DPS .fr

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

26 juillet 2021 – Version 1.4

www.afnic.fr | contact@afnic.fr
Twitter : @AFNIC | Facebook : afnic.fr

IDENTIFICATION DU DOCUMENT	
Titre	DPS .fr
Hyperlien	dps-fr.pdf
Référence	DPS-FR-01
Version	1.4
Date de mise à jour	26 juillet 2021

CLASSIFICATION			
Responsable du document	Vincent Levigneron		
Niveau de classification (insérer un « X » sous le niveau requis)			
Public	Interne	Restreint	Secret
X			
À compléter pour niveau « restreint » ou « secret »			
Destinataire(s) (nom et/ou groupe) **(Liste obligatoirement nominative pour le niveau « Secret »)**			

SUIVI DES RÉVISIONS			
Version	Rédacteur	Date	Nature de la révision
V. 1	Alain Caristan, David Barou	Mars 2012	Création
V. 1.2	Alain Caristan, David Barou	Juin 2013	Mise-à-jour vers la RFC 6841, janvier 2013
V. 1.3	Vincent Levigneron	Mars 2021	Actualisation
V. 1.4	Vincent Levigneron	Juillet 2021	Changement d'algorithme des clés

APPROUVÉ PAR		
Date	Nom	Fonction
Janvier 2012	Alain Caristan	CSO

11 juin 2013	Philippe Renaut	CTO
11 mai 2021	Régis Massé	CTO
27 juillet 2021	Régis Massé	CTO

SOMMAIRE

1. Introduction

- Ce document est nommé « DPS » de la zone .fr, car il décrit l'ensemble des politiques, procédures et outils mis en œuvre pour signer la zone .fr, grâce aux extensions de sécurité du DNS (DNSSEC), en respectant le plan proposé par l'IETF dans le RFC6841 établissant un cadre de référence pour les déclarations de pratiques DNSSEC (*DNSSEC Practice Statement* en anglais)

- 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 précise les conditions de production et de déploiement du DNSSEC sur la zone .fr, permettant ainsi à l'ensemble des utilisateurs d'évaluer le niveau de sécurité de la chaîne de confiance sur cette zone. 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) sont 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 partie publique de la clé dans la hiérarchie DNS pour former, par le jeu des signatures dans les zones parentes respectives, une chaîne de confiance dont l'origine se trouve dans la zone racine.

Huit éléments principaux sont décrits dans ce document :

1. Introduction
2. Publication et référentiel
3. Besoins opérationnels
4. Mesures de sécurité non-techniques
5. Mesures de sécurité techniques
6. Signature de zone
7. Audit de conformité
8. Dispositions légales

1.2. Nom et identification du document

Titre du document : DPS .fr
Version : v1.4
Création : 01/01/2012
Mise à jour : 26/07/2021

1.3. Parties intéressées et conditions 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 :

https://www.afnic.fr/produits-services/services-associes/devenir-bureau-denregistrement-laccreditation-de-lafnic/

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 (ajout, modification et suppression) des données faisant autorité en matière de correspondance entre des noms de domaine et des zones sous la zone .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 KSK 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 empreintes 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-mêmes, les contacts désignés pour un nom de domaine ont la capacité de transmettre les empreintes de KSK et d'assurer la gestion de leurs publications grâce aux interfaces de leur bureau d'enregistrement.

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 informées 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. 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 de l'extension .fr et décrit les procédures, les mesures de sécurité, ainsi que les pratiques applicables pour l'utilisation et la gestion des clés et des signatures relatives à cette extension.

En s'appuyant sur ce DPS les différentes parties intéressées peuvent déterminer le niveau de confiance qu'ils attribuent à l'extension .fr gérée par l'Afnic et en déduire leur propre niveau de risque.

1.4. Administration

1.4.1. Organisation en charge de l'administration

Afnic

1.4.2. Contacts

Autorité de Gestion des Politiques DNSSEC :

Immeuble « le Stephenson »
1, rue Stephenson
Hall A2 - 3ème étage
78180 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 lors d'une modification importante du système ou des procédures ayant un impact significatif sur son contenu. Cette révision est effectuée par l'Administrateur du dispositif de signature (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/observatoire-ressources/documents/politique-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

La version électronique officielle du DPS est celle publiée à l'adresse :

https://www.afnic.fr/observatoire-ressources/documents/politique-de-registre/

Les notifications concernant DNSSEC sont publiées sur :

https://www.afnic.fr/observatoire-ressources/operations-maintenance/

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 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 charte de nommage élaborée avec l'opérateur de registre, disponible à cette adresse :

https://www.afnic.fr/observatoire-ressources/documents/politique-de-registre/

3.2. L'activation de DNSSEC pour les zones filles

DNSSEC est activé pour un nom de domaine par au moins la publication d'un enregistrement DS 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 correct.

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 la RFC 5910 (*Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)*).

Six (6) enregistrements DS peuvent être publiés au maximum.

3.5. Méthode pour prouver la possession de la clé privée

Le registre utilise le test ZoneMaster pour vérifier la correspondance de la clé et la bonne configuration de la zone. Le bureau d'enregistrement reste chargé de mener les contrôles 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 dépend de la mise à jour du DNS programmée par l'Afnic. Le délai maximum de mise à jour est de 10 minutes.

4. Mesures de sécurité non-techniques

4.1. Sécurité physique

L'Afnic a choisi d'héberger son infrastructure DNS dans des datacenters répondants aux exigences suivantes :

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 construction

L'Afnic a déployé ses infrastructures de production dans 2 centres de données géographiquement éloignés de son siège. Ces sites, opérés par des entités distinctes, répondent 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. Chaque centre de données dispose d'une liste (mise à jour régulièrement en fonction des mouvements de personnel à l'Afnic) qui contient l'ensemble des personnes habilitées à accéder aux installations. L'entrée est contrôlée en permanence.

Sur les sites des centres de données, 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 fournie par les systèmes d'alimentation de secours du centre de données (Classification Tier 3 de Uptime Institute (basé sur la norme ANSI : ANSI/TIA-924)). Ils ont la capacité de fournir de l'alimentation pendant 72 heures.

4.1.4. Protection contre l'eau

Les sites sont 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
- Maintenance de la norme NFS 940
- Formation régulière des équipes
- Moyens d'accueil et d'intervention pompiers

4.1.6. 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.

4.1.7. Sauvegarde hors site

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

4.2. Rôles de confiance

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 (dans la limite du périmètre désigné par le dit rôle) de produire et utiliser des clés cryptographiques.

Les rôles de confiance sont :

"Opérateurs Cryptographiques" (2 parmi 9)

- Un opérateur désigné, réalisera l'ensemble des manipulations décrites dans les procédures présentées par le maître de cérémonie sur les boitiers cryptographiques (Hardware Security Module, HSM). Une carte à puce nominative (Smart Card) est nécessaire pour s'authentifier sur le boitier.
- L'action principale de ce rôle est l'activation/désactivation de ces équipements.

"Officiers de Sécurité" (2 parmi 9)

Les Officiers de Sécurité ont accès aux menus de configuration système du HSM (adressage IP, configuration de l'heure, ...). Ils assurent la configuration initiale des boitiers et ne devraient plus avoir à intervenir une fois ceux-ci mis en service. Tout comme les Opérateurs Cryptographiques, une carte à puce nominative est nécessaire pour valider l'accès à ces menus dédiés. Les Officiers de Sécurité Afnic sont aussi Opérateurs Cryptographiques.

"Officiers Cryptographiques" (2 parmi 9)

Les Officiers Cryptographiques ont accès aux différents menus du boitier concernant les opérations sur les clés (choix des algorithmes, backup/restore de SMK, suppression des clés applicatives, ...). Tout comme pour les autres intervenants sur les HSM, une carte à puce nominative donne accès à une série de menus spécifiques. Les Officiers Cryptographiques interviennent surtout lors des cérémonies de clés en réalisant différentes manipulations sur les boitiers, sous le contrôle du maître de cérémonie.

“Porteurs de Clés” applicatives (1 parmi 4)

Les clés applicatives sont stockées sur des clés USB chiffrées accessibles en ayant connaissance d’un code d’accès spécifique. Ce sont les Porteurs de Clés qui donneront cet accès lorsque les Officiers Cryptographiques auront besoin de faire un transfert des clés applicatives du HSM vers ces clés USB (et vice versa). Ce sont les Officiers Cryptographiques qui autoriseront le branchement de ces clés USB sur les HSM.

“Pupitreurs”

Ils n’ont aucun accès au HSM, par contre ce sont eux qui maîtrisent le fonctionnement des applications et scripts nécessaires au bon déroulement de la cérémonie. Ils peuvent se connecter aux différents serveurs sur lesquels les cérémonies de clés seront réalisées et apporter d’éventuelles modifications sur les programmes mis en jeu (par exemple lors de changement d’algorithme, conformément aux instructions fournies par l’Administrateur du système de signature). Ils exécutent les commandes suivant le scénario mis en place par le Maître de Cérémonie.

“Administrateur du dispositif de signature”

Est le responsable des fichiers de configuration et des différents scripts de la solution de signature. Il assure aussi la mise à jour de ce document.

“Le Maître de Cérémonie” (1 parmi 3)

Ils préparent l’ensemble des cérémonies en construisant un scénario à partir des procédures Afnic. Ils donnent l’accès au coffre-fort et distribuent l’ensemble des cartes ainsi que les clés USB contenant les clés applicatives, aux différents acteurs de la cérémonie. Le coffre-fort contiendra aussi la clé physique nécessaire pour activer le HSM utilisé lors des cérémonies de clés. Ils sont responsables de l’arrêt ou de la poursuite de la cérémonie en cas de problème ou d’événement non prévu. En fin de cérémonie ils récupèrent l’ensemble des éléments pour les re-déposer dans le coffre-fort.

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 au système devra présenter une pièce d'identité valide.

4.2.3. Séparation des rôles lors de la cérémonie

Une seule et même personne ne peut simultanément tenir plusieurs mêmes rôles de confiance (Officier de Sécurité, Opérateur Cryptographique, Officier Cryptographique).

Un Pupitreur peut être Porteur de Clés mais ne peut pas occuper un des rôles donnant accès aux HSM (Opérateur Cryptographique, Officier de Sécurité, Officier Cryptographique).

Un Officier de Sécurité peut être en même temps un Opérateur Cryptographique.

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.

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 majeure 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.

Seuls les tiers qualifiés pourront avoir l'un des rôles de confiance décrits en 4.2.1.

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. Journalisation

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 logs

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

4.4.3. Période de conservation des informations des logs

Les informations de log sont conservées dans le système, puis elles sont archivées pendant au minimum 10 ans.

4.4.4. Protection des informations des logs

Toutes les informations des logs 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 logs

Toutes les informations des logs sont sauvegardées et stockées dans un endroit sûr indépendant du système.

4.4.6. Système de Collecte des logs

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

4.4.7. Information sur l'exploitation des logs

Le personnel concerné est informé de l'exploitation des logs. Le personnel n'est pas autorisé à consulter les données des logs.

4.4.8. Analyse des vulnérabilités

Toutes les anomalies dans les informations des logs 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 et corriger les effets qu'il a eu ou pourrait avoir eu,
- de prendre les mesures adéquates pour empêcher qu'il ne se reproduise
- de documenter les informations relatives à la gestion des incidents

Dans le cas où un incident conduirait à établir des soupçons sur une compromission de clé, une rotation immédiate de la clé devra être réalisée 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 (conformément aux procedures décrites dans la RFC 6781) :

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 la zone immédiatement re-signée. 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, peu probable, compte tenu des différents mécanismes de sauvegarde mis en œuvre, de perte d'une KSK, un changement de clé KSK se fera sans chevauchement entre la clé perdue et une nouvelle clé.

À 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 ancre de confiance devront ajouter la nouvelle KSK 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) destiné à assurer la continuité 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 planifiée et avec information préalable du public.

Si l'exploitation d'une zone doit être transférée à une tierce partie, l'Afnic participera à cette transition de manière à la rendre le plus fluide possible.

5. Mesures de sécurité techniques

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 matériel (HSM) qui est opéré par des personnels qualifiés et disposant des rôles de confiance appropriés.

La génération des clés est effectuée via des commandes d'OpenDNSSEC. Leur réplication sur les différents boitiers se fait en présence de deux Officiers Cryptographiques, deux Opérateurs Cryptographiques, un Porteur de Clés, un Pupitreur 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 clés est tracée dans des logs, dont une partie est enregistrée de façon électronique et une partie est consignée sur papier par le Maître de Cérémonie.

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 Cryptographiques et les Opérateurs Cryptographiques.

L'Officier Cryptographique est responsable de la publication de la partie publique de la KSK de manière sécurisé telle que définie au 2.1.

Le Pupitreur 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 qualité comprend la vérification de la longueur de clé.

5.1.4. Utilisation des clés

Les clés générées pour DNSSEC ne sont jamais utilisées pour 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 2 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 d'utiliser les 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 matériel (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 des clés USB elles même chiffrées (chiffrement matériel XTS-AES 256 bits de classe militaire) pour ensuite être conservées dans un coffre-fort.

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 clé USB 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 distribuées entre les différents HSM lors de la cérémonie de clés via un logiciel idoine (AEP load-balancer) assurant ainsi une redondance et une continuité de service dans le cas où un boitier devait tomber en panne ou deviendrait momentanément indisponible (panne électrique, réseau, ...).

5.2.8. Activation des clés Privées

Les clés privées sont activées de façon automatique par le dispositif de gestion de clés (OpenDNSSEC en l'occurrence).

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 lors de la cérémonie de clés suivante.

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 de 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. Ordinateurs et serveurs

Les ordinateurs et serveurs impliqués dans la délivrance des services de Registre et l'administration de ces services bénéficient des mesures de sécurité suivantes :

- application du moindre privilège
- accès distants protégés par une double authentification
- chiffrement des flux réseau
- journalisation et centralisation des événements de sécurité générés sur ces composants
- application des bonnes pratiques en matière de configuration sécurisée
- audits de sécurité réguliers

5.6. 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 applications

Tout le code source est conservé dans un système de gestion de source. 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 documentant notamment les exigences de sécurité,
- Une volonté permanente de réduire la complexité,
- Des tests systématiques automatisés et tests de non régression,
- Fourniture de version de logicielles distinctes,

- Un suivi constant de la qualité et de la correction des défauts constatés.

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 aux standards de l'IETF, être publiques et efficients pour toutes les parties concernées.

Les algorithmes actuellement en vigueur à l'AFNIC sont ECDSA avec une longueur de clé unique de 512 bits pour les ZSK et KSK.

6.2. Authentification des dénis d'existence

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

6.3. Roulement des clés

En mode automatique, la rotation de la ZSK est effectuée tous les 60 jours

En mode automatique, la rotation de la KSK est effectuée tous les 2 ans.

D'autres rotations peuvent être programmées en cas d'opérations de maintenance spécifiques, telles qu'un changement d'algorithme.

6.4. 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 lors de l'introduction d'une nouvelle clé ou lorsque le sel est modifié. Lors de cette opération, la durée de vie des signatures est répartie uniformément afin que l'expiration de celles-ci ne se produise pas le même jour.

Les signatures ont une durée de vie maximale de 2 mois.

6.5. 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 les clés publiées vie les enregistrements de type DNSKEY avant la publication des informations de zone sur l'Internet.

6.6. Vérification des "Resource Records"

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

6.7. 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. Dispositions légales

7.1. Frais d'utilisation

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

7.2. 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 ».

7.3. Durée et résiliation

7.3.1. Période de validité

Ce DPS expire à la publication de la version suivante.

7.4. Résolution des litiges

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

7.4.1. Loi applicable

La Loi française s'applique au présent document.