IDEMIA

Cinq facteurs déterminants pour la création d'un programme national d'identité numérique

IDENTITÉ

POSTÉ LE 08.30.24

Convaincues que l'identité juridique universelle jouera un rôle clé dans l'amélioration de la croissance économique et du bien-être des citoyens du monde, les Nations unies ont fixé l'objectif de garantir à tous une identité juridique d'ici à 2030.[1] Pour atteindre cet objectif, le manifeste de l'Alliance ID2020 de l'ONU soutient que le monde a besoin de l'efficacité, de l'évolutivité et de l'accessibilité renforcées que seule l'identité numérique peut offrir.[2]

Les registres d'état civil et les systèmes d'identité actuellement sous forme papier vont être dématérialisés. Pour les pays où aucun système n'existe à ce jour, la solution sera développée à partir de zéro. En réalité, il existe autant de types de systèmes que de pays, mais nous allons nous pencher ici sur les principaux éléments à considérer pour la sélection et le déploiement d'un programme national d'identité numérique.

Ce rapport examine les cinq facteurs déterminants à prendre en compte lors de la sélection et du déploiement d'un programme national d'identité numérique.

Facteur déterminant n° 1 : S'assurer que des lois, des règles et des normes strictes sont en vigueur

Avant d'étudier les systèmes et technologies d'un nouveau programme d'identité numérique, il convient d'établir une base juridique protectrice reposant sur des facteurs sociaux, économiques et politiques. De toute évidence, ces aspects relèvent des affaires intérieures d'un pays, mais le cadre juridique du pays doit être pleinement compris, car il sert à protéger toutes les personnes concernées par le système d'identité numérique.

Les pays doivent adopter des lois spécifiques régissant la création, l'exploitation et la gestion des systèmes d'identité numérique. Ces lois veillent à ce que le système respecte les mécanismes de protection nationales et internationales, telles que le règlement général sur la protection des données (RGPD) dans l'UE. Elles imposent des exigences strictes en matière de sécurité des données, de consentement et de droits individuels concernant les données personnelles.

La législation en matière de confidentialité et de protection des données établit des droits pour les titulaires des données, des exigences de consentement et des sanctions en cas d'abus. Une différence majeure entre les systèmes physiques et numériques est la quantité d'éléments d'identification contenus dans le document. Dans le cas d'une pièce d'identité physique, les éléments d'identification consultables par un tiers à des fins de vérification sont le nombre limité de données imprimées sur la carte d'identité ou le passeport, si la puce du document électronique n'est pas lue. En revanche, les systèmes d'identité numérique réunissent beaucoup plus d'informations. Les éléments d'identification, ainsi que d'autres données du titulaire du document, sont stockés afin de faciliter l'expérience de l'utilisateur lors de tâches administratives en partageant numériquement les données confiées au système et en évitant les erreurs typographiques. Toutefois, ces données sont ensuite potentiellement accessibles à tous les types de fournisseurs de

services. Il est donc crucial de mettre en place des règles strictes concernant les droits relatifs au consentement des titulaires d'une pièce d'identité numérique à ce que celle-ci soit partagée. La solution technique doit évidemment être élaborée en conformité avec la réglementation, mais elle doit également être basée sur une approche de contrôle et de consentement unique dès le départ. Une identité mobile peut, par exemple, être créée de telle façon que son titulaire peut sélectionner uniquement les attributs personnels spécifiques qui sont pertinents pour le tiers qui les demande, comme le fait d'avoir dépassé un certain âge.

Pour créer un système d'identité nationale interopérable qui inclut les pouvoirs publics, les fournisseurs de services et d'autres acteurs sur une seule plateforme, il est nécessaire d'ajouter une couche d'échange de données. Cette couche permettra au système de communiquer avec d'autres systèmes, en envoyant et recevant des informations. Le recours à des normes ouvertes garantit que différents systèmes et différentes plateformes peuvent communiquer et travailler ensemble.

Les utilisateurs suivront ainsi la même procédure, qu'ils interagissent avec une banque nationale ou étrangère, une entreprise de télécommunications ou tout autre fournisseur de services, et cela leur épargnera bien souvent le désagrément de devoir saisir à nouveau leurs informations à chaque nouvelle opération.

L'interopérabilité et la modularité des systèmes utilisés ne sont pas seulement cruciales pour les interactions entre le secteur public et le secteur privé. Elles sont également essentielle pour stimuler la concurrence entre les fournisseurs, tant pour la gestion des identités physiques que numériques. Cela encourage l'innovation et, en fin de compte, réduit les coûts au bénéfice des citoyens.

Étude de cas — Secteur des télécommunications

La convergence des normes dans le secteur des télécommunications a joué un rôle majeur dans l'interopérabilité mondiale et le progrès technologique.

Grâce à elle, les appareils peuvent communiquer sans obstacle sur différents réseaux et dans différentes zones géographiques, améliorant ainsi considérablement l'expérience utilisateur.

Cette convergence permet également la construction de réseaux d'opérateurs utilisant des composants de différents fabricants (par exemple, Nokia, Ericsson, Huawei), car leurs solutions peuvent interagir de façon fluide sur la base de ces normes. Si un opérateur souhaite changer l'un de ses fournisseurs, il peut le faire sans que cela ait de répercussions sur l'ensemble de son réseau.

Cette harmonisation des normes et cette interopérabilité ont favorisé le déploiement des technologies 4G et 5G, en favorisant des performances cohérentes, en réduisant les coûts et en encourageant l'innovation dans l'ensemble de l'industrie.

Facteur déterminant n° 2 : Renforcer l'efficacité de l'infrastructure existante

Décider de construire un système d'identité numérique en s'appuyant sur le système physique existant ou en partant de zéro n'est pas aussi évident qu'il y paraît. Partir d'un système d'identité physique et d'une base de données existants offre une base solide permettant d'accélérer le développement du système d'identité numérique, en tirant parti des données et de l'infrastructure existantes. L'accès du fournisseur à la « racine de confiance » peut offrir des avantages supplémentaires lors du paramétrage du système d'identité numérique basé sur des bases de données préexistantes. Dans de nombreux cas, nous avons pu voir que l'accès du fournisseur à une base de données existante facilitait le processus de création de la structure d'identité numérique. Le fournisseur existant maîtrise les spécifications du système ainsi que le cadre réglementaire du pays. Cela peut grandement accélérer la mise en place de systèmes

supplémentaires/adjacents tels que ceux nécessaires à une identité mobile, par exemple.

Cependant, l'évaluation nécessaire de l'infrastructure existante pourrait révéler la présence de plusieurs systèmes d'identité physique, notamment l'identité nationale, l'enregistrement fiscal, l'identification électorale et la couverture médicale, chaque système servant différentes finalités et ayant sa propre base de données et ses propres procédures. Ces systèmes sont souvent cloisonnés et nécessitent un mécanisme de vérification de l'identité unifié.

Le système Aadhaar en Inde est un bon exemple de la façon dont un ensemble préexistant de méthodes d'identification physique cloisonnées a été consolidé et transformé en un système d'identité numérique complet, entièrement fondé sur des données biométriques multiples qui garantissent le caractère unique de l'identité stockée.

Lorsque peu d'infrastructures existent pour l'enregistrement formel de l'état civil et la gestion de l'identité, bâtir le système de zéro peut s'avérer plus pratique. Dans ce cas, il est indispensable de faire participer les acteurs pertinents afin de recueillir les contributions des agences gouvernementales, des entreprises et des groupes de citoyens, et de définir les objectifs premiers tels qu'améliorer l'accès aux services gouvernementaux, renforcer la sécurité et faciliter les opérations numériques.

Étude de cas — Carte nationale d'identité électronique française (CNIe)

La carte nationale d'identité électronique française (CNIe) actuelle, lancée en 2021, permet aux citoyens français de réaliser des opérations en ligne depuis leur smartphone. Les citoyens reçoivent une demande d'authentification sur leur smartphone et l'application mobile lit et authentifie de façon sécurisée les données personnelles enregistrées dans la puce de la carte.

Le système d'identité numérique a obtenu une certification de sécurité de premier niveau (CSPN) de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), il respecte donc le règlement eIDAS de l'UE. Ce système protège les données d'identité du citoyen et garantit que seul le citoyen autorisé peut les gérer.

Facteur déterminant n° 3 : Choisir une technologie de pointe basée sur des années d'innovation

Il est essentiel d'utiliser la technologie de façon pertinente et responsable pour créer un système d'identité numérique moderne auquel les gouvernements et les citoyens font confiance. L'expertise nécessaire pour atteindre cet objectif repose sur des années d'innovation et d'expérience technique à la pointe de la gestion de l'identité et de la documentation sécurisée. Il n'est donc pas surprenant que seules quelques entreprises dans le monde disposent du savoir-faire requis pour réunir les technologies physiques et numériques nécessaires à la conception, à la construction et au maintien d'un système d'identité numérique.

Connaissance de la technologie et de la réglementation
Mener un projet de démonstration de faisabilité avec les clients pour mettre en pratique leurs cas d'utilisation et réaliser des tests d'interopérabilité avec d'autres acteurs majeurs de l'industrie sont deux étapes indispensables dans la construction des fondations de la technologie la plus solide d'un programme national d'identité numérique.

Les entreprises doivent faire constamment preuve de clairvoyance et investir dans la R&D pour s'assurer que les solutions d'identité numérique proposées restent à jour et conformes aux normes en constante évolution du secteur. En ce qui concerne le secteur de l'identité numérique, l'accent a été mis ces dernières années sur la mise en œuvre des normes ISO/IEC 18013-5, mais aujourd'hui, OpenID4VC et OpenID4VCI sont tout aussi importantes pour le déploiement prochain des portefeuilles européens d'identité numérique, conformément au règlement eIDAS modifié.

Algorithmes équitables
Dans le domaine de l'identité numérique nationale, l'authentification biométrique est plus fiable que les autres techniques d'authentification (par exemple, les codes PIN, les mots de passe ou les jetons d'authentification). Elle améliore efficacement l'accès aux services publics tout en permettant le passage au numérique à l'échelle nationale. La mise en œuvre d'un tel système suscite donc des attentes élevées, qui ont tendance à rendre toute erreur technique potentielle plus difficile à accepter par le public. Il est important d'en avoir conscience, de mettre en place les processus adéquats et de s'assurer que les opérateurs du système le connaissent bien. À titre d'exemple, il est important de disposer d'une technologie équivalente pour tous les âges, genres, couleurs de peau et ethnies, autrement dit, des algorithmes biométriques équitables. Pour de tels systèmes, la sécurité est également capitale et doit être basée sur des années d'innovations, ainsi que sur des procédés solides pour concevoir, développer et tester les produits.

Pérenniser les solutions
Alors que la technologie évolue rapidement, il est de plus en plus important que les systèmes d'identité numérique soient à l'épreuve du temps. Si les smartphones reçoivent des mises à jour fréquentes pour en renforcer la sécurité et les fonctionnalités, les cartes d'identité électroniques, sur lesquelles les programmes d'identité numérique sont souvent basés, doivent aussi s'adapter pour garder une longueur d'avance sur les menaces émergentes.

Généralement, les documents d'identité électronique ont une durée de validité de dix ans. Pendant cette période, les techniques de fraude évoluent, compromettant potentiellement la sécurité de ces documents. Pour faire face à ces menaces, le système d'exploitation et les applications des documents d'identité électroniques doivent impérativement être mis à jour, même après la délivrance des documents. Les réglementations à venir, telles que celles proposées dans les règlements de l'UE sur la cybersécurité et sur la cyberrésilience, imposent ces exigences évolutives afin de garantir une protection continue.

Auparavant, la mise à jour du système d'exploitation d'une carte d'identité électronique exigeait d'émettre une nouvelle carte, ce qui était à la fois coûteux et chronophage. Mais grâce à l'intégration innovante du logiciel, le système peut être mis à jour en temps réel. Cela renforce encore la sécurité de l'identité numérique.

IDEMIA—Pionnier de l'identité mobile

2015 :
IDEMIA a été la première entreprise à tester un permis de conduire sur téléphone mobile aux États-Unis.

2017 :
Premier document d'identité numérique contribuant à sécuriser les déclarations d'impôt sur le revenu pour les États américains.

2019 :
Premier permis de conduire sur téléphone mobile basé sur des normes aux États-Unis.

2024 :

- Premier projet pilote d'identité numérique de voyage (DTC-1) transatlantique géré par IDEMIA
- 2 millions de cartes d'identité sur téléphone mobile seront délivrées en Colombie
- Déploiement des cartes d'identité sur téléphone mobile pour les opérateurs de télécommunications
- Déploiement des cartes d'identité sur téléphone mobile au Chili

Cas d'utilisation — Mise à jour du système en temps réel

La technologie JPatch de la solution IDEMIA Smart Identity facilite les mises à niveau à distance du logiciel intégré sans compromettre les données ou la confidentialité de l'utilisateur. Les systèmes de gestion des identifiants et de traitement après délivrance, veillent à ce que les mises à jour puissent être exécutées aisément depuis n'importe quel emplacement autorisé, supprimant le besoin de remplacer la carte.

Les données personnelles et techniques telles que les certificats et les codes PIN restent sûrs et intacts pendant le processus de mise à niveau, assurant l'intégrité et la confidentialité des informations. En plus de garantir la sécurité des données, cette approche rationalise le processus de mise à jour, évitant de devoir demander une nouvelle carte et réduisant la charge administrative pour les autorités de délivrance.

Facteur déterminant n° 4 : Sécuriser les identités numériques (et physiques) grâce à la biométrie

La biométrie révolutionne les programmes d'identité nationaux, répondant à certaines inefficacités et vulnérabilités des méthodes d'identification traditionnelles. S'appuyant sur des caractéristiques physiologiques ou comportementales uniques, la biométrie renforce la sécurité et la précision des processus d'identification.

Les données biométriques telles que les empreintes digitales, le motif de l'iris et les caractéristiques du visage sont quasiment impossibles à falsifier ou à voler, ce qui réduit drastiquement le risque de vol d'identité et de fraude. Les systèmes biométriques automatisés réduisent également l'erreur humaine, ce qui garantit une identification et une authentification précises et fiables.

L'efficacité et le caractère pratique de l'identification biométrique sont particulièrement avantageux dans les programmes d'identité nationale à grande échelle. Le citoyen n'a besoin que d'un seul compte pour accéder aux différents services publics et privés, et il n'a pas besoin de mémoriser plusieurs mots de passe. Les systèmes biométriques rationalisent le processus de vérification, ce qui le rend plus rapide et facile d'utilisation, aussi bien pour les citoyens que les administrateurs.

En outre, les données biométriques peuvent renforcer l'inclusion et l'accessibilité en offrant des moyens d'identité aux personnes qui ne possèdent pas de documents traditionnels, garantissant ainsi à tous les citoyens l'accès aux services et aux droits essentiels. Le caractère évolutif et interopérable de la technologie biométrique augmente encore son attrait, car elle peut être facilement développée pour prendre en charge une augmentation démographique et être intégrée dans différents systèmes gouvernementaux et non gouvernementaux.

Étant plus fiable, la biométrie aide également à améliorer l'accès aux services publics et favorise l'inclusion. En effet, le taux d'erreur pour l'authentification à l'aide des technologies biométriques est considérablement plus faible qu'avec des techniques telles que la vérification à l'œil nu de l'identité d'une personne à partir de la photo d'un document d'identité. Par ailleurs, l'identification biométrique est plus durable. Si une personne perd ses documents d'identité, elle peut s'appuyer sur la vérification biométrique pour prouver qui elle prétend être et demander la réédition rapide de ses documents.

Un système d'identité numérique sans données biométriques est presque impensable. Les avancées technologiques, comme la détection de présence au moyen d'un smartphone, ont été telles que la biométrie, et plus particulièrement les données biométriques faciales, offrent le moyen le plus sûr de prouver que l'utilisateur d'une identité mobile spécifique est réellement le détenteur de la carte d'identité physique correspondante. Pour une procédure d'enrôlement potentiellement entièrement à distance, les données biométriques et l'authentification multifactorielle sont les moyens les plus sûrs de vérifier l'authenticité de la personne.

Étude de cas — La « Cédula Digital » en Colombie

En 2018, le gouvernement colombien a lancé officiellement sa politique publique de dématérialisation. Cette politique nationale promeut l'inclusion numérique et l'utilisation d'une technologie de pointe pour favoriser un État compétitif, proactif et innovant et des citoyens qui génèrent de la valeur publique dans un environnement de confiance numérique.

Fin 2020, une nouvelle carte d'identité nationale sous forme numérique et physique a été lancée pour garantir un haut niveau de sécurité dans la numérisation des services publics.

Le plan national de transformation numérique a été alimenté par la délivrance combinée d'une nouvelle carte d'identité et d'une identité mobile appelée Cédula Digital. Dotée de la technologie LASINK™ d'IDEMIA Smart Identity pour renforcer la sécurité du portrait et du document, la nouvelle carte d'identité colombienne répond aux normes de sécurité les plus strictes du marché.

Le nouveau compagnon numérique de la carte d'identité physique colombienne, Cédula Digital, permet aux Colombiens d'avoir accès aux services en ligne de façon sécurisée et rend possible la vérification de l'identité en personne sur la base des dernières normes du secteur, en conformité avec la politique publique de dématérialisation.

La Cédula Digital est attribuée automatiquement dès que la nouvelle carte d'identité est délivrée au citoyen grâce à une vérification biométrique (empreintes digitales et reconnaissance faciale). Lorsque le citoyen retire sa carte d'identité dans un bureau physique officiel, il reçoit un e-mail comprenant un code QR d'activation et un lien d'activation unique. Il peut alors activer sa Cédula Digital en réalisant un selfie d'authentification biométrique pour confirmer son identité, permettant plusieurs interactions numériques.

Facteur déterminant n° 5 : Travailler en étroite collaboration avec le secteur privé

Ce n'est pas parce qu'un système a été lancé qu'il sera effectivement utilisé et adopté par tous les fournisseurs de services. Les autorités gouvernementales de délivrance des documents d'identité peuvent croire à tort que les fournisseurs de services, du secteur public comme du secteur privé, suivent de près le développement de leur programme d'identité numérique, prêts à l'adopter dès qu'il sera déployé. Si les fournisseurs de services et d'autres acteurs pertinents ne sont pas intégrés dès le début dans la conception et le déploiement du programme, ils risquent de ne pas faire preuve du niveau de soutien attendu pour une mise en œuvre et une utilisation efficace. La définition d'avantages cibles pour les citoyens, mais aussi pour les secteurs publics et privés, garantit que les résultats du projet seront salués par tous les partis et que le projet sera automatiquement plus réussi.

Des mesures pratiques, comme la mise à disposition de guides explicatifs par les fournisseurs de technologie et les intégrateurs de systèmes afin d'aider les fournisseurs de services à mettre en œuvre la solution, peuvent renforcer encore la collaboration, car ces derniers ne sauront peut-être pas par où commencer pour la mettre en œuvre.

Étude de cas — Maroc

Voici un exemple de bonnes pratiques du Maroc, où les différents acteurs ont été impliqués dès le début du projet d'identité numérique.

Avant de lancer son programme national, la Commission nationale de contrôle de la protection des données à caractère personnel du pays a mené une étude auprès d'une centaine de fournisseurs de services afin de comprendre leur utilisation des données d'identité numérique. Les conclusions de l'étude ont ensuite été utilisées pour formuler des contrôles de la protection des données à caractère personnel.

Aujourd'hui, après le déploiement de cartes d'identité physiques et d'une plateforme numérique au Maroc, le système enregistre des répercussions positives pour le quotidien des Marocains, en facilitant leur utilisation des services publics et de services commerciaux.

Choisir le bon partenaire de programme — peut-être le facteur déterminant le plus important de la liste

La mise en place d'un programme national d'identité numérique inclut de multiples facteurs et requiert une planification méticuleuse. En résolvant le problème du risque d'exclusion, en adoptant des cadres juridiques et de respect de la vie privée, en se conformant aux normes internationales et en veillant à faire participer les différents acteurs, les pays peuvent réussir à déployer et à maintenir des systèmes d'identité numérique efficaces.

Cependant, ne vous trompez pas, créer le système national d'identité numérique d'un pays, en partant de zéro ou d'une l'infrastructure existante, peut s'avérer impressionnant. Des prestataires établis et expérimentés peuvent offrir une assistance cruciale pour mener un projet d'une telle envergure. Leurs systèmes fonctionnent en permanence et sont soutenus par des équipes compétentes partout dans le monde, qui garantissent la disponibilité maximale du service ainsi qu'une amélioration et une innovation continues. Choisir un partenaire avec lequel travailler tout au long de la création d'un programme national d'identité numérique peut s'avérer l'aspect le plus important.

---

[1] https://unstats.un.org/legal-identity-agenda#:~:text=SDG%20Goal%2016.9%3A%20By%202030,a%20civil%20authority%2C%20by%20age

[2] https://www.id2020.org/assets/pdf/ID2020-Alliance-Manifesto.pdf

---