POLITIQUE DE CERTIFICATION

AC INTERMEDIAIRE SUNU ORGANIZATION

Nature du Document	Gouvernance
Référence	PC-ORG-SUNU-01
Date	Juillet 2026
Emetteur	GAINDE 2000
Destinataires	Public
Version	**1.3.7**
Nombre de page	13

Date	Auteur	Version	Evolutions
17/07/2023	Responsable Contrôle, Référentiel Documentaire & Projet	**1.0**	Première version
01/09/2025	Responsable Pole PKI	**1.3.1**	Modifications

Date	Auteur	Version	Evolutions
22/07/2026	Responsable Pole PKI	**1.3.7**	Ajout de la référence [PROFILS], clarification des usages, certificats de test, algorithmes, tailles de clés, suspension non pratiquée

Table des matières

1 OBJET ET PORTEE

La présente Politique de Certification définit les règles applicables aux certificats émis par l'Autorité de Certification intermédiaire **SUNU Organization**, opérée par **GAINDE 2000 – Confiance Factory** et subordonnée à l'Autorité Racine **SUNU ROOT**.
Sauf mention contraire explicite, les certificats émis par l'AC SUNU Organization dans le cadre de la présente PC sont des certificats non qualifiés au sens du règlement eIDAS applicable et relèvent du niveau d'assurance défini dans le tableau OID de la présente PC. Les exigences CA/Browser Forum ne sont applicables que si des certificats relevant explicitement de ce périmètre sont émis.

2 IDENTIFICATION DU DOCUMENT

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

OID de la Politique de Certification	**1.3.6.1.4.1.45491.2.1.1**

3 REFERENCES DOCUMENTAIRES ET NORMATIVES

- PC SUNU ROOT v1.2 (OID: **1.3.6.1.4.1.45491.2.1**)
- DPC SUNU ORGANIZATION v1.4
- CGU SUNU v1.2
- [PROFILS] – Profils de certificats, LCR, OCSP et algorithmes applicables à l'AC SUNU Organization, version en vigueur
- ETSI EN 319 401
- ETSI EN 319 411-1 Niveau NCP
- ETSI EN 319 411-2, uniquement si applicable aux certificats qualifiés ;
- CA/Browser Forum Baseline Requirements, uniquement si des certificats relevant explicitement de ce périmètre sont émis ;
- Règlement eIDAS, uniquement lorsque le service concerné relève d'un usage eIDAS applicable.
- Loi n° 2008-12 relative à la protection des données personnelles (Sénégal)
- ISO/IEC 27001

Le document [PROFILS] précise les paramètres techniques détaillés des certificats, notamment les extensions X.509, les usages de clés, les OID de politiques, les algorithmes, les tailles de clés, les durées de validité, les points de distribution CRL et les informations OCSP. En cas de divergence entre la présente PC et le document [PROFILS], l'exigence la plus restrictive prévaut, sauf décision formelle documentée et approuvée par l'AC.

4 HIERARCHIE DOCUMENTAIRE ET GOUVERNANCE

- Cette PC **hérite des principes et exigences minimales** de la PC SUNU ROOT.
- En cas de divergence entre la présente PC et la PC ROOT, **la PC ROOT prévaut**.

- Les modalités opérationnelles sont définies dans la **DPC SUNU Organization**.
- La CGU régit la relation contractuelle avec les abonnés.
- L'OID et la version de la présente PC sont publiés et archivés.

5 DEFINITION DES ROLES ET RESPONSABILITES

5.1 Autorités de Certification et fonctions de l'IGC

L'Autorité de Certification est responsable vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. A ce titre, elle édicte la Politique de Certification et valide les Déclarations de Pratique de Certification respectées par les différentes composantes de l'Infrastructure à Clé Publique.

La garantie apportée par l 'Autorité de Certification vient de la qualité des techniques misent en œuvre, mais aussi du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter.

- **Autorité d'enregistrement (AE)** - Cette fonction vérifie les informations d'identification du futur sujet d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC (cf. ci-dessous). L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du sujet du certificat lors du renouvellement du certificat de celui-ci.
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du sujet provenant soit du bénéficiaire, soit de la fonction de génération des éléments secrets du bénéficiaire, si c'est cette dernière qui génère la bi- clé du certificat.
- **Fonction de génération des éléments secrets du bénéficiaire** - Cette fonction génère les éléments secrets à destination du bénéficiaire, et les prépare en vue de leur remise au bénéficiaire (par exemple, personnalisation

de la carte à puce destinée au porteur, courrier sécurisé avec le code d'activation, etc.). Ces éléments secrets sont directement la bi-clé du certificat, les codes (activation / déblocage) sont liés au dispositif de stockage de la clé privée du bénéficiaire.

- **Fonction de remise au bénéficiaire**- Cette fonction remet au bénéficiaire au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif cryptographique, clé privée du porteur, codes d'activation, …).
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux bénéficiaires et/ou aux utilisateurs de certificats, hors informations d'état des certificats. L'AC ne met pas à disposition les certificats valides de ses bénéficiaires.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation (notamment l'identification et l'authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers : LCR, LAR.

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- **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.
- **Mandataire de certification (MC)** - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des

bénéficiaires de cette entité (il assure notamment le face-à-face pour l'identification des bénéficiaires lorsque celui-ci est requis).

- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du bénéficiaire du certificat.

Dans le cadre de ses fonctions opérationnelles, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Être une entité légale au sens de la loi sénégalaise.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des bénéficiaires de cette entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux bénéficiaires, aux utilisateurs de certificats, … qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions de la présente PC, notamment en matière de génération des certificats, de remise au bénéficiaire, de gestion des révocations et d'information sur l'état des certificats.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR), ou faire renouveler ses

certificats si l'AC est rattaché à un AC hiérarchiquement supérieur. Diffuser ses certificats d'AC aux bénéficiaires et utilisateurs de certificats.

5.2 AUTORITE D'ENREGISTREMENT

L'Autorité d'Enregistrement applique des procédures d'identification des personnes physiques ou morales, conformément aux règles définies par l'Autorité de Certification. Son but est d'établir que le demandeur a bien l'identité et les qualités qui seront indiquées dans le certificat. Ces procédures d'identification sont variables selon le niveau de confiance que l'on entend apporter à cette vérification.

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification et le bénéficiaire. Qu'elle soit ou non directement en contact physique avec le bénéficiaire, elle reste dépositaire de ses informations personnelles.

Sa responsabilité ne peut être engagée que par l'Autorité de Certification. L'Autorité de Certification a un devoir de contrôle et d'audit des Autorités d'Enregistrement.

L'AE a pour rôle de vérifier l'identité du futur sujet du certificat. Pour cela, l'AE assure les tâches suivantes:

- la prise en compte et la vérification des informations du futur sujet et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- le cas échéant, la prise en compte et la vérification des informations du futur MC et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du bénéficiaire ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

Cette fonction de validation ne peut en aucun cas être déléguée à un tiers.

5.3 PORTEURS DE CERTIFICATS

Dans le cadre de la présente PC, un porteur de certificats ne peut être qu'une personne physique.

Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle il a un lien contractuel / hiérarchique / réglementaire.

5.4 UTILISATEURS DE CERTIFICATS

L'utilisateur du certificat peut être ;

- Une entité ou une personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du bénéficiaire du certificat.
- Un serveur sous la responsabilité d'une personne physique ou morale, qui utilise un certificat et un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat. L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.

6 TYPES DE CERTIFICATS ET USAGES AUTORISES

La présente Politique de Certification couvre les certificats émis par l'AC **SUNU Organization**, subordonnée à l'Autorité Racine **SUNU ROOT**. Ces certificats sont destinés à des usages de **signature électronique** et d'**authentification**, conformément aux OID définis dans la présente PC, aux règles de nommage, aux procédures d'identification et aux exigences précisées dans la DPC applicable.

Les paramètres techniques détaillés applicables à chaque type de certificat, notamment les extensions X.509, les usages de clés, les OID de politiques, les

algorithmes, les tailles de clés, les durées de validité, les points de distribution CRL et les informations OCSP, sont définis dans le document **[PROFILS] – Profils de certificats, LCR, OCSP et algorithmes**.

6.1 CERTIFICATS DE SIGNATURE

Les certificats de signature émis par l'AC **SUNU Organization** sont destinés à permettre à un porteur, personne physique identifiée dans le certificat, d'apposer une signature électronique dans le cadre de ses activités et de son lien avec l'entité mentionnée dans le certificat.

Ces certificats peuvent être utilisés pour :

- signer électroniquement des documents, messages ou données ;
- assurer l'intégrité des données signées ;
- permettre la vérification de l'identité du signataire ;
- contribuer à la non-répudiation de l'origine, dans les limites prévues par la présente PC, la DPC et les CGU applicables.

L'usage de la clé privée associée au certificat de signature est strictement réservé au porteur identifié dans le certificat. Le porteur est responsable de la protection de sa clé privée et doit signaler sans délai toute suspicion de compromission, de perte de contrôle ou d'usage non autorisé.

Les certificats de signature sont identifiés par l'OID de politique correspondant dans le tableau des OID de la présente PC. Les paramètres techniques associés, notamment le **Key Usage**, les extensions X.509, les algorithmes et la durée de validité maximale, sont définis dans le document **[PROFILS]**.

6.2 CERTIFICATS D'AUTHENTIFICATION

Les certificats d'authentification émis par l'AC **SUNU Organization** sont destinés à permettre l'authentification forte d'un porteur auprès d'un service, d'une application, d'un système d'information ou d'une plateforme autorisée.

Ces certificats peuvent être utilisés pour :

- authentifier le porteur auprès d'un système ou d'une application ;

- établir un lien fiable entre une identité vérifiée et une clé publique ;
- sécuriser l'accès à des services numériques autorisés ;
- contribuer à la protection des échanges électroniques, selon les usages prévus par la présente PC et la DPC.

Le certificat d'authentification ne doit pas être utilisé comme certificat de signature lorsque cet usage n'est pas prévu dans son profil technique. Les usages autorisés sont limités à ceux définis dans le certificat, dans la présente PC, dans la DPC et dans le document **[PROFILS]**.

Les certificats d'authentification sont identifiés par l'OID de politique correspondant dans le tableau des OID de la présente PC. Les paramètres techniques associés, notamment le **Key Usage**, l'**Extended Key Usage**, les extensions X.509, les algorithmes et la durée de validité maximale, sont définis dans le document **[PROFILS]**.

6.3 CERTIFICATS DE TEST

GAINDE 2000 – Confiance Factory peut être amenée à émettre des certificats de test dans le cadre de la validation technique de ses services, de ses plateformes, de ses procédures internes ou de ses intégrations avec des tiers.

Lorsque ces certificats de test sont émis par l'AC **SUNU Organization** de production, au moyen de la même clé de signature d'AC que les certificats de production, ils sont considérés comme des certificats émis dans le périmètre de la présente Politique de Certification. À ce titre, leur émission, leur gestion, leur révocation, leur journalisation et leur publication via les mécanismes CRL et OCSP sont soumises aux mêmes exigences de traçabilité et de contrôle que les certificats de production.

Aucune exclusion de périmètre n'est revendiquée pour les certificats de test signés par la clé de l'AC **SUNU Organization** de production.

Les certificats de test doivent être identifiés de manière non ambiguë, notamment :

- par une mention explicite dans le DN du certificat, par exemple dans le champ **OU** ou **CN** ;
- par une désignation permettant de distinguer clairement le certificat de test d'un certificat de production.

L'utilisation d'une mention explicite de test dans le DN constitue une exception admise au principe général de nommage fondé sur une identité authentifiée. Cette exception

est limitée aux certificats de test et doit être documentée dans la présente PC ainsi que dans le document **[PROFILS]**.

Les certificats de test :

- ne sont couverts par aucune garantie contractuelle de la part de GAINDE 2000 – Confiance Factory ;
- ne doivent être utilisés qu'à des fins de test, de validation technique ou d'intégration ;
- ne doivent pas être utilisés dans un contexte de production opérationnelle ;
- ne doivent pas être utilisés pour créer des effets juridiques ;
- doivent avoir une durée de validité limitée, comprise entre **un (1) mois et six (6) mois**, sauf justification documentée et approuvée.

Les données d'enregistrement, journaux techniques, preuves d'émission, événements de révocation et traces associées aux certificats de test suivent le même régime de conservation que les certificats de production, sauf décision contraire formellement documentée, justifiée et approuvée par les responsables compétents.

Le bénéficiaire ou l'utilisateur d'un certificat de test assume seul les conséquences de tout usage non conforme à la restriction d'usage définie dans le présent article.

Tout utilisateur de certificat ou tiers de confiance doit vérifier l'identifiant de politique, les usages autorisés et les mentions présentes dans le certificat avant de lui accorder confiance. La présence d'un certificat dans les mécanismes de publication CRL ou OCSP ne suffit pas, à elle seule, à qualifier le certificat comme certificat de production.

Les modalités techniques détaillées applicables aux certificats de test, notamment l'OID dédié, les extensions X.509, les usages de clé, la durée de validité, les règles de nommage et les contrôles de révocation, sont définies dans le document **[PROFILS]**.

6.4 USAGES INTERDITS

Les certificats émis par l'AC **SUNU Organization** ne doivent être utilisés que pour les usages explicitement autorisés par la présente Politique de Certification, la DPC, les CGU applicables et le document **[PROFILS]**.

Sont notamment interdits :

- l'utilisation d'un certificat en dehors de son usage prévu ;

- l'utilisation d'un certificat de signature à des fins d'authentification lorsque cet usage n'est pas prévu par son profil ;
- l'utilisation d'un certificat d'authentification à des fins de signature lorsque cet usage n'est pas prévu par son profil ;
- l'utilisation d'un certificat de test dans un contexte de production ou pour créer des effets juridiques ;
- l'utilisation d'un certificat pour signer d'autres certificats ou des LCR ;
- l'utilisation d'un certificat à des fins d'interception, de falsification, d'usurpation d'identité, de contournement de contrôles de sécurité ou d'attaque de type **man-in-the-middle** ;
- la revente, la délégation non autorisée ou la mise à disposition d'un certificat à un tiers non autorisé ;
- tout usage contraire à la loi, aux obligations contractuelles ou aux règles définies par GAINDE 2000 – Confiance Factory.

Tout usage non conforme engage la responsabilité du bénéficiaire ou de l'utilisateur concerné. GAINDE 2000 – Confiance Factory ne garantit pas les conséquences d'un usage réalisé en dehors du périmètre autorisé par la présente PC, la DPC, les CGU et le document **[PROFILS]**.

7 IDENTIFICATION ET AUTHENTIFICATION

- Vérification d'identité basée sur des pièces officielles et sources fiables.
- Enregistrement par AE agréée.
- Conservation des preuves d'identité pour une durée minimale de 10 ans.
- Niveaux d'assurance conformes à ETSI EN 319 411-1.

Les modalités détaillées d'identification, de vérification de l'identité du porteur, de validation de son lien avec l'entité de rattachement, de constitution du dossier d'enregistrement et de conservation des preuves sont définies dans la DPC et les procédures d'enregistrement applicables.

8 ÉMISSION, RENOUVELLEMENT ET REVOCATION

- Délais de traitement standard :
  - Émission après validation : ≤ 1 jour ouvré.
  - Révocation : ≤ 24 heures ouvrées (48 h week-end/fériés).
- Publication CRL sous 24 h maximum, OCSP immédiatement.
- Révocation possible en cas de doute sur la validité ou compromission.
- Notification à l'abonné et aux relying parties sous 24 h.
- Procédure documentée dans la DPC.

L'AC SUNU Organization ne pratique pas la suspension des certificats. En cas de doute sur la validité, la compromission ou l'usage du certificat, la révocation est appliquée selon la procédure définie dans la DPC.

Les étapes détaillées de validation, d'approbation, d'émission, de remise, de renouvellement, de révocation, de publication de l'état et de notification sont définies dans la DPC et les procédures opérationnelles associées.

9 GESTION DES CLES PRIVEES ET RESPONSABILITES

9.1 PROTECTION DES CLES PRIVEES

- Les clés de l'AC Organization sont générées et stockées dans des HSM certifiés FIPS 140-2 L3 ou CC EAL4+.
- La génération des clés des abonnés peut être locale (titulaire) ou centralisée (custody) avec mesures de sécurité équivalentes.
- Le titulaire est responsable de la protection de sa clé privée.
- La compromission doit être signalée immédiatement.

9.2 ALGORITHMES CRYPTOGRAPHIQUES APPLICABLES

- Les certificats porteurs émis par l'AC **SUNU Organization** utilisent des mécanismes cryptographiques conformes aux exigences définies dans la présente Politique de Certification, dans la DPC applicable et dans le document **[PROFILS]**.

- Les algorithmes autorisés pour les certificats porteurs sont précisés dans le document **[PROFILS]**, qui constitue la référence technique détaillée pour les profils de certificats, les extensions X.509, les LCR, l'OCSP et les paramètres cryptographiques.
- À titre de synthèse, les certificats porteurs peuvent reposer sur les familles d'algorithmes suivantes, sous réserve de leur activation dans les profils applicables :

Famille d'algorithme	**Paramètres admis**
RSA	RSA avec une complexité minimale équivalente à **2048 bits**
ECDSA	Courbes **P-256** ou **P-384**
EdDSA / Edwards	**Ed25519**

- Les fonctions de hachage et algorithmes de signature effectivement utilisés sont définis dans le document **[PROFILS]** et doivent rester cohérents avec les recommandations cryptographiques applicables.
- L'utilisation d'algorithmes obsolètes ou insuffisamment robustes, notamment **MD5**, **SHA-1**, **RSA inférieur à 2048 bits**, ou de courbes elliptiques non prévues par le document **[PROFILS]**, est interdite pour toute nouvelle émission de certificat.
-

9.3 TAILLE DES CLES

- Les tailles de clés utilisées pour les certificats porteurs émis par l'AC **SUNU Organization** doivent respecter les exigences minimales définies dans le document **[PROFILS]**.
- À titre de règle générale, les paires de clés associées aux certificats porteurs doivent présenter une robustesse minimale équivalente à :

Algorithme	**Taille / courbe minimale**
RSA	**2048 bits minimum**
ECDSA	**P-256** ou **P-384**
EdDSA / Edwards	**Ed25519**

- Les paramètres détaillés par type de certificat — certificat de signature, certificat d'authentification ou tout autre profil relevant de l'AC SUNU Organization — sont définis dans le document **[PROFILS]**.
- En cas de divergence entre la présente section et le document **[PROFILS]**, l'exigence la plus restrictive prévaut, sauf décision formelle de l'AC documentée, approuvée et limitée dans le temps.
- Toute évolution des tailles de clés, algorithmes ou paramètres cryptographiques doit faire l'objet d'une revue formelle et, le cas échéant, d'une mise à jour coordonnée de la PC, de la DPC et du document **[PROFILS]**.

10 ACCEPTATION DU CERTIFICAT

10.1 DEMARCHE D'ACCEPTATION DU CERTIFICAT

Le certificat étant mis à la disposition du bénéficiaire, le fait que ce dernier procède à son retrait vaut, de sa part, acceptation du certificat dans les conditions commerciales, juridiques et techniques définies par l'AC. La première utilisation du certificat vaut également acceptation tacite.

Compte tenu du risque d'erreur de saisie inhérent à un processus d'enrôlement reposant sur des pièces au format papier, l'AC met en œuvre un contrôle de vérification formelle du contenu du certificat avant que l'acceptation ne devienne opposable :

- Lors de la notification de délivrance (cf. §10.3), l'AE transmet au bénéficiaire un récapitulatif lisible du contenu du champ Subject (Common Name, Organisation, Organizational Unit, et tout autre attribut identifiant) tel qu'il figure dans le certificat émis.
- Le bénéficiaire dispose d'un délai de quinze (15) jours pour vérifier la conformité de ce contenu avec les données qu'il a fournies lors de l'enregistrement, et pour signaler à l'AC toute anomalie constatée, par téléphone, courriel ou courrier simple.
- L'absence de signalement dans ce délai vaut confirmation expresse, par le bénéficiaire, de l'exactitude du contenu du certificat, et acceptation définitive au sens du présent article.
- En cas d'anomalie signalée, l'AC procède à la révocation du certificat erroné et à l'émission d'un nouveau certificat selon la procédure définie au chapitre 4.9, sans frais supplémentaire pour le bénéficiaire si l'erreur est imputable à l'AE.

La première utilisation du certificat, avant l'expiration du délai de quinze (15) jours, vaut également acceptation tacite du contenu du certificat par le bénéficiaire. En acceptant un certificat, le bénéficiaire reconnaît expressément consentir aux termes et aux

conditions d'utilisation contractuelles et, plus généralement, à tous les éléments publiés dans la présente Politique de certification de l'AC.

10.2 PUBLICATION DU CERTIFICAT

Les certificats émis ne font pas l'objet d'une publication par l'AC.

10.3 NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT

L'AC imprime des courriers d'accompagnement pour informer de la délivrance du certificat.

- Notification auprès du bénéficiaire.
- Notification auprès du bureau de remise si applicable.
- Le cas échéant notification au mandataire de certification.

L'AE synchronise l'état des demandes de délivrance, avec l'état de production de l'AC. L'AE filtre les demandes de façon à réaliser un suivi des retours des avis de remise.

11 PUBLICATION ET DISPONIBILITE (CRL/OCSP)

- OCSP disponible 24/7 avec une disponibilité garantie ≥ 99,5 %.
- Latence OCSP ≤ 2 secondes.
- CRL publiée immédiatement après révocation et au minimum toutes les 24 h.
- Points de distribution redondants.
- Supervision continue et journalisation des événements.

12 DONNEES PERSONNELLES ET CONFORMITE LEGALE

- Traitement conforme à la Loi n° 2008-12.
- Conservation des données : 10 ans après expiration.

- Droits : accès, rectification, opposition, suppression.
- Contact DPO : dpo@gainde2000.sn.
- Consentement de l'abonné intégré au processus de demande.

13 NOTIFICATIONS D'INCIDENTS ET COMMUNICATION

- Notification aux autorités de supervision et parties concernées sous 24 h.
- Notification aux abonnés affectés par e-mail et SMS.
- Publication d'un avis d'incident sur le site officiel.
- Rapport post-mortem obligatoire pour tout incident majeur.
- Registre des incidents conservé 10 ans.

14 RESPONSABILITES, LIMITATIONS ET GARANTIES

- Responsabilités définies selon les CGU.
- Limitation de responsabilité selon type de certificat.
- Exclusions en cas de fraude, négligence grave ou usage non conforme.
- Pour les certificats qualifiés, les obligations légales priment sur les limitations contractuelles.

15 AUDITS ET SUPERVISION

- L'AC SUNU Organization fait l'objet de revues internes et, le cas échéant, d'audits de conformité selon les référentiels applicables à son périmètre, notamment ETSI EN 319 401 et ETSI EN 319 411-1 niveau NCP. Les exigences eIDAS ou ETSI EN 319 411-2 ne sont applicables que lorsque le service ou le certificat concerné relève explicitement de ce périmètre.
- Audits annuels indépendants et internes.

- Revues internes périodiques (au moins une fois/an).
- Lorsqu'un rapport d'audit résumé ou une attestation de conformité est disponible et destiné à publication, il est publié selon les modalités définies par l'AC et les exigences applicables.

16 REVISION, MODIFICATION ET PUBLICATION

- Toute modification majeure est notifiée aux abonnés au moins 30 jours avant son entrée en vigueur.
- Notification par e-mail et/ou SMS.
- Historique de version et archivage conservés.
- Publication sur le site officiel de Confiance Factory http://www.confiancefactory.com.

17 TABLEAU OID ↔ USAGES ↔ EXIGENCES

OID	Type de certificat	Usage autorisé	Niveau d'assurance	Publication CRL/OCSP	Révocation
1.3.6.1.4.1.45491.2.1.1.1	Signature	Signature électronique	Élevé	24 h / temps réel	24 h
1.3.6.1.4.1.45491.2.1.1.2	Authentification utilisateur	Authentification forte	Élevé	24 h / temps réel	24 h
Défini dans [PROFILS]	Certificat de test	Test, validation technique, intégration	Interne / Test	Identique aux certificats de productio	Selon procédure standard

				n	

18 GLOSSAIRE

Terme	Définition
PC	Politique de Certification
DPC	Déclaration des Pratiques de Certification
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List
RA	Registration Authority
CA	Certification Authority
TSP	Trusted Service Provider
OID	Object Identifier
MITM	Man-in-the-middle
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