République Algérienne Démocratique et Populaire

Ministère de la Poste et des Télécommunications

Projet de loi fixant les règles générales relatives aux services de confiance pour les transactions électroniques et à l'identification électronique

Exposé des motifs

Le présent projet de loi a pour objet de mettre en place un nouveau cadre national de certification électronique qui permet d'instaurer un environnement numérique de confiance et de renforcer la sécurité des systèmes d'information nationaux tout en levant les contraintes auxquelles s'est heurtée la mise en œuvre de la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques.

D'autre part, et tout en s'inscrivant dans le cadre de la dynamique de numérisation, et afin de permettre à notre pays d'être au diapason de l'évolution technologique en la matière, ce projet de loi consacre l'avènement des services de confiance, de l'identification électronique et des transactions électroniques, favorisant ainsi le développement et l'utilisation sécurisée des services numériques.

Dans ce contexte, un groupe de travail multisectoriel composé de représentants des institutions concernées, a été mis en place sous l'égide du Ministère de la Défense Nationale, sur instruction de Monsieur le Premier Ministre contenue dans son envoi n° 145 du 13 avril 2022 adressé à Monsieur le Chef d'état-major, à l'effet d'étudier et de réviser, le cas échéant, la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015, suscitée, et dont les travaux ont mis en évidence plusieurs contraintes qui ont entravé l'emploi de la certification électronique dans notre pays, d'une manière générale, et au niveau des institutions de l'Etat, en particulier.

Ces observations et contraintes se résument principalement en :

- la multiplicité des autorités et leur rattachement à des institutions différentes engendrant ainsi des difficultés en matière de rationalisation des ressources ;
- les champs de compétence de l'Autorité Gouvernementale de Certification Electronique (AGCE) et de l'Autorité Economique de Certification Electronique (AECE) ne sont pas suffisamment précis ;
- la difficulté d'intégrer les institutions de l'Etat dans le schéma de certification électronique, et ce pour des raisons liées principalement à la lourdeur des procédures et à la tarification appliquées.

En effet, l'AGCE a consenti des dépenses assez conséquentes pour la mise en place du schéma national de confiance et ce pour l'acquisition des équipements et la réalisation des audits internationaux de web trust, impliquant ainsi une hausse des tarifs appliqués aux services de certification électronique proposés aux administrations et institutions publiques relevant de la branche gouvernementale. Ces tarifs appliqués par l'AGCE ont eu pour effet de freiner la dynamique pour l'adoption des services de certification électroniques par les administrations et institutions publiques.

Par conséquent, il a été jugé nécessaire de remplacer le schéma de certification électronique, prévu par la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 en vigueur, par un nouveau cadre organisationnel afin de surmonter ces contraintes, en optant pour une approche progressive, maitrisée, prudente et sécurisée, permettant la préservation des acquis réalisés en termes de compétence et d'infrastructure, la mutualisation des ressources et l'optimisation des dépenses.

Ce nouveau cadre organisationnel se traduit en schéma où sa mise en œuvre repose sur les composantes suivantes :

- prestataires de services de certification électronique pour la branche économique ;
- tiers de confiance pour la branche gouvernementale ;
- titulaire de certificat électronique, l'utilisateur final du certificat électronique dans les deux branches gouvernementale et économique.

Concernant les tiers de confiance pour la branche gouvernementale, il convient de souligner que la loi n°15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015, susmentionnée, ne prévoit pas de mission et d'exigences concernant le tiers de confiance. A ce titre, le présent projet de loi encadre l'activité du tiers de confiance en formalisant la procédure de son intégration dans le schéma national de certification électronique ainsi la définition des exigences lui permettant d'intégrer la chaine de confiance dans la branche gouvernementale.

Il convient de noter que les missions et les obligations assignées au prestataire de service de certification électronique sont les mêmes définies dans la loi n°15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015, suscitée, et qui ont été réadaptés par rapport au nouveau schéma organisationnel prévu par le présent projet de loi.

Ainsi, le présent projet de loi, et après examen des différents aspects, notamment, technique et fonctionnel liés à la certification électronique, propose un nouveau cadre organisationnel basé sur une seule Autorité Nationale de Certification Electronique (ANCE), qui sera chargée des deux domaines gouvernemental et économique. A ce titre, ce projet de loi définit l'ANCE comme étant un établissement public à caractère spécifique, dotée de la personnalité morale et de l'autonomie financière où son organisation et son fonctionnement seront fixés par voie réglementaire.

Cela lui permettra de disposer d'un statut approprié pour assurer la gratuité des services dans le domaine gouvernemental et exercer une activité commerciale dans le domaine économique. A ce titre, l'ANCE sera doté d'un statut juridique approprié qui va lui permettre, d'une part, d'exercer les prérogatives de puissance publique notamment tel que la délivrance des autorisations, le contrôle des prestataires des services, le pouvoir de sanction, et d'autre part d'exercer une activité commerciale à travers la fourniture des services de confiances au profit des parties relevant du domaine économique.

Il est à souligner que l'autorité sera chargée de prester dans un premier temps dans le domaine économique, et ce dans la mesure où il s'agit d'un domaine sensible et complexe, relevant de la souveraineté et la sécurité nationales afin de permettre progressivement l'ouverture du marché sur les acteurs privés et d'assurer une concurrence effective.

En plus de procurer à l'ANCE une meilleure flexibilité dans l'exercice de ses missions et dans la gestion et l'optimisation de ses ressources, et ce, au regard de l'évolution rapide des technologies et de la complexité et la spécificité de ses activités, le statut proposé permettra la fidélisation et la valorisation de la ressource humaine spécialisée dans un domaine relevant de la souveraineté nationale, en lui garantissant les avantages et les motivations nécessaires.

En outre, et considérant que la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015, suscitée, ne prend en charge que la certification et la signature électroniques, le présent projet de loi propose d'élargir le périmètre des services en intégrant les catégories des services de confiance qui englobent ce qui suit :

- la signature électronique ;
- la signature électronique qualifiée ;
- le cachet électronique ;
- le cachet électronique qualifié ;
- la validation et la conservation de la signature et du cachet électroniques qualifiés ;
- l'horodatage électronique qualifié ;
- l'envoi recommandé électronique qualifié ;
- le certificat d'authentification de dispositif Internet.

De plus, ce projet vise à définir un cadre légal pour les documents électroniques, en garantissant leur sécurité juridique et leur reconnaissance au même niveau que les documents papier ; l'accent est mis, à ce titre, sur la nécessité de conserver ces documents de manière à préserver leur intégrité et leur fiabilité dans le temps, en utilisant des technologies et des procédures appropriées.

La validité des documents électroniques en tant que preuve juridique est également affirmée, sous réserve du respect de conditions garantissant leur authenticité et leur intégrité.

De surcroit, ce projet prévoit des dispositions relatives aux contrats électroniques, en reconnaissant leur validité et en définissant les conditions de leur formation, qu'ils soient conclus entre des personnes ou des systèmes automatisés, ainsi que dispositions relatives à l'attribution et à la réception des documents électroniques précisant les responsabilités des parties et les modalités de preuve.

Par ailleurs, le présent projet de loi introduit le principe de l'identification électronique qui permet de prouver de manière fiable l'identité d'une personne ou d'un organisme à l'effet de lui permettre d'accéder à un large éventail de services en ligne et d'interagir, de manière sécurisée avec ces derniers, ce qui constitue le socle de l'emploi des services de confiance.

Sur un autre registre, le projet de loi prévoit un titre consacré au contrôle et sanctions où il aborde :

- les modalités d'exercice de l'audit et du contrôle des tiers de confiance et des prestataires de service de confiances ;

- les modalités d'accréditation des prestataires de service d'audit, habilités à effectuer des audits périodiques ;

- la révision des sanctions pécuniaires et administratives applicables aux prestataires de services de confiance en cas de non-respect des conditions qui leurs sont imposées, et des sanctions pénales applicables en cas d'infractions relatives aux services de confiance.

Le présent projet de loi prévoit également des obligations qui incombent au fournisseur de service de confiance en matière de protection des données recueillies par ce dernier qui doivent être hébergées sur le territoire national et peuvent être transférées en dehors de celui-ci, dans le cadre de son activité, conformément à la législation et la réglementation en vigueur.

Cette obligation d'hébergement obligatoire des données sur le territoire national a pour objet d'assurer la protection des informations sensibles et stratégiques de consolider la souveraineté numérique.

Aussi, et afin de garantir une transition harmonieuse dans la mise en œuvre du nouveau schéma, et pour maintenir l'activité de certification électronique, le présent projet de loi prévoit des dispositions transitoires selon lesquelles les certificats électroniques délivrés par les organismes fournissant les services de confiance, avant l'entrée en vigueur de la présente loi, demeurent valables jusqu'à leur expiration dans la limite des délais fixés par l'Autorité.

Par ailleurs, et jusqu'à la mise en œuvre d'une concurrence effective entre les prestataires de services de confiance, l'autorité assurera l'activité de fourniture des services de confiance dans le domaine économique. Cependant, et jusqu'à la mise en place effective de l'Autorité prévue par le présent projet de loi, l'Autorité Nationale, l'Autorité Gouvernementale et l'Autorité Économique de certification électronique continuent d'exercer les missions qui leur sont conférées, en vertu de la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015, suscitée, et de ses textes d'application, jusqu'à la mise en place effective de l'Autorité.

Enfin, compte tenu du nombre important de modifications que requiert la mise en place du nouveau cadre national de certification électronique, et qui doivent être apportées à la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015, suscitée, le présent projet de loi abroge toutes les dispositions de cette loi. Toutefois, ses textes d'application demeurent en vigueur jusqu'à la publication des textes d'application du présent projet de loi.

Telle est l'économie du présent projet de loi.

Projet de loi n°..... du .....correspondant au ..... fixant les règles générales relatives aux services de confiance pour les transactions électroniques et à l'identification électronique.

Le Président de la République,

- Vu la Constitution notamment, ses articles 114,139, 141 (alinéa 2), 143, 145 et 148 ;
- Vu la loi organique n° 18-15 du 22 Dhou El Hidja 1439 correspondant au 2 septembre 2018, modifiée et complétée, relative aux lois de finances ;
- Vu l'ordonnance n° 66-156 du 8 juin 1966, modifiée et complétée, portant code pénal ;
- Vu l'ordonnance n° 75-58 du 26 septembre 1975, modifiée et complétée, portant code civil ;
- Vu l'ordonnance n° 75-59 du 26 septembre 1975, modifiée et complétée, portant code de commerce ;
- Vu la loi n° 88-01 du 12 janvier 1988, modifiée, portant loi d'orientation sur les entreprises publiques économiques ;
- Vu l'ordonnance n° 03-03 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003, modifiée et complétée, relative à la concurrence ;
- Vu la loi n° 04-02 du 5 Joumada El Oula 1425 correspondant au 23 juin 2004, modifiée et complétée, fixant les règles applicables aux pratiques commerciales ;
- Vu la loi n° 04-04 du 5 Joumada El Oula 1425 correspondant au 23 juin 2004, modifiée et complétée, relative à la normalisation ;
- Vu la loi n° 04-08 du 27 Joumada Ethania 1425 correspondant au 14 août 2004, modifiée et complétée, relative aux conditions d'exercice des activités commerciales ;
- Vu la loi n° 08-09 du 18 Safar 1429 correspondant au 25 février 2008, modifiée et complétée, portant code de procédure civile et administrative ;
- Vu la loi n° 09-03 du 29 Safar 1430 correspondant au 25 février 2009, modifiée et complétée, relative à la protection du consommateur et à la répression des fraudes ;
- Vu la loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication ;
- Vu la loi n° 15-03 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 relative à la modernisation de la justice ;
- Vu la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques ;
- Vu la loi n° 18-04 du 24 Chaâbane 1439 correspondant au 10 mai 2018 fixant les règles générales relatives à la poste et aux communications électroniques ;
- Vu la loi n° 18-05 du 24 Chaâbane 1439 correspondant au 10 mai 2018 relative au commerce électronique ;
- Vu la loi n° 18-07 du 25 Ramadhan 1439 correspondant au 10 juin 2018, modifiée et complétée, relative à la protection des personnes physiques dans le traitement des données à caractère personnel ;
- Vu l'ordonnance n° 21-09 du 27 Chaoual 1442 correspondant au 8 juin 2021 relative à la protection des informations et des documents administratifs ;
- Vu la loi n° 23-07 du 3 Dhou El Hidja 1444 correspondant au 21 juin 2023 relative aux règles de comptabilité publique et de gestion financière ;
- Vu la loi n° 24-02 du 16 Chaâbane 1445 correspondant au 26 février 2024 relative à la lutte contre le faux et l'usage de faux ;

- Vu la loi n° 25-14 du 9 Safar 1447 correspondant au 3 août 2025 portant code de procédure pénale ;
- Après avis du Conseil d'Etat ;
- Après adoption par le Parlement ;

Promulgue la loi dont la teneur suit :

TITRE I

DISPOSITIONS GENERALES

Article 1er. — La présente loi a pour objet de fixer les règles générales relatives aux services de confiance pour les transactions électroniques et à l'identification électronique.

Art.2. — Il est entendu au sens de la présente loi par :

1- **certificat de signature électronique** : un document sous forme électronique attestant du lien entre les données de validation de signature électronique et le signataire.

2- **signature électronique** : des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer, servant de méthode d'authentification.

3- **signataire** : personne physique qui crée la signature électronique.

4- **certificat de cachet électronique :** un document électronique qui associe les données de validation d'un cachet électronique au créateur du cachet et confirme sa dénomination.

5- **cachet électronique :** des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières.

6- **créateur de cachet électronique :** personne morale qui crée un cachet électronique.

7- **données de création d'une signature électronique ou d'un cachet électronique** : des données uniques qui sont utilisées par le signataire ou le créateur du cachet électronique pour créer une signature électronique ou un cachet électronique.

8- **dispositif de création d'une signature électronique ou d'un cachet électronique** : un dispositif logiciel ou matériel configuré servant à créer une signature électronique ou un cachet électronique.

9- **données de validation d'une signature électronique ou d'un cachet électronique** : des données qui servent à valider une signature électronique ou un cachet électronique.

10-**validation :** le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique.

11-**horodatage électronique** : des données sous forme électronique qui associent d'autres données sous forme électronique à un instant donné et établissent la preuve que ces dernières données existaient à cet instant.

12-**service d'envoi recommandé électronique** : un service qui permet de transmettre des données entre des personnes par voie électronique, en fournissant des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

13-**certificat d'authentification de dispositif Internet :** un document électronique qui permet d'authentifier un dispositif internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré.

14-**service de confiance :** un service électronique qui garantit certaines qualités d'un document électronique et comprend notamment les méthodes de création et de gestion de la signature électronique, du cachet électronique, de l'horodatage électronique, de l'authentification des

dispositifs internet, de la conservation électronique et des services d'envoi recommandé électronique.

15-**service de confiance qualifié :** un service de confiance qui satisfait aux exigences de la présente loi.

16-**autorisation** : désigne le régime d'exploitation de services de confiance et se matérialise par un document officiel délivré au prestataire de services de confiance, lui permettant la fourniture effective de ces services.

17-**intervenants dans le domaine gouvernemental** : institutions et administrations publiques, telles que définies par la législation en vigueur, institutions nationales autonomes, autorités de régulation, ainsi que toute personne morale ou organisme autre qu'industriel, économique ou commercial.

18-**tiers de confiance** : intervenant dans le domaine gouvernemental qui fournit des services de confiance ou des services de confiance qualifiés dans son champ de compétence.

19-**prestataire de services de confiance** : personne morale qui fournit des services de confiance ou des services de confiance qualifiés dans le domaine économique.

20-**autorité :** Autorité Nationale de Certification Electronique prévue par la présente loi.

21-**liste de confiance :** liste élaborée, mise à jour et publiée d'une manière sécurisée et adaptée par l'Autorité, comportant notamment les informations relatives aux prestataires de services de confiance ainsi que celles relatives aux services de confiance qu'ils fournissent.

22-**partie utilisatrice** : une personne physique ou morale qui agit sur la base du résultat d'un service de confiance.

23-**titulaire de certificat de signature ou de cachet électronique** : personne physique ou morale à laquelle a été délivré un certificat de signature électronique.

24-**politique de certification électronique** : ensemble de règles et procédures organisationnelles et techniques liées à la certification électronique.

25-**audit** : vérification de la conformité par rapport à un référentiel.

26-**identification électronique** : un processus utilisé pour obtenir une assurance suffisante quant au lien entre une personne et une identité.

27-**attribut** : information ou donnée associée à une personne physique ou morale.

28-**identité** : un ensemble d'attributs qui permet à une personne d'être identifiée de manière unique dans un contexte particulier.

29-**moyen d'identification électronique** : les données, ou l'objet matériel sur lequel elles peuvent se trouver, qu'une personne peut présenter à des fins d'identification électronique.

30-**preuve d'identité** : processus consistant à réunir, à vérifier et à valider suffisamment d'attributs pour établir et confirmer l'identité d'une personne dans un contexte particulier.

31-**système d'identification électronique** : un ensemble de fonctions et de fonctionnalités permettant de gérer la preuve d'identité et l'identification électronique.

32-**document électronique :** tout contenu ou information créé, transmis, reçu ou conservé sous forme électronique et par des moyens électroniques, magnétiques ou optiques ou des moyens analogues.

33-**transaction électronique :** toute transaction conclue, exécutée, fournie et délivrée, totalement ou partiellement, sous forme électronique qui englobe les contrats et conventions et toutes autres transactions et autres services.

Art.3. — Les dispositions de la présente loi s'appliquent :

- aux personnes physiques ou morales utilisant les transactions électroniques et les services de confiance ;
- aux transactions électroniques, aux documents électroniques et aux services de confiance ainsi qu'aux procédures nécessaires pour leur concrétisation.

TITRE II

DE LA FOURNITURE DE SERVICES DE CONFIANCE

Chapitre 1er

Des services de confiance

Art.4. — La signature électronique avancée et le cachet électronique avancé doivent satisfaire les exigences suivantes :

- être liés au signataire ou au créateur de cachet de manière univoque ;
- permettre d'identifier le signataire ou le créateur de cachet ;
- être liés aux données auxquelles ils sont associés de telle sorte que toute modification ultérieure des données soit détectable ;
- avoir été créés à l'aide de données de création de signature électronique ou de cachet électronique que le signataire ou le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer une signature électronique ou un cachet électronique.

Art.5. — Outre les exigences prévues à l'article 4 ci-dessus, la signature électronique qualifiée et le cachet électronique qualifié, doivent :

- être crées sur la base d'un certificat électronique qualifié conformément aux dispositions de la présente loi ;
- être créés par un dispositif qualifié de création de signature électronique ou du cachet électronique.

Art.6. — Les certificats de signature électronique qualifiée et du cachet électronique qualifié doivent contenir :

- une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de signature ou de cachet électronique ;
- un ensemble de données représentant sans ambiguïté le fournisseur de services de confiance délivrant les certificats qualifiés, comprenant la dénomination et, le cas échéant, le numéro d'immatriculation tel que prévu par la législation et la réglementation en vigueur ;

- pour les certificats de signature électronique, au moins le nom du signataire ou un pseudonyme ; si un pseudonyme est utilisé, cela doit être clairement indiqué ;
- pour les certificats de cachet électronique, au moins la dénomination du créateur du cachet et, le cas échéant, son numéro d'immatriculation tel que prévu par la législation et la réglementation en vigueur ;
- des données de validation de la signature ou de cachet électronique qui correspondent aux données de création de la signature ou du cachet électronique ;
- des précisions sur le début et la fin de la période de validité du certificat ;
- le code d'identité du certificat électronique, qui doit être unique pour le fournisseur de services de confiance ;
- la signature électronique avancée ou qualifiée ou le cachet électronique avancé ou qualifié du fournisseur de services de confiance délivrant le certificat ;
- le lien électronique permettant de consulter librement et gratuitement le certificat sur lequel repose la signature électronique ou le cachet électronique du fournisseur de services de confiance ;
- les informations ou l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité des certificats ;
- lorsque les données de création de la signature ou de cachet électronique associées aux données de validation de la signature ou de cachet électronique se trouvent dans un dispositif qualifié de création de signature électronique ou cachet électronique, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

Art.7. — Seule la signature électronique qualifiée est assimilée à une signature manuscrite.

Art.8. — Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

Art.9. — La conformité du dispositif qualifié de création de signature électronique ou du cachet électronique est attestée par l'organisme national en charge de la sécurité des systèmes d'information.

Art.10. — Les exigences applicables aux dispositifs qualifiés de création de signature électronique et du cachet électronique sont :

1. Les dispositifs qualifiés de création de signature électronique garantissent au moins, par des moyens techniques et des procédures appropriées que :
   - la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;
   - les données de création de signature électronique qui servent à créer la signature électronique ne peuvent être pratiquement utilisées qu'une seule fois ;
   - l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que cette dernière est protégée de manière fiable contre toute falsification ;
   - les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par les autres.

- pour les certificats de signature électronique, au moins le nom du signataire ou un pseudonyme ; si un pseudonyme est utilisé, cela doit être clairement indiqué ;
- pour les certificats de cachet électronique, au moins la dénomination du créateur du cachet et, le cas échéant, son numéro d'immatriculation tel que prévu par la législation et la réglementation en vigueur ;
- des données de validation de la signature ou de cachet électronique qui correspondent aux données de création de la signature ou du cachet électronique ;
- des précisions sur le début et la fin de la période de validité du certificat ;
- le code d'identité du certificat électronique, qui doit être unique pour le fournisseur de services de confiance ;
- la signature électronique avancée ou qualifiée ou le cachet électronique avancé ou qualifié du fournisseur de services de confiance délivrant le certificat ;
- le lien électronique permettant de consulter librement et gratuitement le certificat sur lequel repose la signature électronique ou le cachet électronique du fournisseur de services de confiance ;
- les informations ou l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité des certificats ;
- lorsque les données de création de la signature ou de cachet électronique associées aux données de validation de la signature ou de cachet électronique se trouvent dans un dispositif qualifié de création de signature électronique ou cachet électronique, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

Art.7. — Seule la signature électronique qualifiée est assimilée à une signature manuscrite.

Art.8. — Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

Art.9. — La conformité du dispositif qualifié de création de signature électronique ou du cachet électronique est attestée par l'organisme national en charge de la sécurité des systèmes d'information.

Art.10. — Les exigences applicables aux dispositifs qualifiés de création de signature électronique et du cachet électronique sont :

1. Les dispositifs qualifiés de création de signature électronique garantissent au moins, par des moyens techniques et des procédures appropriées que :
   - la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;
   - les données de création de signature électronique qui servent à créer la signature électronique ne peuvent être pratiquement utilisées qu'une seule fois ;
   - l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que cette dernière est protégée de manière fiable contre toute falsification ;
   - les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par les autres.

2. les dispositifs qualifiés de création de signature électronique ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

3. la génération ou la gestion de données de création de signature électronique pour le compte du signataire peut être seulement confiée à un fournisseur de services de confiance qualifiés.

4. sans préjudice des dispositions du dernier tiret du paragraphe 1, un fournisseur de services de confiance qualifiés gérant des données de création de signature électronique pour le compte d'un signataire ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect des exigences suivantes :

   - le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine :
   - le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

Art.11. — Le processus de validation de la signature électronique qualifiée et du cachet électronique qualifié confirme la validité de la signature électronique qualifié et du cachet électronique qualifié à condition que :

- les données de validation de la signature électronique qualifiée et du cachet électronique qualifié soient identiques aux données présentées à la partie utilisatrice ;
- l'ensemble unique de données représentant le signataire ou le créateur du cachet dans le certificat soit correctement fourni à la partie utilisatrice :
- l'utilisation d'un pseudonyme soit clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature ou de la création du cachet.

Art.12. — Les services de validation de la signature électronique qualifiée et du cachet électronique qualifié fournissent à la partie utilisatrice le résultat correct du processus de validation, signé par le fournisseur de ces services, et permettent de détecter tout problème relatif à la sécurité.

Art.13. — La fourniture des services de conservation de signature électronique qualifiée ou de cachet électronique qualifié doit utiliser des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées ou des cachets électroniques qualifiés au-delà de la période de validité technologique.

Art.14. — Un horodatage électronique qualifié doit satisfaire aux exigences suivantes :

- il lie la date et l'heure aux données de manière à exclure la possibilité de modification indétectable des données ;
- il est fondé sur une horloge exacte liée au temps universel coordonné :
- il est signé au moyen d'une signature électronique avancée, ou cacheté au moyen d'un cachet électronique avancé du fournisseur de services de confiance.

Art.15. — Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure.

Art.16. —La signature électronique ou le cachet électronique ou l'horodatage électronique ne peut être privé de son efficacité juridique et ne peut être refusé devant la justice au seul motif qu'il se présente sous une forme électronique ou qu'il ne satisfait pas les exigences de la présente loi.

Art.17. — Les services d'envoi recommandé électronique qualifiés doivent satisfaire aux exigences suivantes :

- ils garantissent l'identification de l'expéditeur avec un degré de confiance élevé ;
- ils garantissent l'identification du destinataire avant la fourniture des données ;
- l'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un fournisseur de services de confiance, de manière à exclure toute possibilité de modification indétectable des données ;
- toute modification des données nécessaires pour l'envoi ou la réception de données est clairement signalée à l'expéditeur et au destinataire des données ;
- la date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié.

Art.18. — Les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié bénéficient d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié.

Art.19. — Les données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique ne peuvent être privés de leur efficacité juridique et ne peuvent être refusés devant la justice au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas les exigences du service d'envoi recommandé électronique qualifié.

Art.20. — Les certificats qualifiés d'authentification de dispositif internet doivent contenir :

- une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié d'authentification de dispositif internet ;
- un ensemble de données représentant sans ambiguïté le fournisseur de services de confiance délivrant les certificats qualifiés, comprenant la dénomination et, le cas échéant, le numéro d'immatriculation tel que prévu par la législation et la réglementation en vigueur ;
- pour les personnes physiques, au moins le nom de la personne à qui le certificat a été délivré, ou un pseudonyme. Si un pseudonyme est utilisé, cela doit être clairement indiqué ;
- pour les personnes morales, au moins la dénomination de la personne morale à laquelle le certificat est délivré et, le cas échéant, le numéro d'immatriculation tel que prévu par la législation et la réglementation en vigueur ;
- des éléments de l'adresse, dont au moins la ville, de la personne physique ou morale à laquelle le certificat est délivré ;

- le(s) nom(s) de domaine exploité(s) par la personne physique ou morale à laquelle le certificat est délivré ;
- des précisions sur le début et la fin de la période de validité du certificat ;
- le code d'identité du certificat, qui doit être unique pour le fournisseur de services de confiance ;
- la signature électronique avancée ou qualifiée ou le cachet électronique avancé ou qualifié du fournisseur de services de confiance ayant délivré le certificat ;
- le lien électronique permettant de consulter librement et gratuitement le certificat sur lequel repose la signature électronique ou le cachet électronique du fournisseur de services de confiance ;
- les informations ou l'emplacement des services qui peuvent être utilisés pour connaitre le statut de validité des certificats.

Art.21. — L'utilisation de pseudonymes dans des certificats électroniques ne doit pas empêcher l'identification des personnes conformément aux dispositions de la présente loi.

Art.22. — Dès la signature de son certificat de signature ou de cachet électronique, le titulaire est seul responsable de la confidentialité des données de création de sa signature ou de son cachet.

En cas de doute quant au maintien de la confidentialité des données de création de la signature ou de cachet électroniques ou de la perte de conformité à la réalité des informations contenues dans le certificat de signature ou de cachet électroniques, le titulaire est tenu de le faire révoquer par l'Autorité, les tiers de confiance ou le prestataire de services de confiance, ayant délivré ce certificat.

Lorsqu'un certificat de signature ou de cachet électroniques est arrivé à échéance ou a été révoqué, le titulaire de celui-ci ne peut utiliser les données de création de signature ou de cachet électroniques correspondantes pour signer ou faire certifier ces données par un autre tiers de confiance ou un autre prestataire de services de confiance.

Art.23. — Le titulaire ne peut utiliser son certificat de signature ou de cachet électroniques à des fins autres que celles pour lesquelles il lui a été délivré.

Art.24. — Outre les services de confiance mentionnés dans le présent chapitre, l'Autorité peut, en tant que de besoin, ajouter d'autres services de confiance et fixer les exigences de leur fourniture.

Art.25. — Les services de confiance fournis par un fournisseur de services de confiance établi dans un pays étranger ont la même valeur que ceux fournis par un fournisseur de services de confiance établi en Algérie, à condition que ce fournisseur étranger agisse dans le cadre d'une convention de reconnaissance mutuelle.

Chapitre 2

Des fournisseurs de services de confiance

Art.26. — Les tiers de confiance et les prestataires de services de confiance sont considérés en tant que fournisseur de services de confiance.

Art.27. — Toutes les données recueillies par les fournisseurs de services de confiance, doivent être hébergées, sur le territoire national et peuvent être transférées en dehors de celui-ci, dans le cadre de leur activité, sans préjudice des dispositions législatives et réglementaires en vigueur.

Art.28. — Les intervenants dans le domaine gouvernemental désirant exercer comme tiers de confiance doivent obtenir un accord préalable de l'Autorité après la soumission d'une demande.

Art.29. — La fourniture des services de confiance est tributaire des résultats concluants d'un audit d'évaluation réalisé par l'Autorité ou l'organisme national en charge de la sécurité des systèmes d'information, conférant aux intervenants dans le domaine gouvernemental la qualité de tiers de confiance.

L'opération d'audit d'évaluation est réalisée sur demande de l'institution concernée, adressée à l'Autorité.

Art.30. — Le tiers de confiance fournit, à titre gratuit dans son champ de compétence, les services de confiance et les services de confiance qualifiés.

Art.31. — Le tiers de confiance est tenu :

- de se conformer aux exigences requises pour la fourniture des services de confiance, définies par l'Autorité ;
- de préserver la confidentialité des données et des informations liées à la fourniture de services de confiance ;
- d'assurer la conservation, de concert avec l'Autorité, des certificats électroniques après leur expiration conformément aux politiques de certification électronique ;
- De se soumettre aux audits périodiques prévus par la présente loi.

Art.32. — Le tiers de confiance ne peut ni conserver, ni copier les données de création de signature de la personne à laquelle il a fourni un certificat électronique, sauf sur accord exprès de la personne concernée.

Art.33. — La prestation de services de confiance, dans le domaine économique, est soumise à une autorisation délivrée par l'Autorité.

L'autorisation est délivrée par service, assortie d'un cahier des charges, élaboré par l'Autorité, fixant la durée de l'autorisation, les conditions et les modalités de la prestation du service s'y rapportant.

Art. 34. — Tout demandeur d'une autorisation pour la prestation de services de confiance doit réunir les conditions suivantes :

- être une personne morale de droit algérien ou de nationalité algérienne pour la personne physique ;
- répondre à toutes les conditions et aux exigences de prestation fixées dans les cahiers des charges ;
- disposer de capacités financières suffisantes ;
- avoir des qualifications et une expérience avérée dans le domaine des technologies de l'information et de la communication pour la personne physique ou le gérant de la personne morale ;
- ne pas avoir fait l'objet de condamnation pour crime ou délit incompatible avec l'activité de prestation de services de confiance.

Art.35.— Préalablement à l'octroi de l'autorisation, une attestation d'éligibilité est délivrée pour une durée de deux (2) ans, renouvelable une seule fois. Celle-ci est délivrée à tout demandeur éligible pour la mise en place de tous les moyens nécessaires à l'activité de prestation de services de confiance.

L'attestation est notifiée dans un délai maximum de soixante (60) jours à compter de la date de réception de la demande attestée par un accusé de réception.

Le détenteur de l'attestation d'éligibilité ne peut fournir les services de confiance qu'après l'obtention de l'autorisation.

Le demandeur d'une autorisation ne peut être inscrit au registre du commerce qu'après détention de l'attestation d'éligibilité.

Art.36. — L'autorisation est délivrée au détenteur de l'attestation d'éligibilité suite à une opération d'audit d'évaluation concluante.

L'opération d'audit d'évaluation est réalisée, sur requête du détenteur de l'attestation d'éligibilité, préalablement à l'octroi de l'autorisation de prestation de services de confiance, par l'Autorité ou par un prestataire de service d'audit accrédité, conformément à la politique de certification électronique de l'Autorité et aux cahiers des charges fixant les conditions et les modalités de la prestation des services de confiance.

L'opération d'audit doit commencer dans un délai n'excédant pas les soixante (60) jours à compter de la date de réception de la demande d'audit.

Art.37. — L'avis défavorable de délivrance de l'attestation d'éligibilité ou de l'autorisation doit être motivé, il est notifié contre un accusé de réception.

Art.38. — L'attestation d'éligibilité et l'autorisation sont personnelles et ne peuvent être cédées à des tiers.

Art.39. — L'autorisation est soumise au paiement d'une contrepartie financière dont les montants et les modalités de recouvrement sont fixés par la loi de finance.

Art.40. — Le prestataire de services de confiance est tenu :

- de préserver la confidentialité des données et des informations liées à la fourniture des services de confiance ;
- de ne recueillir que les données personnelles nécessaires à la fourniture des services de confiance. Ces données ne peuvent être utilisées à d'autres fins ni être recueillies sans consentement exprès de l'intéressé ;
- d'assurer la conservation des certificats électroniques après leur expiration, conformément aux politiques de certification électronique ;
- de ne conserver, ni de copier les données de création de signature et de cachet électroniques qu'après accord exprès de la personne concernée ;
- de fournir à l'Autorité tout document ou information utile pour l'accomplissement des missions qui lui sont dévolues par la présente loi ;
- de souscrire une assurance en garantie de sa responsabilité civile.

Art.41. — Le prestataire de services de confiance doit prendre les mesures nécessaires afin de répondre à une demande de révocation d'un certificat électronique, conformément à sa politique de certification approuvée par l'Autorité.

La révocation est opposable aux tiers à partir de sa publication, conformément à la politique de certification électronique du prestataire de services de confiance.

Art.42. — Le prestataire de services de confiance a l'obligation d'appliquer des tarifs pour les services fournis en adéquation avec les principes de tarification fixés par l'Autorité.

Art.43. — Le prestataire de services de confiance fournit ses services dans le cadre des principes de transparence et de non-discrimination.

Le prestataire de services de confiance ne peut refuser de fournir ses services sans motif valable.

Art. 44. Un fournisseur de services de confiance qui fournit des services de confiance qualifiés doit :

- informer l'Autorité de toute modification dans la fourniture de ses services de confiance qualifiés et de son intention éventuelle de cesser ses activités :
- employer du personnel possédant l'expertise, la fiabilité et les qualifications nécessaires ;
- informer de manière claire et exhaustive, avant d'établir une relation contractuelle, toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation ;
- utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et le vol des données et qui assurent la sécurité technique et la fiabilité des processus qu'ils prennent en charge :
- utiliser des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière à ce que :
    - les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée :
    - seules des personnes autorisées puissent introduire des données et modifier les données conservées ;
    - l'authenticité des données puisse être vérifiée.
- Conserver dans la durée prévue par le cahier des charges, y compris après cessation des activités du prestataire de services de confiance qualifié, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins notamment de pouvoir fournir des preuves devant la justice et d'assurer la continuité du service.

Art.45. — Lorsqu'un fournisseur de services de confiance délivre un certificat électronique qualifié pour un service de confiance qualifié, il vérifie, par des moyens appropriés, l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat électronique qualifié.

Les informations citées au premier alinéa ci-dessus sont vérifiées par le fournisseur de services de confiance qualifiés :

- par la présence en personne de la personne physique ou du représentant légal de la personne morale : ou
- à distance, à l'aide de moyens d'identification électronique pour lesquels, avant la délivrance du certificat qualifié, la personne physique ou le représentant légal de la personne morale s'est présenté en personne et qui satisfont aux exigences mentionnées dans la présente loi, en ce qui concerne les niveaux de garantie substantiel et élevé : ou

- au moyen d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au premier ou au deuxième tiret, ci-dessus, ou
- à l'aide d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente, en termes de fiabilité, à la présence en personne.

La garantie équivalente est confirmée par l'organisme national en charge de la sécurité des systèmes d'information.

Art.46. — Le moyen d'identification électronique utilisé dans les services de confiance qualifiés doit disposer d'un niveau de garantie élevé.

Chapitre 3

De l'Autorité Nationale de Certification Electronique

Art.47.— Il est créé, une Autorité Nationale de Certification Electronique désignée « Autorité ».

L'Autorité est un établissement public à caractère spécifique, doté de la personnalité morale et de l'autonomie financière.

L'organisation et le fonctionnement de l'Autorité sont fixés par voie réglementaire.

Art. 48. — L'Autorité est chargée de la supervision, du contrôle, de la promotion, du développement et de l'organisation des activités liées aux services de confiance. Dans ce cadre elle a pour missions :

- d'élaborer ses politiques de certification électronique et de veiller, après leur approbation conformément à la législation et à la réglementation en vigueur, à leur application ;
- de définir les exigences requises pour la fourniture des services de confiance ;
- d'approuver les politiques de certification électronique élaborées par les fournisseurs de services de confiance ;
- d'élaborer les cahiers des charges fixant les conditions et les modalités de prestation de services de confiance ;
- de fournir les services de confiance et les services de confiance qualifiés ;
- de suivre et de contrôler les fournisseurs de services de confiance, conformément aux exigences et aux modalités de fourniture de services de confiance ;
- d'auditer, à travers les prestataires de service d'audit accrédités ou par ses propres moyens les intervenants dans le domaine gouvernemental désirant être tiers de confiance et les demandeurs d'autorisation désirant devenir prestataire de service de confiance ;
- de veiller à l'exécution des opérations d'audit périodiques ;
- de délivrer les autorisations aux prestataires de services de confiance ;
- d'élaborer, de mettre à jour et de publier la liste de confiance ;
- de contribuer à l'élaboration et à la mise à jour des référentiels nationaux d'audit en matière de fourniture de services de confiance ;

- de veiller à la conservation des certificats électroniques expirés et des données liées à leur délivrance ;
- de prendre les mesures nécessaires pour faire assurer la continuité de services et protéger les intérêts des abonnés en cas d'incapacité d'un prestataire de services de confiance de les fournir ou de retrait de l'autorisation ;
- de conclure, les conventions de reconnaissance mutuelle au niveau international, conformément aux procédures applicables en la matière ;
- de promouvoir l'activité de recherche et développement dans le domaine des services de confiance ;
- de promouvoir l'utilisation et le développement des services de confiance et de garantir la fiabilité de leurs usages.

L'Autorité peut présenter toute suggestion susceptible d'améliorer les cadres législatif et règlementaire relatifs à son domaine de compétence. Elle est consultée, en outre, pour la préparation de tout projet de texte législatif ou réglementaire en relation avec son activité.

Art.49. — L'Autorité est habilitée à requérir des fournisseurs de service de confiance et de toute personne concernée, tout document ou information utile pour l'accomplissement des missions qui lui sont dévolues par la présente loi.

Art.50. — L'Autorité fournit, à titre gratuit, pour les intervenants dans le domaine gouvernemental, les services de confiance et les services de confiance qualifiés. Toutefois, une dérogation à ce principe de gratuité peut être établie par voie réglementaire pour certains services.

Art.51. — Dans le cadre de l'exercice de ses missions, l'Autorité informe le procureur général compétent immédiatement en cas de constatation de faits susceptibles de qualification pénale.

Art.52. — Les décisions prises par l'Autorité peuvent faire l'objet d'un recours devant la juridiction administrative compétente dans les délais prévus par la législation en vigueur.

TITRE III

DES DOCUMENTS ELECTRONIQUES

Chapitre 1

De l'écrit, de la signature, du cachet et du contrat électroniques

Art.53. — Lorsque la législation et la réglementation en vigueur exigent qu'une information, soit écrite, cette exigence est satisfaite dans le cas d'un document électronique si les informations qu'il contient sont conservées de manière à pouvoir les utiliser et s'y référer.

Art.54. — Lorsque la législation et la réglementation en vigueur exige l'existence d'une signature ou d'un cachet sur un document, cette exigence est satisfaite dans le cas d'un document électronique lorsque :

- un moyen d'identification est utilisé pour identifier le signataire ou le créateur de cachet électronique et pour indiquer que ce dernier approuve l'information contenue dans le document ; et que
- la fiabilité de ce moyen d'identification est suffisante au regard de l'objet pour lequel le document électronique a été créé ou communiqué.

Art.55. — L'offre et l'acceptation peuvent être exprimées sous forme électronique pour la conclusion de tout contrat.

Art.56. — Le contrat ne perd pas sa validité, sa force probante ou sa force exécutoire du seul fait qu'il a été conclu au moyen d'un document électronique.

Art.57. — Un contrat peut être conclu en utilisant :

- des moyens électroniques automatisés, contenant un ou plusieurs systèmes d'information électroniques déjà préparés et programmés pour de telles tâches et il est réputé valide, exécutoire et produisant ses effets juridiques.
- un système d'information électronique automatisé, appartenant à une personne, et une autre personne si cette dernière sait ou était censée savoir que ledit système conclura ou exécutera automatiquement le contrat.

Chapitre 2

De la conservation, de l'original et de l'opposabilité des documents électroniques

Art. 58. — Le document signé électroniquement est conservé dans sa forme d'origine, en utilisant des procédures et des technologies permettant d'étendre sa fiabilité tout au long de la durée de son utilité.

Art.59. — Lorsque la législation et la réglementation en vigueur exigent qu'un document ou une information soient conservés, cette exigence est satisfaite dans le cas d'un document électronique s'il est conservé dans les conditions suivantes :

- conservation du document électronique sous la forme dans laquelle il a été créé, envoyé ou reçu, ou sous une forme permettant de prouver qu'il représente exactement les informations initialement créées, envoyées ou reçues ;
- les informations restent conservées d'une manière qui permet de les utiliser et de s'y référer ultérieurement ;
- conservation des informations, le cas échéant, permettant d'identifier l'expéditeur du document électronique, leur destination, la date et l'heure de leur envoi et de leur réception.

Les administrations, les institutions et les organismes publics et privés peuvent ajouter des exigences supplémentaires, qui ne soient pas contraires aux dispositions de la présente loi, afin de conserver les documents électroniques relevant de leurs champs de compétence.

Art.60. — Lorsque la législation et la réglementation en vigueur exigent qu'un document, ou une information soit présenté ou conservé sous sa forme originale, cette exigence est satisfaite dans le cas d'un document électronique lorsque :

- il existe une garantie suffisante quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que document électronique ;
- le document électronique permet d'afficher les informations à chaque fois que celles-ci sont demandées ; et
- il respecte les conditions supplémentaires liées à la présentation ou à la conservation de documents électroniques, spécifiées par les administrations, les institutions et les organismes publics et privés qui supervisent la présentation ou la conservation des documents électroniques soumis à leurs champs de compétence.

Art.61. — L'effet juridique et la recevabilité du document électronique ou des transactions électroniques comme preuve devant la justice ne peuvent être refusés au seul motif qu'ils se présentent sous une forme électronique ou qu'ils ne satisfont pas aux exigences de la présente loi.

Les données contenues dans les documents électroniques ne perdent pas leur opposabilité juridique au motif qu'elles sont contenues, lorsqu'il est possible de consulter les détails de ces données, dans le système d'information électronique par lequel elles ont été créées, et qu'il est indiqué dans les documents électroniques les modalités de leur consultation.

Chapitre 3

De l'attribution

Art.62. — Dans la relation entre l'expéditeur et le destinataire, un document électronique émane ou est réputé émaner de l'expéditeur s'il a été envoyé :

- par l'expéditeur lui-même ;
- par une personne autorisée à agir à cet effet au nom de l'expéditeur ; ou
- par un système d'information programmé par l'expéditeur ou pour son compte pour fonctionner automatiquement.

Art.63. — Le destinataire est en droit de considérer le document électronique émanant de l'expéditeur et d'agir en conséquence dans les cas suivants :

- si le destinataire a correctement appliqué une procédure préalablement agréée par l'expéditeur aux fins de s'assurer que le document électronique a bien été émis par l'expéditeur ;
- si le document électronique reçu par le destinataire résulte des actes d'une personne qui, de par ses relations avec l'expéditeur ou un agent de celui-ci, a eu accès à une procédure que l'expéditeur utilise pour prouver que le document électronique est émis par lui.

Les dispositions du premier alinéa du présent article ne s'appliquent pas dans les cas suivants :

- si le destinataire reçoit une notification de l'expéditeur indiquant que le document électronique n'a pas été émis par lui, à condition qu'il ait été mis à la disposition du destinataire un délai raisonnable pour agir sur la base de la notification ;

- si le destinataire savait, ou était censé savoir en prenant des dispositions raisonnables ou en utilisant une procédure convenue que le document électronique n'a pas été émis par l'expéditeur ;
- s'il est déraisonnable pour le destinataire de considérer que le document électronique a été émis par l'expéditeur.

Art.64. — Lorsqu'un document électronique émane ou est réputé émaner de l'expéditeur, ou lorsque le destinataire est en droit d'agir sur cette présomption, le destinataire peut, considérer que le document électronique tel qu'il a été reçu est le document que l'expéditeur voulait envoyer, et agir en conséquence.

Les dispositions du premier alinéa, ci-dessus, ne s'appliquent pas si le destinataire savait, ou était censé savoir ou s'il avait pris des dispositions raisonnables ou utilisé une procédure convenue, que la transmission avait entraîné une erreur dans le document électronique tel qu'il a été reçu.

Art.65. — Le destinataire a le droit de considérer que chaque document électronique qu'il reçoit est un document distinct et d'agir sur cette base.

Les dispositions de l'alinéa précédent ne s'appliquent pas lorsque le destinataire savait ou était censé savoir que le document électronique était un deuxième exemplaire.

Chapitre 4

De l'accusé et du moment de réception du document électronique

Art.66. — Sauf accord contraire entre l'expéditeur et le destinataire, l'expédition d'un document électronique est considérée accomplie lorsque celui-ci entre dans un système d'information ne dépendant pas de l'expéditeur.

Art.67. — Sauf accord contraire entre l'expéditeur et le destinataire, le moment de la réception du document électronique est défini comme suit :

- si le destinataire a désigné un système d'information pour recevoir un document électronique :
  - c'est le moment où le document électronique entre dans le système d'information désigné ;
  - dans le cas où le document électronique est envoyé à un autre système d'information du destinataire autre que le système désigné, c'est le moment où le document est récupéré par le destinataire.
- si le destinataire n'a pas désigné de système d'information, c'est le moment où le document électronique entre dans un système d'information du destinataire.

Art. 68. — Lorsque l'expéditeur reçoit l'accusé de réception du destinataire, il est supposé que le destinataire a reçu le document électronique en question, sauf preuve contraire.

L'accusé de réception porte sur la réception du document électronique et non pas sur le contenu de celui-ci.

Art.69. — Si l'expéditeur n'a pas convenu avec le destinataire que l'accusé de réception sera donné sous une forme ou selon une méthode particulière, la réception peut être accusée :

- par toute communication, qu'elle soit automatisée ou non, émanant du destinataire ; ou
- par tout acte du destinataire, suffisant pour indiquer à l'expéditeur que le document électronique a été reçu.

Art.70. — Dans le cas où l'expéditeur mentionne au destinataire que l'effet du document électronique soit subordonné à la réception d'un accusé de réception, le document électronique n'a aucun effet juridique jusqu'à ce que l'expéditeur reçoive l'accusé de réception.

Art.71. — Si l'expéditeur d'un document électronique n'a pas mentionné au destinataire que l'effet du document électronique est subordonné à la réception d'un accusé de réception, et qu'il n'en ait pas reçu, il peut, dans un délai raisonnable aviser le destinataire qu'aucun accusé de réception n'a été reçu et lui fixer un délai raisonnable pour sa réception.

Si l'accusé de réception n'est toujours pas reçu dans le délai, cité à l'alinéa ci-dessus, l'expéditeur peut alors considérer le document électronique comme non-envoyé et le notifier au destinataire.

TITRE IV
DE L'IDENTIFICATION ELECTRONIQUE

Art.72. — L'identification électronique est utilisée pour apporter les garanties nécessaires quant au lien entre une personne physique ou morale, ou une personne physique représentant une personne morale et une identité.

Art.73. — Les niveaux de garantie d'un système d'identification électronique et des moyens d'identification électronique qu'il délivre sont de trois degrés : faible, substantiel et élevé.

Chaque niveau renvoie à un moyen d'identification électronique dans le cadre d'un système d'identification électronique. Il est défini en fonction du degré de fiabilité accordé à l'identité revendiquée ou prétendue d'une personne et caractérisé sur la base de spécifications techniques, de normes et de procédures y afférentes, y compris les contrôles techniques dans l'objectif de réduire ou d'empêcher le risque d'utilisation abusive ou l'altération de l'identité.

Art.74. — L'organisme national en charge de la sécurité des systèmes d'information, de concert avec les parties prenantes concernées, définit les critères et les conditions devant satisfaire les niveaux de garantie du système d'identification électronique.

Art.75. — L'organisme national en charge de la sécurité des systèmes d'information certifie la conformité des moyens d'identification électronique aux critères et conditions cités à l'article 74 ci-dessus, définit leur niveau de garantie et assure la publication de la liste de ces moyens.

Art.76. — Le moyen d'identification électronique est présumé fiable jusqu'à preuve du contraire lorsqu'il répond aux critères et conditions définis par l'organisme national en charge de la sécurité des systèmes d'information.

Art.77. — Le résultat de l'identification électronique ne peut être privé de ses effets juridiques, de sa validité, ou de sa recevabilité en tant que preuve au seul motif que :

- la preuve d'identité et l'identification électronique se font sous forme électronique ;
- le moyen d'identification électronique n'est pas certifié conformément aux dispositions de l'article 74 de la présente loi.

TITRE V

DU CONTROLE ET DES SANCTIONS

Chapitre 1

De l'audit et du contrôle

Art.78. — L'organisme national en charge de la sécurité des systèmes d'information arrête les modalités d'accréditation des prestataires de service d'audit en matière de fourniture des services de confiance, de concert avec l'Autorité, conformément à la législation et à la réglementation en vigueur.

Art.79. — Les tiers de confiance font l'objet d'un audit périodique effectué par l'Autorité ou l'organisme national en charge de la sécurité des systèmes d'information ou un prestataire de service d'audit accrédité afin d'évaluer leur conformité par rapport aux référentiels d'audit nationaux.

Le maintien de la fourniture d'un ou de plusieurs services de confiance est tributaire des résultats des opérations d'audit périodiques.

Art.80. — Les prestataires de services de confiance font l'objet d'un audit périodique effectué à leurs frais par l'Autorité ou un prestataire de service d'audit accrédité afin d'évaluer leur conformité par rapport aux référentiels d'audit nationaux et/ou reconnus par l'Autorité.
Le maintien de la fourniture d'un ou de plusieurs services de confiance par les prestataires de services de confiance est tributaire des résultats des opérations d'audit périodiques.

Art.81. — L'Autorité arrête le programme des audits périodiques au sens de la présente loi et elle informe les organismes nationaux en charge de la sécurité des systèmes d'information et de la protection des données à caractère personnel, des résultats des audits lorsqu'il apparaît que les règles en matière de sécurité des systèmes d'information et de protection des données à caractère personnel n'ont pas été respectées, telles que définies par la législation et la règlementation en vigueur.

Art.82. — Le recours à des prestataires de service d'audit de droit étranger est soumis à l'accord préalable de l'Autorité, émis de concert avec l'organisme national en charge de la sécurité des systèmes d'information.

Art. 83. — Des contrôles périodiques et/ou inopinés des prestataires de services de confiance, sont effectués par l'Autorité, conformément à ses politiques de certification électroniques et/ou aux cahiers des charges fixant les conditions et les modalités de la prestation des services de confiance.

Art.84. — L'Autorité peut procéder aux investigations requises par des constatations dans les locaux et lieux concernés par l'exercice de ses missions. Elle peut à ce titre accéder aux données ainsi qu'à toute information et tout document quel qu'en soit le support. Le secret professionnel ne peut être opposé à l'Autorité.

Art.85. — Outre les officiers et les agents de police judiciaire, les agents assermentés de l'Autorité sont habilités, sous le contrôle du procureur de la République territorialement compétant, à procéder à la recherche et à la constatation des infractions prévues par la présente loi.

Art.86.— Pour l'exercice de leurs fonctions, les agents assermentés cités à l'article 85 ci-dessus, prêtent devant la juridiction territorialement compétente le serment suivant :

" أقسم بالله العلي العظيم ان أؤدي مهامي بأمانة وإخلاص وأراعي في كل الأحوال الواجبات التي تفرضها علي وان أحافظ على سرية المعلومات التي أطلع عليها أثناء وبمناسبة مهامي ".

Art.87. — Les infractions aux dispositions de la présente loi sont constatées par des procès-verbaux. Ces derniers doivent être transmis sans délai, au procureur de la République territorialement compétent.

Dans le cadre de l'exercice de leurs fonctions prévues dans la présente loi, les agents assermentés de l'Autorité peuvent faire appel à la force publique, conformément à la législation en vigueur.

Chapitre 2

Sanctions pécuniaires et administratives

Art.88. — Le non-respect des conditions auxquelles sont soumis les prestataires de services de confiance au titre du cahier des charges et des décisions de l'Autorité donne lieu à l'application des sanctions ci-après :

- sanctions pécuniaires ;
- suspension ou réduction de la durée de l'autorisation ;
- retrait de l'autorisation.

Art.89. — Lorsque le prestataire de services de confiance ne respecte pas les conditions auxquelles il est soumis au titre du cahier des charges ainsi que les décisions prises par l'Autorité, celle-ci, le met en demeure de s'y conformer dans un délai qu'elle fixe par décision préalablement.

Si le prestataire de services de confiance ne se conforme pas aux termes de la mise en demeure, l'Autorité, en fonction de la gravité du manquement dont les degrés sont établis dans les cahiers des charges, prononce par décision motivée à l'encontre du prestataire de services de confiance une sanction pécuniaire dont le montant ne peut dépasser 2 % du montant du chiffre d'affaires hors taxe, réalisé dans le cadre de la prestation de services de confiance, du dernier exercice clos. Ce taux peut atteindre 5 % en cas de nouvelle violation de la même obligation. A défaut d'activité antérieure permettant de déterminer le montant de la sanction pécuniaire, celui-ci ne peut excéder un million (1.000.000) dinars montant porté à deux millions (2.000.000) dinars au maximum, en cas de nouvelle violation de la même obligation.

L'Autorité peut, dans les mêmes formes, prononcer des astreintes qui ne sauraient être inférieures à cinq mille (5.000) dinars et supérieures à cinquante mille (50. 000) dinars par jour de retard dans le paiement des redevances contribution et rémunération pour des services fournis.

Les sommes correspondant aux sanctions pécuniaires mentionnées au 2eme et au 3ème alinéas du présent article sont recouvrées par le Trésor public.

Art.90. — Si, en dépit de l'application de sanctions pécuniaires, le prestataire de services de confiance ne se conforme pas aux conditions de la mise en demeure, l'Autorité prononce par décision motivée, à son encontre et à sa charge, l'une des sanctions suivantes :

- la suspension totale ou partielle de l'autorisation pour une durée n'excédant pas trois (3) mois ;
- la réduction de la durée de l'autorisation dans la limite d'une (1) année.

Art.91.— Si, en dépit de l'application des sanctions prévues par l'article 90, ci-dessus, le prestataire de services de confiance ne se conforme pas aux conditions de la mise en demeure, il peut être prononcé à son encontre le retrait de l'autorisation dans les mêmes formes que celles qui ont prévalu à son obtention.

Art.92. — Dans le cas d'une atteinte à des impératifs exigés par la défense nationale et la sécurité publique par un prestataire de services de confiance, l'Autorité procède, au retrait, sans délais, de l'autorisation. Dans ce cas, les équipements du prestataire de services de confiance font l'objet de mesures conservatoires conformément à la législation en vigueur et ce, sans préjudice des poursuites pénales.

Art.93. — Les sanctions prévues par le présent chapitre ne sont prononcées que lorsque les griefs retenus contre le concerné lui ont été notifiés et qu'il a été à même de consulter le dossier et de présenter ses justifications écrites.

Les modalités d'application du présent article sont fixées par décision de l'Autorité.

Chapitre 3

Dispositions pénales

Art.94. — Sans préjudice de sanctions plus graves prévues par la législation en vigueur, les infractions aux dispositions de la présente loi sont sanctionnées par les peines déterminées dans ce chapitre.

Art.95. — Est punie d'une amende de cinquante mille (50.000) dinars à deux cent mille (200.000) dinars, toute personne qui utilise un service de confiance à des fins autres que celles pour lesquelles il lui a été fourni.

Art.96.— Est puni d'un emprisonnement de deux (2) mois à une (1) année et d'une amende de deux cent mille (200.000) dinars à un million (1.000.000) dinars ou de l'une de ces deux peines, tout prestataire de services de confiance ayant failli à l'obligation d'informer l'Autorité de sa cessation d'activité.

Art.97. — Est puni d'un emprisonnement de deux (2) mois à une (1) année et d'une amende de deux cent mille (200.000) dinars à un million (1.000.000) dinars ou de l'une de ces deux peines, tout prestataire de services de confiance qui ne se conforme pas aux dispositions relatives à la préservation de la confidentialité des données et des informations liées à la fourniture des services de confiance, prévues par l'article 40 tiret 1 de la présente loi.

Art.98.— Est puni d'un emprisonnement de deux (2) mois à une (1) année et d'une amende de deux cent mille (200.000) dinars à un million (1.000.000) dinars ou de l'une de ces deux peines, tout prestataire de services de confiance qui reprend ou poursuit son activité après suspension ou expiration de l'autorisation.

Art.99.— Est punie d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de deux cent mille (200.000) dinars à un million (1.000.000) dinars, toute personne qui enfreint sciemment l'obligation d'identifier le demandeur de certificat qualifié de signature électronique ou de cachet électronique, conformément aux dispositions de l'article 45 de la présente loi.

Art.100.— Est punie d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de deux cent mille (200.000) dinars à un million (1.000.000) dinars, toute personne qui utilise de fausses déclarations pour bénéficier d'un service de confiance.

Art.101.— Est puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de deux cent mille (200.000) dinars à un million (1.000.000) dinars, tout prestataire de services de confiance qui ne se conforme pas aux dispositions relatives au recueil des données personnelles nécessaires à la fourniture des services de confiance, prévues par l'article 40 tiret 2 de la présente loi.

Art.102.— Est punie d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende d'un million (1.000.000) dinars à cinq million (5.000.000) dinars, toute personne qui détient, divulgue ou utilise les données de création de signature électronique ou de cachet électronique d'autrui.

Art.103. — Est punie d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende d'un million (1.000.000) dinars à cinq million (5.000.000) dinars, toute personne chargée de l'audit qui révèle sciemment des informations confidentielles dont elle a eu connaissance lors de l'audit à des personnes non-autorisées.

Art.104.— Est punie d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende d'un million (1.000.000) dinars à cinq million (5.000.000) dinars, toute personne qui fournit au public des services de confiance sans autorisation ou tout prestataire de services de confiance qui poursuit son activité après retrait de l'autorisation. Les équipements ayant servi à commettre l'infraction font l'objet de confiscation conformément à la législation en vigueur.

Art.105. — Est punie d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende d'un million (1.000.000) dinars à cinq million (5.000.000) dinars, toute personne qui, volontairement, détruit ou dissimule tout document ou information demandé par l'Autorité conformément aux dispositions de l'article 49 de la présente loi.

Art.106. — En cas de récidive, les peines prévues par la présente loi sont portées au double.

Art.107. — La juridiction compétente peut prononcer, à l'encontre des personnes qui commettent les infractions prévues dans la présente loi, une ou plusieurs des peines complémentaires prévues par le code pénal.

Art.108. — La personne morale est responsable pénalement des infractions citées à la présente loi, conformément aux règles prévues par le code pénal.

TITRE VI

Dispositions transitoires et finales

Art.109. — Les organismes fournissant les services de confiance à la date d'entrée en vigueur de la présente loi, sont tenus de se conformer aux dispositions de la présente loi dans les délais fixés par l'Autorité.

Art.110. — Les certificats électroniques délivrés par les organismes cités à l'article 109 ci-dessus, avant l'entrée en vigueur de la présente loi, restent valables jusqu'à leur expiration dans la limite des délais fixés par l'Autorité.

Art.111. — Les moyens d'identification électronique existants avant la définition des critères et conditions par l'organisme national en charge de la sécurité des systèmes d'information prévus à l'article 74 ci-dessus sont présumés fiables jusqu'à preuve du contraire.

Art.112. — L'Autorité assure l'activité de fourniture des services de confiance dans le domaine économique, jusqu'à la mise en œuvre d'une concurrence effective entre les prestataires de services de confiance.

Art.113. — L'Autorité Nationale de Certification Electronique et l'Autorité Gouvernementale de Certification Electronique continuent d'exercer les missions qui leur sont conférées, en vertu de la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 susvisée et de ses textes d'application, jusqu'à la mise en place effective de l'Autorité.

L'Autorité Economique de Certification Electronique continue d'exercer les missions qui lui sont conférées, en vertu de la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 susvisée et de ses textes d'application et assure la fourniture des services de signature et de certification électroniques jusqu'à la mise en place effective de l'Autorité.

Les biens, droits, obligations, personnel et moyens de toute nature détenus par les autorités dissoutes, seront transférés à l'Autorité selon les modalités qui seront fixées par voie réglementaire.

Art.114. — Les dispositions de la présente loi sont précisées, en tant que de besoin, par voie réglementaire, à l'exclusion des dispositions pénales prévues au Titre V de la présente loi.

Art.115. — Sont abrogées les dispositions de la loi n°15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques.

Toutefois, ses textes d'application demeurent en vigueur jusqu'à la publication des textes d'application de la présente loi.

Art.116. — La présente loi sera publiée au *Journal officiel* de la République algérienne démocratique et populaire.

Fait à Alger, le.....

Abdelmadjid TEBBOUNE