AECK/ICG

REPUBLIQUE DU BENIN

Fraternité-Justice-Travail

PRESIDENCE DE LA REPUBLIQUE

DÉCRET N° 2025 – 366 DU 02 JUILLET 2025

portant modalités de déclaration, d'autorisation et d'agrément des moyens et services de cryptologie ainsi que les modalités des règlements transactionnels.

LE PRÉSIDENT DE LA RÉPUBLIQUE,

CHEF DE L'ÉTAT,

CHEF DU GOUVERNEMENT,

Vu la loi n° 90-32 du 11 décembre 1990 portant Constitution de la République du Bénin, telle que modifiée par la loi n° 2019-40 du 07 novembre 2019 ;

vu la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, telle que modifiée par la loi n° 2020-35 du 06 janvier 2021 ;

vu la décision portant proclamation, le 21 avril 2021 par la Cour constitutionnelle, des résultats définitifs de l'élection présidentielle du 11 avril 2021 ;

vu le décret n° 2025-327 du 26 juin 2025 portant composition du Gouvernement ;

vu le décret n° 2021-401 du 28 juillet 2021 fixant la structure-type des ministères, tel que modifié par le décret n° 2022-476 du 03 août 2022 ;

vu le décret n° 2021-308 du 09 juin 2021 portant attributions, organisation et fonctionnement du Ministère du Numérique et de la Digitalisation ;

sur proposition du Ministre du Numérique et de la Digitalisation,

le Conseil des Ministres entendu en sa séance du 02 juillet 2025,

DÉCRÈTE

CHAPITRE PREMIER : DISPOSITIONS GÉNÉRALES

Article premier : Objet

En application des dispositions de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, telle que modifiée par la loi n° 2020-35 du 06 janvier 2021, le présent décret fixe les modalités :

- de déclaration des moyens de cryptologie fournis, importés et exportés ;
- d'autorisation des moyens de cryptologie ;
- de délivrance de l'agrément pour la fourniture de services de cryptologie ;
- de règlement transactionnel liés aux infractions.

Les dispositions du présent décret ne s'appliquent pas aux moyens de cryptologie utilisés par les missions diplomatiques et consulaires visées par la Convention de Vienne sur les relations diplomatiques de 1961 ainsi qu'à ceux relatifs à la sécurité intérieure et extérieure de l'État de la République du Bénin.

Article 2 : Frais d'étude de dossier

L'autorisation, l'agrément et l'étude de la déclaration des moyens et services de cryptologie sont assujettis au paiement de frais d'étude de dossier.

Lesdits frais sont fixés par arrêté conjoint des ministres chargés des Communications électroniques et des Finances.

CHAPITRE II : MODALITÉS DE DÉCLARATION DES MOYENS ET SERVICES DE CRYPTOLOGIE FOURNIS, IMPORTÉS ET EXPORTÉS

Section première : Importation des moyens de cryptologie

Article 3 : Déclaration préalable

À l'exception des moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité visés à l'annexe 1 du présent décret, la fourniture ou l'importation de tout moyen de cryptologie requiert une déclaration préalable auprès de la commission Cryptologie de la structure en charge de la sécurité des systèmes d'information.

Article 4 : Procédure

L'importation de tout moyen de cryptologie non mentionné à l'annexe 1 du présent décret, fait l'objet, au moins un (01) mois avant la date d'arrivée du moyen sur le territoire national, d'une déclaration par voie électronique ou par envoi recommandé avec demande d'avis de réception du dossier à la commission Cryptologie.

La commission en délivre récépissé revêtu du numéro d'enregistrement du dossier.

Les éléments composant le dossier de la déclaration préalable sont fixés par décision de la commission Cryptologie.

Article 5 : Traitement de la déclaration préalable

La commission Cryptologie dispose d'un délai d'un (01) mois pour délivrer un récépissé à compter de la réception du dossier. Ce délai peut être étendu d'un (01) mois additionnel par notification de la commission. Au bout du deuxième mois sans

récépissé, le silence de la commission Cryptologie vaut approbation. Ainsi, le déclarant peut procéder librement aux opérations faisant l'objet de la déclaration.

Lorsque le dossier est incomplet, la commission Cryptologie invite le déclarant, par voie électronique ou par lettre recommandée avec demande d'avis de réception, à fournir les pièces complémentaires dans un délai maximum de quinze (15) jours calendaires. Dans ce cas, le délai d'un (01) mois prévu à l'alinéa premier du présent article court à compter de la réception des pièces complémentaires.

Article 6 : Intermédiaires

La déclaration de fourniture d'un moyen de cryptologie effectuée conformément aux dispositions du présent décret vaut déclaration pour les intermédiaires qui assurent, le cas échéant, la diffusion du moyen de cryptologie fourni par le déclarant.

Section 2 : Exportation des moyens de cryptologie

Article 7 : Autorisation préalable

L'exportation de tout moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité visé à l'annexe 1 du présent décret requiert une autorisation de la commission Cryptologie.

Article 8 : Procédure

Un (01) mois avant l'exportation de tout moyen de cryptologie non mentionné à l'annexe 1 du présent décret, l'intéressé adresse par voie électronique ou par envoi recommandé avec demande d'avis de réception, ou dépose contre accusé de dépôt, le dossier de demande d'autorisation préalable auprès de la commission Cryptologie. Cette dernière en délivre une décision.

Article 9 : Forme et contenu du dossier de demande d'autorisation

Les éléments composant le dossier de demande d'autorisation préalable sont fixés par décision de la commission Cryptologie.

Article 10 : Traitement de la demande d'autorisation préalable

La commission Cryptologie notifie sa décision, par voie électronique ou par lettre recommandée avec demande d'avis de réception, dans un délai de deux (02) mois à compter de la date de la délivrance de l'avis de réception ou de l'accusé de dépôt de la demande.

Le dossier est réputé complet si, dans le délai de deux (02) mois suivant la réception de la demande, la commission Cryptologie n'a pas invité, par voie électronique ou par lettre recommandée avec demande d'avis de réception, le demandeur à fournir des pièces complémentaires. Dans ce dernier cas, le délai de deux (02) mois fixé à l'alinéa précédent court à compter de la réception des pièces complétant le dossier.

La commission Cryptologie peut également requérir le demandeur, dans le délai de deux (02) mois mentionné à l'alinéa 2 du présent article, de mettre à sa disposition les caractéristiques techniques ainsi que le code source et, pour une durée qui ne peut excéder quatre (04) mois, deux (02) exemplaires du moyen de cryptologie objet de la demande d'autorisation.

Article 11 : Délivrance de l'autorisation

L'autorisation est délivrée pour une durée de trois ans (03) renouvelable.

L'autorisation tient compte de la nécessité d'assurer la protection des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État conformément aux dispositions législatives et règlementaires en vigueur.

A l'expiration du délai mentionné à l'alinéa premier du présent article, l'organisme autorisé formule une nouvelle demande auprès de la commission Cryptologie.

Article 12 : Retrait de l'autorisation

L'autorisation peut être retirée par la commission Cryptologie :

- en cas de fausse déclaration ou de faux renseignement ;
- lorsque son maintien risque de porter atteinte à la défense nationale ou à la sécurité intérieure ou extérieure de l'État ;
- en cas de non-respect des prescriptions dont est, le cas échéant, assortie l'autorisation ;
- lorsque le titulaire de l'autorisation cesse l'exercice de l'activité pour laquelle a été délivrée l'autorisation ;
- lorsque les conditions auxquelles est subordonnée la délivrance de l'autorisation ne sont plus réunies.

Le retrait ne peut intervenir qu'après que le titulaire de l'autorisation a été mis à même de faire valoir ses observations dans un délai de huit (08) jours.

En cas d'urgence, l'autorisation peut être suspendue immédiatement.

CHAPITRE III : AGRÉMENT DES PRESTATAIRES DE SERVICE DE CRYPTOLOGIE

Section première : Conditions de délivrance

Article 13 : Procédure

Toute personne souhaitant exercer l'activité de prestataire de service de cryptologie sollicite et obtient un agrément délivré par la commission Cryptologie de la structure en charge de la sécurité des systèmes d'information.

Les conditions de délivrance de l'agrément aux prestataires de services de cryptologie ainsi que leurs obligations sont fixées par arrêté du ministre chargé des Communications électroniques.

L'intéressé adresse par voie électronique ou par envoi recommandé avec demande d'avis de réception ou dépose contre accusé de dépôt le dossier de demande d'agrément auprès de la commission Cryptologie.

Cette dernière en délivre récépissé revêtu du numéro d'enregistrement du dossier.

Article 14 : Forme et contenu du dossier de demande d'agrément

La forme et les éléments composant le dossier de demande d'agrément sont fixés par décision de la commission Cryptologie.

Article 15 : Traitement de la demande d'agrément

La commission Cryptologie notifie sa décision, par voie électronique ou par lettre recommandée avec demande d'avis de réception, dans un délai de quatre (04) mois à compter de la délivrance de l'avis de réception ou de l'accusé de dépôt de la demande.

Le dossier est réputé complet si, dans le délai de deux (02) mois suivant la réception de la demande, la commission Cryptologie n'a pas invité, par voie électronique ou par lettre recommandée avec demande d'avis de réception, le demandeur à fournir des pièces complémentaires. En cas de dossier incomplet, le délai de quatre (04) mois fixé à l'alinéa premier du présent article court pour compter de la réception des pièces complétant le dossier.

Article 16 : Motif de refus de l'agrément

L'agrément peut être refusé pour non-respect des dispositions relatives à la cryptologie ou pour des motifs liés aux intérêts de la défense nationale, de la sécurité intérieure ou extérieure de l'État.

Article 17 : Obligations relatives à l'obtention de l'agrément

Tout prestataire agréé notifie sans délai à la commission Cryptologie :

1- tout changement :
- dans la nature juridique de l'organisme agréé ;
- dans la nature ou l'objet des activités de l'organisme agréé ;
- de l'adresse de son établissement ;
- de l'identité ou des qualités juridiques de ses dirigeants ;

2- toute fusion ou toute cession d'actions ou de parts sociales susceptibles d'entraîner un changement du contrôle de l'organisme agréé ;

3- toute cessation totale ou partielle de l'activité de l'organisme agréé.

Article 18 : Renouvellement de l'agrément

A l'expiration du délai mentionné à l'article 17, l'organisme titulaire de l'agrément formule une nouvelle demande auprès de la commission Cryptologie.

Article 19 : Application

Le Ministre du Numérique et de la Digitalisation est chargé de l'application du présent décret.

Article 20 : Dispositions finales

Le présent décret, qui prend effet pour compter de la date de sa signature, abroge toutes dispositions antérieures contraires.

Il sera publié au Journal officiel.

Fait à Cotonou, le 02 juillet 2025

Par le Président de la République,
Chef de l'État, Chef du Gouvernement,

Patrice TALON

Le Garde des Sceaux, Ministre de la Justice et de la Législation,

Yvon DETCHENOU

Le Ministre du Numérique et de la Digitalisation,

Aurelie I. ADAM SOULE ZOUMAROU

Le Ministre de l'Industrie
et du Commerce,

Shadiya Alimatou ASSOUMAN

Le Ministre de l'Intérieur et de la
Sécurité publique,

Alassane SEIDOU

Le Ministre délégué auprès du Président de la République,
chargé de la Défense nationale,

Fortunet Alain NOUATIN

AMPLIATIONS : PR : 6 ; AN : 4 ; CC : 2 ; CS : 2 ; C.COM 2 ; CES : 2 ; HAAC : 2 ; HCJ : 2 ; MND : 2 ; MJL : 2 ; MIC : 2 ; MISP :2 ; MDN : 2 ; AUTRES MINISTERES : 16 ; SGG : 4 ; JORB : 1.

Annexe 1 : Moyens de cryptologie dispensés de déclaration préalable en cas d'importation et d'autorisation préalable en cas d'exportation

Partie 1 : Moyens de cryptologie dispensés de déclaration préalable en cas d'importation

Catégories	MOYENS CONCERNÉS
1	Cartes à microprocesseur personnalisées destinées à des applications pour le grand public : a) lorsque la capacité cryptographique est conçue et limitée pour servir uniquement avec les équipements relevant des catégories 2, 3, 4 et 5 de la présente annexe, ou b) lorsque la capacité cryptographique n'est pas accessible à l'utilisateur et qu'elle est spécialement conçue et limitée pour permettre la protection des données qui y sont stockées.
2	Équipements de réception de radiodiffusion ou de télévision, à destination du grand public, dont la capacité de chiffrement est limitée à la facturation, la gestion ou la programmation, et où le déchiffrement est limité aux fonctions vidéo, audio ou de gestion technique.
3	Équipements spécialement conçus et limités pour servir dans des opérations bancaires ou financières, à destination du grand public, et dont la capacité cryptographique n'est pas accessible à l'utilisateur.
4	Équipements de radiocommunication mobiles, destinés au grand public, dont les seules capacités de chiffrement sont celles mises en œuvre par l'opérateur du réseau pour la protection du canal radio, et qui ne sont pas en mesure de procéder au chiffrement direct entre radio équipements.
5	Équipements téléphoniques sans fil, destinés au grand public, qui ne sont pas capables de procéder au chiffrement direct de téléphone à téléphone et lorsque la portée entre le téléphone et sa station de base n'excède pas 400 mètres conformément aux spécifications du fabricant.
6	Équipements spécialement conçus et limités pour assurer la protection de logiciels ou de données informatiques contre la copie ou l'utilisation illicite et dont la capacité cryptographique n'est pas accessible à l'utilisateur.
7	Équipements autonomes spécialement conçus et limités pour assurer la lecture de données audio-vidéo, sans capacité de chiffrement, et où le déchiffrement est limité aux informations audio, vidéo et de gestion technique.
8	Équipements, dotés de moyens de cryptologie, transportés par : a) une personnalité étrangère sur invitation officielle de l'Etat, ou b) une personne physique et lorsque l'équipement est destiné exclusivement à l'usage de cette personne.
9	Stations de base de radiocommunications cellulaires commerciales civiles, conçues pour assurer le raccordement d'équipements mobiles destinés au grand public, et qui ne permettent pas d'appliquer des capacités de chiffrement direct au trafic de données entre ces équipements mobiles.

10	Équipements, destinés au grand public, permettant d'échanger entre eux des données par radiocommunications, et lorsque les seules capacités cryptographiques de l'équipement sont conçues conformément aux normes de l'*Institute of Electrical and Electronics Engineers* suivantes : IEEE 802.15.1, IEEE 802.15.3, IEEE 802.15.4, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.
11	Moyens de cryptologie spécialement conçus et limités pour administrer, gérer, configurer un système d'information sous réserve qu'ils ne permettent de chiffrer que les seules données nécessaires à l'administration, la gestion ou la configuration du système à l'exclusion de toutes autres données.
12	Moyens de cryptologie destinés exclusivement : a) à l'usage de la personne physique qui procède à son importation ou à son transfert, y compris par voie électronique, ou b) à des fins de développement, de validation ou de démonstration par la personne qui procède à son importation ou à son transfert, y compris par voie électronique.

Partie 2 : Moyens de cryptologie dispensés d'autorisation préalable en cas d'exportation

Catégories	MOYENS CONCERNÉS
1	Moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité et mettant en œuvre : a) soit un algorithme cryptographique symétrique employant une clé de longueur inférieure à 56 bits ; b) soit un algorithme cryptographique asymétrique fondé soit sur la factorisation d'entiers de taille inférieure à 512 bits, soit sur le calcul de logarithme discret dans un groupe multiplicatif d'un corps fini de taille supérieure à 512 bits ou dans un autre type de groupe de taille supérieure à 112 bits.
2	Moyens de cryptologie permettant de générer un code d'étalement de fréquences y compris un code de saut de fréquences ou permettant de générer un code de découpage en canaux, un code de brouillage, ou un code d'identification de réseau, pour des systèmes de modulation ultra-large bande et présentant l'une des caractéristiques suivantes : a) une bande passante inférieure à 500 MHz ; b) une bande passante fractionnelle, définie comme la bande passante pour laquelle la puissance demeure constante à 3 dB, divisée par la fréquence centrale et exprimée en pourcentage, de 20 % ou plus.
3	Moyens de cryptologie relevant des catégories 1 ou 2 de la présente annexe et pour lesquels toutes les conditions ci-après sont remplies : a) sont couramment à la disposition du public en étant vendus directement

	sur stock, sans restriction, à des points de vente au détail, que cette vente soit effectuée en magasin, par correspondance, par transaction électronique ou par téléphone ; b) la fonctionnalité cryptographique ne peut pas être modifiée facilement par l'utilisateur ; c) sont conçus pour être installés par l'utilisateur sans assistance ultérieure importante de la part du fournisseur.

Annexe 2 : Sommes mentionnées à l'article 638 du Code du Numérique

Les chiffres indiqués ci-dessous doivent être validés. Ils correspondent à la somme minimale prévue pour chaque infraction + 50% et la somme maximale prévue pour chaque infraction – 50 %

INFRACTION DANS LE CODE DU NUMERIQUE	MONTANT MINIMUM EN FRANCS CFA	MONTANT MAXIMUM EN FRANCS CFA
Visée à l'article 626	[600 000]	[1 600 000]
Visée à l'article 627, al. 1	[1 200 000]	[4 000 000]
Visée à l'article 627, al. 2	[6 000 000]	[16 000 000]
Visée à l'article 628	[1 200 000]	[16 000 000]
Visée à l'article 629	[1 200 000]	[16 000 000]
Visée à l'article 630	[1 200 000]	[16 000 000]
Visée à l'article 632, al. 1	[1 200 000]	[16 000 000]
Visée à l'article 632, al. 2	[6 000 000]	[16 000 000]