



CONDITIONS GENERALES D'UTILISATION

SUNU CERTIFICAT ORGANISATION

I, 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.confiancefactory.com

Nature du Document	CGU
Référence	CGU_CERT_ORG_SUNU
Document de Référence	DPC AC SUNU ROOT v1.4 (OID : 1.3.6.1.4.1.45491.2.3) et PC SUNU ROOT v1.2 (OID : 1.3.6.1.4.1.45491.2.1)
Date	03/07/2026
Emetteur	GAINDE 2000
Destinataires	Public
Version	1.2
Nombre de page	10

Date	Auteur	Version	Evolutions
17/07/2013	Responsable Autorité d'Enregistrement	1.0	Création du document
22/12/2015	Responsable Référentiel Documentaire	1.0	Révision du document
12/05/2022	Chef du pole technique	1.1	Mise à jour du document
03/07/2026	Responsable Autorité d'Enregistrement	1.2	Mise à jour du document

PREAMBULE

Les présentes Conditions Générales d'Utilisation (CGU) régissent l'utilisation des certificats électroniques émis par l'Autorité de Certification SUNU ROOT. En souscrivant à un certificat, l'Utilisateur accepte sans réserve les présentes CGU.

Procédure

ARTICLE 1 : OBJET ET CHAMP D'APPLICATION

I-1 Objet

Les présentes CGU définissent les conditions d'émission, d'utilisation, de suspension et de révocation des certificats délivrés par l'Autorité de Certification SUNU ROOT (« l'AC »).

I-2 Champ d'Application

Les présentes CGU s'appliquent à l'ensemble des abonnés, titulaires, mandataires et tiers utilisateurs des certificats émis sous la Racine SUNU ROOT, opérée par GAINDE 2000 – Confiance Factory.

1.3 Références documentaires :

Les présentes CGU sont établies conformément à la Déclaration des Pratiques de Certification (DPC) de l'Autorité de Certification SUNU ROOT, version 1.4 (OID : 1.3.6.1.4.1.45491.2.3) et à la Politique de Certification (PC) SUNU ROOT, version 1.2 (OID : 1.3.6.1.4.1.45491.2.1).

En cas de divergence entre les dispositions, la DPC prévaut sur la PC et sur les présentes CGU.

ARTICLE 2 : DEFINITIONS

Pour l'application des présentes, les termes suivants ont les significations indiquées ci-après :

- **AC** : Autorité de Certification SUNU ROOT
- **Abonné/Titulaire** : Personne physique ou morale titulaire d'un certificat
- **Mandataire** : Représentant d'une organisation responsable des utilisateurs finaux
- **DPC** : Déclaration des Pratiques de Certification
- **PC** : Politique de Certification
- **CRL** : Liste de certificats révoqués
- **OCSP** : Protocole de vérification en ligne du statut des certificats
- **HSM** : Module matériel de sécurité
- **PC** : Politique de Certification ; Document établissant les devoirs et responsabilités de CONFIANCE FACTORY, de ses CLIENTS, MANDATAIRES et BENEFICIAIRES intervenant dans l'ensemble du cycle de vie d'un CERTIFICAT (consultable sur www.confiancefactory.com rubrique « politiques de certification »)
- **CERTIFICAT** : Attestation électronique émise par CONFIANCE FACTORY liant les données afférentes au chiffrement ou à la vérification de signature des échanges, messages et documents électroniques au BENEFICIAIRE, afin d'en assurer la confidentialité ou l'authentification et l'intégrité.
- **BENEFICIAIRE** : Personne physique identifiée par l'Autorité d'Enregistrement, qui porte la responsabilité des CERTIFICATS qui lui sont remis. Le bénéficiaire peut être le PORTEUR, il s'engage sur ses conditions d'utilisation et ses obligations vis-à-vis de l'Autorité de Certification.
- **PORTEUR** : La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.
- **CLIENT** : Organisme, personne morale ou physique qui contracte avec CONFIANCE FACTORY pour disposer de CERTIFICATS.

- **CONTRAT** : ensemble contractuel constitué des présentes Conditions générales, des Conditions d'Utilisation du certificat commandé, du dossier de demande ainsi que de la Politique de Certification afférentes figurant sur le site : www.confiancefactory.com applicables à la date de conclusion du CONTRAT. Procédure
 - **MANDATAIRE** : Personne ayant, directement par la loi ou par délégation, le pouvoir d'autoriser une demande de certificat portant le nom de l'organisation. Il peut aussi avoir d'autres pouvoirs au nom de l'organisation, comme celui de révocation. A défaut de désignation, le représentant légal est l'unique mandataire de certification
 - **SUPPORT** : Support physique (carte à crypto-processeur ou mini CD) contenant notamment le(s) CERTIFICAT(s) du BENEFICIAIRE. Le SUPPORT devient la propriété du CLIENT au moment de sa mise à disposition par CONFIANCE FACTORY.
- TIERS UTILISATEUR** : Personne utilisant le CERTIFICAT d'un BENEFICIAIRE afin de vérifier son identité ou de chiffrer des messages à son attention.

ARTICLE 3 : REFERENCES NORMATIVES

L'AC respecte les normes et réglementations suivantes :

- ETSI EN 319 401 : Exigences générales de politique pour les fournisseurs de services de confiance
 - ETSI EN 319 411-1 : Exigences de politique et de sécurité pour les TSP émettant des certificats
 - ETSI EN 319 412-x : Profils de certificats
 - Règlement (UE) 910/2014 (eIDAS)
 - ISO/IEC 2700: 2013 et A.18.1 (Sécurité et conformité)
 - Règlement Général sur la Protection des Données (RGPD)
- Loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel au Sénégal (CDP Sénégal)

ARTICLE 4 : ROLES ET RESPONSABILITES

4-1 Autorité de Certification (AC sunu root) Obligations Principales

- Émettre, publier et gérer certificats conformément à la DPC ;
- Protéger les clés CA et sensibles en HSM certifié **FIPS 140-2 L3 / CC EAL4+** ;
- Conserver journaux/preuves selon la DPC (durée minimale : voir §9).
- Assurer disponibilité CRL/OCSP (engagements SLA) ;
- Notifier incidents et autorités conformément au §7 des présentes.

4-2 Bénéficiaires / Abonnés Obligations Principales

- Fournir données exactes à la demande ; protéger sa clé privée et ses codes
- Notifier l'AC immédiatement en cas de perte/compromission.

4-3 Mandataires / Clients Organisationnels Obligation

S'assurer de la conformité des utilisateurs, délégations et justificatifs.

ARTICLE 5 : EMISSION, VALIDATION ET ACCEPTATION DU CERTIFICAT

5-1 Vérifications Préalables

L'AC vérifie l'identité et l'autorité du demandeur selon la DPC avant émission.

5-2 Acceptation

Procédure

Le **retrait du support physique** (smartcard/token) contenant le certificat vaut **acceptation expresse et irrévocable** des présentes CGU, sauf rétractation écrite notifiée à l'AC dans un délai de **7 jours calendaires**.

5-3 Preuve d'acceptation

L'AC conserve la preuve d'acceptation sous forme de formulaire signé ou de trace électronique datée pour une durée de 7 ans.

ARTICLE 6 : AUTORISATIONS AUTORISEES ET INTERDITES

6-1 Principe sur la génération des clés privées

Par défaut, la clé privée est générée et gardée par le titulaire ; l'AC **n'est pas dépositaire** des clés privées des utilisateurs.

6-2 Utilisations autorisées

Les certificats peuvent être utilisés pour :

- Authentification des utilisateurs et des équipements
- Signature électronique de documents et de transactions

6-3 Utilisations interdites

Sont strictement interdits :

- Tout usage frauduleux, illégal ou contraire à l'ordre public
- Toute utilisation hors du périmètre défini par la PC/DPC
- La falsification ou la modification non autorisée du certificat
- L'utilisation du certificat après sa révocation ou expiration

ARTICLE 7 : SUSPENSION & REVOCATION (PROCEDURE OPERATIONNELLE)

7-1 Motifs :

La révocation peut être demandée pour les motifs suivants :

- Compromission, perte ou vol du support ou de la clé privée
- Fin de fonction du titulaire (certificats organisationnels)
- Non-conformité constatée du certificat
- Demande légitime de l'abonné
- Décision de l'AC pour des raisons de sécurité avérée.

7-2 Demande de révocation :

Peut-être initiée par le titulaire, le mandataire, l'AC ou une Autorité habilitée ; doit être authentifiée (formulaire signé).

7-3 Délais de traitement :



Instruction de la demande : **24 heures ouvrées** (48 h weekend & jours fériés) ; suspension possible immédiatement si la suspicion est avérée.

7-4 Publication & disponibilité

Procédure

- **OCSP** : mise à jour immédiate en cas de révocation et publication selon SLA (OCSP mis à jour en permanence et disponible 24/7 ; latence nominale ≤ 2 s).
- **CRL** : publication sans délai et/ou à la prochaine génération de CRL selon mode opératoire ; points de distribution redondants 24/7.

7-5 Obligations des tiers utilisateurs

Vérifier l'état des certificats via OCSP ou CRL avant de se fier à un certificat.

ARTICLE 8 : **DISPONIBILITE & SLA (EXIGENCES MINIMALES)**

8-1 OCSP :

Disponibilité garantie $\geq$ 99,5 % / mois ; latence nominale $\leq$ 2 s.

8-2 CRL :

publication 24/7 sur points redondants ; mécanismes de basculement documentés (PCA).

8-3 Mesures en cas de non-respect :

Droits de l'abonné (remise en cause, réduction proportionnelle de frais, droit à indemnisation plafonnée tel que §10). (Détails contractuels dans annexes SLA).

ARTICLE 9 : **PROTECTION DES DONNEES A CARACTERE PERSONNEL**

9-1 Base légale du traitement

Le traitement des données personnelles est nécessaire à :

- L'exécution du contrat de certification
- Le respect des obligations légales et réglementaires
- La sauvegarde des intérêts vitaux de l'AC et des abonnés

9-2 Données collectées

L'AC collecte et traite les données suivantes :

- Identité civile du titulaire (nom, prénom, date de naissance)
- Coordonnées professionnelles (pour les certificats organisationnels)
- Preuves d'identité et documents justificatifs
- Historique des transactions et des vérifications

9-3 Durée de conservation

- Pendant la validité du certificat
- Plus **10 ans** après révocation ou expiration
- Puis **anonymisation ou destruction sécurisée**



9-4 Droits des personnes

Conformément au RGPD et à la Loi 2008-12, les personnes disposent des droits suivants :

- Droit d'accès et de rectification
- Droit à l'effacement dans les limites autorisées
- Droit de limitation du traitement

9-5 Contact DPO

Pour toute question relative à la protection des données :
khoulamou@gainde2000.sn

ARTICLE 10 : SECURITE DES CLEFS & HABILITATIONS

10-1 Clés CA & OCSP :

Elle stockées et protégées en HSM certifiés ; séparation des rôles et double contrôle pour opérations sensibles.

10-2 Habilitations :

Les rôles critiques sont attribués nominativement et font l'objet de vérifications et formations (DPC).

ARTICLE 11 : NOTIFICATIONS & GESTION DES INCIDENTS

11-1 Obligations de notification

Tout abonné ou mandataire doit notifier l'AC **immédiatement et au plus tard dans les 24 heures** :

- En cas de perte, vol ou compromission du support ou de la clé privée
- Lors de suspicion d'usage non autorisé du certificat
- En cas d'incident impactant la chaîne de confiance PKI

11-2 Canaux de notification

Les notifications doivent être envoyées par :

- Email sécurisé à : incident@gainde2000.sn
- Téléphone au : **[33 859 39 99]**
- Formulaire de contact sur le site officiel de l'AC (<http://www.confiancefactory.com>)

11-3 Communication de l'AC

L'AC s'engage à :

- Communiquer toute compromission majeure aux autorités compétentes dans les **24 heures**
- Informer les abonnés affectés dans les **48 heures**
- Publier un rapport d'incident conformément à la DPC §12-13

ARTICLE 12 : AUDITS, CONFORMITE & TRANSPARENCE

12-1 Audit et conformité

L'AC est auditée au moins tous les 24 mois par un organisme indépendant (PC/DPC).

12-2 Publication des documents

Les PC, DPC, CGU, CRL, OCSP, formulaires et rapports d'audit (résumés non sensibles) sont publiés sur le site officiel.

ARTICLE 13 : RESPONSABILITE, PLAFONDS ET ASSURANCE

13-1 Principe général

La responsabilité du Fournisseur/Autorité de Certification est limitée aux dommages directs, personnels et certains, résultant d'une faute prouvée dans l'exécution de ses obligations. Cette limitation ne s'applique pas en cas de faute lourde, de manquement intentionnel, ou lorsque la loi en dispose autrement (notamment pour les services de confiance qualifiés soumis au règlement eIDAS).

13-2 Plafonds d'indemnisation

Sous réserve des dispositions légales impératives, les montants maximaux d'indemnisation sont fixés comme suit :

- Certificat utilisateur individuel : jusqu'à 250 000 FCFA ;
- Certificat organisationnel ou serveur : jusqu'à 500 000 FCFA ;
- Certificat d'administration ou de signature applicative : jusqu'à 1 000 000 FCFA.

Ces plafonds pourront être révisés en fonction des garanties d'assurance et des conditions contractuelles convenues avec l'assureur.

13-3 Certificats qualifiés

Pour les certificats de signature qualifiés, les limitations ci-dessus ne s'appliquent que dans la mesure permise par la législation en vigueur. Les obligations légales du Prestataire de Services de Confiance Électronique (TSP) au titre du règlement eIDAS et des textes nationaux prévalent sur toute clause contraire.

13-4 Assurance

L'Autorité de Certification maintient en permanence une couverture d'assurance responsabilité civile professionnelle, destinée à garantir la réparation des dommages directs causés à ses clients ou utilisateurs dans le cadre de ses activités de certification électronique.

13-5 Exclusions

Préjudice indirect, perte de bénéfices, ainsi que situations résultant d'une négligence grave du titulaire (sauf si imputable au PSCE).

ARTICLE 14 : MODIFICATION DES CGU

Toute modification substantielle des présentes Conditions Générales d'Utilisation (CGU) DPC / PC fera l'objet d'une notification préalable adressée aux utilisateurs par tout moyen approprié, notamment par courrier électronique.

Ces modifications entreront en vigueur **cinq (5) jours calendaires** après leur notification, sauf disposition légale contraire.

En cas de désaccord avec les nouvelles dispositions, l'utilisateur dispose du droit de refuser les modifications et de résilier son contrat sans frais ni pénalité, sous réserve d'en informer l'Autorité de Certification avant la date d'entrée en vigueur desdites modifications.

ARTICLE 15 : PUBLICATION, VERSION & CONTACTS

Documents publics : PC, DPC, CGU, CRL, OCSP, formulaires. Liens : [site officiel : <http://www.confiancefactory.com>].

Contacts: Procédure

DPO — dpo@gainde2000.sn;

Support helpDesk — [33 859 39 99].

ARTICLE 16 : REGLEMENT DES LITIGES

16-1 Réclamation et règlement amiable

Tout utilisateur dispose d'un droit de réclamation auprès de l'Autorité de Certification (AC). La réclamation doit être formulée par écrit.

- Un accusé de réception est délivré dans un délai de 24 heures ;
- Une réponse substantielle est communiquée dans un délai de 7 jours ;
- Une réponse détaillée est transmise dans un délai maximal de 10 jours.

16-2 Escalade interne

En cas de réponse jugée insatisfaisante, la réclamation peut être portée successivement devant :

- Le Responsable de la Sécurité des Systèmes d'Information (RSSI) ;
- La Direction de la Conformité ;
- La Direction Générale de l'AC.

16-3 Recours externe et contentieux

Si le litige persiste après épuisement des recours internes, les parties s'engagent à recourir à une procédure de médiation préalable, sauf en cas d'urgence ou de mesure conservatoire nécessaire. À défaut d'accord à l'issue de la médiation, le différend sera tranché conformément au droit sénégalais par les tribunaux compétents de Dakar.

16-4 Mesures conservatoires

Pour des raisons de sécurité ou en cas d'enquête interne, l'AC se réserve le droit de suspendre temporairement un service en cas de risque majeur avéré.

ARTICLE 17 : LOI APPLICABLE & JURIDICTION COMPETENTE

Les présentes CGU sont régies par le droit sénégalais.

Tout différend relatif à leur interprétation ou à leur exécution relève de la compétence exclusive des tribunaux de Dakar.

Avant toute action judiciaire, les parties s'engagent à recourir à une procédure de médiation, sauf en cas d'urgence ou de mesure conservatoire nécessaire.

ARTICLE 18 : DISPOSITIONS FINALES

18-1 Durée et entrée en vigueur

Les présentes CGU :

- S'appliquent pendant toute la durée du contrat de souscription, conclu pour un an renouvelable tacitement.



- Entrent en vigueur à la date de leur publication
- Remplacent toute version antérieure
- Sont archivées pendant **7 ans** après leur abrogation

Procédure

18-2 Nullité partielle

Si une disposition des présentes CGU est déclarée nulle ou inapplicable, les autres dispositions conservent pleinement leur effet.

18-3 Langue

Les présentes CGU sont rédigées en français. En cas de contradiction avec une traduction, la version française prévaut