POLITIQUE DE CERTIFICATION

AC SUNU ROOT

Groupement d'Intérêt Economique
Capital social: 100 000 000 FCFA
RC n° SN DKR 2002B1149
NINEA 21516952G6
1, Allées Thierno Saïdou Nourou TALL , Point E
Immeuble ORBUS ■ Dakar, Sénégal

■ BP 6856 Dakar Etoile

■ Tel (+221) 33 859 39 99 ■ Fax (+221) 33 824 17 24

■ www.gainde2000.sn

Nature du Document	Gouvernance
Référence	PC_AC_SUNU_ROOT
Date	Oct 2025
Emetteur	GAINDE 2000
Destinataires	Public
Version	**1.5**
Nombre de page	46

Date	Auteur	Version	Evolutions
17/07/2023	Responsable Contrôle, Référentiel Documentaire & Projet	**1.0**	Première version
01/09/2025	Responsable Pole PKI	**1.3**	
15/01/2026	Responsable Pole PKI	**1.5**	

TABLE DE MATIERES

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions de la loi n°2008-09 du 25 janvier 2008 sur le droit d'auteur et les droits voisins, qui régissent la propriété littéraire et artistique et les droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de GAINDE 2000. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisées préalablement par écrit par GAINDE 2000 ou ses ayants droits, sont strictement interdites.

La loi sur le droit d'auteur et les droits voisins autorise, aux termes de l'article 40 , d'une part, que « l'auteur ne peut interdire la reproduction destinée à un usage strictement personnel et privé » et, de l'article 44 d'autre part, les analyses et les courtes citations conformes aux bons usages dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (article 35 de la loi sur les droits d'auteur et les droits voisins).

La représentation ou la reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée, notamment par les articles 142 et suivants de la loi sur les droits d'auteur et les droits voisins.

La Déclaration des Pratiques de Certification, propriété de la société GAINDE 2000 peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.

1. INTRODUCTION

1.1. PRESENTATION GENERALE

Le métier historique de GAINDE 2000 est de concevoir des solutions innovantes et de les héberger sur son propre centre de production informatique. GAINDE 2000 opère ainsi depuis plus de 20 ans des systèmes douaniers et de facilitation au Sénégal.

Ce positionnement confère à GAINDE 2000 une parfaite connaissance des problématiques et des enjeux de l'hébergement de solutions transactionnelles à temps réel à fort trafic. Cette connaissance permet aujourd'hui à nos experts de travailler main dans la main avec les équipes de nos clients ou partenaires, éditeur de solutions logicielles et matérielles pour assurer une meilleure intégration et par conséquent une meilleure qualité de service.

De plus, ce positionnement permet à GAINDE 2000 d'avoir une relation contractuelle et financière vertueuse vis-à-vis de ses clients. Ainsi, GAINDE 2000 s'efforce de proposer un service répondant parfaitement aux attentes, tant par sa couverture fonctionnelle que par sa performance et sa disponibilité.

L'acquisition de l'infrastructure d'autorité de certification permet aujourd'hui à GAINDE 2000 d'exercer les activités de prestataire des services de certification et d'horodatage. En conséquence, GAINDE 2000 renforce son offre par l'acquisition et la mise en œuvre d'une solution de signature centralisée complétant son infrastructure pour opérer les activités d'opérateur de signature.

Aujourd'hui, GAINDE 2000 dispose de toutes les solutions permettant de garantir à ses clients et partenaires, une couverture parfaite des besoins de confiance numérique d'où l'acquisition d'une IGC.

Une Infrastructure à Clé Publique (IGC) est un ensemble de moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques.

La mise en place d'une IGC, nécessaire à la sécurité et à la confiance, ouvre une palette de services à valeur ajoutée pour les transactions électroniques (par exemple : courrier électronique, transactions commerciales, télé procédures, protection locale des données, etc.).

Ils ont pour fonctions d'assurer :

- l'intégrité des informations,
- l'identification et l'authentification de l'émetteur,
- la non répudiation de la transaction / opération
- et la confidentialité.

Cette politique de certificat est le principal énoncé de politique régissant les Autorités de certification au sein de l'infrastructure à clé publique Gainde2000. Il énonce les aspects commerciaux, juridiques, techniques et les exigences relatives à l'approbation, à la délivrance, à la gestion, à l'utilisation, à la révocation et au renouvellement.

Ces exigences protègent la sécurité et l'intégrité de la PKI de Gainde2000 et comprennent un ensemble unique de règles qui s'appliquent de manière cohérente à toutes les autorités de certification de manière à assurer une confiance uniforme dans leur ensemble.

L'AC Sunu Root se réserve le droit de ne pas conclure d'accord de certification croisée avec une autorité de certification externe.

L'AC Sunu Root sera assujetti aux lois et règlements en vigueur sur le territoire sénégalais et qui touchent à l'application, l'élaboration, l'interprétation et la validité des politiques de certification mentionnées dans le présent document.

L'Autorité de Certification Racine, dénommée *AC Sunu Root*, est exploitée et opérée par GAINDE 2000.

1.2. IDENTIFICATION DU DOCUMENT

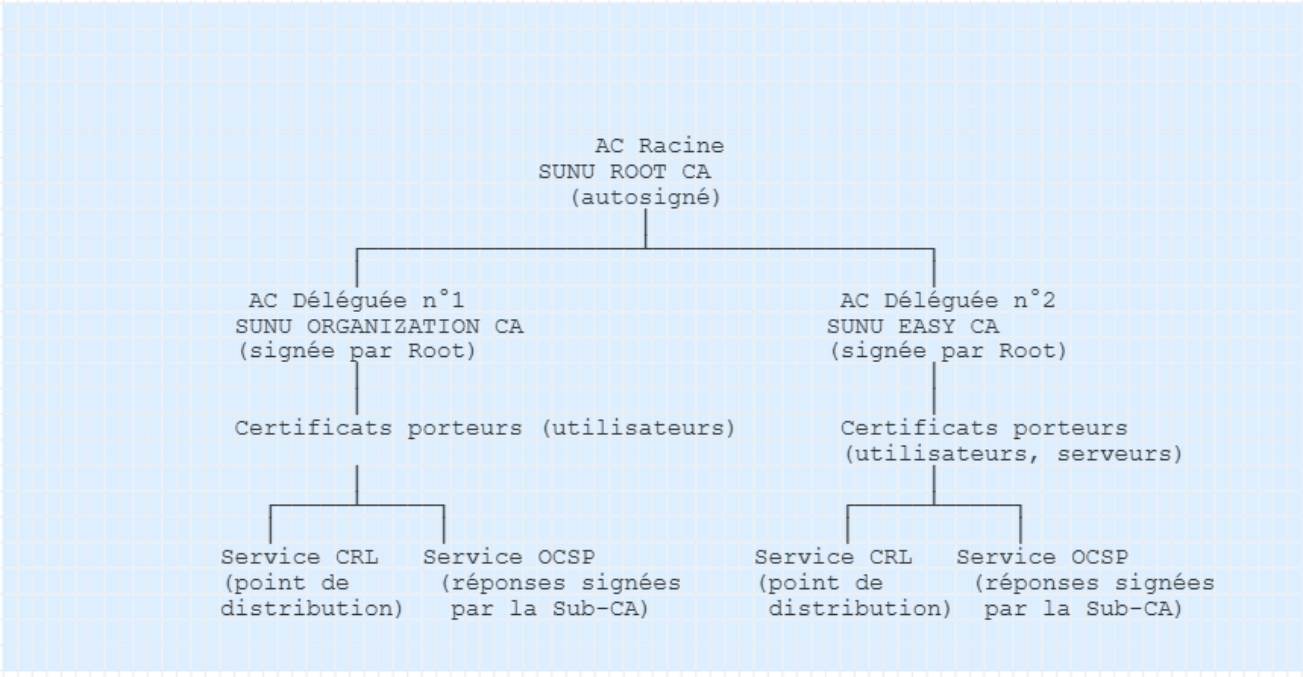
La désignation du numéro d''identification d'objet (OID) pour la présente politique est :

AUTORITE DE CERTIFICATION SUNU ROOT	
OID de la Politique de Certification	**1.3.6.1.4.1.45491.2.1**

1.3. ENTITES INTERVENANT DANS L'IGC

Les entités intervenantes dans l'IGC de GAINDE2000 sont :

- Autorité de certification Sunu Root,
- Autorités de certification Déléguées,
- Autorité d'enregistrement,
- Mandataire de certification,
- Porteur de certificat



2. DOMAINE D'APPLICATION

2.1. DOMAINES D'UTILISATION APPLICABLES

L'objectif principal de cette politique est de permettre une administration électronique efficace et sécurisée. , tout en répondant aux préoccupations des parties utilisatrices au sujet de la fiabilité des certificats.

La présente PC couvre les certificats suivants :

- Le certificat de l'ACR de signature de certificats d'AC et de signature de la Liste des certificats d'AC Révoqués (LAR), des ACD rattachées à l'ACSR (autosigné), utilisé pour signer les certificats de la hiérarchie d'AC (certificats des AC filles) et pour signer les LAR ;
- Les certificats des AC filles (signature des certificats porteurs et des LCR) rattachées à l'ACSR (signés par l'ACSR) ;
- Le cas échéant, les certificats de signature des réponses OCSP pour les porteurs des ACD considérées (un certificat ACD OCSP Responder par ACD, signé par l'ACD correspondante).

Par ailleurs, Gainde2000/Confiance Factory peut être amené à émettre des certificats de test. Ces certificats de test sont identifiés comme tels dans leur DN. Ils ne sont couverts par aucune garantie par Gainde2000/Confiance Factory et ils ne doivent en aucun cas être utilisés à d'autres fins qu'à des fins de test.

L'Autorité de Certification agit dans le cadre d'une gouvernance indépendante, garantissant l'impartialité des décisions relatives à l'émission, à la gestion et à la révocation des certificats. Cette activité est exercée sans influence ou pression financière, commerciale ou politique susceptible d'affecter l'intégrité, la disponibilité ou la sécurité des services de confiance.

2.2. DOMAINES D'UTILISATION INTERDITS

Toute utilisation d'un certificat autre que celles prévues dans le cadre de la présente PC et des conditions générales d'utilisation (cf. CGU) est interdite. En cas de non-respect de cette interdiction, la responsabilité de Gainde2000/Confiance Factory ne saurait être engagée.

3. REFERENCES INFORMATIVES

3.1. IDENTIFICATION ET AUTHENTIFICATION

3.1.1. NOMMAGE

3.1.2. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme [X.500].

Dans chaque certificat conforme à la norme [X.509] l'ACR (Issuer) et l'ACD (Subject) sont identifiés par un "Distinguished Name" (DN) de type [X.501].

Des règles sur la construction du DN de ces champs sont précisées dans la DPC.

3.1.3. Nécessité d'utilisation de noms explicites

Le contenu des champs de nom Subject doit avoir un lien explicite avec l'ACD authentifiée.

Les noms utilisés dans les champs "issuer" et "subject" d'un certificat d'AC sont explicites dans le domaine de certification de Gainde2000 (utilisation des identifiants nationaux de structure NINEA/RCCM, identification du type de certificats couverts par l'AC,...).

3.1.4. Anonymisation ou pseudonymisation des identités

Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes. L'identifiant de l'entité dans son certificat ne peut être un pseudonyme.

3.1.5. Règles d'interprétation des différentes formes de nom

Le document [PROFILS] fournit des règles à ce sujet.

3.1.6. Unicité des noms

Les noms distinctifs sont uniques pour toutes les entités identifiées d'une ACD.

3.1.7. Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles 11 et suivants de l'Accord portant révision de l'Accord de Bangui du 02 mars 1977 instituant l'Organisation Africaine de la Propriété Intellectuelle et ses modifications ultérieures appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

L'ACSR ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par les clients et bénéficiaires des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.

3.2. DEFINITIONS ET ACRONYMES

3.2.1. Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- AC : Autorité de Certification
- AE : Autorité d'Enregistrement
- AGP : Autorité de Gestion des Politiques
- AH : Autorité d'Horodatage
- DN : Distinguished Name
- DPC : Déclaration des Pratiques de Certification
- ETSI : European Telecommunications Standards Institute
- IGC : Infrastructure de Gestion de Clés.
- LAR : Liste des certificats d'AC Révoqués
- LCR : Liste des Certificats Révoqués
- OID : Object Identifier
- PC : Politique de Certification
- PSCE : Prestataire de Services de Certification Electronique
- PSCo : Prestataire de Services de Confiance

- RSA : Rivest Shamir Adelman
- SP : Service de Publication
- SSI : Sécurité des Systèmes d'Information
- URL : Uniform Resource Locator
- TSP : Trust Services Provider - PSCo

3.2.2. Définitions

- **Autorité de Certification (AC) :**

Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

- **Autorité d'enregistrement (AE) :**

Cf. chapitre 1.3.1.

- **Autorité de Gestion de la Politique (AGP) :**

L'Autorité de Gestion de la Politique, pour les usages qui la concerne, établit les besoins et les exigences en termes de sécurité dans l'ensemble du processus de certification et d'utilisation des certificats. Elle établit des lignes directrices, qui peuvent prendre la forme d'un canevas de Politique de Certification, que doivent respecter toutes les Autorités de Certification qu'elle accrédite. Elle valide et suit toute évolution des politiques de certification des Autorités de Certification qu'elle accrédite.

Son rôle est celui d'une autorité morale qui indique par l'accréditation la confiance que l'on peut accorder à une Autorité de Certification.

- **Certificat :**

Attestation électronique liant les données afférentes au chiffrement ou à la vérification de signature, des échanges, messages et documents électroniques à un sujet, afin d'en assurer la confidentialité ou d'en assurer l'authentification et l'intégrité. Un format standard de certificat est défini dans la recommandation X.509 v3.

- **Sujet :**

Identités portées dans le certificat. Le sujet peut contenir l'identité d'une personne, d'un serveur, d'une organisation.

- **Politique de Certification (PC) :**

Ensemble de règles identifiées par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les bénéficiaires et les utilisateurs de certificats.

- **Déclaration des Pratiques de Certification (DPC) :**

Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

- **Prestataire de services de certification électronique (PSCE) :**

Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des bénéficiaires et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Déléguées). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

4. STRUCTURE ET ALIGNEMENT NORMATIF

Afin de garantir une meilleure compréhension par toutes les parties prenantes (auditeurs, autorités de contrôle, utilisateurs de certificats), la présente Politique de Certification (PC) intègre, en complément des références faites à la Déclaration des Pratiques de Certification (DPC), un ensemble d'engagements minimaux applicables à l'Autorité de Certification.
Ainsi, la PC précise notamment :

- Délais de révocation : toute demande de révocation d'un certificat est traitée dans un délai maximal de 24 heures ouvrées et 48 heures les week-ends et jours fériés, avec publication immédiate dans la CRL et mise à jour de l'OCSP.
- Durée de conservation des journaux et archives : les journaux de sécurité, données d'audit et documents justificatifs sont conservés pendant une durée minimale de 7 ans, conformément aux bonnes pratiques et aux exigences réglementaires.

Exigences de formation du personnel : les rôles critiques de l'IGC (opérateurs HSM, administrateurs PKI, responsables RA) font l'objet d'une formation initiale obligatoire et de sessions de remise à niveau au moins tous les 3 ans, afin de garantir la maîtrise des procédures de sécurité.
De plus, les références normatives sont alignées sur les dernières versions publiées par l'ETSI :

- ETSI EN 319 401 V2.3.1 : General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.3.2 : Policy and Security Requirements for TSPs issuing Certificates (general requirements)
- ETSI EN 319 411-2 V2.3.1 : Policy Requirements for Certification Authorities issuing Qualified Certificates

Ces corrections et précisions visent à assurer une lisibilité accrue du présent document, à clarifier les engagements de l'AC Sunu Root et à faciliter les audits de conformité.

5. PRESENTATION GENERALE

La Politique de Certification définie dans le présent document est destinée à être utilisée par les utilisateurs des services de certification GAINDE 2000 souscrit par une personne physique ou morale, publique ou privée, dans le cadre de la mise en oeuvre d'applications sécurisées accessibles.

La Politique de Certification couvre la gestion et l'utilisation de Certificats contenant les clés publiques servant aux fonctions de vérification, d'authentification, d'intégrité et de concordance des clés.

La délivrance d'un Certificat de clé publique en vertu de la présente Politique de Certification ne signifie pas que le Client ou l'Abonné soit autorisé de quelque façon que ce soit à effectuer des transactions commerciales, ou autres, au nom de l'organisation qui exploite l'AC SUNU ROOT .

GAINDE 2000 s'engage à vérifier, grâce aux moyens techniques mis en place, que les demandes d'émission et de révocation des Certificats sont effectuées par des personnes autorisées par ses clients.

GAINDE 2000 est assujetti aux lois et règlements en vigueur sur le territoire sénégalais, ainsi qu'aux normes en vigueur relatives à la mise en œuvre d'un service TSP (trust services provider).

Cette présente Politique régie les dispositions appliquées par l'AC SUNU ROOT , son personnel et les diverses entités composant l'IGC, dont notamment l'AE. Elle régie également les obligations auxquelles doivent se conformer les parties utilisatrices des services de certification. Il précise également un certain nombre de dispositions juridiques relatives, notamment, à la loi applicable et à la résolution des litiges.

L'AC SUNU ROOT , l'AE, leur personnel respectif, les composantes de l'IGC et les parties utilisatrices des services de certification sont responsables pour tous dommages et intérêts découlant du nonrespect de leurs obligations respectives telles que définies aux termes de la présente Politique de Certification.

5.1. OBLIGATIONS COMMUNES

Les différentes composantes de l'IGC ont pour obligations :

- d'assurer l'intégrité et la confidentialité des clés privées dont elles sont dépositaires, ainsi que des données d'activation desdites clés privées, le cas échéant ;
- de n'utiliser les clés publiques et privées dont elles sont dépositaires qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés ;
- de mettre en oeuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent ;
- de documenter leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de l'IGC ;

- de respecter et appliquer les termes de la présente PC qu'elles reconnaissent ;
- d'accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées et ;
- de respecter les conventions qui les lient aux autres entités composantes de l'IGC.

5.2. RESPONSABILITE DE L'AC SUNU ROOT ET DE SON PERSONNEL

L'AC SUNU ROOT est responsable vis-à-vis des Clients, Abonnés et Tiers utilisateurs, des opérations relatives aux services de certification réalisés par l'une quelconque des composantes de l'IGC. Elle garantit le lien qui existe entre une Entité identifiée et une bi-clé.

L'AC SUNU ROOT est responsable de l'information des Clients et des Abonnés, relativement aux procédures appliquées durant le cycle de vie des Certificats, dont notamment l'émission, la révocation et le retrait des Certificats.

Les fonctions critiques liées à la gestion des clés, à l'émission des certificats et à la gestion des incidents sont exercées par des personnels habilités opérant de manière indépendante. Les décisions opérationnelles ne sont soumises à aucune pression hiérarchique, contractuelle ou financière qui pourrait compromettre la sécurité ou la conformité de la PKI. L'AC dispose d'une gouvernance et de mécanismes internes pour préserver cette indépendance.

5.3. RESPONSABILITE DU PORTEUR

Le Porteur est responsable de :

- la protection, de l'intégrité et de la confidentialité de ses clés privées et des éventuelles données d'activation, liées aux Certificats ;
- la sécurité de ses équipements matériels, logiciels et réseaux impliqués dans l'utilisation de ses Certificats ;
- l'authenticité, de l'exactitude, et de la complétude des données d'identification de l'Entité identifiée fournies à l'AE lors de l'enregistrement et ;
- l'utilisation de ses clés et Certificats, qui doit être conforme à la présente Politique de Certification.

5.4. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

L'AC SUNU ROOT DOIT élaborer, mettre en œuvre, appliquer et mettre à jour annuellement une certification Énoncé de pratique qui décrit en détail comment l'AC met en œuvre la dernière version de ces exigences.

5.4.1. ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

L'AC DOIT divulguer publiquement sa politique de certification et/ou sa certification Énoncé de pratique par des moyens en ligne appropriés et facilement accessibles qui sont disponible 24h/7.

La fonction de publication de l'AC Sunu Root met à disposition l'information sur l'état des certificats par le biais de fichier « LAR ».

La LAR de l'AC Sunu Root est accessible par internet suivant ce point d'accès :

- http://sunulb.btrsut360.com:80/g2rootca/crl/g2rootca.crl

Les liens exacts sont définis dans l'extension « Point de distribution de la LCR » de chaque certificat émis par l'AC.

Les informations suivantes sont accessibles via le site https://www.confiancefactory.com :

- Les présentes PC ;
- Les CGU ;
- Les formats de certificats et de LCR objet des présentes PC ;
- Les LCR et LAR
- Les certificats d'AC.

5.4.2. DELAIS ET FREQUENCES DE PUBLICATION

Les délais et les fréquences de publication dépendent des informations concernées :

- **Certificats d'ACR :** diffusés préalablement à toute émission de certificats et/ou de LCR correspondants sous délai de 24 heures.
- **Informations d'état des certificats d'ACD :** les Listes des Autorités Révoquées sont mises à jour tous les mois. Une mise à jour exceptionnelle peut survenir aussi en cas de besoin. Une fois la mise à jour effectuée, la LAR est publiée dans un délai maximum de 24 heures.

- **Informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) :** publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'ACR.
- **Disponibilité :** La disponibilité des systèmes publiant les certificats d'AC est assurée 24h/24 et 7j/7.

5.4.3. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (authentification par certificat sur support).

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion des mots de passe.

5.4.4. PUBLICATION ET DISPONIBILITE DU SERVICE OCSP

En complément des CRL, l'Autorité de Certification Sunu Root met à disposition un service **OCSP** (Online Certificate Status Protocol) permettant de vérifier en temps réel l'état des certificats émis.

Les engagements suivants sont garantis :

- **Fréquence de mise à jour** : les réponses OCSP sont mises à jour au minimum toutes les 24 heures et immédiatement en cas de révocation d'un certificat.
- **Disponibilité du service** : le service OCSP est accessible en ligne avec un taux de disponibilité garanti d'au moins **99,5 % par mois**.
- **Authenticité des réponses** : chaque réponse OCSP est signée par un certificat OCSP Responder émis par l'AC déléguée correspondante et rattaché à la hiérarchie Sunu Root.
- **Points d'accès** : l'URL du service OCSP est intégrée dans l'extension **Authority Information Access (AIA)** de chaque certificat émis.

5.4.5. TRANSPARENCE VIS-A-VIS DES UTILISATEURS

L'AC SUNU Root s'engage à publier et maintenir accessibles en permanence les informations suivantes :

- La présente Politique de Certification (PC) et ses mises à jour,
- La Déclaration des Pratiques de Certification (DPC),
- Les Conditions Générales d'Utilisation (CGU),
- Les certificats racine et intermédiaires,
- Les CRL et les services OCSP correspondants.

Ces informations sont disponibles en accès libre sur le site officiel de Confiance Factory, conformément aux exigences de transparence et de confiance prévues par les normes ETSI EN 319 401 et EN 319 411.

5.4.6. OBLIGATIONS DES TIERS UTILISATEURS (RELYING PARTIES)

Les tiers utilisateurs de certificats (relying parties) doivent, avant de se fier à un certificat émis par l'AC Sunu Root ou par un AC délégué :

- Vérifier systématiquement l'état du certificat en consultant la **Liste des Certificats Révoqués (CRL)** et/ou le service **OCSP** associé, afin de s'assurer que le certificat n'a pas été révoqué ou suspendu.
- S'assurer que l'usage qu'ils font du certificat est conforme au domaine d'application prévu par la présente Politique de Certification.
- Vérifier la validité de la chaîne de certification en s'appuyant sur le certificat racine Sunu Root, tel que publié sur les points officiels de distribution.
- Reconnaître que l'utilisation d'un certificat à des fins non prévues ou interdites dans la présente Politique est faite sous leur seule responsabilité.

5.4.7. LIMITES DE RESPONSABILITE DE L'AUTORITE DE CERTIFICATION

L'Autorité de Certification Sunu Root et ses AC déléguées engagent leur responsabilité uniquement dans le cadre défini par la présente Politique de Certification et par les Conditions Générales d'Utilisation associées.

À ce titre :

- L'AC garantit l'authenticité du lien entre l'entité identifiée et la clé publique contenue dans le certificat, conformément aux procédures d'enregistrement et de validation décrites.
- La responsabilité de l'AC est limitée aux dommages directs et prouvés résultant d'une défaillance avérée de ses services de certification.
- L'AC ne saurait être tenue responsable :
    - des dommages indirects, consécutifs ou immatériels (ex. perte de profit, perte d'image),
    - de l'utilisation abusive ou frauduleuse d'un certificat par son porteur,
    - du non-respect par les tiers utilisateurs de leur obligation de vérifier l'état du certificat avant usage,
    - d'un usage du certificat en dehors des domaines explicitement autorisés.
- Un plafond d'indemnisation pourra être défini dans les Conditions Générales d'Utilisation, en fonction du type de certificat concerné et du niveau d'assurance associé.

6. EVALUATION DES RISQUES

GAINDE 2000 a procédé à une appréciation des risques afin d'identifier, analyser et évaluer les risques associés à son service de confiance. Cette appréciation des risques tient en compte les problématiques liées à l'activité et à la technique.
Suite à l'appréciation des risques, GAINDE 2000 a mis en œuvre un plan d'action de traitement permettant de couvrir les risques identifiés.
Cette évaluation des risques risques est revue, a minima, tous les deux ans et lors de toute évolution significative d'un système ou d'une composante de l'IGC.

La plan de traitement des risques ainsi que les risques résiduels sont formellement acceptés par la direction de GAINDE 2000. Les mesures de traitement du risque sont décrites dans la DPC ainsi que dans la PSSI.

7. POLITIQUES ET METHODES

7.1. ÉNONCE DES METHODES DE SERVICE DE CONFIANCE

Dans le cadre de l'exercice de sa fonction d'AC, GAINDE 2000 établit :

- Une **Politique de Certification** (PC) qui indique le niveau de confiance auquel il souhaite se hisser, suivant les principes énoncés. Elle établit les devoirs et responsabilités de l'Autorité de Certification de GAINDE 2000, de ses Clients et Abonnés, des Tiers utilisateurs, et de toutes les composantes de l'IGC intervenant dans l'ensemble du cycle de vie d'un Certificat. La Politique de Certification est librement consultable par les Clients, les Abonnés ainsi que par tous les Tiers utilisateurs. Définissant un cadre clair, elle permet d'établir la confiance à l'égard des Certificats émis par l'Autorité de Certification de GAINDE 2000. Ce présent document représente cette PC de GAINDE 2000.
- Une **Déclaration des Pratiques de Certification** (DPC) qui stipule, au plan pratique, comment est établi ce niveau de confiance visé par la PC, en particulier, les pratiques de toutes les composantes de l'IGC intervenant dans l'ensemble du cycle de vie d'un Certificat. La Déclaration des Pratiques de Certification fournit une description détaillée des services offerts et de toutes les procédures associées à la gestion du cycle de vie des Certificats. Elle peut comprendre également des services spécifiques.

Texte contractuel qui, selon l'usage et la finalité recherchés.

La Politique de Certification relève de la seule responsabilité de l'Autorité de Certification qui l'énonce et la publie.

7.2. GESTION DE LA PC

7.2.1. Entité gérant la PC

La présente Politique de certification est sous la responsabilité de la société GAINDE 2000.

7.2.2. Point de contact

AUTORITE DE CERTIFICATION RACINE	
Contact	**GAINDE 2000** **I, Allées Thierno Saïdou Nourou TALL , Point E.** **Immeuble ORBUS ■ Dakar, Sénégal** **■Tel (+221) 33 859 39 99 ■ Fax (+221) 33 824 17 24** **Courrier électronique : confiancefactory@confiancefactory.com**

7.2.3. Entité déterminant la conformité d'une DPC avec cette PC

Le Comité des Changements de la PKI de GAINDE 2000 détermine la conformité de la DPC avec la présente politique de certification (PC).

7.2.4. Procédures d'approbation de la conformité de la DPC

L'AC SUNU ROOT est garante de l'application de la DPC avec la Politique de Certification. Elle est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC suit le processus d'approbation mis en place et est publiée, sans délai, à la fin du processus.

Une AGP peut demander l'examen de la DPC conformément aux procédures en vigueur.

7.3. TERMES ET CONDITIONS

Cf. les Conditions Générales d'Utilisation.

7.4. POLITIQUE DE SECURITE DE L'INFORMATION

Cf. la Politique de Sécurité.

8. GESTION ET EXPLOITATION DU PSCE

8.1. ORGANISATION INTERNE

8.1.1. Fiabilité de l'organisation :

Le service de certification numérique de GAINDE 2000 est accessible à tout demandeur, personne physique ou morale, qui remplit les conditions définies dans la présente PC et dans la DPC, sans aucune discrimination.
GAINDE 2000 dispose des ressources financières nécessaires à l'exercice de sa fonction TSP et, le cas échéant, il contractera une assurance de responsabilité civile appropriée, conformément au droit applicable au Sénégal, pour couvrir les responsabilités résultant de ses opérations et/ou activités.
Gainde 2000 dispose de politiques et de procédures pour la résolution des réclamations et des litiges de la part de ses clients.
Dans l'exercice de sa mission de PSCE, GAINDE 2000 ne fait pas appel à de la prestation externe. Le cas échéant, un accord contractuel permettra de régir la relation de prestation.

8.1.2. Séparation des attributions

Afin de prévenir les modifications non autorisé, involontaire ou l'utilisation incorrecte des actifs, GAINDE 2000 assure une séparation des attributions et domaines de responsabilité incompatibles. Une matrice des rôles permet de garantir une séparation des fonctions et attributions incompatibles.

8.2. RESSOURCES HUMAINES

8.2.1. Qualifications, compétences et habilitations requises

Le responsable de l'AC SUNU ROOT s'assure que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une ACR :

- sont nommés à un poste faisant l'objet d'une description détaillée par écrit ;
- sont liés par contrat ou par la loi aux postes qu'ils occupent ;
- ont reçu toute la formation nécessaire pour accomplir leurs tâches ;
- sont tenus par contrat ou par la loi de ne pas divulguer de renseignements ayant trait à la sécurité de l'ACsR, aux clients ou aux bénéficiaires ; une clause de confidentialité est expressément inscrite dans les contrats de travail des membres du personnel de l'ACSR ;

Des obligations identiques sont portées à la charge du responsable de l'AE et le résultat communiqué à l'AC SUNU ROOT .

8.2.2. Procédures de vérification des antécédents

Des vérifications des antécédents sont faites conformément à la politique de l'AC SUNU ROOT en matière de sécurité.

Le salarié s'engage sur l'honneur sur l'exactitude de toutes les informations fournies lors de la phase d'embauche.

Des obligations identiques sont portées à la charge du responsable de l'AE et d'en communiquer le résultat à l'AC SUNU ROOT .

8.2.3. Exigences en matière de formation

L'AC SUNU ROOT s'assure que tous les membres du personnel qui accomplissent des tâches touchant à l'exploitation d'une AC ou d'une AE ont reçu une formation concernant :

- les principes de fonctionnement et les mécanismes de sécurité de l'AC Sunu Root ou de l'AE.

Le personnel de l'AC Sunu Root suit un programme de formation pour accomplir correctement ses fonctions. Il porte :

- sur les différentes applications et versions d'applications auxquelles il pourrait avoir accès dans le cadre de ses fonctions au sein du système de l'AC Sunu Root ;
- sur toutes les tâches qu'il devra accomplir dans le cadre de l'IGC ;
- sur le matériel et les systèmes d'exploitation formant l'environnement opérationnel de l'AC Sunu Root;
- sur le plan de secours de l'AC Sunu Root après un sinistre et les procédures de maintien des activités. Avant l'entrée en fonction, il sera procédé à une familiarisation aux règles de sécurité en vigueur.
- sur tout autre sujet jugés pertinent par l'AC Sunu Root.

Des obligations identiques sont portées à la charge de l'AE et de leur personnel.

Des cours de formation professionnelle sont offerts en fonction des besoins, et l'AC Sunu Root revoit ses exigences au moins une (01) fois tous les trois ans.

Le personnel de l'AC Sunu Root participe régulièrement à des séances de formation sur la sécurité. Des obligations identiques sont portées à la charge de l'AE et de leur personnel.

8.2.4. Sanctions en cas d'actions non autorisées

Si une personne a réellement fait ou est soupçonnée d'avoir fait une action non autorisée dans l'accomplissement de ses tâches en rapport avec l'exploitation d'une ACR ou d'une AE, On peut lui interdire l'accès au système.

En outre, si les faits sont avérés, elle peut prendre toutes sanctions disciplinaires adéquates en application de la réglementation en vigueur.

8.2.5. Exigences vis-à-vis du personnel des prestataires externes

L'AC Sunu Root s'assure que les personnels des entreprises cocontractantes peuvent accéder à ses locaux conformément à l'évaluation des risques l'article 5.

Les prestataires externes devraient signer un NDA avant de pouvoir accéder aux environnements de production de l'IGC.

Des obligations identiques sont portées à la charge du responsable de l'AE et le résultat communiqué à l'AC SUNU ROOT .

8.2.6. Documentation fournie au personnel

L'AC SUNU ROOT met à la disposition des membres son personnel et celui de l'AE les Politiques de Certification qu'elle accepte, ainsi que toute loi, toute politique ou tout contrat qui s'appliquent aux postes qu'ils occupent.

Tout le personnel de l'AC Sunu Root a accès à des manuels complémentaires relatifs à leurs responsabilités. Ces manuels portent sur l'ensemble des procédures en vigueur.

Des obligations identiques sont portées à la charge l'AE et de son personnel.

8.2.7. Exigences générales

GAINDE 2000, lors de son appréciation des risques sur le périmètre de l'activité de l'IGC, a fait l'inventaire de l'ensemble des actifs matériels et informationnels. Une classification des actifs en fonction des critères de Disponibilité, Intégrité et Confidentialité est effectuée.

Une protection appropriée est apportée à chaque actif en fonction de sa criticité et de sa sensibilité.

L'inventaire est revu en même temps que l'appréciation des risques ou en cas de changement important des actifs. Pour des actifs, considérés comme critique, un processus de revue plus fréquentes peut être mis en place.

8.2.8. Conservation des supports

Dans le cadre de l'analyse de risque, les différentes informations intervenant dans les activités de l'IGC ont été identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont traités et conservés conformément à ces besoins de sécurité.

8.3. CONTROLE D'ACCES

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC sont contrôlés.

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusions physiques et logiques.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Remarque : On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

8.4. CONTROLES CRYPTOGRAPHIQUES

Les bi-clés d'AC sont générées dans des modules cryptographiques sécurisés au cours de cérémonies de clés. Des modules cryptographiques assurent également la génération des certificats correspondants.

Les longueurs des clés d'AC sont précisées dans le document [Profils de Certificats].

Le certificat Sunu Root de l'IGC est téléchargeable sur le site Web de Confiance Factory. L'utilisateur peut vérifier l'empreinte du certificat racine sur le site sécurisé https://www.confiancefactory.com ou en contactant Gainde2000 par téléphone.

8.5. SECURITE PHYSIQUE ET ENVIRONNEMENTALE

Les locaux techniques, qui accueillent les moyens de certification et notamment sa clé privée de signature, sont fortement protégés. Ils sont dans une zone à accès contrôlé, protégée contre tous les risques courants (incendie, inondation, intrusion physique, …).

La DPC précise les conditions de sécurité physique et les règles appliquées– ainsi que dans les locaux, en particulier sur les sujets suivants :

- Emplacement, construction et accès physique;
- Système électrique et système de conditionnement d'air;
- Dégâts causés par l'eau;
- Prévention et détection d'intrusion physique,
- Prévention et protection-incendie;
- Entreposage des supports;
- Mise au rebut du matériel, destruction;
- Sauvegarde à l'extérieur des locaux.

8.6. SECURITE DES OPERATIONS

Les dispositions nécessaires au respect de cette exigence sont décrite sur le chap 10.

8.7. SECURITE DU RESEAU

Les dispositions nécessaires au respect des exigences de ce point sont décrites au sein du document [DAT] « Dossier d'architecture de l'AC SUNU ROOT ».

8.8. COLLECTE DE PREUVES

Les différents évènements liés au fonctionnement de l'IGC font l'objet d'une journalisation d'évènements enregistrée de façon manuelle ou automatique.

Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées. Ces journaux d'évènements sont datés, protégés et font

l'objet d'un archivage. Ils sont régulièrement contrôlés afin d'évaluer les éventuelles vulnérabilités pesant sur l'IGC.

8.9. GESTION DE LA CONTINUITE DES ACTIVITES

Le service est disponible 24 heures / 24 et 7 jours / 7 via la plateforme de Confiance Factory.

La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats est de 1 heure.

La durée maximale totale d'indisponibilité de la fonction d'information sur l'état des certificats est de 4h par mois.

8.10. CESSATION DU PSCE ET PLANS DE CESSATION

Une ou plusieurs composantes de l'IGC, ou la totalité de l'IGC, peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses. Gainde2000 mettra en œuvre les mesures requises pour assurer au minimum la continuité de l'archivage des informations et la continuité des services de révocation.

Gainde2000 a pris les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où Gainde2000 serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, Gainde2000 les en avisera aussitôt que nécessaire et, au moins, sous le délai d'un mois. De même, Gainde2000 informera les autorités publiques concernées.

8.11. CONFORMITE

8.11.1. VALIDATION INITIALE DE L'IDENTITÉ

8.11.2. Validation de l'identité d'un organisme

L'AE vérifie l'identification de l'organisation, de son représentant légal et de toutes personnes désignées par ce dernier, directement ou indirectement, pour le représenter vis-à-vis de l'AC ou de l'AE. Le représentant légal et ces personnes, qu'il aura désignées en donnant l'étendue de leur mandat, sont les mandataires de certification.

A défaut de désignation, le représentant légal est l'unique mandataire de certification.

Lors de l'enregistrement, l'organisation doit apporter la preuve de son existence, la preuve de l'identité de son représentant légal ainsi que la chaîne des mandats conférant leur pouvoir aux mandataires de certification.
L'AC ou l'AE archive toutes les informations pertinentes relatives à cet enregistrement.
La DPC précise les documents à fournir et les procédures d'enregistrement mises en œuvre par l'AE, en concertation avec l'AC.

8.11.3. Validation de l'identité du bénéficiaire

Le certificat doit toujours contenir le nom de l'entité identifiée et, éventuellement, toutes les informations complémentaires permettant d'identifier son titulaire sans ambiguïté.
Pour toute demande de certificat faite au titre de l'appartenance à une organisation, il faut que ladite demande soit signée par le mandataire de certification et que les pièces justificatives soient envoyées à GAINDE2000.
La DPC précise les documents à fournir et les procédures d'enregistrement mises en œuvre par l'AE, en concertation avec l'AC.

8.11.4. Enregistrement d'un Mandataire de Certification

Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification (MC) pour répondre aux besoins suivants :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les bénéficiaires présentés par le MC.
- Éventuellement, fourniture d'un certificat au MC pour qu'il puisse signer les dossiers d'enregistrement de bénéficiaires de l'entité qu'il représente et les transmettre sous forme électronique.

L'identification du futur MC représentant une entité nécessite, d'une part, l'identification de cette entité et, d'autre part, l'identification de la personne physique.

8.12. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLÉS

Le renouvellement de la bi-clé d'un certificat entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au bénéficiaire sans renouvellement de la bi-clé correspondante.

8.12.1. Identification et validation pour un renouvellement courant

À l'occasion du premier renouvellement l'AE doit vérifier que le porteur est toujours en possession du certificat et que celui-ci est en cours de validité ; elle vérifie également que les informations en sa possession sont toujours valides.
L'AE identifie le sujet selon la même procédure que pour l'enregistrement initial dans les cas suivants :

- En cas de modifications demandées par le bénéficiaire,
- ou en cas d'expiration des justificatifs, de non-détention du certificat initial ou d'expiration de celui-ci,
- Lorsque le porteur souhaite renouveler son certificat pour la seconde fois.

La DPC précise les modalités de renouvellement.

8.12.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial.

8.13. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RÉVOCATION

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat de l'ACD :

- les informations du sujet figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat,
- l'ACD n'a pas respectée les modalités applicables d'utilisation du certificat,
- l'ACD n'a pas respectée ses obligations découlant de la PC de l'ACR, une erreur (intentionnelle ou non) a été détectée dans le dossier de l'ACD,
- la clé privée de l'ACD est suspectée de compromission, est compromise, est perdue ou est volée,
- le représentant légal de l'ACD demande la révocation du certificat, la cessation d'activité de l'entité de l'ACD.

Lorsqu'une des circonstances ci-dessus se réalise et que l'ACR en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

La DPC précise les modalités de révocation.

8.14. SECURITE OPERATIONNELLE

8.14.1. Délais de traitement des révocations

Toute demande de révocation d'un certificat reçue par l'Autorité de Certification ou l'Autorité d'Enregistrement est :

- **analysée et validée dans un délai maximal de 24 heures ouvrées**,
- **traitée dans un délai maximal de 48 heures en week-end et jours fériés**,
- suivie d'une **publication immédiate** dans la Liste des Certificats Révoqués (LCR) et via le service OCSP.

Ces engagements garantissent la conformité avec les exigences de l'ETSI EN 319 411-1 relatives à la gestion du cycle de vie des certificats.

8.14.2. Sécurité des modules cryptographiques (HSM)

- Les clés privées de l'AC Sunu Root et des AC déléguées sont générées et stockées exclusivement dans des **Modules de Sécurité Matérielle (HSM)** certifiés **FIPS 140-2 niveau 3 ou supérieur** ou équivalent **CC EAL4+**.
- Les cérémonies de clés font l'objet de procédures documentées et impliquent plusieurs rôles de confiance afin de garantir la séparation des responsabilités.
- Les clés privées ne quittent jamais le HSM sous forme exploitable en clair.

8.14.3. Sécurité réseau et séparation des environnements

- L'infrastructure PKI est exploitée dans des environnements **séparés logiquement et physiquement** (production, pré-production, administration).
- Les communications critiques (émission de certificats, publication des LCR/OCSP) utilisent uniquement des protocoles sécurisés (TLS 1.2 ou supérieur, SSH v2).
- Les accès aux équipements de l'IGC sont restreints aux personnels habilités via une **authentification forte** (certificat sur support matériel ou équivalent).
- Des dispositifs de détection d'intrusion (IDS/IPS) et de journalisation centralisée assurent la surveillance continue du réseau.

9. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

Le présent chapitre définit les pratiques opérationnelles relatives à la gestion des clés et des certificats des autorités.

9.1. DISPOSITIONS GENERALES

L'AC SUNU ROOT est garante de la bonne gestion du cycle de vie des certificats émis via les processus suivants :

- Établissement d'une demande de certificat.
- Traitement d'une demande de certificat.
- Délivrance du certificat.
- Acceptation du certificat
- Renouvellement d'un certificat
- Délivrance d'un nouveau certificat suite à changement de la bi-clé
- Révocation des certificats
- Fonction d'information sur l'état des certificats
- Fin de la relation entre le porteur et l'AC

L'ensemble de ces processus sont décrits au sein des documents [PROC].

9.1.1. Durée de validité des certificats

La durée de vie des certificats émis dans la hiérarchie Sunu Root est fixée comme suit :

- **Certificat de l'AC Racine (Sunu Root)** : 15 à 20 ans maximum.
- **Certificats des AC déléguées (Sub-CA)** : 5 à 10 ans maximum.
- **Certificats d'authentification administrateur et certificats techniques associés** : 1 à 3 ans maximum.

- **Certificats de test** : durée limitée 1 à 6 mois, sans valeur contractuelle ni garantie.

Toute modification de ces durées doit être validée par le Comité des Changements de la PKI de GAINDE 2000 et publiée dans une nouvelle version de la PC.

9.2. EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS AUTO-SIGNES DE L'AC RACINE

Les dispositions relatives à la Génération d'une bi-clé et d'un certificat auto-signé de l'AC Sunu Root, au Renouvellement d'une bi-clé et d'un certificat auto-signé de l'ACSR et à la Révocation d'un certificat auto-signé de l'ACR sont décrits au sein des documents [KC] « Procédure de cérémonie des clés de l'AC SUNU ROOT ».

9.3. EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS D'AC DELEGUEES

Les dispositions relatives à la Génération d'un certificat pour une AC Déléguée, au Renouvellement d'un certificat d'un AC Délégué et à la Révocation d'un certificat d'un AC Déléguée sont décrites au sein des documents [KC] « Procédure de cérémonie des clés de l'AC SUNU ORGANIZATION et SUNU EASY ».

9.3.1. Révocation des certificats d'AC déléguées

La révocation d'un certificat d'AC déléguée peut intervenir dans les cas suivants :

- Compromission avérée ou suspectée de la clé privée de l'AC déléguée.
- Utilisation du certificat en dehors des usages autorisés par la présente Politique.
- Violation grave des obligations contractuelles par l'AC déléguée.
- Cessation d'activité de l'entité exploitant l'AC déléguée.
- Demande expresse du représentant légal de l'entité exploitante.

La procédure de révocation suit les principes suivants :

- **Acteurs habilités** : seules l'Autorité de Certification Racine (Sunu Root) ou l'Autorité de Gestion des Politiques peuvent ordonner la révocation d'un certificat d'AC déléguée.
- **Modes de demande** : la demande doit être transmise par écrit, signée par le représentant légal ou le mandataire habilité, et confirmée par des canaux sécurisés (courrier recommandé, signature électronique qualifiée, ou canal en ligne authentifié avec certificat).
- **Délais de traitement** : la demande est instruite sous 24 heures ouvrées, et la révocation est publiée immédiatement dans la CRL et diffusée via OCSP.
- **Suspension éventuelle** : en cas de suspicion mais avant confirmation d'une compromission, l'AC Sunu Root peut décider de **suspendre temporairement** le certificat de l'AC déléguée, afin de limiter les risques en attendant la décision finale.

9.4. EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS D'AUTHENTIFICATION ADMINISTRATEUR DE L'AC SUNU ROOT

Les dispositions relatives à la **Génération d'un certificat,** au **Renouvellement d'un certificat** et à la **Révocation d'un certificat** d'authentification administrateur sont décrites au sein du document [PROC] « Procédure de Génération de Certificats ».

10. MESURES DE SECURITE NON TECHNIQUES

10.1. MESURES DE SECURITE PHYSIQUE

L'Autorité de Certification Sunu Root met en œuvre les mesures de sécurité physique, au sein des différentes composantes de l'IGC, nécessaire pour assurer le fonctionnement sécurisé de ses services conformément aux engagements pris dans le présent document, notamment en termes de disponibilité (contrôle d'accès physique, services supports (alimentation électrique, climatisation,…), protection contre les dégâts des eaux, protection contre les incendies et protection des supports).

10.2. MESURES DE SECURITE PROCEDURALE

Les dispositions nécessaires au respect des exigences des points ci-dessous sont décrites au sein de la DPC et les documents [KC] « Procédure de cérémonie des clés »:

- rôles de confiance relatifs aux Cérémonies des Clés
- rôles de confiance auprès de l'ACSR
- rôles de confiance mutualisés
- nombre de personnes requises par tâche
- identification et authentification pour chaque rôle
- rôles exigeant une séparation des attributions

10.3. MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

L'ensemble du personnel, interne et externe à Confiance Factory, amené à travailler au sein des composantes de l'IGC sont soumis à des obligations de qualifications, de compétences, de formations initiales et continues et d'habilitations en fonction de leurs rôles.

L'honnêteté de ces personnels est vérifiée conformément à ce qui est autorisée par la loi.

10.4. PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

Constitution des données d'audit :

Les dispositions nécessaires au respect des exigences des points ci-dessous sont décrites ci-dessus :

- type d'évènements enregistrés
- fréquence de traitement des journaux d'évènements et dossiers d'enregistrement
- notification de l'enregistrement d'un évènement au responsable de l'évènement
- évaluation des vulnérabilités.

Sauvegarde des données d'audit :

Les dispositions nécessaires au respect des exigences des points ci-dessous sont décrites au sein de la DPC :

- période de conservation des journaux d'évènements et dossiers d'enregistrement sur site
- protection des journaux d'évènements et dossiers d'enregistrement
- procédure de sauvegarde des journaux d'évènements
- système de collecte des journaux d'évènements

10.5. ARCHIVAGE DES DONNEES

La DPC détaille les dispositions relatives aux points suivants :

- type de données archivées
- période de conservation des archives
- procédure de sauvegarde des archives
- système de collecte des archives

L'AC Sunu Root traite les données à caractère personnel conformément au Règlement Général sur la Protection des Données (RGPD) et à la législation nationale applicable (CDP).

10.6. CHANGEMENT DE CLE D'ACSR

L'AC Sunu Root ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'ACR.

Au regard de la date de fin de validité de ce certificat, son renouvellement est demandé dans un délai au moins égal à la durée de vie maximale des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'ACR est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis avec la clé privée correspondante et ce jusqu'à l'expiration de tous les certificats signés par cette dernière.

Le certificat ne peut être prorogé au-delà de sa date de validité. Donc, l'émission d'un nouveau certificat nécessitera un renouvellement des clés.

10.7. REPRISE SUITE A UNE COMPROMISSION OU UN SINISTRE

Les dispositions nécessaires au respect des exigences des points ci-dessous sont décrites au sein de la DPC et du document « Plans de Continuité et de Reprise d'Activité »:

- procédures de remontée et de traitement des incidents et des compromissions
    - procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)
    - procédure de reprise en cas de compromission de la clé privée de l'AC ou de l'une de ses composantes
- capacités de continuité d'activité suite à un sinistre.

De même, les mesures en cas de désastre ou autres catastrophes naturelles pour les données, les équipements et les logiciels de l'AC Sunu Root sont documentées.

10.8. FIN DE VIE DE L'IGC

Ce point fait l'objet du document [KC] « Procédure de cérémonie des clés » et sont aussi détaillé dans la DPC.

11. MESURES DE SECURITE TECHNIQUES

Le présent chapitre a pour objet de définir les dispositions de gestion des bi-clés de l'AC Sunu Root, du personnel de l'ACR, des AE déléguées, et des bénéficiaires.

11.1. GENERATION DES BI-CLES

Le principe de séparation des clés est appliqué à toutes les clés utilisées dans le cadre du système technique de l'AC Sunu Root.

L'AC Sunu Root produit sa propre bi-clé de signature électronique au moyen d'un algorithme de cryptographie et selon une procédure impliquant plusieurs rôles.

Les documents [KC] « Procédure de cérémonie des clés » et la DPC traitent les points suivants :

- génération des bi-clés des Autorités de l'AC SUNU ROOT
- transmission de la clé publique d'une AC Déléguée à l'AC Sunu Root

11.2. MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

Le document [KC] « Procédure de cérémonie des clés » précise les dispositions relatives aux mesures de sécurité liées aux Modules cryptographiques de l'AC.

11.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES

Les dispositions relatives à l'Archivage des clés publiques sont décrites au sein de la DPC.

11.4. DONNEES D'ACTIVATION DES CLES D'AC

La génération et l'installation des données d'activation des modules cryptographiques d'AC sont réalisées par du personnel de confiance lors des phases d'initialisation et de personnalisation de ces modules.

Ces données d'activation sont protégées en confidentialité, intégrité et disponibilité.

11.5. MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

Les dispositions nécessaires au respect des exigences de ce point sont décrites au sein du document [DAT] «Document Architecture Technique».

11.6. MESURES DE SECURITE RESEAU

L'AC définit les protocoles et commandes dans la DPC.

11.7. SYSTEME DE DATATION

L'AC Sunu Root précise les modalités techniques permettant l'horodatage des événements liés à l'activité des composantes de l'IGC dans la DPC.

11.8. DISPONIBILITE DES CRL

L'Autorité de Certification (AC) garantit une disponibilité continue (24 heures sur 24, 7 jours sur 7) de la Liste de Révocation des Certificats (CRL), afin d'assurer un contrôle permanent sur l'état de validité des certificats émis.

Afin de renforcer cette disponibilité et de prévenir toute interruption, les mesures suivantes sont mises en œuvre :

- Infrastructure redondante : les serveurs hébergeant les CRL sont répartis sur des sites géographiquement distincts avec mécanismes de basculement automatique en cas d'incident sur un site principal.
- Supervision 24/7 et alertes : un système de supervision en temps réel est en place pour détecter toute anomalie dans la publication ou l'accessibilité des CRL, avec génération d'alertes immédiates auprès de l'équipe de sécurité.
- Plan de continuité (PCA) : un plan spécifique de continuité d'activité pour les composants critiques de l'IGC, incluant les CRL, a été formalisé. Il prévoit des procédures de reprise rapide ainsi que des moyens de publication de secours.
- Tests réguliers : des tests périodiques de disponibilité et de basculement sont réalisés

pour garantir l'efficacité des mécanismes mis en place.

- Résilience énergétique : les équipements critiques sont protégés par des onduleurs et générateurs permettant de maintenir la disponibilité même en cas de coupure électrique.

12. PROFILS DES CERTIFICATS, OCSP ET DES LCR

Ce chapitre contient les règles et directives relatives à l'utilisation de certains types de certificats X.509, des champs, des extensions des LCR conformes aux normes PKIX.

Le contenu des certificats et des LCR, sont conformes aux exigences de la RFC 5280 : « Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ».

Les modalités opérationnelles sont traitées dans la DPC.

13. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre ne concerne que les audits et évaluations de la responsabilité de l'AC Sunu Root afin de s'assurer du bon fonctionnement de son IGC.

L'AC Sunu Root est auditée au moins une fois tous les 24 mois conformément aux exigences ETSI EN 319 411, par un organisme indépendant et accrédité.

7.1 AUDITS INTERNES

Les dispositions nécessaires au respect des exigences de ce point sont décrites ci-dessus :

- fréquences et/ou circonstances des évaluations
- identités/qualifications des évaluateurs
- relations entre évaluateurs et entités évaluées
- sujets couverts par les évaluations
- actions prises suite aux conclusions des évaluations
- communication des résultats

7.2 AUDITS DE CONFORMITE

La DPC apporte des précisions complémentaires aux modalités opérationnelles sur les points suivants:

- fréquence des contrôles de conformité
- identification et qualifications du contrôleur
- sujets couverts par le contrôle de conformité
- mesures à prendre en cas de non-conformité
- communication des résultats

14. ANNEXES DOCUMENTS DE REFERENCE

14.1. REGLEMENTATION

Renvoi	Document
[CDP]	Loi 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel
[LOIPI]	Loi 2008-09 du 25 janvier 2008 sur les droits d'auteurs et droits voisins
[LCC]	Loi n°2008-11 du 25 janvier 2008 sur la cybercriminalité
[LC]	Loi n°2008-41 du 20 août 2008 portant sur la cryptologie
[LSIG]	Loi 2008-08 du 25 janvier 2008 sur les transactions électroniques
[Décret CDP]	Décret N°2008-721 du 30 juin 2008 portant application de la loi n°2008-12 du 25 janvier 2008 sur la protection des données à caractères personnel
[Décret CC]	Décret N°2010-1209 du 13 septembre 2010 portant application de la loi sur la cryptologie
[Décret SIG]	Décret N°2008-720 du 30 juin 2008 relatif à la certification électronique pris en application du décret n°2008-08 du 25 janvier 2008 relatif aux transactions électroniques.

14.2. NORMES ET STANDARDS

Renvoi	Document
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complétée par les correctifs techniques n° 1 d'octobre 2001, n° 2 d'avril 2002 et n° 3 d'avril 2004)
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[RFC2560]	Internet PKI Online Certificate Status Protocol-OCSP. Cf. http://www.ietf.org/
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Cf. http://www.ietf.org/.
[EN-319411-2]	« Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for Certification Authorities issuing qualified certificates ». ETSI EN 319 411-3 V1.1.1 (2013-01).
[EN-319411-3]	« Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates ». ETSI EN 319 411-2 V1.1.1 (2013-01).
[TS-101456]	ETSI TS 101 456 V1.4.3 (mai 2007) Policy Requirements for Certification Authorities issuing qualified certificates
[TS-102042]	ETSI TS 102 042 V2.1.1 (mai 2009) Policy Requirements for Certification Authorities issuing public key certificates

14.3. AUTRES DOCUMENTS

Renvoi	Document
[PROFILS]	Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques DT-FL-1001-001-PC-PROFILS-1.0.doc – version 1.0