# Décret n° 2022-009 du 02 février 2022 relatif aux échanges électroniques entre les usagers et les autorités administratives et, entre les autorités administratives.

## TITRE I – Définitions

**Article premier** : Les termes employés dans le présent décret s'entendent comme suit :

- « **Autorités administratives** » : les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif et les autres organismes chargés de la gestion d'un service public administratif ;
- « **Autorité de certification** » : l'Autorité dont la création est prévue par l'article 90 de la loi n° 2018-022 du 12 juin 2018 portant sur les transactions électroniques aux fins notamment de délivrer les accréditations requises et de contrôler les prestataires de services de certification ;
- « **Loi** » : Les dispositions législatives pertinentes notamment celles de la loi n° 2018-022 du 12 juin 2018 portant sur les transactions électroniques ;
- « **Système d'Information** » ou « **SI** » : tout ensemble de ressources matérielles et immatérielles d'un système informatique destiné à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives ;
- « **Prestataire de services de confiance** » : toute personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique ;
- « **Produit de sécurité** » : tout dispositif, matériel ou logiciel, mettant en œuvre des fonctions qui contribuent à la sécurité des informations échangées par voie électronique ;
- « **Téléservice** » : tout service permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives.

**Article 2** : Les dispositions du présent décret s'appliquent à toute information, de quelque nature qu'elle soit, prenant la forme d'un échange électronique entre les usagers et les autorités administratives et entre les autorités administratives.

## TITRE II - Dispositions relatives à la signature électronique des actes administratifs et la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives et entre les autorités administratives

**Article 3** : Les actes des autorités administratives peuvent faire l'objet d'une signature électronique. Celle-ci n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du Référentiel Général de Sécurité « RGS » mentionné à l'alinéa un (1) de l'article

4 ci-après, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte.

**Article 4** : Un référentiel général de sécurité fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs. Ces règles sont définies selon des niveaux de sécurité prévus par le référentiel pour des fonctions de sécurité, telles que l'identification, la signature électronique, la confidentialité ou l'horodatage, qui permettent de répondre aux objectifs de sécurité mentionnés à l'alinéa précédent.

La conformité d'un produit de sécurité et d'un service de confiance à un niveau de sécurité prévu par ce référentiel peut être attestée par une qualification, le cas échéant à un degré donné, régie par le présent décret.

**Article 5** : Le référentiel général de sécurité ainsi que ses mises à jour sont approuvés par arrêté du Premier Ministre.

Le Ministre chargé du numérique élabore ce référentiel et procède à sa mise à jour. Ce référentiel est mis à la disposition du public par voie électronique.

**Article 6** : Dans les conditions fixées par le référentiel général de sécurité mentionné à l'article précédent du présent décret, l'autorité administrative doit, afin de protéger un système d'information :

a) Identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite, eu égard notamment aux conditions d'emploi du système ;

b) Fixer les objectifs de sécurité, notamment en matière de disponibilité et d'intégrité du système, de confidentialité et d'intégrité des informations ainsi que d'identification des utilisateurs du système, pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés ;

c) En déduire les fonctions de sécurité et leur niveau qui permettent d'atteindre ces objectifs et respecter les règles correspondantes du référentiel général de sécurité.

Dans les conditions fixées par le référentiel susmentionné, l'autorité administrative réexamine régulièrement la sécurité du système et des informations en fonction de l'évolution des risques.

**Article 7** : Pour mettre en œuvre dans un système d'information les fonctions de sécurité ainsi déterminées, l'autorité administrative recourt à des produits de sécurité et/ou à des prestataires de services de confiance ayant fait l'objet d'une qualification ou d’une accréditation dans les conditions prévues au présent décret et/ou par la réglementation

applicable aux prestataires de services de confiance, ou à tout autre produit ou prestataire pour lesquels elle s'est assurée de la conformité de leurs fonctions de sécurité au référentiel général de sécurité.

**Article 8** : L'autorité administrative atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité fixés en application de l'article 6 du présent décret.

Dans le cas d'un téléservice, les autorités administratives rendent accessibles cette attestation par tout moyen de communication possible, accessible par tous.

## TITRE III - Qualification et référencement des produits de sécurité

**Article 9** : La demande de qualification d'un produit de sécurité prévue par l'article 4 du présent décret est adressée à la structure compétente désignée par le Ministre chargé du numérique par tout commanditaire, notamment un fabricant ou un fournisseur du produit ou une autorité administrative.

La qualification est obtenue à l'issue d'une évaluation des fonctions de sécurité du produit au regard des règles du référentiel général de sécurité.

**Article 10** : La demande de qualification contient une description du produit et de ses fonctions de sécurité ainsi que les objectifs de sécurité qu'il vise à satisfaire.

La structure compétente désignée par le Ministre chargé du numérique s'assure que le niveau et les objectifs de sécurité sont cohérents avec le besoin de sécurité des autorités administratives. Elle instruit cette demande lorsque l'ensemble des matériels, des logiciels et de la documentation nécessaires pour réaliser l'évaluation sont disponibles et accessibles.

**Article 11** : La structure compétente désignée par le Ministre chargé du numérique délivre la qualification du produit pour l'un des niveaux fixés par le référentiel, attestant ainsi de sa conformité aux exigences fixées par ce dernier.

Cette attestation est assortie, le cas échéant, de conditions et de réserves et précise sa durée de validité. Elle mentionne les objectifs de sécurité que le produit satisfait et, le cas échéant, le degré de qualification obtenu. Tout changement des circonstances dans lesquelles la qualification a été délivrée peut conduire la Structure compétente désignée par le Ministre chargé du numérique à suspendre ou à retirer la qualification, après que le commanditaire a pu faire valoir ses observations.

La structure compétente désignée par le Ministre chargé du numérique, peut demander à des personnalités bénéficiaires et/ou à des utilisateurs du produit de l'assister dans sa décision d'octroi, de suspension ou de retrait de la qualification.

**Article 12** : Le référencement d'un produit de sécurité qualifié est subordonné au respect des prescriptions contenues dans un cahier des charges approuvé, arrêté et publié par la structure compétente désignée par le Ministre chargé du numérique.

Le cahier des charges détermine notamment les conditions dans lesquelles l'interopérabilité des produits de sécurité qualifiés dans les conditions prévues au présent décret est vérifiée ainsi que les tests qui sont réalisés à cette fin.

Le référencement mentionné au premier alinéa est prononcé par arrêté du Premier Ministre.

## TITRE IV - Validation des certificats électroniques utilisés par les autorités administratives et leurs agents

**Article 13** : Les certificats électroniques délivrés aux autorités administratives et à leurs agents dans le cadre d'un système d'information font l'objet d'une validation par la structure compétente désignée par le Ministre chargé du numérique selon la procédure mise en œuvre par cette dernière.

Pour accorder cette validation, la structure compétente désignée par le Ministre chargé du numérique peut prendre en compte l'existence d'une accréditation délivrée par l'Autorité de certification au fournisseur du certificat électronique utilisé par l'autorité administrative concernée, conformément aux compétences qui sont confiées à cette dernière en cette matière par la Loi et les réglementations en vigueur.

**Article 14** : La validation des certificats électroniques d'une autorité administrative ou de ses agents est subordonnée au respect par cette autorité des règles du référentiel général de sécurité relatives à la délivrance de ces certificats. La structure compétente désignée par le Ministre chargé du numérique peut vérifier sur place les conditions de délivrance de ces certificats.

Dans le cas d'un téléservice, les autorités administratives mettent à la disposition de leurs usagers les informations, dont la liste est fixée par arrêté du Premier ministre, relatives à la délivrance et à la validation de leurs certificats électroniques.

**Article 15** : Les autorités administratives doivent obtenir la validation de leurs certificats électroniques et de ceux de leurs agents au plus tard dans le délai de deux ans à compter de la publication du présent décret.

**Article 16** : Les produits de sécurité et les prestataires de services de confiance qualifiés à un certain niveau de sécurité dans les conditions prévues à l'article 9 du présent décret peuvent faire en outre l'objet d'un référencement par l'Etat. Ils sont alors utilisables par les usagers pour l'ensemble des téléservices pour lesquels ce niveau de sécurité est requis.

Les agents des autorités administratives chargés du traitement et de l'exploitation des informations recueillies dans le cadre de systèmes d'information utilisent, pour accéder à ces systèmes, des produits de sécurité référencés.

**Article 17** : La Banque Centrale de Mauritanie (BCM) et l'Agence Nationale du Registre des Populations et des Titres Sécurisés (ANRPTS), chacune dans le cadre des missions que leur attribue la loi, sont autorisées à créer, valider ou qualifier des certificats et des signatures électroniques et/ou accréditer et autoriser des prestataires fournissant ces services. Le cas échéant, ces services sont soumis à la réglementation spécifique qui leur est propre.

La BCM et l'ANRPTS sollicitent l'avis de l'Autorité de certification aux fins d'aligner leurs pratiques sur les meilleures pratiques internationales et de prévenir tout conflit de compétence.

## TITRE V : Dispositions relatives à l'interopérabilité des téléservices offerts par voie électronique

**Article 18** : Un Référentiel Général d'Interopérabilité « RGI » fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives.

**Article 19** : Le Ministre chargé du numérique est responsable de la conception et de l'adaptation du Référentiel Général d'Interopérabilité mentionné à l'article précédent.

Pour ce faire, il est assisté d'un comité du Référentiel Général d'Interopérabilité qu'il préside lui ou son représentant.

Ce comité peut délibérer sur tout sujet de nature à favoriser l'interopérabilité.

Il est consulté sur le projet de Référentiel Général d'Interopérabilité et sur ses évolutions.

**Article 20** : Les membres du comité de Référentiel Général d'Interopérabilité reçoivent les commentaires sur les propositions d'évolutions du Référentiel Général d'Interopérabilité des autorités administratives. Ils y répondent dans un délai raisonnable qui ne saurait dépasser trois (3) mois.

**Article 21** : Le comité du Référentiel Général d'Interopérabilité se réunit au moins une fois par an.

Le président établit l'ordre du jour. Une question doit y figurer si un tiers au moins des membres du comité en font la demande.

Le comité du Référentiel Général d'Interopérabilité est composé de :

- Un représentant de chacun des ministères du gouvernement mauritanien ;

- Six personnalités qualifiées choisies pour leur compétence et leur expérience dans le domaine de l'administration électronique et des technologies de l'information et de la communication, désignées par le Ministre chargé du numérique ;
- Le Responsable de la structure compétente désigné par le Ministre chargé du numérique.

**Article 22** : Le Référentiel Général d'Interopérabilité est approuvé par arrêté du Premier ministre.

**Article 23** : Le Référentiel Général d'Interopérabilité est mis à la disposition du public par voie électronique

## TITRE VI : Dispositions finales

**Article 24** : Les systèmes d'information des autorités administratives existant à la date de publication du référentiel général de sécurité mentionné à l'alinéa un (1) de l'article 4 du présent décret sont mis en conformité avec celui-ci dans un délai de trois ans à compter de cette date. Les applications créées dans les six mois suivant la date de publication du référentiel sont mises en conformité avec celui-ci au plus tard douze mois après cette date.

**Article 25** : Les systèmes d'informations traitant d'informations relevant du secret de la défense nationale n'entrent pas dans le champ d'application du présent décret.

**Article 26** : Les Ministres sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République Islamique de Mauritanie.