GLOBAL STANDARDS PROPORTIONALITY (GSP) WORKING GROUP

MODÈLE STRATÉGIQUE POUR L'IDENTITÉ NUMÉRIQUE ET LES PROCÉDURES ÉLECTRONIQUES DE CONNAISSANCE DU CLIENT (E-KYC)

MODÈLE STRATÉGIQUE

TABLE DES MATIÈRES

Cette publication est la version traduite de la publication originale en anglaise: Policy Model for Digital Identity and Electronic Know Your Customer (e-KYC).

CONTEXTE ET HISTORIQUE

Partout dans le monde, les pays ont modernisé leurs infrastructures publiques afin d'améliorer les prestations de services à l'ère du numérique. La mise en place d'un système d'identité numérique (« digital ID ») a constitué une avancée majeure dans de nombreux pays. L'une des principales applications de l'identité numérique sont les procédures électroniques de connaissance du client (« e-KYC »), rendus possibles par le système d'identité numérique. Parmi les avantages obtenus, il peut être citéune efficacité accrue, des réductions de coûts et l'accélération de l'inclusion financière dans de nombreux pays. L'expérience acquise par plusieurs pays membres de l'AFI en témoigne.

À mesure que les pays mettent en place l'infrastructure et un environnement réglementaire et politique robuste pour favoriser la mise en place de l'identité numérique et de l'e-KYC, il est impératif que l'approche reste centrée sur l'utilisateur. Le Groupe de travail de l'AFI sur la proportionnalité des normes mondiales (Global Standards Proportionality Working Group, GSPWG) a répertorié dans le présent Modèle stratégique les bonnes pratiques des pays membres de l'AFI ainsi que d'autres expériences recensées à travers le monde. Le Modèle stratégique prend appui sur la reconnaissance par les membres de l'AFI de l'identité numérique comme un pilier essentiel d'un cadre politique global en matière de technologie financière inclusive, tel qu'inscrit dans l'Accord de Sotchi sur les technologies financières au service de l'inclusion financière approuvé par les membres en 2018.

OBJECTIF

Le Modèle stratégique offre une orientation aux pays qui souhaitent développer ou améliorer leurs systèmes d'identité numérique et les utiliser à des fins d'e-KYC. L'objectif est de leur permettre de construire des systèmes robustes, interopérables, inclusifs et durables et de contribuer ainsi à l'atteinte des objectifs d'inclusion financière et d'intégrité financière inclusive.

PORTÉE ET CHAMP D'APPLICATION

Le Modèle stratégique propose un cadre qui emprunte les approches utilisées par les pays membres de l'AFI pour développer un environnement politique et réglementaire permettant la mise en place de l'identité numérique et de l'e-KYC, concevoir et mettre en place l'infrastructure et les caractéristiques techniques du système et utiliser l'identité numérique à des fins d'e-KYC. L'inclusion financière des femmes et d'autres groupes défavorisés tels que les jeunes, les personnes âgées, les personnes handicapées et les personnes déplacées sont des enjeux récurrents au sein du modèle. Des principes ont été définis en vue de répondre aux besoins spécifiques de ces groupes.

Ces principes mettent en évidence les principaux aspects pratiques et opérationnels à considérer lors du développement d'un système d'identité numérique et de son utilisation dans le cadre de l'e-KYC. Ils sont basés sur les bonnes pratiques et les expériences de pays membres de l'AFI ainsi que de prestataires de services et de partenaires disposant de connaissances techniques en la matière. Si ce Modèle stratégique peut servir de guide autonome, il convient de noter que les technologies, les pratiques sectorielles et les applications évoluent rapidement et que les approches stratégiques doivent pouvoir s'adapter à ces évolutions. Le Modèle stratégique fera l'objet de révisions et de mises à jour régulières afin de prendre en compte ces évolutions.

RECOMMANDATION POUR LE LECTEUR

Les principaux thèmes du Modèle stratégique sont interdépendants. Nous vous invitons à lire le présent document dans son intégralité.

PRINCIPALES NOTIONS ET DÉFINITIONS

ACCÈS AU SYSTÈME D'IDENTITÉ NUMÉRIQUE (CLARIFICATION DE L'AUTHENTIFICATION, E-KYC)

Pour les besoins de ce modèle, l'accès désigne le fait d'être un utilisateur ou un administrateur autorisé du système en mesure d'authentifier l'identité d'une personne sur la base d'un ou plusieurs facteurs, ou d'effectuer une opération d'e-KYC en authentifiant et en visualisant ou en recevant les données utilisateurs requises pour le respect des normes de connaissance du client (KYC).

LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME (LBC/FT)

Ensemble des politiques, lois et règlements visant à maintenir l'intégrité du système financier par le biais de la dissuasion et de la prévention de l'utilisation du système financier à des fins de blanchiment de capitaux, de financement du terrorisme et d'autres activités illicites apparentées.

AUTHENTIFICATION

Ce terme désigne le processus consistant à vérifier si l'identité revendiquée par une personne est bien la sienne, sur la base d'un ou plusieurs facteurs (quelque chose que cette personne possède, qu'elle sait ou qu'elle est) préalablement fournis dans le cadre des informations de KYC.

JUSTIFICATIF D'IDENTITÉ

Désigne tout document, objet ou structure de données permettant de confirmer numériquement l'identité d'une personne par une méthode d'authentification au sein d'un système d'identité.[1] Différents types de facteurs peuvent être utilisés comme justificatifs d'identité, tels que les cartes à puce, les données biométriques, les mots de passe, les mots de passe à usage unique (one-time passwords, OTP).

DÉDUPLICATION

Désigne l'élimination des informations dupliquées ou redondantes. Dans le cadre d'un système d'identité numérique, il s'agit du processus de recherche des doublons, généralement par le biais d'un processus de correspondance biométrique, afin de garantir le caractère unique des nouvelles données saisies.

IDENTITÉ NUMÉRIQUE

Désigne tout document d'identité numérisé ou numérique fourni ou délivré par les autorités. Elle peut également inclure des formes d'identité numérique fournies en collaboration avec le secteur privé ou avec d'autres entités autorisées, telles que le Haut Commissariat des Nations unies pour les réfugiés, mais qui sont liées à l'identité « officielle » ou « légale » d'une personne et reconnues officiellement par le gouvernement.[2]

SYSTÈME D'IDENTITÉ NUMÉRIQUE

Système permettant de conduire le processus de vérification de l'identité, d'enrôlement et d'authentification. La vérification de l'identité et l'enrôlement peuvent être effectués au moyen de documents numériques ou physiques, ou d'une combinaison des deux. Cependant, la liaison des données, l'accréditation, l'authentification et la portabilité ou la fédération des données doivent être numériques.[3]

PROCÉDURE ÉLECTRONIQUE DE CONNAISSANCE DU CLIENT (E-KYC)

Procédure électronique de vérification de l'identité d'un client conformément aux processus de connaissance du client définis par un pays suivant une approche fondée sur les risques. Par exemple, cela peut inclure un système d'identification biométrique et/ou vidéo, comme le recommande le Groupe d'action financière (GAFI) dans ses lignes directrices sur l'identité numérique (2020).

GROUPE D'ACTION FINANCIÈRE

Le GAFI est un organisme intergouvernemental de normalisation chargé de définir et de promouvoir des normes internationales pour lutter contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive.

IDENTITÉ DE BASE

Les pièces d'identité de base sont des pièces d'identité à usages multiples, telles qu'une carte d'identité nationale ou un extrait d'état civil, qui permettent l'identification de la population en général.

IDENTITÉ FONCTIONNELLE

Les pièces d'identité fonctionnelles permettent l'identification, l'authentification et l'autorisation pour des secteurs ou des cas d'utilisation spécifiques, tels que le vote, la fiscalité ou la protection sociale.[4]

---

1 Banque mondiale, 2019. ID4D Practitioner' Guide: Version 1.0 (octobre 2019). Washington : Banque mondiale. Disponible (en anglais) à l'adresse : http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

2 Ibid.

3 GAFI (2020), Guidance on Digital ID (Lignes directrices sur l'identité numérique), GAFI, Paris. Disponible (en anglais) à l'adresse : http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

4 Banque mondiale, 2019. ID4D Practitioner's Guide: Version 1.0 (octobre 2019). Disponible (en anglais) à l'adresse : http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

VÉRIFICATION/PREUVE D'IDENTITÉ

Processus permettant d'établir ou de confirmer l'identité d'une personne en recueillant et en vérifiant les informations d'identité pertinentes.

INTÉGRITÉ FINANCIÈRE INCLUSIVE

Ce terme désigne un alignement réussi des objectifs de la politique d'inclusion financière avec ceux de la LBC/FT ou de l'intégrité financière. Elle est obtenue principalement lorsqu'un pays applique les normes mondiales d'intégrité financière et élargit l'accès et l'utilisation de services financiers formels de qualité. Une vision nationale claire, une coordination efficace des parties prenantes publiques et privées, et l'intégration des processus de LBC/FT et d'inclusion financière au niveau national sont des facteurs clés pour atteindre l'intégrité financière inclusive.

PRINCIPE DE PROPORTIONNALITÉ

Aux fins du Modèle stratégique, le principe de proportionnalité préconise que les pays collectent les données adéquates et pertinentes pour assurer le fonctionnement optimal du système d'identité numérique. Aucune information non nécessaire ne devrait être collectée.

DONNÉES SENSIBLES

Ces données sont constituées d'informations biographiques dont la collecte est particulièrement sensible car ces informations pourraient servir à établir un profil, à discriminer une personne ou à mettre gravement en danger sa sécurité. Les informations biographiques ne doivent donc pas être rendues facilement accessibles à des tiers ou placées dans le domaine public. Elles comprennent, entre autres, les données sur l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses, l'orientation sexuelle, etc.[5]

UTILISATEUR

Désigne la personne qui est enrôlée dans le système d'identité numérique et qui fournit les informations d'identité requises pour les différentes applications.

5 Ibid.

Ce modèle de politique a été développé autour

TROIS CONSIDÉRATIONS POLITIQUES:

1

CADRE POLITIQUE ET RÉGLEMENTAIRE POUR LA MISE EN PLACE DE L'IDENTITÉ NUMÉRIQUE ET DE L'E-KYC

Voir la page 6

2

POLITIQUE RELATIVE À LA CONCEPTION DE LA PLATEFORME ET À LA CONSTRUCTION DU SYSTÈME D'IDENTITÉ NUMÉRIQUE ET DE L'INFRASTRUCTURE TECHNOLOGIQUE

Voir la page 14

3

APPROCHES STRATÉGIQUES POUR LA MISE EN PLACE DE PROCESSUS CLÉS ET D'APPLICATIONS METTANT À PROFIT L'IDENTITÉ NUMÉRIQUE À DES FINS D'E-KYC

Voir la page 19

PARTIE I. CADRE POLITIQUE ET RÉGLEMENTAIRE POUR LA MISE EN PLACE DE L'IDENTITÉ NUMÉRIQUE ET DE L'E-KYC

Dans cette partie, nous détaillons le cadre permettant de créer un environnement réglementaire favorable à l'utilisation la plus efficace possible de l'identité numérique et des procédures d'e-KYC. La législation générale sur la protection des données et la gouvernance est également présentée en détail, ainsi que les stratégies d'inclusion financière et les considérations liées au genre.

I. LOIS ET RÈGLEMENTS SUR L'IDENTITÉ NUMÉRIQUE ET L'E-KYC

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
LOIS, RÈGLEMENTS ET POLITIQUES RELATIFS À L'IDENTITÉ NUMÉRIQUE ET À L'E-KYC	Adopter des lois fondamentales spécifiques dans le pays pour régir les aspects clés suivants : **a.** Mesures de LBC/FT et procédures de KYC à plusieurs niveaux et fondées sur les risques **b.** Documents d'identité et identité numérique[6] **c.** Protection et confidentialité des données **d.** Cybersécurité Textes complémentaires aux lois fondamentales ou intégrés à celles-ci : **e.** e-KYC Il n'est pas nécessaire d'adopter des lois spécifiques dans le pays pour régir l'identité numérique et l'e-KYC. Il suffit de les inclure dans le cadre réglementaire.	Assurer la clarté dans l'application de la loi, du règlement ou de la directive concernant l'utilisation et la gestion de l'identité numérique et de ses diverses applications. Cela favorise ce qui suit : > Une plus grande conformité et une prise de décision éclairée pour les parties prenantes > Une réduction des risques d'atteinte à la vie privée et de fraude > Des avantages sociaux et économiques pour le secteur public et le secteur privé
CONTENU ET PORTÉE DES LOIS, RÈGLEMENTS ET POLITIQUES	Les lois, règlements et directives doivent être rédigés avant la mise en œuvre d'un programme national sur l'identité numérique ou l'e-KYC, afin de favoriser l'instauration d'un environnement favorable au sein d'un cadre légal et réglementaire. Les principaux aspects devant être couverts par le cadre réglementaire d'un pays peuvent inclure :[7] **a.** L'objectif et le champ d'utilisation de l'identité numérique, y compris les applications de l'identité numérique, telles que l'e-KYC **b.** Les données à collecter et les justificatifs d'identité à délivrer **c.** Le contexte et les enjeux **d.** La validité et le processus de renouvellement **e.** Les modalités détaillées et les restrictions relatives au traitement des données	Des politiques et des cadres favorables détaillant l'utilisation et la portée des documents d'identité numérique permettront aux parties prenantes de prendre des mesures concrètes pour élargir le spectre autour de l'identité numérique, telles que la gouvernance, les politiques, les opérations, les technologies, le cadre juridique, etc. La définition précise des données devant être collectées garantira la protection des consommateurs et atténuera les arbitrages réglementaires.

6 Les systèmes d'identité numérique sont ceux qui font appel à la technologie numérique tout au long du cycle de vie de l'identité, notamment pour la saisie, la validation, le stockage et le transfert des données ; la gestion des justificatifs d'identité ; et la vérification et l'authentification de l'identité. Voir Banque mondiale, 2019. ID4D Practitioner's Guide: Version 1.0 (octobre 2019). Disponible (en anglais) à l'adresse : http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

7 La présente liste n'est pas exhaustive. D'autres éléments peuvent être ajoutés en fonction du contexte et des priorités du pays concerné.

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
CONTENU ET PORTÉE DES LOIS, RÈGLEMENTS ET POLITIQUES *a continué*	**f.** Les modalités détaillées du mécanisme/de l'architecture de consentement, y compris les modalités de révocation du consentement **g.** Les restrictions relatives au partage des informations, y compris concernant l'accès et les autorisations à des tiers **h.** L'intégration des données et l'interopérabilité **i.** Les modalités détaillées de stockage et de gestion des données, y compris les plans de reprise après sinistre et de continuité des activités **j.** La sécurité et la confidentialité des informations **k.** La gouvernance et les structures institutionnelles régissant l'identité numérique et l'e-KYC **l.** Les rôles, les responsabilités et l'obligation de reddition de comptes des entités compétentes et des utilisateurs/participants **m.** Les infractions et les sanctions **n.** Les mécanismes de règlement des plaintes et la procédure d'escalade **o.** Les procédures de mise à jour des informations **p.** Les mesures spéciales en faveur des femmes et des autres groupes défavorisés tels que les jeunes, les personnes âgées et les personnes handicapées, et les amendements spécifiques aux lois existantes visant l'intégration des personnes déplacées **q.** Les audits et les révisions **r.** L'utilisation de la signature numérique Pour favoriser leur efficacité, les lois doivent être adaptables et cohérentes avec les autres lois connexes applicables dans les juridictions concernées.	La formulation de directives claires permet également de favoriser la coopération et la coordination entre les différentes parties prenantes, en les aidant à comprendre ce que l'infrastructure de l'identité numérique autorise, quelles en sont les limites et les avantages, ce qui doit être modifié, les personnes impactées et la manière dont elles le sont.
GLOBAL STANDARD REFERENCES FOR KYC	Consulter et adhérer aux normes du GAFI et aux orientations connexes lors de la[8] formulation des politiques relatives à la LBC/FT, aux procédures de connaissance du client et d'e-KYC[9]. Cela inclut les lignes directrices du GAFI sur l'identité numérique.[10] Inclure des critères de performance et/ou de résultats lors de l'établissement des attributs, justificatifs et processus requis pour établir l'identité officielle au titre du devoir de vigilance à l'égard de la clientèle.	Construire un cadre de KYC robuste avec une portée maximale pour les parties prenantes. Le fait de suivre les recommandations et les lignes directrices du GAFI permet de rester en phase avec les lois et règlements en cours d'élaboration. Toutefois, il est important que les politiques en matière de LBC/FT, de KYC et d'e-KYC soient soigneusement adaptées au contexte unique du pays et aux risques en matière de blanchiment de capitaux et de financement du terrorisme.

8 GAFI. 2012-2021. Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération. Disponible (en anglais) à l'adresse : https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

9 Il n'existe pas de norme internationale en matière d'e-KYC. Toutefois, cette question est abordée dans une certaine mesure dans : GAFI, 2020. Guidance on Digital Identity. Disponible (en anglais) à l'adresse : http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf

10 Ibid.

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
PROCÉDURES DE KYC À PLUSIEURS NIVEAUX ET FONDÉES SUR LES RISQUES	Conduire régulièrement des évaluations des risques au niveau national, sectoriel et institutionnel, qui devraient servir de base à la mise en place d'un système de KYC à plusieurs niveaux fondé sur les risques. Cela permettra de détecter tout problème d'exclusion financière auquel serait confronté une catégorie de la population et qui pourrait justifier la définition d'exigences de KYC adaptées ou spécifiques pour éviter de limiter indûment l'accès à des produits et services à faibles risques. Une approche fondée sur les risques permet de veiller à ce que les exigences de KYC appliquées soient proportionnelles au niveau de risque identifié, notamment en envisageant des exigences allégées lorsque les risques recensés sont plus faibles. La mise en œuvre efficace de l'approche fondée sur les risques en matière de vigilance à l'égard de la clientèle devrait favoriser l'atteinte des objectifs d'inclusion financière. Des évaluations des risques peuvent être effectuées à plusieurs niveaux : > Au niveau du client/du pays/d'une zone géographique > Au niveau des produits/des services/des transactions/des canaux Il convient de prévoir un calendrier pertinent pour procéder à des évaluations des risques ultérieures.	Déterminer le niveau de risque auquel sont exposés les prestataires de services financiers lorsqu'ils s'adressent à différentes catégories de la population. Il s'agit d'une étape importante pour s'assurer que les services et produits financiers soient conçus pour les plus défavorisés et ne les empêchent pas d'y accéder et de les utiliser, ainsi que pour maintenir un niveau de connaissance actualisé des risques de blanchiment de capitaux et de financement du terrorisme dans le pays. L'approche fondée sur les risques garantira que les mesures prises pour prévenir ou limiter le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes restent proportionnelles aux risques identifiés. Il est nécessaire de procéder régulièrement à des évaluations des risques au niveau national, sectoriel ou institutionnel pour garantir l'actualisation des pratiques et la réduction des nouveaux risques.
E-KYC	Élaborer une politique claire et un plan de mise en œuvre précis des procédures d'e-KYC, en s'appuyant sur des pièces d'identité de base, telles que la carte d'identité nationale ou des pièces d'identité fonctionnelles très répandues au sein de la population. Veiller à ce que le système d'e-KYC intègre des pratiques de connaissance du client à plusieurs niveaux fondées sur les risques. *(Voir la partie III pour plus de précisions)*	Selon l'expérience des pays, l'authentification et la vérification de l'identité par le biais des procédures d'e-KYC ont permis aux prestataires de services financiers de réaliser d'importantes économies en termes de temps et de coûts. Elles favorisent également l'inclusion financière des femmes en supprimantcertains obstacles liés au genre (nécessité de se rendre jusqu'aux points de transaction, d'être accompagné par un homme, etc.)
ACCOMPAGNEMENT À LA MISE EN ŒUVRE	Fournir à toutes les parties prenantes concernées des orientations sur l'interprétation des lois et règlements. Cet accompagnement concerne plus particulièrement les institutions financières, y compris, sans s'y limiter, les banques, les compagnies d'assurance, les courtiers, etc. et les intermédiaires. Les orientations doivent être claires et prévoir des étapes précises pour mettre en œuvre les éléments liés à la conformité et à la réglementation des opérations transfrontalières dues à des juridictions étrangères.	Garantir la clarté de la réglementation auprès des institutions financières et comprendre leurs défis les plus urgents en ce qui concerne le respect des réglementations de LBC/FT. Ilfavorisera la mise en place des actions et des mesures d'atténuation nécessaires pour surmonter ces défis.

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
ACCOMPAGNEMENT À LA MISE EN ŒUVRE *a continué*	Les banques centrales et les autorités compétentes devraient suivre l'évolution des normes de LBC/FT au niveau local, régional et mondial, fournir des orientations aux institutions concernées pour que celles-ci respectent à tout moment leurs obligations, documenter et partager les interprétations des recommandations du GAFI et des orientations connexes. Ilpermettra une mise en œuvre efficace et une meilleure compréhension de la part des institutions financières. Proposer des hypothèses, le cas échéant, ainsi qu'un plan de mise en œuvre standardisé afin d'éviter toute difficulté ou divergence potentielle. Apporter un soutien à la mise en œuvre, promouvoir un dialogue ouvert et apporter une réponse aux différents défis pouvant apparaître après la mise en œuvre.	
COLLECTE D'INFORMATIONS PERSONNELLES PERMETTANT L'IDENTIFICATION	Collecter auprès des citoyens le nombre minimum de données nécessaires pour répondre aux exigences de KYC, et informer explicitement les clients de l'utilisation possible des données collectées. Il convient de définir les informations personnelles d'identification qui sont collectées en tenant compte de la portée et de la facilité d'utilisation du système et de déterminer, selon le principe de proportionnalité, quelles sont les informations dont le recueil est obligatoire. Les informations sensibles, si elles sont collectées, doivent être classées selon plusieurs niveaux pour garantir une confidentialité et une sécurité supplémentaires en limitant un accès complet à ces données par des entités tierces.	Respecter la vie privée des utilisateurs et appliquer les principes de proportionnalité en se limitant au recueil des informations strictement nécessaires. Cette démarche permet de : > minimiser les risques d'atteinte à la vie privée des utilisateurs ; > limiter le temps et les coûts nécessaires pour le recueil et la vérification de chacun des types de données collectées ; > réduire les risques de fuite de données sensibles et de surveillance.
VÉRIFICATION DES DONNÉES ET DE L'IDENTITÉ	Vérifier les données collectées en les comparant à des données ou documents indépendants et fiables établis par des entités émettrices, tels que les cartes d'identité nationales. La vérification par comparaison avec d'autres bases de données civiles et l'authentification biométrique sur place sont des méthodes de vérification d'identité couramment utilisées. À titre de mécanisme de traitement des exceptions, envisager des stratégies de vérification communautaire pour les utilisateurs ne possédant aucun document dans les catégories à faible risque.[11]	Se prémunir contre la fraude et l'usurpation d'identité dans la mesure du possible.
COLLECTE DES DONNÉES BIOMÉTRIQUES	Élaborer des politiques claires en matière de collecte, de stockage et d'utilisation des données biométriques. Identifier les données biométriques les plus pertinentes pour le système en cours d'élaboration, en gardant à l'esprit le principe de proportionnalité et d'utilité. Il convient de collecter le niveau minimum de données biométriques permettant d'identifier une personne de manière unique ¬— les empreintes digitales, le visage et l'iris sont les caractéristiques les plus utilisées. La voix peut être envisageable dans les pays où l'utilisation des téléphones à fonctionnalités multiples est élevée. Les méthodes invasives	La collecte de données biométriques est à la fois un moyen d'identification et d'authentification. L'authentification basée sur la correspondance des données biométriques est plus efficace et plus précise. Elle permet également la déduplication des données d'identité.

11 GAFI, 2020. Guidance on Digital Identity, p. 38. Disponible (en anglais) à l'adresse : http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
COLLECTE DES DONNÉES BIOMÉTRIQUES *a continué*	telles que la collecte d'ADN doivent être soumises à un processus intégral de diligence raisonnable et être conformes aux lois existantes sur la protection des données et de la vie privée.	
MISE À JOUR DES DONNÉES BIOMÉTRIQUES	Élaborer des procédures pour la mise à jour des données biométriques susceptibles de changer en raison de l'âge, de la profession, de l'état physique ou de santé de la personne. Rédiger des directives prévoyant une mise à jour obligatoire dans certains cas, comme pour les enfants, les personnes âgées et les personnes handicapées.	Faire en sorte de réduire au minimum les difficultés et les échecs lors de l'authentification et de la vérification biométriques.
MISE À JOUR DES DONNÉES DE L'UTILISATEUR	Rédiger des directives pour procéder à des corrections, des modifications ou des suppressions de données inexactes au sein de l'identité numérique. Ces directives devraient permettre une certaine flexibilité pour que les utilisateurs soient reconnus par le genre auquel ils s'identifient, plutôt que par le genre qui leur a été assigné à la naissance, et autoriser la mise à jour de cette information.	Préserver l'intégrité des données, garantir leur exactitude et s'assurer que les données les plus récentes sont stockées et utilisées.

II. LOIS SUR LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
POLITIQUE DE PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE	Inclure les principaux éléments de la protection des données et de la vie privée dans les directives, les orientations et les lois existantes sur la collecte, le traitement, la gestion et le stockage des données personnelles des individus, telles que : a. Le consentement obligatoire pour le traitement des données personnelles, en examinant la validité d'un consentement général par rapport à un consentement exprimé dans le cadre d'une opération. b. Les cas de figure précis dans lesquels le consentement n'est pas requis, par exemple, en cas de décision judiciaire. c. Les dispositions spéciales applicables aux enfants (collecte d'informations démographiques limitées et de celles pouvant être liées au tuteur légal) et aux groupes défavorisés d. Les principes de protection de la vie privée dès la conception étendus aux dépositaires de données e. La classification des données sensibles f. La suppression des données lorsque le motif qui avait justifié la collecte des données devient caduc g. Les mesures à prendre et les sanctions à appliquer en cas de mauvaise gestion des données, y compris la soumission de données erronées par le personnel.	Il est nécessaire de mettre en place une politique globale de protection des données et de la vie privée pour régir les secteurs public et privé, car il est difficile pour les parties prenantes de se conformer à de multiples lois et règlements sur l'utilisation et la gestion de l'identité numérique.
AUDITS ET ÉVALUATIONS DE LA CONFIDENTIALITÉ	Créer une autorité indépendante pour la protection des données qui sera chargée de veiller à ce que les processus de traitement des données personnelles soient conformes aux dispositions légales et aux directives. Préciser le processus de conduite des examens/évaluations des risques en matière de vie privée pour l'ensemble du système. Les directives doivent préciser les tiers qui sont autorisés à procéder à ces examens/évaluations ainsi que la périodicité à respecter.	Examiner la politique et les procédures relatives à la collecte, à la gestion et au stockage des données. Cela permettra également de contrôler le respect des directives sur la protection des données et de la vie privée, et contribuera à l'identification des risques et à l'élaboration de stratégies d'atténuation.

III. GOUVERNANCE ET STRUCTURES INSTITUTIONNELLES

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
STRUCTURES D'APPLICATION DU DROIT ET DE GOUVERNANCE	Créer une entité indépendante chargée de la planification, de la gestion et de l'administration de l'identité numérique. Cette entité doit avoir le pouvoir de faire appliquer le droit en vigueur et d'attribuer les responsabilités sur la base des dispositions légales et réglementaires. Il convient de créer un conseil composé de représentants issus des principales institutions de réglementation financière, de la cellule de renseignement financier et des ministères impliqués tels que l'informatique, les télécommunications, la justice et la protection sociale, qui sera chargé de superviser les activités de cette entité indépendante. Dans le but d'assurer la coopération, la collaboration et l'harmonisation des parties prenantes dans la mise en place de l'identité numérique, cette entité indépendante devrait aussi avoir une compétence et un mandat de surveillance d'autres entités tierces qui utilisent les données d'identité afin d'éviter toute utilisation abusive de ces données. Renforcer la capacité des acteurs de l'écosystème à mettre en avant les principes de coopération dans le cadre de la mise en place du système d'identité numérique, l'adoption d'une procédure d'e-KYC efficace par les prestataires de services financiers, ainsi que la mise en place d'un contrôle et d'une supervision appropriés. Les partenaires de mise en œuvre doivent aussi faire la promotion de la culture numérique et sensibiliser leurs clients à la nécessité de l'identité numérique, à ses utilisations et avantages, avant son lancement.	Promouvoir l'efficacité, la responsabilisation, la transparence et prévenir l'exclusion et les abus.
PROMOTION DE L'INNOVATION	Encourager les initiatives dans le pays pour favoriser les innovations en matière d'identité numérique. Les bacs à sable réglementaires, les centres d'innovation ou les approches de test et d'apprentissage ont permis de créer un environnement propice aux innovations liées à : a. Des moyens peu coûteux de proposer des services par le biais de canaux axés sur la technologie b. Un enrôlement à distance et une procédure d'e-KYC, en mettant à profit l'identité numérique pour proposer différents services et produits c. Des options alternatives de notation de crédit pour les personnes n'ayant pas de score de crédit formel, en particulier les femmes entrepreneurs d. Des technologies émergentes Envisager la création de bacs à sable régionaux pour élaborer un modèle de travail plus durable grâce à un financement conjoint et au partage des connaissances techniques. Le bac à sable peut faciliter des innovations dans différents secteurs et pour diverses applications. Cet environnement peut être notamment utilisé pour les innovations visant à accélérer l'inclusion financière spécifiquement pour les groupes défavorisés tout en permettant de créer de nouveaux produits et services pour les clients existants.	Les approches visant à promouvoir l'innovation, telles que les bacs à sable réglementaires, les centres d'innovation ou les approches de test et d'apprentissage, permettent de créer un environnement favorable à la surveillance, à la visibilité et au contrôle par les organismes de régulation, tout en permettant l'innovation par le secteur privé autour de solutions efficaces et d'applications intéressantes.

IV. STRATÉGIES D'INCLUSION FINANCIÈRE

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
STRATÉGIES NATIONALES D'INCLUSION FINANCIÈRE	Intégrer clairement le développement de l'identité numérique et de l'e-KYC dans les politiques, stratégies et initiatives nationales visant à accélérer l'inclusion financière, notamment : a. La stratégie nationale d'inclusion financière (SNIF)[12] b. La stratégie nationale d'éducation financière c. Une structure de coordination pour mener les efforts nationaux en matière d'inclusion financière, qui devrait être placée sous la direction de la banque centrale et/ou du ministère des finances, et composée de parties prenantes pertinentes telles que les ministères des finances, de l'informatique, des télécommunications, de la protection sociale, de l'éducation, des femmes, etc. Cette structure peut inclure des groupes de travail consacrés aux différents piliers de la SNIF et comprenant des représentants du secteur privé, de la société civile, des acteurs du développement et des organisations humanitaires. d. Des mesures spécifiques d'enrôlement des populations défavorisées dans le système d'identité numérique,[13] telles que l'enrôlement à domicile, l'acceptation de documents alternatifs et la vérification communautaire, par exemple l'aval d'un intermédiaire ou d'une entité qualifiée comme le HCR. e. La création de produits et services spécifiquement destinés aux groupes défavorisés, y compris les personnes âgées et les personnes handicapées, tels que des produits et services à faibles risques, des assurances à faible coût subventionnées par le gouvernement, des comptes bancaires sans frais de tenue de compte, des crédits à faible taux d'intérêt pour les groupes à faible revenu et les femmes, etc. f. Les initiatives de sensibilisation et d'éducation financière	Veiller à ce que la conception et la mise en place de l'identité numérique et de l'e-KYC contribuent à faire progresser l'inclusion financière d'une manière cohérente, coordonnée et ciblée, afin de garantir un meilleur accès et une meilleure utilisation des services financiers de qualité et abordables, en particulier pour les populations non desservies ou mal desservies.
MISE EN ŒUVRE DE STRATÉGIES NATIONALES D'INCLUSION FINANCIÈRE	S'appuyer sur la structure de coordination nationale pour l'inclusion financière afin de susciter un effort de collaboration pour la mise en œuvre de la SNIF sous la direction d'agences publiques, établies par une loi ou un décret, et en impliquant les parties prenantes du secteur privé et de la société civile. Cette structure veillera à la bonne coordination entre les différents acteurs, à la répartition des responsabilités et à une responsabilisation efficace. La mise en œuvre de la SNIF doit être en phase avec les politiques et stratégies nationales d'éducation financière et de protection des consommateurs. La mise en œuvre peut être accélérée au moyen de projets intégrés, aux objectifs et calendriers clairement définis, pour obtenir des résultats rapides. Les pays dotés de systèmes d'identité numérique peuvent se baser sur ces derniers pour assurer l'efficacité de l'enrôlement et des procédures d'e-KYC.	Garantir l'atteinte des objectifs nationaux d'inclusion financière, notamment en suscitant l'adhésion des différentes parties prenantes et ministères clés, ainsi que la mobilisation des ressources et du budget nécessaires pour mettre en œuvre les politiques et entreprendre les activités définies.

12 Alliance pour l'inclusion financière, 2020. Modèle de stratégie nationale d'inclusion financière. Disponible à l'adresse : https://www.afi-global.org/wp-content/uploads/2020/09/AFI_NFIS_PM_FRENCH_AW2_digital.pdf

13 Les populations défavorisées comprennent les personnes démunies sur le plan économique, les jeunes, les personnes âgées, les personnes handicapées, les personnes déplacées, les minorités raciales et ethniques, les enfants issus de groupes à faible revenu, ainsi que d'autres groupes que le pays pourrait avoir explicitement définis.

V. STRATÉGIES INCLUANT LA DIMENSION DE GENRE

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
PROCESSUS INCLUANT LA DIMENSION DE GENRE	Élaborer une stratégie et procéder à une analyse approfondie des politiques et du système d'identité numérique afin de garantir la prise en compte de la dimension de genre tout au long du cycle de vie[14] du système d'identité numérique. Certains éléments clés concernent des solutions hors ligne et des journées d'enregistrement mobiles ou réservées aux femmes, ainsi que la promotion d'interfaces tenant compte de la dimension de genre. La collaboration et la coopération entre les institutions publiques et privées spécialisées dans la condition de la femme contribueraient à l'élaboration d'une stratégie ciblée incluant la dimension de genre.	Faire en sorte qu'il n'y ait pas d'exclusion dans le système d'identité numérique en raison des obstacles supplémentaires auxquels sont confrontées les femmes.
COLLECTE DE DONNÉES VENTILÉES PAR SEXE ET PAR ÂGE	Promouvoir la collecte, le suivi, l'analyse et le contrôle des données ventilées par sexe et par âge. Déterminer la fréquence et les sources (côté offre et côté demande) de la collecte. Envisager de permettre l'accès et la diffusion des données à d'autres entités publiques auxquelles ces informations pourraient être utiles.	Veiller à ce que les données soient collectées dans l'objectif d'une meilleure prise de décision politique et stratégique.

14 Microsave Consulting, 2021. Working Paper: A Framework for Building Gender-Sensitive Identity Systems. Disponible (en anglais) à l'adresse : https://www.microsave.net/wp-content/uploads/2021/03/Working-paper-A-framework-for-building-gender-sensitive-identity-systems.pdf

PARTIE II. POLITIQUE RELATIVE À LA CONCEPTION DE LA PLATEFORME ET À LA CONSTRUCTION DU SYSTÈME D'IDENTITÉ NUMÉRIQUE ET DE L'INFRASTRUCTURE TECHNOLOGIQUE

Dans cette partie sont détaillés les principes et considérations pour la conception et la construction du système d'identité numérique, l'infrastructure technologique ainsi que l'architecture sous-jacente. Ces principes sont inspirés, entre autres, de ceux de la gestion des données et des services aux utilisateurs, qui constituent également des considérations clés pour le système d'identité numérique.

I. CONCEPTION DU SYSTÈME D'IDENTITÉ NUMÉRIQUE

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
TYPE ET CARACTÉRISTIQUES DE L'IDENTITÉ NUMÉRIQUE	Définir clairement le type de pièce d'identité numérique[15] (de base ou fonctionnelle) en cours de déploiement dans le pays. Cette décision doit se baser sur un examen approfondi des besoins et des objectifs du programme d'identité et faire suite à plusieurs séries de discussions avec toutes les parties prenantes impliquées. Les principaux paramètres à prendre en compte sont les suivants : **a.** La disponibilité d'un système et d'une infrastructure d'identité de base sur lesquels l'identité numérique peut s'appuyer **b.** Son extensibilité et les projets d'application du système d'identité numérique **c.** Les implications en termes de coûts (y compris l'analyse des ressources humaines et de l'infrastructure, la propriété des dispositifs numériques)[16] ainsi que les mesures incitatives telles que les régimes fiscaux favorables et le partage des coûts **d.** Les plans de mise en œuvre et de déploiement auront une incidence sur la nature de la pièce d'identité et sur la décision d'utiliser une pièce d'identité fonctionnelle actuelle et de la convertir en une pièce d'identité de base **e.** Le caractère obligatoire ou facultatif de l'inscription pour certains, et les éventuelles conditions préalables telles que l'âge, la citoyenneté	Optimiser l'utilisation des ressources disponibles, notamment le budget, les ressources humaines, les bases de données existantes et la technologie. Permettre aux secteurs public et privé de mettre en évidence le type de services (santé, finances, sécurité sociale, etc.) auxquels il est possible d'accéder grâce à la pièce d'identité numérique.

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX

15 Les pièces d'identité de base sont des pièces d'identité à usages multiples, telles qu'une carte d'identité nationale ou un extrait d'état civil, qui permettent l'identification de la population en général. Les pièces d'identité fonctionnelles permettent l'identification, l'authentification et l'autorisation pour des secteurs ou des applications spécifiques, tels que le vote, la fiscalité ou la protection sociale. Voir Banque mondiale, 2019. ID4D Practitioner's Guide: Version 1.0 (octobre 2019). Disponible (en anglais) à l'adresse : https://id4d.worldbank.org/guide/types-id-systems.

16 Banque mondiale, 2018. Understanding Cost Drivers of Identification Systems. Disponible (en anglais) à l'adresse : https://documents1.worldbank.org/curated/en/702641544730830097/pdf/Understanding-Cost-Drivers-of-Identification-Systems.pdf

ADOPTION DE NORMES INTERNATIONALES	Prendre connaissance des normes internationales en matière de conception et de déploiement de pièces d'identité et suivre les recommandations relatives à la protection de la vie privée. Certains principes clés peuvent être trouvés dans les textes suivants : a. Banque mondiale : « Principles of Identification » (Principes en matière d'identité numérique) b. ID4D : « Technical Standards for Digital Identification » (Normes techniques relatives à l'identité numérique) c. Respect de la vie privée dès la conception d. « FATF Guidance on Digital Identity Guidelines » (Lignes directrices du GAFI sur l'identité numérique) e. G20 f. ISO g. Good ID h. « International Association of Privacy Professionals » (Association internationale des professionnels de la vie privée) i. Norme ISO 27001:2013 sur la sécurité de l'information D'importantes décisions stratégiques peuvent être prises en se basant sur les expériences, les analyses et les défis recensés par d'autres pays, mais en veillant à ce que le contexte et les exigences du pays soient au cœur de la conception.	Veiller à ce que le développement soit basé sur les bonnes pratiques et les enseignements tirés dans d'autres juridictions et s'assurer que les éléments de conception les plus appropriés sont examinés avec soin.
DÉLIVRANCE DE JUSTIFICATIFS D'IDENTITÉ	Évaluer en fonction du contexte du pays les justificatifs d'identité les plus appropriés pour l'usage de la population en général. Prendre en compte des facteurs tels que la fonction assignée, les préférences des utilisateurs et la sécurité. À titre d'exemple, nous pouvons citer, sans s'y limiter, les justificatifs d'identité suivants : a. Les pièces physiques (cartes) b. Les pièces numériques (cartes électroniques, numéro d'identification) c. Des identifiants supplémentaires (code PIN, mot de passe, mot de passe à usage unique) d. Le code QR Les cartes physiques procurent un sentiment de sécurité ; les cartes à puce permettent de bénéficier de diverses fonctionnalités ; les justificatifs d'identité numériques sont plus avantageux mais peuvent représenter un obstacle supplémentaire pour les utilisateurs n'ayant pas accès à la technologie et vivant dans des zones à faible connectivité. Veiller à ce que les justificatifs d'identité choisis soient inclusifs et n'empêchent pas l'utilisation de l'identité numérique par certains segments de la population. Les pièces d'identité numériques qui nécessitent la possession d'un smartphone ou d'un appareil similaire risquent de désavantager certains segments de la population, comme les femmes dans certains pays qui n'ont peut-être pas accès à un smartphone ou ne peuvent pas l'utiliser. Le fait de délivrer plus d'un justificatif d'identité contribuera à résoudre ces problèmes.	Promouvoir une utilisation égale de l'identité numérique et des services associés, tout en veillant à ce qu'aucun obstacle supplémentaire à l'utilisation ne soit créé pour une quelconque catégorie d'utilisateurs.

II. PROCÉDURES D'ENRÔLEMENT ET D'ENREGISTREMENT

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
EXIGENCES POUR L'ENRÔLEMENT	Publier des directives sur les exigences et le processus d'enrôlement pour les différentes catégories de résidents (citoyen, résident étranger, demandeur d'asile, genre). Fixer des exigences minimales claires et faciles à satisfaire pour l'enrôlement dans la plateforme/ le système d'identité, en fonction des objectifs du système. Veiller à ce que les exigences minimales fixées ne constituent pas un obstacle supplémentaire à l'enrôlement de certaines catégories de personnes dans le système. Tenir compte du contexte du pays et de l'utilisation de l'identité numérique pour décider si l'enrôlement doit être automatique pour tous les citoyens ou si les citoyens doivent formuler une demande explicite. En ce qui concerne les pièces d'identité de base qui sont utilisées dans le cadre de l'e-KYC, l'enrôlement doit couvrir la majeure partie de la population adulte. Les pays disposant de bases de données numériques fiables qui couvrent déjà une certaine partie de la population peuvent adopter une approche d'enrôlement automatique de tous les citoyens. Toutefois, un processus d'enregistrement pourrait être lancé pour la population non encore recensée s'il existe des lacunes dans la couverture des bases de données numériques. Les pays qui préfèrent créer une nouvelle base de données pour éviter d'utiliser une base de données présentant des lacunes peuvent utiliser une approche dans laquelle les citoyens doivent faire une demande explicite.	Faire en sorte que la couverture de l'identité numérique soit large et inclusive et que l'enrôlement soit facile pour tous les citoyens et utilisateurs.
OINTS D'ACCÈS POUR LES UTILISATEURS	Élaborer des directives basées sur les exigences des pays concernant les points d'accès permettant aux utilisateurs d'interagir avec la plateforme d'identité numérique et de mener les procédures d'e-KYC. Ces points d'accès, qui peuvent être utilisés pour l'enrôlement, la vérification, l'authentification et d'autres services, selon les besoins, doivent être dotés d'un système de contrôle robuste pour promouvoir l'intégrité du processus d'enregistrement. Les directives doivent permettre une couverture géographique adéquate et des ajustements pour répondre aux besoins des groupes défavorisés de la population. Les points d'accès peuvent consister en un centre géré par une entité publique, un ensemble autonome de centres d'enregistrement, des guichets gérés par d'autres parties prenantes sous la supervision des pouvoirs publics, ou encore être des points d'accès à distance. Mobiliser les acteurs du secteur privé pour une plus large couverture et une plus grande efficacité. Envisager une collaboration avec des points d'accès numériques pour les services bancaires qui pourraient déjà constituer un réseau établi.	Faire en sorte que les utilisateurs disposent de points d'accès à leur portée pour s'enregistrer et interagir avec le système d'identité numérique, afin de gagner leur confiance et de les inciter à utiliser la pièce d'identité numérique pour diverses applications.
COÛTS DIRECTS POUR L'UTILISATEUR	Publier des directives et les faire appliquer afin que les coûts directs assumés par les citoyens ou les utilisateurs pour être intégrés au système d'identité numérique ou utiliser des services d'e-KYC soient minimes ou nuls. Si les coûts sont minimes pour les utilisateurs, cela les encouragera à utiliser le système. Si des coûts doivent être prélevés, ils doivent l'être en cas de perte de justificatifs d'identité (cartes) nécessitant une nouvelle délivrance.	L'un des principaux objectifs de l'utilisation d'un système d'identité numérique est la réduction des coûts et du temps passé pour les utilisateurs. Si des coûts supplémentaires sont prélevés pour l'utilisation de ce système, ils seront moins enclins à participer.

III. CAPACITÉS DU SYSTÈME

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
NORMES TECHNIQUES	Définir les normes techniques spécifiques à respecter pour l'élaboration de la plateforme et de la base de données d'identité numérique. Les normes techniques peuvent être définies à partir des exemples fournis par d'autres applications de l'identité numérique et procédures d'e-KYC, ainsi que par les orientations émanant d'organismes de normalisation.[17] En plus des normes techniques, le système doit prendre en compte les aspects clés suivants : a. La robustesse et le haut niveau de fonctionnalité b. Le caractère personnalisable et configurable c. Le respect de la vie privée intégré dans la conception[18] d. Normes pour la collecte, le stockage et le partage des données avec des tiers, si cela est autorisé e. L'accès en temps réel aux données à des fins d'e-KYC et pour d'autres applications f. L'infrastructure supplémentaire pour prendre en charge les interfaces de programmation d'applications (API) relatives à l'identité numérique à des fins d'e-KYC et de procédures d'authentification, et pour rationaliser l'accès aux données en vue d'une utilisation productive Envisager des solutions de logiciels libres pour le développement technologique afin d'éviter le verrouillage par les fournisseurs, et pour permettre un développement économique. Les décisions portant sur le caractère centralisé ou décentralisé de l'identité numérique doivent tenir compte de l'infrastructure et des besoins du pays.	Contribuer à l'évaluation de l'infrastructure technologique disponible dans le pays et apporter des modifications supplémentaires en fonction des normes internationales. Cela permettra également de garantir que les normes relatives à l'identité numérique et à l'e-KYC répondent aux objectifs de performance souhaités. L'infrastructure API offrira aux parties prenantes des mécanismes pratiques de vérification et d'authentification à l'aide de la base de données d'identité numérique.
CARACTÉRISTIQUES TECHNIQUES DU SYSTÈME	Donner des orientations sur les caractéristiques techniques à intégrer dans le système pour en assurer l'efficacité. Au nombre des principales caractéristiques qui permettront d'améliorer les capacités du système, nous pouvons citer : a. La déduplication automatisée et dynamique b. Les contrôles anti-fraude et les processus anti-fraude intégrés c. La séparation des bases de données pour les données biométriques et démographiques d. L'établissement de liens en temps réel avec les registres des naissances et des décès pour des mises à jour automatiques e. La prise en charge de plusieurs mécanismes d'authentification biométrique f. L'authentification et l'enrôlement hors ligne g. Les procédures de gestion des exceptions h. L'architecture de gestion des consentements i. L'établissement de liens avec d'autres systèmes d'identité pour promouvoir différentes applications, telles que le permis de conduire, les prestations sociales, l'identification fiscale, le système national de santé, etc..	Veiller à ce que le système se conforme aux bonnes pratiques mondiales en prévoyant des mises à jour et une maintenance continues.
AUDITS ET ÉVALUATIONS TECHNIQUES	Publier des directives et procéder à des contrôles périodiques de l'efficacité, de l'innovation et de la rentabilité de la technologie sous-jacente.	Veiller à ce que des mises à niveau soient effectuées en temps opportun et à ce que les normes sectorielles et les bonnes pratiques les plus récentes soient respectées.

17 Banque mondiale, 2018. ID4D Practitioner's Note. Catalog of Technical Standards for Digital Identification Systems. Banque internationale pour la reconstruction et le développement / Banque mondiale. Disponible (en anglais) à l'adresse : https://olc.worldbank.org/system/files/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

18 Alliance pour l'inclusion financière, 2021. Guideline Note on Data Privacy for Digital Financial Services. Disponible (en anglais) à l'adresse : https://www.afi-global.org/publications/guideline-note-on-data-privacy-for-digital-financial-services/

IV. GESTION DES DONNÉES

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
GESTION DES DONNÉES À 360 DEGRÉS (DONNÉES AU REPOS, EN COURS D'UTILISATION ET EN MOUVEMENT)	Établir et faire respecter des procédures strictes de gestion des données pour toutes les parties prenantes impliquées dans la collecte, le traitement et le stockage des données des utilisateurs. a. Tokenisation, virtualisation et authentification à deux facteurs lors de l'utilisation des données b. Mise en place de barrières physiques et techniques à l'accès lorsque les données sont stockées et au repos, en précisant les méthodes d'accès, de stockage et de réalisation autorisées c. Cryptage et lignes sécurisées lors de la transmission des données Les données collectées de manière légale peuvent être utilisées dans le cadre de la production de données agrégées ou de résumés statistiques anonymisés, sans identification possible des personnes.	Faire respecter toutes les mesures de confidentialité et de sécurité des données et veiller à ce que les pratiques de gestion des données assurent la protection des données des utilisateurs contre les attaques extérieures.

V: USER SERVICES

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
SERVICES AUX UTILISATEURS	Les services aux utilisateurs doivent inclure : a. La possibilité de fournir un consentement et des autorisations pour l'utilisation par des tiers. b. La possibilité de révoquer un consentement c. La possibilité de verrouiller les données biométriques d. La visibilité et la capacité de suivre les opérations pour lesquelles des données personnelles ont été demandées et traitées e. Les options de portabilité des informations f. Les mécanismes de contestation et de demande de dédommagement Des directives sur la manière dont les utilisateurs peuvent accéder à ces services doivent être publiées et diffusées aux utilisateurs. De nombreux canaux doivent être prévus, de préférence pour faciliter l'accès. Les applications mobiles, l'accès par USSD et par site web peuvent être privilégiés par rapport aux demandes manuelles. Les entités chargées de la mise en œuvre doivent également trouver des moyens de communiquer efficacement avec les utilisateurs pour les sensibiliser sur les dispositions applicables, le consentement, les droits, les services et les applications des systèmes d'identité numérique. Les utilisateurs doivent aussi être informés des canaux et des dispositifs utilisés dans l'écosystème.	Faire en sorte que les systèmes construits soient centrés sur l'utilisateur et que les utilisateurs aient le contrôle des données.

PARTIE III. APPROCHES STRATÉGIQUES POUR LA MISE EN PLACE DE PROCESSUS CLÉS ET D'APPLICATIONS METTANT À PROFIT L'IDENTITÉ NUMÉRIQUE À DES FINS D'E-KYC

Dans cette partie, l'accent est mis sur l'une des principales applications de l'identité numérique, à savoir les services d'e-KYC et d'authentification. Nous ferons ici un résumé des pratiques efficaces mises en œuvre par les membres de l'AFI et au niveau mondial, et nous présenterons en détail un cadre et des principes directeurs permettant de mettre en place des procédures solides d'e-KYC, y compris l'accès, l'interopérabilité, l'infrastructure du dernier kilomètre et le traitement des exceptions.

I. CADRE DE MISE EN ŒUVRE POUR L'E-KYC ET L'AUTHENTIFICATION

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
CADRE DE MISE EN ŒUVRE DE L'E-KYC	Fournir des orientations et élaborer un cadre d'e-KYC en détaillant les aspects clés suivants, le cas échéant : a. La portée de l'e-KYC simplifié et régulier pour les différentes parties prenantes en fonction du risque identifié b. L'applicabilité de l'e-KYC (pour les personnes disposant d'une pièce d'identité numérique et dérogations pour les personnes sans pièce d'identité numérique) c. Le recueil du consentement de l'utilisateur pour le traitement, le stockage et la gestion des données d. L'autorisation des tiers pour l'accès à des fins d'utilisation légitime e. L'utilisation de l'identification vidéo[19]	Définir clairement la portée et l'utilisation des services d'e-KYC et d'autres opérations. Cela permettra d'élaborer une stratégie de mise en œuvre assortie de cibles et d'objectifs clairs.
AUTHENTICATION MECHANISM	Consulter les parties prenantes et les experts techniques appropriés pour élaborer un mécanisme d'authentification qui soit adapté au contexte du pays et qui réponde aux exigences en matière de LBC/FT. Le système d'identité numérique peut être exploité pour répondre à différents niveaux de certitude grâce à l'authentification démographique et biométrique. Certains des facteurs clés servant à l'authentification de l'identité en se basant sur un système d'identité numérique sont les suivants : a. Les facteurs de possession (numéro d'identification, code QR) Justificatif qu'une personne détient et peut présenter sur demande, comme une carte ou un certificat physique ou virtuel b. Les facteurs biométriques (empreinte digitale, iris, visage) c. Les facteurs de connaissance (code PIN, mot de passe à usage unique, identifiant de connexion). Élément qui a été porté à la connaissance de l'utilisateur.	Construire des systèmes d'authentification flexibles, sûrs et efficients, dotés de mesures de recours efficaces pour la vérification de l'identité et l'authentification des personnes vulnérables (personnes dont les empreintes digitales sont usées par l'âge ou en raison de la profession exercée, personnes handicapées qui ne sont pas en mesure de s'authentifier à l'aide de leur iris, etc.)

19 La transmission de vidéo haute résolution permettant l'identification et la vérification à distance et la « preuve de vie » de l'utilisateur. Voir GAFI, 2020. Guidance on Digital Identity. Disponible (en anglais) à l'adresse : http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
AUTHENTICATION MECHANISM *a continué*	Déterminer s'il s'agit d'un système d'authentification décentralisé, grâce à des dispositifs du dernier kilomètre tels que des lecteurs de cartes, ou centralisé, avec consultation en temps réel d'une base de données d'identité numérique. Le mécanisme d'authentification doit aussi dans l'idéal ne pas être associé à un dispositif unique mais être multimodal (c'est-à-dire capable d'utiliser différents facteurs et justificatifs d'identité pour la vérification). Les systèmes d'authentification à deux facteurs satisfont à des exigences de sécurité plus élevées et les systèmes multimodaux offriront un processus intégré de traitement des exceptions.	
PARAMÈTRES DE CORRESPONDANCE POUR L'AUTHENTIFICATION	Élaborer des paramètres de correspondance appropriés sur la base de références et de limites techniquement acceptées. Les paramètres de correspondance en ce qui concerne les données numériques, telles que la date de naissance, les numéros de téléphone, devraient idéalement être de 100 %. Les facteurs biométriques doivent être compris entre 80 et 100 pour cent afin de tenir compte de la qualité des scanners et des dispositifs du dernier kilomètre.	Les paramètres de correspondance permettent de définir la précision du système ; des niveaux élevés de paramètres de correspondance contribueront à renforcer la confiance dans les capacités du système. Il convient toutefois de mettre en balance la précision avec le risque d'une augmentation des taux d'échec, afin de garantir une mesure finale équilibrée.

II. ACCÈS ET INTEROPÉRABILITÉ POUR LES PARTIES PRENANTES TIERCES

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
PROCÉDURES SIMPLIFIÉES D'ACCÈS ET D'UTILISATION	Définir un ensemble normalisé de règles d'engagement pour les parties prenantes tierces qui veulent accéder au système. Mettre en évidence les exigences minimales et les permissions requises pour l'accès. Détailler les étapes et procédures d'accès ainsi que les exigences de la tierce partie, en termes de protection des données et de mesures de sécurité, selon que l'accès est accordé à des parties prenantes individuelles dans le cadre d'un protocole d'accord[20] ou par le biais d'entités autorisées.	Faire en sorte que les parties prenantes bénéficient d'un accès uniforme et équitable au marché pour tirer parti du système. Veiller à la normalisation des documents tels que les protocoles d'accord, les accords de confidentialité (NDA) et autres accords contractuels.
ACCÈS À PLUSIEURS NIVEAUX AUX DONNÉES	Définir et publier une liste normalisée des différents niveaux de services qui se servent de l'identité numérique, comme l'authentification et l'e-KYC (démographique et biométrique), et la saisie automatique des données de l'utilisateur, entre autres. Ce système à plusieurs niveaux doit être basé sur les principes et le niveau d'accès plutôt que sur les besoins des entités individuelles.	Permettre aux acteurs du secteur de choisir dans la liste établie en fonction de leurs besoins et les aider à préparer leurs systèmes internes en conséquence.
CANAUX D'ACCÈS	Fournir des directives précises sur les canaux et mécanismes disponibles pour accéder aux données de la plateforme d'identité numérique pour les tiers. Les canaux peuvent être déterminés sur la base d'une analyse des risques des différentes alternatives et de leurs avantages et inconvénients. L'accès peut être assuré par des API, des liens de services Web ou des liens directs au système par le biais d'autorisations.	Les canaux disponibles doivent permettre un accès facile et rationalisé pour une utilisation économique sans interruption des données et des services.

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
STRUCTURES DE COÛTS ÉCONOMIQUES	Il convient d'évaluer la disposition à payer des parties prenantes, par le biais de consultations détaillées et de discussions sur la stratégie de tarification. Les modèles suivants pourraient être adoptés : a. Une structure de coûts à plusieurs niveaux basée sur les opérations, avec une redevance en fonction du niveau d'accès et du service fourni b. Un modèle basé sur un abonnement annuel ou mensuel Les modèles de tarification[21] actuellement utilisés sont gratuits pour les entités publiques, tandis que les entités privées doivent payer des montants minimes. Une authentification simple basée sur le système d'identité numérique entraîne des coûts négligeables, tandis qu'une demande d'e-KYC avec partage de données suppose des coûts légèrement plus élevés.	Des coûts abordables associés aux services stimuleront l'adoption par les parties prenantes et procureront un certain revenu aux administrateurs du système, permettant d'assurer la durabilité du système.
CONTRÔLE ET SUPERVISION DE L'ACCÈS ET DE L'UTILISATION	Donner des directives aux entités chargées de la mise en œuvre sur les mécanismes de surveillance qui devraient être mis en place concernant les tiers qui ont accès aux données. Ces mécanismes doivent être définis dans le protocole d'accord. Les mécanismes de surveillance doivent inclure des rapports réguliers, des notifications de toute violation, et des détails sur les frais et les pénalités perçus. Ces mesures doivent être acceptées par les entités chargées de la mise en œuvre ainsi que par les parties prenantes tierces.	Faire en sorte que les pratiques de protection des données soient également suivies par tous les acteurs de l'écosystème et sanctionner toute utilisation abusive ou frauduleuse.

III. DISPOSITIFS ET INFRASTRUCTURES DU DERNIER KILOMÈTRE

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
INFRASTRUCTURE DU DERNIER KILOMÈTRE	Élaborer et publier des directives ou des normes sectorielles portant sur les dispositifs utilisés pour l'authentification du dernier kilomètre des utilisateurs, tels que les scanners biométriques et les lecteurs de cartes. Envisager une certification des dispositifs du dernier kilomètre pouvant garantir des caractéristiques techniques, une qualité et des exigences de sécurité normalisées. Les normes et les directives doivent permettre de garantir que seuls des dispositifs autorisés/certifiés sont utilisés pour accéder à la plateforme d'identité numérique. Des systèmes de suivi des numéros de série ou d'enregistrement auprès d'une autorité centrale peuvent être mis en place pour prévenir les abus et offrir un moyen de contrôler les appareils utilisés par les agents du dernier kilomètre.	Faire en sorte que les protocoles de sécurité, la protection des données et la confidentialité des données soient respectés pendant le transfert et l'utilisation des données.

21 Banque mondiale, 2019. ID4D Practitioner's Note. Identity Authentication and Verification Fees: Overview of Current Practices. Washington : Banque mondiale. Disponible (en anglais) à l'adresse : http://documents1.worldbank.org/curated/en/945201555946417898/pdf/Identity-Authentication-and-Verification-Fees-Overview-of-Current-Practices.pdf

I. APPLICATIONS

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
INTEROPÉRABILITÉ ET INFRASTRUCTURE PARTAGÉE	Impliquer les acteurs du marché et les autres parties prenantes pour promouvoir la discussion et fournir des orientations sur l'interopérabilité et les applications permettant de tirer parti de l'infrastructure construite.[22] Susciter des échanges sur les exigences politiques et réglementaires afin de faciliter l'interopérabilité pour : a. Les prestations de services gouvernementaux b. Les prestations de services de protection sociale des différents départements/ministères c. Les institutions financières formelles d. Les entreprises de technologie financière (FinTechs) e. Les institutions non-financières, telles que les opérateurs de télécommunications f. Les sociétés tierces autorisées à effectuer des procédures d'e-KYC/KYC g. Les scrutins électoraux h. Les administrations fiscales i. Le traitement des litiges	Veiller à une utilisation durable et à l'efficacité du marché grâce à des services interopérables et encourager les parties prenantes à adhérer à l'infrastructure partagée.

V. TRAITEMENT DES EXCEPTIONS ET RÉSOLUTION DES PLAINTES

CHAMP RÉGLEMENTAIRE	PRINCIPE DIRECTEUR	ENJEUX
PROCÉDURES DE TRAITEMENT DES EXCEPTIONS	Documenter certains des principaux défis qui pourraient survenir ainsi que les procédures de traitement des exceptions et les protocoles correspondants. Procédures à suivre en cas d'échec de l'authentification ou de non-correspondance des données biométriques, particulièrement pour les opérations d'e-KYC. Des procédures alternatives pour les zones à faible connectivité ou confrontées à d'autres défis infrastructurels doivent également être décrites. Des options telles que le mode hors ligne peuvent être envisagées au moyen d'un code QR ou de lecteurs de cartes.	Faire en sorte que des processus rationalisés et décentralisés autour de l'authentification biométrique soient mis en place en éliminant les obstacles à la technologie et à l'alphabétisation.
RÉSOLUTION DES PLAINTES	Proposer une infrastructure robuste de résolution des plaintes par le biais de canaux multiples intégrant des interfaces humaines et technologiques. Les canaux doivent être facilement accessibles, disposer de mécanismes de rétroaction adéquats et de délais de résolution rapides. Des dispositions doivent également être prises pour traiter les plaintes et les litiges des institutions financières utilisatrices. On peut envisager des accords de niveau de service pour le traitement des plaintes des consommateurs entre les principales institutions responsables du système d'identité numérique. Le fonctionnement détaillé des mécanismes de résolution des plaintes doit être diffusé publiquement, et les utilisateurs doivent être informés lors de l'enrôlement. Les canaux efficaces pouvant être mis à la disposition des utilisateurs en tant qu'options sont un numéro vert, un site Web ou une adresse e-mail, ou encore une application mobile si le système inclut cette solution à l'intention des utilisateurs.	Aider les personnes à obtenir facilement réparation pour toute difficulté liée à la gestion de l'identité (enrôlement, échec de l'authentification, non-correspondance des données biométriques, usurpation d'identité, utilisation abusive des données, etc.)

22 Alliance pour l'inclusion financière, 2019. Modèle stratégique pour la monnaie électronique. Disponible à l'adresse : https://www.afi-global.org/wp-content/uploads/2019/09/AFI_DFS_Emoney_F_FINAL_digital.pdf, p. 7

ANNEXE 1 : PRATIQUES DES PAYS MEMBRES DE L'AFI EN MATIÈRE DE POLITIQUE D'IDENTITÉ NUMÉRIQUE ET D'E-KYC

NOM DU PAYS	POLITIQUE RÉPERTORIÉE
BANGLADESH	LBC/FT : (Lien) Directives relatives à l'e-KYC : (Lien) Protection des données : Loi sur la sécurité numérique, 2018 (Lien)
BCEAO	Directive n°02/2015/CM/UEMOA relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme dans les États membres de l'UEMOA (Lien) CEDEAO : Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel (Lien) CEDEAO : Directive C/DIR/1/08111 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO (Lien)
EL SALVADOR	Le Salvador œuvre à la mise en place de l'identification numérique, avec l'élaboration d'un avant-projet de la « Loi spéciale relative à la prévention, au contrôle et à la pénalisation du blanchiment de capitaux ». (Lien)
GHANA	Loi de 2006 relative à l'Autorité nationale d'identification (loi n° 707), Loi de 2017 relative au Registre national d'identité (Amendement) (loi n° 750) Loi de 2020 relative à la lutte contre le blanchiment de capitaux (Loi n° 1044). Lignes directrices en matière de LBC/FT à l'intention des banques et institutions financières non bancaires au Ghana, juillet 2018. Loi de 2012 relative à la protection des données (loi n° 843) Loi de 2020 relative à la cybersécurité (loi n° 1038) Loi de 2019 relative aux systèmes et services de paiement (loi n° 987) Loi de 2008 relative aux transactions électroniques (loi n° 772)
INDE	LBC/FT : Circulaire principale concernant les normes de connaissance du client (KYC)/lutte contre le blanchiment de capitaux (LBC)/lutte contre le financement du terrorisme (FT)/obligations des banques en vertu de la Loi relative à la prévention du blanchiment de capitaux, 2002. (Lien) Identité numérique : Programme biométrique Aadhaar et lois connexes (loi de modification), 2019 (Lien) Protection des données à caractère personnel :
MADAGASCAR	LBC/FT : (Lien) Protection des données à caractère personnel : Loi n°2014-038 sur la protection des données à caractère personnel (Lien), établissant une autorité indépendante chargée de la protection des données à caractère personnel (Commission Malagasy de l'informatique et des libertés). L'autorité est chargée de veiller à ce que le traitement des données à caractère personnel respecte les dispositions de la loi. Cybersécurité : (Lien)

COUNTRY	REPORTED POLICY
MEXIQUE	Identité numérique : Cadre juridique du Registre national de la population et de l'identité (Lien) LBC/FT : Article 15 de la loi relative aux établissements de crédit (Lien) Protection des données à caractère personnel et de la vie privée : Loi fédérale relative à la protection des données à caractère personnel détenues par des particuliers (Lien) Cybersécurité : Dispositions générales concernant la sécurité de l'information pour les établissements de crédit (Lien)
NAMIBIE	LBC/FT : Loi relative au renseignement financier (Lien)
NIGÉRIA	Règlements LBC/FT (Règlement modificatif de 2019 (Lien) Règlement de 2019 relatif à la protection des données (Lien) Loi relative à la lutte contre la cybercriminalité (interdiction et prévention (Lien) Loi de 2007 relative à la Commission nationale de gestion de l'identité (Lien)
PÉROU	Identité numérique : Décret suprême n° 029-20221-PCM, décret approuvant la loi sur l'administration numérique (Lien) — En espagnol Protection des données à caractère personnel : Loi n° 29733 et règlement connexe. Définit le traitement approprié des données par les entités publiques et privées (Lien) Règlement sur la cybersécurité (Lien) — En espagnol
PHILIPPINES	LBC/FT : Loi n° 9160, dite « loi anti-blanchiment de 2001 ». (Lien) Identité numérique : Loi « PhillID » n° 11055 (Lien), ou loi relative au système d'identification philippin, signée par le président Rodrigo Roa Duterte le 6 août 2018. Il s'agit d'une loi instaurant un système d'identité nationale unique qui vise à fournir une preuve d'identité valide aux citoyens philippins et aux étrangers résidents aux Philippines. Protection des données à caractère personnel : Loi relative à la confidentialité des données - Loi n° 10173 (Lien) Cybersécurité : Loi de 2012 relative à la prévention de la cybercriminalité - Loi n° 10175 (Lien)
RUSSIE	Protection des données à caractère personnel et de la vie privée : Loi fédérale relative aux données personnelles, 2006 (Lien) LBC/FT : (Lien) Identité numérique : Résolution du Gouvernement de la Fédération de Russie n° 710 de 2019 (Lien)
SÉNÉGAL	Sénégal : Loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel (Lien) Sénégal : Loi n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité (Lien)
SINGAPOUR	LBC/FT : Lignes directrices concernant la lutte contre le blanchiment de capitaux et le financement du terrorisme (Lien) Identité numérique : (Lien) Loi de 2012 relative à la protection des données (Lien)
ZAMBIE	LBC/FT : Loi de 2016 relative au Centre de renseignement financier (Lien) Protection des données à caractère personnel : Loi relative à la protection des données, 2021 (Lien) Cybersécurité : Loi relative à la cybersécurité et à la cybercriminalité (Lien)

ANNEXE 2 : RÉFÉRENCES

1. Banque mondiale, 2019. ID4D Practitioner's Guide: Version 1.0 (octobre 2019). Washington : Banque mondiale. Disponible (en anglais) à l'adresse : http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

2. Banque mondiale, 2018. ID4D Practitioner's Note. Catalog of Technical Standards for Digital Identification Systems. Washington : Banque internationale pour la reconstruction et le développement / Banque mondiale. Disponible (en anglais) à l'adresse : https://olc.worldbank.org/system/files/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

3. The Centre for Internet and Society, 2020. Governing ID: Principles for Evaluation. Disponible (en anglais) à l'adresse : https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf

4. Alliance pour l'inclusion financière, 2021. « Four policies to promote inclusive financial integrity in 2021 ». Disponible (en anglais) à l'adresse : https://www.afi-global.org/newsroom/blogs/four-policies-to-promote-inclusive-financial-integrity-in-2021/

5. Alliance pour l'inclusion financière, 2019. KYC Innovations, Financial Inclusion and Integrity. Disponible (en anglais) à l'adresse : https://www.afi-global.org/wp-content/uploads/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries_0.pdf

6. Alliance pour l'inclusion financière, 2020. Inclusive Financial Integrity: A Toolkit for Policymakers. Disponible (en anglais) à l'adresse : https://www.afi-global.org/sites/default/files/publications/2020-07/AFI_CENFRI_toolkit_AW_digital.pdf

7. Alliance pour l'inclusion financière, 2021. Guideline Note on Data Privacy for Digital Financial Services. Disponible (en anglais) à l'adresse : https://www.afi-global.org/wp-content/uploads/2021/02/AFI_GN43_AW3_digital.pdf

8. GAFI, 2020. Guidance on Digital Identity. GAFI, Paris. Disponible (en anglais) à l'adresse : http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf

9. Banque mondiale, 2018. G20 Digital Identity Onboarding. Disponible (en anglais) à l'adresse : https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org
Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork