REPOBLIKAN'I MADAGASIKARA

MINISTÈRE DU DÉVELOPPEMENT NUMÉRIQUE, DES POSTES ET DES TÉLÉCOMMUNICATIONS
****

DÉCRET N° 2025-1602
Fixant les modalités d'application de la Loi n°2014-025 du 10 décembre 2014 sur la signature électronique

Le Premier Ministre, Chef du Gouvernement,

Vu la Constitution ;
Vu la décision n° 10-HCC/D3 du 14 octobre 2025 accordant à l'autorité militaire compétente, représentée par le Colonel RANDRIANIRINA Michael, l'exercice des fonctions de Chef de l'Etat ;
Vu la Loi n° 66-003 du 02 juillet 1966 relative à la Théorie Générale des Obligations, modifiée et complétée par la Loi n°2015-036 du 03 février 2016, notamment l'insertion de la notion de la signature électronique à l'article 272.1 ;
Vu la Loi n° 2014-006 du 17 juillet 2014 modifiée et complétée par la Loi n°2016-031 du 23 août 2016 sur la lutte contre la cybercriminalité ;
Vu la Loi n° 2014-024 du 10 décembre 2014 sur les transactions électroniques ;
Vu la Loi n° 2014-025 du 10 décembre 2014 sur la signature électronique ;
Vu la Loi n° 2014-026 du 10 décembre 2014 fixant les principes généraux relatifs à la dématérialisation des procédures administratives ;
Vu la Loi n° 2014-038 du 09 janvier 2015 sur la protection des données à caractère personnel ;
Vu le Code de Procédure Civile Malagasy, modifié et complété par la Loi n° 2015-035 du 03 février 2016, notamment en son article 9.2 nouveau ;
Vu la Loi n° 2018-027 du 08 février 2019 relative à l'état civil ;
Vu la Loi n° 2025-019 du 27 août 2025 relative à l'identification des personnes physiques ;
Vu le Décret n° 2022-866 du 08 juin 2022 portant création de l'Unité de Gouvernance Digitale (UGD) et fixant ses Statuts ;
Vu le Décret n° 2023-515 du 09 mai 2023 relatif au Numéro Unique d'Identification (NUI) ;
Vu le Décret n° 2023-1541 du 06 décembre 2023, modifié et complété par le Décret n° 2025-696 du 18 juin 2025 portant attributions, organisation et fonctionnement de la Commission Malagasy de l'Informatique et des Libertés (CMIL) ;
Vu le Décret n° 2024-107 du 31 janvier 2024 fixant les attributions du Ministre du Développement Numérique, des Postes et des Télécommunications ainsi que l'organisation générale de son Ministère ;
Vu le décret n° 2025-1101 du 20 octobre 2025 portant nomination du Premier Ministre, Chef du Gouvernement ;
Vu le décret n° 2025-1114 du 28 octobre 2025 portant nomination des membres du Gouvernement ;

Sur proposition du Ministre du Développement Numérique, des Postes et des Télécommunications,

En Conseil du Gouvernement,

D É C R È T E :

TITRE I
DISPOSITIONS GÉNÉRALES

CHAPITRE PREMIER : FONDAMENTAUX SUR LA CONFIANCE NUMÉRIQUE

Article 1 - Objet

Le présent décret, pris en application de la loi n° 2014-025 du 10 décembre 2014 relative à la signature électronique, fixe les modalités techniques, juridiques et institutionnelles encadrant la mise en œuvre de la signature électronique.

Il institue un Espace Numérique de Confiance « ENC » destiné à garantir la sécurité, la fiabilité et la reconnaissance juridique des services de confiance, notamment ceux relatifs à la certification de signature électronique et de cachet électronique.

Il désigne l'Unité de Gouvernance Digitale « UGD » comme Autorité Nationale de Confiance Numérique « ANCN », chargée de la régulation, de l'accréditation, de la supervision et de la gestion de la racine de confiance nationale, assurant également les fonctions de prestataire public qualifié « PSCo public » pour les besoins de l'État.

Article 2 - Définitions

Les termes ci-après sont entendus au sens des définitions suivantes :

Accréditation : attestation délivrée par une autorité de contrôle et d'évaluation de la conformité constituant une reconnaissance formelle de la compétence à réaliser des activités spécifiques ;

Agrément : autorisation écrite accordée à un prestataire de services de confiance lui permettant d'opérer au niveau national des prestations de certification de signature ou de cachet électronique ;

Authentification : processus permettant au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature ;

Autorité Nationale de Confiance Numérique : Autorité nationale chargée de la régulation, supervision et accréditation des services de confiance ;

Biométrie : ensemble des techniques informatiques d'identification et d'authentification permettant de reconnaître automatiquement un individu bien déterminé à partir de ses caractéristiques physiques, biologiques, voire comportementales, tout en se basant sur le traitement informatisé des données collectées ;

Cachet électronique : par analogie à un cachet physique, un cachet électronique désigne une signature électronique associée à une personne morale et pouvant être utilisée par plusieurs personnes physiques au sein de cette entité dans le cadre de leurs interactions avec les tiers ;

Certificat de conformité de dispositif de certification électronique : document délivré par un organisme accréditeur attestant que le dispositif de création de signature électronique respecte les normes et standards techniques internationaux. Ce certificat garantit que le dispositif est sécurisé, fiable et capable de produire des signatures électroniques conformes aux standards légaux, assurant ainsi l'intégrité et l'authenticité des documents signés ;

Certificat de signature électronique : attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et qui confirme au moins le nom ou le cas échéant le pseudonyme de cette personne ;

Certificat électronique : document numérique délivré au titulaire de la signature, qui atteste de l'authenticité de la signature électronique ou du cachet électronique, et qui lie cette signature à une identité via un dispositif de création de signature ;

Certificate Revocation List - CRL : liste électronique, régulièrement mise à jour par une autorité de certification, recensant les certificats numériques qu'elle a émis et qui ont été révoqués avant leur date d'expiration, et qui ne doivent plus être considérés comme valides.

Confidentialité : état de sécurité permettant de garantir le secret des informations et ressources stockées dans les réseaux et systèmes de communication électroniques, systèmes d'information et/ou des équipements terminaux, afin d'en prévenir la divulgation non autorisée d'informations à des tiers, par la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

Dispositif de certification : ensemble des moyens matériels, logiciels ou technologiques mis en œuvre par le prestataire de services de confiance pour générer et gérer des certificats électroniques ainsi que pour garantir la sécurité des dispositifs de création de signatures électroniques ;

Dispositif de création de signature électronique ou de cachet électronique : tout matériel et/ou logiciel comportant les éléments distinctifs caractérisant le signataire, destiné à mettre en application les données de création de signature électronique et servant à la création de cette demande ;

Données biométriques : caractéristique physique ou biologique spécifique permettant d'identifier une personne, éléments prépondérants de l'identité numérique d'une personne ;

Fiabilité : aspect du caractère intègre de l'identification du signataire et l'adhésion à l'acte par le titulaire de la signature électronique ;

Identification électronique : processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou une personne morale, ou une personne physique représentant une personne morale ;

Intégrité : qualité garantissant que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte ;

Online Certificate Status Protocol , OCSP : protocole normalisé permettant à un système de vérifier en temps réel l'état de validité d'un certificat numérique auprès de l'autorité de certification qui l'a émis, notamment pour déterminer s'il est valide, révoqué ou expiré.

Prestataire de services de certification électronique : personne morale qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique

Prestataire de services de confiance : personne morale offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

Révocation : une procédure engagée par un titulaire de la signature électronique qui vise le refus de la véridicité des données qui le concernent figurant sur le certificat attestant la signature électronique ;

Service de certification de signature électronique de confiance :

Tout service fourni par un prestataire de services de confiance consistant à :

- Créer et gérer des certificats électroniques relatifs aux signatures électroniques ;
- Valider les signatures électroniques et assurer leur vérification de conformité ;
- Fournir un service d'horodatage électronique garantissant l'intégrité et la date certaine des signatures ;
- Conserver ou archiver les signatures électroniques et les certificats qui y sont associés, conformément aux exigences légales et réglementaires.

Signataire : toute personne habilitée à signer qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou personne physique ou morale qu'elle représente ;

Signature électronique : donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques qui sert de méthode d'authentification de l'identité d'un signataire ;

Système biométrique : système permettant l'enrôlement des données biométriques d'une personne dans une banque de données pour pouvoir effectuer sa reconnaissance et son identification ;

Validation : processus de vérification et de confirmation de la validité d'une signature électronique et être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Article 3 - Champ d'application

Le présent décret s'applique à l'ensemble des acteurs intervenant dans le domaine de la signature électronique à Madagascar, notamment :

- Les prestataires de services de confiance, qu'ils soient publics ou privés;
- Les usagers, personnes physiques ou morales, qui recourent à la signature électronique dans le cadre de leurs échanges numériques;
- Les entités administratives et institutions publiques utilisant ou fournissant des services de certification ou de signature électronique.

Article 4 - Types de signature électronique

La signature électronique est de trois types, chacun étant déterminé par le niveau d'avancée technologique et de fiabilité requis en fonction de son utilisation :

- la signature simple,
- la signature avancée,
- la signature qualifiée.

La durée de validité des certificats associés à chaque type de signature est fixée à l'article 39 du présent décret.

Article 5 - Signature électronique simple

Une signature électronique simple correspond au niveau le plus couramment utilisé en raison de son accessibilité et de sa simplicité.

Elle désigne toute signature électronique ne répondant pas aux exigences spécifiques des signatures avancées ou qualifiées prévues par les articles 6 et 7 du présent décret.

Elle est admise dans les échanges numériques ne nécessitant pas de formalité renforcée.

Article 6 - Signature électronique avancée

La signature électronique avancée satisfait aux conditions suivantes :

- être liée uniquement au signataire ;
- permettre l'identification du signataire ;
- être créée par des moyens que le signataire puisse garder sous contrôle exclusif ;
- être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ;
- reposer sur un certificat électronique ou tout procédé jugé équivalent reconnu par voie réglementaire ;
- et être liée aux données associées à cette signature de telle sorte que toute modification ultérieure soit détectable.

Elle est utilisée lorsque l'exigence de formalité spécifique est impérative.

Article 7 - Signature électronique qualifiée

Une signature électronique qualifiée est créée à l'aide d'un dispositif sécurisé reposant sur un certificat qualifié délivré par un prestataire accrédité. Elle correspond au niveau le plus élevé de signature électronique.

Elle garantit :

- Une identification fiable du signataire, notamment en raison de sa fonction ou de son statut s'assurer, en se reposant sur un certificat qualifié de signature électronique ;
- La sécurité des données contenues dans le document signé, grâce à l'utilisation d'un dispositif de création de signature électronique qualifié.

Ce type de signature bénéficie d'une présomption de fiabilité renforcée et est exigée pour les actes à portée juridique ou réglementaire élevée.

Article 8 - Dispositif qualifié de création de signature électronique

Un dispositif qualifié de création de signature électronique est un ensemble matériel et/ou logiciel certifié conforme aux normes techniques et de sécurité reconnues par l'Autorité Nationale de Confiance Numérique. Il est attesté par un certificat de conformité délivré par ladite Autorité.

Ce dispositif doit satisfaire aux exigences ci-après :

- garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique ne peuvent être trouvés par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par des moyens techniques disponibles ;
- garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique ne peuvent être établies plus d'une fois et que leur confidentialité est assurée et peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers ;
- n'entraîner aucune altération ou modification du contenu du document électronique à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

En outre, la génération ou la gestion de données de création de signature électronique qualifiée pour le compte du signataire ne peut être confiée qu'à un prestataire de services de confiance.

CHAPITRE 2 : PRINCIPES DE BASE DE LA SIGNATURE ÉLECTRONIQUE

Article 9 - Équivalence fonctionnelle des signatures électroniques

La signature électronique bénéficie de la même valeur juridique que la signature manuscrite, conformément à l'article 9 des dispositions liminaires du Code de Procédure Civile Malagasy. Elle est réputée valable dès lors qu'elle est acceptée par les parties, sauf preuve contraire.

Toute signature électronique créée ou utilisée dans un autre État est reconnue comme ayant les mêmes effets juridiques qu'une signature électronique créée ou utilisée à Madagascar, à condition qu'elle repose sur un procédé offrant un niveau de fiabilité substantiellement équivalent à celui exigé par la législation nationale, conformément aux dispositions de l'article 9 de la Loi n°2014-025 du 10 décembre 2014.

Article 10 - Valeur juridique de la signature électronique

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé :

- Met en œuvre une signature électronique sécurisée, établie au moyen d'un dispositif qualifié de création de signature électronique ;

- Repose sur un certificat électronique qualifié délivré par un prestataire de services de confiance accrédité.

En cas de contestation portant sur la validité technique d'une signature électronique, toute partie intéressée peut saisir la juridiction compétente. Celle-ci peut ordonner une expertise technique contradictoire, le cas échéant avec le concours de l'ANCN ou d'experts agréés, afin de vérifier la conformité du procédé de signature aux exigences légales et réglementaires.

Les résultats de l'expertise constituent un élément de preuve soumis à l'appréciation souveraine du juge.

Article 11 - Usage des données biométriques

Les données biométriques peuvent être utilisées comme moyen d'authentification du signataire dans le cadre d'un processus de signature électronique, sans se substituer à la signature elle-même.

Le recours à ces données doit respecter les principes de proportionnalité, de finalité et de minimisation, conformément aux dispositions de la loi n°2014-038 du 09 janvier 2015 relative à la protection des données à caractère personnel notamment :

- Le consentement éclairé du signataire qui doit être informé, de manière claire et accessible, des finalités du traitement, des types de données collectées, de leur durée de conservation et des droits dont il dispose.
- Sécurité et confidentialité, données biométriques stockées et traitées dans des conditions garantissant leur intégrité, leur confidentialité et leur protection contre tout accès non autorisé.
- Encadrement réglementaire, tout système biométrique doit faire l'objet d'une déclaration ou d'une autorisation préalable auprès de l'autorité compétente en matière de protection des données personnelles.

Article 12 - Contenu du certificat électronique

Les certificats délivrés par les prestataires de certification de signature électronique doivent répondre à des critères et contenir les informations complètes liées à son titulaire.

Le certificat électronique pour une signature électronique ou un cachet électronique délivré par le prestataire de services de confiance, comporte des mentions obligatoires notamment les données et informations ci-après :

- Identification du certificat
  - Le code unique d'identification du certificat ;
  - La mention explicite qu'il s'agit d'un certificat électronique, sous une forme adaptée au traitement automatisé.

- Identification du prestataire
  - La dénomination ou raison sociale du prestataire de services de confiance concerné ;
  - L'adresse de son siège social ;
  - Son identifiant commun d'entreprise ou son numéro d'inscription au Registre du Commerce et des Sociétés.

- Identification du titulaire
  - Le nom du signataire ou, le cas échéant, un pseudonyme, clairement identifié comme tel ;
  - La qualité ou fonction du signataire, lorsque celle-ci est pertinente pour l'usage du certificat.

- Données techniques de vérification
  - Les données de vérification de signature électronique correspondant aux données de création ;
  - L'indication du début et de la fin de la période de validité du certificat électronique ;
  - L'emplacement des services permettant de vérifier le statut du certificat (CRL, OCSP ou autres);

- Dispositif de création de signature
  - Une mention indiquant, sous une forme adaptée au traitement automatisé, si les données de création de signature sont contenues dans un dispositif ;
  - L'emplacement où peut être obtenu le certificat électronique du prestataire de services de confiance concerné.

- Authentification du certificat
  - La signature électronique et/ou le cachet électronique du prestataire de services de confiance ayant émis le certificat.

En matière de certificats délivrés par l'Administration publique, le code d'identification du certificat électronique est délivré par l'UGD en sa qualité d'autorité d'accréditation.

Pour les certificats électroniques émis par un prestataire privé accrédité, le certificat comporte à la fois le code d'identification de la demande attribué par l'UGD et celui attribué par le prestataire.

Article 13 - Intégrité du certificat électronique

Tout prestataire de services de confiance accrédité est tenu de notifier sans délai à l'UGD toute atteinte à la sécurité ou toute perte d'intégrité susceptible d'affecter les certificats électroniques qu'il délivre, les services de confiance fournis ou les données à caractère personnel qu'il conserve.

Lorsque l'incident est de nature à porter préjudice à une personne physique ou morale bénéficiaire du service de confiance, le prestataire doit en informer immédiatement ladite personne, en précisant la nature de l'atteinte, les risques encourus et les mesures correctives engagées.

La notification des incidents de sécurité ou des pertes d'intégrité s'effectue conformément aux modalités définies dans le référentiel national de gestion des incidents de cybersécurité.

Article 14 - Durée de validité du certificat électronique

Le certificat électronique est délivré pour une durée de un (1) an ou deux (2) ans, selon le type de certificat et le niveau de sécurité requis.

À l'expiration de sa période de validité, le certificat peut être renouvelé à la demande de son titulaire, sous réserve :

- D'une vérification actualisée de son identité ;
- Du respect des conditions techniques et réglementaires fixées par l'Autorité Nationale de Confiance Numérique « ANCN » ou par le prestataire de services de certification.

Le prestataire de services de confiance peut procéder à la suspension ou à la révocation anticipée du certificat dans les cas suivants:

1. Usage frauduleux ou compromission des données de création de signature ;
2. Perte ou vol du dispositif de création de signature électronique ;
3. Changement de statut juridique du titulaire affectant la validité du certificat;
4. Décès, incapacité ou cessation d'activité du titulaire ;
5. Demande expresse du titulaire ou injonction d'une autorité compétente.

Les modalités de délivrance, de renouvellement, de suspension et de révocation des certificats électroniques sont définies par arrêté du Ministre chargé du Numérique ou par l'autorité réglementaire désignée.

TITRE II : DU CADRE INSTITUTIONNEL

CHAPITRE 1 : DE L'AUTORITÉ NATIONALE DE CONFIANCE NUMÉRIQUE OU ANCN

Article 15 - Désignation de l'ANCN

L'Unité de Gouvernance Digitale « UGD » est désignée comme Autorité Nationale de Confiance Numérique « ANCN ».

À ce titre, elle exerce les fonctions suivantes :

- Régulation des services de confiance liés à la signature électronique ;
- Accréditation des prestataires de services de confiance, publics et privés ;

- Supervision technique, juridique et opérationnelle des acteurs accrédités ;
- Gestion de la racine nationale de confiance, incluant la délivrance des certificats intermédiaires et la validation des chaînes de certification.

L'ANCN exerce ses missions en toute autonomie fonctionnelle, conformément aux principes de neutralité, d'indépendance et de sécurité juridique.

Tous les certificats intermédiaires et finaux reconnus dans la chaîne nationale de confiance doivent être rattachés, directement ou indirectement, au certificat racine détenu et administré par l'ANCN.

Article 16 - Missions de l'ANCN

L'Autorité Nationale de Confiance Numérique ou ANCN, représentée par l'Unité de Gouvernance Digitale « UGD », exerce les missions suivantes dans le cadre de la régulation des services de confiance liés à la signature électronique :

- Elaborer, publier et mettre à jour les référentiels techniques, juridiques et de sécurité applicables aux dispositifs de signature électronique, aux certificats et aux services de confiance ;
- Délivrer les agréments et accréditations aux prestataires de services de confiance « PSCo », selon les procédures prévues par le présent décret et les référentiels en vigueur ;
- Assurer la supervision continue des prestataires accrédités, notamment par des audits périodiques ou inopinés, en vue de garantir leur conformité aux normes nationales et internationales ;
- Administrer la Public Key Infrastructure (PKI) racine nationale, signer les autorités de certification subordonnées (AC intermédiaires) et garantir la traçabilité des chaînes de certification ;
- Assurer la reconnaissance nationale et internationale des certificats et signatures électroniques, notamment par la participation à des accords bilatéraux ou multilatéraux ;
- Proposer les adaptations législatives et réglementaires nécessaires pour garantir l'alignement du cadre national aux standards internationaux en matière de signature électronique et de confiance numérique.

Article 17 - Attributions de l'ANCN

Dans le cadre de ses missions de régulation, de supervision et d'accréditation des services de confiance, l'Autorité Nationale de Confiance Numérique ou ANCN, représentée par l'Unité de Gouvernance Digitale « UGD », exerce les attributions suivantes :

- Délivrer, suspendre ou retirer l'accréditation des prestataires de services de confiance « PSCo », après évaluation documentaire, technique et opérationnelle ;
- Réaliser des audits périodiques ou inopinés pour vérifier la conformité aux référentiels en vigueur ;
- Émettre des prescriptions techniques obligatoires applicables aux dispositifs de certification et de signature électronique ;
- Valider les référentiels de sécurité, les politiques de certification (CP/CPS) et les procédures de gestion des certificats ;
- Imposer des mesures correctives en cas de non-conformité ;
- Prononcer des sanctions administratives proportionnées aux manquements constatés ;

- Publier et maintenir à jour la Liste Nationale de Confiance (Trust List), recensant les prestataires accrédités et les certificats reconnus ;
- Assurer la traçabilité des décisions d'accréditation, de suspension et de révocation ;
- Représenter l'État dans les accords bilatéraux ou multilatéraux relatifs à la reconnaissance des certificats et signatures électroniques ;
- Participer aux instances régionales et Internationales de normalisation et de coopération technique.

CHAPITRE 2 : DES PRESTATAIRES DE SERVICE DE CONFIANCE

Section 1 - De l'accréditation

Article 18 - Accréditation du prestataire de certification de signature électronique

Tout prestataire privé souhaitant délivrer des certificats électroniques doit obtenir une accréditation formelle délivrée par l'Autorité Nationale de Confiance Numérique « ANCN ».

L'accréditation est valable pour une durée de deux (2) ans, renouvelable après audit, et atteste de la conformité du prestataire aux normes technologiques, juridiques et de sécurité définies par l'ANCN.

Tout refus de renouvellement doit être expressément motivé.

Lorsqu'un prestataire accrédité agit en qualité d'autorité de certification subordonnée « AC intermédiaire », il doit préalablement recevoir un certificat intermédiaire émis et signé par l'ANCN, l'intégrant formellement à la chaîne nationale de confiance.

Les certificats finaux émis par un prestataire de services de confiance ne sont réputés valides dans la chaine nationale que s'ils sont rattachés à un certificat intermédiaire signé par l'ANCN.

L'ANCN peut suspendre ou révoquer un certificat intermédiaire en cas de compromission, de non-conformité technique ou de menace avérée pour la sécurité, indépendamment de la procédure de suspension ou de retrait de l'accréditation du prestataire.

La délivrance, la validité, le renouvellement et la révocation des certificats intermédiaires sont régis par les référentiels techniques publiés par l'ANCN, en cohérence avec les normes internationales applicables.

L'Unité de Gouvernance Digitale « UGD », en tant que prestataire public qualifié (PSCo public), est également soumise à la procédure d'accréditation prévue à l'article 29 du présent décret.

Article 19 - Rôles de l'UGD comme PSCo public qualifié

En complément de ses fonctions de régulation en qualité d'Autorité Nationale de Confiance Numérique ou ANCN, l'Unité de Gouvernance Digitale agit également en tant que prestataire public qualifié de services de confiance (PSCo public), pour les besoins de l'État et des entités publiques.

Dans ce cadre, l'UGD est habilitée à :

- Délivrer des certificats électroniques et des services de signature ou de cachet électronique pour les administrations, institutions publiques et agents de l'État ;
- Assurer la certification des documents officiels dans le cadre des procédures administratives dématérialisées ;
- Garantir la conformité des dispositifs de signature utilisés par les entités publiques aux référentiels techniques et juridiques publiés par l'ANCN.

Les activités de l'UGD en tant que PSCo public sont strictement séparées, sur les plans fonctionnel, organisationnel et technique, de ses missions de supervision et d'accréditation exercées en tant qu'ANCN.

Les droits, frais et redevances afférents aux prestations de services de confiances pour l'État et les établissements public sont à la charge de ces derniers, versés au compte de l'ANCN.

Ils sont fixés par décisions prises par l'ANCN et publiées sur le site web de l'ANCN. Chaque changement est assorti d'un préavis de un (1) mois avant son effectivité.

Article 20 - Neutralité et audits

Afin de préserver l'intégrité de la chaîne nationale de confiance et d'éviter tout conflit d'intérêts, les principes suivants s'appliquent à l'Unité de Gouvernance Digitale « UGD » dans l'exercice de ses fonctions :

- L'UGD, en sa qualité d'Autorité Nationale de Confiance Numérique « ANCN », ne peut héberger, administrer ou intervenir dans les infrastructures techniques des prestataires de services de confiance privés (PSCo privés). Toute interconnexion ou dépendance technique est strictement interdite.

- Les services de confiance fournis par l'UGD en tant que prestataire public qualifié (PSCo public) sont soumis à un audit externe périodique (annuel) validé par le Comité National d'Interopérabilité ou CNIOp.

  Ce contrôle porte sur la conformité aux référentiels techniques, juridiques et organisationnels publiés par l'ANCN.

- LUGD doit mettre en œuvre une séparation fonctionnelle, organisationnelle et technique documentée entre ses missions de régulation (Root CA) et ses activités de prestation (PSCo public).

La Liste Nationale de Confiance publiée par l'ANCN mentionne explicitement l'UGD en tant que PSCo public accrédité, avec indication de ses certificats, de leur statut et de leur rattachement à la chaîne nationale de certification.

Section 2 – Des conditions et obligations

Article 21 - Conditions d'exercice du prestataire de certification de signature électronique

Tout prestataire de services de certification de signature électronique exerçant sur le territoire national doit héberger l'ensemble des données, dispositifs techniques et journaux d'activité sur une infrastructure physiquement localisée à Madagascar. Ces éléments doivent être accessibles, sur demande, à l'organisme d'accréditation ou aux autorités judiciaires compétentes.

L'accréditation délivrée autorise son titulaire à exercer, sur le territoire national, les activités relatives à la certification de signature électronique, conformément aux normes, standards et prescriptions édictés par l'Autorité Nationale de Certification Numérique ou ANCN.

Le prestataire de services de confiance « PSCo » s'engage à respecter l'ensemble des référentiels techniques, de sécurité, d'interopérabilité et de conservation publiés par l'ANCN. Ces référentiels couvrent notamment :

- l'horodatage certifié des transactions électroniques ;
- la révocation immédiate des certificats via les protocoles OCSP et CRL ;
- la conservation sécurisée des preuves et journaux de sécurité ;
- l'interopérabilité des certificats, au niveau national et international, conformément aux standards reconnus et à la Liste Nationale de Confiance.

Les modalités techniques d'application sont précisées dans les référentiels publiés par l'ANCN et approuvés par arrêté du Ministre chargé du Numérique. Les obligations opérationnelles incombant aux PSCo accrédités sont définies à l'article 22 du présent décret.

Article 22 - Obligations du prestataire de services de confiance accrédité

Le prestataire de services de confiance accrédité est tenu de :

- Assurer la sécurité, l'intégrité, la confidentialité et l'authenticité des données traitées;
- Gérer le cycle de vie des certificats conformément aux référentiels techniques publiés par l'Autorité Nationale de Certification Numérique « ANCN » ;
- Vérifier l'identité des titulaires de certificats ainsi que, le cas échéant, leurs qualités déclarées ;
- Conserver les données et éléments de preuve liés à la certification pendant la durée minimale prévue par la réglementation en vigueur ;
- Garantir l'interopérabilité des services et leur conformité aux normes internationales applicables ;
- Informer l'ANCN de tout incident de sécurité et se soumettre aux audits et contrôles prescrits par celle-ci.

Les modalités techniques d'application de ces obligations sont définies dans un référentiel élaboré par l'ANCN et approuvé par arrêté du Ministre chargé du Numérique.

Article 23 - Conservation des documents électroniques

La conservation des documents électroniques revêt la même valeur juridique que celle des documents écrits. Elle doit garantir l'intégrité, la disponibilité et la traçabilité des contenus certifiés. L'émetteur ainsi que le destinataire de documents électroniques certifiés sont responsables, chacun en ce qui les concerne, de la conservation des documents en leur possession.

L'émetteur est tenu de préserver le document électronique dans sa forme d'émission, tandis que le destinataire doit le conserver dans la forme reçue.

Le document électronique doit être archivé sur un support permettant :

- La consultation de son contenu pendant toute sa période de validité ;
- La conservation dans sa forme finale, assurant son intégrité ;
- La conservation des informations relatives à son origine et sa destination, ainsi que la date et le lieu de son émission ou de sa réception.

Section 3 – De l'hébergement technique des PSCo

Article 24 - Hébergement des Prestataires de Services de Confiance privés

Lorsqu'un prestataire de services de confiance privé est hébergé sur une infrastructure appartenant à un tiers, y compris un organisme public, une séparation stricte des fonctions, des structures organisationnelles et des environnements techniques doit être assurée.

L'environnement technique dédié au prestataire hébergé doit répondre aux conditions suivantes :

- Être totalement isolé, tant physiquement que logiquement, des autres environnements, y compris ceux du tiers hébergeur ou d'autres prestataires ;
- Être configuré de manière sécurisée, conformément aux normes internationales applicables aux services de confiance, notamment en matière d'accès sécurisé à la gestion des clés cryptographiques, de journalisation et d'authentification ;

Faire l'objet d'audits et de contrôles réguliers réalisés par un organisme indépendant accrédité ou par ANCN elle-même, selon les modalités définies dans les référentiels de sécurité.

Les résultats des audits doivent être transmis à l'ANCN pour validation. Tout manquement constaté peut entrainer la suspension ou la révocation de l'autorisation d'hébergement.

Les modalités de mise en œuvre de l'hébergement technique des PSCo privés, ainsi que les exigences de traçabilité, d'accès sécurisé et de non-conflictualité, sont précisées par arrêté du Ministre chargé du Numérique, sur proposition de l'ANCN.

Article 25 - Isolation et sécurité des environnements

Les prestataires de services de confiance opérationnels privés doivent garantir que leurs infrastructures techniques :

- Sont isolées physiquement et/ou logiquement de tout environnement partagé ;
- Intègrent un chiffrement robuste des données ainsi que des clés privées de signature ;
- Permettent une traçabilité exhaustive de l'ensemble des opérations réalisées.

Article 26 - Audit et contrôle

Les prestataires de services de confiance privés ou PSCo hébergeant leurs environnements techniques en dehors du territoire national sont soumis à un audit annuel portant sur la conformité réglementaire et la sécurité des infrastructures.

Cet audit est réalisé par l'Autorité Nationale de Certification Numérique « ANCN » ou par un organisme tiers agréé.

Tout manquement constaté peut entraîner :

- La suspension ou le retrait de l'agrément délivré ;
- Le cas échéant, l'application de sanctions administratives.

TITRE III

DU CADRE PROCÉDURAL

CHAPITRE I : DE L'ACQUISITION DE L'ACCRÉDITATION

Article 27 - Demande d'accréditation de prestataire de signature électronique

Tout prestataire souhaitant exercer des activités de certification de signature électronique doit adresser une demande officielle à l'Autorité Nationale de Certification Numérique « ANCN », soit contre récépissé, soit par voie postale recommandée ou électronique.

La demande doit être conforme aux modalités fixées par l'ANCN et comporter, de manière explicite, les informations détaillées relatives à l'entité requérante, à ses activités, à ses processus de certification, ainsi qu'à sa conformité aux normes et textes réglementaires en vigueur et sous réserve des dispositions de l'article 43 de la loi n°2014-038 sur la protection des données à caractère personnel.

Article 28 - Instruction de la demande d'accréditation

Toute demande d'accréditation est instruite par l'ANCN, qui procède, aux frais du demandeur, à une évaluation documentaire et sur place. Cette évaluation vise à vérifier la conformité du service de certification concerné aux exigences législatives et réglementaires en vigueur relatives à la signature électronique, ainsi qu'aux règles de sécurité applicables, telles que définies dans les référentiels d'exigences établis et publiés par l'ANCN.

L'octroi de l'accréditation est subordonné à la réussite de trois niveaux d'évaluation préalables :

- Évaluation documentaire : Analyse approfondie des pièces fournies par le demandeur, visant à vérifier la conformité aux exigences législatives et réglementaires applicables, notamment en matière de politiques de sécurité et de procédures internes.
- Évaluation technique: Vérification de la fiabilité des infrastructures et des systèmes utilisés, du niveau de sécurité opérationnelle, ainsi que de la conformité aux normes techniques en vigueur, à travers des tests et contrôles spécifiques.

- Évaluation sur site : Inspection effectuée dans les locaux du prestataire, permettant de s'assurer de la mise en œuvre effective des processus de certification électronique, de la gestion des clés cryptographiques, et de la compétence opérationnelle du personnel.

Le demandeur est tenu d'informer l'ANCN, durant toute la phase d'instruction, de toute modification affectant les éléments sur lesquels repose sa demande d'accréditation.

Article 29 - Accréditation de l'UGD en tant que PSCo

L'Unité de Gouvernance Digitale « UGD », en tant que PSCo, est accréditée selon la procédure suivante :

a) Constitution d'un dossier complet de demande d'accréditation ;
b) Réalisation d'un audit initial par un organisme indépendant dûment accrédité ;
c) Validation des résultats de l'audit par le Comité National d'Interopérabilité ;
d) Décision d'accréditation formalisée par arrêté du Ministre chargé du Numérique ;
e) Signature de l'accord de certification (AC) par la Root CA nationale, suivie de l'inscription de l'UGD sur la liste nationale de confiance.

Article 30 - Issue de l'instruction de la demande d'accréditation

À l'issue de l'instruction, l'organe d'accréditation transmet au prestataire de certification électronique un rapport détaillé des évaluations réalisées. Ce rapport comporte les constatations, observations et recommandations permettant au prestataire de démontrer sa conformité aux normes et standards applicables.

Lorsque les exigences sont jugées satisfaites, l'ANCN procède à la délivrance de l'agrément d'accréditation pour une durée maximale de deux (2) ans, renouvelable.

L'agrément est accompagné d'un certificat de conformité du dispositif de certification électronique, précisant notamment:

- La dénomination et l'adresse du prestataire ;
- Le service objet de l'accréditation ;
- La date de délivrance et le numéro de l'accréditation ;
- La durée de validité, ne pouvant excéder deux (2) ans;
- Les exigences en matière de sécurité, de conformité et de fiabilité.

Le prestataire de services de confiance est tenu d'informer l'ANCN de toute modification affectant les éléments ou conditions ayant fondé l'accréditation.

Les droits, frais et redevances afférents à la délivrance de l'accréditation sont à la charge du prestataire, versés au compte de l'ANCN.

Ils sont fixés par décisions prises par l'ANCN publiées sur le site web de l'ANCN. Chaque changement est assorti d'un préavis de un (1) mois avant son effectivité.

Article 31 - Suivi et contrôle des prestations de certification

Une fois accrédité, le prestataire de certification électronique est soumis à des audits de suivi périodiques, réalisés par l'équipe technique de l'ANCN. Ces audits visent à vérifier le maintien de la conformité aux normes et standards en vigueur.

Les contrôles peuvent être effectués sur pièces ou directement sur site.

Article 32 - Renouvellement de l'accréditation

Le renouvellement de l'accréditation du prestataire de services de confiance s'effectue selon les mêmes modalités que celles prévues pour son obtention initiale.

La demande de renouvellement doit être déposée auprès de l'ANCN au moins trois (3) mois avant la date d'expiration de l'accréditation en cours de validité.

Article 33 - Suspension de l'accréditation

L'accréditation du prestataire de services de confiance peut être suspendue en cas de non-conformité temporaire ou de suspicion de compromission. La durée de suspension ne peut excéder trois (3) mois, renouvelable une seule fois.

Article 34 - Révocation de l'accréditation

L'accréditation du prestataire de services de confiance peut être révoquée en cas de compromission avérée, de fraude établie, de manquement grave aux exigences de conformité, ou de cessation définitive d'activité.

Article 35 - Retrait de l'accréditation du prestataire de certification de signature électronique

L'ANCN peut procéder au retrait de l'accréditation d'un prestataire de services de confiance en matière de certification électronique dans les cas suivants :

a) Manquements graves et répétés aux normes et référentiels applicables ;
b) Compromission avérée de la sécurité ou de la confidentialité des certificats émis ;
c) Cessation d'activité ou incapacité technique durable à assurer les obligations de certification ;
d) Décision juridictionnelle définitive entraînant l'inaptitude à poursuivre l'activité.

Préalablement à la décision de retrait, l'ANCN adresse une mise en demeure au prestataire, l'invitant à régulariser sa situation dans un délai de sept (7) jours. Le prestataire peut faire valoir ses observations écrites dans le même délai.

La décision de retrait est notifiée au prestataire concerné et publiée sur la Liste nationale de confiance, entraînant la révocation immédiate ou programmée des certificats concernés.

Dans un délai de trente (30) jours à compter de la notification, le prestataire est tenu de transmettre à l'ANCN :

- Les registres de certification et de révocation ;
- Les clés et preuves de certification nécessaires à la continuité du service.

Article 36 - Obligations en cas de retrait d'accréditation

En cas de retrait de l'accréditation, le prestataire de services de confiance est tenu, dans un délai de trente (30) jours à compter de la notification, de transmettre à l'ANCN :

- Les registres de certification, de révocation et d'horodatage ;
- Les preuves de sécurité et les journaux de traçabilité;
- Les clés et configurations techniques nécessaires à la continuité des vérifications et audits.

La notification du retrait ainsi que la mise à jour de la Liste Nationale de Confiance relèvent exclusivement de l'ANCN.

La confidentialité, l'intégrité et la traçabilité des données transmises doivent être garanties conformément aux normes et référentiels publiés par l'ANCN.

Article 37 - Cessation d'activité et accompagnement

En cas de cessation d'activité, le prestataire de certification électronique est tenu de respecter les obligations suivantes :

1. Soumettre à l'ANCN un plan de cessation détaillé, incluant les mesures de transfert, de conservation ou de destruction sécurisée des données et certificats;
2. Assurer, sous le contrôle de l'ANCN, le transfert des certificats valides et des journaux d'audit vers un autre PSCo qualifié ou vers l'ANCN ;
3. Informer les titulaires de certificats et leur garantir une période de migration ou de révocation adaptée ;
4. Se soumettre à un audit de sortie validé par l'ANCN avant toute radiation définitive.

CHAPITRE 2 : DE LA CERTIFICATION DE SIGNATURE ÉLECTRONIQUE

Article 38 - Demande et délivrance de Certificat électronique de signature

1. La demande de certificat électronique de signature et/ou de cachet électronique est adressée à un prestataire de services de confiance accrédité « PSCo », y compris à l'UGD pour les personnes morales de droit public. Elle peut être transmise par voie électronique ou postale.

2. La demande peut également être déposée auprès d'un prestataire étranger dont le niveau de fiabilité est reconnu équivalent par l'ANCN, sur la base :

- D'un accord bilatéral ou multilatéral de reconnaissance des signatures électroniques ; ou
- D'une décision officielle de l'ANCN publiée sur son site internet.

3. Le demandeur doit remplir le formulaire prévu à cet effet et fournir l'ensemble des pièces et informations requises, conformément aux modalités définies dans le référentiel technique approuvé par

4. Dès réception de la demande, le prestataire de services de confiance procède aux opérations suivantes :

- Vérification de l'identité du demandeur sur la base de documents officiels ;
- Génération des clés cryptographiques ;

- Validation du certificat de signature par un code d'identification du document électronique ;
- Émission à l'intention du demandeur le certificat de signature électronique d'un dispositif de création de signature électronique personnelle assortie d'un certificat électronique.

5. Le dispositif de création de signature électronique, qu'il s'agisse d'un logiciel, d'une carte à puce, d'un token USB ou de toute autre technologie cryptographique reconnue, est indispensable pour générer et apposer une signature électronique sécurisée.

6. Le certificat électronique atteste de la conformité du dispositif de création de signature ou de cachet électronique aux normes en vigueur, telles que reconnues par l'ANCN. Il précise également la durée de validité du dispositif.

Les certificats électroniques délivrés doivent répondre aux exigences suivantes :

- Indiquer de manière explicite leur date de début et de fin de validité ;
- Être conformes aux normes nationales et internationales reconnues par l'ANCN ;
- Être inscrits dans la Liste nationale de confiance tenue à jour par l'ANCN.

Article 39 - Durée de validité des certificats électroniques

Les certificats électroniques délivrés par les prestataires de services de confiance qualifiés (PSCo) ont une durée de validité définie comme suit :

- Le certificat de signature électronique avancée est valable pour une durée d'un (1) an, renouvelable ;
- Le certificat de signature électronique qualifiée est valable pour une durée de deux (2) ans, renouvelable ;
- Les certificats de la Root CA et root sub CA sont régis par des dispositions spécifiques.

À l'expiration de leur période de validité, les certificats concernés sont automatiquement révoqués et doivent être renouvelés conformément aux procédures établies par l'ANCN.

La durée de validité des certificats racines et intermédiaires, ainsi que des certificats destinés aux serveurs ou cachets électroniques, est fixée par instruction technique de l'ANCN en cohérence avec les normes internationales applicables.

Article 40 - Conditions d'émission spécifiques

La certification des signatures électroniques apposées sur les documents émis par l'Administration publique, en son nom ou par ses agents dans le cadre de missions d'intérêt général, relève d'un régime particulier défini par l'ANCN par Arrêté conjoint des Ministres chargés du Développement Numérique, des Finances, de l'Intérieur et de la Fonction Publique.

L'accord préalable de l'autorité d'accréditation peut être sollicité lorsque l'usage d'un type de signature spécifique est requis par une personne morale dans le cadre de la dématérialisation des procédures administratives. Dans ce cas, les modalités d'utilisation de ces signatures spécifiques sont portées à la connaissance des usagers par voie réglementaire.

La certification des signatures électroniques de document entre tiers peut être opérée par les prestataires de signatures électroniques accrédités par l'ANCN, émanant du territoire national malagasy.

L'autorité d'accréditation est tenue de vérifier périodiquement la conformité des installations de certification, des formats utilisés, des procédures mises en œuvre, ainsi que des dispositifs de vérification de la preuve de signature électronique, conformément aux règles de l'art et aux normes techniques en vigueur, afin d'assurer la continuité du service.

Article 41 - Obligations du demandeur

Le demandeur est tenu d'informer sans délai le prestataire de services de certification de toute modification affectant les éléments ayant fondé sa demande, et ce, durant toute la phase d'examen du dossier.

En cas de modification ou d'évolution significative du dispositif de création de signature électronique:

- Pour les personnes morales, un rapport d'analyse des risques et impacts doit être fourni au prestataire ;
- Le prestataire vérifie la conformité et confirme, le cas échéant, la continuité de validité du certificat.

Les personnes physiques sont dispensées de fournir un rapport technique, sauf demande expresse du prestataire pour des raisons de sécurité.

Article 42 - Fin de validité du certificat et renouvellement du certificat électronique

À l'échéance de sa période de validité ou en cas de révocation, le certificat électronique cesse de produire ses effets et ne permet plus au titulaire d'utiliser les données qui y sont associées.

La demande de renouvellement doit être déposée au moins un (1) mois avant la date d'expiration du certificat concerné.

Le cas échéant, un nouveau certificat doit être demandé conformément aux procédures établies par l'ANCN.

Article 43 - Obligations et responsabilité du prestataire de signature électronique en cas de fin de validité du certificat électronique

1. En cas d'expiration du certificat, le prestataire est tenu de :

- Informer et/ou notifier le titulaire du certificat au moins trente (30) jours avant la date d'expiration ;
- Proposer des solutions de renouvellement ou de remplacement du certificat;
- Publier l'expiration du certificat dans les listes de statut, conformément aux référentiels techniques de l'ANCN.

2. En cas de révocation anticipée du certificat, le prestataire doit :

- Notifier immédiatement le titulaire du certificat concerné ;
- Justifier la décision de révocation, sauf lorsqu'elle résulte d'une décision judiciaire ou administrative imposant la confidentialité ;
- Publier la révocation dans les listes de statut (CRL ou OCSP), pour assurer la vérification par les tiers.

Le prestataire conserve les preuves des notifications transmises ainsi que des mises à jour des listes de statut, aux fins d'audit périodique réalisé par l'ANCN.

Il n'est pas tenu responsable des dommages éventuellement subis par les utilisateurs d'un certificat arrivé à expiration ou révoqué, ni des préjudices résultant d'un usage abusif d'un certificat.

Article 44 - Suspension du certificat électronique

Le prestataire de services de confiance peut suspendre temporairement un certificat de signature électronique dans les cas suivants :

a) Les conditions ayant motivé sa délivrance ne sont plus réunies ;
b) Un incident ou un fait nouveau compromet la sécurité ou la conformité du certificat;
c) La clé privée associée est présumée compromise ;
d) Une demande de suspension temporaire est formulée par le titulaire ou par une autorité compétente.

La durée de suspension ne peut excéder trois (3) mois, renouvelable sur justification technique dûment motivée.

Le prestataire est tenu de :

- Notifier sans délai le titulaire du certificat ainsi que l'ANCN ;
- Publier la suspension dans les listes de statut (CRL/OCSP) ;
- Documenter les mesures correctives engagées.

La suspension d'un certificat électronique est levée dès que les conditions de conformité sont rétablies, après vérification par le prestataire de services de confiance et, le cas échéant, contrôle de l'ANCN.

À l'issue de la période maximale de suspension, si les conditions de conformité ne sont pas rétablies, le certificat est révoqué de plein droit.

Article 45 - Révocation du certificat électronique

Un certificat de signature électronique ou de cachet électronique est révoqué dans les cas suivants :
- Usurpation d'identité signalée par un tiers ;
- Fourniture de fausses informations lors de la demande ou modification substantielle des données déclarées ;
- Non-respect par le titulaire des dispositions légales et réglementaires en vigueur ;
- Non-conformité aux prescriptions de suspension notifiées au titulaire ;

- Cessation d'activité pour laquelle le certificat avait été délivré.

Article 46 - Litiges et conflits liés à la gestion de signature électronique certifié

La responsabilité en cas de litige portant sur les procédures techniques d'émission de certificats de signature électronique incombe exclusivement à l'organisme émetteur, devant la juridiction compétente.

Les certificats émis par un État tiers produisent des effets juridiques à Madagascar sous réserve du respect des conditions suivantes :
- Application par les deux États de référentiels techniques actualisés et conformes aux normes internationales en vigueur ;
- Existence d'un accord bilatéral ou multilatéral de reconnaissance mutuelle en matière de signature électronique.

En cas de différend, la compétence juridictionnelle est déterminée conformément aux règles du droit international privé.

CHAPITRE 3 : DES RESPONSABILITÉS DU PRESTATAIRE DE CERTIFICATION DE SIGNATURE ÉLECTRONIQUE

Article 47 - Régime de responsabilité des prestataires de service de certification

Les prestataires de certification accrédités sont soumis au régime de droit commun applicable en matière contractuelle et de responsabilité civile, avec présomption de responsabilité en cas de manquement.

Lorsqu'un prestataire relève du droit public et agit en qualité de prestataire de services de certification qualifié (PSCo public), sa responsabilité est régie par les règles de la responsabilité administrative applicables aux établissements publics.

La responsabilité pénale du prestataire peut être engagée en cas d'infraction aux dispositions légales, notamment en matière de falsification, de contrefaçon ou de violation des obligations de confidentialité.

Article 48 - Traitement des données à caractère personnel

La certification des signatures électroniques est assimilée à un traitement de données à caractère personnel au sens de l'article 8 de la loi n°2014-038 du 9 janvier 2015.

En cas de manquement à ses obligations en matière de protection des données, le prestataire de services de certification est passible des sanctions prévues par ladite loi, par l'autorité compétente.

Article 49 - Obligation de confidentialité

Tous les documents et données électroniques échangés dans le cadre du processus de signature électronique sont réputés strictement confidentiels. Leur divulgation est limitée aux seules personnes dûment habilitées, impliquées dans les opérations de validation ou de vérification, et agissant dans le strict cadre de leurs fonctions.

Cette obligation de confidentialité demeure applicable au-delà de la date d'expiration du certificat ou de la cessation d'activité du prestataire de services de certification.

Article 50 - Conservation des données techniques

1.Sans préjudice des délais prévus par la législation en vigueur; le prestataire de services de confiance accrédité est tenu de conserver les données relatives à la fourniture des services de confiance pendant une durée minimale de sept (7) ans à compter de la date d'expiration du certificat électronique concerné. Ces données techniques incluent notamment :

- Les certificats délivrés, suspendus ou révoqués ;
- Les notifications adressées aux titulaires ;
- Les audits internes.

2. La révision de la durée de conservation relève de la compétence de l'ANCN.

3. La nature des données à conserver est définie dans les référentiels d'exigences établis et publiés par l'ANCN.

Article 51 - Confidentialité et sécurité des données de signature électronique

1- Les prestataires de services de confiance accrédités doivent assurer :

- la confidentialité, l'intégrité et la disponibilité de toutes les données de signature électronique traitées ou conservées ; et
- l'usage des moyens techniques conformes aux standards internationaux (ISO/ETSI).

La conservation de ces données est strictement limitée aux besoins du service de certification et à la durée prévue par la réglementation.

2- En cas de violation de la sécurité ou d'accès non autorisé aux données de signature électronique :

- Le prestataire en informe immédiatement le titulaire concerné ;
- l'ANCN est notifiée dans les 24H suivant l'incident, conformément aux procédures de supervision et de reporting des incidents.

L'obligation de confidentialité demeure après l'expiration du certificat et après la cessation d'activité du prestataire accrédité, jusqu'à destruction sécurisée ou transfert des données sous contrôle de l'ANCN.

3- Les données non nécessaires à la preuve ou à la traçabilité sont détruites ou rendues inaccessibles en toute sécurité.

Article 52 - Dispositions relatives à l'expiration du certificat racine « Root CA»

1. **Principes généraux**

Le certificat racine constitue l'autorité de référence de la chaîne de certification. Sa gestion en fin de validité doit être anticipée afin d'éviter toute rupture de service.

Le renouvellement ou le remplacement du certificat racine doit être effectué dans des conditions garantissant la continuité de la chaîne de confiance.

2. **Durée de validité**

La durée de validité du certificat racine est fixée entre quinze (15) et vingt (20) ans. Aucun certificat subordonné, qu'il soit intermédiaire ou final, ne peut excéder la durée de validité du certificat racine auquel il est rattaché.

3. **Plan de transition (Rollover)**

Afin d'assurer la continuité de la chaîne de confiance :

- Une nouvelle paire de clés cryptographiques racine doit être générée **entre deux (2) et cinq (5) ans** avant l'expiration du certificat racine en cours.

- Le certificat racine de remplacement est émis, publié et diffusé dans les infrastructures techniques concernées, y compris les systèmes, navigateurs, appareils, intergiciels, et plateformes interconnectées.

- Les prestataires de services de confiance qualifiés « PSCo » sont tenus de migrer progressivement vers la nouvelle chaîne de certification, selon les modalités définies dans le référentiel technique de l'ANCN.

- Le plan de transition inclut le remplacement coordonné de l'ensemble des certificats intermédiaires rattachés au certificat racine expirant, conformément aux modalités fixées dans les référentiels techniques de l'ANCN.

4. **Double signature temporaire (Cross-certification)**

Pendant la période de transition, les certificats peuvent être simultanément signés par les anciennes et les nouvelles autorités racines, dans la limite d'une période transitoire maximale fixée par instruction technique de l'ANCN. Cette mesure vise à garantir la compatibilité entre les environnements existants et ceux nouvellement déployés.

5. **Notification officielle**

L'autorité Nationale de Confiance Numérique ou ANCN publie une note officielle de migration au moins dix-huit (18) mois avant l'expiration du certificat racine en cours de validité. Cette note précise les échéances, les exigences techniques et les obligations applicables aux prestataires de services de confiance qualifiés ou PSCo ainsi qu'aux entités concernées.

6. **Audit et supervision**

L'Autorité Nationale de Confiance Numérique ou ANCN veille à la bonne exécution du plan de transition par les prestataires de services de confiance qualifiés ou PSCo, notamment en assurant :

- La mise à jour des certificats installés sur les serveurs publics et les infrastructures critiques (administration, santé, services financiers, ou autres) ;

- L'intégration de la nouvelle autorité racine dans les bases de données et les systèmes des tiers de confiance.

7. **Formation et communication**

L'Autorité Nationale de Confiance Numérique ou ANCN, en coordination avec les prestataires de services de confiance qualifiés ou PSCo et les parties prenantes concernées, organise une campagne d'information ciblée à l'attention :

- Des développeurs de logiciels et intégrateurs de systèmes ;
- Des administrateurs d'infrastructures ;
- Des entités institutionnelles, publiques et privées.

TITRE IV

DISPOSITIONS DIVERSES ET FINALES.

Article 53 - Référentiels techniques et juridiques

L'ANCN publie et tient à jour les référentiels définissant les normes techniques, les politiques de certification (CP/CPS) et les procédures de sécurité applicables.

Article 54 – Mise en conformité

Toutes entités œuvrant dans le domaine de la signature électronique disposent d'un délai d'un (01) an pour se conformer aux dispositions du présent décret à compter de la date de son entrée en vigueur.

Article 55 - Dispositions abrogatoires

Toutes dispositions antérieures contraires au présent décret, sont et demeurent abrogées.

Article 56 - Dispositions d'urgence

En raison de l'urgence, et conformément aux dispositions des articles 4 et 6 alinéa 2 de l'Ordonnance n° 62-041 du 19 septembre 1962 relative aux dispositions générales de droit interne et de droit international privé, le présent décret entre immédiatement en vigueur dès sa publication par émission radiodiffusée ou télévisée, indépendamment de son insertion au Journal Officiel de la République.

Article 57 - Dispositions finales

Le Ministre de l'Economie et des Finances, le Ministre du Développement Numérique, des Postes et des Télécommunications, le Ministre du Commerce et de la Consommation et le Ministre de la Communication et de la Culture sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret qui sera publié au Journal Officiel de la République de Madagascar.

Fait à Antananarivo, le 08 décembre 2025

Par le Premier Ministre, Chef du Gouvernement,

***Herintsalama* RAJAONARIVELO**

Le Ministre de l'Economie et des Finances

***Herinjatovo Aimé* RAMIARISON**

La Ministre de l'Industrialisation et du Commerce

***Haingotiana Michela* ANDRIAMADISON**

Le Ministre du Développement Numérique, des Postes et des Télécommunications

***Mahefa* ANDRIAMAMPIADANA**

Le Ministre de la Communication et de la Culture

***Ogascar Fenosoa* MANDRINDRARIVONY**

« POUR AMPLIATION CONFORME »

Antananarivo, le -2 FEV. 2026

LE SECRETAIRE GENERAL DU GOUVERNEMENT

GOUVERNEMENT REPOBLIKAN'I MADAGASIKARA

RAZAFIMANANTSOA Heritiana Joël