'Afnic. La classification des informations définit les conditions imposées de stockage, notamment pour les données sensibles.

4.1.7. Élimination des matériels sensibles

Tout le matériel de stockage ou ayant contenu des informations sensibles doit être réformé ou détruit de manière sécurisé par l'Afnic ou un contractant.

4.1.8. Sauvegarde hors site

Les données de l'Afnic sont répliquées automatiquement sur deux sites distants.

4.2.Procédures de contrôle

4.2.1. Rôles de confiance

Les rôles de confiance sont attribués à des personnes ayant la capacité de gérer le contenu du fichier de zone, les ancres de confiances. Elles sont aussi capables de produire et utiliser des clés cryptographiques.

Les rôles de confiance sont :

- Opérateurs Cryptographiques (2 parmi 9)

  Un opérateur désigné, saisira l'ensemble des instructions décrites dans les procédures présentées par le maître de cérémonie sur les boitiers cryptographiques.
  Le HSM en mode auto-online remplit une partie des fonctions de l'opérateur.

- Officiers de sécurité (2 parmi 9)
  Les officiers de sécurité donnent accès aux différents menus du boitiers grâce à leur carte et s'assure que l'ensemble de la cérémonie se déroule bien selon les procédures de l'Afnic. Les officiers de sécurité Afnic sont aussi Opérateurs Cryptographiques

- "Porteurs de clé" (1 parmi 4)

  Conserve les cartes à puce de sauvegarde (SMK/ISMK) qui définissent les droits d'utilisation de clés des HSM et application Keys, les clés de signatures sauvegardées. Chaque clé est nécessaire pour effectuer la sauvegarde ou l'import de ces clés de signature (application keys) sur des cartes à puce à part. Par contre les SMK sont sauvegardées dans le boitier et il n'y a besoin que de deux clés parmis 4 pour restaurer la SMK. Les officiers de sécurité doivent autoriser les opérations mettant en œuvre ces acteurs

- "Administrateurs du dispositif de signature"
  Sont les responsables des fichiers de configuration de la solution de signature et de la fourniture des backups à placer dans un coffre.

- "Auditeurs"
  Ils vérifient périodiquement les logs machine et s'assurent que les processus automatisés via l'API fonctionne comme attendu.

- "Le maître de cérémonie" (1 parmi 3)
  Il prépare l'ensemble des cérémonies en construisant un scénario à partir des procédures Afnic. Il donne l'accès au coffre fort et distribue l'ensemble des cartes aux différents acteurs de la cérémonie. Il est responsable de l'arrêt ou de la poursuite de la cérémonie en cas de problème ou d'événement non prévu.

4.2.2. Recrutement et autorisation des personnes dans les rôles de confiance

Seules les personnes ayant signé un accord de confidentialité et ayant reçu l'agrément de l'Afnic peuvent assurer l'un des rôles de confiance. Toute personne souhaitant accéder système devra présenter une pièce d'identité valide.

4.2.3. Séparation des rôles

Une seule et même personne ne peut simultanément tenir plusieurs mêmes rôles de confiance (Officier de sécurité ou opérateur). Ce qui signifie que deux personnes au moins sont nécessaires pour tenir une cérémonie.

Un Administrateur du dispositif de signature ne peut pas être opérateur.

Un Officier de sécurité peut être en même temps un opérateur;

4.3.Contrôle du personnel

4.3.1. Antécédents et qualifications

Les candidats souhaitant opérer un rôle de confiance devront apporter la preuve de leurs qualifications et expériences passées.

4.3.2. Contexte des procédures de recrutement

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.

4.3.3. Exigence de formation

L'Afnic fournit la formation nécessaire et pertinente sur ses procédures, l'administration et les systèmes techniques qui sont associées à chaque rôle de confiance. Les tests sont effectués après chaque cours de formation achevée et améliorent les compétences reconnues de la personne.

Ces formations sont :

- Formation aux opérations de l'Afnic
- Formation à la gestion des noms de domaine
- Formation à la théorie du DNS et de DNSSEC
- Information sur la politique de sécurité
- Formation aux procédures qualité

4.3.4. Fréquence des formations et exigences

Les personnes assumant des rôles de confiance doivent suivre des cours et tests complémentaires en cas de modification majeur du fonctionnement ou tous les trois ans.

4.3.5. Fréquence de rotation et séquence

La responsabilité de conduire les opérations sera donnée, autant que possible, alternativement à toutes les personnes ayant un rôle de confiance.

4.3.6. Les sanctions pour actions non autorisées

Les sanctions résultant d'actions non autorisées sont précisées dans l'accord de responsabilité correspondant aux rôles de confiance. Une négligence grave peut entraîner un licenciement et la responsabilité de la personne des dommages engendrés.

4.3.7. Exigence envers les contractants

Dans certaines circonstances, l'Afnic peut avoir besoin de recourir à des tiers pour compléter les ressources internes à plein temps. Ces tiers devront signer le même type d'engagement de responsabilité que celui des employés à plein temps.
Les tiers qui ne seront pas qualifiés pour les rôles de confiance ne pourront participer aux activités décrites en 4.2.2

4.3.8. Documentation fournie au personnel

L'Afnic et ses équipes techniques fournissent la documentation nécessaire pour que l'employé ou le contractant puisse accomplir leur travail de manière satisfaisante et en toute sécurité.

4.4.L'audit des procedures automatisées

Les procédures automatisées impliquent la collecte d'information au fil de l'eau de la vie du registre, établissant un livre de bord de l'activité.
Ce livre de bord est utilisé pour le suivi des opérations à des fins statistiques et à des fins d'enquête en cas de suspicion ou de constat de violation des politiques et règlements de l'Afnic.
Les informations du journal de bord comprennent également des revues, des listes et autres documents papier vitaux pour la sécurité et l'audit.
L'objectif du stockage d'information dans le journal de bord est de pouvoir reconstituer le déroulement des faits et les analyser, pour déterminer quelles personnes ou applications / systèmes a fait quoi et à quel moment.
Le livre de bord et l'identification des utilisateurs permettent d'établir une traçabilité et le suivi des utilisations non-autorisées.

4.4.1. Les événements faisant l'objet d'un enregistrement

Les événements suivants sont inclus au journal de bord :

- Toutes les activités qui impliquent l'utilisation d'un HSM, comme la génération de clé, l'activation de clé ainsi que la signature et l'export de clés.
- Les accès à distance, réussis et non réussi.
- Les opérations privilégiées.
- L'accès à une installation.

4.4.2. Fréquence de contrôle des Log(s)

Les Log(s) est analysé en permanence au travers de contrôles automatisés et manuels. Des contrôles spécifiques sont conduits pour la gestion des clés cryptographiques, redémarrage des systèmes et détection d'anomalies.

4.4.3. Période de conservation des informations des Log(s)

Les informations de Log(s) sont conservées dans le système, puis elles sont archivées pendant au minimum 10 ans.

4.4.4. Protection des informations des Log(s)

Toutes les informations des Log(s) sont stockées en même temps dans au moins 2 sites distincts et distants l'un de l'autre. Le système d'enregistrement est protégé contre la manipulation et l'affichage non autorisé de ces informations

4.4.5. Sauvegarde de sécurités des Log(s)

Toutes les informations des Log(s) sont sauvegardées et stockées dans un endroit sûr indépendant du système.

4.4.6. Système de Collecte des Log(s)

Toutes les informations papier sont scannées et stockées de manière électronique à la fois dans au moins deux distincts et distants l'un de l'autre.

4.4.7. Information sur l'exploitation des Log(s)

Le personnel concerné est informé de l'exploitation des Log(s). Le personnel n'est pas autorisé à consulter les données des Log(s).

4.4.8. Analyse des vulnérabilités

Toutes les anomalies dans les informations des Log(s)s sont étudiées pour analyser les vulnérabilités potentielles.

4.5. Compromission et reprise d'activité suite à une catastrophe

4.5.1. Gestion des incidents

Est défini comme incident :

- tout événement réel de nature critique pour la sécurité ou perçu comme tel qui a causé ou pourrait avoir causé une panne, un dommage au système d'information,
- toute perturbation et/ou défaut du à des renseignements inexacts,
- toute atteinte à la sécurité.

Tous les incidents sont traités conformément aux procédures de l'Afnic. La procédure de gestion des incidents impose de :

- rechercher les causes de l'incident,
- d'identifier les effets qu'il a eu ou pourrait avoir eu,
- de prendre les mesures adéquates pour empêcher qu'il ne se reproduise et à rapporter cette information.

Dans le cas où un incident conduirait à établir des soupçons sur une compromission de clé, une rotation immédiate de la clé sera à réaliser conformément aux procédures indiquées dans le chapitre 4.5.3.

4.5.2. Corruption matérielle, logicielle ou d'information

En cas de corruption matérielle, logicielle ou d'information, les procédures de gestion des incidents doivent être appliquées et des mesures appropriées doivent être prises.

4.5.3. Procédures en cas de suspicion de compromission ou d'utilisation non appropriée de la clé privée

La suspicion de compromission ou d'utilisation non appropriée de la clé privée mène à la génération d'une nouvelle clé de la façon suivante :

Pour la ZSK
Si une clé de signature de zone (ZSK) est suspectée d'être compromise, elle sera immédiatement retirée de la production et ne sera plus utilisée. Si nécessaire, une nouvelle clé ZSK sera générée et l'ancienne clé sera supprimée du jeu de clés dès que la signature aura expirée.
La notification de cette compromission sera notifiée par les canaux indiqués au point 2.1.

Pour la KSK
Si une KSK est suspectée d'avoir été compromise, une nouvelle clé sera immédiatement générée et utilisée en parallèle de l'ancienne clé. L'ancienne KSK restera en place et sera utilisée pour la signature de l'ensemble des clés tout le temps nécessaire à la prise en compte de la nouvelle clé par l'ensemble des résolveurs validant et qu'une rotation puisse être effectuée sans risque d'erreur de résolution.
La rotation de KSK sera toujours notifiée par les canaux indiqués au point 2.1.

Dans le cas de perte d'une KSK, un changement de clé KSK se fera sans chevauchement entre la clé perdue et la clé d'urgence pré-publiée.
A ce moment, l'information sera notifiée par les canaux indiqués au point 2.1.

Les tierces parties utilisant une des KSK de l'Afnic comme des ancres de confiance devront ajouter la KSK d'urgence prévue à cet effet comme ancre de confiance. Pendant ce temps, le jeu de clés sera figé, aucune rotation de ZSK n'aura lieu tant que la KSK n'aura pas été remplacée.

4.5.4. Plan d'urgence

L'Afnic a un PCA (Plan de Continuité d'Activité) qui assure que la continuation des services critiques.
Dans cet objectif, les installations de secours sont équivalentes en termes de protection physique et logistique. Les données sont répliquées en temps réel entre les installations.

Le PCA et les procédures de reprise sont régulièrement testés et si besoin améliorés.

Le PCA définit :

- les responsabilités sur l'activation des procédures de reprise d'urgence,
- Le fonctionnement de la gestion des crises,
- Le lancement des opérations de sauvegarde.
- La nomination d'un gestionnaire de tâches.
- Les conditions à remplir pour un retour à la normale.

4.6. Défaut du registre

Si pour quelque raison que ce soit, l'Afnic devait désactiver DNSSEC pour une de ses zones et ne plus signer cette zone, cela se fera de manière ordonnée qui comprend l'information au public.
Si l'exploitation d'une zone doit être transféré à tierce partie, l'Afnic participera à cette transition de manière à la rendre le plus fluide possible.

5. Contrôles techniques de sécurité

5.1. Génération de paires de clés et installation

5.1.1. Production de paires de clés

La génération des clés est réalisée par un module de Sécurité matérielle (HSM) qui est opéré par des personnels qualifiés et dûment appointés pour ces rôles de confiance.
La Génération des clés est effectuée via des commandes d'open-dnssec. Leur réplication sur les boitiers de spair se fait en présence de deux officiers de sécurité, deux opérateurs, un porteur de clé et un maître de cérémonie. Ces personnes doivent être présentes pendant toute la durée de l'opération.
L'ensemble de la procédure de génération de clé est tracée par des logs, dont une partie est enregistrée de façon électronique et une partie est consignée sur papier par les Officiers de Sécurité.

5.1.2. Distribution de clés publiques

La partie publique de chaque KSK générée est récupérée dans le système de signature et vérifiée par les officiers de sécurité et les opérateurs.
L'Officier de Sécurité est responsable de la publication de la partie publique de la KSK de manière sécurisé telle que définie au 2.1.
L'administrateur système vérifie que les clés publiées sont bien celles qui ont été générées.

5.1.3. Contrôle de Qualité des paramètres de clés

Les paramètres de clé sont définis par la Politique de gestion des clés et de signature de l'Afnic et le contrôle de comprend la vérification de la longueur de clé.

5.1.4. Utilisation des clés

Les clés générées pour DNSSEC ne sont jamais utilisées à autre chose que DNSSEC pas plus qu'elles ne sont utilisées en dehors du système de signature.
Que ce soit pour la ZSK ou la KSK, une signature produite avec une clé DNSSEC ne peut avoir une durée de vie supérieure à 3 mois.

5.2. Protection de la clé privée et des modules cryptographiques

Toutes les opérations cryptographiques sont effectuées par le module matériel de sécurité et il n'est pas possible de disposer des clés privées à l'extérieur de ce module.

5.2.1. Normes et contrôles des modules de Sécurité cryptographique

Le Système utilise un module de Sécurité matérielle (HSM) conforme aux exigences du standard FIPS 140-2 Niveau 4 (Federal Information Processing Standards : *Security Requirements for Cryptographic Modules*).

5.2.2. Contrôle multi - personnes (2 – parmi – 9) des clés Privées

Le Registre n'applique pas le contrôle multi-personnes pour l'activation du module. La présence de l'Officier de Sécurité est requise pour activer le module de sécurité, mais l'accès physique est opéré par l'Administrateur des Systèmes qui est le seul habilité.

5.2.3. Entiercement de clés (Key escrow)

L'Afnic n'a pas recours à l'entiercement des clés.

5.2.4. Sauvegarde de sécurité

Les clés créées sont :

- recopiées en format chiffré sur les cartes de sauvegarde (SMK) spécifiques au HSM exploité par l'Afnic.

  Ensuite les options possibles :

  - les clés sont recopiées dans les HSM de PCA depuis les cartes de sauvegarde qui sont ensuite effacées,
  - les clés sont recopiées dans les HSM de PCA depuis les cartes de sauvegarde qui sont ensuite rangées dans un endroit qui n'est accessible que par un Officier de Sécurité,

Les clés sont sauvegardées de façon sûre et synchronisée après chaque génération de clé.

5.2.5. Stockage dans un module de Sécurité cryptographique

Chaque module assure les opérations de signature et la gestion automatique des clés.
De ce fait, les clés de production sont présentes en permanence dans chacun des modules de sécurité qui contiennent les mêmes informations pour des besoins de redondance.
Chaque carte de sauvegarde est utilisable sur chacun des modules de sécurité.

5.2.6. Archivage de clé privée

Les clés Privées qui ne sont plus utilisées sont uniquement archivées sous forme de copies de sauvegarde.

5.2.7. Transfert de clé Privée vers et depuis le module de Sécurité cryptographique

Les clés privées sont échangées entre les différents à travers le mécanisme de sauvegarde et restauration par les cartes de sauvegarde (SMK).

Les cartes de sauvegardes sont gérées conformément aux règles édictées en 5.2.4.

5.2.8. Activation des clés Privées

Les clés privées sont activées de façon automatique par le dispositif de gestion de clés.
L'activation se fait conformément à la configuration mise en place par l'Administrateur du dispositif de signature (cf. 4.2.1).

5.2.9. Désactivation des clés Privées

Le HSM est automatiquement verrouillé si le dispositif de signature est coupé ou redémarré.

5.2.10. Destruction des clés Privées

Après leur utilisation effective, les clés Privées sont effacées du dispositif de signature.

5.3. Autres aspect de la gestion des paires de clés

5.3.1. Archivage des clés publiques

Les clés publiques sont archivées conformément à l'archivage des autres informations relevant de la traçabilité du système, telles les données de logs.

5.3.2. Durée d'utilisation des clés

Une paire de clé devient invalide lorsqu'elle est révoquée et/ou retirée de la production.

5.4. Données d'activation

Une donnée d'activation est le code d'authentification utilisé par chaque officier de Sécurité pour activer le HSM.

5.4.1. Génération et installation des Données d'Activation

Chaque Officier de Sécurité est responsable de la création de ses propres codes d'authentification en respectant une règle de différentiation maximale des séquences caractères.

5.4.2. Protection des données d'activation

Chaque Officier de Sécurité est responsable de la protection de ses données d'activation de la meilleure façon qu'il soit. En cas de suspicion de compromission de ces données, il doit immédiatement les changer.

5.4.3. Autres aspects concernant les Données d'Activation

Une enveloppe scellée et cachetée contenant les données d'activation sera détenue dans un endroit sûr. Elle ne pourra être utilisée qu'en cas d'urgence selon un protocole qui s'appliquera à un Officier de Sécurité qui officiera dans le cadre du PCA de l'Afnic sur le DNSSEC.

5.5. Contrôles de Sécurité du traitement de l'information

Tous les composants critiques des systèmes du Registre sont situés dans des lieux sécurisés conformément à l'article 4.1. L'accès au système opératoire des serveurs est strictement limité aux personnes habilitées, c'est-à-dire les Administrateurs Systèmes.
Tous les accès sont enregistrés et traçables sur un plan individuel.

5.6. Contrôles de Sécurité des communications

Le registre a segmenté son réseau de façon logique en plusieurs zones sécurisées interconnectées de façon sécurisées. Les accès se font à travers des pare-feux. Toutes les communications comportant des informations sensibles sont chiffrées de manière robuste.

5.7. Horodatage

La synchronisation des horloges des serveurs est obtenue sur les serveurs NTP de l'Afnic.

L'horodatage est basé sur l'heure UTC. Elle est consignée dans un format identique pour toutes les informations de logs ainsi que pour la définition des périodes de validité des signatures.

5.8. Cycle de vie des contrôles techniques

5.8.1. Contrôles du système de développement

Tout le code source est conservé dans un système de subversion. Le code source est archivé régulièrement et les copies sont stockées séparément dans un lieu sûr et ignifugé.

Les développements effectués à l'Afnic sont basés sur les standards de l'industrie et comprennent :

- Des spécifications fonctionnelles complètes et documentés des exigences sur la sécurité,
- Une volonté permanente de réduire la complexité,
- Des tests systématiques automatisés et tests de régression,
- Fourniture de version de logicielles distinctes,
- Un suivi constant de la qualité et de correction des défauts constatés.

5.8.2. Contrôles du système de signature

Les registres des personnes habilités sont conservés et suivis de façon régulière.
L'Afnic diligente des audits réguliers sur la sécurité du dispositif de signature.
L'Afnic élabore et maintient un "plan de sécurité du dispositif de signature" fondé sur une analyse des risques récurrents.

6. Signature de zone

6.1. Longueurs de clés et algorithmes de chiffrement

Les longueurs de clé et les algorithmes doivent être d'une longueur suffisante pour l'usage qui en sera fait durant leur durée de vie (2 ans pour la KSK, 3 mois pour la ZSK).
Les algorithmes doivent répondre au standard de l'IETF, être publiques et efficientes pour toutes les parties concernées.
L'algorithme RSA est actuellement utilisé avec une longueur de 2048 bits actuellement pour la KSK et de 1024 bits pour la ZSK

6.2. Authentification des dénis d'existence

Le Registre utilise les enregistrements NSEC3 + Opt-out tels que spécifiés dans le RFC 5155.

6.3. Signature Format

Les signatures sont générées par une opération RSA en utilisant une fonction de hachage cryptographique basée sur SHA2 (RSA/SHA-256, RFC 5702) .

6.4. Roulement des clés

La rotation de la ZSK est effectuée tous les 60 jours

La rotation de la KSK est effectuée selon le besoin (environ tous les ans).

6.5. Durée de vie de la signature et fréquence de la resignature

La zone est signée de manière incrémentale à chaque publication (voir la fréquence de publication annoncée par l'Afnic).
La "resignature" complète intervient au moins une fois par semaine.

Les signatures ont une durée de vie de 3 mois.

6.6. Vérification de jeu des clés de signature de la zone

Afin de garantir la validité des clés et des signatures, des contrôles de sécurité sont effectués avec la clé DNSKEY avant la publication des informations de zone sur l'Internet.

6.7. Vérification des "Resource Records"

Le Registre vérifie qu'avant la distribution tous les "Resource Records" (RR) sont valides conformément aux normes en vigueur.

6.8. Time-to-live des RR(s) (TTL)

Les Time-to-live (TTL) pour chaque RR (RFC 4034) sont les suivants, en secondes :

RRtype	TTL
DNSKEY	172800
DS	172800
NSEC3	Comme minimum SOA (5400)
RRSIG	comme RR (variable)

7. Audit de conformité

Pour vérifier l'intégrité du processus et évaluer l'état de sécurité du système de registre, l'Afnic procède à des audits internes et externes.

L'Audit de conformité s'appuie sur:

- les documents (politiques, procédures, exigences),
- les informations concernant des faits observés,
- toute information vérifiable permettant de répondre aux critères retenus pour l'audit.

7.1. Fréquence de vérification de la Conformité

L'Afnic peut décider de lancer un audit:

- en cas d'anomalies récurrentes,
- en cas de changements significatifs apportés à l'organisation, ou dans la gestion du processus.
- Pour toute autre raison relative à la compétence des personnels impliqués, à des modifications de l'équipement ou tout autre changement majeur.

7.2. Qualifications de l'auditeur

L'auditeur devra être expert en Sécurité Informatique, sur le DNS et DNSSEC.

7.3. Relations entre l'auditeur et la partie auditée

La gestion de l'audit est confiée à un Gestionnaire externe. Si nécessaire le Gestionnaire recrutera un expert pour le besoin de l'audit. Le Gestionnaire de l'audit est entièrement responsable de la conduite de l'audit.

7.4. Couverture de l'audit

Le Gestionnaire de l'audit veille à :

- À être en relation avec les autorités compétentes de l'Afnic,
- L'audité est informé et se prépare à l'audit,
- L'audité est averti par avance de l'audit et informé de la nature,
- Les procédures de suivi des résultats de l'audit sont en place.

7.5. Mesures entreprises à la suite des défaillances

Le Gestionnaire de l'audit doit immédiatement informer les responsables de l'Afnic de toutes anomalies.

7.6. Communication des Résultats

Le Gestionnaire de l'audit devra fournir un rapport écrit consignant l'ensemble des résultats au plus tard 30 jours après la fin de l'audit.

8. Dispositions légales

8.1. Frais d'utilisation

L'Afnic ne fera pas payer la gestion des publications de DS à ses bureaux d'enregistrement.

8.2. Protection des données personnelles

Conformément aux dispositions de la Charte de Nommage, toutes les données personnelles faisant l'objet d'un traitement et dont l'Afnic est le responsable du traitement s'inscrivent dans le cadre de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Loi Informatique et Libertés ».

8.3. Limites de responsabilités

Conformément à une politique de nommage qui est élaboré avec l'opérateur de registre.

Le guide des procédures pour l'enregistrement des noms de domaine est disponible ici:
https://www.afnic.fr/fr/ressources/documents-de-reference/documents-techniques/

8.4. Durée et résiliation

8.4.1. Période de validité

Ce DPS s'applique jusqu'à nouvel ordre.

8.4.2. Période de validité

Ce DPS expire à la publication de la version suivante.

8.5. Résolution des litiges

Tout conflit ou différend résultant de cet agrément sera réglé devant la Cour pertinente pour le .fr.

8.5.1. Loi applicable

La Loi française s'applique au présent document.