DPS

Politique de signature des domaines .CM et conditions de mise en œuvre

(Version 1.0 – 15/05/2025)
Gestion du document - Identification du document

Responsable du document
Gestionnaire du .CM

Titre	DPS.cm
Hyperlien	dps-cm.pdf
Référence	DPS-CM-01
Version	1.0
Dernière mise-à-jour	15/05/2025

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

Approuvé par

Date	**Nom**	**Fonction**
20/05/2025	Prof. EBOT EBOT ENAW	Directeur Général de l'ANTIC

Révisions

Version	Author	Date	Révision
V1	Équipe de ANTIC	24/04/2025	Création

1. Introduction

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

Ce document fournit les éléments permettant à l'ensemble des utilisateurs de la zone .cm, d'évaluer le niveau de sécurité de la chaîne de confiance sur le « .cm ». Il présente également les procédures et infrastructures mises en œuvre pour la sécurité du registre.
Le présent document est rédigé conformément à la RFC 6841 de l'IETF qui présente le canevas des déclarations et politiques d'opérations DNSSEC.

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 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.cm
Version : v1.0
Création : 24/04/2025
Mise à jour : 15/05/2025

1.3. Parties concernées et condition d'application

Les rôles et délégations suivants ont été identifiés.

1.3.1. Registre

L'ANTIC (Agence Nationale des Technologies de l'Information et de la Communication), est responsable de la gestion de la zone « .cm ». Cela signifie que l'ANTIC administre, ajoute, modifie et supprime des données pointant des noms de domaine vers des zones faisant autorité sous « .cm ». Cela signifie aussi que l'ANTIC administre et fait évoluer l'infrastructure technique assurant performance et résilience à la zone .cm à son niveau.
De la même manière, l'ANTIC, gère les clés permettant de signer cryptographiquement les enregistrements de la zone .cm, selon les modalités et les procédures décrites ci-dessous.
L'ANTIC s'engage à signer régulièrement avec sa ZSK le résumé cryptographique des KSKs des délégations signées sous «.cm ».

1.3.2. Les bureaux d'enregistrement

Le bureau d'enregistrement ou Registrar 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 *Délégation Signer*, à la demande du titulaire ou du contact technique du nom de domaine correspondant.
La procédure de demande d'agrément pour devenir Registrar du « .cm » est publiée sur la page https://nic.cm/devenir-bureau-denregistrement/ et la liste des Registrars agrées par l'ANTIC est disponible sur la page https://nic.cm/liste-des-registrars/.

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 informées de toute mise à jour de l'ANTIC sur ses zones si la clé de .cm est utilisée comme Trust Anchor. Elles doivent également se tenir informées 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 que la façon dont l'ANTIC 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'ANTIC. Ce DPS est exclusivement applicable, au niveau des extensions « .CM » et décrit les procédures, les contrôles de sécurité, ainsi que les pratiques applicables pour l'utilisation et la gestion des clés et des signatures pour les extensions gérées par l'ANTIC.

En s'appuyant sur ce DPS les différentes tierces parties peuvent déterminer le niveau de confiance qu'ils attribuent aux extensions gérées par l'ANTIC 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

ANTIC

1.4.2. Contacts

Autorité de Gestion des Politiques DNSSEC : Agence Nationale des Technologies de l'Information et de la Communication
Bastos - Rue Ambassade de Chine
Yaoundé

E-mail : dotcm@antic.cm
Téléphone : +237 694 405 868

1.4.3. Procédures de modifications des spécifications

Le DPS de l'ANTIC est révisé sur une base annuelle ou en cas de force majeure. Cette révision est effectuée par le Responsable du DPS du « .cm ».
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://nic.cm/documentation/**

Seule la version la plus récente du DPS est applicable.

2. Publication et référentiel

2.1. Publications sur le site de l'ANTIC

L'ANTIC publie les informations importantes sur DNSSEC pour chacune de ses extensions à l'adresse https://nic.cm/actualites/
La version électronique officielle du DPS est celle publiée à : https://nic.cm/documentation/

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 « .cm » 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 : https://nic.cm/2018/01/30/enregistrement-nd/

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 .cm, 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'ANTIC 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'ANTIC.

3.4. Enregistrement des empreintes de clés (DS)

L'ANTIC accepte les demandes de publication de DS via la plateforme de gestion des noms de domaine soit par l'interface graphique soit par connexion 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)).

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 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 un bureau d'enregistrement via l'interface graphique ou via une connexion EPP. 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 « .cm ».
Le Bureau d'Enregistrement exécute la demande de retrait en appliquant les procédures définies par l'ANTIC.
Le temps nécessaire à la suppression d'un enregistrement DS de la zone « .cm » après avoir reçu la demande de suppression dépend de la mise à jour du DNS programmée par l'ANTIC. Le délai maximum de mise à jour est de 60 minutes.

3.6.3. Procédure d'urgence pour un titulaire

Le titulaire d'un nom de domaine sous une extension gérée par l'ANTIC 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 de modification des enregistrements via le registre.

4. Contrôle des accès, opérations et de gestion

4.1. Contrôle physique

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

Afin d'assurer un niveau de protection optimale, le site bénéficie d'une architecture de sécurité d'accès multifactorielle, comprenant :

- Protocole d'Authentification et d'Inspection des Accès : Mise en œuvre d'un processus de checking systématique pour tout intervenant (personnel interne, prestataires, visiteurs) transitant par les points d'entrée et de sortie. Ce protocole inclut la vérification d'identité, l'inspection des effets personnels, la palpation de sécurité (le cas échéant), et la validation des

autorisations d'accès préalables. L'exécution de ce protocole est assurée par un service de sécurité dédié ;

- Surveillance Active du DataCenter (DC) : Déploiement d'un système de rondes de sécurité continues (24/7) au sein du DataCenter, complété par une présence humaine permanente (24/7) pour une réactivité immédiate ;

- Système d'Authentification Biométrique : Intégration d'un système de reconnaissance biométrique pour le contrôle d'accès aux zones sensibles ;

- Système d'Identification par Badge Individuel Nominatif : Utilisation de badges d'accès nominatifs individuels comme mécanisme d'identification et de contrôle d'accès.

- Système de Vidéosurveillance Intelligent (CCTV NVR) : Infrastructure de vidéosurveillance (Closed-Circuit Television Network Video Recorder) enrichie par des caméras infrarouges, assurant une surveillance et un enregistrement numérique continu des locaux ;

- Mur d'Images pour la Supervision Vidéo Temps Réel : Implémentation d'un wallvidéo permettant la visualisation en temps réel et l'archivage des flux vidéo issus des caméras de surveillance. Les données d'enregistrement sont conservées pour une période pouvant atteindre plusieurs mois, en adéquation avec les politiques de rétention des données ;

- Architecture de Sécurité Périmétrique Segmentée : Afin de renforcer le contrôle d'accès et la sécurité du périmètre, trois points de contrôle d'accès distincts sont stratégiquement positionnés entre l'entrée principale du site et la zone dédiée aux visiteurs.

4.1.1. Emplacement et construction

L'ANTIC a procédé à une délocalisation stratégique de son infrastructure, géographiquement éloignée de son siège social. Ce positionnement distinct obéit à une architecture redondante et à des impératifs de conformité avec les spécifications du standard Tier 3. Cette disposition normative assure un niveau élevé de résilience et une disponibilité accrue (High Availability - HA) des systèmes critiques hébergés. Le Plan de Continuité d'Activité (PCA) de l'ANTIC est aligné avec les meilleures pratiques ITIL et les normes ISO 27001. Il 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 est assuré par un contrôle multicouche rigoureux. L'accès à ce périmètre sécurisé est strictement limité au personnel accrédité, dont l'habilitation est préalablement établie et régulièrement réévaluée.
La surveillance du point d'entrée principal est assurée en continu par un agent de sécurité physique, agissant comme premier rempart contre toute tentative d'intrusion non autorisée.
Le passage du seuil du Datacenter est conditionné par les exigences suivantes :

- Authentification biométrique multi facteur (MBFA) pour le personnel interne : Ce mécanisme avancé d'identification repose sur la vérification de caractéristiques biologiques uniques, garantissant une identification positive et robuste de chaque individu autorisé ;

- Registre d'accès horodaté pour le personnel et les tiers autorisés : Tout accès physique est consigné dans un registre numérique sécurisé, horodaté avec précision, permettant de maintenir une piste d'audit détaillée des entrées et sorties ;
- Procédure d'autorisation formelle et documentée pour les intervenants externes : L'accès des personnels non internes est conditionné par la présentation d'une autorisation préalable émise par les autorités compétentes, spécifiant la durée, le périmètre et l'objet de leur intervention.
- Système de badges d'identification nominatifs pour le personnel : Chaque membre du personnel autorisé est doté d'un badge unique intégrant une technologie de lecture électronique, permettant un contrôle d'accès précis et l'enregistrement des mouvements au sein du Datacenter.

En complément de ces mesures de sécurité périmétrique, une gestion méticuleuse des accès logiques aux serveurs est implémentée. Un journal d'audit détaillé est maintenu pour chaque interaction avec les ressources serveur, assurant une traçabilité exhaustive des opérations critiques. Cette fiche de contrôle d'accès logique documente de manière exhaustive :

- L'identifiant unique de l'utilisateur authentifié (UID) ayant accédé au serveur ;
- L'horodatage précis (date et heure) de la session d'accès ;
- L'adresse IP source de la connexion et l'identifiant du serveur cible ;
- La nature précise des commandes exécutées ou des actions entreprises (e.g., maintenance corrective, application de patch de sécurité, redémarrage).
- La justification technique ou fonctionnelle motivant l'accès ;
- L'enregistrement de toute anomalie, alerte ou incident de sécurité détecté durant la session.

Ce journal d'audit constitue un artefact critique pour la traçabilité des activités et l'attribution des responsabilités. Il permet la détection proactive et l'analyse forensique de toute activité potentiellement malveillante ou non conforme aux politiques de sécurité. Les journaux d'audit sont stockés de manière sécurisée, conformément aux exigences réglementaires et aux meilleures pratiques, et sont soumis à des revues périodiques dans le cadre d'audits de sécurité réguliers.

4.1.3. Puissance et climatisation

L'intégrité opérationnelle de l'infrastructure est intrinsèquement liée à la robustesse et à la redondance de son système d'alimentation électrique. Afin de garantir une continuité de service maximale, l'architecture d'alimentation électrique repose sur une topologie multi-sources.

L'architecture de secours, conforme aux spécifications du niveau Tier 3 de Uptime Institute (basé sur la norme ANSI/TIA-924), intègre une commutation automatique vers les sources secondaires en cas de défaillance de l'alimentation primaire. Cette conception garantit une autonomie électrique minimale de 72 heures en pleine charge, renforçant la résilience de l'infrastructure face à des interruptions prolongées du réseau principal.

Climatisation

Le maintien des conditions thermiques est assuré par un système de refroidissement redondant, composé de huit unités de climatisation de précision.

Ces unités, présentant une capacité frigorifique nominale individuelle comprise dans la plage de 5000 à 7000 frigories par heure (F/h), sont orchestrées selon un protocole de permutation optimisé. Cette configuration implémente une redondance de type N+1, voire supérieure, permettant de tolérer la défaillance d'une unité sans compromettre la capacité de refroidissement globale.

De plus, cette approche dynamique de gestion de la charge thermique permet d'optimiser l'efficacité énergétique du système en modulant la puissance frigorifique active en fonction des charges

thermiques instantanées générées par l'équipement informatique.

4.1.4. Protection contre l'eau

Le site du Datacenter est situé dans une zone non inondable. Néanmoins une stratégie de protection multicouche a été déployée afin de mitiger les risques liés à l'eau. Cette stratégie repose sur les mesures suivantes :

- Un réseau distribué de capteurs d'humidité a été stratégiquement positionné au sein du faux plancher et à l'ensemble des équipements critiques. Cette instrumentation permet une surveillance en temps réel et une alerte précoce en cas d'anomalie,
- L'architecture du faux plancher favorise l'évacuation des liquides minimisant ainsi le risque de contact prolongé avec les infrastructures IT.

4.1.5. Protection incendie

Le site répond aux normes de sécurité industrielles

Un système de détection incendie avancé est déployé dans l'ensemble du Datacenter. Ce système comprend :

- Des détecteurs de fumée et de flammes sont installés et stratégiquement positionnés pour une couverture optimale des lieux. Ces détecteurs déclenchent une alerte en cas de détection d'un événement suspect, permettant ainsi une intervention rapide ;
- Des extincteurs de classes A (feux de matériaux solides), B (feux de liquides et gaz inflammables) et C (feux d'origine électrique), d'une capacité nominale de 10 kg chacun, sont distribuées selon une cartographie des risques et une analyse des besoins spécifiques des différentes zones du Datacenter. Cette distribution stratégique garantit un accès rapide aux agents extincteurs appropriés en cas de départ de feu.

4.1.6. Stockage des données

Le stockage est fait suivant la politique de stockage de l'ANTIC. 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'ANTIC.

4.1.8. Sauvegarde hors site

Les données de l'ANTIC sont répliquées automatiquement sur un site distant.

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.

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'ANTIC 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

Deux personnes au moins sont nécessaires pour chaque tâche.

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'ANTIC, 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'ANTIC 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'ANTIC
- Formation à la gestion des noms de domaine
- Formation à la théorie du DNS et de DNSSEC
- Information sur la politique de sécurité

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 jouant 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 pour les dommages engendrés.

4.3.7. Exigence envers les contractants

Dans certaines circonstances, l'ANTIC 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'ANTIC 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 procédures 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'ANTIC.
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) sont analysés 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 endroits 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 à la suite d'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 dû à des renseignements inexacts,
- toute atteinte à la sécurité.

Tous les incidents sont traités conformément aux procédures de l'ANTIC. 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 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 prépubliée.
A ce moment, l'information sera notifiée par les canaux indiqués au point 2.1.

Les tierces parties utilisant une des KSK de l'ANTIC 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'ANTIC a un PCA (Plan de Continuité d'Activité) qui assure 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 besoins 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'ANTIC 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'ANTIC 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'OpenDNSSEC. Leur réplication sur les boitiers de secours se fait en présence des personnes dûment appointés. Ces personnes doivent être présentes pendant toute la durée de l'opération.

L'ensemble de la procédure de génération de clé est tracé par des logs.

5.1.2. Distribution de clés publiques

N/A

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'ANTIC 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 au moins aux exigences du standard FIPS 140-2 Niveau 2 (Federal Information Processing Standards : *Security Requirements for Cryptographic Modules*).

5.2.2. Contrôle multi - personnes des clés Privées

Le Registre n'applique pas le contrôle multi-personnes pour l'activation du module. L'accès physique est opéré par l'Administrateur des Systèmes qui est le seul habilité.

5.2.3. Entiercement de clés (Key escrow)

L'ANTIC 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'ANTIC.

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 qu'aux personnes autorisées 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 HSM 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 aspects 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 pour activer le HSM.

5.4.1. Génération et installation des Données d'Activation
Les codes d'authentification sont créés en respectant une règle de différentiation maximale des séquences caractères.

5.4.2. Protection des données d'activation
La protection des données d'activation est faite de la meilleure façon qu'il soit. En cas de suspicion de compromission de ces données, le Responsable désigné en charge des données d'activation 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 dans le cadre du PCA de l'ANTIC 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 pares-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'ANTIC.

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'ANTIC 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'ANTIC diligente des audits réguliers sur la sécurité du dispositif de signature. L'ANTIC 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 (1 an pour la KSK, 1 an pour la ZSK).
Les algorithmes doivent répondre au standard de l'IETF, être publiques et efficientes pour toutes les parties concernées.
L'algorithme ECDSA est actuellement utilisé avec une longueur de 256 bits actuellement pour la KSK et la ZSK.

6.2. Authentification des dénis d'existence

Le Registre utilise les enregistrements NSEC3 tels que spécifiés dans le RFC 5155.

6.3. Signature Format

Les signatures sont générées par une opération ECDSA en utilisant une fonction de hachage cryptographique basée sur SHA2 (RSA/SHA-256, RFC 6605).

6.4. Roulement des clés

La rotation de la ZSK est effectuée selon le besoin (environ une fois par an)
La rotation de la KSK est effectuée selon le besoin (environ une fois par an).

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

La zone est signée de manière incrémentale à chaque publication.
Les signatures ont une durée de vie de 28 jours et sont rafraîchies après 14 jours

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	3600
DS	3600
NSEC3	Comme minimum SOA (3600)
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'ANTIC 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'ANTIC 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 la Structure en charge de l'Audit de Sécurité à l'ANTIC, en collaboration avec la Structure en charge de la cryptographie et de la certification électronique. Si nécessaire, un expert externe peut être recruté pour un audit sous la supervision du Gestionnaire 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'ANTIC,
- 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.

Le Gestionnaire de l'audit s'assurera également que l'audit couvre les points suivants :

- toute la documentation et les enregistrements ;
- les termes des contrats et les prestations ;
- la conformité avec les lois et règlements applicables ;
- le contrôle physique et logique des installations abritant le système ;
- les ressources humaines et leur organisation ;
- le contrôle des équipements et des logiciels qui y sont installés ;

le contrôle de conformité des clés, des certificats, du chiffrement et de la signature électronique.

7.5. Mesures entreprises à la suite des défaillances

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

Frais d'utilisation

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

8.1. Protection des données personnelles

Les opérations de gestions du « .cm » sont menées dans le respect des lois et règlements en vigueur au Cameroun et en particulier la loi n°2024/017 du 23 décembre 2024 relative à la protection des données à caractère personnel.

8.2. Limites de responsabilités

Conformément à une politique de nommage qui est élaboré par le registre.
Le guide des procédures pour l'enregistrement des noms de domaine est disponible ici : https://nic.cm/2018/01/30/enregistrement-nd/

8.3. Durée et résiliation

8.3.1. Période de validité

Ce DPS s'applique jusqu'à nouvel ordre.

8.3.2. Période de validité

Ce DPS expire à la publication de la version suivante.

8.4. Résolution des litiges

L'ANTIC dispose d'un Comité de règlement des différends relatifs aux noms de domaine « .cm ».
En cas de non-acceptation des résolutions prises par ce Comité ou faute d'être parvenues à un accord à l'amiable, les parties peuvent saisir la juridiction camerounaise compétente. Toutefois, la décision prise par le Comité sera appliquée, sauf ordre contraire du juge, jusqu'à la notification à l'ANTIC de la décision de justice devenue définitive.

La politique de gestion de litiges élaborée par l'ANTIC et publiée sur la page https://nic.cm/documentation/.

8.5. Loi applicable

La présente Déclaration des Pratiques de Signature est expressément élaborée, appliquée et interprétée selon les Lois et Règlements en vigueur au Cameroun, bien que les activités qui en découlent puissent avoir des effets juridiques en-dehors du territoire national.