



Paraissant
du Lundi au Vendredi

JOURNAL OFFICIEL DE LA REPUBLIQUE D'HAÏTI

Directeur Général
Ronald Saint Jean

180^e Année — Spécial N° 58-D

PORT-AU-PRINCE

Vendredi 19 Septembre 2025

SOMMAIRE

ARRÊTÉ

FIXANT LES MODALITÉS D'APPLICATION DE LA LOI DU 14 FÉVRIER 2017
SUR LA SIGNATURE ÉLECTRONIQUE
ADAPTANT LE DROIT DE LA PREUVE AUX TECHNOLOGIES DE L'INFORMATION
ET ÉLARGISSANT LES COMPÉTENCES DU CONSEIL NATIONAL
DES TÉLÉCOMMUNICATIONS (CONATEL) AMENDÉE PAR LE DÉCRET DU 20 AOÛT 2025

AVIS

AVIS DE LA DÉNONCIATION À LA VACANCE
DGI, 15 Juillet 2025, Réf: DOM/170

NUMÉRO SPÉCIAL

LIBERTÉ

ÉGALITÉ

FRATERNITÉ

RÉPUBLIQUE D'HAÏTI

ARRÊTÉ

FIXANT LES MODALITÉS D'APPLICATION DE LA LOI DU 14 FÉVRIER 2017
SUR LA SIGNATURE ÉLECTRONIQUE
ADAPTANT LE DROIT DE LA PREUVE AUX TECHNOLOGIES DE L'INFORMATION
ET ÉLARGISSANT LES COMPÉTENCES DU CONSEIL NATIONAL
DES TÉLÉCOMMUNICATIONS (CONATEL) AMENDÉE PAR LE DÉCRET DU 20 AOÛT 2025

LE CONSEIL PRÉSIDENTIEL DE TRANSITION :

RÉGINE ABRAHAM
SMITH AUGUSTIN
LOUIS GÉRALD GILLES
FRITZ ALPHONSE JEAN
FRINEL JOSEPH
EDGARD LEBLANC FILS
LAURENT SAINT-CYR
EMMANUEL VERTILAIRE
LESLIE VOLTAIRE

Vu la Constitution de la République ;

Vu la Loi du 14 février 2017 portant sur la signature électronique adaptant le droit de la preuve aux technologies de l'information et élargissant les compétences du Conseil National des Télécommunications (CONATEL), amendée par le Décret du 20 août 2025 ;

Vu le Décret du 10 avril 2024 portant création du Conseil Présidentiel de Transition ;

Vu le Décret du 23 mai 2024 déterminant l'organisation et le mode de fonctionnement du Conseil Présidentiel de Transition ;

Considérant qu'il y a lieu d'adopter l'Arrêté d'application de la Loi du 14 février 2017 sur la signature électronique susvisée ;

Sur le rapport du Premier Ministre, du Ministre des Travaux Publics, Transports et Communications, du Ministre de l'Économie et des Finances, du Ministre de la Justice et de la Sécurité Publique, et du Ministre du Commerce et de l'Industrie ;

Et après délibération en Conseil des Ministres ;

ARRÊTE

CHAPITRE I^{er}

DISPOSITIONS GÉNÉRALES

Article 1^{er}. Le présent Arrêté a pour objet de fixer les modalités d'application de la Loi du 14 février 2017 sur la signature électronique adaptant le droit de la preuve aux technologies de l'information et élargissant les compétences du Conseil National des Télécommunications (CONATEL), amendée par le Décret du 20 août 2025.

Article 1.1.- La signature électronique vise à :

- a) Garantir l'intégrité d'un document, c'est-à-dire s'assurer qu'il n'a pas été altéré entre sa signature et sa consultation ;
- b) Authentifier son auteur, c'est-à-dire s'assurer de l'identité de la personne signataire ;
- c) Rapporter la preuve du consentement.

CHAPITRE II

NIVEAUX DE SIGNATURE ÉLECTRONIQUE

Article 2.- Conformément aux dispositions de l'article 1.1 de la Loi du 14 février 2017 sur la signature électronique adaptant le droit de la preuve aux technologies de l'information et élargissant les compétences du Conseil National des Télécommunications, amendée par le Décret du 20 août 2025, la signature électronique est catégorisée en trois niveaux : simple, avancée et qualifiée.

Article 2.1.- Une signature électronique est dite Signature Électronique Simple (SES) quand elle permet d'identifier le signataire sans mesure de sécurité particulière. Sa valeur probante est faible, mais peut toutefois valoir comme commencement de preuve par écrit tant qu'elle n'est pas contestée par la partie adverse.

Article 2.2.- Une signature électronique est dite Signature Électronique Avancée (SEA) quand elle permet d'identifier le signataire, de lier la signature à son auteur et de garantir l'intégrité de l'acte signé. Elle ajoute une couche supplémentaire de sécurité en identifiant chaque signataire et en détectant toute modification de document ou de donnée. Elle utilise des clés cryptographiques.

La SEA est admise pour les actes sous seing privé. Elle a une valeur probante plus forte que la SES.

Les signatures manuscrites capturées par des dispositifs biométriques peuvent être considérées comme des SEA.

Article 2.3.- Une signature électronique est dite Signature Électronique Qualifiée (SEQ) lorsqu'elle est réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif qualifié de création de signature électronique. Elle possède l'équivalence légale de la signature manuscrite.

La SEQ bénéficie de l'effet juridique de la signature manuscrite et l'assurance d'une tierce partie. Elle

nécessite une évaluation de la conformité au préalable et des méthodes standardisées de haut niveau de sécurité et de protocole de confiance. Au niveau judiciaire, elle est considérée comme une preuve littérale parfaite au même titre qu'une signature manuscrite sur papier.

L'acte public au format électronique est établi conformément aux critères définis pour une SEQ et implique l'utilisation d'un code de vérification sécurisé et l'indication de la plateforme en ligne sur laquelle l'authenticité peut être vérifiée.

Le CONATEL peut établir des exigences ou désigner des normes spécifiques pour l'évaluation de ces services de confiance et pour le dispositif sécurisé de création de signature électronique s'il le juge nécessaire.

CHAPITRE III

DISPOSITIFS SÉCURISÉS DE CRÉATION DE SIGNATURE ÉLECTRONIQUE

Article 3.- Pour être réputé sécurisé, un dispositif de création de signature électronique doit :

- a) Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique, comme les clés privées :
 - 1) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;
 - 2) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
 - 3) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers ;
- b) Être protégé contre toute altération du contenu de l'acte à signer et de toute entrave pouvant empêcher au signataire d'en prendre connaissance avant de le signer ;
- c) Être certifié conforme aux exigences établies par le CONATEL.

Article 4.- Un service de vérification de signature électronique peut faire l'objet d'une certification, s'il répond aux exigences suivantes :

- a) Les données de vérification de signature électronique utilisées sont dérivées des champs prévus, à cet effet, dans le certificat qui accompagne la signature électronique du fichier. Ce sont ceux qui ont été portés à la connaissance du vérificateur, comme l'Uniform Resource Locator (URL) du fichier journal Certificate Revocation List (CRL) ou celle du service en ligne d'état des certificats Online Certificate Status Protocol (OCSP) ;
- b) Le certificat appartient à une hiérarchie de certification incluse dans le Trust Service List (TSL) d'Haïti. Les TSL sont des documents officiels, tenus et publiés par le CONATEL, qui contiennent des informations sur les fournisseurs de services de confiance qualifiés (QTSP) et les services qu'ils proposent, tels que les signatures électroniques, les cachets électroniques, les services d'horodatage, etc. Elles ont un effet constitutif, ce qui signifie qu'un fournisseur ou un service n'est considéré comme « qualifié », c'est-à-dire ayant une validité juridique, que s'il figure dans la TSL. Ces listes sont conçues pour être traitées automatiquement et sont également publiées dans des formats lisibles par l'homme. Il existe une norme technique qui établit leur codification ;
- c) Il doit être possible d'indiquer si un dispositif qualifié de création de signature électronique a été utilisé ;
- d) Il doit être possible d'indiquer si un pseudonyme a été utilisé ;
- e) Le rapport contenant le résultat du processus de validation doit inclure la signature électronique avancée ou le cachet électronique avancé du Prestataire de Services de Confiance Qualifié.

Des services de validation non qualifiés peuvent être fournis et, dans ce cas, la dernière exigence ne sera pas obligatoire.

Article 5.- Un service d'horodatage sera qualifié s'il est conforme à la réglementation technique applicable.

Les horodatages électroniques qualifiés bénéficieront d'une présomption d'exactitude de la date et de

l'heure qu'ils indiquent et de l'intégrité des données auxquelles la date et l'heure sont liées.

Un horodatage électronique qualifié doit répondre aux exigences suivantes :

- a) Relier la date et l'heure aux données de manière à éliminer raisonnablement la possibilité de modifier les données sans détection ;
- b) Être basé sur une source d'information temporelle liée au Temps Universel Coordonné ; et
- c) Avoir été signé, au moins, à l'aide d'une signature électronique avancée ou cachetée avec un cachet électronique avancé du Prestataire de Services de Confiance Qualifié ou par toute méthode équivalente.

Article 6.- Un certificat électronique qualifié est délivré par un Prestataire de Services de Confiance Qualifié et comporte:

- a) Une mention dans un champ du certificat indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;
- b) L'identité du Prestataire de Services de Confiance incluant son siège et le lieu de son enregistrement;
- c) Le nom du signataire ou, le cas échéant, un pseudonyme identifié comme tel ;
- d) L'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;
- e) Les données de vérification de signature électronique (clé publique) qui correspondent exactement aux données de création de signature électronique (clé privée) ;
- f) L'indication du début et de la fin de la période de validité du certificat électronique ;
- g) Le code d'identité du certificat électronique ou le numéro de série du certificat attribué par le Prestataire de Services de Confiance ;
- h) La signature électronique ou cachet électronique du Prestataire de certification subordonné du Prestataire de Services de Confiance qui délivre le certificat électronique ;
- i) L'URL du certificat du Prestataire de certification subordonné qui signe le certificat afin que la chaîne de confiance puisse être construite ;
- j) Les URL des fichiers CRL et des services OCSP dans les champs prévus, à cet effet, dans le certificat;
- k) Si un dispositif qualifié de création de signature ou de cachet est utilisé, cette circonstance sera indiquée dans le champ prévu, à cet effet, sur le certificat ;
- l) Le cas échéant, les conditions d'utilisation du certificat électronique.

Article 7.- Un Prestataire de Services de Confiance suspend la validité d'un certificat électronique dans l'un ou l'autre des cas suivants :

- a) À la requête du signataire ;
- b) Par le déclenchement d'une procédure d'absence, de disparition ou de mise sous tutelle concernant le signataire ;
- c) Par la décision du Prestataire de Services de Confiance pour des raisons techniques ; avis en étant donné par tous les moyens de communication dans les vingt-quatre heures au signataire et au CONATEL ;
- d) Par l'exécution d'une décision de justice définitive déclarant l'absence, la disparition ou la mise sous tutelle du signataire ;
- e) Par l'exécution de toute décision de justice ayant acquis l'autorité de la chose définitivement et souverainement jugée.

La suspension de la validité d'un certificat électronique qualifié en empêche l'utilisation par le signataire dès la notification au Prestataire de Services de Confiance de la circonstance qui la déclenche.

Article 7.1.- La suspension prend fin :

- a) Par décision du signataire lorsque la suspension était due à son initiative;
- b) Par la décision du Prestataire de Services de Confiance de lever la suspension une fois disparues les raisons techniques qui l'avaient motivé ;
- c) Par une décision du CONATEL ;
- d) Par une décision de justice.

Article 8.- Un Prestataire de Services de Confiance révoque le certificat dans l'un ou l'autre des cas suivants :

- a) À la requête du signataire ou de son représentant légal ;
- b) Si les données ou renseignements, servant à l'établissement du certificat électronique, sont reconnus faux ;
- c) Si le résultat d'une évaluation de la conformité détermine le caractère peu fiable des procédures d'établissement et de vérification ;
- d) En cas d'une décision de justice ;
- e) En cas de décès, de disparition, de mise sous tutelle de la personne physique ou de dissolution de la personne morale, titulaire du certificat ;
- f) En cas de cessation des activités du Prestataire de Services de Confiance.

Article 9.- La requête en suspension ou en révocation du certificat sera adressée au Prestataire de Services de Confiance.

La suspension ou la révocation du certificat sera notifiée à son titulaire dans un délai ne dépassant pas vingt-quatre heures.

En cas de suspension pour raisons techniques ou de révocation pour les raisons exprimées aux a) et f) de l'article 8, la requête contenant les motifs et les pièces justificatives sera notifiée au Prestataire de Services de Confiance au plus tard vingt-quatre heures avant sa prise d'effet.

CHAPITRE IV

EXIGENCES POUR LA QUALIFICATION DES PRESTATAIRES DE SERVICES DE CONFIANCE

Article 10.- Un Prestataire de Services de Confiance, qui demande à être reconnu comme qualifié, adresse une requête à cette fin au CONATEL. Il devra satisfaire aux conditions de la Loi sur la signature électronique amendée par le Décret du 20 août 2025 et aux exigences techniques prévues dans la réglementation.

Le Prestataire est tenu de fournir tous les éléments nécessaires au bon accomplissement de la procédure d'évaluation.

La demande sera accompagnée du Rapport d'Évaluation de la Conformité (REC) délivré soit par un Organisme d'Évaluation de la Conformité agréé, soit par le CONATEL.

Article 11.- Les Prestataires de Service de Confiance haïtiens ou étrangers, désirant être qualifiés pour être habilités à fournir des services de confiance, doivent respecter les conditions suivantes :

- a) Démontrer une capacité financière suffisante pour assurer la prestation des services de confiance de manière fiable et continue ;
- b) Démontrer une capacité technique adéquate pour la fourniture des services de confiance.

Article 11.1.- Outre les exigences générales prévues par le présent Arrêté, les dirigeants et le personnel des Prestataires de Services de Confiance, désirant être qualifiés pour être habilités à fournir des services de confiance, doivent respecter les conditions suivantes :

- a) N'avoir jamais été condamné à une peine afflictive ou infamante en Haïti ou à l'étranger ;
- b) N'avoir pas été suspendu ou radié de l'exercice de leur profession pour faute éthique. Cette disqualification demeure en vigueur pendant toute la durée de la sanction.

Article 11.2.- Les Prestataires de Services de Confiance communiquent au CONATEL, selon le cas, le nom de leur dirigeant ou les noms des membres de leur Conseil d'administration, ainsi que leur fonction correspon-

dante.

Article 12.- Le Prestataire de Services de Confiance, pour être qualifié, doit satisfaire aux exigences techniques suivantes :

- a) Faire preuve de la fiabilité des services de confiance qu'il fournit ;
- b) Être capable d'assurer :
 - 1) Le fonctionnement d'un service d'annuaire recensant les certificats électroniques délivrés ;
 - 2) Le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer, sans délai et avec certitude, ce certificat ;
 - 3) L'horodatage électronique pour prouver que des documents ont été créés ou des transactions effectuées à un moment précis ;
 - 4) L'archivage électronique sécurisé des documents et des transactions avec une garantie d'intégrité et d'accessibilité ;
 - 5) La conservation de signatures électroniques, de cachets électroniques ;
- c) Être doté d'un personnel ayant les connaissances, l'expérience et l'éthique nécessaires à la fourniture de services de confiance ;
- d) Être en mesure d'appliquer des procédures de sécurité appropriées.

Article 13.- Le Prestataire de Services de Confiance qualifié est évalué sur une base périodique par le CONATEL. L'objet de cette évaluation est de vérifier que le Prestataire se conforme aux spécifications techniques exigées.

À l'issue de cette évaluation, le CONATEL communique, le cas échéant, au Prestataire ses recommandations pour les suites utiles.

Article 13.1- Les systèmes cryptographiques utilisés par le Prestataire de Services de Confiance doivent être certifiés conformes par le CONATEL aux exigences ci-après :

- a) Assurer la confidentialité et l'intégrité des données de création de signature du Prestataire de Services de Confiance durant tout leur cycle de vie ;
- b) Être capable d'identifier et d'authentifier ses utilisateurs ;
- c) Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- d) Détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée ;
- e) Permettre de créer une signature électronique sécurisée qui ne révèle pas les données de création de signature du Prestataire de Services de Confiance et qui ne peut pas être falsifiée sans la connaissance des données de création de signature du Prestataire de Services de Confiance ;
- f) Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- g) Garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration, si une fonction de sauvegarde et de restauration des données de création de signature du Prestataire de Services de Confiance est offerte ;
- h) Prendre toute disposition propre à prévenir la falsification des certificats électroniques ;
- i) Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de les conserver ou de les reproduire.

Article 13.2- Le Prestataire de Services de Confiance doit utiliser des systèmes de conservation des certificats électroniques garantissant que :

- a) L'introduction et la modification des données sont réservées aux seules personnes autorisées, à cet effet, par le Prestataire ;

- b) L'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;
- c) Toute modification, de nature à compromettre la sécurité du système, peut être détectée.

Article 13.3- Le Prestataire de Services de Confiance doit vérifier l'identité et la qualité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation de documents officiels qui les justifient.

Il doit conserver une copie des documents présentés.

Article 13.4- Avant la conclusion d'un contrat de prestation de services de confiance, le Prestataire doit informer par écrit le demandeur d'un certificat électronique :

- a) De son statut de Prestataire de Services de Confiance qualifié ou non qualifié ;
- b) Des modalités et des conditions d'utilisation du certificat ;
- c) Des modalités de contestation et de règlement des litiges.

Article 14.- Le CONATEL reconnaît ou non la qualification du Prestataire de Services de Confiance sur la base du rapport d'évaluation et des éventuelles observations du Prestataire.

Lorsqu'il reconnaît la qualification d'un Prestataire, le CONATEL délivre une attestation qui décrit les activités couvertes ainsi que la durée de sa validité qui ne peut excéder trois ans.

Pendant cette durée, le Prestataire doit faire l'objet, de la part du CONATEL, d'un audit trimestriel régulier de surveillance qui peut, le cas échéant, conduire à une suspension ou à un retrait de l'attestation.

Les Prestataires, dont la qualification est reconnue, communiquent à toute personne qui en fait la demande une copie de l'attestation délivrée par le CONATEL.

Les Prestataires de services, qui fournissent des services techniques aux Prestataires de Services de Confiance délivrant des certificats électroniques qualifiés, doivent solliciter auprès du CONATEL, dans les mêmes conditions, une attestation de conformité de ces services aux spécifications techniques applicables exigées.

Les expressions « Prestataire de Services de Confiance Qualifié » ou « Prestataire de Services de Certification Électronique Qualifié » ou toute autre expression similaire ne peuvent être utilisées que par les Prestataires de Services de Confiance titulaires d'une attestation de qualification délivrée par le CONATEL.

Tout contrevenant verra ses locaux fermés et son matériel saisi par le CONATEL qui informe les utilisateurs de la nécessité de migrer vers un autre Prestataire.

Article 15.- Les Prestataires de Services de Confiance sont soumis à l'inspection ordinaire du CONATEL qui a lieu, au moins, une fois par an et a des inspections inopinées.

Les inspections seront conduites par les agents du CONATEL habilités à cet effet ou par des experts mandatés, à cette fin, par le CONATEL.

Toute information ou tout document requis, par les inspecteurs, doit leur être fourni séance tenante.

Article 16.- Un certificat électronique délivré par un Prestataire de Services de Confiance établi dans un État étranger a la même valeur juridique que celui délivré par un Prestataire établi en Haïti, si l'une des conditions suivantes est remplie :

- a) Le Prestataire satisfait aux exigences fixées par le présent Arrêté et a été qualifié dans l'État où il est établi ;
- b) Le certificat électronique délivré par le Prestataire a été garanti par un Prestataire qualifié établi en Haïti ;
- c) Un Traité International auquel la République d'Haïti est partie a prévu la reconnaissance mutuelle.

Article 17.- Les Prestataires de Services de Confiance notifient toute cessation d'activités aux signataires, au plus tard, quatre-vingt-dix (90) jours avant la date prévue de cessation en indiquant le Prestataire de Services

de Confiance auquel leurs services de confiance seront transférés. Les signataires ont quinze (15) jours, à partir de la réception de l'avis, pour s'opposer au transfert. Toute opposition des signataires entraîne la suspension de leurs certificats jusqu'à la résolution de l'opposition.

Les Prestataires, qui entendent mettre fin à leurs activités, en donnent avis au CONATEL, au plus tard, quatre-vingt-dix (90) jours avant la date prévue de cessation. Le CONATEL supervise le transfert ordonné des certificats à un autre Prestataire de Services de Confiance au moins de niveau équivalent (qualifié ou non qualifié). Le CONATEL veille au respect de la confidentialité, de la sécurité et de l'intégrité des données.

En cas de cessation involontaire des activités, pour cause notamment de suspension ou de retrait de la qualification par le CONATEL, les Prestataires de Services de Confiance concernés en avisent immédiatement les signataires et procèdent, dans les quinze (15) jours précédant la date de cessation d'activités, au transfert des services de confiance dans les conditions prévues au deuxième alinéa.

Article 18.- Les données fournies par les titulaires de certificats électroniques ainsi que les pièces justificatives sont conservées par les Prestataires de Services de Confiance dix (10) ans après la révocation ou l'expiration des certificats correspondants.

En cas de cessation d'activités des Prestataires de Services de Confiance et de transfert des données à d'autres Prestataires qualifiés, ces derniers conservent lesdites données et pièces pour le temps qui reste à courir.

Ces données sont transmises annuellement au CONATEL pour conservation.

Article 19.- Les Prestataires de Services de Confiance sont assujettis au paiement des frais de traitement de dossier et des droits suivants :

- a) Les frais qui se réfèrent aux coûts directement encourus pour le traitement du dossier, l'évaluation, la qualification et autres procédures déterminées par le CONATEL ;
- b) Les droits et redevances prévus par la réglementation ; et
- c) Les frais d'inspection et de supervision correspondant à la réalisation des inspections et audits.

Article 20.- Les droits de traitement ou de frais de procédure sont dus quel que soit le service.

Les droits de supervision ou frais d'inspection tiennent compte des coûts correspondant aux inspections et audits. Ils sont payables, au plus tard, quatre-vingt-dix (90) jours à partir de la réception de la facture du CONATEL.

Le montant des droits de traitement de dossier ou frais de procédure, de supervision et d'inspection est établi et perçu par le CONATEL.

CHAPITRE V

NOTIFICATIONS

Article 21.- Toutes les notifications auxquelles se réfèrent la Loi sur la signature électronique amendée par le Décret du 20 août 2025 et le présent Arrêté sont formulées par écrit en utilisant l'une ou l'autre de ces moyens:

- a) Documents électroniques ou messages de données porteurs de signatures électroniques transmis selon un protocole de communication électronique ;
- b) Correspondance avec accusé de réception ;
- c) Tout autre moyen électronique.

Les Prestataires de Services de Confiance fournissent au CONATEL une adresse électronique où seront envoyées les communications et notifications. Toute notification effectuée à cette adresse est réputée avoir été reçue.

CHAPITRE VI

DISPOSITIONS PARTICULIÈRES

Article 22.- Outre les attributions prévues dans les dispositions précédentes du présent Arrêté, le CONATEL, par

voie de circulaires, définit et met à jour les normes techniques pour la signature électronique et la prestation de services de confiance.

Le CONATEL s'assure que les normes techniques sont harmonisées avec les normes internationales pour la reconnaissance transfrontalière et l'interopérabilité des signatures électroniques en Haïti.

Article 23.- La Direction Générale du CONATEL met en place un Conseil Consultatif chargé de produire des recommandations sur tout sujet relatif à la signature électronique.

Le Conseil Consultatif se réunit sur convocation du Directeur Général du CONATEL.

Il est composé d'experts reconnus et des représentants des institutions publiques et privées concernées.

Le Bureau Haïtien de Normalisation (BHN), l'Institut Haïtien de Statistique et d'Informatique (IHSI), l'Université d'État d'Haïti (UEH), la Banque de la République d'Haïti (BRH) sont d'office membres du Conseil Consultatif.

Ne peuvent être membres du Conseil Consultatif :

- a) Les institutions Prestataires de Services de Confiance ou les Organismes d'évaluation de la conformité ainsi que ceux qui y travaillent ;
- b) Les institutions ayant vocation à devenir des Prestataires de Services de Confiance.

Les modalités de fonctionnement du Conseil Consultatif sont définies par le CONATEL dans ses règlements intérieurs.

CHAPITRE VII

DISPOSITIONS FINALES

Article 24.- Le présent Arrêté sera publié et exécuté à la diligence du Premier Ministre et de tous les Ministres, chacun en ce qui le concerne.

Donné au Palais National, à Port-au-Prince, le 18 septembre 2025, An 222^e de l'Indépendance.

Par le Conseil Présidentiel de Transition :

Pour le Conseil :

Le Conseiller-Président



Laurent SAINT-CYR

Le Premier Ministre



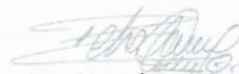
Alix Didier FILS-AIMÉ

Le Ministre de l'Intérieur et des Collectivités Territoriales



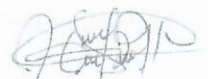
Paul Antoine BIEN-AIME

Le Ministre de la Justice et de la Sécurité Publique



Patrick PÉLISSIER

Le Ministre des Affaires Étrangères et des Cultes



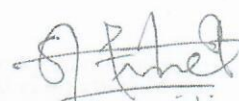
Jean-Victor Harvel JEAN-BAPTISTE

La Ministre des Haïtiens vivant à l'étranger



J. E. Kathia VERDIER

Le Ministre de l'Économie et des Finances



Alfred Fils METELLUS

La Ministre de la Planification et de la Coopération Externe

Marie D. A. Ketleen FLORESTAL

Le Ministre de l'Agriculture, des Ressources Naturelles et du Développement Rural

Vernet JOSEPH

Le Ministre des Travaux Publics, Transports et Communications

Raphaël HOSTY

Le Ministre du Commerce et de l'Industrie

James MONAZARD

Le Ministre du Tourisme

John Herrick DESSOURCES

Le Ministre de l'Environnement

Moïse JEAN-PIERRE Fils

Le Ministre de l'Éducation Nationale et de la Formation Professionnelle

Augustin ANTOINE

Le Ministre de la Culture et de la Communication

Patrick DELATOUR

Le Ministre des Affaires Sociales et du Travail

Georges Wilbert FRANCK

Le Ministre de la Santé Publique et de la Population

Sinal Bertrand
Bertrand SINAL

La Ministre de la Condition Féminine et des Droits de la Femme

Pédrica SAINT JEAN

La Ministre de la Jeunesse, des Sports et de l'Action Civique

Niola Lynn Sarah DEVALIS OCTAVIUS

Le Ministre de la Défense

Jean Michel MOÏSE