AECK/ICG

REPUBLIQUE DU BENIN

Fraternité-Justice-Travail

PRESIDENCE DE LA REPUBLIQUE

DÉCRET N° 2025 – 364 DU 02 JUILLET 2025

fixant les spécifications techniques, normes et procédures minimales relatives aux niveaux de garantie des schémas d'identification électronique et leur cadre d'interopérabilité.

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 : Définitions

Aux fins du présent décret, on entend par :

métadonnées : données qui servent à caractériser et/ou structurer d'autres données ;

nœud : point de connexion qui fait partie de l'architecture de l'interopérabilité d'identification électronique et participe au processus d'authentification nationale ou transfrontalière des personnes, et qui a la capacité de reconnaître et de traiter ou

d'envoyer des transmissions à d'autres points de connexion en permettant à l'infrastructure d'identification électronique nationale de la République du Bénin de fonctionner en interface avec les infrastructures d'identification électronique nationales d'autres États ;

opérateur de nœud : entité chargée de faire en sorte que les fonctions du nœud en tant que point de connexion soient assurées de manière correcte et fiable.

Article 2 : 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 spécifications techniques, normes et procédures minimales relatives aux niveaux de garantie des schémas d'identification électronique et leur cadre d'interopérabilité.

CHAPITRE II : SPÉCIFICATIONS TECHNIQUES, NORMES ET PROCÉDURES MINIMALES DES NIVEAUX DE GARANTIE DES SCHÉMAS D'IDENTIFICATION ÉLECTRONIQUE

Article 3 : Détermination des niveaux de garantie des moyens d'identification électronique

Les niveaux de garantie faible, substantiel et élevé des moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique sont déterminés par référence aux spécifications techniques, normes et procédures figurant en annexe 1 du présent décret.

Article 4 : Spécifications et procédures à utiliser pour déterminer le niveau de garantie

Les spécifications et procédures figurant en annexe 1 du présent décret doivent être utilisées pour déterminer le niveau de garantie des moyens d'identification électronique à travers la fiabilité et la qualité des éléments suivants :

- inscription des personnes physiques et morales conformément aux dispositions du point 1 de l'annexe 1 du présent décret ;
- gestion des moyens d'identification électronique conformément aux dispositions du point 2 de l'annexe 1 du présent décret ;

- authentification conformément aux dispositions du point 3 de l'annexe 1 du présent décret ;
- gestion et organisation conformément aux dispositions du point 4 de l'annexe 1 du présent décret.

Article 5 : Établissement du niveau de garantie d'un moyen d'identification électronique

Un moyen d'identification électronique délivré dans le cadre d'un schéma d'identification électronique pour correspondre à un niveau de garantie donné, comporte tous les éléments énumérés à l'annexe 1 du présent décret.

Article 6 : Respect des exigences d'un niveau de garantie inférieur

Lorsque les moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique répondent à une exigence énoncée pour un niveau de garantie plus élevé, ils sont réputés respecter l'exigence équivalente de tout niveau de garantie inférieur.

CHAPITRE III : CADRE D'INTEROPÉRABILITE DES SCHÉMAS D'IDENTIFICATION ÉLECTRONIQUE

Article 7 : Exigences techniques et opérationnelles relatives au cadre d'interopérabilité des schémas d'identification électronique

Les exigences techniques et opérationnelles relatives au cadre d'interopérabilité des schémas d'identification électronique incluent notamment :

- le niveau minimal de garantie, tel que décrit à l'annexe 1 du présent décret ;
- les exigences techniques minimales en matière d'interopérabilité, telles que décrites aux articles 9 et 12 du présent décret ;
- l'ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique ou morale, tel que décrit à l'article 15 et à l'annexe 2 du présent décret ;
- les normes de sécurité opérationnelle communes, telles que décrites aux articles 10, 11, 13 et 14 du présent décret ;
- les modalités de règlement des litiges.

Article 8 : Exigences techniques minimales relatives aux niveaux de garantie

Les exigences techniques minimales relatives aux niveaux de garantie sont celles fixées conformément aux articles 4 et 5 du présent décret.

Article 9 : Nœuds

Les nœuds doivent être en mesure de faire la distinction entre les organismes du secteur public et les autres personnes physiques ou morales qui, tous, se fient à une identification électronique ou à un service de confiance par le biais de moyens techniques.

Article 10 : Respect de la vie privée et confidentialité des données

Le respect de la vie privée, la confidentialité des données échangées et le maintien de l'intégrité des données entre les nœuds sont assurés au moyen des meilleures solutions techniques et pratiques conformément aux recommandations internationales.

Sauf aux seules fins des dispositions du troisième alinéa de l'article 13 du présent décret, les nœuds ne peuvent stocker aucune donnée personnelle.

Article 11 : Intégrité et authenticité des données dans le cadre de la communication

L'opérateur de nœud veille à ce que la communication entre les nœuds assure l'intégrité et l'authenticité des données de manière à garantir que toutes les demandes et réponses sont authentiques et n'ont pas fait l'objet de manipulations non autorisées.

Article 12 : Format des messages dans le cadre de la communication

La syntaxe utilisée par les nœuds est celle de formats de message communs fondés sur des normes dont la capacité de fonctionnement dans un environnement opérationnel est prouvée. La syntaxe permet :

- de traiter convenablement l'ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique ou morale ;
- de traiter convenablement le niveau de garantie du moyen d'identification électronique ;
- d'établir la distinction entre les organismes du secteur public et les autres parties utilisatrices ;

- de disposer de la flexibilité nécessaire pour répondre aux besoins d'attributs supplémentaires relatifs à l'identification.

Article 13 : Gestion des informations de sécurité et des métadonnées

L'opérateur de nœud communique les métadonnées relatives à la gestion de nœud sous un format normalisé traitable par machine, d'une façon sûre et digne de confiance.

Les paramètres relatifs à la sécurité, au moins, doivent être susceptibles d'être récupérés automatiquement.

L'opérateur de nœud stocke les données qui, en cas d'incident, permettent de reconstruire la séquence de l'échange de messages pour déterminer le lieu et la nature de l'incident. Les données sont stockées pendant une durée d'un (01) an et comportent, au minimum, les éléments suivants :

- identification du nœud ;
- identification du message ;
- date et heure du message.

Article 14 : Normes d'assurance et de sécurité de l'information

Les opérateurs de nœuds assurant une authentification apportent la preuve que, eu égard aux nœuds participant au cadre d'interopérabilité, le nœud respecte les exigences de la norme ISO/CEI 27001 par certification, ou par des méthodes d'évaluation équivalentes ou par conformité aux lois et règlements en vigueur.

Les opérateurs de nœud déploient les mises à jour de sécurité critiques sans retard injustifié.

Article 15 : Données d'identification personnelle

Lorsqu'un ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique ou morale est utilisé dans un contexte national ou transfrontalier, il respecte les exigences visées à l'annexe 2 du présent décret.

Lorsqu'un ensemble minimal de données pour une personne physique représentant une personne morale est utilisé dans un contexte national ou transfrontalier, il contient la combinaison des attributs énumérés à l'annexe 2 du présent décret.

Les données sont transmises sur la base des caractères d'origine et, le cas échéant, également transcrites en caractères latins.

Article 16 : Spécifications techniques additionnelles

Lorsqu'il est justifié par le processus de mise en œuvre du cadre d'interopérabilité, l'organe de contrôle des prestataires de service de confiance numérique peut collaborer avec les autorités compétentes d'autres États pour élaborer des spécifications techniques apportant des précisions sur les exigences techniques visées par le présent décret.

CHAPITRE IV : DISPOSITIONS DIVERSES ET FINALES

Article 17 : Responsables

La structure en charge de la sécurité des systèmes d'information et celle en charge de l'identification des personnes sont responsables de la délivrance des moyens d'identification électronique en République du Bénin. Elles peuvent déléguer leur compétence.

Article 18 : Application

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

Article 19 : 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 Ministre de l'Intérieur et de la Sécurité publique,

Alassane SEIDOU

Le Ministre du Numérique et de la Digitalisation,

Aurelie I. ADAM SOULE ZOUMAROU

AMPLIATIONS : PR : 6 ; AN : 4 ; CC : 2 ; CS : 2 ; C.COM 2 ; CES : 2 ; HAAC : 2 ; HCJ : 2 ; MND : 2 ; MISP : 2 ; AUTRES MINISTERES : 19 ; SGG : 4 ; JORB : 1.

1. ANNEXE

SPECIFICATIONS TECHNIQUES, NORMES ET PROCEDURES POUR LES NIVEAUX DE GARANTIE FAIBLE, SUBSTANTIEL ET ELEVE DES MOYENS D'IDENTIFICATION ELECTRONIQUE DELIVRES DANS LE CADRE D'UN SCHEMA D'IDENTIFICATION ELECTRONIQUE PREVU PAR L'ARTICLE 278 DU CODE DU NUMERIQUE

Définitions applicables

Aux fins de la présente annexe, on entend par :

source faisant autorité : toute source, quelle que soit sa forme, à laquelle on peut se fier pour obtenir des données, des informations et/ou des éléments d'identification exacts pouvant être utilisés pour prouver l'identité ;

facteur d'authentification : facteur confirmé comme étant lié à une personne, qui relève de l'une des catégories suivantes :

- « facteur d'authentification basé sur la possession », un facteur d'authentification dont il revient au sujet de démontrer la possession ;
- « facteur d'authentification basé sur la connaissance », un facteur d'authentification dont il revient au sujet de démontrer la connaissance ;
- « facteur d'authentification inhérent », un facteur d'authentification qui est basé sur un attribut physique d'une personne physique, et dont il revient au sujet de démontrer qu'il possède cet attribut physique ;

Authentification dynamique : processus électronique utilisant la cryptographie ou d'autres techniques pour fournir un moyen permettant de créer sur demande une preuve électronique attestant que le sujet contrôle ou possède les données d'identification et qui

	change avec chaque authentification entre le sujet et le système vérifiant l'identité du sujet ;
système de gestion de la sécurité de l'information :	ensemble de processus et de procédures visant à gérer les risques associés à la sécurité de l'information pour les maintenir à des niveaux acceptables.

Spécifications techniques et procédures

Les éléments des spécifications techniques et des procédures décrits dans la présente annexe servent à déterminer de quelle façon les exigences et les critères de l'article 278 du code numérique sont appliqués aux moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique.

1. *Spécifications, normes et procédures minimales*

N°	Etapes de fabrication, utilisation ou autres usages du moyen d'identification électronique		Niveau de garantie		
			Faible	Substantiel	Elevé
	Inscription	1.1 Demande et enregistrement	a) S'assurer que le demandeur est informé des conditions associées à l'utilisation du moyen d'identification électronique. b) S'assurer que le demandeur est informé des précautions de sécurité recommandées relatives au moyen d'identification électronique. c) Recueillir les données d'identité pertinentes requises pour la preuve et la vérification d'identité.	Identique au niveau faible.	Identique au niveau faible.

1		1.2 Preuve et vérification d'identité (pour une personne physique)	a) La personne peut être présumée en possession d'un élément d'identification reconnu par l'État et représentant l'identité alléguée. b) L'élément d'identification peut être présumé authentique ou on peut présumer qu'il existe selon une source faisant autorité et cet élément semble être valide. c) L'existence de l'identité alléguée est connue d'une source faisant autorité et on peut présumer que la personne est bien celle qu'elle prétend être.	Niveau faible, plus l'une des options énumérées aux points (a) à (d) ci-après : (a) il a été vérifié que la personne est en possession d'un élément d'identification reconnu par l'État et représentant l'identité alléguée et l'élément d'identification fait l'objet d'une vérification visant à déterminer son authenticité ou l'existence de cet élément est connue d'une source faisant autorité et il se rapporte à une personne réelle et des mesures ont été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de l'élément d'identification ; Ou (b) une pièce d'identité est présentée au cours d'un processus d'enregistrement sur le territoire national et la pièce d'identité semble se rapporter à la personne qui la présente et des mesures ont été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de	Les exigences du point 1 ou 2 ci-dessous doivent être respectées : 1. Niveau substantiel, plus l'une des options énumérées aux points a) à c) ci-dessous : a) Lorsqu'il a été vérifié que la personne est en possession d'un élément d'identification biométrique ou photographique reconnu par l'État et que cet élément correspond à l'identité alléguée, l'élément fait l'objet d'une vérification visant à déterminer sa validité selon une source faisant autorité et le demandeur est identifié comme ayant l'identité alléguée par comparaison d'une ou de plusieurs caractéristiques physiques de la personne auprès d'une source faisant autorité ; ou b) lorsque les procédures précédemment utilisées par une entité publique ou privée sur le territoire nationale dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée au point 2.1.2 pour le niveau de garantie élevé, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que ladite garantie équivalente soit confirmée par l'Organe de contrôle des prestataires de service de confiance numérique et que des mesures soient prises pour prouver que les résultats des procédures antérieures demeurent valides ; ou c) lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique prévu à

				perte, de vol, de suspension, de révocation ou d'expiration de la pièce d'identité Ou (c) lorsque les procédures précédemment utilisées par une entité publique ou privée sur le territoire national dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle énoncée au point 2.1.2 pour le niveau de garantie substantiel, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que ladite garantie équivalente soit confirmée par l'Organe de contrôle des prestataires de service de confiance numérique ; ou (d) lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique prévu par l'article 278 valide ayant le niveau de garantie élevé ou substantiel et tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Le niveau de garantie élevé ou substantiel doit être confirmé par l'Organe de contrôle des prestataires de service de confiance numérique.	l'article 278 valide ayant le niveau de garantie élevé, et en tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Le niveau de garantie élevé doit être confirmé par l'Organe de contrôle des prestataires de service de confiance numérique et des mesures doivent être prises pour prouver que les résultats de cette précédente procédure de délivrance d'un moyen d'identification électronique demeurent valides ; ou lorsque le demandeur ne présente pas d'élément d'identification biométrique ou photographique reconnu, les mêmes procédures que celles utilisées sur le territoire national afin d'obtenir ledit élément d'identification biométrique ou photographique reconnu sont appliquées.

		1.3 Preuve et vérification d'identité (pour une personne morale)	a) L'identité alléguée de la personne morale est établie sur la base d'éléments d'identification reconnus par l'État. b) L'élément d'identification semble être valide et on peut présumer qu'il est authentique ou qu'il existe selon une source faisant autorité, l'inscription d'une personne morale auprès de la source faisant autorité étant une démarche volontaire et régie par un accord entre la personne morale et la source faisant autorité. c) La personne morale n'est pas connue par une source faisant autorité comme étant dans une situation qui l'empêcherait d'agir en qualité de personne morale.	Niveau faible, plus l'une des options énumérées aux points 1 à 3 ci-après : 1. l'identité alléguée de la personne morale est établie sur la base d'éléments d'identification reconnus par l'État, y compris le nom de la personne morale, sa forme juridique et (le cas échéant) son numéro d'immatriculation et l'élément d'identification est soumis à une vérification visant à déterminer s'il est authentique, ou si son existence est connue d'une source faisant autorité, l'inscription de la personne morale auprès de la source faisant autorité étant requise pour que la personne morale puisse exercer ses activités dans son secteur et des mesures ont été prises pour minimiser le risque que l'identité de la personne morale ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration des documents ; ou 2. lorsque les procédures précédemment utilisées par une entité publique ou privée sur le territoire national dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée au point 2.1.3 pour le niveau de garantie substantiel, l'entité responsable de l'enregistrement n'est	Niveau substantiel, plus l'une des options énumérées aux points 1 à 3 ci-après : 1. l'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État, y compris le nom de la personne morale, sa forme juridique et au moins un identifiant unique représentant la personne morale utilisé sur le territoire national et l'élément d'identification est soumis à une vérification visant à déterminer s'il est valide selon une source faisant autorité ; ou 2. lorsque les procédures précédemment utilisées par une entité publique ou privée sur le territoire national dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle énoncée au point 2.1.3 pour le niveau de garantie élevé, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que ladite garantie équivalente soit confirmée par l'Organe de contrôle des prestataires de service de confiance numérique et que des mesures soient prises pour prouver que les résultats de cette procédure antérieure demeurent valides ; ou 3. lorsque les moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique prévu par l'article 278 valide ayant le niveau de garantie élevé, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Le niveau de garantie élevé doit être confirmé par l'Organe de contrôle des prestataires de service de confiance numérique ; et

6

				pas tenue de répéter ces précédentes procédures sous réserve que ladite garantie équivalente soit confirmée par l'Organe de contrôle des prestataires de service de confiance numérique ; ou 3. lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique prévu par l'article 278 valide ayant le niveau de garantie élevé ou substantiel, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Le niveau de garantie élevé ou substantiel doit être confirmé par l'Organe de contrôle des prestataires de service de confiance numérique.	des mesures sont prises pour prouver que les résultats de cette précédente procédure de délivrance d'un moyen d'identification électronique prévu par l'article 278 demeurent valides.

		1.4 Lien établi entre les moyens d'identification électronique de personnes physiques et morales Le cas échéant, pour établir un lien entre le moyen d'identification électronique d'une personne physique et le moyen d'identification électronique d'une personne morale (« lien établi »), les conditions suivantes s'appliquent : - Il doit être possible de suspendre et/ou de révoquer le lien établi. Le cycle de vie d'un lien établi (par exemple activation, suspension, renouvellement, révocation) doit être géré selon des procédures reconnues au Bénin. - La personne physique dont le moyen d'identification électronique est lié au moyen d'identification électronique de la personne morale peut déléguer l'établissement du lien à une autre personne physique sur la base de procédures reconnues au	a) Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau faible ou supérieur. b) Le lien a été établi sur la base de procédures reconnues au Bénin. c) La personne morale n'est pas connue par une source faisant autorité comme étant dans une situation qui l'empêcherait d'agir au nom de la personne morale.	Point 3 du niveau faible, plus : a) Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau substantiel ou élevé. b) Le lien a été établi sur la base de procédures reconnues au Bénin, qui ont abouti à l'enregistrement du lien établi auprès d'une source faisant autorité. c) Le lien établi a été vérifié sur la base d'informations provenant d'une source faisant autorité	Point 3 du niveau faible et point 2 du niveau substantiel, plus : a) Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau élevé. b) Le lien a été vérifié sur la base d'un identifiant unique représentant la personne morale et utilisé sur le territoire national, et sur la base d'informations représentant de façon unique la personne physique et provenant d'une source faisant autorité.

		Bénin. Toutefois, la personne physique délégante reste responsable. - L'établissement du lien s'effectue comme suit :			
2	Gestion des moyens d'identification électronique	2.1 Caractéristiques et conception des moyens d'identification électronique	a) Le moyen d'identification électronique utilise au moins un facteur d'authentification. b) Le moyen d'identification électronique est conçu pour que l'émetteur prenne des mesures raisonnables afin de vérifier qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.	a) Le moyen d'identification électronique utilise au moins deux facteurs d'authentification de différentes catégories. b) Le moyen d'identification électronique est conçu de sorte qu'on puisse présumer qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.	Niveau substantiel, plus : a) Le moyen d'identification électronique protège contre les doubles emplois et les manipulations ainsi que contre les attaquants à potentiel d'attaque élevé. b) Le moyen d'identification électronique est conçu de sorte que la personne à laquelle il appartient puisse le protéger de façon fiable contre toute utilisation non autorisée.
		2.2 Délivrance, mise à disposition et activation	Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il ne sera reçu que par le destinataire prévu.	Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il sera exclusivement remis en la possession de la personne à laquelle il appartient.	Le processus d'activation vérifie que le moyen d'identification électronique a été remis exclusivement en la possession de la personne à laquelle il appartient.

		2.3 Suspension, révocation et réactivation	a) Il est possible de suspendre et/ou de révoquer un moyen d'identification électronique de manière rapide et efficace. b) Des mesures ont été prises pour prévenir toute suspension, révocation et/ou réactivation non autorisées. c) La réactivation ne pourra avoir lieu que si les exigences de garantie établies avant la suspension ou la révocation sont toujours respectées.	Identique au niveau faible.	Identique au niveau faible.
		2.4 Renouvellement et remplacement	En tenant compte des risques d'une modification des données d'identification personnelles, le renouvellement ou le remplacement doit satisfaire aux mêmes exigences de garantie que la preuve et la vérification d'identité initiales ou reposer sur un moyen d'identification électronique valide ayant un niveau de garantie identique ou supérieur.	Identique au niveau faible.	Niveau faible, plus : Lorsque le renouvellement ou le remplacement est basé sur un moyen d'identification électronique valide, les données d'identité sont vérifiées auprès d'une source faisant autorité.

3	Authentification La présente section met l'accent sur les menaces liées à l'utilisation du mécanisme d'authentification et répertorie les exigences applicables à chaque niveau de garantie. Dans la présente section, les contrôles sont censés être proportionnés aux risques au niveau donné.	3.1 Mécanisme d'authentification Le tableau suivant définit les exigences par niveau de garantie eu égard au mécanisme d'authentification employé par la personne physique ou morale pour utiliser le moyen d'identification électronique destiné à confirmer son identité à une partie utilisatrice.	a) La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité. b) Lorsque des données d'identification personnelle sont mémorisées dans le cadre du mécanisme d'authentification, ces informations sont sécurisées afin d'assurer leur protection contre toute perte ou compromission, y compris une analyse hors ligne. c) Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque de base renforcé puissent nuire aux mécanismes d'authentification.	Niveau faible, plus : a) La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité par une authentification dynamique. b) Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification.	Niveau substantiel, plus : Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque élevé puissent nuire aux mécanismes d'authentification

4	Gestion et organisation Tous les participants fournissant un service lié à l'identification électronique dans un contexte transfrontalier (« **fournisseurs** ») doivent disposer de pratiques de gestion de la sécurité de l'information documentées, de politiques, d'approches de la gestion des risques et d'autres contrôles reconnus afin de garantir aux organes de gouvernance appropriés responsables des schémas d'identification électronique dans les différents États concernés que des pratiques efficaces sont en place. Tous les éléments/exigences figurant au point 2.4 sont censés être proportionnés aux risques au niveau donné.	4.1 Dispositions générales	a) Les fournisseurs fournissant un service opérationnel visé par les articles [•] à [•] [ref aux articles sur les spécifications techniques, normes et procédures] sont une autorité publique ou une personne morale reconnue comme telle par le droit national qui leur est applicable, avec une organisation établie et pleinement opérationnelle à tous les égards pertinents pour la fourniture des services. b) Les fournisseurs respectent toute exigence légale qui leur incombe dans le cadre du fonctionnement et de l'exécution du service, y compris les types d'informations pouvant être recherchés, la façon dont la preuve d'identité est établie, le type d'informations pouvant être conservées et leur durée de conservation. c) Les fournisseurs sont en mesure de démontrer leur capacité à assumer la responsabilité d'éventuels dommages, ainsi que le fait qu'ils disposent de ressources financières suffisantes pour la poursuite de leurs activités et la fourniture des services. d) Les fournisseurs sont responsables de l'exécution de toute tâche sous-traitée à une autre entité, ainsi que du respect de la politique du schéma, comme s'ils s'étaient	Identique au niveau faible.	Identique au niveau faible.

			acquittés eux- mêmes de leur mission. e) Les schémas d'identification électronique non constitués selon le droit national qui leur est applicable doivent mettre en place un plan de cessation d'activités efficace. Ce plan comporte des mesures concernant l'organisation en cas d'arrêt de fourniture du service ou de la reprise de la fourniture par un autre fournisseur, la façon dont les autorités compétentes et les utilisateurs finaux sont informés, ainsi que des détails sur les modalités de protection, conservation et destruction des informations conformément à la politique du schéma.		

		4.2 Avis publiés et information des utilisateurs	a) Il doit exister une définition de service publiée qui inclut toutes les modalités, conditions et frais, y compris les éventuelles limitations de son utilisation. La définition de service doit inclure une politique de confidentialité. b) Il convient de mettre en place des procédures et politiques appropriées permettant de garantir que les utilisateurs du service sont informés de façon fiable et rapide de tout changement apporté à la définition de service et à toute modalité, condition et politique de confidentialité relative au service spécifié. c) Il y a lieu de mettre en place des procédures et politiques appropriées permettant d'apporter des réponses complètes et exactes aux demandes de renseignements.	Identique au niveau faible.	Identique au niveau faible.
		4.3 Gestion de la sécurité de l'information	Il existe un système de gestion de la sécurité de l'information efficace pour la gestion et le contrôle des risques de sécurité de l'information.	Niveau faible, plus : Le système de gestion de la sécurité de l'information adhère à des normes ou principes éprouvés pour la gestion et le contrôle des risques de sécurité de l'information.	Identique au niveau substantiel.

		4.4 Conservation d'informations	a) Enregistrer et conserver les informations pertinentes à l'aide d'un système efficace de gestion des informations, en tenant compte de la législation applicable et des bonnes pratiques en matière de protection et de conservation des données. b) Conserver, autant qu'il est permis par la législation nationale applicable ou par tout autre arrangement administratif national, et protéger les informations pendant aussi longtemps qu'elles sont nécessaires pour auditer et enquêter sur les atteintes à la sécurité, et à des fins de conservation, après quoi les informations doivent être détruites en toute sécurité.	Identique au niveau faible.	Identique au niveau faible.

		4.5 Installations et personnel Le tableau suivant présente les exigences relatives aux installations, au personnel et aux sous-traitants, le cas échéant, qui se chargent des tâches visées par les articles [•] à [•] [ref aux articles sur les spécifications techniques, normes et procédures]. Le respect de chacune des exigences doit être proportionné au niveau de risque associé au niveau de garantie fourni.	a) Il existe des procédures garantissant que le personnel et les sous-traitants sont suffisamment formés, qualifiés et expérimentés eu égard aux compétences nécessaires pour exécuter les tâches qui leur sont confiées. b) Le personnel et les sous-traitants doivent être en nombre suffisant pour faire fonctionner et gérer de manière adéquate le service conformément à ses politiques et procédures. c) Les installations utilisées pour fournir le service sont surveillées en permanence et protégées contre les dommages causés par des événements environnementaux, l'accès non autorisé et d'autres facteurs susceptibles d'avoir une incidence sur la sécurité du service. d) Les installations utilisées pour fournir le service garantissent que l'accès aux zones de conservation ou de traitement d'informations personnelles, cryptographiques ou autres informations sensibles est limité au personnel ou aux sous-traitants autorisés.	Identique au niveau faible.	Identique au niveau faible.

		4.6 Contrôles techniques	a) Il existe des contrôles techniques proportionnés pour gérer les risques menaçant la sécurité des services, en protégeant la confidentialité, l'intégrité et la disponibilité de l'information traitée. b) Les canaux de communication électronique utilisés pour échanger des informations personnelles ou sensibles sont protégés contre les écoutes clandestines, la manipulation et le rejeu. c) L'accès à du matériel cryptographique sensible, si ce dernier est utilisé pour la délivrance de moyens d'identification électronique et l'authentification, est limité aux rôles et aux applications pour lesquels il est strictement nécessaire. Il convient de s'assurer que ce matériel n'est jamais conservé de manière permanente en texte clair. d) Il existe des procédures permettant de garantir que la sécurité est maintenue sur la durée et qu'il est possible de réagir aux changements des niveaux de risque, incidents et atteintes à la sécurité. e) Tous les supports contenant des informations personnelles, cryptographiques ou autres informations sensibles sont stockés, transportés et mis au rebut de façon sécurisée.	Identique au niveau faible, plus : Le matériel cryptographique sensible, s'il est utilisé pour la délivrance de moyens d'identification électronique et l'authentification, est protégé contre toute manipulation non autorisée.	Identique au niveau substantiel.

		4.7 Conformité et audit	Il existe des audits internes périodiques dont le champ couvre tous les aspects relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes.	Il existe des audits internes ou externes indépendants périodiques dont le champ couvre tous les sujets relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes.	a) Il existe des audits externes indépendants périodiques dont le champ couvre tous les sujets relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes. b) Lorsqu'un schéma est directement géré par une personne publique, il est audité conformément à la loi.

ANNEXE 2

EXIGENCES RELATIVES A L'ENSEMBLE MINIMAL DE DONNEES D'IDENTIFICATION PERSONNELLE REPRESENTANT DE MANIERE UNIVOQUE UNE PERSONNE PHYSIQUE OU MORALE VISE A L'ARTICLE [DONNEES D'IDENTIFICATION PERSONNELLE]

(a) Ensemble minimal de données pour une personne physique

(b) L'ensemble minimal de données pour une personne physique doit contenir tous les attributs obligatoires suivants :

e) nom(s) de famille actuel(s) ;

f) prénom(s) actuel(s) ;

g) date de naissance ;

h) un identifiant unique créé par l'État expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontalière et qui soit aussi persistant que possible dans le temps.

(c) L'ensemble minimal de données pour une personne physique peut contenir un ou plusieurs des attributs supplémentaires suivants :

i) prénom(s) et nom(s) de famille à la naissance ;

j) lieu de naissance ;

k) adresse actuelle ;

l) sexe.

Ensemble minimal de données pour une personne morale

(d) L'ensemble minimal de données pour une personne morale doit contenir tous les attributs obligatoires suivants :

m) dénomination légale actuelle ;

n) un identifiant unique créé par l'État expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontalière et qui soit aussi persistant que possible dans le temps.

(e) L'ensemble minimal de données pour une personne morale peut contenir un ou plusieurs des attributs supplémentaires suivants :

o) adresse actuelle ;

p) numéro d'immatriculation TVA et/ou numéro de référence fiscal ;

q) l'identifiant de la personne morale au registre du commerce de son lieu d'immatriculation ;

r) autres numéros d'identification émis par les autorités nationales compétentes.