

CADRE D'INTEROPÉRABILITÉ DES SYSTÈMES D'IDENTIFICATION NUMÉRIQUE DE L'UA



TABLE DES MATIÈRES

RÉSUMÉ ANALYTIQUE	1
ACRONYMES ET ABRÉVIATIONS	4
1. CONTEXTE	5
1.1. APERÇU	5
1.2. ÉTAT DES SYSTÈMES D'IDENTIFICATION EN AFRIQUE	6
1.3. AUTRES INITIATIVES	9
1.4. LA SOUVERAINETÉ NUMÉRIQUE ET DES DONNÉES	11
2. INTRODUCTION	13
2.1. VISION, OBJECTIFS ET CAS D'UTILISATION INDICATIFS	13
2.2. CHAMP D'APPLICATION	15
2.3. CADRE DE CONFIANCE, CONFIDENTIALITÉ DES DONNÉES, INTEROPÉRABILITÉ ET NORMES	16
3. LE CADRE	18
3.1. PRINCIPES DIRECTEURS	19
3.2. MODÈLE DE MISE EN ŒUVRE	20
3.3. PROCESSUS ÉPROUVÉ – LE CADRE DE CONFIANCE	22
3.4. OPTIONS D'AUTHENTIFICATION POTENTIELLES	25
4. FEUILLE DE ROUTE DÉTAILLÉE POUR LA MISE EN ŒUVRE	29
4.1. PHASE 1 : ADOPTION DU CADRE ET ENVIRONNEMENT FAVORABLE	29
4.2. PHASE 2 : MISE EN ŒUVRE DU CADRE ET ADOPTION DES SPÉCIFICATIONS TECHNIQUES DE L'IDC-ID	31
4.3. PHASE 3 : DÉVELOPPEMENT DE L'INFRASTRUCTURE POUR PERMETTRE L'AUTHENTIFICATION À DISTANCE	32

RÉSUMÉ ANALYTIQUE

Des centaines de millions de personnes en Afrique n'ont pas d'identification (ID) légale et beaucoup d'autres ont des documents d'identité qui ne sont pas adaptés à l'ère du numérique. En conséquence, ces personnes sont confrontées à des difficultés pour accéder aux services et aux opportunités créés par la numérisation. Les identités numériques fondamentales interopérables, fiables et inclusives, qui permettent aux gens de vérifier leur identité légale hors ligne et en ligne, peuvent aider à relever ces défis et ont un potentiel important pour accélérer la numérisation des économies et des sociétés africaines en soutenant l'esprit d'entreprise et en contribuant à la mise en œuvre réussie de la Zone de libre-échange continentale africaine (ZLECAf). C'est pour ces raisons que la plupart des pays africains modernisent actuellement leurs écosystèmes d'identification, bien qu'à des stades différents.

Le Cadre d'interopérabilité des systèmes d'identification numérique de l'UA (le Cadre) définit une vision qui **permettra à tous les citoyens africains d'avoir la possibilité d'accéder facilement et en toute sécurité aux services publics et privés nécessaires, à tout moment, indépendamment de leur localisation**. Dans cette optique, le Cadre définit des exigences communes, des normes minimales, des mécanismes de gouvernance et un alignement plus poussé entre les cadres juridiques, en vue d'atteindre les objectifs suivants :

1. Permettre aux citoyens africains de vérifier leur identité légale hors ligne et en ligne afin d'accéder aux services des secteurs public et privé dans les États membres de l'UA en contribuant à l'accélération des progrès vers l'unité et l'intégration continentales pour assurer une croissance soutenue, promouvoir le commerce, les échanges de biens et de services, la libre circulation des personnes et des capitaux par la création d'une Afrique unie et l'accélération de l'intégration économique par le biais de la ZLECAf, comme indiqué dans l'aspiration 2 de l'Agenda 2063 ;
2. Donner aux citoyens africains le contrôle de leurs données personnelles, y compris la possibilité de ne divulguer de manière sélective que les attributs nécessaires à une transaction particulière. Les informations à caractère personnel à divulguer doivent être minimales, proportionnées et ne doivent contenir que les informations pertinentes à ce genre de transaction, compte tenu de la situation particulière de l'Afrique et conformément aux meilleures pratiques internationales.¹et
3. Renforcer la confiance et l'interopérabilité entre les systèmes d'identification fondamentaux des États membres de l'UA.

Le Cadre prévoit une norme commune au niveau continental pour représenter numériquement les preuves d'identité délivrées par des sources fiables des États membres de l'UA et pour assurer l'interopérabilité sur tout le continent. Les personnes titulaires d'une pièce d'identité d'un système national pourront obtenir un justificatif d'identité numérique légal interopérable pour l'identité (IDC-ID) qui prendra la forme d'un renseignement vérifiable². Des normes seront établies pour le cadre d'interopérabilité qui définira des éléments clés de l'IDC-ID, qui

1 Voir le règlement général de l'UE sur la protection des données (RGPD), 2016: <https://gdpr.eu>.

2 Les renseignements désignent un ensemble d'attributs concernant une personne concernée, comme le nom de famille ou la date de naissance. Un renseignement vérifiable est une version inviolable de ces informations qui peut être vérifiée de manière cryptographique afin d'en contrôler l'authenticité.

démontrera la confiance accordée aux justificatifs numériques créés sous la gouvernance d'un cadre de confiance définissant les conditions dans lesquelles ces justificatifs seront délivrés par des sources fiables des États membres de l'UA.

Les États membres de l'UA sont libres de choisir la manière dont ils souhaitent délivrer ce justificatif d'identité numérique. Il pourra être stocké dans un format purement numérique sur une application smartphone, un serveur en nuage, une carte à puce ou un lien permettant d'accéder à la représentation numérique qui pourra être établie à l'aide d'un code-barres à une ou deux dimensions sur un document papier (imprimé sur papier, carte plastique). Les États membres peuvent également décider de réutiliser cette norme pour représenter les données d'identité au niveau national, continental ou des CER, ou même émises séparément en complément de systèmes d'identification numérique préexistants.

Le Cadre sera basé sur le développement de systèmes d'identification fondamentaux interopérables, inclusifs et fiables, car ils constituent l'épine dorsale des sources de données faisant autorité sur l'identité légale des personnes et permettent ainsi à l'IDC-ID d'atteindre des niveaux d'assurance plus élevés. Les États membres de l'UA sont ainsi encouragés à renforcer leurs systèmes d'identification de base et les principes d'identification pour le développement durable. Ce cadre tient également compte des efforts continentaux parallèles pour créer un environnement favorable visant à protéger les données personnelles, à maintenir la cybersécurité et à sauvegarder les droits des personnes, grâce à l'adoption de la Convention de Malabo sur la cybersécurité et la protection des données personnelles³ et à l'élaboration en cours d'un cadre politique continental sur les données.

La délivrance de l'IDC-ID pourra être achevée par une infrastructure permettant des cas d'utilisation plus avancés tels que l'authentification à distance. Ce Cadre met en évidence plusieurs options techniques à la disposition des États membres de l'UA pour mettre en œuvre cette couche, par exemple une fédération de fournisseurs d'identité assurant des mécanismes d'authentification aux détenteurs de l'IDC-ID, ou le développement de solutions de portefeuille d'identité numérique ou tout autre modèle permettant l'interopérabilité. Les États membres de l'Union africaine pourront également trouver un accord supplémentaire sur la manière d'établir cette infrastructure relative à la couche d'authentification et s'associer aux CER et à d'autres initiatives continentales qui étudient déjà la mise en place de solutions interopérables d'identification numérique fondamentales pour accéder aux services à distance.

La mise en œuvre du Cadre est fondée sur la supposition qu'il sera validé et approuvé par les États membres de l'UA. L'exclusivité potentielle, la faiblesse des mécanismes de sécurité, l'érosion de la protection de la vie privée, l'incertitude quant aux avantages d'un système d'identité numérique fondamental, le manque de capacités techniques et financières, le manque de centres de données en Afrique pour stocker les données sensibles, la présence de systèmes d'identité non interopérables et de cadres juridiques et réglementaires obsolètes sont les défis identifiés à relever.

3 Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, voir : <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

Ce document comprend les sections suivantes :

1

Un **contexte** sur le travail de l'Union africaine qui a conduit à la création de ce document, un aperçu de l'état des systèmes d'identification en Afrique et une série d'initiatives favorisant l'interopérabilité des identités numériques sur le continent.

2

Une **introduction** à la vision, aux objectifs, à la portée et aux cas d'utilisation potentiels du cadre d'interopérabilité des systèmes d'identification numérique proposé par l'UA.

3

Une **vue d'ensemble des éléments clés constituant le Cadre**, notamment les principes directeurs pour sa conception et sa mise en œuvre, le modèle choisi, les composants clés du cadre qui devront être définis plus avant (ex. : les règles de participation, l'interopérabilité et les exigences techniques), ainsi que trois options architecturales potentielles pour mettre en place une couche d'authentification d'interopérabilité.

4

Une **feuille de route détaillée** sur l'approche progressive proposée pour la définition et la mise en œuvre du Cadre, ainsi que des actions concrètes à entreprendre par les États membres et l'Union africaine.

5

Hypothèses, défis et risques majeurs à traiter et mécanismes d'atténuation recommandés.

Le Cadre n'appelle pas à la création d'un système continental unifié d'identité numérique mais à l'établissement d'un cadre d'interopérabilité pour les systèmes d'identification numérique fondamentaux existants parmi les États membres de l'UA, qui tienne compte de la souveraineté numérique des États membres de l'UA, des divergences dans la mise en œuvre de l'infrastructure numérique, de la disponibilité des politiques et réglementations associées, des différents types de systèmes d'identification et de la vulnérabilité des populations pendant et après la mise en œuvre des systèmes d'identification numérique interopérables.

ACRONYMES ET ABRÉVIATIONS

ZLECAF	Zone de Libre-Echange Continentale Africaine
LCBA/FT	Lutte Contre le Blanchiment D'argent Et le Financement du Terrorisme
API	Interface de Programmation D'application
UA	Union Africaine
CUA	Commission de L'union Africaine
CIRT	Equipes de Reponse Aux Incidents Informatiques
CRVS	Systemes D'enregistrement des Faits D'etat Civil Et D'etablissement des Statistiques de L'etat Civil
APD	Autorite de Protection des Donnees
AIPD	Analyse D'impact Relative a la Protection Des Donnees
CAE	Communaute D'afrique de L'est
CEDEAO	Communaute Economique des États de L'afrique de L'ouest
GIZ	Gesellschaft Für Internationale Zusammenarbeit
GSMA	Gsm Association
HSM	Modules Materiels de Securite
TIC	Technologies de L'information et de La Communication
IDC-ID	Justificatifs D'identite Numerique Interoperable
UIT	Union Internationale des Telecommunications
KYC	Systeme de Gestion de La Connaissance du Client
LOA	Niveau D'assurance
PATF	Cadre de Confiance Panafricain
CER	Communaute Economique Regionale
RP	Partie Interessee
SATA	Alliance Smart Africa Trust
LE CADRE	Cadre D'interoperabilite des Systemes D'identification Numerique de L'ua
CEA	Commission Economique des Nations Unies Pour L'afrique
WURI	Projet D'identification Unique Pour L'integration Regionale Et L'inclusion En Afrique de L'ouest

Voir l'annexe i pour les definitions de travail.

1. CONTEXTE

1.1. APERÇU

Il est essentiel que les personnes puissent prouver leur identité pour pouvoir accéder aux services et exercer leurs droits. Traditionnellement, la preuve de l'identité pouvait se faire sur la base de la familiarité, de l'apparence et du témoignage d'autres personnes, ce qui fonctionnait dans les petites communautés informelles. À mesure que les sociétés et les économies se sont développées, des justificatifs physiques plus formels et intégrés, tels que les cartes d'identité et les passeports, ont été introduits pour établir la confiance. Cependant, à mesure que les pays évoluent vers des sociétés et des économies numériques, ces justificatifs physiques ne sont pas très utiles pour prouver l'identité sur l'internet et effectuer d'autres transactions numériques telles que les paiements numériques et le partage de données personnelles. La confiance en ligne repose ainsi sur les identités numériques, représentées par des systèmes d'identification numérique qui utilisent des technologies et des approches modernes pour permettre aux personnes de prouver et de vérifier leur identité en toute sécurité.

Les pièces d'identité, et en particulier les identités numériques, peuvent offrir un large éventail d'avantages aux pays, tels que la bonne gouvernance, l'inclusion financière, l'égalité des sexes et l'autonomisation des femmes, ainsi qu'une meilleure protection sociale, des résultats en matière de soins de santé et d'éducation. Pour les individus, ils constituent un outil permettant de faire valoir leurs droits et leur éligibilité aux services et aux transactions. De même, ils constituent une plateforme permettant aux gouvernements et aux entreprises de rationaliser, d'étendre et d'innover dans la prestation de leurs services opérationnels grâce à la numérisation et à l'automatisation, en particulier lorsqu'ils sont envisagés comme une « pile numérique » avec des plateformes de partage de données et de paiement numérique fiables. L'apparition de la pandémie COVID-19 a montré l'importance des piles numériques, car les pays qui les avaient mises en place, en totalité ou en partie, avant le début de la pandémie ont été mieux à même de fournir rapidement et efficacement une assistance sociale et ont mieux résisté lorsque les services en personne ont dû passer en ligne. Compte tenu du fait que l'internet ne connaît pas de frontières, les identités numériques délivrées dans un pays et reconnues dans d'autres peuvent également constituer un puissant moteur d'intégration sociale et économique, que ce soit au niveau bilatéral, régional ou mondial.

La sécurité et l'impact des identités numériques sont optimaux lorsque ces dernières sont fondées sur l'identité légale des personnes. L'identité légale est généralement gérée par l'écosystème d'identité fondamental d'un pays, y compris l'enregistrement civil, l'identité nationale et d'autres systèmes similaires. Malheureusement, des centaines de millions de personnes en Afrique n'ont toujours pas de pièce d'identité de base, comme une carte d'identité nationale ou un certificat de naissance⁴⁴. C'est dans ce contexte qu'en juillet 2016, la Conférence des Chefs d'État et de Gouvernement de l'Union africaine a déclaré la période 2017-2026 comme la décennie de repositionnement des systèmes d'enregistrement des faits d'état civil et d'établissement des statistiques d'état civil (CRVS) en Afrique en tant qu'agenda de développement continental, régional et national, et a exhorté les gouvernements à répondre par des actions appropriées.

4 Banque mondiale, Ensemble de données mondiales ID4D 2018 : <https://id4d.worldbank.org/global-dataset>

L'Agenda 2063 : L'Afrique que nous voulons, qui est le cadre stratégique pour le développement socio-économique et la transformation du continent sur une période de 50 ans, a demandé une identité légale pour tous. La Stratégie de transformation numérique pour l'Afrique (STN) approuvée lors de la 36e Session ordinaire du Conseil exécutif de l'Union africaine en février 2020 à Addis-Abeba, en Éthiopie (EX.CL/Déc. 1074(XXXVI)) a également souligné l'importance de l'identité numérique en tant qu'élément constitutif de l'établissement d'un marché unique numérique (une mission qui est également partagée par l'Alliance Smart Africa) conformément à la ZLECAf.

La Stratégie de transformation numérique pour l'Afrique a également reconnu que le développement de l'économie et de la société numériques repose sur des catalyseurs importants, notamment un environnement favorable solide en matière de cybersécurité et de protection des données. La Convention de Malabo de 2014 sur la cybersécurité et la protection des données personnelles⁵ établit un cadre juridique, politique et réglementaire soutenant l'établissement d'un environnement numérique sûr pour les transactions numériques, le commerce électronique et le transfert de données. Malheureusement, ce cadre juridique n'a pas encore été signé et ratifié par le nombre requis d'États membres de l'UA pour qu'il entre en vigueur, ce qui limite effectivement son efficacité⁶⁶. Ce cadre juridique contribuera non seulement à promouvoir la confiance dans le cadre et l'inclusion, mais aussi à atténuer les risques liés à la surveillance non autorisée et à la discrimination, en particulier pour les groupes vulnérables ou marginalisés, ainsi qu'à garantir la responsabilité des instances chargées de la mise en œuvre.

1.2 L'ÉTAT DES SYSTÈMES D'IDENTIFICATION EN AFRIQUE

Les systèmes d'identification fiables et inclusifs sont un catalyseur pour de nombreux résultats de développement tels que l'élimination de la pauvreté, la bonne gouvernance, la migration sûre et ordonnée, la protection sociale, l'égalité des sexes, et finalement jouent un rôle important dans la transformation numérique. Compte tenu du besoin fondamental d'une identification et d'une authentification électroniques sûres et précises, l'identité numérique et les autres services fiduciaires, tels que les signatures électroniques, représentent le nouvel horizon pour les pays du continent. Une fois activés par l'infrastructure numérique qui met les personnes et les organisations en ligne, l'identité numérique et les services fiduciaires peuvent être exploités par les plateformes gouvernementales et commerciales pour faciliter une variété de transactions numériques, y compris les paiements numériques. Au niveau national, l'identité numérique pourrait servir d'identifiant unique pour les systèmes centrés sur le citoyen, ce qui rendrait viable l'intégration des systèmes. Les plateformes d'identité numérique et de paiement permettent d'évoluer vers une société sans numéraire, de réaliser des gains de productivité, de réduire la corruption et la fraude et d'améliorer le confort des utilisateurs.

À travers le continent, il existe un large éventail de types de systèmes d'identification et de niveaux de liens entre le développement et la prestation de services. De nombreux pays se trouvent à des niveaux intermédiaires de développement, avec des lacunes dans la couverture des populations vulnérables et des capacités numériques naissantes, tandis que d'autres n'ont toujours pas de

5 Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, voir : <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

6 En juillet 2021, 14 États membres sur 55 ont signé la convention de Malabo, dont 8 l'ont ratifiée. Pour entrer en vigueur, une ratification par au moins 15 États membres est nécessaire.

systèmes d'identification fondamentaux ou en sont à leurs débuts. Dans l'ensemble, le nombre de pays mettant en œuvre des systèmes d'identification nationaux a augmenté de manière exponentielle au cours des deux dernières décennies, poussés par le désir d'améliorer l'efficacité et le ciblage des paiements et des transferts gouvernementaux, de renforcer l'intégrité du secteur financier (notamment par le biais de KYC (système de gestion de la connaissance du client) et de l'enregistrement des cartes SIM) et celle des élections, de renforcer la sécurité publique et de favoriser une migration sûre et ordonnée. La réforme et la modernisation de la conception du système et des approches de mise en œuvre se poursuivent, conformément à la multiplication des bonnes pratiques et des enseignements tirés des programmes d'identité réussis⁷.

Un bon exemple est fourni par le Rwanda, qui a mené une campagne de numérisation de son économie et d'autonomisation de sa classe moyenne en menant des actions telles que le passage à une économie sans numéraire, que le gouvernement vise à réaliser par une pénétration omniprésente de la téléphonie mobile et un accès à l'Internet à haut débit. Le Rwanda a rejoint l'Alliance Better Than Cash, un partenariat mondial qui s'engage à passer des paiements en espèces aux paiements numériques. Le Rwanda réalise déjà une augmentation de l'efficacité et des revenus en éliminant les coûts de collecte et autres dépenses. Il est également devenu un leader en matière de connaissances dans la région et il partage ses meilleures pratiques avec d'autres pays désireux de suivre une voie similaire (Cadre d'investissement numérique au service des ODD, UTI/DIAL, 2019).

Les capacités numériques des systèmes d'identification se sont considérablement accrues, même si l'identification numérique dans le contexte des transactions en ligne n'en est encore qu'à ses débuts. Au cours de la dernière décennie, de nombreux pays se sont engagés dans des efforts de modernisation de leurs systèmes d'identification, dans le but de créer une plateforme numérique et de délivrer des justificatifs d'identité qui sous-tendent une variété d'utilisations et de services. Ces réformes impliquent fréquemment une transition du papier vers des systèmes numériques utilisant la capture et la gestion électroniques des données, et introduisant pour l'instant des mécanismes de vérification et d'authentification numériques de l'identité, principalement dans le cadre de transactions en personne.

La majorité (85 %) des pays africains disposent de systèmes d'identification nationaux étayés par une base de données électronique, bien que nombre d'entre eux s'appuient encore sur des registres et des processus d'état civil sur papier, et que de nombreux systèmes offrent une utilité limitée pour la prestation de services. Les données biométriques sont collectées par plus de 70 % des pays africains au moment de l'enregistrement afin de garantir l'unicité des identités. Bien que certains pays - comme l'Afrique du Sud, le Kenya, le Lesotho, le Nigeria et le Rwanda - proposent des services de vérification numérique de l'identité (aux ministères, aux banques, etc.) pour valider les informations d'identité ou les justificatifs dans une base de données centrale, l'authentification pour la plupart des transactions continue de reposer sur l'inspection manuelle des cartes d'identité physiques. Les solutions d'identité numérique permettant une authentification sécurisée pour les services et les transactions électroniques n'en sont encore qu'à leurs débuts sur le continent, ces services n'étant disponibles que dans une poignée de pays (ex. : en Afrique du Sud pour les banques, au Cap-Vert, aux Seychelles pour les services d'administration en ligne).

En dépit de nombreuses améliorations et du lancement de nouveaux systèmes ces dernières années, les pays africains et leurs résidents sont confrontés à plusieurs défis en matière d'identification. Parmi les domaines clés qui ont dû être renforcés figurent l'accessibilité des

⁷ Une enquête menée en 2018 auprès de responsables gouvernementaux africains a révélé que 60 % des pays africains prévoyaient de lancer un système d'identification ou de moderniser le système existant d'ici à la fin de 2020.

systèmes d'identification, leur capacité à soutenir efficacement la prestation de services et la mise en œuvre de garanties favorisant la confiance et la confidentialité des données.

Garantir l'accessibilité universelle des systèmes d'identification est un défi permanent. On estime qu'un milliard de personnes dans le monde n'ont pas de documents d'identité de base - et environ la moitié de cette population réside en Afrique⁸. L'Afrique abrite également 8 des 10 pays présentant les plus grands écarts entre les sexes en matière d'identification au niveau mondial et la couverture d'identification des adultes en Afrique subsaharienne est inférieure de près de 10 points de pourcentage chez les femmes par rapport aux hommes⁹. Les problèmes d'identification commencent dès la naissance¹⁰: en Afrique, 100 millions d'enfants de moins de cinq ans n'ont pas été enregistrés à la naissance. Les raisons de ces écarts de couverture sont multiples et comprennent : les coûts directs et (surtout) indirects élevés de l'inscription, y compris le coût des déplacements vers des sites d'enregistrement souvent éloignés, des exigences documentaires et administratives complexes pour l'enregistrement et une demande limitée où les systèmes d'identification offrent une valeur limitée en termes de facilitation de l'accès aux services¹¹.

L'utilisation des technologies modernes a également accru la complexité et présente de nouveaux risques. Par exemple, toutes les solutions ne sont pas bien adaptées aux besoins et contextes locaux où la connectivité à Internet, l'accès à l'électricité ou la culture numérique des fonctionnaires ou de la population en général peuvent être limités. Le verrouillage des fournisseurs est une préoccupation commune, et est souvent associé à des coûts d'exploitation élevés insoutenables, à une interopérabilité limitée du système d'identification et à de faibles niveaux de surveillance et de contrôle des données d'identité par les gouvernements et les particuliers. En outre, avec l'adoption accrue des technologies numériques dans l'identification et l'authentification, ainsi que le passage à des justificatifs numériques, les personnes dont la culture numérique et l'accès aux appareils connectés sont limités risquent d'être laissées pour compte.

Avec la numérisation des systèmes et du traitement des données, la nécessité de mettre en place des garanties efficaces pour protéger les données et la vie privée des personnes s'est également accrue. Des garanties inadéquates en matière de protection des données, de respect de la vie privée et de droits des utilisateurs - qu'elles soient juridiques, institutionnelles ou technologiques - peuvent rendre les systèmes d'identification vulnérables aux violations et laisser les données des personnes sans protection. De nombreux pays ont encore des progrès à faire pour mettre en place des systèmes d'identification sûrs et fiables : selon la CNUCED, seuls 28 pays d'Afrique (50 %) ont adopté une législation sur la protection des données et de la vie privée et 39 (70 %) ont mis en place une législation sur la cybercriminalité¹². En outre, même lorsque de tels cadres existent, il peut être difficile de traduire efficacement les dispositions légales en contrôles institutionnels, opérationnels et techniques. À ce jour, seuls un petit nombre de pays stockent et gèrent leurs données selon les meilleures pratiques internationales pour se protéger contre le vol ou la perte involontaire de données¹³.

8 Ensemble de données mondiales ID4D 2018 : <https://id4d.worldbank.org/global-dataset>

9 <https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf>

10 <https://www.unicef.org/media/62981/file/Birth-registration-for-every-child-by-2030.pdf>

11 <https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf>

12 https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

13 <https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf>

Les systèmes d'identification numérique sont confrontés aux mêmes défis que le développement des écosystèmes numériques. Ces défis englobent notamment les questions de financement, car les cycles de financement, principalement ceux des donateurs qui sont basés sur des projets et limités dans le temps, sont déconnectés des cycles de développement technologique. En outre, la planification en vase clos et la prise de décision entre les groupes de parties prenantes limitent les possibilités de coordination entre eux, ce qui limite la réutilisation des solutions numériques et compromet leur applicabilité potentielle dans les programmes et les secteurs. Les lacunes en matière de culture numérique, à savoir le manque de capacités en matière de leadership dans le domaine des TIC et de sélection, de conception, de mise en œuvre, de mise à l'échelle et de maintenance des solutions TIC, sont souvent un problème pour les gouvernements et les praticiens du développement. Enfin, l'absence de financement pour la mise à l'échelle des solutions TIC est une autre grande préoccupation, dans la mesure où des fonds peuvent généralement être disponibles pour financer les premières étapes du cycle de vie du développement technologique, mais où les fonds disponibles pour la mise à l'échelle au niveau national sont limités (Cadre d'investissement numérique au service des ODD, UTI/DIAL, 2019).

1.3 AUTRES INITIATIVES

Un certain nombre d'initiatives existantes, complémentaires au Cadre, favorisent par ailleurs la reconnaissance mutuelle et l'interopérabilité des identifications numériques en Afrique. Elles comprennent, sans y être limitées :

1.3.1. STRATÉGIE DE TRANSFORMATION NUMÉRIQUE POUR L'AFRIQUE (2020-2030)

L'identité numérique est reconnue comme l'un des cinq thèmes transversaux de la stratégie, qui formule également dix recommandations politiques et propositions d'actions à travers deux thèmes : assurer l'inclusion, la sécurité, la confidentialité et la propriété des données, et soutenir l'interopérabilité et la neutralité. Bien que ces recommandations portent principalement sur le développement de systèmes nationaux d'identité numérique, une recommandation appelle à la création d'une « identité numérique ouverte et interopérable à l'échelle du continent, permettant la validation et l'authentification des personnes », tandis qu'une autre recommandation demande à la CUA, à la CEA et à d'autres partenaires de « collaborer à l'élaboration de normes continentales et régionales, notamment sur les protocoles d'authentification, les champs de données minimums, les protocoles de déduplication, les formats biométriques ainsi que d'autres formats, les réglementations types et d'autres normes ».

1.3.2. INITIATIVE DE LA CEA SUR L'IDENTITÉ NUMÉRIQUE

La Commission économique des Nations Unies pour l'Afrique (CEA) a lancé une initiative sur l'identité numérique, le commerce numérique et l'économie numérique (DITE), faisant office de centre d'excellence, qui vise à harmoniser des normes connexes, à adopter des règlements pour garantir la sécurité, à augmenter les investissements et à développer les capacités et les compétences des acteurs clés¹⁴. Le Centre d'excellence numérique de la CEA soutient les travaux visant à établir un cadre continental africain d'identité numérique harmonisé, à définir

14 CEA, DITE pour l'Afrique, voir : <https://www.uneca.org/dite-africa><https://www.uneca.org/dite-africa>

et à façonner des politiques et des normes d'identité numérique, à assurer le développement des capacités des États membres, des communautés économiques régionales et de l'Union africaine. La CEA a produit un livre blanc sur un cadre pour l'interopérabilité numérique par l'établissement d'un cadre de confiance panafricain (PATF).

1.3.3. ALLIANCE SMART AFRICA TRUST (SATA)

Smart Africa est une initiative des chefs d'État africains visant à accélérer le développement socio-économique de l'Afrique en tirant parti des TIC. En 2020, le Bénin a préconisé un projet phare de Smart Africa visant à élaborer le schéma directeur d'identité numérique, soutenu par un groupe de travail comprenant le Rwanda, la Tunisie, l'Union africaine (UA), l'Union internationale des télécommunications (UIT), la Banque mondiale, le réseau Omidyar, la Commission économique des Nations unies pour l'Afrique (CEA), la GSM Association, le Forum économique mondial, la Gesellschaft für Internationale Zusammenarbeit (GIZ) et plusieurs entreprises privées. Ce projet a été adopté par le conseil d'administration de Smart Africa, qui comprend ses 32 États membres, l'UA et l'UIT. Le schéma directeur¹⁵ propose SATA comme plateforme pour faciliter la reconnaissance mutuelle de confiance des identités numériques entre une série d'acteurs par le biais de mécanismes de certification fédérés. Des projets pilotes de SATA devraient avoir lieu au Bénin, au Rwanda, en Tunisie et dans d'autres États membres de Smart Africa. SATA servira de solution agile et adaptable pour permettre l'interopérabilité entre divers systèmes d'identité publics et privés sur le continent. Plus de détails seront disponibles sur sata.smartafrica.org.

1.3.4. PROJET D'IDENTIFICATIONS UNIQUES POUR L'INTÉGRATION RÉGIONALE ET L'INCLUSION EN AFRIQUE DE L'OUEST (WURI)

Le WURI constitue¹⁶ un programme régional qui bénéficie d'un financement de la Banque mondiale pour accroître l'accès aux services dans les États membres de la CEDEAO participants en construisant des systèmes d'identification fondateurs qui sont accessibles à toutes les personnes sur le territoire du pays - sans considération de nationalité ou de statut juridique - et qui sont conçus dans une optique d'interopérabilité transfrontalière pour débloquer l'accès aux services sociaux, sanitaires, financiers et autres à travers les frontières. La Côte d'Ivoire, la Guinée et la Commission de la CEDEAO ont rejoint la phase 1 en 2018, et le Bénin, le Burkina Faso, le Niger et le Togo ont rejoint la phase 2 en 2020. Les principes clés du WURI comprennent l'enregistrement accessible à tous et inclusif, la minimisation des données et les références de base qui sont fournies sans aucun coût à la population.

1.3.5. PROTOCOLE DU MARCHÉ COMMUN DE LA CAE

En vertu de l'article 8 du Protocole, les six États partenaires de la Communauté de l'Afrique de l'Est (CAE) se sont engagés à travailler progressivement à la mise en place « d'un système standard commun de délivrance de documents d'identification nationaux à leurs ressortissants »¹⁷. Cet engagement est étroitement lié à la réalisation d'autres objectifs du Protocole, notamment la libre circulation des marchandises (article 6), des personnes (article 7), de la main-d'œuvre/des

15 Smart Africa, Schéma directeur | Alliance Smart Africa - Identité numérique, octobre 2020, voir : <https://smartafrica.org/knowledge/digital-id/>.

16 Banque Mondiale. Programme d'identification unique pour l'intégration régionale et l'inclusion en Afrique de l'Ouest (WURI). <https://projects.worldbank.org/en/projects-operations/project-detail/P161329> ; <https://projects.worldbank.org/en/projects-operations/project-detail/P169594>

17 https://www.eac.int/images/doc_image_png_NnlwzXikEvuHdytNzkKNVDMScreen%20Shot%202017-06-20%20at%20153445.png

travailleurs (article 10), des services (article 16) et des capitaux (article 24), ainsi que les droits d'établissement et de résidence (articles 13 et 14, respectivement). Les systèmes nationaux d'identification sont toutefois à des stades de développement différents. Néanmoins, dans le cadre de la géométrie variable et à l'initiative des projets d'intégration du corridor nord (NCIP), le Kenya, le Rwanda et l'Ouganda ont commencé en 2014 à reconnaître les cartes d'identité nationales des uns et des autres comme des documents de voyage valables. Dans le cadre du NCIP, il y a eu des discussions pour s'appuyer sur cette initiative pour des cas d'utilisation supplémentaires tels que les services électroniques, mais elles ne se sont pas encore concrétisées. En 2018, la Banque mondiale et le secrétariat de la CAE ont réalisé une étude sur les possibilités de reconnaissance mutuelle des cartes d'identité nationales (NID) au sien de la CAE qui proposait quatre étapes.

1.4. LA SOUVERAINETÉ NUMÉRIQUE ET DES DONNÉES

Avec 55 nations souveraines, l'Afrique compte en effet 55 entités juridiques à prendre en compte. La souveraineté numérique décrit un spectre de différents concepts techniques et réglementaires, allant de l'emplacement physique des serveurs à la construction de câbles sous-marins, en passant par les lois et pratiques relatives à la protection des données et à la taxation des marchés de données, qui permettent aux États de prendre leurs propres décisions sur les choix technologiques et leur réglementation.

Dans le but de garantir la souveraineté numérique et des données¹⁸, les États membres de l'UA sont encouragés à :



Mettre en place des systèmes de stockage sécurisés pour les données à caractère personnel (y compris les données sensibles) en concevant et en créant des centres de données nationaux qui devront permettre le contrôle des données par l'État et comprendre au minimum de l'espace de stockage et de traitement dédiés exclusivement aux données à caractère personnel et sensibles. Il sera également nécessaire de mettre en place les garanties requises (techniques, en particulier) pour s'assurer que les données utilisées dans les échanges d'informations transfrontaliers ne comprennent en aucun cas des données à caractère personnel ou sensibles dont le traitement ou le stockage présenterait des risques graves pour les droits des personnes ou la souveraineté des États membres de l'UA.



Renforcer les capacités et les infrastructures pour le développement des talents et des compétences africaines afin de relever les nouveaux défis et de renforcer la souveraineté numérique. Les États membres sont censés prendre l'initiative de faire progresser les compétences (y compris les compétences en matière de cyber-résilience) de tous les citoyens et résidents, et devraient donner aux gens les moyens de contrôler leurs données personnelles.

¹⁸ L'expression "souveraineté en matière de données" utilisée dans le présent Cadre a la signification suivante : les données à caractère personnel (y compris les données sensibles) liées aux systèmes d'identification numérique dans un État membre de l'UA doivent être collectées, stockées et traitées (i) dans des installations détenues ou contrôlées par l'État membre de l'UA et (ii) conformément au droit applicable de cet État,



Établir un partenariat basé sur le respect mutuel, une situation gagnant-gagnant sans compromettre la souveraineté et la propriété nationale et éviter les interférences étrangères qui pourraient affecter négativement la sécurité nationale, les intérêts économiques et les développements numériques des États membres de l'UA.

Le Cadre sera guidé par les règles souveraines représentées par la ou les autorités d'enregistrement et de délivrance de l'identité de chaque État membre de l'UA, ainsi que par la structure de gouvernance, y compris la création d'une institution de coordination continentale de surveillance qui sera approuvée par les États membres de l'UA. En outre, les mécanismes de responsabilité, y compris le traitement des obligations en cas de faute, seront définis et approuvés par les États membres de l'UA. Le développement de la confiance à l'échelle du continent entre des États souverains dotés de systèmes d'identification numérique divergents est une tâche complexe mais réalisable, qui nécessite la collaboration de plusieurs parties prenantes. Afin de parvenir à l'interopérabilité pour l'échange d'informations sur l'identité légale dans les différents pays africains, les points communs entre les règles et normes nationales existantes doivent être reconnus, sur la base d'un ensemble minimal de critères qui permettront à la fois la souveraineté locale et une confiance suffisante dans l'approche de chacun.

Les États membres de l'UA doivent à cette fin renforcer et améliorer leurs cadres légaux et leurs capacités d'exécution, en particulier les capacités des autorités chargées de la protection des données à surveiller les transferts transfrontaliers de données et à faire appliquer les lois et règlements pertinents en cas de violation ou d'utilisation abusive.

Le Cadre proposé englobera les technologies de pointe et respectera les lois et réglementations des pays. Les gouvernements ne devraient pas être obligés d'utiliser des technologies spécifiques. L'utilisation de normes et de standards ouverts devrait garantir une grande diversité de choix technologiques par les États tout en facilitant l'appropriation et l'interopérabilité par les pays.

2. INTRODUCTION

En 2020, les États membres de l'Union africaine ont adopté la Stratégie de transformation numérique (STN) pour l'Afrique (2020-2030) avec la vision suivante:

Une société et une économie numériques intégrées et inclusives en Afrique qui améliorent la qualité de vie des citoyens africains, renforcent le secteur économique existant, permettent sa diversification et son développement, et assurent une appropriation continentale avec l'Afrique en tant que producteur et pas seulement consommateur dans l'économie mondiale.

La réalisation de cette ambition - ainsi que celle de la ZLECAf - dépend du développement de systèmes d'identification numérique fondamentaux inclusifs et fiables qui permettent à tous les citoyens africains de prouver et de vérifier leur identité légale de manière fiable et sûre lors de transactions en personne et en ligne, et qui permettent aux prestataires de services des secteurs public et privé de reconnaître les pièces d'identité, quel que soit l'endroit d'Afrique où elles ont été émises. Il est important de noter que les systèmes d'identité numérique fondamentaux doivent être conçus de manière à renforcer l'autonomie des personnes, notamment des populations défavorisées et marginalisées. Cela permettra à tous les citoyens africains de participer de manière significative à l'économie et à la société numériques, de débloquent l'accès aux services à l'intérieur des pays et au-delà des frontières, de promouvoir le commerce dans le cadre de la ZLECAf, de renforcer la confiance dans la société et l'économie numériques, et de réduire la fraude et le coût des transactions commerciales.

Il est important de noter que les systèmes d'identité numérique fondamentaux peuvent également soutenir le développement de « piles numériques »¹⁹ plus larges avec des plateformes de paiement numérique et de partage de données fiables afin de créer des opportunités d'innovation et un large éventail de transactions sans présence, sans papier et sans argent liquide sur le continent. Cependant, cela nécessite également une atténuation complète des risques liés à l'exclusion, à la protection des données, à la cybersécurité et au verrouillage des technologies et des fournisseurs. C'est pour ces raisons que l'identité numérique est l'un des cinq thèmes transversaux de la STN, fournissant le mandat et la base du présent Cadre.

2.1. VISION, OBJECTIFS ET CAS D'UTILISATION INDICATIFS

La vision du Cadre d'interopérabilité des systèmes d'identité numérique de l'UA est que toutes les citoyens africains en Afrique peuvent accéder facilement et en toute sécurité aux services dont ils ont besoin, quand ils en ont besoin, auprès de fournisseurs des secteurs public et privé, ce qui encouragera une participation inclusive et significative dans l'économie et la société numériques au sens large et de permettre permettra aux services de fonctionner avec une plus grande confiance et certitude.

¹⁹ Dans le contexte des technologies numériques, une « pile » constitue un ensemble de composants logiciels ou d'infrastructures indépendants qui fonctionnent ensemble pour permettre l'exécution d'un cas d'utilisation.

Dans cette optique, le Cadre définit des exigences communes, des règles minimales, des normes, des mécanismes de gouvernance, ainsi qu'un alignement entre les cadres juridiques, avec les objectifs de:

1. Permettre aux citoyens africains de vérifier leur identité légale hors ligne et en ligne pour accéder aux services des secteurs public et privé dans tous les États membres de l'UA participants en contribuant à l'accélération des progrès vers l'unité et l'intégration continentales pour assurer une croissance soutenue, promouvoir le commerce, les échanges de biens et de services, la libre circulation des personnes et des capitaux par la création d'une Afrique unie et l'accélération de l'intégration économique par le biais de la ZLECAf, comme indiqué dans l'aspiration 2 de l'Agenda 2063;
2. Donner aux citoyens africains le contrôle de leurs données personnelles, y compris la possibilité de ne divulguer que les attributs requis pour une transaction particulière;
3. Renforcer la confiance et l'interopérabilité entre les systèmes d'identification fondamentaux des États membres de l'UA.

Le Cadre n'appelle pas à la création d'un système continental unifié d'identification numérique mais fournit une base pour l'interopérabilité entre les systèmes d'identification numérique existants des États membres de l'UA, qui prend en compte la souveraineté numérique des États membres de l'UA, les divergences dans la mise en œuvre de l'infrastructure numérique, la disponibilité des politiques et réglementations associées, les différents niveaux des systèmes d'identification et la vulnérabilité des populations pendant et après la mise en œuvre des systèmes d'identification numérique.

Il est primordial que ce Cadre soit développé conformément aux meilleures pratiques et aux normes internationales²⁰ visant à protéger les données personnelles, à maintenir la cybersécurité et à sauvegarder les droits des personnes. Avec l'adoption de la Convention de Malabo sur la cybersécurité et la protection des données personnelles et le travail en cours pour développer un cadre continental de politique des données²¹, l'Union africaine a pris une mesure importante pour établir un environnement numérique crédible pour les transactions en ligne via l'adoption d'un ensemble commun de règles pour régir le transfert transfrontalier des données personnelles sur le continent et l'alignement des cadres nationaux de protection des données et de cybersécurité.

Un cadre continental peut faciliter **l'accès aux services dans tous les pays participants en permettant aux personnes et aux entreprises** de vérifier les justificatifs d'identification et d'autres faits sans divulguer de données personnelles. Cela inclut la possibilité d'authentifier leur identité lorsqu'ils accèdent à des services en ligne (ex. : services gouvernementaux) dans un autre pays avec leur identité numérique sans avoir besoin de s'inscrire aux solutions d'identité fondatrices locales reconnues par les prestataires de services étrangers. L'interopérabilité des identités numériques facilitent également le partage et le consentement pour des références vérifiables et des données fiables lors de la demande de services où la loi exige une telle vérification (ex. : preuve d'assurance, statut de vaccination), permettant aux gens de gagner du temps et de réduire la paperasserie.

20 Il s'agit notamment de l'UIT-T X.1058, de l'ISO/IEC 29151, des principes et recommandations des Nations unies pour les systèmes de statistiques de l'état civil, des dix principes de l'identification pour le développement durable, des normes internationales sur la protection des données, du règlement général européen sur la protection des données, etc.

21 Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, voir : <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

Elle peut également **renforcer l'intégrité et l'accessibilité des paiements transfrontaliers et des services financiers en Afrique, et créer des opportunités d'innovation**. Les systèmes d'identification faibles et non fiables, l'absence d'harmonisation des règles créent des risques de blanchiment d'argent et de lutte contre le financement du terrorisme (AML/CFT),²² qui entravent les échanges transfrontaliers, augmentent les coûts des services (ex. : les transferts de fonds) et freinent l'innovation. L'identité numérique peut faciliter l'identification et la vérification des clients lors de l'intégration, soutenir les processus de la connaissance du client et faciliter le suivi des transactions dans le but de détecter et de signaler les transactions suspectes. L'interopérabilité permettra non seulement aux migrants d'envoyer plus facilement de l'argent chez eux en allégeant la vérification de la connaissance du client et la charge d'authentification, mais elle contribuera également à réduire les coûts, aidant ainsi l'Afrique à se rapprocher de la cible de l'ODD (10.c) de 3 % d'ici 2030.

Un Cadre continental peut également **renforcer le commerce et le commerce électronique en augmentant la confiance dans les transactions commerciales électroniques et en facilitant les affaires et le commerce à travers l'Afrique**. En 2020, le commerce intra-africain ne représentait approximativement que 16,6 % du PIB de l'Afrique²³. La ZLECAf a été lancé en 2019 afin de débloquent de nouvelles opportunités pour les échanges commerciaux et le commerce électronique d'ici 2030. La reconnaissance transfrontalière des pièces d'identité numériques peut contribuer à renforcer les contrôles d'identité des acheteurs et des vendeurs, en particulier pour les biens soumis à restrictions vendus en ligne. Elle peut également permettre des signatures électroniques pour des transactions 100 % en ligne et sans papier, ce qui permet aux entreprises et aux clients de gagner du temps et de renforcer la sécurité en réduisant les risques d'usurpation d'identité. Elle simplifie également le commerce transfrontalier en permettant aux entreprises de gérer numériquement leur interaction avec les pouvoirs publics, par exemple en déclarant des taxes, en participant à des procédures de passation de marchés, en requérant un numéro de TVA et en demandant des autorisations.

2.2. CHAMP D'APPLICATION

Pour atteindre ces objectifs, le Cadre définira :

- le **type d'informations/données** qui peuvent être partagées sous la forme d'un ensemble minimal de données pour les informations d'identité fondamentales²⁴;
- la **manière de prouver qui a émis les données** et qu'elles sont dignes de confiance;
 - établir un processus pour communiquer les sources autorisées fiables pour les données d'identité dans chaque État membre de l'UA;
 - déterminer la manière dont vérifier l'authenticité du renseignement numérique;
- les normes et processus qui décrivent **comment les données sont partagées** par les utilisateurs et vérifiées par d'autres dans un environnement hors ligne et en ligne.

22 Les risques AML/CFT font référence aux risques de blanchiment d'argent et de financement du terrorisme. Le FATF recommande aux gouvernements de mettre en place une approche multipartite intégrée pour comprendre les opportunités et les risques liés à l'identification numérique et pour élaborer des réglementations et des conseils afin d'atténuer ces risques.

23 CNUCED, Rapport sur le développement économique en Afrique 2019: Made in Africa : Des règles d'origine pour un commerce intra-africain renforcé, voir : <https://unctad.org/press-material/facts-figures-0>

24 Bien que le champ d'application de ce document se concentre sur les données d'identité, le cadre de confiance proposé peut être étendu par les États membres de l'UA pour représenter d'autres preuves et réalisations, comme les diplômes, les qualifications professionnelles, etc.

Ce document présente les fondements d'un cadre de confiance et d'interopérabilité des systèmes d'identification numérique sur le continent africain. Il définit les exigences minimales nécessaires pour assurer l'interopérabilité entre les systèmes d'identité numérique existants et futurs. L'interopérabilité désigne la capacité des différentes parties du Cadre - telles que les systèmes d'identité numérique et les systèmes des parties intéressées - à communiquer et à s'interfacer efficacement aux niveaux technique et sémantique. L'interopérabilité peut faciliter la reconnaissance mutuelle, ce qui représente une construction juridique, mais elle n'est pas une condition préalable et ne garantit pas la reconnaissance mutuelle. Le Cadre ne définit pas un système d'identification numérique unifié pour l'Afrique et ne traite pas des accords commerciaux et de responsabilité entre les États membres participants.

De nombreux pays africains disposent déjà de systèmes d'identification numérique bien établis et certains ont introduit des capacités d'authentification numérique. **Le Cadre fournit des exigences communes pour la communication des données et des processus d'identité fondamentaux qui seraient interopérables et acceptés dans d'autres États membres africains, tandis que les États membres conservent le plein contrôle et le choix pour la conception de leurs systèmes nationaux.**

Le Cadre complétera et s'appuiera sur, plutôt que de dupliquer, les activités associées au Protocole au Traité instituant la Communauté économique africaine relatif à la libre circulation des personnes, au droit de résidence et au droit d'établissement, et à la Conférence des ministres africains chargés de l'enregistrement des faits d'état civil et au Programme africain pour amélioration accélérée des systèmes CRVS (APAI-CRVS). La mise en œuvre du Cadre doit être étroitement coordonnée avec cette initiative et d'autres initiatives pertinentes, notamment pour étudier la migration en tant que cas d'utilisation supplémentaire des cartes d'identité numériques au moment opportun et pour veiller à ce que la couverture et la qualité des systèmes CRVS soient améliorées en tant que contribution importante aux systèmes d'identification numérique de base.

2.3. CADRE DE CONFIANCE, CONFIDENTIALITÉ DES DONNÉES, INTEROPÉRABILITÉ ET NORMES

Les systèmes d'identité doivent favoriser la confiance entre les différentes parties participantes, en veillant à ce que les droits légaux des utilisateurs individuels et des organismes d'exploitation soient respectés, et à ce que l'utilisation éthique des systèmes d'identité soit encouragée. **Pour garantir cette confiance, il convient de définir un ensemble de règles auxquelles toutes les parties adhèrent et qu'elles respectent**, à savoir un Cadre de confiance.

Si la technologie constitue un élément clé, les cadres de confiance se concentrent également sur les processus et les procédures. Un cadre de confiance solide doit définir clairement:

- **les exigences commerciales** (ex. : champ d'application, services fournis, exigences en matière de participation) ;
- **les exigences techniques** (ex. : formats de données, interfaces, normes);
- **les exigences opérationnelles** (ex. : le fonctionnement de la preuve d'identité et de l'authentification, le support, les communications); et
- **les exigences juridiques** (ex. : niveaux de service, responsabilité, résolution des litiges, reconnaissance de la légalité des transactions électroniques dans les pays) pour le système d'identité.

Le Cadre est fondé sur l'interopérabilité. Pour faciliter l'interopérabilité, une entité doit pouvoir faire confiance à une autre entité en se basant non seulement sur l'intégrité des processus techniques (ex. : preuve cryptographique, etc.), mais aussi sur la provenance des données partagées (ex. : les processus de collecte et d'attribution d'un certain enregistrement à un individu).

L'interopérabilité n'exige pas que les systèmes d'identification fondamentaux soient uniformes, mais simplement que certaines normes communes et ouvertes soient respectées. En vertu de ce Cadre, chaque pays participant peut créer des systèmes d'identification fondamentaux adaptés aux besoins, aux traditions et à la législation locaux, à condition que certaines normes permettant l'interopérabilité soient respectées. Les normes ouvertes établissent des protocoles d'échange, des régimes d'essai, des mesures de qualité et des bonnes pratiques universellement compris et cohérents concernant la saisie, le stockage, la transmission et l'utilisation des données d'identité légale, ainsi que le format et les caractéristiques des justificatifs d'identité légale et des protocoles d'authentification.

Lors de l'examen de l'interopérabilité des justificatifs d'identité numérique et de l'authentification sur le continent, il sera important d'envisager des normes ouvertes pour les renseignements d'identité, la manière dont elles sont émises et la manière dont la confiance est communiquée entre les entités impliquées dans le Cadre de confiance. Ces renseignements, qui formeront la base de l'identité numérique légale, proviendront souvent de sources faisant autorité, telles que les agences gouvernementales. Un mécanisme d'authentification doit également être défini pour permettre aux détenteurs d'une identité numérique légale de partager ces renseignements avec les fournisseurs de services de manière appropriée, en veillant à ce que la divulgation des données soit binaire et que toute métadonnée soit masquée, et à ce que la vie privée et les droits des personnes soient protégés à tout moment.

Ce Cadre définira **la manière dont la confiance peut être établie dans ces renseignements vérifiables, et le fonctionnement des éléments de gouvernance et des normes pour les données**. La mise en œuvre technique de la solution peut être pilotée par le marché qui pourra s'appuyer sur le cadre de confiance pour développer des solutions innovantes d'identification numérique fondatrice. Le Cadre place la confidentialité, l'audit et la protection des données au premier plan et établit une procédure transparente applicable à toutes les parties utilisatrices concernées sur la façon dont les données sont demandées, collectées, transmises et stockées et qui respecte des normes bien acceptées sur la procédure de partage des informations/données. L'importance de la tokenisation pour réduire les possibilités de collecte de données, de clonage et de fraude, en présentant au détenteur de l'identité la possibilité d'émettre des identités virtuelles, ce qui permet de protéger les identités réelles, est un aspect supplémentaire qui sera approfondi pour renforcer la confidentialité des données au niveau national/continental.

3. LE CADRE

Le Cadre d'interopérabilité des systèmes d'identification numérique de l'UA propose de définir, au niveau continental, une approche harmonisée permettant aux individus de partager avec les fournisseurs de services des preuves d'identité numérique²⁵ délivrées par des autorités de confiance, afin de prouver leur identité légale dans un environnement en ligne et hors ligne. Il s'agira de convenir d'une **norme commune pour représenter les preuves d'identité légale existantes délivrées par les États membres de l'UA dans un format numérique**²⁶. L'authenticité de ces justificatifs d'identité²⁷ pourrait être vérifiée afin de garantir un niveau élevé de confiance et de sécurité.

Les systèmes nationaux d'identité fondamentaux ne sont soumis à aucune restriction quant à leur mode de fonctionnement ou aux types d'informations d'identification qu'ils utilisent pour authentifier les personnes ; chaque pays est souverain à cet égard. L'intention du Cadre est de créer les conditions de l'interopérabilité à l'échelle continentale en s'appuyant sur les systèmes existants là où ils existent et plutôt que de restreindre leur utilisation, d'étendre leur portée.

Les justificatifs d'identité numérique interopérable (IDC-ID) émises conformément au Cadre de l'UA prendront la forme d'un renseignement vérifiable qui viendra compléter les systèmes d'identification nationaux fondamentaux existants et les projets de coopération régionale, sans remplacer les systèmes d'identification numérique nationaux des États membres de l'UA. **Les États membres de l'UA restent libres de choisir la manière dont ils souhaitent délivrer ce justificatif d'identité numérique.** Il peut être stocké dans un format purement numérique sur une application smartphone, un serveur en nuage, une carte à puce ou un lien vers la représentation numérique qui peut être établi à l'aide d'un code-barres à une ou deux dimensions sur un document papier (imprimé sur papier, carte plastique).

Le Cadre sera fondé sur le développement de systèmes d'identification interopérables, inclusifs et fiables, car ils constituent l'épine dorsale des sources de données faisant autorité sur l'identité légale des personnes et permettent ainsi à l'IDC-ID d'atteindre des niveaux d'assurance plus élevés. Les États membres de l'UA sont ainsi encouragés à renforcer leurs systèmes d'identification, ainsi que les principes d'identification pour le développement durable. Des solutions alternatives pour obtenir un IDC-ID pour les personnes qui sont actuellement exclues d'un système d'identification peuvent être envisagées.

Les normes relatives à une identité numérique légale interopérable pourraient être utilisées au niveau national ou soutenir des cas d'utilisation transfrontaliers. Par exemple, la norme pourrait être adoptée pour:

- représenter les données d'identité numérique fondamentales au niveau national sur les justificatifs d'identité numérique nouvellement émis ou mis à jour ; ou
- représenter les données d'identité numérique fondamentale au niveau continental ou de la CER ;

²⁵ Les renseignements constituent un ensemble d'attributs concernant une personne concernée, comme le nom de famille ou la date de naissance. Un renseignement vérifiable est une version inviolable de ces informations qui peut être vérifiée de manière cryptographique afin d'en contrôler l'authenticité.

²⁶ Le cadre actuel se concentre sur la définition de renseignements vérifiables pour prouver des données d'identité, mais il pourrait être étendu pour partager des renseignements vérifiables sur des réalisations académiques, des qualifications professionnelles, etc...

²⁷ Un justificatif est composé d'un renseignement d'identité, de métadonnées sur l'émetteur et d'une preuve d'authenticité qui est généralement une signature numérique.

- être émise séparément en complément des systèmes d'identification numérique fondamentaux préexistants.

Les éléments d'interopérabilité, de confiance et d'inclusion définis dans ce cadre constituent une rampe de lancement pour un cadre continental plus complet et une infrastructure pour l'identification et l'authentification numériques sur le continent.

3.1. PRINCIPES DIRECTEURS

Les principes suivants guident la mise en œuvre de l'interopérabilité transfrontalière du cadre:

1. Transparence de la gouvernance et du fonctionnement.
2. Facilement accessible, rentable, financièrement et opérationnellement durable et largement utilisable.
3. Promotion du respect et la défense des droits de l'homme et de la liberté²⁸.
4. Assurance de l'intégrité technique, y compris une identité unique, sûre, évolutive et précise.
5. Garantie de la souveraineté des États membres et assurance que la souveraineté des données, notamment les données d'identité numérique, appartient à l'Afrique et reste sous son contrôle.
6. Interopérabilité entre les États membres de l'UA.
7. Utilisation de normes ouvertes²⁹ et prévention du verrouillage des fournisseurs et des technologies.
8. Protection de la vie privée des données numériques et possibilité pour les personnes de contrôler leurs données personnelles, y compris la proportionnalité des données par la conception du système.
9. Protection de la confidentialité des données, de la sécurité et des droits grâce à un cadre juridique et réglementaire complet.
10. Définition de mandats et de responsabilités institutionnels clairs.

Compte tenu du fait que le Cadre dépend de sources faisant autorité, comme les systèmes d'identification légaux, la qualité et la couverture de ces systèmes ont un impact sur sa mise en œuvre. L'exclusion de ces systèmes et d'autres défis tels que la faiblesse de la sécurité, par exemple, se traduiront par la même situation en termes de capacité à délivrer et à utiliser correctement les justificatifs d'identification.

Les États membres de l'UA doivent en conséquence s'acquitter de leur obligation de veiller à ce que toutes les personnes présentes sur leur territoire aient accès à une identification légale, conformément à la Convention relative aux droits de l'enfant et aux autres instruments juridiques internationaux et régionaux. En outre, ils sont également fortement encouragés à adhérer aux normes³⁰ et principes³¹ internationaux pertinents existants et à veiller à ce que

28 Conformément à la Charte africaine (Banjul) des droits de l'homme et des peuples (adoptée le 27 juin 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entrée en vigueur le 21 octobre 1986)

29 Normes ouvertes désignent des normes mises à la disposition du grand public et sont développées (ou approuvées) et maintenues via un processus collaboratif et consensuel. Les « normes ouvertes » facilitent l'interopérabilité et l'échange de données entre différents produits ou services et sont destinées à être largement adoptées (adoptées de l'UIT-T).

30 Il s'agit notamment de la convention de Budapest sur la cybercriminalité, des principes et recommandations de la CEI, de l'ISO et de l'UIT-T pour les systèmes de statistiques de l'état civil, des normes internationales sur la protection des données (telles que le règlement général européen sur la protection des données et la convention 108+ du Conseil de l'Europe), des normes mondiales et régionales et des cadres de confiance pour l'identification.

31 Par exemple, les dix principes d'identification pour le développement durable, qui ont été approuvés par 30 organisations internationales et régionales, dont des institutions africaines telles que la CEA, la BAD et Smart Africa, et adoptés par un certain nombre de pays africains (voir <https://id4d.worldbank.org/principles>), et les principes du développement numérique, qui ont été approuvés par plus de 200 organisations (voir <https://digitalprinciples.org/>).

les sources d'autorité, et en particulier leurs systèmes d'identification légale, soient inclusifs, protègent les données et les droits des personnes, et soient conçus pour soutenir l'intégration économique et sociétale du continent.

3.2. MODÈLE DE MISE EN ŒUVRE

Le Cadre proposera une mise en œuvre en trois phases:

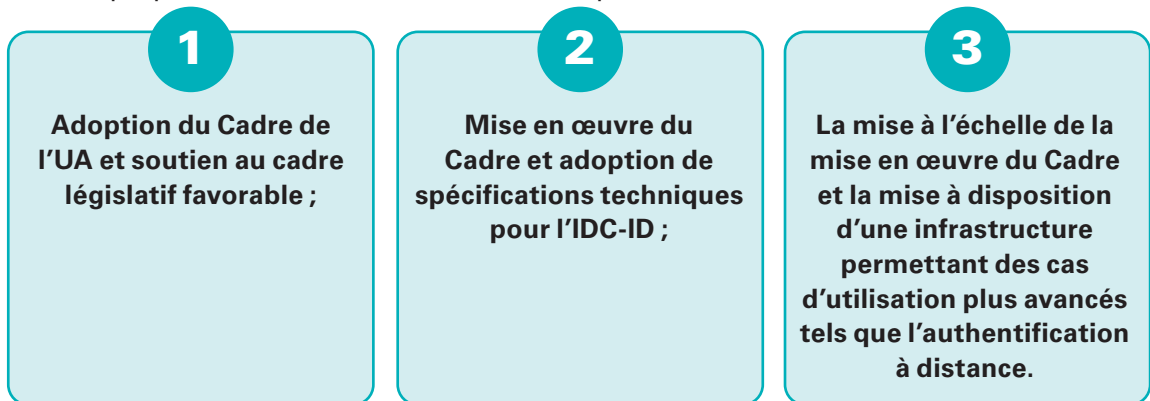
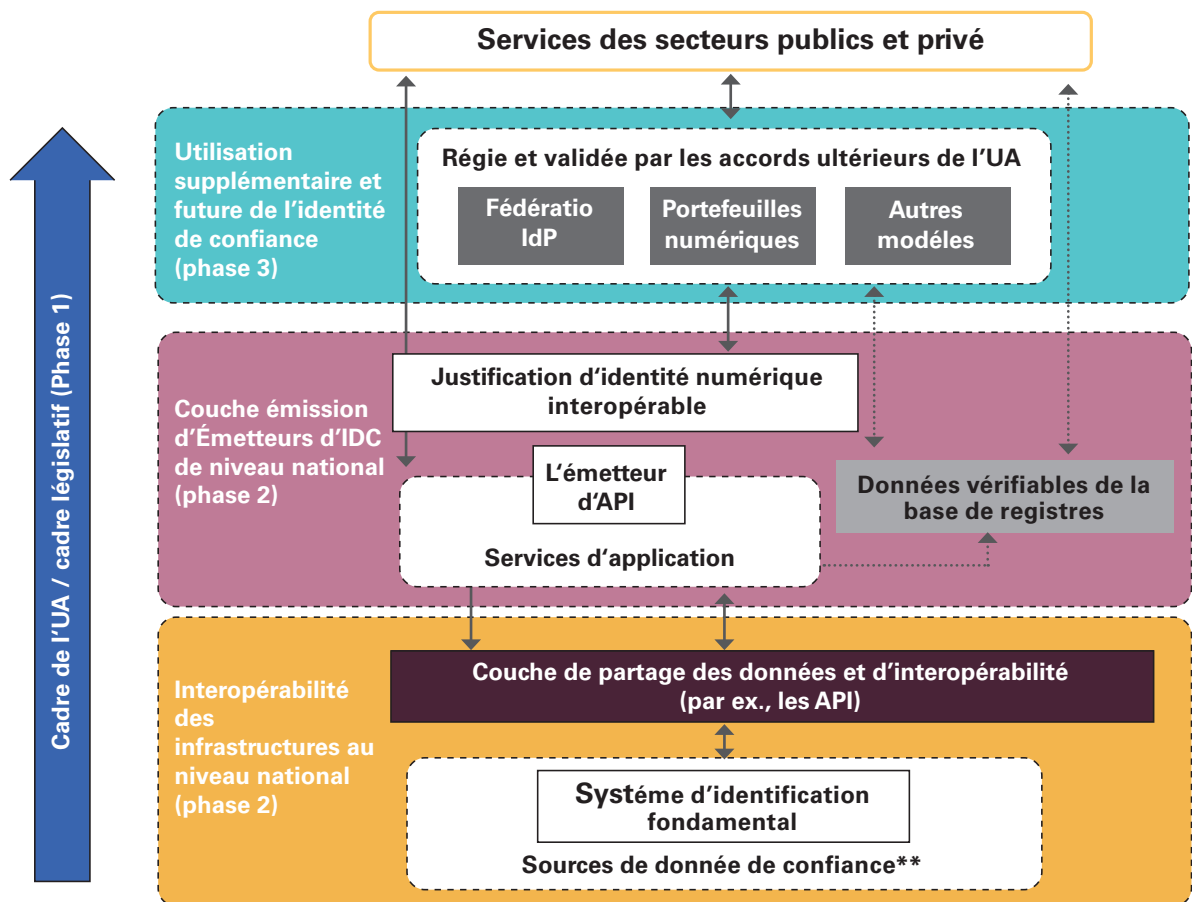


FIGURE 1 – APPROCHE DE LA MISE EN ŒUVRE DU CADRE PAR ÉTAPES



* Les détails de la mise en œuvre de la phase 2 seront discutés plus avant avec les États membres de l'UA.

** Les États membres décideront de ce que les sources de données fiables impliquent dans leurs systèmes d'identification

L'IDC-ID garantit que **l'autorité émettrice ne sait pas à quels services les individus accèdent avec leur ID** numérique, mais l'authenticité des justificatifs d'identité peut être vérifiée. Cela offre des garanties en termes de protection des données et de la vie privée et permet à l'individu de mieux contrôler l'utilisation de ses données.

La couche infrastructure permettra des cas d'utilisation plus avancés et consistera à lier les justificatifs d'identité émises dans le format IDC-ID aux personnes réelles. Plusieurs options techniques sont à la disposition des États membres de l'UA pour mettre en œuvre cette couche, qui pourrait être composée d'une fédération de fournisseurs d'identité offrant des mécanismes d'authentification aux détenteurs de l'IDC-ID ou le développement de solutions de portefeuilles d'identité numérique ou tout autre modèle permettant l'interopérabilité. Chacune de ces mises en œuvre peut offrir une approche de minimisation des données et des services de divulgation sélective pour des cas d'utilisation spécifiques, par exemple ne partager que les points de données pertinents d'une carte d'identité et d'un dossier de crédit pour obtenir un prêt, demander des prestations sociales ou de santé, obtenir une pension, demander des bourses d'études ou anonymiser l'ensemble de données minimum de l'IDC-ID (nom, date de naissance) en une preuve de majorité (+18 ans ou +21 ans ou une réponse oui/non).

3.2.1. COMPOSANTS DE L'ARCHITECTURE

Les sources de données fiables doivent répondre aux normes fixées par le cadre de l'UA en matière de qualité et d'intégrité des données. Dans de nombreux cas, ces normes seront remplies par un système d'identification fondamental (dont les sources de données fiables seront décidées par les États membres) qui peut fournir une preuve d'identité légale.

La figure 1 illustre l'extension de l'accès aux systèmes nationaux existants et aux sources de données fiables par le biais d'une couche de partage de données et d'interopérabilité fondée sur des normes et des protocoles permettant la délivrance d'IDC fiables. Les fournisseurs de services vérifient et récupèrent les données d'identité légale lors de la création justificatifs d'identité numérique fondamentale.

La couche d'émission d'IDC représente l'émission normalisée d'un justificatif d'identification basée sur une source de données fiable d'un système d'identification fondamental/national. Chaque émetteur de documents d'identité (au moins un par État membre participant) aura un certain nombre de fonctions clés (non limitées aux suivantes):

- une API de l'émetteur qui permet aux portefeuilles et autres systèmes de demander et de récupérer des justificatifs d'identification.
- un registre de données vérifiables qui permet de vérifier les identifiants et de contrôler la révocation des justificatifs d'identification.
- gestion des clés cryptographiques.
- visibilité et vérifiabilité des justificatifs utilisées pour le détenteur d'IDC.
- fourniture de métadonnées de justificatifs d'identification à côté de chaque IDC émis pour décrire la qualité, la provenance et le niveau de confiance associés à l'IDC émis.

3.2.2. NIVEAU NATIONAL ET EXIGENCES D'INTEROPÉRABILITÉ

Il n'est pas nécessaire de remanier les systèmes d'identité existants au niveau national pour réaliser l'interopérabilité au niveau continental. En revanche, des normes pour

l'interopérabilité des données, l'interopérabilité technique via des API et des protocoles, et la représentation technique des justificatifs d'identification seront adoptées. La délivrance de ces identifications et leur création sont séparées des systèmes nationaux existants, mais seraient sous le contrôle d'agences nationales responsables.

La confiance technique, étayée par une cryptographie avancée, peut ne pas nécessiter une infrastructure à clé publique (ICP) continentale ou une autre infrastructure supranationale, mais résulterait plutôt de la préférence et/ou de la capacité des États membres de l'UA à utiliser une ICP nationale (le cas échéant) ou des alternatives légalement reconnues. Chaque État membre de l'UA continuera à exercer sa souveraineté nationale dans la conception des systèmes d'identité nationaux, y compris la manière dont ces systèmes interagissent avec le Cadre de l'UA.

3.2.3. NORMES POUR UNE PARTICIPATION DES SOURCES DE DONNÉES FIABLES

Des normes seront établies selon le Cadre de l'UA pour la qualité, la sécurité, la fiabilité et le niveau minimum d'assurance associé à chaque source de données fiable. Les systèmes des États membres devront fournir la preuve qu'ils ont atteint les exigences minimales de participation avant de pouvoir participer au Cadre de l'UA et de délivrer des justificatifs d'identification conformes à l'IDC. La nature de ces normes sera déterminée par un accord entre les États membres de l'UA.

3.3. PROCESSUS ÉPROUVÉ : LE CADRE DE CONFIANCE

Le Cadre de confiance doit décrire des règles claires pour la participation des entités (ex. : les émetteurs, les détenteurs et les vérificateurs d'identité), le fonctionnement du cadre et les exigences techniques pour l'interopérabilité des informations d'identification fiables.

Toutes les entités pourront ainsi faire confiance aux informations d'identification partagées par les détenteurs d'identité sur la base de la confiance établie par l'autorité émettrice (pour l'information d'identification) et des processus que chaque entité a accepté de respecter dans le cadre de confiance.

Il est prévu que les sections clés suivantes soient rédigées par les États membres en tant que partie intégrante du cadre de confiance.

3.3.1. RÔLES ET RESPONSABILITÉS

Une définition claire de chaque entité (ex. : un émetteur de justificatifs d'identification), et des responsabilités qui lui incombent pour que la confiance soit maintenue, comme la gestion sûre et sécurisée des données et des services, et la notification des incidents.

Les rôles clés qui devraient être inclus dans le cadre de confiance seraient les suivants:

- **Les autorités de confiance** sont des sources de données faisant autorité en matière de preuve d'identité légale, approuvées par les États membres de l'UA.
- **Les émetteurs** sont des entités chargées de délivrer au titulaire la preuve d'identité légale dans le format numérique standardisé conformément au Cadre. Les autorités de confiance peuvent soit délivrer elles-mêmes les justificatifs d'identification, soit mandater une autre entité disposant de compétences plus adéquates (ex. : une agence TIC, le secteur privé).
- **Le détenteur** de l'IDC-ID est la personne qui possède un ou plusieurs justificatifs d'identification numériques. Le détenteur peut être, mais pas toujours, le sujet des attributs d'identité partagés via l'IDC.
- **Le vérificateur** est une partie intéressée (ex. : un fournisseur de services public ou privé) qui souhaite vérifier la déclaration d'identité d'un sujet donné.
- **Les fournisseurs d'identité, les fournisseurs de justificatifs d'identification et les fournisseurs de portefeuilles numériques** peuvent contribuer davantage à l'écosystème en fournissant un authentificateur pour lier l'identité du titulaire aux justificatifs d'identification et permettre ainsi des cas d'utilisation plus avancés nécessitant une authentification à distance.

Un organe de surveillance indépendant, à mettre en place par les États membres, est susceptible d'être nécessaire pour garantir que les entités participantes respectent les règles établies par le Cadre de confiance et définissent les outils et technologies minimaux nécessaires à la conformité. L'organe de surveillance devrait également être chargé de sensibiliser le continent aux compétences en matière de cyber-résilience afin de garantir la durabilité du cadre.

3.3.2. RÈGLES DE PARTICIPATION

Les règles de participation peuvent inclure des exigences légales, opérationnelles ou organisationnelles minimales requises pour une entité de confiance faisant autorité et fournissant un service dans le Cadre de confiance. Par exemple, un émetteur peut être tenu d'avoir un accord officiel pour fonctionner (d'une source autorisée / agence gouvernementale).

Les services acceptant l'IDC-ID peuvent être invités à confirmer leur conformité aux exigences de base en matière de protection des données, de respect de la vie privée et de recours (pour les détenteurs d'identité).

Un protocole d'accord peut également être exigé pour garantir que toutes les entités opérationnelles acceptent les conditions du Cadre de confiance.

3.3.3. GOUVERNANCE

Des mécanismes de gouvernance, à approuver par les États membres de l'UA, seront nécessaires pour établir et maintenir les règles du cadre de confiance, approuver les modifications des exigences d'interopérabilité et déléguer la responsabilité de la conception et de l'élaboration des modifications du cadre à des sous-groupes de gouvernance, le cas échéant.

Un organe de surveillance indépendant, à établir par les États membres de l'UA, est susceptible d'être nécessaire pour garantir que les entités participantes restent conformes aux règles établies par le Cadre de confiance. Cet organisme devrait également être chargé de veiller à ce que toutes les parties respectent formellement les normes et, en cas d'écart, fassent l'objet d'un audit ou soient amenées à rendre des comptes si nécessaire, par exemple en cas de violation de données.

La protection des personnes devrait être primordiale. L'organe de surveillance devrait être habilité à recevoir et à traiter les plaintes des titulaires d'IDC-ID victimes de mauvaises pratiques, de violations de données, d'usurpation d'identité ou d'autres incidents liés à l'identité numérique. Il devrait également être le point de convergence des mécanismes de recours, même s'il ne s'agit que d'un rôle de coordination, et devrait se faire le défenseur des individus et de leurs droits.

3.3.4. EXIGENCES D'INTEROPÉRABILITÉ

3.3.4.1. NIVEAU D'ASSURANCE

Un moyen de communiquer le niveau de confiance accordé à un justificatif d'identification présenté par un titulaire à un vérificateur. Le Cadre doit définir les conditions dans lesquelles chaque niveau de confiance peut être atteint en fonction de la vérification de l'identité par une source faisant autorité, du processus de délivrance, et des moyens de détenir et de présenter un justificatif d'identité.

3.3.4.2. ENSEMBLE MINIMAL DE DONNÉES

La quantité minimale de données concernant l'identité d'un titulaire, telle qu'elle est fournie dans un justificatif d'identité, doit être suffisante pour permettre l'identification de la personne dans la majorité des transactions courantes, tout en respectant la nécessité de minimiser les données. Les attributs contenus dans l'ensemble minimal de données peuvent être fournis par différentes entités de confiance.

L'organe directeur est libre de définir la manière dont des renseignements supplémentaires (ensembles de données) peuvent être inclus de manière facultative dans le Cadre de confiance. Toute délivrance des justificatifs d'identification correspondants doit être soumise aux mêmes conditions et règles que les émetteurs des justificatifs d'identité fondamentaux.

3.3.5. EXIGENCES TECHNIQUES

3.3.5.1. SÉCURITÉ

Des exigences de sécurité de base doivent être définies pour chaque entité fournissant un service dans le cadre de l'infrastructure d'identité.

3.3.5.2. PREUVE CRYPTOGRAPHIQUE

Les justificatifs d'identité seront vérifiés par l'inclusion d'une signature numérique créée par l'autorité émettrice. La vérification de la validité de la signature constitue une preuve cryptographique de la crédibilité de la déclaration faite par le titulaire du justificatif d'identification. Pour vérifier une signature numérique, une clé publique est nécessaire. La clé publique peut être fournie par une méthode décentralisée ou centralisée à déterminer dans le Cadre de confiance et ses exigences techniques.

3.3.5.3. FORMAT DES JUSTIFICATIFS D'IDENTITÉ

Les spécifications techniques pour la création et la transmission des justificatifs d'identité doivent être définies en s'inspirant des normes existantes telles que les « Verifiable Credentials » (justificatifs vérifiables) du W3C, le cas échéant.

- **Le justificatif numérique interopérable d'identité (IDC-ID)** est un ensemble de renseignements d'identité légaux (ex. : des attributs) et de relations faites par un émetteur qui peuvent être vérifiées de manière cryptographique. Il comprend plus particulièrement
 - des métadonnées de justificatif concernant le type de justificatif délivré, la date de délivrance, le nom de l'émetteur ;
 - des informations sur le sujet du justificatif et le justificatif d'identité légal réel (ex. : la date de naissance) ;
 - une preuve d'authenticité qui est généralement une signature numérique.

Le détenteur de l'IDC-ID est capable de générer des présentations vérifiables d'un ou plusieurs IDC-ID de manière que l'authenticité du justificatif puisse toujours être vérifiée (ex.: divulgation sélective).

3.4. OPTIONS D'AUTHENTIFICATION POTENTIELLES

Plusieurs approches architecturales peuvent être adoptées pour permettre au détenteur de l'IDC-ID d'être authentifié à un niveau d'assurance donné. Toutes les options suivantes peuvent coexister et être mises en œuvre à différents niveaux de coopération (ex. : entre des acteurs sectoriels spécifiques ou au niveau des CER).

En fonction de la disponibilité d'autres technologies dont les pratiques de mise en œuvre ont fait leurs preuves, d'autres options pourront être explorées.

3.4.1. PORTEFEUILLES NUMÉRIQUES PERSONNELS

Cette option consiste à fournir aux particuliers et aux entreprises un portefeuille numérique personnel contenant des attributs de preuve vérifiable d'identité légale qui peuvent être utilisés pour prouver l'identité d'une personne ou partager des faits spécifiques avec un fournisseur de services. Cette option d'architecture fait référence aux cas d'utilisation des Verifiable Credentials (justificatifs vérifiables) du W3C³².

³² W3C, Verifiable Credentials Use cases, voir : <https://www.w3.org/TR/vc-use-cases/>.

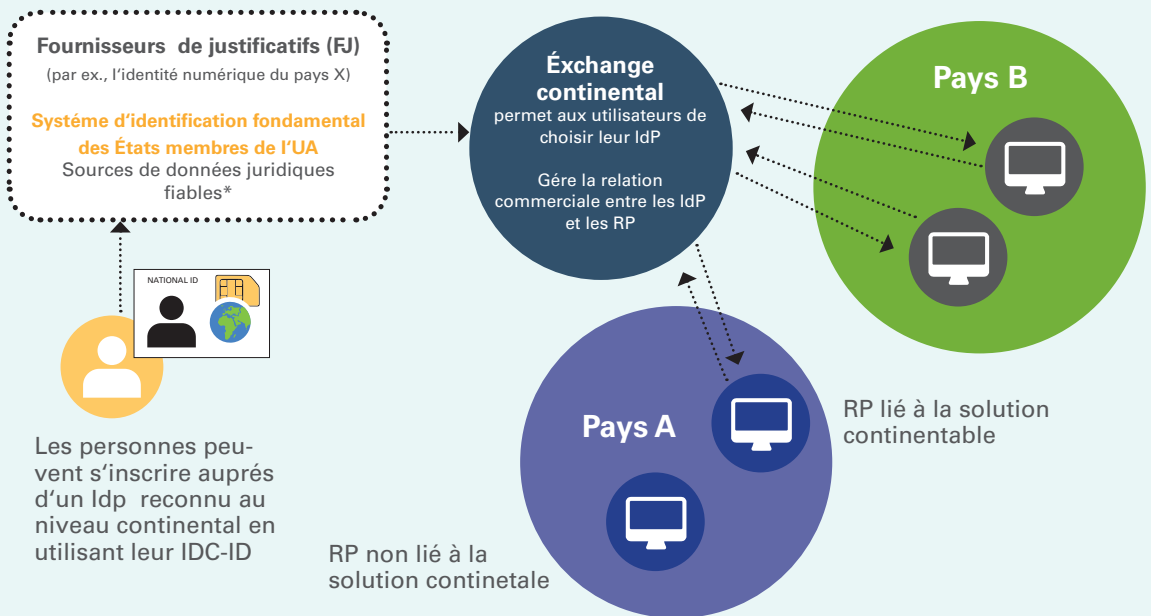
FIGURE 2 – VUE DE L'OPTION 1 - PORTEFEUILLES NUMÉRIQUES PERSONNELS



3.4.2. OPTION 2 - FÉDÉRATION CONTINENTALE D'IDENTITÉS NUMÉRIQUES

Dans le cadre de ce modèle, chaque résident africain pourrait s'inscrire auprès d'un fournisseur de justificatifs d'identité de niveau continental de son choix.

FIGURE 3 – VUE DE L'OPTION 2 - FÉDÉRATION CONTINENTALE D'IDENTITÉS NUMÉRIQUES



*Les États membres décideront quelles sources de données fiables impliquent dans leurs systèmes d'identification fondamentaux.

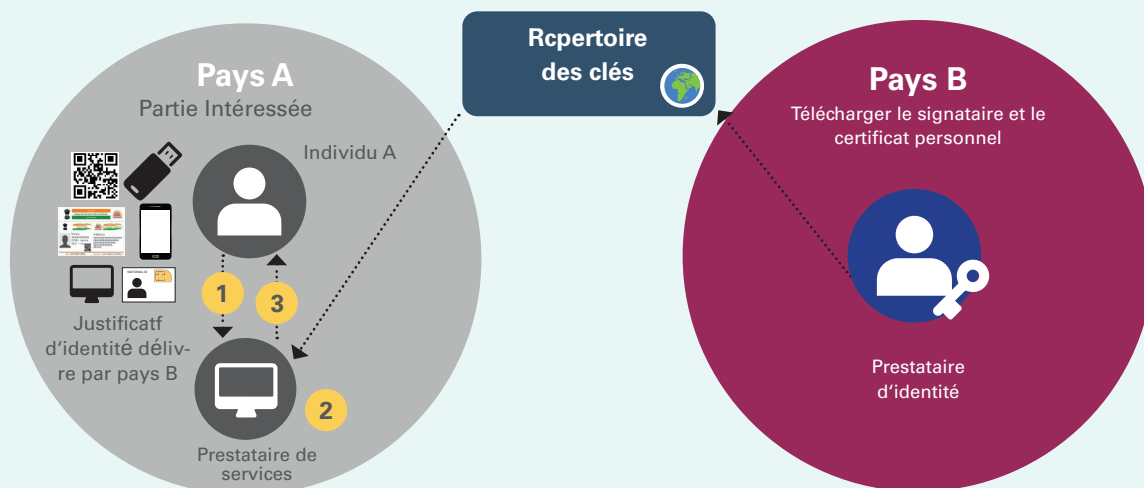
PROCESSUS D'AUTHENTIFICATION

1. **Une fédération continentale de fournisseurs de justificatifs (FJ) d'identité est établie** : opérateurs de télécommunications, banques, gouvernements, etc... peuvent fournir des services d'authentification.
2. **Un échange continental** est créé, fournissant un point de contact unique pour tous les fournisseurs de justificatifs participants et les parties intéressées qui veulent authentifier des personnes.
3. **Les personnes peuvent utiliser leur IDC délivré par une source faisant autorité (par ex., ex. : un système d'identification légal) pour s'inscrire auprès du fournisseur de justificatifs de leur choix.** Le FJ peut vérifier l'authenticité de l'IDC.
4. Si la vérification est réussie, le FJ délivre un moyen d'authentification au particulier.
5. La personne peut utiliser son moyen d'authentification pour **accéder aux services en ligne et en personne** qui sont connectés à l'échange continental.

3.4.3. OPTION 3 - JUSTIFICATIFS D'IDENTITÉ À SIGNATURE NUMÉRIQUE

Ce modèle permet l'authentification en vérifiant les données d'identité légale signées numériquement sur un justificatif d'identité avec une clé publique, ainsi qu'un moyen supplémentaire de partager la photo du titulaire.

FIGURE 4 – VUE DE L'OPTION 3 - JUSTIFICATIFS D'IDENTITÉ À SIGNATURE NUMÉRIQUE



PROCESSUS D'AUTHENTIFICATION

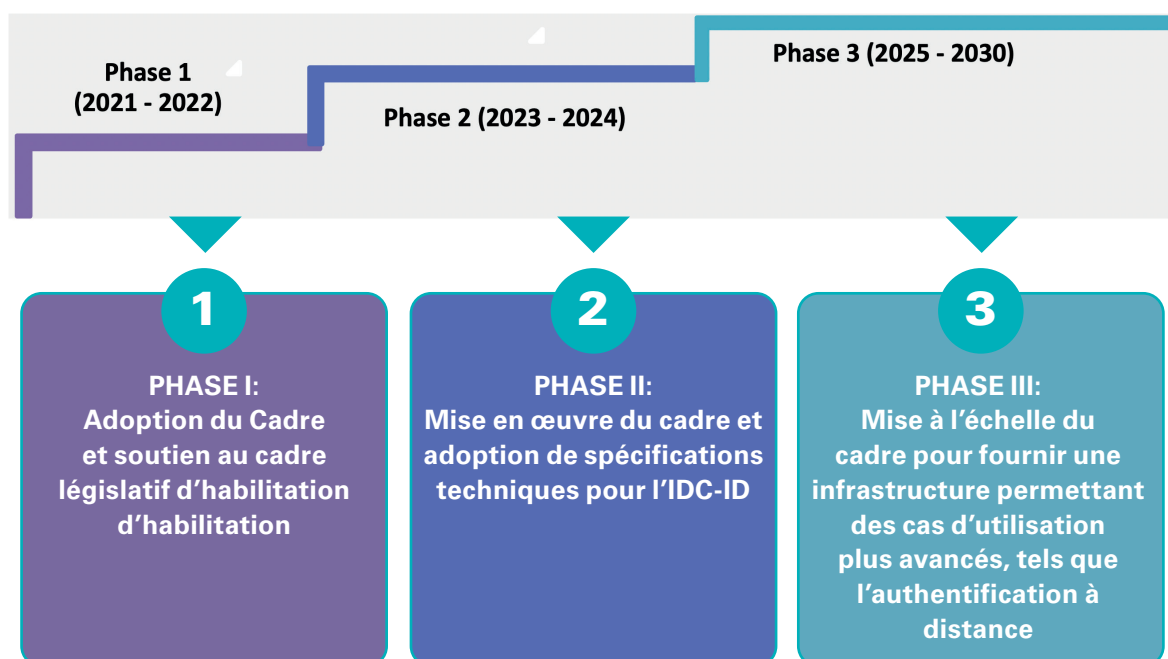
1. Les pays se mettent d'accord sur une norme (par ex., ex. : un code QR) et les sources émettrices signent de manière cryptographique les justificatifs (via une clé privée).
2. Les sources autorisées partagent leur clé publique dans un répertoire de clés publiques (RCP) dont la gouvernance sera approuvée par les États membres de l'UA et gérée au niveau continental.
3. Les pays créent un service distinct permettant de partager une copie de la photo du titulaire de l'IDC-ID accessible via une API sécurisée afin d'authentifier le titulaire. Pour travailler hors ligne, il est également possible pour un groupe de pays (par ex., ex. : les CER) de se mettre d'accord sur l'émission d'un justificatif physique contenant une photo du titulaire³³.
4. Les sources autorisées des pays délivrent des formes normalisées d'IDC aux personnes.
5. **Un logiciel de vérification** (application ou site web) est créé pour permettre aux fournisseurs de services de vérifier l'authenticité et l'intégrité de la signature sur l'IDC.
6. Les personnes peuvent utiliser leur IDC pour faire vérifier numériquement leur identité légale par des parties intéressées publiques ou privées dans leur pays ou à l'étranger et **accéder à des services**.
7. Chaque État membre sera tenu de conserver dans un espace de stockage sécurisé, tel qu'un module matériel de sécurité (HSM), les clés privées, les certificats personnels et les algorithmes de hachage à utiliser pour le cryptage et la vérification de l'intégrité.

33 La délivrance de justificatifs physiques a un coût supplémentaire. Les États membres participants devront discuter plus avant du financement de cette solution afin de ne pas créer d'obstacles à l'accès.

4. FEUILLE DE ROUTE DETAILLÉE POUR LA MISE EN ŒUVRE

Pour accélérer la voie vers la réalisation des objectifs ambitieux de ce Cadre, les États membres de l'UA doivent intensifier leur collaboration pour affiner les détails du cadre technique et de référence, des normes et du processus communs.

La proposition consiste à diviser la mise en œuvre du Cadre en trois phases, comme le montre le schéma ci-dessous:



Pour chaque phase, des possibilités de consultation des États membres de l'UA, de la société civile et des parties prenantes de l'écosystème de l'identité seront prévues afin de garantir que le Cadre et sa mise en œuvre restent alignés sur les besoins des personnes et des contextes locaux. La documentation clé sera publiée et offrira une fenêtre de temps adéquate pour les contributions.

4.1. PHASE 1 : ADOPTION DU CADRE ET ENVIRONNEMENT FAVORABLE

Présentation du projet de Cadre à la 4ème session ordinaire du CTS sur la Communication et les TIC pour adoption et entérinement par les organes délibérants.

Après l'approbation du présent document, les détails du cadre Cadre de confiance seront précisés, et les activités suivantes seront menées, notamment notamment :

- Sensibilisation sensibilisation ;
- Étude étude de faisabilité sur le paysage actuel du système d'identification numérique en Afrique ;
- Mise mise en place d'un cadre de consultation des acteurs de l'écosystème numérique visant à préserver l'intérêt de chaque acteur ;
- La mise en place d'instruments juridiques et réglementaires harmonisés ;
- Mise mise en place des mécanismes de gouvernance et d'un forum pour partager les meilleures pratiques tout au long du processus de mise en œuvre œuvre ;
- Les définition des dispositions juridiques qui devront être intégrées dans les environnements juridiques nationaux des États membres de l'UA afin de mettre en œuvre le Cadre, y compris les garanties appropriées en matière de cybersécurité et ainsi que la ratification de la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel personnel ;
- L'adoption du cadre politique continental sur les données. ;
- La nomination de groupes d'experts par les États membres de l'UA pour définir l'interopérabilité et les exigences techniques. ;
- La mise en place de structures institutionnelles indépendantes au niveau national (autorités chargées de la protection des données, autorités de certification du contrôleur et équipes de réponse aux incidents informatiques(CIRT) ;
- Mettre développement en place des d'initiatives de renforcement des capacités ;
- soutenir soutien de la mise en place d'une infrastructure numérique, y compris des centres de données aux niveaux national, régional et continental, nécessaire pour soutenir et maintenir l'opérationnalisation des systèmes d'identification numérique numérique ; et
- Mobilisation mobilisation des ressources.

Afin d'assurer le succès du Cadre, une série de cas d'utilisation représentant les plus grandes opportunités pour le continent sera définie. Un groupe d'États membres de l'UA pourra ensuite collaborer pour tester et piloter des cas d'utilisation spécifiques, avec d'autres parties prenantes si nécessaire.

Une évaluation des principaux coûts et avantages du cadre proposé et des options d'authentification ultérieures devrait être réalisée afin de fournir une plus grande visibilité sur les besoins de financement pour éclairer la prise de décision des États membres de l'UA. En ce moment, on s'attend à ce que la conformité à une norme harmonisée pour représenter les informations d'identité engendre des coûts limités pour les États membres de l'UA, car elle pourrait être intégrée comme une exigence technique aux projets de numérisation existants de leurs systèmes d'identification fondamentaux. En revanche, la mise en place de l'infrastructure d'authentification devrait générer des coûts supplémentaires et, selon les types de parties prenantes concernées, elle nécessite la définition de modèles économiques. Concernant cette phase, une analyse d'impact détaillée devra être réalisée afin de s'assurer que les options d'authentification proposées restent inclusives.

Les États membres de l'UA s'engagent également à:

- Élaborer élaborer et mettre en œuvre des cadres juridiques et réglementaires harmonisés qui renforcent la confiance dans les systèmes d'identification numérique fondamentaux ;
- Élaborer élaborer une législation et une réglementation harmonisées en matière de données personnelles qui renforcent les capacités des individus, tout en préservant la souveraineté des données ;
- Mettre déployement en place de l'infrastructure numérique, y compris l'infrastructure de données (centres de données nationaux), qui constitue la base de la mise en œuvre du système d'identification numérique. ;
- De ratifier la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel (si cela n'a pas encore été fait), d'accélérer son entrée en vigueur et de travailler à l'accélération de la mise en place d'autorités de protection des données chargées de la surveillance dans les pays participants participants ;
- Élaboration de élaborer la stratégie nationale de cybersécurité et mise mettre en place d'es équipes de réponse aux incidents informatiques (CIRT) afin d'atténuer les risques et les menaces liés aux cyberattaques, au vol de données et à la mauvaise manipulation l'utilisation abusive d'informations sensibles ;
- Adopter adopter le cadre de la politique continentale de l'UA en matière de données ;, qui demande que les systèmes d'identification numérique soient élaborés et mis en œuvre de manière cohérente, conformément à un cadre général de gouvernance des données garantissant que la combinaison et la réutilisation des données administratives publiques qu'impliquent les systèmes d'identification numérique s'effectuent avec des garanties appropriées. Ces politiques devraient donner aux individus les moyens d'agir et protéger la vie privée en ligne en tant que droit fondamental (y compris le choix et le contrôle de l'utilisateur, le consentement éclairé/manifeste, la souveraineté/la propriété des données, etc. ;)
- Lancer lancer et/ou intensifier les efforts visant à renforcer les systèmes d'identification fondamentaux, afin de s'assurer qu'ils sont inclusifs et fiables, conformément aux normes et initiatives pertinentes telles que le Programme africain pour amélioration accélérée des systèmes d'enregistrement des faits d'état civil et des statistiques de l'état civil (APAI-CRVS) et les principes Principes d'identification pour le développement durable.
- Ces phases seront finalisées avec l'adoption de la version complète du Cadre par les États membres de l'UA.

4.2. PHASE 2 : MISE EN ŒUVRE DU CADRE ET ADOPTION DES SPÉCIFICATIONS TECHNIQUES DE L'IDC-ID

La deuxième phase consistera à établir le cadre Cadre de confiance et les mécanismes de gouvernance et de coopération et, ainsi qu' à fournir la spécification technique pour la mise en place de l'IDC-ID qui inclura entre autres autres :

- Élaborer l'élaboration des normes et des règles minimales pour l'interopérabilité ;
- Profils l'attribution de profils d'attribution pour l'ensemble minimal de données (formats de données) et les métadonnées associées associées ;
- Présentation la présentation du format (par ex. : codes à barres 2d2D, justificatifs vérifiables W3C) ;
- Niveau le niveau d'assurance (comme point de référence pour l'interopérabilité) ;
- Éléments des éléments de cryptographie pour la signature et le cryptage des données ; et
- Protocoles des protocoles de vérification pour les cas d'utilisation en ligne et hors ligne

Un exemple de mise en œuvre (application ou site web) pour la vérification de base de l'IDC-ID sera conçu par un groupe d'États membres de l'UA afin de tester l'interopérabilité des justificatifs d'identité et de prendre déjà en charge les preuves vérifiables de l'identité légale. La mise en œuvre permettra de garantir la confidentialité et la sécurité dès la conception.

Un accord sur la définition de **solutions alternatives pour obtenir un IDC-ID** pour les personnes qui sont actuellement exclues de tout système d'identification fondamental sera envisagé.

Une cartographie des autres initiatives de l'Union africaine en cours qui pourraient s'appuyer sur le cadre sera réalisée (par ex., ex. : le cadre continental africain des qualifications).

La phase 2 sera conclue par la mise en place d'un plan d'action clair pour la définition de l'infrastructure d'authentification dans le cadre de la phase 3.

4.3. PHASE 3 : DÉVELOPPEMENT DE L'INFRASTRUCTURE POUR PERMETTRE L'AUTHENTIFICATION À DISTANCE

La Phase 3 commencera à mettre en œuvre le cadre Cadre de confiance défini en phase 2.

La couche qui représente la délivrance de l'IDC-ID, pourra être achevée dans une deuxième phase par une infrastructure permettant des cas d'utilisation plus avancés tels que l'authentification à distance. Cette couche d'authentification permettra aux individus de prouver leur identité numériquement en exerçant le contrôle d'un ou plusieurs facteurs d'authentification (par ex., ex. : un code biométrique ou PIN) liés à leur identité légale préalablement vérifiée, à savoir l'IDC-ID.

Plusieurs options techniques sont à la disposition des États membres de l'UA pour mettre en œuvre cette couche, par exemple : la mise en place d'une fédération de fournisseurs d'identité fournissant des mécanismes d'authentification aux détenteurs de l'IDC-ID, ou le développement de solutions de portefeuille d'identité numérique ou tout autre modèle permettant l'interopérabilité. Chacune de ces mises en œuvre peut offrir une approche de minimisation des données et des services de divulgation sélective pour des cas d'utilisation spécifiques, tels que le partage des points de données pertinents d'une carte d'identité et d'un dossier de crédit pour l'obtention d'un prêt, la demande de prestations sociales ou de santé, l'obtention d'une pension, lorsque l'authentification est légalement requise ou l'anonymisation de l'ensemble minimal de données de l'IDC-ID (par ex., ex. : le nom, la date de naissance) dans une preuve de majorité (+18 18 ans ou +21 21 ans ou une réponse oui/non).

Les États membres de l'Union africaine pourront également trouver un accord supplémentaire sur la manière d'établir cette infrastructure de couche d'authentification et s'associer aux CER et à d'autres initiatives continentales qui étudient déjà la mise en place de solutions interopérables d'identification numérique pour accéder à des services à distance. En effet, les États membres et les organisations seront en mesure de tirer parti de la représentation commune, basée sur des normes, des informations relatives à l'identité dans un format numérique fiable et sécurisé, et de créer des services supplémentaires sur cette base.

Les États membres de l'UA poursuivront leur collaboration pour renforcer le cadre de confiance et les mécanismes de gouvernance et de coopération faisant suite à l'accord sur les infrastructures supplémentaires, de la manière suivante :

- **coordination avec d'autres initiatives** visant à établir l'interopérabilité au niveau continental (par ex., ex. : SATA et les CER).
- **accord sur la meilleure option architecturale** (par ex. : fédération, portefeuilles numériques, etc.) pour développer la fonction d'authentification à distance qui s'appuierait sur les justificatifs numériques interopérables (IDC-ID).

La phase 3 sera conclue par un plan d'action clair sur la mise en œuvre de la couche d'authentification selon l'option architecturale à convenir entre les États membres de l'UA et les institutions.

5. HYPOTHÈSES, DÉFIS ET RISQUES MAJEURS

5.1. HYPOTHÈSES

Les États membres adopteront le cadre, collaboreront, s'engageront à mettre en œuvre et à prendre réaliser les réformes juridiques et réglementaires nécessaires et requises.

5.2. DÉFIS GÉNÉRAUX ET MESURES D'ATTÉNUATION IMPORTANTES PROPOSÉES

Le tableau ci-dessous décrit les défis généraux et les mécanismes d'atténuation proposés.

#	Défis	Atténuations proposées
1	Exclusion, faiblesse de la sécurité et érosion de la protection des données personnelles.	Appliquer les principes définis dans le Cadre (3.1) et renforcer les cadres juridiques et les infrastructures de sécurité et de protection des données dans les États membres de l'UA.
2	Réticence des États membres de l'UA à adopter et à mettre en œuvre le cadre.	Sensibiliser aux avantages du cadre d'interopérabilité aux niveaux national et continental et renforcer le système d'identification fondamental.
3	Manque de capacités techniques et financières des États membres de l'UA	Renforcer les capacités et promouvoir les échanges de connaissances entre pairs parmi les États membres de l'UA, et examiner la rentabilité des solutions technologiques à convenir dans le cadre des phases 2 et 3.
4	Centres de données inadéquats aux niveaux national/régional/continental	Construire des centres de données nationaux/ régionaux/continentaux et promouvoir leur utilisation en Afrique.

5.3. RISQUES ET MESURES D'ATTÉNUATION PROPOSÉES

Le tableau ci-dessous décrit les risques et les mécanismes d'atténuation proposés.

#	Risques	Atténuations proposées
1	Absence de définition correcte de la norme commune, manque de compréhension de la part des États membres de l'UA et incapacité à suivre et à adopter les normes communes.	<p>Définition de normes et communication de celles-ci aux États membres de l'UA pendant la mise en œuvre et suivi régulier par un organisme panafricain fiable et habilité, soutenu et approuvé par tous les États membres de l'UA pour garantir le respect des normes.</p> <p>Discussions et ateliers ciblés avec les parties prenantes pour garantir une définition claire des normes pour la stratégie de mise en œuvre choisie.</p> <p>Comparaison de la stratégie de mise en œuvre standardisée de l'État membre de l'UA avec des programmes nationaux d'identification fondamentaux similaires dans les États membres de l'UA.</p>
2	Les faibles niveaux de confiance entre les autorités nationales, dont les capacités de mise en œuvre sont hétérogènes, entraînent une lente adoption du cadre à l'échelle continentale. En outre, la réticence des États membres à accepter un organe de surveillance supranational ralentit la mise en œuvre du cadre Cadre de confiance.	Le Cadre devrait viser l'harmonisation et la reconnaissance mutuelle comme objectif à long terme, mais rester ouvert à l'élaboration de solutions souples et agiles, qui pourraient créer des mécanismes d'audit partagés entre les pays désireux d'établir la confiance entre eux tout en restant souverains - par la reconnaissance unilatérale des certificats de confiance émis.
3	La solution, les avantages et les options ne sont pas bien adaptés à l'environnement local ou l'information est mal diffusée et les personnes n'utilisent pas la solution, ce qui entraîne une faible adoption et, en fin de compte, des coûts élevés avec peu d'avantages.	<p>Développer de solides structures de conception centrées sur l'utilisateur afin d'identifier des solutions faciles à utiliser et accessibles à tous ;</p> <p>Développer de solides mécanismes de diffusion dans les États membres de l'UA, qui intègrent tous les acteurs locaux partageant les mêmes idées.</p>

<p>4 Les États membres décideront de la technologie appropriée pendant la phase de mise en œuvre, mais s'ils optent pour la technologie ICP, absence d'institution de certification au niveau continental et manque de gouvernance adéquate des exigences cryptographiques pour la signature numérique qui s'avère être un obstacle à la mise en place du système d'interopérabilité.</p>	<p>Création d'un cadre juridique permettant l'établissement d'une institution de coordination au niveau continental, soutenue par une structure de gouvernance équitable tenant compte de la souveraineté de chaque État membre pour la mise en œuvre et la gestion des signatures numériques, leur émission, leur révocation, leur remplacement et leur mise à jour en temps voulu.</p> <p>Création d'une structure organisationnelle détaillée et dynamique pour permettre la gouvernance de l'infrastructure de signature numérique / ICP tout au long de la phase de mise en œuvre et d'opération.</p>
<p>5 En raison de données incorrectes et incomplètes, la conception et la stratégie de mise en œuvre de certains composants d'interopérabilité, tels que les signatures numériques, peuvent être affectées. Un retard dans le partage des données et des informations pertinentes des citoyens ou des résidents pourrait également avoir un impact sur les délais du projet.</p>	<p>Réunions avec les agences gouvernementales pour la collecte de données relatives à la mise en œuvre des lacunes en matière d'information, en tirant parti de l'expérience des experts par l'apprentissage entre pairs pour encourager la collaboration et l'appropriation régionale et continentale. Suivi des délais et des étapes du projet pour éviter les retards. Il est également impératif d'avoir un calendrier de mise en œuvre détaillé et complet qui a été convenu par les États membres de l'UA et les principales parties prenantes.</p>
<p>6 Absence de lignes directrices clairement définies en matière de gestion du changement pour garantir que le cadre reste aligné sur les pratiques, les besoins et le développement technologique actuels :</p>	<p>Mettre en place un processus de gestion du changement solide et bien défini dans le cadre de la gouvernance.</p>

7	Les États membres décideront de la technologie appropriée pendant la phase de mise en œuvre, mais s'ils optent pour la technologie ICP, les agences de certification en Afrique peuvent ne pas parvenir à un consensus concernant la gestion de l'ICP au niveau du déploiement à l'échelle du continent. Deuxièmement, il n'y aura pas forcément de consensus sur la mise en place d'un échange de signatures numériques.	Les États membres de l'UA peuvent soit créer une nouvelle institution de certification pour la gestion de l'ICP au niveau du continent, soit approuver un mécanisme permettant de réunir les agences existantes sur une plateforme commune.
8	L'absence d'un environnement juridique minimum favorable aux niveaux national et régional.	Les États membres de l'UA sont tenus d'accélérer la mise en œuvre des cadres juridiques et réglementaires harmonisés requis.

6. ANNEXE

6.1 DÉFINITIONS PRATIQUES

Attribut désigne une qualité ou une caractéristique nommée inhérente ou attribuée à quelqu'un ou quelque chose (adapté de NIST 800-63 :2017). Dans les systèmes d'identification, les attributs d'identité courants comprennent le nom, l'âge, le sexe, le lieu de naissance, l'adresse, les empreintes digitales, la photo, la signature, le numéro d'identité, etc.

Authentification désigne le processus qui permet d'établir la confiance dans le fait qu'une personne est bien celle qu'elle prétend être. L'authentification numérique implique généralement qu'une personne présente électroniquement un ou plusieurs « facteurs » pour « affirmer » son identité, c'est-à-dire pour prouver qu'elle est la même personne que celle à laquelle l'identité ou le justificatif a été initialement délivré. Ces facteurs peuvent inclure un élément que la personne connaît (par ex., ex. : un mot de passe ou un code PIN), possède (par ex., ex. : une carte d'identité, un jeton ou une carte SIM mobile) ou est (par ex., ex. : ses empreintes digitales) (adapté de NIST 800-63 :2017 et OWI 2017).

Autorisation désigne le processus qui consiste à déterminer quelles actions peuvent être réalisées ou quels services peuvent être accédés sur la base de l'identité affirmée et authentifiée (Nyst et al. 2016).

Source faisant autorité : la source faisant autorité en matière d'informations d'identité désigne un référentiel ou un système qui contient des attributs sur un individu et qui est considéré comme la source primaire ou la plus fiable pour ces informations. Dans le cas où deux ou plusieurs systèmes ont des données non concordantes ou contradictoires, les données de la source de données faisant autorité sont considérées comme les plus précises (FICAM, non daté).

Renseignements désigne qualification, réalisation, qualité ou élément d'information sur les antécédents d'un sujet, comme un nom, une pièce d'identité officielle, une adresse personnelle ou un diplôme universitaire. (Adapté adapté du W3C).

Consentement de la personne concernée désigne toute indication librement donnée, spécifique, informée et non ambiguë de la volonté de la personne concernée par laquelle celle-ci, par une déclaration ou par un acte positif clair, manifeste son accord au traitement des données à caractère personnel la concernant.

Justificatif désigne un document, un objet ou une structure de données qui garantit l'identité d'une personne par une méthode de confiance et d'authentification. Les types courants de justificatifs d'identité comprennent, sans s'y limiter, les cartes d'identité, les certificats, les numéros, les mots de passe ou les cartes SIM. Dans le cas de ce cadre, le justificatif est une déclaration vérifiable appelée IDC-ID.

Responsable du traitement des données désigne toute personne physique ou morale, publique ou privée, toute autre organisation ou association qui, seule ou conjointement avec d'autres, décide de collecter et de traiter des données à caractère personnel et en détermine les finalités.

Protection des données régit la manière dont les données sont utilisées ou traitées et par qui, et elle garantit aux citoyens des droits sur leurs données. Elle est particulièrement importante pour garantir la dignité numérique, car elle permet de remédier directement au déséquilibre de pouvoir inhérent entre les « personnes concernées » et les institutions ou les personnes qui ont collecté les données.

Autorités de protection des données (APD) sont des autorités publiques indépendantes qui contrôlent et supervisent, grâce à des compétences d'enquête et de correction, l'application de la loi sur la protection des données. Elles fournissent des conseils d'experts sur les questions de protection des données et traitent les plaintes qui pourraient avoir enfreint la loi.

Souveraineté des données, dans le présent Cadre, fait référence aux données personnelles (y compris les données sensibles) liées aux systèmes d'identification numérique dans un État membre de l'UA, qui doivent être collectées, stockées et traitées (i) dans des installations détenues ou contrôlées par l'État membre de l'UA et (ii) en vertu du droit applicable de ce dernier.

Personnes concernées désignent toute personne physique qui fait l'objet d'un traitement de données à caractère personnel.

Dignité numérique (dans le contexte de l'identification numérique) désigne le fait que l'identité humaine qui se cache derrière l'identification numérique bénéficie d'une certaine confidentialité et que ses données sont protégées.

Système d'identification numérique (ID) désigne un système d'identification qui utilise 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, ainsi que la vérification et l'authentification de l'identité (adapté du rapport de coopération public-privé ID4D).

Identité numérique désigne un ensemble d'attributs et/ou d'informations d'identification saisis et stockés électroniquement qui identifient une personne de manière unique (adapté de Harbitz & Kentala 2013 et du rapport ID4D Technology Landscape).

Signature numérique désigne une opération à clé asymétrique où la clé privée est utilisée pour signer numériquement les données et la clé publique est utilisée pour vérifier la signature. Les signatures numériques assurent une protection de l'authenticité, de l'intégrité et de la non-répudiation, mais pas de la confidentialité (NIST 800-63 :2017).

Pile numérique, dans le contexte des technologies numériques, est un ensemble de composants de logiciels ou d'infrastructures indépendants qui fonctionnent de pair pour soutenir l'exécution d'un cas d'utilisation.

Système d'identification fondamental désigne un système d'identification créé principalement pour gérer les informations relatives à l'identité de la population générale et fournir des justificatifs qui servent de preuve d'identité afin d'accéder à des services publics et privés tels que l'éducation, les soins de santé, la protection sociale et les services financiers, etc. (adapté de Gelb & Clark 2013a et de diverses publications ID4D). Aux fins du présent Cadre, les États membres de l'UA décideront quelles sources de données fiables correspondent à leurs systèmes d'identification fondamentaux.

Systèmes d'identification fonctionnels désignent un système d'identification créé pour gérer l'identification, l'authentification et l'autorisation pour un service ou une transaction particulière, comme le vote, l'administration fiscale, les programmes et transferts sociaux, les services financiers, etc. Les justificatifs d'identité fonctionnels - tels que les cartes d'électeur, les dossiers de santé et d'assurance, les numéros d'identification fiscale, les cartes de rationnement, les permis de conduire, etc. - peuvent être communément acceptés comme preuve d'identité à des fins plus larges que leur objectif initial, en particulier lorsqu'il n'existe pas de système d'identification fondamental (adapté de Gelb & Clark 2013a et de diverses publications ID4D).

Harmonisation consiste à assurer l'uniformité des systèmes par l'utilisation de normes minimales pour faciliter l'interopérabilité et de cadres juridiques et de confiance (par ex., ex. : pour les niveaux d'assurance) pour fixer des règles et instaurer la confiance dans les systèmes respectifs.

ID désigne un justificatif d'identité ou un document d'identité dans certains domaines.

Système d'identification (ID) désigne les bases de données, les processus, la technologie, l'infrastructure, les justificatifs d'identité et les cadres juridiques associés à la saisie, à la gestion et à l'utilisation des données d'identité personnelles dans un but général ou spécifique (adapté des Principes d'identification).

Identification désigne le processus d'établissement, de détermination ou de reconnaissance de l'identité d'une personne. (Adapté adapté de l'ISO/IEC 24760-1 : 2011 et de l'ITU-T X.1252)

Identité désigne les coordonnées sociales relatives qui distinguent un individu d'un autre. L'identité peut changer en fonction des acteurs ou du cadre dans lequel les individus se trouvent et n'est donc ni fixe ni absolue.

Fournisseur d'identité désigne une entité faisant autorité - par ex., une agence gouvernementale ou une entreprise privée - qui émet et gère les identités légales, les justificatifs d'identité et les processus d'authentification tout au long du cycle de vie de l'identité (document ID4D Public-Private Cooperation).

Interopérabilité désigne la capacité de différentes unités fonctionnelles - par ex., telles que des systèmes, des bases de données, des dispositifs ou des applications -, à communiquer, à exécuter des programmes ou à transférer des données d'une manière qui exige que l'utilisateur ait peu ou pas de connaissances de ces unités fonctionnelles (adapté de la norme ISO/CEI 2382 : 2015).

Niveau d'assurance (LOA) désigne la capacité de déterminer, avec un certain niveau de certitude ou d'assurance, qu'un renseignement d'une identité particulière faite par une personne ou une entité peut être considérée comme étant la « véritable » identité du demandeur (ID4D Public-Private Cooperation). Le niveau global d'assurance est une fonction du degré de confiance dans le fait que l'identité revendiquée par le demandeur est sa véritable identité (le niveau d'assurance de l'identité ou IAL), de la force du processus d'authentification (niveau d'assurance de l'authentification ou AAL), et - en cas d'utilisation d'une identité fédérée - du protocole d'assertion utilisé par la fédération pour communiquer les informations d'authentification et d'attribut (niveau d'assurance de la fédération ou FAL) (adapté de NIST 800-63:2017).

Normes ouvertes désignent des normes mises à la disposition du grand public et, qui sont développées (ou approuvées) et maintenues via un processus collaboratif et consensuel. Les « normes ouvertes » facilitent l'interopérabilité et l'échange de données entre différents produits ou services et sont destinées à être largement adoptées (adopté de l'UIT-T).

Données personnelles désigne toute information relative à une personne physique identifiée ou identifiable par laquelle cette personne peut être identifiée, directement ou indirectement notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Protection de la vie privée et de la sécurité dès la conception désigne l'intégration proactive de mécanismes de protection de la vie privée et de sécurité dans la conception et le fonctionnement des produits et services, qu'il s'agisse de systèmes informatiques ou non, d'infrastructures en réseau ou de pratiques commerciales. Cela exige que la gouvernance de la vie privée et de la sécurité soit prise en compte tout au long du processus de conception et du cycle de vie du produit.

Analyse d'impact sur la protection des données (AIPD) désigne un processus conçu pour identifier les risques découlant du traitement des données à caractère personnel et pour minimiser ces risques autant et aussi tôt que possible. Les analyses d'impact sur la protection des données sont des outils importants pour éliminer les risques et pour démontrer la conformité aux lois et règlements sur la protection des données.

Traitement de données à caractère personnel désigne toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la combinaison et le verrouillage, le cryptage, l'effacement ou la destruction de données à caractère personnel.

Preuve d'identité légale désigne un justificatif, tel qu'un certificat de naissance, une carte d'identité ou un justificatif d'identité numérique, qui est reconnu comme une preuve d'identité légale en vertu du droit national et conformément aux normes et principes internationaux émergents (définition opérationnelle de l'identité légale du groupe d'experts en identité légale des Nations unies).

Partie intéressée (RP) désigne une entité qui s'appuie sur les justificatifs d'identité et les mécanismes d'authentification fournis par un système d'identification, généralement pour traiter une transaction ou accorder l'accès à des informations ou à un système (adapté de NIST 800-63 : 2017).

Cadre de confiance désigne les exigences commerciales, techniques, opérationnelles et juridiques du système d'identité afin de favoriser l'interopérabilité entre les différentes parties participantesprenantes.

Présentation vérifiable désigne une présentation inviolable (données dérivées d'un ou de plusieurs justificatifs vérifiables) codée de telle sorte que l'on puisse faire confiance à l'auteur des données après un processus de vérification cryptographique. Par exemple, les approches de divulgation sélective qui synthétisent les données et ne transmettent pas les informations d'identification vérifiables originales (adapté de W3C).

Vérification désigne le processus qui consiste à vérifier des attributs d'identité spécifiques ou à déterminer l'authenticité de justificatifs d'identité afin de faciliter l'autorisation d'un service particulier.

