Union internationale des télécommunications

INITIATIVE MONDIALE EN FAVEUR DE L'INCLUSION FINANCIÈRE (FIGI)

TÉLÉCOMMUNICATIONS
SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/2021)

Groupe de travail sur la sécurité, l'infrastructure et la confiance

Exemples d'utilisation du processus d'e-KYC dans le cadre des services financiers numériques

Rapport sur l'axe de travail "Sécurité"

DÉCHARGE DE RESPONSABILITÉ

L'Initiative mondiale en faveur de l'inclusion financière (FIGI) est un programme triennal mis en œuvre dans le cadre d'un partenariat entre le Groupe de la Banque mondiale, le Comité sur les paiements et les infrastructures de marché (CPMI) et l'Union internationale des télécommunications (UIT), et financé par la Bill and Melinda Gates Foundation. Il vise à faciliter et à accélérer l'application de réformes nationales en vue d'atteindre les objectifs nationaux en matière d'inclusion financière et, à terme, l'objectif mondial consistant à garantir un accès universel aux services financiers à l'horizon 2020. La FIGI finance des initiatives dans trois pays – la Chine, l'Égypte et le Mexique – et lutte contre les grands obstacles à l'accès universel aux services financiers à travers le soutien qu'elle apporte aux trois groupes de travail suivants: 1) le Groupe de travail sur l'acceptation des paiements électroniques (dirigé par le Groupe de la Banque mondiale); 2) le Groupe de travail sur l'identité numérique pour les services financiers (dirigé par le Groupe de la Banque mondiale); et 3) le Groupe de travail sur la sécurité, l'infrastructure et la confiance (dirigé par l'UIT). La FIGI organise également trois colloques annuels rassemblant les autorités nationales, le secteur privé et les parties prenantes du secteur public autour de thèmes transversaux, afin de partager les dernières conclusions des groupes de travail et des programmes nationaux.

Le présent rapport a été élaboré par le Groupe de travail de la FIGI sur la sécurité, l'infrastructure et la confiance, dirigé par l'UIT.

Les résultats, interprétations et conclusions exprimés dans ce rapport ne reflètent pas nécessairement les opinions des partenaires de la FIGI, notamment le CPMI, la Bill and Melinda Gates Foundation, l'UIT ou la Banque mondiale (y compris son Conseil d'administration ou les gouvernements qu'il représente). Les références éventuelles à certaines sociétés ou aux produits de certains fabricants ne signifient pas que l'UIT approuve ou recommande ces sociétés ou ces produits de préférence à d'autres de nature similaire, mais dont il n'est pas fait mention. Sauf erreur ou omission, les noms des produits propriétaires comprennent une lettre majuscule initiale. Les partenaires de la FIGI ne garantissent pas l'exactitude des données figurant dans le présent rapport. Les frontières, couleurs, dénominations et autres informations figurant sur les cartes de cet ouvrage n'impliquent aucune prise de position de la part des partenaires de la FIGI concernant le statut juridique d'un pays, d'un territoire, d'une ville ou d'une région ou de ses autorités, ni aucune reconnaissance ou acceptation de ces frontières.

À propos du présent rapport

Ce rapport a été rédigé par Vijay Mauree et Arnold Kibuuka, de l'UIT. Les auteurs tiennent à remercier les contributeurs et réviseurs suivants: Vinod Kotwal, Département des télécommunications, Ministère des communications, Inde; Abbie Barbir, Corapporteur pour la Question 10 de la Commission d'études 17 du Secteur de la normalisation des télécommunications de l'UIT (UIT-T); Jason Burnett, de Digital Trust; Rehan Masood, de la Banque d'État du Pakistan; Matthew Davie, de Kiva, ainsi que les membres du Groupe de travail sur la sécurité, l'infrastructure et la confiance pour leurs commentaires.

Si vous souhaitez nous communiquer des informations complémentaires, veuillez contacter Vijay Mauree à l'adresse tsbfigisit@itu.int.

TABLE DES MATIERES

LISTE DES TABLEAUX

TABLEAUX

LISTE DES FIGURES

Sommaire de direction

La vérification d'identité numérique, sous l'impulsion des initiatives prises dans le cadre de la transformation numérique et en conséquence directe des perturbations causées par la pandémie de COVID-19, connaît une croissance rapide. Les ouvertures de comptes sont de plus en plus fréquemment effectuées en ligne, et les fournisseurs de services appellent à mettre en place des méthodes de vérification d'identité et de connaissance électronique du client (e-KYC) sûres et sécurisées. Les principaux objectifs du présent rapport sont d'entreprendre une analyse des innovations technologiques en matière d'e-KYC, de comparer les différentes approches adoptées par les pays pour mettre en œuvre ce processus, ainsi que de fournir des informations sur les normes techniques qui pourraient être établies pour garantir l'interopérabilité du processus de vérification d'identité numérique. Des exemples d'utilisation en Inde, au Pakistan et en Sierra Leone ainsi que la nouvelle approche de l'architecture globale pour l'identité numérique (GADI) seront étudiés à ces fins.

En Inde, afin d'émettre une carte SIM mobile, il fallait jusque récemment remplir un formulaire de demande de client et fournir des copies physiques d'un justificatif d'identité, d'un justificatif d'adresse ainsi que des photographies. La gestion des dossiers physiques et le gaspillage de papier constituaient des difficultés majeures. Le Gouvernement indien, par l'intermédiaire du Ministère des télécommunications, s'appuie sur les fonctions d'authentification et d'e-KYC d'Aadhaar pour établir de nouveaux contrats de téléphonie mobile et changer le processus d'émission des cartes SIM. Les fournisseurs de services de télécommunications (FST) tirent parti de la fonction d'e-KYC d'Aadhaar dans le cadre de cette nouvelle procédure. Ainsi, une fois le consentement du client obtenu à l'aide de son numéro Aadhaar et du processus d'e-KYC ayant recours aux technologies biométriques, l'Autorité d'identification unique de l'Inde (UIDAI) envoie ses données démographiques (nom, adresse complète, date de naissance, genre et photographie) signées numériquement et chiffrées, ainsi que son numéro Aadhaar et son timbre horodateur, au FST.

Ces données démographiques sont ensuite saisies dans le formulaire de demande du client (de l'anglais *Customer Application Form*) par le FST et stockées dans sa base de données. Une fois tous les champs requis du formulaire de demande du client remplis, le FST délivre la carte SIM au client. Ce nouveau processus permet non seulement de tirer parti de la fonction d'e-KYC, mais aussi de réduire l'utilisation de papier et d'adopter une approche plus durable des télécommunications en Inde.

Au Pakistan, un système de vérification biométrique (BVS) qui permet les flux de données entre les systèmes de gestion de la relation client des FST, la base de données nationale et l'autorité d'enregistrement est utilisé pour émettre de nouvelles cartes SIM et des duplicatas, remplacer des cartes SIM, effectuer des changements de propriétaire, ainsi que pour réaliser des opérations de portabilité des numéros de mobile et mettre en œuvre des processus de revérification (de cartes SIM actives existantes). Une carte SIM vérifiée émise par le BVS peut être utilisée pour ouvrir à distance des comptes de services financiers numériques (DFS) de niveau 0.

Des identificateurs décentralisés (DID) peuvent être adoptés en vue d'effectuer les opérations de vérification d'identité en ligne et de faciliter l'ouverture de comptes à distance. Un système d'identification décentralisée bien conçu peut permettre aux utilisateurs d'effectuer de nombreuses opérations de vérification d'identité et d'authentification en ayant recours à des preuves à divulgation nulle de connaissance – des protocoles empêchent toute fuite d'informations et peuvent même contrecarrer les risques d'atteinte à la vie privée qui découlent de la corrélation d'événements. Les fournisseurs de services bénéficient de coûts réduits et d'un

niveau de garantie bien plus élevé pour chaque opération de vérification, ainsi que de preuves de vérification vérifiables qui peuvent être enregistrées dans un registre distribué.

Le protocole Kiva, un réseau de nœuds renfermant un registre public de DID mis en place en Sierra Leone, constitue un exemple d'utilisation de DID ayant recours à la technologie de blockchain. Ce registre garantit la fiabilité des identifiants numériques utilisés dans le cadre des vérifications d'identité. Le protocole Kiva permet aux citoyens de présenter et d'authentifier leurs identifiants numériques officiels auprès des institutions financières, afin de faciliter le processus de KYC et de se conformer à la politique de diligence voulue.

L'Alliance pour l'identité décentralisée (Alliance DID ou DIDA) cherche à réaliser le plein potentiel des systèmes d'identification décentralisée en assurant l'interopérabilité commerciale et technologique grâce à la plate-forme GADI. L'adresse numérique constitue un élément central de cette dernière. Il s'agit d'un identifiant GADI spécial, délivré à un individu par un émetteur d'adresses numériques certifié au terme des processus de KYC.

La technologie des registres distribués (de l'anglais *Distributed Ledger Technology*, ou DLT) est également compatible avec les identifiants permanents, qui permettent de vérifier l'identité des titulaires à l'aide de technologies de chiffrement. Ce nouveau type d'identité numérique vérifiable et décentralisée, dont le contrôle repose entièrement dans les mains des utilisateurs indépendamment de tout registre centralisé, de tout fournisseur d'identité ou de toute autorité de certification, est unique, global et portable à vie.

Pour que les solutions proposées soient interopérables et fiables, il est nécessaire d'établir une norme technique visant à encadrer la gestion décentralisée de l'identité des individus à des fins d'e-KYC et d'enregistrement à distance de nouveaux clients. Les exigences techniques de cette norme sont examinées dans la section 7 du rapport. Elles portent notamment sur la relation entre les principales entités participantes, ainsi que les interactions au cours du cycle de vie de l'identité décentralisée dans le cadre de l'émission, de la remise et de la réception des identifiants vérifiables. Une telle norme pourrait simplifier le déploiement de ces technologies et promouvoir l'interopérabilité des différentes plates-formes utilisées dans le cadre de ce mécanisme d'authentification.

Abréviations et acronymes

ADIA	Accountable Digital Identity Association
API	Interfaces de programmation d'applications
ASA	Agence de services d'authentification
AUA	Agence d'utilisateurs d'authentification
BVS	Système de vérification biométrique
CIDR	Référentiel central de données d'identités
CNIC	Carte nationale d'identité informatisée
DAP	Émetteur d'adresses numériques
DFS	Services financiers numériques
DID	Identificateur décentralisé
DIDA	Alliance DID
DIF	Fondation pour l'identité décentralisée
DLT	Technologie des registres distribués
EDGE	Enhanced Data Rates for Global Evolution
e-KYC	Connaissance électronique du client
FIDO	Norme ouverte d'authentification sans mot de passe
FST	Fournisseur de services de télécommunications
GADI	Architecture globale pour l'identité numérique
GPRS	Service de transmission de données en mode paquet
HSM	Module matériel de sécurité
KSA	Agence de services d'e-KYC
KUA	Agence d'utilisateurs d'e-KYC
NCRA	Bureau national d'enregistrement des actes d'état civil
NDIP	Plate-forme nationale d'identité numérique
NPCI	Société nationale des paiements de l'Inde
OASIS	Organization for the Advancement of Structured Information Standards
OTP	Mot de passe à usage unique
PKI	Infrastructure à clés publiques
SBP	Banque d'État du Pakistan
UIDAI	Autorité d'identification unique de l'Inde
UPI	Interface de paiement unifiée
USSD	Données de service complémentaire non structurées
W3C	World Wide Web Consortium

Glossaire

Portefeuille d'identité numérique: Un logiciel (ou d'autres supports), généralement une application mobile, capable de stocker en toute sécurité des identifiants numériques.

Identificateur décentralisé (DID): Un identifiant portable sous forme d'URL associé à une entité. Ces identificateurs sont le plus souvent utilisés pour les identifiants et sont associés à des sujets de sorte que les identifiants puissent être facilement transférés d'un référentiel à un autre sans qu'il soit nécessaire d'en émettre de nouveaux. En voici un exemple: did:exemple:123456abcdef [1].

Adresse numérique: Un identifiant GADI unique délivré à un individu au terme d'un processus de KYC par un émetteur d'adresses numériques (de l'anglais *Digital Address Issuers*, ou DAP) certifié.

Émetteur d'adresses numériques (DAP) (rôle): Une solution ou un fournisseur de services ayant recours à la technologie des DID pour gérer les données d'identité décentralisée des utilisateurs dans l'écosystème GADI.

Registre distribué (DLT): Un registre distribué est une base de données partagée et synchronisée d'un commun accord entre plusieurs sites, institutions ou zones géographiques. Il prend souvent la forme d'une blockchain.

Norme ouverte d'authentification sans mot de passe (FIDO): La spécification d'authentification forte gérée par l'Alliance FIDO [2].

Architecture globale pour l'identité numérique (GADI): Une plate-forme qui garantit la fiabilité de la localisation des sources, rend possible la réalisation d'opérations croisées entre registres distribués et permet l'inclusion de tous les types d'utilisateurs [3].

Connaissance du client (KYC): Un processus dans le cadre duquel un agent d'une organisation effectue une série de contrôles préalables en vue de vérifier l'identité d'un utilisateur ou d'un demandeur. Lorsque cette opération est effectuée à l'aide d'un système ou d'outils en ligne, on parle d'**e-KYC** (connaissance électronique du client).

Fournisseur de services (rôle): Une partie utilisatrice de l'écosystème GADI qui consomme des identifiants vérifiables.

Identifiant vérifiable: Ces identifiants peuvent représenter les mêmes informations que les identifiants physiques. L'avènement de nouvelles technologies telles que les signatures numériques complique la falsification des identifiants vérifiables. Ces derniers sont par conséquent plus fiables que leurs équivalents physiques. Leurs spécifications sont gérées par le World Wide Web Consortium (W3C) [4].

1 Introduction

L'absence d'identification légale est un obstacle majeur à l'inclusion financière. Les solutions de gestion de l'identité numérique peuvent jouer un rôle déterminant dans l'amélioration de l'inclusion financière, en facilitant la gestion et en favorisant l'accessibilité de l'identité. Les technologies émergentes, les données biométriques, les registres distribués et l'intelligence artificielle créent de nouvelles solutions plus rentables et plus efficaces en matière d'e-KYC. Les parties prenantes des secteurs public et privé, afin de s'acquitter de leurs responsabilités en matière de diligence voulue, conçoivent des solutions innovantes ayant recours à ces technologies.

Dans le cadre des DFS, l'identification et la vérification des clients constituent des éléments clés du processus de diligence voulue à l'égard de la clientèle [5] – des éléments auxquels le terme KYC fait ici référence. Les registres KYC sont des services qui stockent les données relatives à l'identité des clients dans un référentiel unique destiné à plusieurs fournisseurs de services financiers.

Le fournisseur de services financiers doit vérifier l'identité des clients à l'aide des documents ou des données de source fiable et indépendante disponibles. Lorsque l'on a affaire à des clients non bancarisés, une telle vérification n'est pas toujours possible, ce qui peut constituer un obstacle à l'inclusion financière. Il peut alors être justifié de suivre un processus de KYC à plusieurs niveaux. Ce n'est toutefois pas toujours envisageable en raison des risques induits par cette opération. Il convient en effet d'évaluer d'abord ces derniers au regard des avantages éventuels pour le fournisseur dans le cadre de cette relation. Afin de mieux pallier ces difficultés, les solutions de gestion de l'identité numérique peuvent être intégrées dans le processus de KYC à plusieurs niveaux.

Dans certains pays, le secteur public contribue au processus de vérification de l'identité numérique des fournisseurs de DFS. Dans ce contexte, les autorités nationales chargées de la délivrance des documents d'identité fournissent généralement l'infrastructure nécessaire à la vérification de l'identité numérique et jouent un rôle important dans le cadre du processus d'e-KYC. De telles initiatives ont notamment été menées en Inde, en Malaisie, au Pakistan, en Sierra Leone et à Singapour.

Les principaux objectifs du présent rapport sont d'entreprendre une analyse des innovations technologiques en matière d'e-KYC, de comparer les différentes approches adoptées par les pays pour mettre en œuvre ce processus, ainsi que de fournir des informations sur les normes techniques qui pourraient être établies pour garantir l'interopérabilité du processus de vérification d'identité numérique.

2 Inde

En Inde, le programme Aadhaar fournit un identifiant unique (un numéro aléatoire à 12 chiffres) aux résidents. Les fournisseurs de DFS peuvent vérifier l'identité d'un client à l'aide de son numéro Aadhaar ainsi que d'un scan de ses empreintes digitales et/ou de l'iris. Afin de simplifier le processus de diligence voulue à l'égard des clients, les fournisseurs de DFS s'appuient sur les résultats de l'authentification Aadhaar sans procéder à d'autres vérifications de l'identité.

En septembre 2018, la Cour suprême de l'Inde a jugé qu'une section de la loi encadrant Aadhaar liée à l'utilisation du processus d'e-KYC par le secteur privé était inconstitutionnelle. Par conséquent, le secteur privé n'a pas pu bénéficier des services d'e-KYC. Leur utilisation dans le cadre des services publics, notamment pour les paiements d'aide sociale, n'a pas été affectée. Un règlement a été adopté en 2019 pour ouvrir l'accès aux services d'e-KYC au secteur privé, notamment aux fournisseurs de DFS et aux entreprises de télécommunication.

2.1 India Stack

Tirant parti de la fonctionnalité Aadhaar, India Stack dispose de capacités ouvertes et programmables, organisées en quatre couches distinctes:

- **Une couche "sans présence requise"** grâce à laquelle l'identité numérique biométrique universelle permet aux individus de bénéficier de n'importe quel service depuis n'importe quel endroit du pays.
- **Une couche "sans papier"** qui comprend une version numérique des documents, lesquels sont rattachés à l'identité numérique des individus, éliminant ainsi la nécessité de collecter et de stocker d'importantes quantités de documents au format papier.
- **Une couche "sans espèces"** qui correspond à une interface unique disponible pour l'ensemble des comptes bancaires et portefeuilles numériques du pays.
- **Une couche consacrée à l'obtention du consentement**, qui garantit une circulation sécurisée et efficace des données des utilisateurs, qui dépend de leur consentement et qui est contrôlée par ces derniers.

Chaque couche de cette pile repose sur une intervention technologique spécifique, comme indiqué ci-dessous:

Tableau 1: India Stack

Couche	Fonctionnalité	Intervention technologique
Sans présence requise	Identité biométrique numérique unique	Authentification Aadhaar
Sans papier	Croissance rapide des systèmes sans papier avec des milliards d'artefacts	e-KYC Aadhaar, eSign et Digilocker
Sans espèces	Des systèmes de paiement électronique qui facilitent la transition vers une économie sans argent liquide	Service de paiement immédiat, passerelle de paiement Aadhaar, système de paiement activé par Aadhaar et interface de paiement unifiée (UPI)
Consentement	Fournit un cadre pour le partage de données confidentielles	Interfaces de programmation d'applications (API) publiques correspondantes dans le cadre de la politique relative aux API ouvertes

Les données qui transitent par les différentes couches d'India Stack peuvent être suivies numériquement afin d'en garantir la traçabilité. En adhérant aux principes de gouvernance, à savoir la participation, la transparence, la responsabilité, la réactivité, l'efficacité et l'efficience, India Stack a ainsi amorcé une nouvelle ère dans la prestation de services.

S'appuyer sur India Stack pour fournir des services financiers et faciliter les paiements numériques

- Aadhaar, un moyen d'authentification d'identité pour mettre en place l'e-KYC et rendre possible l'ouverture de comptes clients à un coût très faible et avec le moins de contraintes possible
- Aadhaar, un moyen d'authentification d'identité pour les transactions
- Aadhaar, une destination financière – pour envoyer de l'argent au numéro Aadhaar au lieu d'un compte bancaire ou d'un code IFSC à l'aide de la plate-forme UPI de la Société nationale des paiements de l'Inde (NPCI)

2.2 Autorité d'identification unique de l'Inde

L'UIDAI est responsable de l'émission des numéros Aadhaar. L'UIDAI est en charge de trois processus fonctionnels clés: l'inscription, l'identification et l'authentification. Au moyen d'un vaste réseau d'agences d'inscription, l'UIDAI recueille les informations démographiques (nom, date de naissance, genre, adresse) et biométriques (empreintes digitales, scan de l'iris et photographie) des individus en vue de les inscrire dans le système Aadhaar.

Ces données biométriques et démographiques sont conservées dans un référentiel central de données d'identités (CIDR), et les revendications d'identité ainsi que les services d'authentification sont fournis par le biais d'API ouvertes comprenant des questions auxquelles il est demandé de répondre par oui ou non. Plusieurs applications, telles que eSign, les casiers numériques, les applications bancaires mobiles, etc., utilisent les services d'authentification biométrique d'Aadhaar.

L'UADAI fournit les processus fonctionnels suivants permettant d'inscrire et de vérifier l'identité des utilisateurs d'Aadhaar:

- **Processus d'inscription**: création et stockage de registres de données d'inscription d'individus soumis au processus de capture biométrique conformément à la politique d'inscription. Ces derniers présentent généralement leurs caractéristiques biométriques à un capteur ainsi que leur référence d'identité. L'échantillon biométrique capturé est traité afin d'en extraire des caractéristiques qui serviront de données de référence dans la base de données d'inscription, de même que la référence d'identité.
- **Processus de vérification**: vérification de l'affirmation selon laquelle l'individu qui fait l'objet du processus de capture biométrique est la source de la référence biométrique spécifiée. Le sujet présente sa référence d'identité ainsi que ses caractéristiques biométriques au dispositif de capture, afin de revendiquer une identité. Ce dispositif collecte ensuite le ou les échantillon(s) biométrique(s) et les compare avec la référence biométrique liée à la référence d'identité à identifier. Le processus de vérification peut avoir un impact sur la confidentialité des informations du sujet dans la mesure où il requiert à la fois une référence biométrique et une référence d'identité.

Le processus d'identification nécessite une recherche exhaustive dans la base de données d'inscription. Il peut donc également avoir un impact sur la vie privée physique du sujet. Il est généralement admis que le processus de vérification est moins susceptible de porter atteinte à la vie privée que le processus d'identification. Dans le système Aadhaar, la vérification est effectuée par le biais d'une question d'authentification en ligne à laquelle il suffit de répondre par oui ou non.

2.3 Société nationale des paiements de l'Inde

Le système Aadhaar assure l'authentification de base de l'identité. La NPCI, une organisation mère mise en place avec le soutien et la supervision de la Banque de réserve de l'Inde et de l'Association des banques indiennes, constitue la structure au sein de laquelle l'ensemble du système bancaire assure la gestion des paiements et des règlements aussi bien physiques et qu'électroniques.

La NPCI a collaboré avec l'UIDAI en vue de créer un mappeur Aadhaar centralisé. Ce dernier permet de relier le numéro Aadhaar du client, son numéro de téléphone mobile et ses comptes bancaires. Ce référentiel central peut être utilisé pour acheminer des instructions de paiement en fonction du numéro Aadhaar ou du numéro de téléphone mobile. En raison de la mise en correspondance du numéro Aadhaar avec le numéro de compte en tant qu'adresse financière, le mappeur Aadhaar fait à l'heure actuelle office de facilitateur de paiement. Pour renforcer les capacités, la NPCI a déjà mis en place des solutions telles que le processus d'e-KYC et la passerelle de paiement Aadhaar. L'UPI, le service de paiement immédiat et la plate-forme nationale unifiée USSD peuvent tirer parti du mappeur central pour récupérer et acheminer leurs paiements. L'existence d'un tel référentiel commun peut donc considérablement augmenter la valeur du processus pour l'ensemble de l'écosystème de paiement et, par conséquent, pour le client final.

2.4 Services d'authentification et d'e-KYC dans le cadre des DFS

L'UIDAI offre deux types de services/d'installations au secteur privé et aux fournisseurs de DFS:

a) Des services d'authentification visant à authentifier une revendication d'identité grâce à des questions auxquelles il convient de répondre par oui ou non, à l'aide de la biométrie ou d'un mot de passe à usage unique (OTP) mobile; et
b) L'authentification e-KYC permettant explicitement à l'UIDAI de partager les données démographiques avec la partie requérante seulement après l'obtention du consentement du titulaire de la carte Aadhaar.

Afin d'expliquer le fonctionnement des services d'authentification et d'e-KYC, ce document fournit d'abord un aperçu de l'écosystème d'authentification et de KYC d'Aadhaar, qui décrit le rôle de chaque partie prenante.

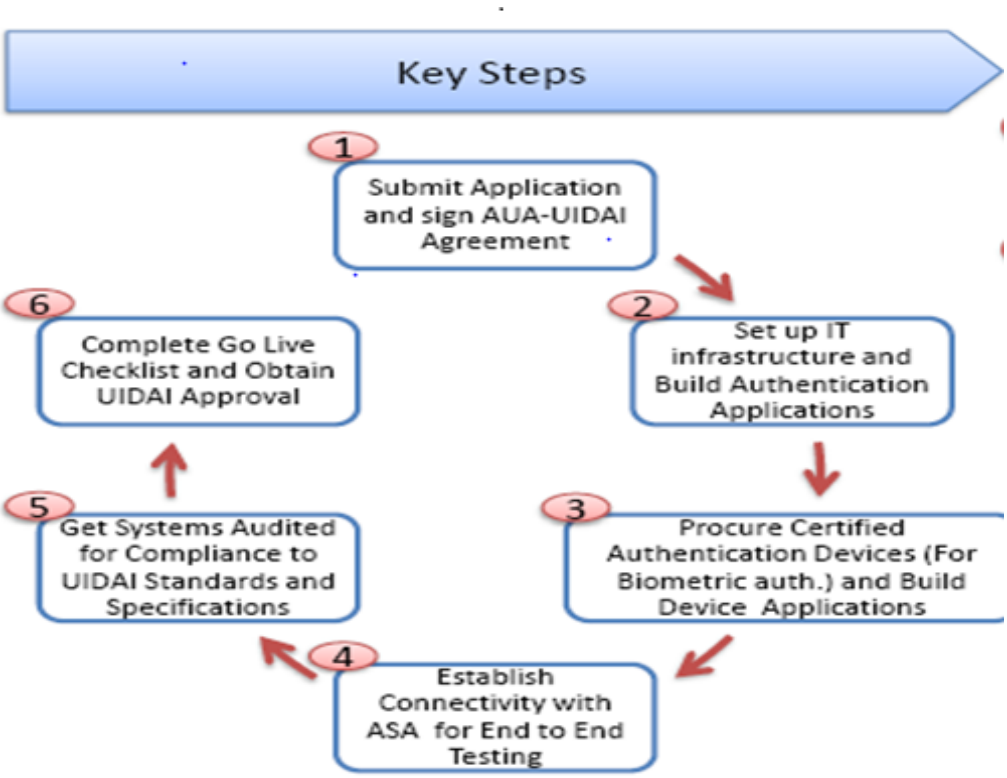
2.4.1 Écosystème d'authentification Aadhaar

L'écosystème d'authentification Aadhaar comprend les organismes suivants:

a) Agences d'utilisateurs d'authentification

Les agences d'utilisateurs d'authentification (AUA) se connectent à la base de données Aadhaar et utilisent l'authentification Aadhaar pour valider un utilisateur et activer leurs

services. Parmi les AUA figurent les banques, les ministères de différents États et du gouvernement central fournissant des services tels que le système de distribution publique, le Plan national pour la garantie de l'emploi rural, ainsi que des organismes privés tels que les opérateurs de téléphonie mobile. Les AUA doivent conclure un contrat officiel avec l'UIDAI afin d'utiliser les services d'authentification Aadhaar (voir figure 2). Tout autre organisme souhaitant procéder à l'authentification Aadhaar de ses clients ou associés dans le cadre de la prestation de services peut conclure un accord avec une AUA. Ces organismes deviennent alors des sous-AUA. Figure 1: Processus d'accueil de l'AUA



b) Agences de services d'authentification
Les agences de services d'authentification (ASA) sont les entités chargées de transmettre les demandes d'authentification à la base de données Aadhaar au nom d'une ou de plusieurs AUA. Elles jouent ainsi le rôle d'intermédiaires. Ces agences bénéficient d'une connexion sécurisée à la base de données Aadhaar, à laquelle elles transmettent les demandes d'authentification de plusieurs AUA à la fois. Lorsqu'elles reçoivent la réponse de la base de données Aadhaar, les ASA la transmettent aux AUA. Une ASA peut conclure un contrat officiel avec les AUA. L'UIDAI a établi un ensemble de directives qui peut être inclus dans le contrat entre une ASA et une AUA. Cependant, les termes du contrat (et les conditions commerciales, le cas échéant) entre les ASA et les AUA sont à la seule discrétion des parties signataires.

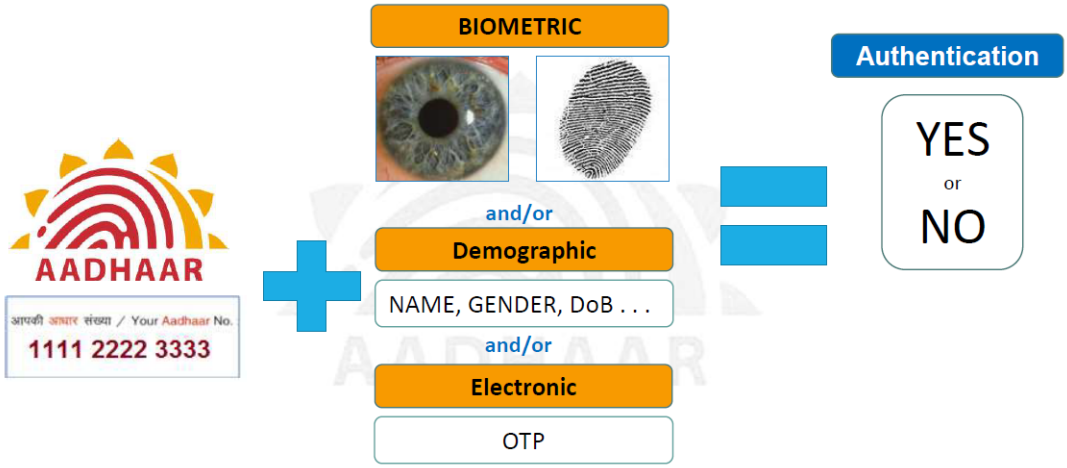
c) Agences d'utilisateurs d'e-KYC

Les agences d'utilisateurs d'e-KYC (KUA) sont les entités qui utilisent l'authentification Aadhaar pour activer leurs services et se connectent à la base de données Aadhaar par l'intermédiaire d'une ASA.

d) Agences de services d'e-KYC
Les agences de services d'e-KYC (KSA) sont des entités connectées à la base de données Aadhaar autorisées à partager le profil démographique du titulaire de la carte Aadhaar avec les KUA à des fins d'authentification. Les KSA sont également des ASA.

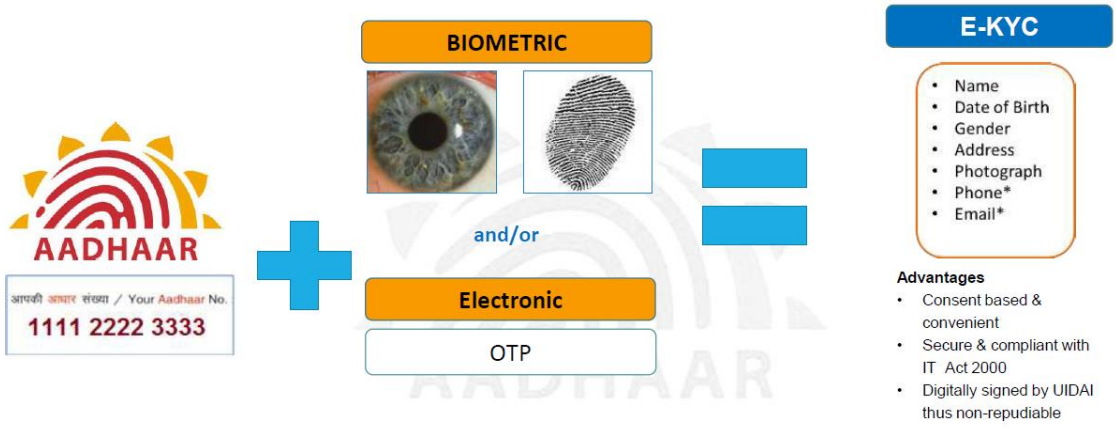
2.4.2 Services d'authentification et d'e-KYC Aadhaar

Figure 2: Service d'authentification



L'authentification Aadhaar est le processus par lequel le numéro Aadhaar ainsi que d'autres attributs, notamment les données biométriques, sont soumis en ligne à la base de données Aadhaar pour être vérifiés sur la base des informations, données ou documents disponibles. Au cours de l'authentification, le dossier de l'individu est d'abord sélectionné à l'aide du numéro Aadhaar, puis les données démographiques et biométriques sont comparées aux données stockées fournies par l'individu au cours du processus d'inscription ou de mise à jour. L'authentification peut également être effectuée en utilisant un OTP.

Figure 3: Service d'e-KYC d'Aadhaar

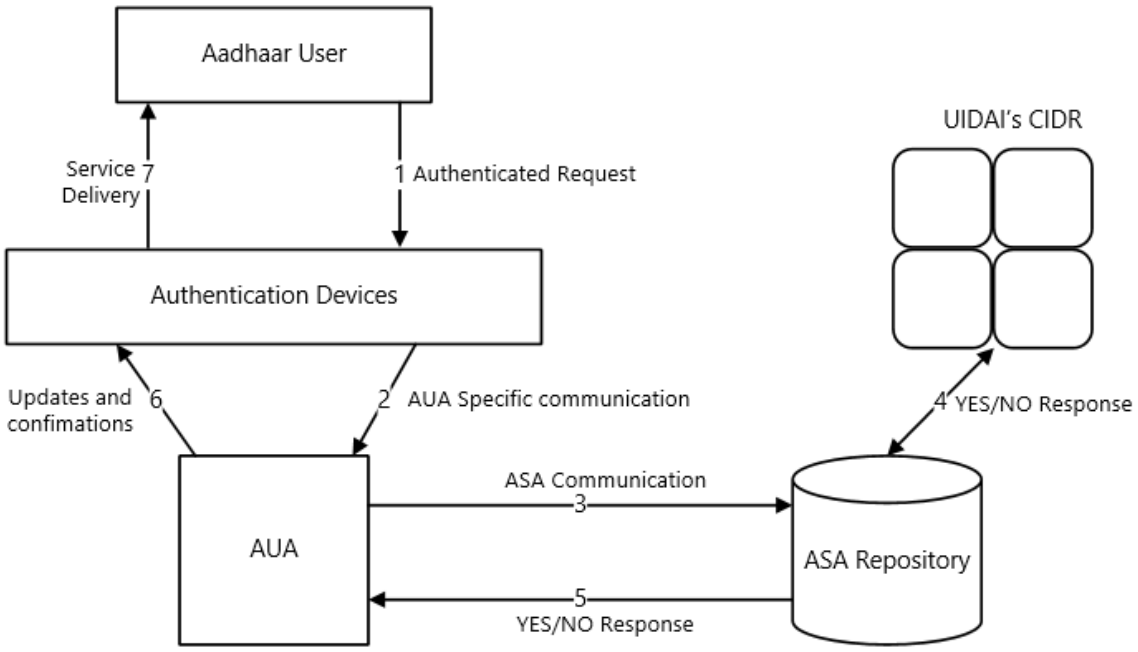


Le service d'e-KYC d'Aadhaar permet à l'UIDAI de partager la version électronique des informations du système (données démographiques et photographie UNIQUEMENT) avec le consentement explicite de la personne concernée. Pendant le processus d'e-KYC, l'UIDAI chiffre les données de réponse du processus contenant les informations démographiques et photographiques les plus récentes de l'individu concerné en utilisant la clé publique de la KUA et transmet la réponse chiffrée à cette dernière. Dès réception de la réponse chiffrée, la KUA déchiffre les données à l'aide de sa propre clé privée et renvoie un fichier XML contenant les sept éléments: nom, adresse, date de naissance, genre, numéro de téléphone, adresse électronique et photographie. Il n'est donc plus nécessaire de demander une photocopie de la lettre Aadhaar au résident. Tous les systèmes d'authentification biométrique ou par OTP sont compatibles avec le service d'e-KYC.

2.5 Processus technique des services d'authentification et d'e-KYC

Les dispositifs d'authentification utilisés par l'AUA ou la KUA enclenchent la demande d'authentification (figure 2) et créent un bloc de données d'identité personnelles chiffrées qu'ils transmettent au serveur d'authentification de l'AUA ou de la KUA, où la transaction spécifique au domaine sera ensuite traitée. Un fichier XML d'authentification est également créé par le biais de l'API d'authentification de l'UIDAI. En outre, l'ASA transmet le fichier XML d'authentification de l'AUA au CIDR dès qu'elle le reçoit. Afin d'en assurer l'intégrité et la non-répudiation, le serveur d'authentification du CIDR n'accepte que le fichier XML d'authentification signé numériquement et transmis par l'ASA.

Figure 4: Processus technique des services d'authentification et d'e-KYC



Voici les principales étapes du processus d'authentification Aadhaar telles qu'illustrées dans la figure 4 ci-dessus:

- Le titulaire de la carte Aadhaar envoie la demande d'authentification par l'intermédiaire de son appareil.
- Le logiciel d'application chargé de l'authentification Aadhaar installé sur l'appareil chiffre et envoie les données au serveur de l'AUA.
- Celui-ci, après validation, ajoute les en-têtes nécessaires (wrapper XML spécifique à l'AUA avec clé de licence, signature, etc.) et transmet la demande au CIDR de l'UIDAI par le biais du serveur de l'ASA.
- Le serveur d'authentification Aadhaar répond par oui ou non en fonction de la correspondance des paramètres d'entrée.
- Selon la réponse du serveur d'authentification Aadhaar, l'AUA ou la sous-AUA effectue la transaction et le titulaire de la carte Aadhaar reçoit le service.

2.6 Fonctions de sécurité supplémentaires des services d'authentification et de KYC

a) Afin de renforcer la sécurité de l'écosystème d'authentification Aadhaar, en vertu des règlements 14(n) et 19(o) de 2016 de la réglementation relative au système d'authentification Aadhaar, il a été décidé qu'il est obligatoire d'utiliser un module matériel de sécurité (HSM) pour signer numériquement le fichier XML d'authentification et déchiffrer les données du processus d'e-KYC.
b) Concernant la signature numérique du fichier XML d'authentification, la demande d'authentification est signée numériquement par l'entité requérante (AUA/KUA) et/ou par l'ASA utilisant le HSM, selon l'accord mutuel convenu. Cependant, pour déchiffrer les données de réponse du processus d'e-KYC transmises par l'UIDAI, la KUA doit utiliser son propre HSM.
c) Le HSM à utiliser pour signer le fichier XML d'authentification ainsi que pour déchiffrer les données du processus d'e-KYC est conforme à la norme FIPS 140-2.
d) Toutes les AUA/KUA/ASA assurent la mise en place du HSM dans les services d'authentification Aadhaar.
e) Pour arrêter l'utilisation de données biométriques stockées, l'UIDAI a rendu obligatoire l'utilisation d'appareils enregistrés par les AUA/KUA ainsi que les ASA. Par rapport aux appareils publics, les appareils enregistrés offrent les fonctionnalités supplémentaires suivantes:

    - Identification de l'appareil: chaque appareil dispose d'un identifiant unique afin d'en permettre la traçabilité et l'analyse ainsi que d'améliorer la gestion des fraudes.
    - Interdiction d'utiliser des données biométriques stockées: les données biométriques sont signées dans l'appareil à l'aide de la clé du fournisseur afin de garantir qu'elles sont effectivement capturées en temps réel. Le service des appareils enregistrés du fournisseur de l'appareil doit ensuite constituer le bloc de données d'identité personnelles chiffrées avant de retourner à l'application hôte.

2.7 Intégration de la norme FIDO et d'Aadhaar: fusionner l'identité réelle avec les identités virtuelles

Cette section fournit quelques indications sur la manière dont l'Alliance FIDO pourrait être intégrée au système Aadhaar en Inde.

L'Alliance FIDO est le plus grand écosystème au monde d'authentification interopérable basée sur des normes [2]. Google en est le président, Microsoft le vice-président et les principaux segments des marchés mondiaux y sont représentés. La mission de l'Alliance FIDO consiste à éliminer la dépendance aux mots de passe de réseau, qui constituent la principale source

d'usurpation d'identité et représentent un risque considérable pour les utilisateurs ordinaires. La norme FIDO a déjà fait l'objet d'importants déploiements dans le monde entier, aussi bien au sein d'organisations financières qu'auprès d'opérateurs de réseaux, de fournisseurs de services de commerce électronique et de fournisseurs de services en nuage. La norme FIDO élimine les sources d'usurpation d'identité les plus courantes, telles que les attaques par hameçonnage, les attaques côté serveur, les attaques par interception, les attaques par dictionnaire et les attaques globales.

Le W3C intègre l'authentification FIDO aux spécifications d'authentification Web pour navigateurs. Depuis deux ans, les téléphones mobiles des grands fabricants d'équipement d'origine comme Apple, Samsung, Huawei et Lenovo la prennent également en charge. Dans l'architecture FIDO, la fiabilité de l'identité est assurée par le service auquel l'utilisateur veut se connecter. Pour le même utilisateur et le même appareil, l'appareil de l'utilisateur reçoit une clé publique ou privée différente.

Pour un pays fortement peuplé comme l'Inde dont l'économie repose sur la téléphonie mobile et qui investit de façon conséquente dans les systèmes d'identification centralisés comme Aadhaar, la norme FIDO offre de nombreuses possibilités en matière de conception de systèmes d'authentification forte.

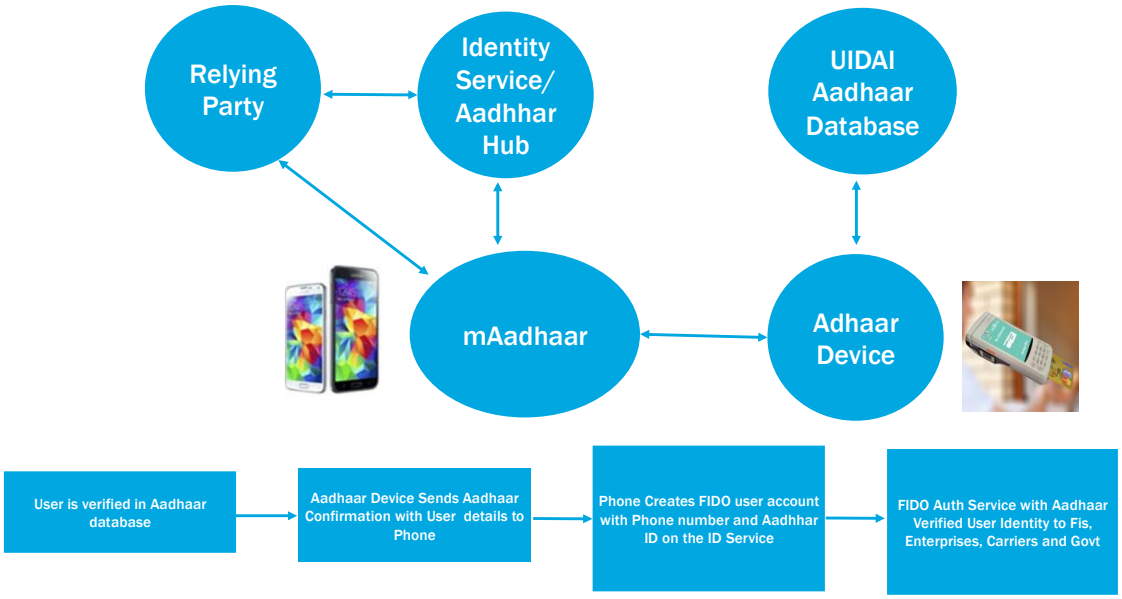
Il est possible de s'inspirer à cette fin des bases solides que l'Inde a déjà posées. Aadhaar rencontre d'ailleurs un franc succès dans le domaine des services de KYC et de la mise en relation de l'identité avec le numéro Aadhaar. Il pourrait en outre s'avérer particulièrement avantageux de produire un identifiant dérivé afin d'effectuer la vérification Aadhaar depuis le smartphone de l'utilisateur par le biais d'un service d'identification en nuage. Cet identifiant dérivé pourrait être utilisé pour chaque transaction effectuée par un citoyen à divers endroits sans pour autant interagir systématiquement avec la base de données Aadhaar.

L'application mobile mAadhaar pourrait être le maillon idéal pour intégrer l'authentification FIDO et fournir un service d'identité en nuage vérifié par Aadhaar. Bien que mAadhaar soit un excellent outil d'authentification hors ligne, aucune piste d'audit ni aucune trace ne pourraient toutefois être enregistrées en dehors de l'appareil de l'utilisateur. Cela exposerait l'utilisateur à la fraude et il ne pourrait par ailleurs pas effectuer d'opérations sans l'assistance d'un opérateur.

Selon cette approche, l'utilisateur peut simplement utiliser l'authentification FIDO pour s'authentifier avec l'application mobile mAadhaar à l'aide d'une plate-forme de gestion des identités basée sur le nuage (appelé "AadhaarHub") et liée à l'application, et ce, à tout moment et à chaque fois que l'utilisateur doit être authentifié. La validation de l'authentification est directement effectuée sur la plate-forme de gestion des identités. Procéder ainsi garantit la confidentialité des données dans la mesure où aucune information spécifique à l'utilisateur n'est envoyée au serveur en dehors de l'assertion FIDO. Les données biométriques de l'utilisateur ne quittent jamais l'appareil, et l'authentification ne peut se faire que sur cet appareil, pour cet utilisateur et par le biais d'AadhaarHub.

Cela pourrait également être un excellent moyen de fournir des services publics aux citoyens, de permettre les paiements entre particuliers, et, grâce à une simple fonctionnalité tactile, d'effectuer divers paiements dans les transports publics et d'autres sites marchands à l'aide d'une authentification côté serveur qui garantit l'authenticité de l'identité.

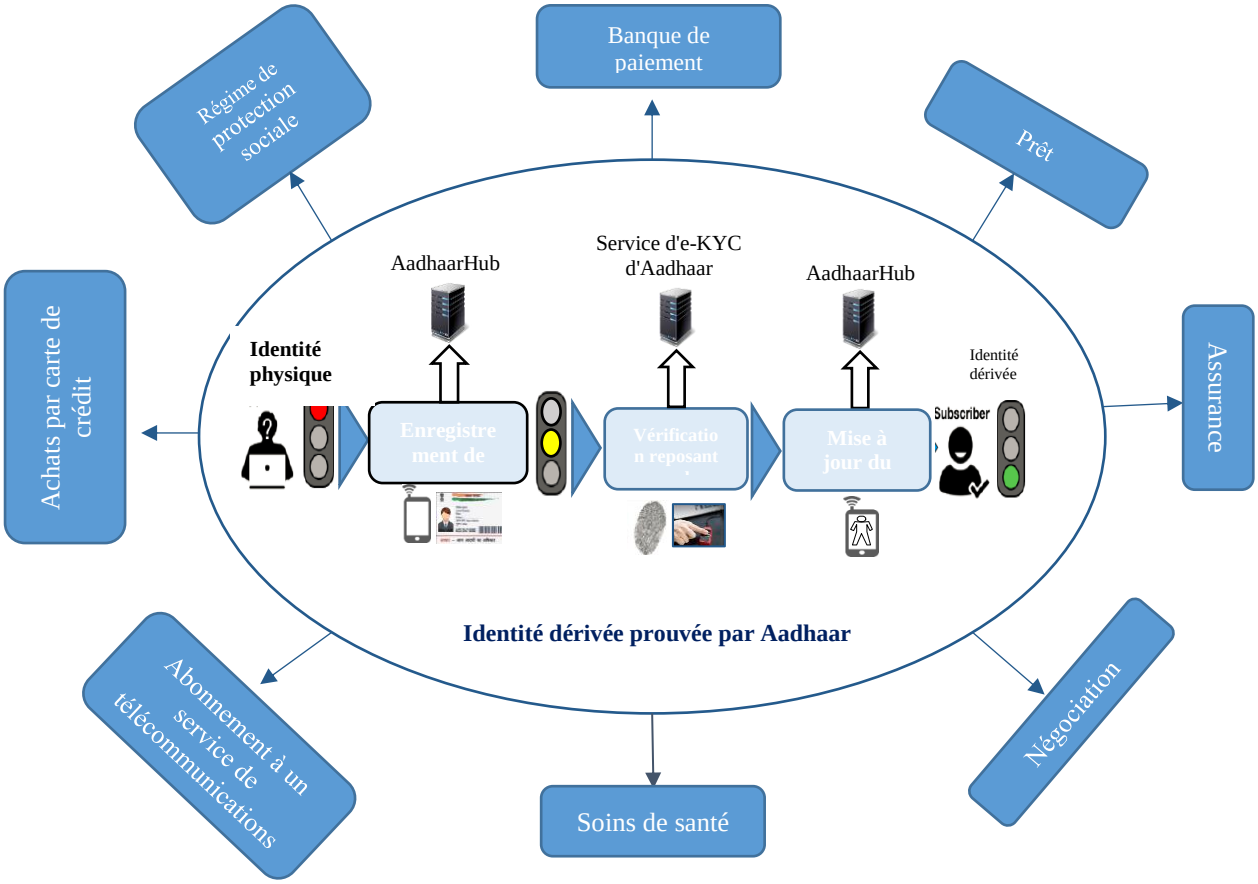
Figure 5: Serveur d'authentification avec preuve d'identité: aucun identifiant utilisateur



En intégrant India Stack, mAadhaar et AadhaarHub pourraient rejoindre la pile logicielle des fabricants d'appareils. Chaque appareil vendu en Inde pourrait en être doté sans imposer de contraintes supplémentaires aux fabricants d'appareils. Les principaux fournisseurs de services pourraient ainsi proposer grâce à India Stack des services d'authentification sans identifiant ni mot de passe aux citoyens indiens. L'adoption de cette nouvelle norme permettrait de relier leurs identités virtuelles et leur identité réelle et donc de diminuer considérablement la cyberfraude.

Cette approche unique de la cybersécurité, qui vise à garantir l'anonymat et la confidentialité en ligne ainsi qu'à vérifier l'identité de manière non intrusive lors d'enquêtes cybercriminelles, pourrait inspirer le monde entier à s'engager dans cette voie.

Figure 6: Identité dérivée prouvée par Aadhaar



3 Pakistan

3.1 Système de vérification biométrique

Avant la mise en place du BVS, les procédures de vente de cartes SIM fonctionnaient correctement. Cependant, la demande de cartes SIM frauduleuses, notamment pour la terminaison illégale du trafic international (boîte SIM), a ouvert la voie au contournement du système. La publication des listes électorales et leur accès au public lors des élections générales de 2013 ont indirectement donné accès à des informations secrètes, notamment le nom de la mère et le lieu de naissance inscrits sur la carte nationale d'identité informatisée (CNIC) des citoyens. Les fraudeurs s'en sont servi pour mener une opération d'usurpation d'identité à grande échelle. Il s'est donc avéré nécessaire de mettre au point un système sécurisé d'émission de cartes SIM qui puisse fournir une "preuve de vie".

3.2 Flux de données au sein du BVS

Dans le BVS, les données circulent du canal de vente à la base de données de l'Autorité nationale responsable des bases de données et de l'enregistrement (NADRA) par le biais des systèmes de gestion de la relation client des opérateurs de téléphonie mobile en suivant les étapes suivantes:

a. Lorsqu'un abonné potentiel se rend dans un canal de vente pour effectuer une transaction liée à une carte SIM, l'agent de vente lui demande son numéro CNIC, saisit son numéro de téléphone mobile, scanne son pouce ou son doigt et envoie les données (numéro CNIC et fiche d'informations biométriques) à l'opérateur de téléphonie mobile.
b. Les systèmes des opérateurs de téléphonie mobile vérifient l'éligibilité du canal de vente (grâce à son identifiant unique) ainsi que l'éligibilité de l'abonné (le nombre de cartes SIM doit être inférieur à cinq). Si celui-ci est éligible, ils transmettent les informations à la NADRA.
c. La NADRA vérifie la validité du numéro CNIC ainsi que les informations reçues dans sa base de données. L'issue positive ou négative de l'opération ainsi que les données (nom, nom du père, adresse) sont communiquées sur demande à l'opérateur de téléphonie mobile en fonction du résultat de la vérification.
d. Les données reçues sont utilisées pour mettre à jour le système. Le résultat est ensuite transmis au dispositif du canal de vente.
e. Si la vérification aboutit, la carte SIM est remise au client. En cas d'échec, des orientations sont fournies en fonction du code d'erreur généré par la NADRA.

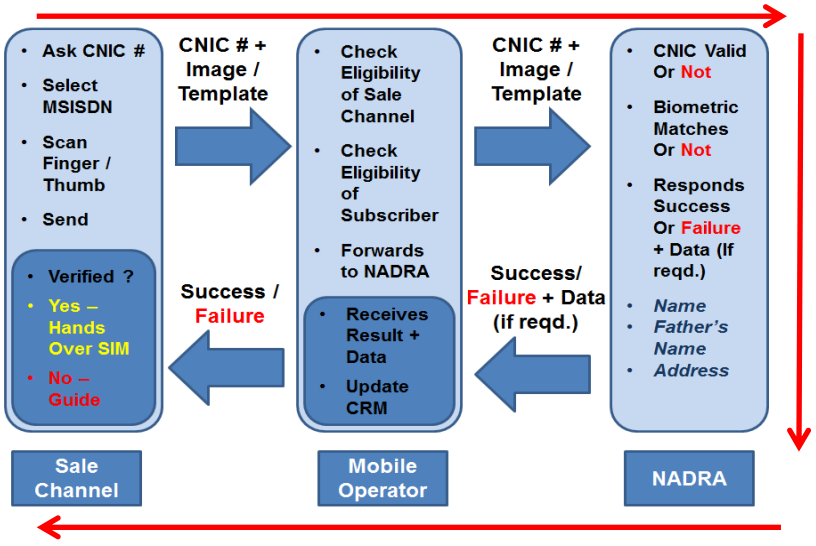


Figure 7: Flux de données au sein du BVS

3.3 Principales caractéristiques du BVS

Le BVS est un processus entièrement automatisé à faible degré d'intervention humaine. Ses principales caractéristiques sont les suivantes:

3.3.1 Processus du BVS

Les données d'entrée comprennent le numéro de la CNIC et le relevé des empreintes digitales (pouce droit, index droit, pouce gauche, index gauche). À l'issue du processus, nous obtenons le résultat de la vérification (positif ou négatif) et, au besoin, les données des abonnés (nom, nom du père, adresse).

3.3.2 Dispositifs utilisés dans le cadre du BVS

Trois types d'appareils sont utilisés dans ce processus:

a) Un ordinateur personnel utilisant le système d'exploitation Microsoft Windows avec un lecteur d'empreintes digitales connecté par câble USB. L'ordinateur personnel héberge une application qui capture les empreintes digitales et communique les informations à l'opérateur de téléphonie mobile. Cette solution est surtout utilisée dans les centres de service aux clients et les franchises qui disposent généralement d'un local fixe et d'un générateur de secours.

b) Des terminaux spécialisés et des tablettes utilisant le système d'exploitation Android et équipées de lecteurs d'empreintes digitales (figure 2) ont été déployés principalement dans les magasins.

c) Dans certaines circonstances, ce processus est également effectué à l'aide d'un téléphone équipé d'un lecteur d'empreintes et d'une fonctionnalité Bluetooth.

Les appareils sont connectés aux bases de données en ligne via réseau privé virtuel, et l'accès y est assuré par le biais d'une ligne d'abonné numérique, en utilisant la technologie EDGE (de l'anglais *Enhanced Data Rates for Global Evolution*) ou le service de transmission de données en mode paquet (de l'anglais *General Packet Radio Service*, ou GPRS), ou par technologie large bande mobile (3G/4G) selon le type d'appareil et la zone de service.

3.3.3 Transactions effectuées par le biais du BVS

Actuellement, les transactions effectuées par le biais du BVS sont les suivantes:

a) Émission d'une nouvelle carte SIM
b) Émission d'un duplicata de carte SIM (remplacement ou changement de carte SIM)
c) Changement de propriété (passage d'un propriétaire à un autre)
d) Portabilité du numéro du mobile
e) Désactivation (désactivation d'une carte SIM enregistrée sur une CNIC)
f) Revérification (revérification d'une carte SIM active)

3.3.4 Source des données et format des images

La vérification des informations biométriques est réalisée en temps réel dans la NADRA (la base de données nationale du Pakistan contenant des informations biométriques). Un identifiant de transaction unique est attribué à chaque transaction à des fins de suivi et d'audit. Les informations biométriques à vérifier doivent être capturées à une résolution d'au moins 500 points par pouce (dpi), et les normes prises en charge pour l'acquisition d'images sont Pkmat, ANSI 378 et ISO 19794.

3.3.5 Normes techniques

La NADRA est l'organisme dépositaire des données des citoyens pakistanais. À des fins de vérification, elle a mis en place une API Web qui prend en charge les normes suivantes afin que les opérateurs de télécommunications puissent interagir avec le Système automatisé d'identification par empreintes digitales (AFIS) de la NADRA:

a) Pkmat
b) ANSI 378
c) ISO/IEC 19794-2
d) Les empreintes digitales sont envoyées à la NADRA sous la forme d'un modèle ou d'une image (au format WSQ/JPG/BMP) en utilisant l'une des normes adoptées par l'opérateur de télécommunications.
e) Les empreintes digitales sont disponibles dans la base de données de la NADRA. La mise en correspondance du numéro de la CNIC et de l'empreinte digitale (image ou modèle selon la norme utilisée) envoyés par l'opérateur de téléphonie mobile est effectuée par la NADRA, et la réponse (positive ou négative) est renvoyée à l'opérateur concerné.
f) Le chiffrement complet des paquets (AES 256 bits) est utilisé pour chiffrer les données envoyées aux opérateurs de téléphonie mobile et à la NADRA.

3.3.6 Vérification biométrique des banques directes

Pour les comptes bancaires en ligne, la Banque d'État du Pakistan (SBP) a opté pour une approche fondée sur le risque en matière de diligence voulue à l'égard de la clientèle sans pour autant compromettre ses exigences en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Conformément à la réglementation de la SBP relative aux services bancaires en ligne publiée dans la circulaire BPRD nº 9 de 2016, la vérification biométrique dans le cadre des transactions au guichet des banques directes est devenue obligatoire à partir du 1er juillet 2017.

Cette réglementation est disponible à l'adresse suivante: http://www.sbp.org.pk/bprd/2016/C9.htm. En outre, conformément aux objectifs de la Stratégie nationale de 2015 pour l'inclusion financière, la réglementation susmentionnée a autorisé l'ouverture à distance de comptes de niveau 0 pour les titulaires d'une carte SIM vérifiée. [Remarque: dans sa circulaire BPRD nº 18 de 2018, la SBP a demandé aux banques de procéder à la vérification biométrique des clients enregistrés [6].)

4 Processus d'e-KYC utilisant des DID.

L'ouverture de comptes à distance se heurte principalement au problème de la fiabilité de la vérification d'identité en ligne, et il est nécessaire de concevoir des méthodes en vue de garantir cette dernière.

En donnant à l'utilisateur le contrôle de ses propres actifs d'identité, le concept d'identité décentralisée promet d'atténuer, voire d'éliminer les problèmes des interactions conventionnelles liées à l'identité. Le système d'identification décentralisée consiste en un ensemble d'outils et de services qui mettent en œuvre ce concept.

De nombreux systèmes d'identification décentralisée sont déployés sur des registres distribués. Les registres offrent divers avantages, notamment:

a) Gestion des clés: les registres simplifient considérablement les tâches traditionnellement attribuées aux autorités de certification et aux systèmes utilisant une infrastructure à clés publiques (PKI).

b) Piste d'audit: au besoin, les registres peuvent enregistrer les preuves de transaction pour les événements entraînant des conséquences juridiques ou économiques.

c) Modèle économique: les registres peuvent mettre en œuvre et appliquer les flux de paiement associés aux transactions liées à l'identité.

Ces outils technologiques offrent la possibilité à l'utilisateur de gérer ses informations et de déterminer le contenu qu'il souhaite divulguer et dans quelles circonstances. Un système d'identification décentralisée bien conçu peut permettre aux utilisateurs d'effectuer de nombreuses opérations de vérification d'identité et d'authentification en ayant recours à des preuves à divulgation nulle de connaissance – des protocoles empêchent toute fuite d'informations et peuvent même contrecarrer les risques d'atteinte à la vie privée qui découlent de la corrélation d'événements.

Les fournisseurs de services bénéficient de coûts réduits et d'un niveau de garantie bien plus élevé pour chaque opération de vérification, ainsi que de preuves de vérification vérifiables qui peuvent être enregistrées de façon indélébile dans un registre distribué.

Les émetteurs d'identifiants vérifiables peuvent ainsi baisser considérablement leurs coûts d'émission d'identifiants au format papier et étendre le champ de leurs activités grâce aux revenus générés par l'utilisation des identifiants émis et des capacités de traitement des paiements des registres distribués.

Les sections suivantes illustrent deux exemples de systèmes d'identification décentralisée utilisés aux fins de l'enregistrement biométrique et de l'e-KYC.

5 Plate-forme nationale d'identité numérique de la Sierra Leone

La Sierra Leone a lancé la Plate-forme nationale d'identité numérique (NDIP) en août 2019. La NDIP est une infrastructure d'identité numérique extensible. Construite à l'aide de la technologie à code source ouvert du protocole Kiva, elle permet aux citoyens de présenter et d'authentifier des identifiants numériques officiels auprès des institutions financières. La NDIP, une fois pleinement intégrée au secteur financier et appuyée par le régime réglementaire approprié, constituera la base des services d'e-KYC à l'échelle du marché en Sierra Leone.

La NDIP s'appuie sur les données d'identité collectées et détenues par le Bureau national d'enregistrement des actes d'état civil (de l'anglais *National Civil Registration Authority*, ou NCRA), un registre de citoyens créé par le gouvernement de la Sierra Leone pour encourager la participation aux élections générales de 2018. En partenariat avec le Programme des Nations Unies pour le développement et en s'appuyant sur plus de 2 500 sites d'enregistrement d'identité à travers le pays, les efforts d'enregistrement des actes d'état civil déployés en amont de l'élection ont permis d'attribuer des identifiants officiels à la quasi-totalité de la population adulte de la Sierra Leone.

En collaboration avec Kiva, une organisation à but non lucratif basée aux États-Unis et axée sur l'inclusion financière, la NDIP a contribué à la conversion des données d'identité de la base de données du NCRA en identifiants vérifiables détenus dans des portefeuilles numériques contrôlés par les citoyens [7]. Le secteur financier intègre actuellement l'infrastructure des portefeuilles de la NDIP. Cela signifie que tout citoyen adulte possédant une pièce d'identité délivrée par le NCRA pourra prochainement authentifier de manière sécurisée son identité

officielle auprès des fournisseurs de services financiers afin de faciliter le processus d'e-KYC mené pour l'ouverture de nouveaux comptes ainsi que pour les opérations de diligence voulue à l'égard de la clientèle.

5.1 Protocole Kiva – aperçu du système

Le protocole Kiva mis en œuvre en Sierra Leone est conçu en trois couches afin que les citoyens puissent partager en toute sécurité leurs identifiants officiels authentifiés avec le secteur financier en vue de mener à bien le processus d'e-KYC et les opérations de diligence voulue à l'égard de la clientèle.

5.1.1 Services publics

Le protocole Kiva se compose d'un réseau de nœuds contenant un registre public de DID. Ce registre garantit la fiabilité des identifiants numériques utilisés dans le cadre des vérifications d'identité.

5.1.2 Connexions fiables

La couche suivante de l'architecture permet d'établir des connexions fiables par le biais de services d'authentification et de services de portefeuille. Dans le cadre de ses efforts d'enregistrement des identités et à des fins d'authentification, le NCRA collecte des informations biométriques depuis 2018. Tous les identifiants émis par le NCRA peuvent être authentifiés à l'aide d'un service d'appariement biométrique d'empreintes digitales conçu et mis en œuvre en Sierra Leone. Les services de portefeuille stockent les identifiants des citoyens dans des portefeuilles équipés d'agents de communication visant à permettre l'échange d'identifiants entre pairs.

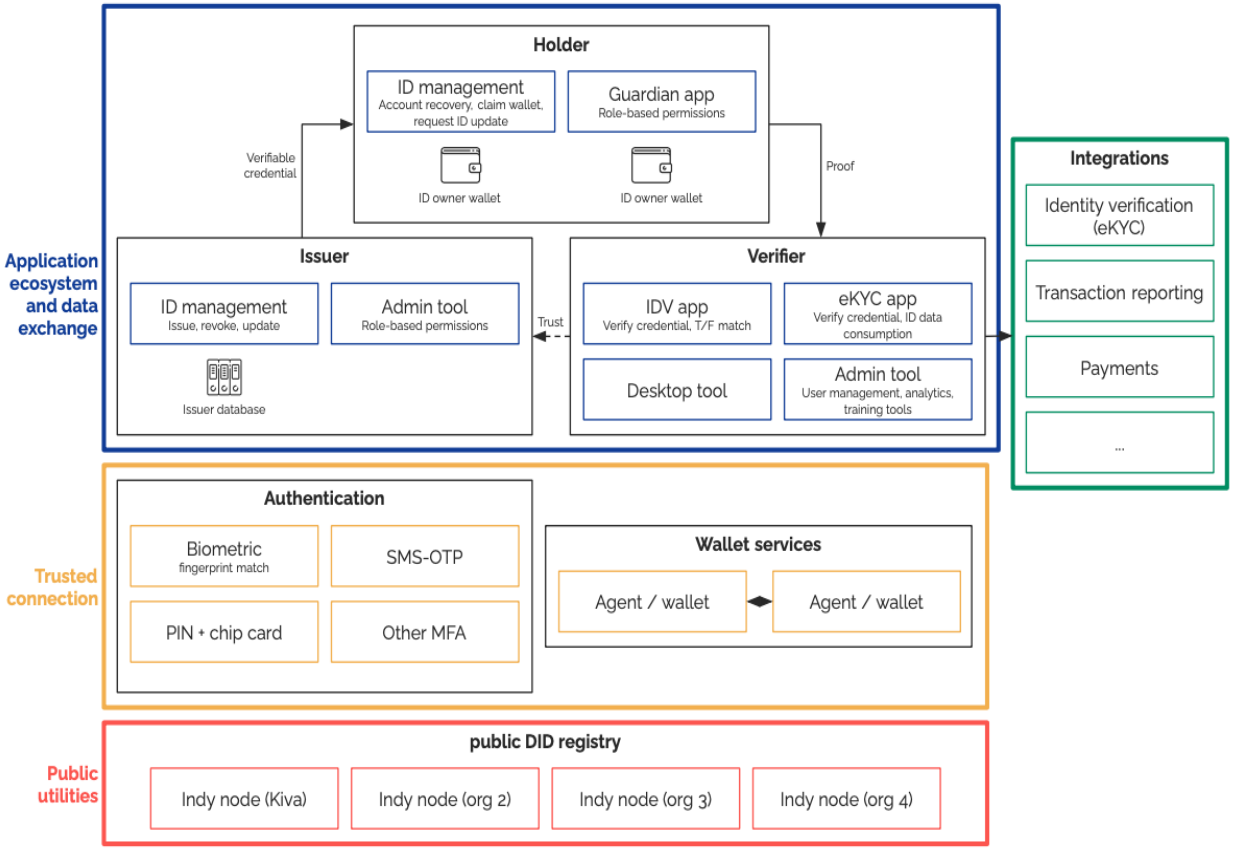
Ces outils permettent aux citoyens de s'authentifier et d'accéder en toute sécurité à leur portefeuille numérique, puis d'envoyer et de recevoir des identifiants à l'aide du protocole intégré de communication d'agent à agent.

5.1.3 Écosystème de l'application et échange de données

Les technologies des deux premières couches alimentent un processus de vérification d'identité en temps réel et sécurisé, centré sur l'utilisateur et compatible avec le processus d'e-KYC. En Sierra Leone, le NCRA a délivré plus de 3,6 millions d'identifiants numériques, et les outils de gestion et d'administration de ces derniers sont intégrés dans les processus d'enregistrement et de gestion des identités existants. Ces identifiants sont conservés dans le cadre d'un accord de protection des données conclu avec le NCRA. Cet accord autorise les citoyens à accéder à leurs données et à les gérer en toute sécurité par le biais d'un service d'appariement biométrique d'empreintes digitales. Les vérificateurs (fournisseurs de services financiers) peuvent ainsi demander aux clients (ou aux clients potentiels) de partager leurs identifiants officiels aux fins du processus d'e-KYC ou des opérations de diligence voulue à l'égard de la clientèle.

La NDIP est accessible aux fournisseurs de services financiers par le biais d'API simples d'intégration de vérificateurs ainsi que d'applications en marque blanche, que les fournisseurs peuvent intégrer directement dans leurs processus d'accueil et de mise en conformité.

Un aperçu de la structure est présenté dans la figure 8.Figure 8: Structure sommaire



Les personnes qui souhaitent ouvrir un nouveau compte auprès d'un fournisseur de services financiers peuvent donc procéder sans aucune contrainte:

a) Un client se rend au bureau local du fournisseur de services financiers.

b) Il saisit son numéro d'identification national et fournit son empreinte digitale.

c) Une notification de divulgation l'informe des données qu'il s'apprête à partager avec le fournisseur de services.

d) S'il y consent, les données sont transmises depuis son portefeuille au fournisseur de services financiers.

e) Ce dernier utilise ces données pour vérifier l'identité du client, satisfaire aux exigences de conformité en matière de KYC et ouvrir le compte.

5.2 Normes ouvertes

Le protocole Kiva adhère aux Principes d'identification pour le développement durable, qui préconisent l'élaboration de normes ouvertes et la neutralité des fournisseurs dans la conception des systèmes d'identité numérique afin d'encourager l'innovation et de garantir l'efficacité ainsi que la durabilité financières et opérationnelles [8]. Une grande partie du code de base utilisé dans le protocole Kiva est hébergée par la Linux Foundation au sein du projet à code source ouvert Hyperledger. Les sous-projets principaux faisant partie d'Hyperledger sont [9] [10]:

a. **Hyperledger Indy**: des outils, bibliothèques et composants réutilisables visant à fournir des identités numériques contenues dans des blockchains afin de faciliter leur interopérabilité sur le plan administratif, d'une application à l'autre et avec tout autre silo de données [11].

b. **Hyperledger Aries**: une boîte à outils partagée, réutilisable et interopérable conçue pour élaborer des solutions axées sur la création, la transmission et le stockage d'identifiants numériques vérifiables dans le cadre d'interactions de pair-à-pair au sein d'une blockchain [12].

c. **Hyperledger Ursa**: une bibliothèque cryptographique partagée conçue pour éviter de dupliquer d'autres travaux de chiffrement et augmenter le niveau de sécurité du système [13].

d. **Groupe de travail sur l'identité du projet Hyperledger**: un groupe de discussion, de recherche ainsi que de documentation des méthodes de capture, de stockage, de transmission et d'utilisation des identités dans la blockchain dans le cadre de sous-projets faisant partie d'Hyperledger [14].

Afin d'assurer la compatibilité entre les différents protocoles mis en œuvre de façon indépendante, la communauté Hyperledger maintient un répertoire de types de messages et de protocoles ratifiés généralement acceptés comme nécessaires, à condition que le logiciel en question les prenne en charge. L'état actuel de l'interopérabilité peut être consulté dans le répertoire Aries-RFC, dans la section "Aries Interoperability Profile RFC" [15].

L'interopérabilité, l'efficacité et les effets atteignables de réseau constituent un grand avantage de ce type de protocole d'identité normalisé:

a) **Absence de verrouillage de fournisseur.** Le protocole Kiva est un logiciel à code source ouvert. Cela signifie que le maintien ou la modification du système par l'entité chargée de sa mise en œuvre (généralement un organisme gouvernemental ou un partenariat public-privé) ne dépend pas d'un seul fournisseur.

b) **Normes.** Les normes et la terminologie techniques sont partagées au sein de la communauté des logiciels à code source ouvert, ce qui simplifie considérablement l'intégration du protocole Kiva dans les systèmes nouveaux ou existants des gouvernements, des fournisseurs de services financiers et d'autres entités autorisées.

c) **Interopérabilité et extensibilité.** Le protocole Kiva peut être étendu au-delà de la vérification reposant sur le processus d'e-KYC. Il est par exemple possible d'y ajouter des services adjacents tels que l'enregistrement d'entités commerciales, les permis de conduire numériques, l'identité numérique des électeurs, les données de santé portables, ou encore, les dossiers scolaires vérifiables. De plus, étant donné que le protocole Kiva étend la fonctionnalité des systèmes d'identification existants – qu'il s'agisse de systèmes d'identification nationaux, d'identités fonctionnelles ou de listes d'éligibilité aux services de protection sociale – il peut être déployé sans interruption dans le cadre des programmes des secteurs public et privé.

d) **Résilience.** La nature libre du protocole Kiva en garantit la résilience dans la mesure où aucune partie externe ne peut révoquer l'utilisation du système. En plus de supprimer le verrouillage des fournisseurs, même en cas de coupure d'accès externe au système, les opérateurs locaux seraient en mesure de fournir une copie à jour des données du registre. Les clients pourraient ainsi continuer à effectuer de nouvelles transactions au niveau local jusqu'à ce que les mises à jour soient réintégrées dans le système national.

5.3 État d'avancement de la mise en œuvre

Une fois l'infrastructure des portefeuilles numériques mise en place, Kiva a commencé à prendre en charge les intégrations d'API des fournisseurs de services financiers dans la NDIP en début 2020. Une fois achevé, ce travail d'intégration permettra aux citoyens de transmettre leurs identifiants vérifiables depuis leur portefeuille numérique directement aux systèmes bancaires de base des vérificateurs (fournisseurs de services financiers). Compte tenu des capacités techniques limitées dans l'ensemble du secteur – en particulier dans les provinces reculées de la Sierra Leone – les équipes de Kiva présentes dans le pays ont travaillé en étroite collaboration avec les premiers fournisseurs de services financiers partenaires pour veiller à ce que la vérification d'identité effectuée sur la NDIP s'intègre parfaitement aux flux de travail existants ainsi qu'aux processus d'accueil des clients.

6 Introduction à la spécification ADIA pour les systèmes d'identification décentralisée

L'Accountable Digital Identity Association (ADIA) est une spécification technologique de l'Alliance DID. L'Alliance DID est une association industrielle ouverte dont l'objectif est d'orienter l'élaboration d'un cadre normalisé et interopérable visant à aider les services d'identification décentralisée à garantir l'authenticité des identités numériques ainsi que la fiabilité du processus de vérification. Ce groupe contribuera à la création d'un écosystème mondial, à la formation et à la gestion d'un réseau collaboratif, à la diffusion de technologies normalisées ainsi qu'au développement du secteur de l'identité décentralisée.

La finalité de la spécification ADIA est d'instaurer une interopérabilité effective entre les systèmes d'identification décentralisée en déployant les technologies et les processus requis qui se trouvent en-dehors du champ d'application d'initiatives existantes menées dans le domaine de l'interopérabilité, notamment par le W3C, la Fondation pour l'identité décentralisée (DIF) et le projet Hyperledger Aries. À cette fin, la spécification ADIA porte sur trois domaines principaux:

- **Localisation de sources fiable**

L'ADIA s'appuie sur des sources fiables pour vérifier l'identité numérique des individus. Le fonctionnement du système ADIA est basé sur la recommandation X.1254 de l'UIT-T, qui prévoit la vérification de l'identité pendant le processus de validation d'un individu en amont de l'attribution de l'adresse numérique. Le processus de résolution d'identité y est intégré afin de garantir l'unicité de l'individu avec les domaines.

- **Prise en charge des transactions entre les registres**

Le système ADIA part du principe que les informations d'identité sont stockées en nuage et qu'elles sont liées à un portefeuille numérique ainsi qu'à un registre spécifiques. L'ADIA utilise des techniques basées sur l'informatique en nuage pour s'assurer que n'importe quelle application peut tenir compte des demandes des individus, l'interopérabilité étant par ailleurs assurée par des protocoles standard basés sur le nuage.

- **Inclusivité**

L'ADIA est une plate-forme ouverte: tout participant peut faire partie du système et y contribuer sans être tributaire d'un système de redevances ou de règles.

L'Alliance DID cherche à réaliser le plein potentiel des systèmes d'identification décentralisée grâce à l'interopérabilité commerciale et technologique en contribuant à résoudre certains des principaux défis pratiques liés à leur fonctionnement ainsi qu'à leur adoption.

6.1 Comment fonctionne l'ADIA?

Le système ADIA, une fois mis en œuvre, permettra aux fournisseurs de services en ligne et hors ligne de mener facilement le processus d'e-KYC en s'appuyant sur les plates-formes de DID connectées disponibles. Ces plates-formes pourront interagir et identifier les utilisateurs par le biais d'une adresse numérique.

6.1.1 Format d'adresse numérique

L'objectif est que l'adresse numérique ADIA soit conforme au format standard du W3C pour les DID.

Pour l'ADIA, le format proposé est le suivant:

did:adia:1234567ABCDEFGHI

Cette adresse serait conforme à la norme du W3C et pourrait être résolue à l'aide du projet de résolveur universel proposé par la DIF.

Elle se compose des éléments standard d'un DID:

a) Un identificateur de schéma URL (DID);

b) Un identificateur (proposé) pour la méthode DID (ADIA);

c) Un identificateur spécifique à la méthode DID (qui serait la propriété de l'ADIA et impliquerait de suivre le processus de "désambiguïsation de l'identité" en attente d'obtenir le brevet de l'Alliance DID).

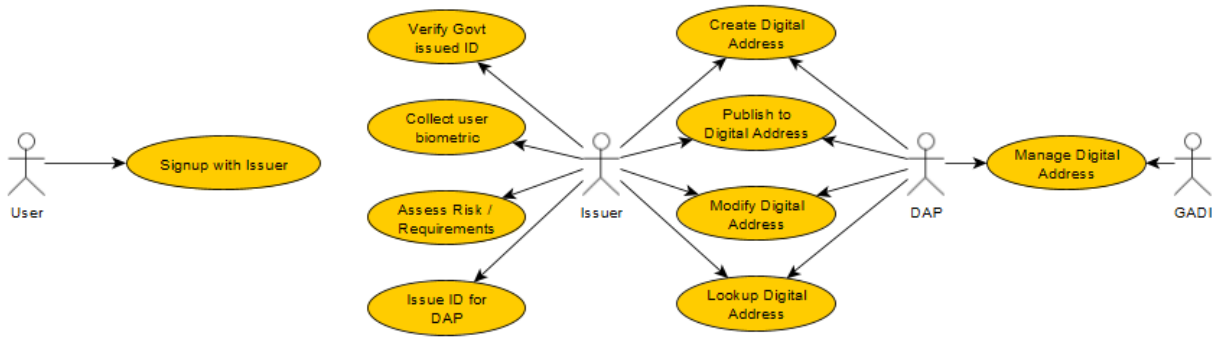
6.1.2 Émission de l'adresse numérique

Il existe deux types d'émetteurs dans l'écosystème ADIA: les émetteurs d'identifiants vérifiables et les émetteurs d'adresses numériques. Les DAP sont capables de vérifier l'identité de leurs clients en vue de répondre aux exigences réglementaires relatives au processus de KYC. Les émetteurs d'identifiants vérifiables utilisent la capacité de KYC des adresses numériques afin d'ajouter d'autres revendications d'identité en tant qu'identifiants vérifiables.

L'adresse numérique est un identifiant ADIA spécial délivré à un individu par un DAP certifié au terme du processus de KYC en face à face. Les candidats à cette certification peuvent être des entités telles que des banques qui ont ouvert des comptes en personne, certaines agences gouvernementales, des assureurs, etc. À l'aide d'un capteur biométrique spécialisé, l'émetteur pourra combiner une caractéristique biométrique de l'utilisateur à d'autres caractéristiques liées à l'identité (telles que le prénom, le nom, la date de naissance, la ville de naissance, etc.) et, une fois qu'il aura appliqué un algorithme de hachage, générer une adresse numérique en collaboration avec un DAP participant. Les DAP sont des fournisseurs de solutions qui proposent actuellement des services d'identité liés au concept d'identité décentralisée. L'adresse numérique peut être délivrée dans un portefeuille sécurisé par la FIDO sur le smartphone de l'utilisateur (ou d'autres supports) ou être présentée sous forme de carte sécurisée par un code PIN défini par l'utilisateur. Dans les deux cas, l'adresse numérique est étroitement attachée à l'utilisateur par la combinaison de ses attributs d'identité et de ses mesures biométriques.

Le DAP a accès à un nombre limité d'API (créer l'adresse numérique, publier l'adresse numérique et mettre à jour l'adresse numérique). Celles-ci peuvent également être utilisées pour révoquer les identifiants au besoin.

Figure 9: Émission de l'adresse numérique de l'utilisateur



6.1.3 Modèle en couches du système ADIA

Le modèle en couches du système ADIA distingue les services basés sur l'identité au niveau de la couche commerciale de ceux situés au niveau de la couche de sécurité du réseau ainsi que de celle des données (voir figure 10). Il s'agit ici d'établir une couche d'identité fiable et compatible avec la logique commerciale tout en la protégeant par une couche de sécurité des données.

6.2 Utilisation des codes QR dans le système ADIA

Les codes QR font partie intégrante des flux d'authentification modernes, notamment pour les adresses numériques. Un comité technique a été formé au sein de l'Organization for the Advancement of Structured Information Standards (OASIS) afin de traiter de certains problèmes de flux d'authentification ayant recours aux codes QR et d'établir des directives visant à renforcer la sécurité de ces derniers. Le comité technique d'OASIS étudiera les méthodes basées sur les codes QR que les partenaires utilisateurs et les fournisseurs de services en ligne utilisent actuellement pour authentifier les identités numériques. Il comparera ces méthodes en vue de proposer un ensemble de protocoles fiables aux fournisseurs de services. Cet ensemble de protocoles permettra d'effectuer des authentifications sans identifiants ni mot de passe statiques, de renforcer progressivement le

processus de vérification d'identité, d'atténuer les risques et d'améliorer le degré de certitude du processus d'authentification.

Figure 10: Modèle en couches du système ADIA

6.3 Flux d'utilisateurs dans le cadre du processus d'e-KYC

6.3.1 e-KYC en personne

Un utilisateur souhaitant s'identifier lors d'une interaction en personne devra présenter les attributs d'identité nécessaires pour répondre aux exigences établies par le fournisseur de services (par exemple, un individu souhaitant ouvrir un nouveau compte bancaire dans une agence locale).

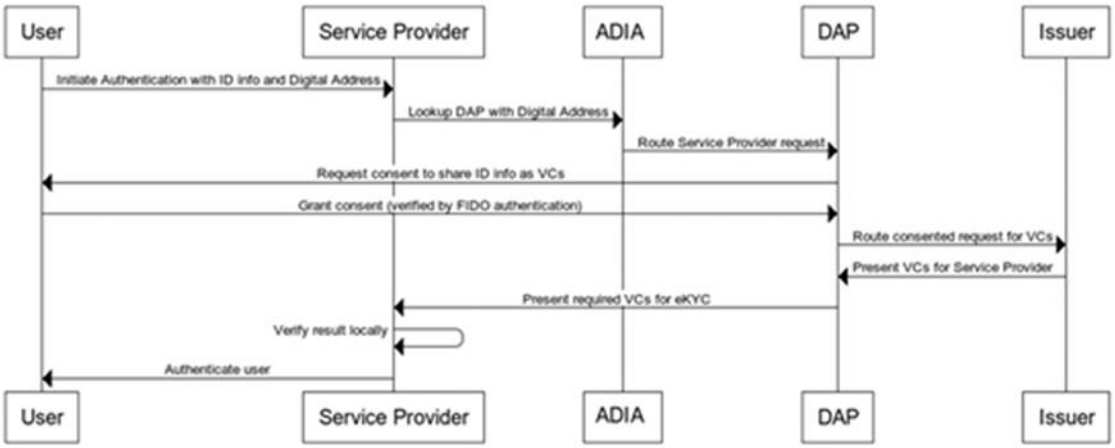
L'utilisateur devra ainsi fournir son adresse numérique en plus de son nom, de son adresse, de son lieu de travail, etc. Le fournisseur de services peut vérifier les attributs d'identité de l'utilisateur ainsi que son adresse numérique via une interface en ligne du système ADIA. Lorsque le fournisseur de services saisit les données de l'utilisateur ainsi que son adresse numérique, la demande d'identifiant vérifiable basé sur l'identité décentralisée (ainsi que les champs de données d'identité demandés) est envoyée au DAP chargé de fournir le portefeuille d'identifiants de l'utilisateur. L'utilisateur reçoit une notification sur son appareil intelligent lui demandant de consentir à fournir les attributs d'identité demandés par le fournisseur de services. Une fois que l'utilisateur a donné son consentement et s'est identifié localement sur son appareil à l'aide de l'authentification FIDO, le DAP peut envoyer les identifiants vérifiables au fournisseur de services.

6.3.2 Processus d'e-KYC à distance (inscription en ligne sur un site Web ou une application)

Le système fonctionne de manière identique, cependant, au lieu de présenter ses données d'identité en personne afin que le fournisseur de services les saisisse dans son terminal, l'utilisateur saisit lui-même les données d'identité à vérifier ainsi que son adresse numérique.

Le niveau de contrôle de l'identité de l'utilisateur est le même à distance qu'en personne puisque le contrôle de l'adresse numérique originale est sécurisé par un processus d'enregistrement FIDO au moment de l'émission.

Figure 11: Processus d'e-KYC utilisant le système ADIA pour rechercher les identifiants vérifiables gérés par le DAP



6.4 Interopérabilité des portefeuilles du système ADIA

Comme mentionné ci-dessus, de nombreux projets de plates-formes d'identité sont basés sur les registres et axés sur l'identité décentralisée. Ce qui différencie le projet ADIA de l'Alliance DID, c'est l'accent mis sur l'interopérabilité des registres. En exploitant les possibilités des protocoles de communication existants (comme le projet Hyperledger Aries et DIDCOM de la DIF pour les flux d'identité, ainsi que la couche de contrats intelligents pour les flux commerciaux), l'ADIA pourra les rendre opérationnels dans différents systèmes de registres au lieu de se limiter aux instances d'une seule et même technologie de registres. La communication entre les registres, en plus d'offrir la possibilité de confier le règlement des paiements effectués entre les registres à des teneurs de marchés tiers (qui peuvent fournir différents types de jetons), permet d'instaurer un écosystème souple qui tire parti de chacune de ses composantes afin d'optimiser les performances dans leur ensemble.

L'abandon des identifiants spécifiques à un dispositif donné atténue également d'autres difficultés (par exemple, la prise en charge de plusieurs appareils). Les portefeuilles peuvent être conçus de manière à contrôler les métadonnées d'authentification en nuage créées à partir des données réelles de l'émetteur et contrôlées par l'utilisateur par le biais des interactions avec l'authentification forte (par exemple, FIDO).

6.4.1 Interopérabilité du système ADIA avec la norme FIDO

Le système ADIA utilise l'authentification FIDO au niveau de la couche des applications pour veiller à ce que l'accès aux identifiants vérifiables soit protégé par un processus d'authentification sécurisé. N'importe quel protocole FIDO peut être utilisé pour sécuriser

l'accès au portefeuille de l'application ADIA. L'interopérabilité est assurée au niveau de la couche d'authentification et garantit l'utilisation de produits certifiés par la FIDO.

6.4.2 Sécurité des codes QR

Les méthodes d'authentification sans mot de passe par code QR sont vulnérables aux attaques par interception. Un groupe de travail d'OASIS cherche actuellement à sécuriser l'utilisation des codes QR dans le cadre des processus d'authentification sans mot de passe.

6.5 Normalisation

Le travail de normalisation de l'Alliance DID ne vise pas à élaborer de nouveaux protocoles, mais plutôt à normaliser l'interopérabilité des protocoles existants. Il porte en outre sur la publication d'un schéma commun pour les identités et identifiants utilisés dans certains secteurs cibles (par exemple, les soins de santé, les services financiers, etc.).

Grâce à la mise en œuvre du système ADIA et à l'application d'une norme mondiale, les diverses solutions d'identification basées sur les DID pourront être décloisonnées. Tout émetteur ou fournisseur de services souhaitant tirer parti de l'authentification basée sur les DID ou du processus d'accueil des clients n'aura plus à déterminer la meilleure solution à intégrer, en espérant avoir choisi la pile logicielle la plus performante. Les émetteurs auront la garantie que les identifiants qu'ils émettent pourront éventuellement atteindre un public mondial de fournisseurs de services. De même, les fournisseurs de services pourront traiter n'importe quel type d'identifiant vérifiable certifié par l'ADIA. Étant donné que les données d'identité personnelles associées sont conservées en sécurité chez l'émetteur de l'identité d'origine, les organisations situées dans les pays disposant de contrôles d'exportation de données stricts sont également autorisées à participer dans la mesure où aucune donnée d'identité personnelle ne peut passer les frontières.

En parallèle des technologies, des normes sont requises pour établir les "rôles en matière d'identité" ou "les responsabilités". Ce système s'appuie sur la capacité des organismes concernés à déterminer la légitimité ainsi que la fonctionnalité des identifiants en vue de créer et d'utiliser des identifiants portables qui indiquent le statut de chaque individu (par exemple, s'il s'agit d'un étudiant ou d'un médecin). Il est par ailleurs possible de créer des identifiants qui peuvent être utilisés dans le cadre de transactions financières tout en répondant aux normes mondiales en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.

7 Principes recommandés pour l'établissement d'une norme relative aux DID à des fins d'e-KYC

La pandémie de COVID-19 a accéléré le rythme de la numérisation des paiements publics. Du commerce électronique aux banques directes, en passant par le processus d'accueil à distance dans le secteur de la finance numérique, tous les services subissent une transformation numérique qui vise à simplifier l'expérience des utilisateurs. Toutefois, compte tenu des menaces majeures en matière de sécurité telles que la fraude aux transactions, l'usurpation d'identité et d'autres cyberattaques compromettant les données personnelles des clients, il est désormais essentiel de prendre des mesures pour protéger les données ainsi que la vie privée des usagers dans le cadre des interactions numériques. Des solutions émergentes basées sur la technologie de blockchain telles que l'identité décentralisée et les identifiants vérifiables ont le potentiel de révolutionner le domaine de l'identité et de la vérification en protégeant la confidentialité des données, en partageant les données avec le consentement de l'utilisateur

ainsi qu'en sécurisant les transactions, tout en améliorant le processus d'e-KYC global et l'expérience utilisateur.

Un DID est un type d'identité centrée sur l'utilisateur créé, possédé et géré par les utilisateurs de leur plein gré (on parle parfois d'identité souveraine). L'utilisateur est identifié par un DID unique au monde. Chaque DID est associé à un matériel cryptographique qui permet d'authentifier les utilisateurs et de vérifier les identifiants qui leur sont délivrés ou qu'ils présentent. Les identifiants vérifiables permettent aux utilisateurs d'émettre des identifiants de façon numérique et d'y apposer une signature numérique. Ce processus peut être vérifié à l'aide du registre distribué ou de la blockchain. Divers identifiants tels que les diplômes, les antécédents professionnels, les données personnelles, les licences, les certificats, etc. sont ainsi mis à disposition des parties autorisées de manière inviolable et authentifiée.

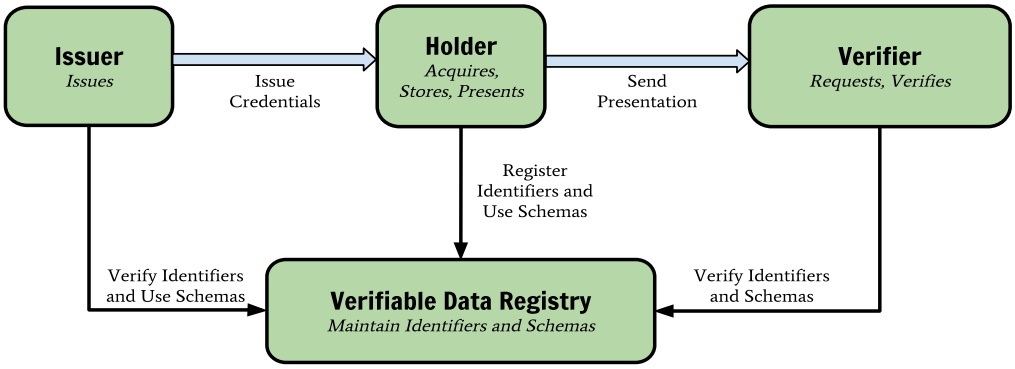
Le registre distribué ou la blockchain constituent la clé de voûte du système d'identité décentralisée. Les DID des utilisateurs peuvent être privés ou publics. L'utilisation de l'identité décentralisée à des fins d'e-KYC est renforcée lorsque les utilisateurs acquièrent les identifiants de manière numérique auprès de l'émetteur (une organisation gouvernementale). Les identifiants sont acquis et stockés numériquement dans un portefeuille d'identité. Ils peuvent également être présentés à des organismes de services financiers, qui peuvent procéder aux vérifications de façon numérique afin de simplifier le processus d'accueil et la vérification de l'identité à distance. Cette section étudie les exigences en matière d'établissement d'une norme relative aux DID ayant recours à des registres distribués et aux identifiants vérifiables à des fins d'e-KYC dans le secteur de la finance numérique. Cette norme portera sur les domaines suivants:

- La création du DID et l'ancrage en vue d'effectuer les opérations d'identification telles que le processus d'e-KYC;
- L'émission de l'identifiant vérifiable par l'émetteur, sa remise et l'enregistrement des informations liées à son émission dans le registre distribué;
- Le processus de présentation, à savoir l'action la plus couramment requise par les vérificateurs pour vérifier l'identité de l'utilisateur (par exemple, dans le cadre du processus d'e-KYC) avant de fournir le service.

7.1 Rôles des parties prenantes et échange d'informations

La figure 12 illustre les principaux rôles des parties prenantes impliquées et le flux d'informations.

Figure 12: Rôles et relations des parties prenantes



Les principaux rôles des parties prenantes et les flux d'informations sont décrits ci-dessous:

Émetteur

Une entité qui fait valoir des revendications concernant un ou plusieurs sujets, crée un identifiant vérifiable sur la base de ces revendications et transmet cet identifiant à un titulaire. Dans le contexte de la finance numérique, il pourrait s'agir d'une entité gouvernementale ou de toute autre entité disposant d'un mandat qui lui permet d'émettre un identifiant basé sur l'identité nationale du titulaire. Ces identifiants vérifiables sont détenus dans des portefeuilles numériques contrôlés par les citoyens.

Vérificateur

Une entité qui reçoit une ou plusieurs présentations vérifiables à traiter. Dans certains contextes, elle est qualifiée de partie utilisatrice. Dans le domaine de la finance numérique, le vérificateur est la partie qui effectue la vérification reposant sur le processus d'e-KYC (par exemple, le fournisseur de DFS).

Titulaire

Une entité qui possède un ou plusieurs identifiants vérifiables. Le titulaire est généralement, mais pas toujours, le sujet des identifiants vérifiables qu'il détient. Les titulaires stockent leurs identifiants dans des référentiels d'identifiants. Tout titulaire disposant d'un identifiant délivré par le gouvernement sera en mesure d'authentifier de manière sécurisée son identité officielle auprès des fournisseurs de DFS afin de faciliter le processus d'e-KYC mené pour l'ouverture de nouveaux comptes ainsi que pour les opérations de diligence voulue à l'égard de la clientèle.

Registre de données vérifiables

Un système qui agit en tant qu'intermédiaire dans le cadre de la création et de la vérification d'identifiants, de clés et d'autres données pertinentes telles que les schémas d'identifiants vérifiables et les registres de révocation, qui peuvent être nécessaires pour utiliser les identifiants vérifiables. Dans le cas du processus d'e-KYC pour les DFS, il s'agirait d'un réseau de nœuds contenant un registre public de DID. Ce registre garantit la fiabilité des identifiants numériques utilisés dans le cadre des vérifications d'identité.

Identifiants vérifiables

Extrait de la spécification relative au modèle de données des identifiants vérifiables du W3C:

Les identifiants vérifiables peuvent représenter les mêmes informations que les identifiants physiques. L'avènement de nouvelles technologies telles que les signatures numériques

complique la falsification des identifiants vérifiables. Ces derniers sont par conséquent plus fiables que leurs équivalents physiques.

Il est possible d'envoyer un message spécifique du titulaire à l'émetteur (à l'aide d'un mécanisme de communication hors chaîne) afin de déposer une demande d'identifiant vérifiable. Les informations d'identité sont intégrées dans l'identifiant vérifiable remis au titulaire par l'émetteur par le biais d'un canal sécurisé hors chaîne. Ces informations ne seront jamais envoyées ni stockées dans le registre distribué. Un mécanisme de contrôle (par exemple, une signature) est intégré à l'identifiant vérifiable.

Présentations

Les titulaires/utilisateurs peuvent générer des présentations et les partager avec les vérificateurs pour prouver qu'ils possèdent des identifiants vérifiables présentant certaines caractéristiques. Ces identifiants et présentations peuvent être transmis plus rapidement que leurs équivalents physiques. Ils sont dans ce sens plus pratiques et plus fiables.

Lorsqu'un titulaire souhaite accéder à un service financier numérique, le vérificateur peut avoir besoin de rassembler certaines informations à son sujet avant d'accepter de fournir le service en question. Les informations spécifiques requises sont demandées à l'aide d'une demande de présentation dans laquelle doivent être spécifiées la finalité de la collecte ainsi que les informations minimales requises pour l'accès à ce service.

Le titulaire envoie alors une réponse vérifiable comprenant les identifiants adéquats parmi ceux stockés dans son portefeuille (et non dans le registre distribué). Il est possible que le titulaire ait besoin d'enregistrer les informations relatives au processus de présentation sur un registre distribué. D'autres informations relatives à la réception de ces données peuvent être enregistrées indépendamment par le vérificateur dans le même registre distribué.

7.2 Exigences en matière de vérification d'identifiants

Voici les exigences proposées pour les identifiants vérifiables (demande, émission, remise et réception):

a) Le contenu doit être conforme à la recommandation du W3C "Verifiable Credentials Data Model 1.0".
b) Les identifiants vérifiables doivent prendre en charge les schémas de dénomination des attributs existants et futurs tels que X.520, schema.org, ISO 20022 ou les normes spécifiques au secteur.
c) Les identifiants vérifiables doivent inclure les informations suivantes:
    - Des informations générales sur la finalité de leur utilisation;
    - L'identificateur de l'identifiant vérifiable;
    - Des informations sur le titulaire, y compris la liste de ses attributs, conformément à la demande, et son DID;
    - Les informations sur l'émetteur, y compris son DID;
    - La date d'émission de l'identifiant vérifiable;

- Les métadonnées sur le système de gestion de l'identité numérique utilisé, par exemple le niveau de fiabilité des attributs du titulaire;
- La signature numérique de l'émetteur; et
- La date d'expiration de l'identifiant vérifiable, le cas échéant.

d) Demande d'identifiant vérifiable par le titulaire/l'utilisateur.
   - Le titulaire doit envoyer la demande à un émetteur au moyen d'un canal sécurisé hors chaîne avec une preuve mutuelle de possession par DID.

e) Émission d'identifiants au titulaire.
   - Les émetteurs ne doivent créer des identifiants qu'en réponse à une demande du titulaire.
   - Toutes les informations contenues dans la recommandation du W3C "Verifiable Credentials Data Model 1.0" doivent être respectées par l'émetteur.
   - Une fois créé, l'identifiant vérifiable doit être envoyé au titulaire à l'aide d'un
   - canal sécurisé hors chaîne avec une preuve mutuelle de possession par DID.
   - L'émetteur ne doit pas partager les identifiants vérifiables avec d'autres entités.
   - L'émetteur doit enregistrer l'événement d'émission dans le registre distribué.
   - L'émetteur doit enregistrer l'événement de remise dans le registre distribué.
   - L'identifiant vérifiable ne doit pas être enregistré directement dans le registre distribué.

f) Réception de l'identifiant vérifiable
   - La signature numérique de l'identifiant vérifiable doit être validée à sa réception.
   - L'identifiant vérifiable peut être accepté, ou non, par le titulaire/l'utilisateur.
   - L'identifiant vérifiable doit être stocké dans un portefeuille numérique sous le contrôle exclusif du titulaire, dans son format original et sans aucune modification de contenu.
   - La réception de l'identifiant vérifiable peut être enregistrée sur le registre distribué, après acceptation, par le titulaire.

7.3 Identificateurs décentralisés

Les spécifications relatives aux DID ont été conçues pour établir un espace de noms d'identifiants vérifiables grâce à des techniques de chiffrement et adressables à l'échelle mondiale dans les systèmes de registres distribués et de blockchain. Les DID constituent le schéma d'adressage utilisé pour les identifiants vérifiables.

La conception de DID doit reposer sur les principes suivants:

a) Décentralisation: L'architecture du DID est telle qu'il ne devrait plus être nécessaire d'avoir recours aux autorités centralisées ou aux points de défaillance uniques pour assurer la gestion des identités, notamment en ce qui concerne l'enregistrement des identifiants uniques au niveau mondial, des clés de vérification publiques, des points de terminaison de services et d'autres métadonnées.
b) Contrôle des identifiants par les entités: L'architecture du DID devrait donner aux entités, humaines et non humaines, le pouvoir de contrôler directement leurs propres identifiants numériques sans l'intervention d'autorités externes.
c) Protection des informations personnelles identifiables: L'architecture du DID devrait permettre aux entités de contrôler les données identifiables de leurs identités numériques ainsi que de divulguer leurs attributs ou d'autres données d'identité de façon minimale, sélective et progressive.

d) Sécurité: L'architecture du DID doit garantir un degré de sécurité suffisant pour que les parties utilisatrices puissent se fier aux DID pour leur niveau d'assurance requis.
e) Mise à disposition de preuves: L'architecture du DID doit permettre aux entités de fournir une preuve cryptographique d'authentification ainsi qu'une preuve des droits d'autorisation.
f) Accessibilité: L'architecture du DID doit permettre aux entités d'accéder aux DID d'autres entités pour en savoir plus à leur sujet ou interagir avec elles.
g) Interopérabilité: L'architecture du DID doit utiliser des normes interopérables afin que l'infrastructure des DID puisse utiliser les outils et bibliothèques logicielles conçus à des fins d'interopérabilité.
h) Portabilité: L'architecture du DID doit être indépendante des systèmes et des réseaux et permettre aux entités d'utiliser leurs identités numériques dans tout système compatible avec les DID et les méthodes de DID.
i) Simplicité: Pour atteindre ces objectifs de conception, l'architecture du DID doit être "aussi simple que possible".
j) Extensibilité: Lorsque c'est possible, l'architecture du DID doit permettre l'extensibilité des identifiants, à condition qu'elle n'entrave pas excessivement leur interopérabilité, leur portabilité ou leur simplicité.

Extrait du projet de spécification relative aux DID du W3C:

a) L'émergence de la DLT, parfois appelée technologie de la blockchain, offre la possibilité de gérer les identités de façon entièrement décentralisée. Dans les systèmes d'identification décentralisée, les entités sont libres d'utiliser n'importe quelle base de confiance partagée. Les registres distribués à l'échelle mondiale (ou tout réseau de pair-à-pair décentralisé offrant des capacités similaires) permettent de gérer une base de confiance sans autorité centralisée ni point de défaillance unique. De même, les registres distribués et les systèmes d'identification décentralisée permettent aux entités de créer et de gérer leurs propres identifiants sur un nombre indéfini de bases de confiance distribuées et indépendantes.

b) Les entités sont identifiées par des DID. Elles peuvent s'authentifier en utilisant des preuves (par exemple, signatures numériques, protocoles biométriques préservant la confidentialité, etc.). Les DID orientent vers des documents de DID. Un document de DID contient un ensemble de points de terminaison de services qui permettent d'interagir avec l'entité. Conformément au principe de confidentialité dès la conception, chaque entité peut avoir autant de DID que nécessaire afin de respecter la séparation souhaitée des identités, des avatars et des contextes.

c) Pour utiliser un DID avec un registre distribué ou un réseau donné, il convient de définir une méthode de DID dans le cadre d'une spécification de méthode de DID distincte. La méthode de DID spécifie l'ensemble des règles d'enregistrement, de résolution, de mise à jour et de révocation des DID sur le registre ou réseau en question.

d) Il n'est ainsi plus nécessaire de disposer d'identifiants pour accéder aux registres centralisés ni d'avoir recours aux autorités de certification centralisées pour assurer la gestion des clés – le modèle standard de PKI hiérarchique. Les DID résident dans

un registre distribué; chaque entité peut donc servir d'autorité de base. Cette architecture est appelée PKI décentralisée (DPKI).

7.4 Exigences relatives aux DID et authentification

Voici certaines des exigences proposées pour les DID:

a) Les entités doivent être en mesure de gérer leurs propres DID sur un registre distribué à l'aide d'une méthode de DID.
b) La méthode de DID doit être conforme au projet de spécification du W3C "Decentralized Identifiers (DIDs) v1.0".
c) La méthode de DID doit garantir que le titulaire/l'utilisateur est le propriétaire exclusif du DID (par exemple, avec la clé privée correspondant à la clé publique utilisée pour authentifier le contrôleur du DID).
d) Lorsqu'elle est assistée par un tiers dans le processus de création du DID, toute partie doit toujours conserver le contrôle exclusif du DID.
e) Un DID doit être ancré dans un registre distribué.
f) Chaque DID doit pouvoir être systématiquement rattaché au document de DID correspondant.
g) Le document de DID peut être produit sur demande lors du déréférencement du DID; et
h) Le document de DID d'une personne physique ne doit pas être stocké dans un registre distribué, à l'exception de sa clé publique, qui pourrait être située sur le registre distribué.

Le processus d'authentification des DID permet aux titulaires de prouver qu'ils détiennent le contrôle sur leurs DID lorsque ces derniers interagissent avec un vérificateur (parfois appelé partie utilisatrice). L'authentification des DID doit être compatible avec les flux Web et mobiles.

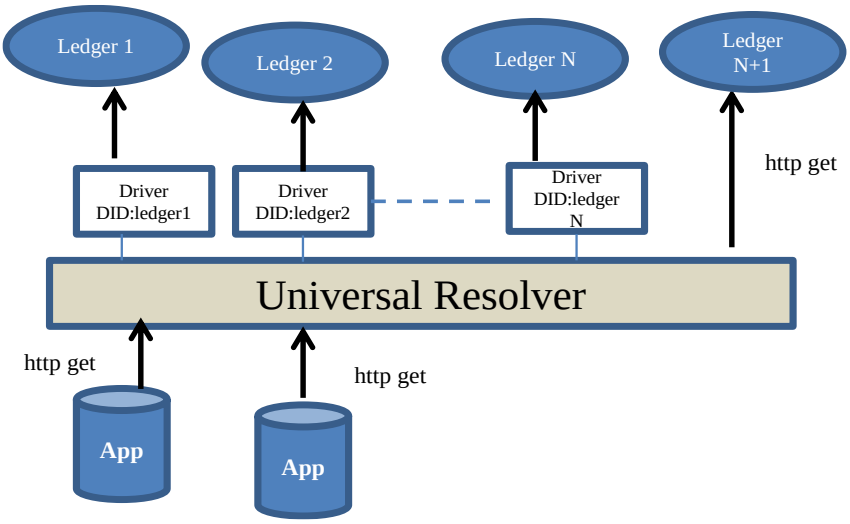
Le vérificateur doit suivre les étapes générales suivantes:

a) Le vérificateur récupère le document de DID associé au titulaire du DID.
b) Le vérificateur utilise la propriété d'authentification du document de DID pour déterminer la manière d'effectuer l'authentification, par exemple au moyen de signatures numériques, en établissant la preuve du contrôle d'une clé publique ou en utilisant un point de terminaison du service d'authentification.
c) Le vérificateur exécute le mécanisme d'authentification fourni.

7.5 Résolution des DID

La spécification du DID exige que chaque registre distribué soit doté d'une spécification de la méthode de DID qui décrive le déroulement des opérations de DID. La multiplicité des spécifications de méthodes de DID complique néanmoins la résolution des chaînes de texte (le DID), une étape requise pour localiser la base de confiance et le document de DID associé. La fonction de résolution des DID pourrait devenir un obstacle majeur à leur interopérabilité. Une architecture ainsi qu'un ensemble d'outils de résolution universels de DID, qui peuvent se baser sur n'importe quel DID valide pour produire un document de DID, sont ainsi à l'étude. Les résolveurs universels ont été conçus de manière à fonctionner avec les DID ainsi qu'à prendre en charge la résolution des DID sur de nombreux types de registres distribués. Le résolveur universel résout le problème des réseaux hétérogènes qui adoptent différentes spécifications de méthode pour leurs propres DID. La figure 13 illustre le concept de résolveur universel.

Figure 13: Résolveur universel de DID



7.6 Portefeuilles d'identité décentralisée

L'individu doit disposer d'un logiciel et/ou d'un dispositif lui permettant d'interagir avec le système d'identité décentralisée. Ces composants sont les agents et les portefeuilles.

La fonction principale d'un agent est de communiquer avec d'autres agents et de coordonner la résolution ainsi que l'authentification des DID. L'agent garde la trace des DID liés à d'autres entités du réseau. Un agent contient ou est connecté à un portefeuille dans lequel les clés de chiffrement secrètes sont conservées et protégées. Ce portefeuille contient les clés privées sans lesquelles l'individu ne peut ni prouver le contrôle d'un DID ni participer au système d'identité décentralisé. L'agent et le portefeuille contiennent des identifiants ainsi que des preuves vérifiables appartenant à l'individu.

Ce portefeuille peut être entièrement localisé sur l'appareil de l'utilisateur ou se présenter sous la forme d'un portefeuille virtuel dont une partie se trouve sur l'appareil mobile de l'utilisateur et l'autre, sur le nuage. Cette dernière configuration permet de créer des agents qui agissent au nom de l'utilisateur et exécutent des services sans que l'utilisateur ait à intervenir directement.

8 Références

[1] UIT, *Implementation of secure authentication technologies for digital financial services* (en ligne). Disponible à l'adresse suivante: https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Implementation%20of%20Secure%20Authentication%20Technologies%20for%20DFS.pdf.

[2] Alliance FIDO (en ligne). Disponible à l'adresse suivante: https://fidoalliance.org/.

[3] Alliance DID (en ligne). Disponible à l'adresse suivante: http://didalliance.org/content.php.

[4] W3C (en ligne). Disponible à l'adresse suivante: https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials.

[5] Groupe d'action financière, *Digital Identity* (en ligne). Disponible à l'adresse suivante: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf (consulté le 04/03/2021).

[6] SBP, "Circulaire BPRD n° 9 de 2016" (en ligne). Disponible à l'adresse suivante: http://www.sbp.org.pk/bprd/2016/C9.htm (consulté le 04/03/2021).

[7] W3C, "Verifiable Credentials Data Model v1.1" (en ligne). Disponible à l'adresse suivante: https://www.w3.org/TR/vc-data-model/ (consulté le 04/03/2021).

[8] Banque mondiale, *Principes sur l'identification pour un développement durable: Vers l'ère numérique* (en ligne). Disponible à l'adresse suivante: https://documents1.worldbank.org/curated/en/470971616532207747/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

[9] Linux Foundation (en ligne). Disponible à l'adresse suivante: https://www.linuxfoundation.org/.

[10] Hyperledger Foundation (en ligne). Disponible à l'adresse suivante: https://www.hyperledger.org/.

[11] Hyperledger Foundation, "Hyperledger Indy" (en ligne). Disponible à l'adresse suivante: https://www.hyperledger.org/use/hyperledger-indy.

[12] Hyperledger Foundation, "Hyperledger Aries" (en ligne). Disponible à l'adresse suivante: https://www.hyperledger.org/use/aries.

[13] Hyperledger Foundation, "Hyperledger Ursa" (en ligne). Disponible à l'adresse suivante: https://www.hyperledger.org/use/ursa.

[14] Hyperledger Foundation, "Groupe de travail sur l'identité" (en ligne). Disponible à l'adresse suivante: https://wiki.hyperledger.org/display/IWG.

[15] Hyperledger Foundation, "Hyperledger Aries" (en ligne). Disponible à l'adresse suivante: https://github.com/hyperledger/aries-rfcs/blob/master/index.md.

[16] W3C, "A simple example", exemple de DID (en ligne). Disponible à l'adresse suivante: https://www.w3.org/TR/did-core/#a-simple-example.

[17] Internet Identity Workshop, "DIF – Universal Resolver + Universal Registrar" (en ligne). Disponible à l'adresse suivante: https://iiw.idcommons.net/DIF_%E2%80%93_Universal_Resolver_%2B_Universal_Registrar_(DID%E2%80%99s_across_blockchains

[18] W3C, "DID method" (en ligne). Disponible à l'adresse suivante: https://www.w3.org/TR/did-core/#dfn-did-methods.

[19] OASIS, "OASIS Electronic Secure Authentication (ESAT) TC" (en ligne). Disponible à l'adresse suivante: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=esat.

[20] DIF, "DID Communication Working Group" (en ligne). Disponible à l'adresse suivante: https://identity.foundation/working-groups/did-comm.html.

[21] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant et M. Sabadello, "Decentralized Identifiers (DIDs) v0.11", 23 août 2018 (en ligne). Disponible à l'adresse suivante: https://w3c-ccg.github.io/did-spec/ (consulté le 20 septembre 2018).

[22] M. Sabadello, K. Den Hartog, C. Lundkvist, C. Franz, A. Elias, A. Hughes, J. Jordan et D. Zagidulin, "Introduction to DID Auth", 26 juillet 2018 (en ligne). Disponible à l'adresse suivante: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/did-auth.pdf (consulté le 15/03/2019).

[23] M. Sabadello, "A Universal Resolver for self-sovereign identifiers", 1er novembre 2017 (en ligne). Disponible à l'adresse suivante: https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c (consulté le 15/03/2019).

[24] D. Reed, J. Law, D. Hardman et M. Lodder, "DKMS (Decentralized Key Management System) Design and Architecture", 2 avril 2018 (en ligne). Disponible à l'adresse suivante: https://github.com/hyperledger/indy-sdk/blob/677a0439487a1b7ce64c2e62671ed3e0079cc11f/doc/design/005-dkms/DKMS%20Design%20and%20Architecture%20V3.md (consulté le 15/03/2019).