L'EXPRESSION DES IDENTITÉS NUMÉRIQUES DANS LE MONDE

EXPÉRIENCES ET OBSERVATIONS CLÉS POUR RELEVER LES DÉFIS COMMUNS

2021

SECURE IDENTITY ALLIANCE

onepoint.
beyond the obvious

PRODUCTION DU RAPPORT

Ce rapport a été produit par le groupe de travail Digital ID de la Secure Identity Alliance et l'équipe onepoint :

Membres du groupe de travail Digital ID de la SIA:
Kristel Teyras, Présidente du groupe de travail Digital ID, Secure Identity Alliance
Responsable marché identité numérique, plateformes et services, Thales
Marie Sophie Bellot, Pavlina Navratilova, IDEMIA
Olivier Dussutour, INGroupe
Fabian Bach, Mike Edwards, Veridos
Eric Piroux, Entrust
Andreas Zechmann, OSD

Membres de l'équipe onepoint :
Marie Alice Manderscheid, leader onepoint
Helene Le Héricy, leader onepoint
Corentin Marsily, consultant onepoint

DROITS ET PERMISSIONS

© 2021 onepoint
29 rue des Sablons
75116 PARIS
Site Internet: https://www.groupeonepoint.com/

Le contenu de ce travail est soumis à des droits d'auteur. Les membres de la SIA encouragent la diffusion de leurs connaissances. C'est pourquoi des parties de ce travail peuvent être reproduites ou diffusées, à des fins non-commerciales sans permission, à condition d'en indiquer la source complète. Vous n'avez aucun droit de diffuser ce travail en tout. Toute demande de renseignements sur les droits et les licences, y compris les droits subsidiaires, doit être adressée à la Secure Identity Alliance : www.secureidentityalliance.org

CRÉDITS

Couverture :
Photo par Carson Arias sur Unsplash

Additionnel :
Photo par Omar Albeik sur Unsplash
Photo par HONG LIN sur Unsplash

Quatrième de couverture :
Photo par NeONBRAND sur Unsplash

Traduction :
Traducation de l'anglais vers le français par Oriane Duboz

TABLE DES MATIÈRES

ÉDITO 6

INTRODUCTION 9

Termes clés et définitions 10

OBSERVATIONS 13

Vue d'ensemble 14
Propositions de valeur pour l'utilisateur final 16
Ecosystème & gouvernance 24
Mise en oeuvre technologique 30
Mise sur le marché & promotion 36

PROGRAMMES D'IDENTITÉ NUMÉRIQUE DES PAYS INTERROGÉS 43

Pays étudiés en Europe 44
Pays étudiés au Moyen-Orient & Asie-Pacifique 46
Pays étudiés en Amérique & Afrique 48

Australie, Queensland - Application de Permis de Conduire Numérique 50
Autriche - Carte de Citoyen et Identité Mobile 52
Azerbaïdjan - Asan Imza 54
Canada - Réseau d'Identité Verified.Me 56
Colombie - Nouvelle Carte d'Identité Électronique et Identité Mobile 58
Danemark - NemID et MitID 60
Estonie - Carte d'Identité Électronique 62
France - FranceConnect 64
Italie - SPID 66
Liechtenstein - eID.li 68
Pays-Bas - DigID 70
Nigéria - NIN et Application d'Identité Mobile 72
Portugal - Chave Móvel Digital et Carte de Citoyen 74

Singapour - Identité Numérique Nationale 76
États-Unis, Arizona - Permis de Conduire Mobile (MVD) 78

PROGRAMMES D'IDENTITÉ NUMÉRIQUES DE PAYS ADDITIONNELS 80

Belgique - Itsme 81
Brésil - Application Portefeuille d'Identités CPF 82
Inde - Aadhaar 83
Lettonie - eParaksts 84
Oman - Omanuna 85
Royaume-Uni - Gov.UK Verify 86

REMERCIEMENTS 87

ÉDITO

Stéphanie de Labriolle, Affaires Publiques & Relations Internationales, Secure Identity Alliance

Tenir les promesses de l'identité numérique

En fournissant des observations détaillées sur la manière dont divers gouvernements à travers le monde utilisent au mieux le potentiel de l'Identité Numérique afin de fournir des services innovants et inclusifs aux citoyens, cette étude mondiale unique en son genre révèle les principes directeurs qui sont la clé de la réussite.

En tant qu'organisme consultatif international à but non-lucratif tenant aux identités et services numériques sécurisés, Secure Identity Alliance (SIA) rassemble des organisations publiques, privées et non gouvernementales afin de favoriser la collaboration internationale, élaborer des stratégies et fournir des conseils techniques. Il nous tient à coeur de partager les meilleures pratiques de mise en œuvre de programmes d'identité.

Alors que la demande de programmes gouvernementaux d'identité numérique continue d'augmenter, nous avons commandé cette étude afin de collecter les enseignements tirés de réelles mises en œuvre à travers le monde, en explorant les opportunités, les défis, les cas d'usage et les facteurs clés d'une stratégie gagnante.

En partenariat avec le cabinet de conseil onepoint, qui accompagne les administrations publiques dans la conception de leur vision numérique, nous avons mené une recherche auprès de 25 programmes d'identité numérique régaliens afin d'identifier les questions importantes à se poser lors de l'élaboration d'un tel programme.

Nos conclusions montrent comment, quel que soit le modèle d'écosystème d'identité numérique adopté - centralisé ou fédéré - un certain nombre de thèmes et de principes directeurs communs se sont avérés essentiels pour en stimuler l'utilisation, l'adoption et le succès. En plus de mettre en évidence des exemples de meilleures pratiques adoptées dans le monde, nous espérons que les informations contenues dans cette étude permettront aux gouvernements de développer des programmes d'identité numérique sûrs, accessibles et bénéfiques sur le plan social, ainsi que des politiques qui soutiennent et nourrissent une identité numérique de qualité.

Kristel Teyras, Présidente du Group de Travail Digital ID, Secure Identity Alliance

Identité Numérique – Apprendre des autres

Partout dans le monde, les projets d'identité numérique prennent de l'ampleur. Des papiers d'identité au permis de conduire ou au passeport électronique... les documents physiques se numérisent à une vitesse fulgurante. Ces nouvelles formes d'identité numérique nous permettent l'accès en ligne à des services publics essentiels, des dossiers médicaux, nos documents de voyages ou d'affaires, de traiter avec de nouveaux fournisseurs de service et de protéger notre identité dans tous les aspects de notre vie quotidienne.

Responsable du développement et de l'adoption de services sécurisés, fiables, efficaces et inclusifs, le groupe de travail Digital ID de la SIA guide les gouvernements et les conseille sur la meilleure manière de proposer des mécanismes d'identification et de vérification sécurisés, ainsi que de définir des spécifications techniques pour la création d'identités numériques.

La récente crise liée à la COVID-19 a encore renforcé l'importance de ces systèmes, qui permettent aux citoyens de prouver leur identité et d'accéder facilement aux services publics et privés par voie numérique. La présente recherche fournit des informations essentielles aux gouvernements quant à l'élaboration de stratégies nécessaires au développement de leurs programmes d'Identité Numérique nationaux et à mieux se reconstruire après la pandémie.

L'utilisation des identités numériques ayant atteint un point charnière, l'identité mobile est amenée à devenir la principale source de connexion, vérification et authentification aux systèmes d'identité numérique pour plus de 3 milliards de personnes d'ici 2024[1]. Les technologies d'identité mobile nouvelle génération, qui prennent en charge l'identification tant physique qu'en ligne, contribuent déjà à impulser une nouvelle ère de services innovants qui redéfinissent la manière dont les personnes interagissent avec les autorités publiques et les entreprises du secteur privé.

Toutefois, pour tenir cette promesse, les résultats de cette recherche soulignent l'importance vitale de lancer des programmes d'identité mobile construits à partir d'un cadre de confiance de l'identité numérique solide et fiable.

Yannick Ragonneau, Partner, onepoint

Les transactions passant d'un format physique à numérique, une identité numérique fiable est désormais la pierre angulaire d'une gamme de services publics qui se veut novatrice et croissante. Dans ce rapport, nous donnons la parole aux responsables derrière les projets d'identité les plus innovants et stimulants observés dans le monde – en mettant à profit leurs observations et perspectives "sur le terrain" afin d'aider les décideurs publics et privés à comprendre l'art du possible, et pour informer et façonner leurs propres programmes.

En collaboration avec la Secure Identity Alliance, onepoint a identifié 25 projets d'identité et a mené des entretiens individuels avec les responsables de ces programmes. Il nous était nécessaire d'élaborer plus qu'un simple rapport. Nous avons voulu comprendre les défis uniques liés à la conception et au déploiement de chacun de ces programmes, les facteurs de leurs réussites, et les choix de trajectoire individuelle spécifique dans un contexte où tant d'options sont envisageables.

Cette approche nous semble offrir une source de contenus beaucoup plus riche pour les organisations publiques et privées – surtout si l'on prend en considération la rapidité d'évolution, ansi que la volonté des gouvernements de développer une approche permettant l'ouverture des systèmes d'informations à des écosystèmes étendus de fournisseurs tiers.

Après avoir mené et analysé ces entretiens d'experts, nous avons rassemblé divers enseignements en 13 observations clés afin d'éclairer l'élaboration de politiques tout au long du cycle de planification et de déploiement : de la proposition de valeur pour l'utilisateur final à l'écosystème et la gouvernance, en passant par la mise en œuvre technologique ou la mise sur le marché et la promotion.

Au final, l'évolution continue du marché de l'identité numérique et le succès des nombreux programmes publics et privés dépendent de la capacité de l'ensemble de la communauté à collaborer efficacement, à partager les bonnes pratiques et à apprendre les uns des autres. En donnant la parole aux identités numériques du monde entier, nous espérons que ce rapport contribuera à cet effort.

1. Juniper Research, Why Digital Identity Is Critical To Post-Pandemic Society, Nick Maynard and Susan Morrow, 2020

INTRODUCTION
UNE ÉTUDE BASÉE SUR DES RETOURS CONCRETS ET LES BONNES PRATIQUES

La Secure Identity Alliance (SIA) et onepoint ont rassemblé leurs compétences et expérience afin de produire une étude mondiale portée sur les identités numériques et mobiles observées à l'échelle globale : « L'expression des identités numériques dans le monde, expériences et observations clés pour relever les défis communs ».

La SIA et onepoint considèrent l'Identité Numérique comme un moteur d'inclusion sociale et économique, l'opportunité de proposer un accès égal, rapide et pratique aux services publics et privés. En tant que tel, l'accent et la priorité ont été donnés aux identités numériques et mobiles nationales qui sont dirigées et/ou réglementées par un gouvernement.
Les programmes nationaux d'Identité Numérique varient d'un pays à l'autre en fonction d'une multitude de critères tels que les spécificités culturelles, la structure d'écosystème et de gouvernance, l'infrastructure technologique, le cadre juridique et institutionnel, les exigences en matière de sécurité et de confidentialité, etc. Il n'existe certes pas de système d'identité numérique "unique" à reproduire et à mettre en œuvre, mais certaines observations clés et bonnes pratiques peuvent par contre être partagées.

L'objectif de ce rapport est double :

1. Mettre en lumière les spécificités des programmes d'identité numérique, plonger au cœur de cas d'usage innovants, de diverses gouvernance et méthodes, de choix technologiques et de stratégies de mise sur le marché.
2. Comprendre les facteurs et motifs qui justifient les prises de décision, et bénéficier d'un retour concret d'informations et de bonnes pratiques de la part d'acteurs clés.

LES OBSERVATIONS IDENTIFIÉES SONT BASÉES SUR LE RETOUR D'EXPÉRIENCES DE LA SIA ET DE ONEPOINT, SUR DES SOURCES ANALYTIQUES OFFICIELLES ET DOCUMENTÉES, AINSI QUE SUR UNE ANALYSE CROISÉE DE **25 ENTRETIENS AVEC DES ACTEURS INTERNATIONAUX CLÉS ET REPRÉSENTANTS DE PAYS. FAIRE PARLER L'EXPÉRIENCE DE CES DIFFERENTS ACTEURS** A ÉTÉ LE FIL ROUGE DE CETTE ÉTUDE.

PRÉSENTATION DES DEUX STRUCTURES

SECURE IDENTITY ALLIANCE

Organisation à but non-lucratif, la Secure Identity Alliance rassemble des organisations publiques, privées et non gouvernementales afin de travailler en collaboration internationale sur la mise à disposition pour tous d'une identité légale et digne de confiance, ainsi que sur le développement de services d'identité numérique nécessaires à un développement et une prospérité économiques durables. Son Conseil d'Administration compte IDEMIA, IN Groupe, Thales et Veridos.
www.secureidentityalliance.org

onepoint. beyond the obvious

Onepoint est l'architecte des grandes transformations des entreprises et des acteurs publics. Elle accompagne ses clients de la définition de la stratégie à sa mise en œuvre technologique. Onepoint a été sélectionnée pour apporter son point de vue et son expérience sur les modèles innovants d'identité numérique à travers le monde.
https://www.groupeonepoint.com/fr

TERMES CLÉS ET DÉFINITIONS

DÉFINITIONS

Partage d'attributs
Les attributs peuvent être révélés, accompagnés de leurs conditions d'utilisation respectives déterminant à quelles fins autorisées ils sont destinés. Les utilisateurs ont un contrôle très précis sur chaque partage d'attribut.[1]

Authentifiant
Un authentifiant, ou facteur d'authentification, est un objet utilisé pour vérifier l'identité d'un individu. Les facteurs d'authentification peuvent être quelque chose que l'utilisateur connaît (un mot de passe, ou PIN), quelque chose qu'il/elle possède (une carte, un document physique ou un dispositif, par exemple un téléphone portale), ou ce qu'il est, une caractéristique physique de l'utilisateur (une image de son visage, ou une empreinte digitale).

Biométrie
Une caractéristique physique mesurable ou un trait comportemental personnel utilisé pour reconnaître l'identité d'un demandeur ou vérifier l'identité qu'il déclare. Les images faciales, les empreintes digitales et les échantillons de scan de l'iris sont tous des exemples de biométrie.[2]

Titre d'Identité
Un document, dispositif ou une structure de données qui atteste de l'identité d'une personne par le biais d'une méthode de mise en confiance et d'authentification. Parmi les titres d'identité les plus courants, on trouve notamment — mais pas seulement — les cartes d'identité, certificats, numéros, noms d'utilisateur et mots de passe, cartes SIM, etc. Une attestation numérique (signée ou non) peut également servir de titre d'identité, tout comme l'identification biométrique, après avoir été enregistrée auprès du fournisseur d'identité.

Authentification numérique
Le procédé de vérification de l'identité numérique d'une personne en utilisant un ou plusieurs facteurs ou titres d'identité afin d'établir qu'elle est bien la personne qu'elle déclare être. L'authentification est donc un procédé qui fonde la confiance en l'identité numérique d'un individu.

Identification numérique
Le procédé qui consiste à valider sans équivoque les attributs ou caractéristiques d'une personne — y compris sa singularité — afin d'établir son identité numérique.

Identité Numérique ou Électronique (IDN ou eID)
Terminologie utilisée durant tout ce document pour désigner un ensemble d'attributs et titres d'identités capturés et stockés de manière électronique et qui peuvent identifier une personne de manière unique. Elle peut prendre la forme d'une carte électronique, d'une application mobile, d'un jeton matériel, etc.

Programme d'identité numérique
Un système qui permet à des personnes physiques uniques de prouver, sans ambiguïté et en toute sécurité, qui elles sont lors de transactions numériques et de les habiliter à faire valoir leurs droits légaux dans un contexte numérique. Le système est basé sur des transactions numériques (identification, authentification, signature numérique, etc.) effectuées entre les utilisateurs, avec le(s) fournisseur(s) d'identité et les fournisseurs de services qui peuvent être publics et/ou privés. Il suit des règles nationales et/ou internationales, des procédures, et s'appuie sur des technologies spécifiques. Un système d'identité numérique repose sur un Cadre de Confiance. Par exemple, tous les systèmes d'identité numérique notifiés en Europe reposent sur le règlement eIDAS.

Portefeuille d'identité numérique
Une application sûre de portefeuille mobile qui héberge un ensemble de documents d'identité numérique et titres d'identité, qui se base sur le standard ISO 18013-5 et permet à l'utilisateur final d'avoir le contrôle sur ses données personnelles et peut être vérifié via une application de vérification d'identité.

Signature électronique
Résultat d'une transformation cryptographique de données qui, lorsqu'elle est correctement mise en œuvre, permet l'authentification de l'origine, l'assurance de l'intégrité des données et la non-répudiation du signataire.[3]

eSIM
eSIM est l'abréviation de "Embedded Subscriber Identity Module", ou "Embedded SIM" - pour SIM intégrée. L'utilisateur a seulement besoin de télécharger et activer son profil sur la eSIM pour pouvoir commencer à l'utiliser.

Identité Fédérée
La fédération est un processus qui permet la transmission d'attributs d'authentification et d'attributs d'abonnés à travers des systèmes en réseau. Dans le cas d'une fédération, le vérificateur est appelé fournisseur d'identité, ou IdP. La tierce partie (RP) est la partie qui reçoit et utilise les informations fournies par l'IdP.[4]

Système Centralisé dirigé par le Gouvernement
Un système national dirigé par le gouvernement qui fournit des identités numériques et des titres d'identité vérifiés - stockés et contrôlés par une autorité centrale unique qui est établie sur une base de données d'identité nationale unique et définie par un cadre juridique.

Fournisseur d'Identité
Une entité - par exemple : une agence gouvernementale ou une entreprise privée - qui délivre et gère des identités, titres d'identité, et des procédés d'authentification tout au long du cycle de vie de l'identité.[5]

KYC (pour "Know Your Customer" - ou Connaissance du Client)
Terme général utilisé pour désigner les règlements exigeant des organisations qu'elles fassent preuve de la diligence requise dans l'établissement de l'identité d'un client.[6]

LoA (pour Level of Assurance - ou Niveau d'Assurance)
Quand il est relatif à l'identité, le niveau d'assurance est le degré de certitude avec lequelle on peut déclarer que la revendication d'une identité particulière lors de la vérification de l'identité, de l'authen-

1 Secure Key, *https://www.securetechalliance.org/resources/media/scag13_preconference/09.pdf*

2 Richard Kissel (May 2013). Glossary of Key Information Security Terms. NIST Retrieved from: *http://nvlpubs.nist.gov/nistpubs/ ir/2013/NIST.IR.7298r2.pdf*

tification et de la fédération soit effectivement la "véritable" identité du demandeur. ISO/IEC 29115 et NIST SP 800-63-3A définissent le Niveau de Confiance dans le processus de délivrance afin de décrire la qualité du contrôlé de l'identité d'une personne, et à quel point le document d'identité électronique mobile correspond au propriétaire de l'appareil mobile.

Niveau de confiance
Le taux de confiance qu'une entité vérifiante peut accorder à un document d'identité électronique mobile, ou qu'un émetteur peut fournir ; il dépend de quatre facteurs : preuve d'identité, lien titre d'identité-dispositif, actualité des données, et authentification du détenteur.[7]

Identité Mobile
Une identité numérique fournie par le biais de réseaux, de données et d'appareils mobiles.

Une PKI (pour Public Key Infrastructure - ou infrastructure de gestion de clés)
Ensemble de matériels, logiciels, politiques, processus et procédures nécessaires pour créer, gérer, distribuer, utiliser, stocker et révoquer des certificats numériques et des clés publiques. Les PKI sont la base qui permet l'utilisation de technologies, telles que les signatures électroniques et le cryptage, par une grande quantité d'utilisateurs. Les PKI fournissent les éléments essentiels à un environnement commercial sûr et fiable pour le commerce électronique et l'Internet des Objets (IdO ou IoT) en pleine expansion.[8]

Tierce Partie ou fournisseur de services (SP)
Une organisation ou entreprise qui a besoin de vérifier l'identité de l'utilisateur final ; cette entité s'appuie sur les titres d'identité et les mécanismes d'authentification fournis par un système d'identité, généralement pour traiter une transaction, afin de pouvoir fournir un service numérique ou donner accès à des informations ou à un système.[9]

Authentification Unique (ou SSO pour Single Sign-On)
Un service de sessions centralisées et d'authentification d'utilisateur dans lequel une seule combinaison de titres de connexion peut être utilisée afin d'accéder à des usages multiples.

Cadre de Confiance (ou "Trust Framework")
Le "règlement" qui sous-tend la gestion fédérée de l'identité, consistant généralement en : système, juridique, conformité et reconnaissance.[10]

Numéro Identifiant Unique (NIU)
Un numéro qui identifie de manière unique un individu et qui peut être utilisé pour établir un lien entre une identité dans les bases de données et les systèmes des secteurs public et privé. Les fournisseurs d'identité nationaux peuvent délivrer un NIU aux citoyens et aux résidents pour la durée de leur vie.

3 NIST SP 800-12

4 NIST 800-63-3, https://pages.nist.gov/800-63-3/sp800-63c.html

5 World Bank, GSMA and SIA paper : Towards Shared Principles for Public and Private Sector Collaboration https://openknowledge.worldbank.org/handle/10986/11866

6 Caribou Digital, Private-Sector Digital Identity in Emerging Markets, Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2016.

7 ISO/IEC 23220-5 (still at working draft stage)

8 Thales, What is Public Key Infrastructure (PKI)?, *https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki*

9 Adapted from NIST 800-63:2017, ID4D Draft for consultation.

10 NIST IR 8149

ABRÉVIATIONS

API: Application Programming Interface
eID: Electronic Identification
HSM: Hardware Security Module
ICT: Information and Communication Technologies
IDP: Identity Provider
IoT: Internet of Things
ISO: International Organization for Standardization
KBA: Knowledge-Based Authentication
KYC: Know your customer
LoA: Level of Assurance
MDL: Mobile Driver License
MNO: Mobile Network Operator
NFC: near-field communication
NIN: National Identity Number (may or may not be unique, i.e., a UIN)
OTP: One-Time Password
PKI: Public Key Infrastructure
PPP: Public Private Partnership
QeS: Qualified Electronic Signature
RFP: Request For Proposal
ROI: Return On Investment
SIM: Subscriber Identity Module
SP: Service Provider
SSI: Self Sovereign Identity
SSO: Single Sign-On
UI: User Interface
UX: User Experience

Organisatiosns, régulations et standards / protocoles
eIDAS : Electronic Identification, Authentication and Trust Services
FIDO : Fast Identity Online – L'Alliance FIDO est un groupement d'industriels dont l'objectif est le développement de standards pour l'authentification des individus par l'utilisation de la technologie mobile
OACI : Organisation Aviation Civile Internationale
NIST : Institut national américain de normalisation
OAuth : Protocol standardisé pour le partage de jetons d'authorisation
OCDE : Organisation de Coopération et de Développement Economiques
OpenID Connect : Protocol standardisé pour les identités
OSIA : Open Standards Identity APIs (www.osia.io)

PLONGÉE AU CŒUR DES OBSERVATIONS CLÉS À TRAVERS LE MONDE

APERÇU DES OBSERVATIONS

PROPOSITIONS DE VALEUR POUR L'UTILISATEUR FINAL	PAYS DES CAS D'USAGE	
OBSERVATION #1 ENVISAGER L'IDENTITÉ NUMÉRIQUE COMME UN MOTEUR D'INCLUSION ET DE DIGNITÉ	> FRANCE > AZERBAÏDJAN > AUSTRALIE, QUEENSLAND	16
OBSERVATION #2 CONCEVOIR DES MÉCANISMES DE PROTECTION DE LA VIE PRIVÉE AFIN DE PROTÉGER L'INDIVIDU AVANT TOUT	> AUSTRALIE, QUEENSLAND > AUTRICHE > CANADA	18
OBSERVATION #3 TROUVER LE BON ÉQUILIBRE ENTRE EXPÉRIENCE D'UTILISATION ET SÉCURITÉ	> ESTONIE > USA, ARIZONA > SINGAPOUR	20
OBSERVATION #4 INTÉGRER L'UTILISATEUR FINAL DANS LE PROCESSUS DE DÉVELOPPEMENT & MISE EN PLACE DE L'ID NUMÉRIQUE	> AUSTRALIE, QUEENSLAND > DANEMARK	22

ÉCOSYSTÈME ET GOUVERNANCE	PAYS DES CAS D'USAGE	
OBSERVATION #5 FAVORISER LA COLLABORATION ENTRE LES SECTEURS PUBLIC ET PRIVÉ POUR UNE STABILITÉ FINANCIÈRE	> INDE > DANEMARK > ITALIE	24
OBSERVATION #6 CRÉER UN GROUPE DE TRAVAIL INTERGOUVERNEMENTAL ET PLURIDISCIPLINAIRE POUR DIRIGER L'IDENTITÉ NUMÉRIQUE	> COLOMBIE > NIGÉRIA > FRANCE	26
OBSERVATION #7 S'IMPLIQUER DANS LES ORGANISMES INTERNATIONAUX DE RÉGULATION & STANDARDISATION	> AUSTRALIE, QUEENSLAND & ARIZONA > AMÉRIQUE LATINE > NIGÉRIA	28

MISE EN ŒUVRE TECHNOLOGIQUE	PAYS DES CAS D'USAGE	
OBSERVATION #8 PENSER MOBILE AVANT TOUT	> LIECHTENSTEIN > AZERBAÏDJAN > ITALIE	30
OBSERVATION #9 METTRE EN PLACE DES PROCÉDURES AGILES ET ITÉRATIVES – DE MANIÈRE EXPLICITE	> AUSTRALIE, QUEENSLAND > FRANCE > SINGAPOUR	32
OBSERVATION #10 METTRE EN PLACE DES INFRASTRUCTURES ADAPTABLES & MODULAIRES QUI FONT LE LIEN ENTRE PASSÉ ET FUTUR	> DANEMARK > INDE > CANADA	34

MISE SUR LE MARCHÉ & PROMOTION	PAYS DES CAS D'USAGE	
OBSERVATION #11 FOURNIR DES SERVICES UTILES ET RÉCURRENTS EN S'APPUYANT SUR LE SECTEUR PRIVÉ	> PORTUGAL > FRANCE > DANEMARK	36
OBSERVATION #12 FOURNIR UNE PROCÉDURE D'INSCRIPTION SÛRE, SIMPLE ET MULTIPLE	> FRANCE > ITALIE > PORTUGAL	38
OBSERVATION #13 CONCEVOIR UNE CAMPAGNE PERSONNALISÉE AUX DIFFÉRENTS ACTEURS AFIN DE STIMULER L'ADOPTION	> PAYS-BAS > AUTRICHE > SINGAPOUR	40

OBSERVATION #1

ENVISAGER L'IDENTITÉ NUMÉRIQUE COMME UN MOTEUR D'INCLUSION ET DE DIGNITÉ

A travers le monde, près d'un milliard de personnes ne disposent pas d'une forme d'identification légalement reconnue, tels qu'un certificat de naissance ou une carte d'identité (Banque Mondiale, 2020). Elles sont donc privées de services de base, de participation socio-économique, d'inclusion financière et de leurs droits démocratiques. Dans la grande majorité des pays, prouver son identité est une étape obligatoire pour ouvrir un compte bancaire, s'inscrire dans une école, demander des prestations sociales, louer un appartement, trouver un emploi, etc. La pandémie COVID-19 a encore prouvé aux gouvernements, aux entreprises et aux citoyens le rôle clé de l'identité numérique en tant que filet de sécurité socio-économique fondamental et l'importance de disposer d'une infrastructure prête et disponible. Par exemple, l'enregistrement et l'utilisation se sont poursuivis au moins au même rythme ou ont été multipliés par deux dans des pays comme l'Azerbaïdjan ou l'Italie.

En ouvrant à tous l'accès aux services publics et privés en ligne 24h/24, 7 j/7, de manière sûre, transparente et immédiate, l'identité numérique est de plus en plus considérée comme un moyen d'améliorer les questions d'inclusion et de dignité. L'accès à tous étant la condition préalable à l'inclusion, toutes les identités numériques sont confrontées à des préoccupations et des défis communs : comment l'identité numérique peut-elle s'adresser à l'ensemble de la population, et le peut-elle ? Comment permettre l'accès aux personnes en situation de handicap et à celles qui vivent dans des zones sans couverture internet ?

« Il est important d'admettre qu'il y aura toujours quelqu'un qui ne pourra pas utiliser la solution. Quel que soit notre niveau de numérisation, nous devons donc continuer à leur fournir un moyen d'interagir avec le secteur public. »

Charlotte Jacoby, Cheffe de service de la Division pour le Développement de l'Infrastructure, Danemark

QUE PENSENT-ILS DE L'IDENTITÉ LÉGALE ET DE L'INCLUSION ?

Cheffe de l'Unité de Protection des Données du Conseil de l'Europe

« Beaucoup considèrent que l'un des objectifs du Développement Durable est d'avoir une **identité numérique** pour tous, ce qui est un malentendu. L'objectif est d'avoir une **identité légale** pour tous, ce qui est une composante fondamentale pour exercer nos droits. Les outils numériques devraient faciliter l'accès aux droits, mais ne devraient en aucun cas être une condition pour accéder, par exemple, aux services publics. »

Christopher Goh, Manager Général, Modernisation des Permis et Immatriculations – Département des Transports et Routes Principales, Queensland, Australie

« Les personnes sans identité perdent leur dignité et n'ont pas accès aux services sociaux, aux transports publics ni à tous les services que vous et moi considérons comme acquis. Ici, l'identité est une question de dignité individuelle.»

Joni Brennan, Présidente du Conseil canadien de l'identification & authentification numériques (CCIAN)

« Nous cherchons à utiliser des titres d'identité qui peuvent favoriser la dignité, afin que l'aide publique qui vous est attribuée ne soit pas connue de tous. Notre objectif est d'aider les gens à accéder aux prestations sociales sans que cet accès ne les rende trop visibles. »

Andrea Spallacci, Chargé de Projet, Agenzia per l'Italia Digitale (AgID)

«SPID n'est actuellement pas disponible pour les mineurs - même si plusieurs services publics et privés sont conçus spécialement pour eux. Nous travaillons sur une solution impliquant l'autorisation des parents. De plus, comme certaines associations de personnes en situation de handicap ont demandé des solutions pour les aider dans le processus d'authentification, nous étudions des solutions plus inclusives, car SPID ne doit pas être un obstacle.»

CAS D'USAGE #1

AIDANTS ET E-REPRÉSENTATION POUR LES PERSONNES EN DIFFICULTÉS EN FRANCE

En France, environ 13 millions de personnes font face à des difficultés avec les outils numériques, soit à cause d'un problème d'accessibilité ou d'un handicap. Pour remédier à cela, le dispositif public d'identité numérique FranceConnect teste un nouveau service, Aidants Connect, destiné à fournir une représentation électronique aux personnes dans le besoin.

Aidants Connect permet à des professionnels autorisés d'effectuer des démarches administratives en ligne, de manière sécurisée et légale, au nom de personnes rencontrant des difficultés avec les outils numériques. Concrètement, les aidants accompagnent les utilisateurs dans la création de leurs comptes en ligne, définissent les procédures pour lesquelles la représentation est nécessaire, et procèdent à la signature électronique d'un mandat en ligne. Actuellement testé dans 13 organisations publiques et sociales, le service sera étendu au reste du pays s'il s'avère efficace.

CAS D'USAGE #2

DES SOLUTIONS VERBALES QUI ASSURENT L'INCLUSION NUMÉRIQUE EN AZERBAÏDJAN

Afin d'être inclusive et de s'adresser aux personnes moins compétentes en matière de technologie, l'identité mobile d'Azerbaïdjan comprend 9 services basés sur des solutions verbales et des centres d'appel.

Ces services sont populaires dans les zones rurales, en particulier pour les services de déclaration d'impôts. Les utilisateurs peuvent compléter leur déclaration d'impôts sans rien remplir. Ils appellent, répondent aux questions posées et signent de manière électronique. Ces services sont actuellement assurés par des agents, mais l'intelligence artificielle est envisagée pour l'avenir.

CAS D'USAGE #3

LE PORTEFEUILLE D'ID NUMÉRIQUE AIDE LES VICTIMES DE VIOLENCES DOMESTIQUES DANS LE QUEENSLAND, EN AUSTRALIE

Dans le Queensland, Australie, l'application de permis de conduire numérique, qui sert également de portefeuille d'identité numérique, a joué un rôle clé pour aider les femmes victimes de violences domestiques. Dans un pays où une femme sur quatre est confrontée à des violences domestiques et où plus de la moitié d'entre elles quittent leurs partenaires sans papiers d'identité, l'identité numérique permet d'accéder aux services sociaux dans la journée, alors que renouveler ces documents de manière physiques peut prendre jusqu'à 4 mois.

« Le renouvellement d'un document d'identité physique peut prendre jusqu'à 4 mois, une période durant laquelle ces femmes et leurs enfants sont vulnérables. Maintenant, si une femme quitte son partenaire, elle peut nous appeler ou utiliser un appareil de reconnaissance faciale, et peut commencer sa vie le jour même .»

Christopher Goh, Manager Général, Modernisation des Permis et Immatriculations – Département des Transports et Routes Principales, Queensland, Australie

L'INCLUSION ET LA DIGNITÉ PEUVENT ÊTRE ABORDÉES DE PLUSIEURS MANIÈRES :

1. **Tenez compte du contexte socio-économique du pays et de la région pour choisir la technologie et les titres d'identité pertinents : Un mélange de moyens matériels et logiciels, et de solutions d'identité numérique peut, dans certains cas, permettre une plus grande inclusion.**

2. **Consultez et prenez en compte les besoins des populations spécifiques pour développer des solutions et des processus inclusifs (solutions verbales basées sur des centres d'appel, codes QR inversés, fonctions natives d'accessibilité pour les populations plus âgées, validation hors ligne, etc.) et conservez des alternatives physiques.**

3. **Considérez l'identité numérique comme une opportunité d'accroître la dignité humaine et pensez à de nouvelles façons de proposer des titres d'identité moins intrusives et discriminatoires.**

OBSERVATION #2

CONCEVOIR DES MÉCANISMES DE PROTECTION DE LA VIE PRIVÉE AFIN DE PROTÉGER L'INDIVIDU AVANT TOUT

« Qui est propriétaire de nos données, qui y a accès et comment sont-elles utilisés ? » Les citoyens de plus en plus vigilants se posent ces questions de manière récurrente, conscients de la nécessité de protéger leur vie privée. Pour répondre à ces préoccupations, les gouvernements réfléchissent de plus en plus à de nouveaux modèles. Cela inclut des modèles décentralisés, permettant aux utilisateurs de ne distribuer et de ne partager que les données qui sont nécessaires lors de la validation de leur identité et l'accès à des services en ligne. La technologie évolue elle-aussi rapidement vers une protection accrue des données : conception d'outils respectueux de la vie privée, outils de protection de données, filtres de données entre les fournisseurs d'identité et de services, bases de données décentralisées, etc.

Si des mécanismes de confiance et de protection de la vie privée sont nécessaires, la priorité doit rester la conception d'un cadre juridique et réglementaire visant à protéger les personnes. L'efficacité croissante de technologies telles que la reconnaissance faciale, ainsi que l'accroissement des flux de données personnelles à travers les frontières renforcent la pertinence d'une compréhension commune et harmonisée de la protection des données. Le Conseil de l'Europe encourage la généralisation de la Convention 108, la Convention pour la Protection des Personnes à l'égard du Traitement Automatisé des Données à Caractère Personnel. Cette convention protège les personnes, leurs droits, et leurs libertés fondamentales, et en particulier le droit au respect de la vie privée. Aujourd'hui, les pays du monde entier consultent le Conseil de l'Europe pour obtenir un soutien réglementaire et méthodologique, mais trop nombreux sont ceux qui continuent à concevoir et à mettre en œuvre des identités numériques nationales sans cadre ni législation en matière de protection des données.

« La principale question que nous posent nos clients, 100% du temps c'est: Que faites-vous avec nos données ? »

Christopher Goh, Manager Général, Modernisation des Permis et Immatriculations – Département des Transports et Routes Principales, Queensland, Australie

« Au Kenya, la société civile a fermé le projet d'identité numérique en raison d'un manque de dispositif de sécurité et de législation sur la protection des données »

Peter Kimpian, Unité de Protection des Données Personnelles au Conseil de l'Europe

QUE PENSENT-ILS DE LA PROTECTION DES DONNÉES PERSONNELLES ?

Quek Sin Kwok, Directeur Principal, Plateforme et Produits d'Identité Numérique Nationale, GovTech Singapour

« Je demande souvent aux gens de vérifier que leurs méthodes de partage des données sont bien « privées ». Lors d'une demande de prêt ou de carte de crédit, les gens doivent envoyer des dizaines de documents à un employé ou intermédiaire bancaire, contenant plus d'informations personnelles que nécessaire. Les moyens numériques de partage des données par consentement explicite des individus leur permettent de partager uniquement les données nécessaires en évitant les intermédiaires, et d'avoir une traçabilité numérique du consentement et du but du partage. C'est un moyen plus respectueux de la vie privée que le partage de documents physiques.»

Peter KIMPIAN, Unité de Protection des Données Personnelles au Conseil de l'Europe

« Nous discutons ouvertement avec nos partenaires chinois et il y a un clair intérêt aujourd'hui. La Chine a adopté une loi sur la protection de la vie privée et vient juste d'en adopter une sur la protection des données. Ils ont étudié la RGPD. Nous devons poursuivre une coopération ouverte malgré nos divergences initiales. Il n'y a qu'un seul avenir, et c'est celui de garantir un niveau de protection adéquat pour les personnes du monde entier, tout en facilitant la circulation des données, en convergeant vers les normes internationales qui existent déjà.»

Joni Brennan, Présidente du Conseil canadien de l'identification & authentification numériques (CCIAN)

« Le Canada est un pays qui met l'accent sur la protection de la vie privée. Nous pensons que les gens doivent pouvoir faire leurs propres choix en matière de données, qu'ils ont un droit de regard et peuvent décider de la manière dont leurs données sont partagées et dans quel but. »

Sophie KWASNY, Cheffe de l'Unité de Protection des Données du Conseil de l'Europe

« Si les différentes régions du monde veulent continuer à échanger, il faudra qu'il y ait une compréhension commune. Notre Convention 108 modernisée peut convenir pour toutes les démocraties.»

CAS D'USAGE #1

LE CONSENTEMENT AU PARTAGE D'ATTRIBUTS ET DE DONNÉES PERSONNELLES EN AUSTRALIE

Le département des transports et des routes principales du Queensland a lancé l'Application mobile de Permis Numérique, en phase d'essai depuis le premier semestre 2020. Elle sert de portefeuille d'identité numérique, stockant un large éventail de documents dans un seul coffre-fort numérique sécurisé. L'objectif est d'établir un modèle de consentement distribué, par lequel les utilisateurs décident de partager leurs données afin d'accéder à une gamme de services publics en ligne ou pour permettre une identification physique.

Les utilisateurs choisissent et contrôlent les informations qu'ils souhaitent partager et rendre visibles. Si un utilisateur veut prouver son âge, il peut utiliser l'application pour ne divulguer que l'attribut «J'ai plus de 18 ans», avec un code QR validé en ligne par le vérificateur. Le titre d'identité n'affichera pas le nom, la date de naissance ou le lieu de résidence du/de la titulaire du permis numérique.

CAS D'USAGE #2

EN AUTRICHE, DES IDENTIFIANTS SPÉCIFIQUES AU SECTEUR

Dès le départ, le programme d'identité numérique autrichien a mis en place des mécanismes solides en matière de protection et de sécurité. Tous les citoyens et résidents reçoivent un numéro du registre central des résidents (le CRR), mais ne sont pas obligés de demander une carte d'identité physique. En revanche, l'Autriche dispose d'une Carte de Citoyen (CC) virtuelle qui peut être installée sur plusieurs dispositifs selon une approche technologique neutre : cartes à puce, dispositifs USB ou applications mobiles.

L'un des aspects clés du programme autrichien en matière de protection des données est l'identifiant spécifique au service. Pour un même individu, chaque fournisseur de services utilise un identifiant différent, dérivé cryptographiquement du numéro CRR. Cela évite que les individus correspondent d'un service à l'autre, et permet la suppression et le remplacement d'identifiants cryptés en cas de fraude.

CAS D'USAGE #3

UNE PROTECTION EN «TRIPLE-BLIND» VIA LA BLOCKCHAIN AU CANADA

Verified.Me, ainsi que Government Sign-in de Verified.Me, suivent tous deux l'approche « triple-blind » : personne dans le réseau d'identification n'a accès aux transactions complètes de l'utilisateur, ni le gouvernement, ni les banques, ni l'opérateur.

Lancé pour le secteur privé en 2019, Verified.Me utilise la blockchain pour l'authentification, ce qui a joué un rôle essentiel dans la mise en place du partage de données d'identité en triple blind. Le réseau de confiance Verified.Me et le hachage cryptographique garantissent que les données proviennent d'une source fiable, qu'elles n'ont pas été altérées et que les données sont partagées par la personne à laquelle elles appartiennent.

« Sans blockchain, il est difficile de déplacer des données d'un point A à un point B sans mettre le réseau en danger : ce réseau va accéder à beaucoup de données, le mettant à risque de devenir une cible de violation."

Andre Boysen, Directeur d'Identité, SecureKey Technologies Inc.

LA PROTECTION DES DONNÉES DOIT ÊTRE JURIDIQUE AVANT D'ÊTRE TECHNOLOGIQUE

1. **Commencez par concevoir et instaurer une réglementation sur la protection des données et des organismes de contrôle indépendants avant de déployer l'identité numérique. Les organisations internationales, telles que le Conseil de l'Europe, offrent des conseils et des ressources utiles.**

2. **Répondez de manière proactive aux préoccupations concernant les données personnelles grâce à des mécanismes de protection conçus «nativement» (protection de la vie privée assurée dès la conception, partage d'attributs, etc.) et fournir aux utilisateurs des outils de contrôle et de gestion de leurs données (outils de protection des données privées).**

3. **Évitez de centraliser les données dans une base de données unique : Les identités peuvent appartenir à la fois aux fournisseurs d'identités publics et/ou privés, sur la base du consentement des utilisateurs. Pour garantir le respect de la vie privée, les données peuvent être échangées via un système de bases de données communes suivant des protocoles normalisés.**

4. **Pour éviter que les données explicites des utilisateurs ne soient partagées au sein de l'écosystème, mettez en place des filtres d'information entre les fournisseurs de services et d'identité avec un cryptage continu ou une passerelle qui garantit un niveau maximum de confidentialité pour les utilisateurs.**

OBSERVATION #3

TROUVER LE BON ÉQUILIBRE ENTRE EXPÉRIENCE D'UTILISATION ET SÉCURITÉ

Aujourd'hui, deux systèmes de pensée coexistent et créent une tension entre une expérience utilisateur sans faille et des niveaux de sécurité plus élevés :
> un niveau commun et préétablis de sécurité et des garanties pour les pays qui souhaitent disposer d'identités numériques interopérables avec une reconnaissance transfrontalière en suivant des cadres de confiance tels que le règlement eIDAS en Europe ou le cadre de confiance pancanadien au Canada lancé par le CCIAN (Conseil Canadien de l'Identification et de l'Authentification Numériques)

> un niveau de sécurité basé sur le marché, fixé par des acteurs comme Google et Facebook qui fournissent des services d'identité en ligne et établissent des normes relatives à l'expérience utilisateur dans le monde entier. Ces services sont simples et faciles à utiliser, complètement accessibles et disponibles à tout moment, partout et sur n'importe quel appareil, avec de faibles exigences d'authentification.

L'expérience eIDAS montre que certains États membres ont une approche très définie de la sécurité, tandis que d'autres sont plus flexibles. Trouver le bon équilibre entre une expérience utilisateur sans faille et des normes de sécurité élevées est essentiel pour une large adoption de l'identité numérique, mais cela reste un défi, en particulier dans les pays où l'identité numérique n'est pas obligatoire.

« Pour de nombreux petits services, il n'est pas nécessaire d'avoir un niveau de sécurité élevé. La question réside dans la définition de ce que signifie «petit». »

Eric A. Caprioli, Avocat à la Cour, Représentant France de la CNUDCI/UNCITRAL

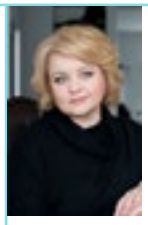
QUE PENSENT-ILS DE L'ARBITRAGE EXPERIENCE CLIENT ET SÉCURITÉ ?

Valérie Péneau, Directrice du Programme Interministériel France Identité Numérique

« Pour avoir une stratégie de sécurisation par étape, commencez par séduire l'usager en l'embarquant avec une application simple, et sécurisez-la progressivement. D'une part, les fournisseurs de services ont des difficultés à se positionner sur les différents niveaux de garantie et, d'autre part, l'écosystème d'usage n'est pas prêt pour un niveau de sécurité élevé. »

Quek Sin Kwok, Directeur Principal, Plateforme et Produits de l'Identité Numérique Nationale, GovTech Singapour

« Grâce aux progrès technologiques, il est maintenant possible d'améliorer à la fois la sécurité et l'expérience utilisateur. Par exemple, notre jeton numérique mobile SingPass est plus sûr que les mots de passe ou les SMS, et plus facile à transporter et à utiliser que les jetons matériels. Nous concevons également notre plateforme d'identité numérique pour offrir des facteurs d'authentification multiples, de sorte que les parties prenantes puissent choisir d'en ajouter si les transactions sont considérées comme plus sensibles. Nous laissons nos parties utilisatrices évaluer le profil de risque associé à leur cas d'usage . »



Jana Krimpe, Représentante du consortium Public/Privé d'Azerbaïdjan

« En Azerbaïdjan, nous avons décidé de ne pas mettre en place plusieurs solutions avec différents niveaux d'assurance : cela demanderait deux fois plus d'énergie pour expliquer la différence aux individus qui n'aiment pas changer d'instrument trop souvent. Ils ne comprennent pas pourquoi ils peuvent utiliser un mot de passe pour accéder à un service et pourquoi il ne fonctionne pas pour un autre. Nous préférons ne passer par cette procédure qu'une seule fois et nous assurer que les gens disposent de tous les instruments dont ils ont besoin, partout.»

Andre Vasconcelos, Conseiller eID du Comité de Direction, Agence pour la Réforme des Services Publics, Portugal

«Pour la Carte de Citoyen, nous avions priorisé la sécurité. Pour la Digital Mobile Key (CMD), ou Clé Mobile Numérique, nous avons conservé les mêmes exigences de sécurité mais avons mis l'accent sur l'expérience utilisateur. Cela ne demande qu'une chose : un téléphone portable avec un code PIN, sur lequel les utilisateurs reçoivent leur OTP par SMS. Aujourd'hui, il est également possible d'utiliser la biométrie au lieu d'un deuxième facteur d'authentification comme l'OTP, ce qui est plus facile que de copier celui-ci d'un appareil à un autre».

CAS D'USAGE #1

EN ESTONIE, UN PROFIL DE RISQUE PAR CAS D'USAGE

L'Estonie est l'une des sociétés avec la plus grande intégration numérique au monde, avec trois systèmes d'identité numérique interopérables (ID-Kaart, Mobiil-ID, Smart-ID). Pour les services publics, seules quelques transactions nécessitent encore une présence physique et ne peuvent être effectuées en ligne, comme l'enregistrement d'un mariage ou l'achat d'une maison.

Étant donné la haute sensibilité de certains cas d'usage (vote électronique, données médicales ou virements bancaires), le gouvernement estonien exige une inscription en personne. Il a également développé un parcours utilisateur basé sur un risque acceptable. Pour la plupart des cas d'usage quotidiens, le gouvernement profite du large éventail d'authentifiants dont il dispose pour assurer la sécurité des transactions, et garantit la meilleure expérience utilisateur possible en lui laissant le choix. Actuellement, pour accéder aux services publics et privés en ligne, les utilisateurs sont libres d'utiliser une application (Smart-ID), une carte à puce avec un lecteur de carte (ID-Kaart), ou un smartphone équipé d'une carte SIM compatible PKI (Mobiil-ID).

CAS D'USAGE #2

UN SYSTÈME DE NOTATION POUR L'AUTHENTIFICATION EN ARIZONA

Pour garantir un niveau de sécurité optimal sans dégrader l'expérience utilisateur, le ministère des transports de l'Arizona (ADOT) utilise une approche différente du système binaire oui/non de l'authentification.

Une note de risque est créée pour chaque interaction. Elle est basée sur ce qui est connu de l'utilisateur, de la date de sa dernière vérification approfondie s'il en a fait une. Elle s'appuie en partie sur un outil de détection de la fraude qui fournit des informations relatives à la connexion (type d'appareil utilisé, localisation, téléphone à prépaiement, appareil lié à une fraude, etc.).

Si la transaction n'a pas une note suffisante, un niveau d'authentification plus élevé sera requis avant de poursuivre. Les outils d'authentification améliorés comprennent la reconnaissance faciale ou l'authentification basée sur les connaissances (appelée KBA).

« Nous avons besoin de différentes stratégies d'authentification, jusqu'à la plus élevée - l'utilisation d'une identité numérique à authentification biométrique liée au smartphone. Cela nous permet d'aller aussi loin que nécessaire sans gêner nos clients».

Eric Jorgensen, Directeur de la Division des Véhicules Automobiles au Département des Transports de l'Arizona, USA

CAS D'USAGE #3

UN SERVICE DE RECONNAISSANCE FACIALE À SINGAPOUR

Quand SingPass a été lancé en 2003, il fournissait une combinaison identifiant/mot de passe aux citoyens pour accéder à tous les services publics en ligne. Pour remédier au problème des mots de passe facilement oubliés, GovTech a introduit d'autres titres d'authentification comme l'application SingPass Mobile. En outre, GovTech pilote un projet de reconnaissance faciale pour l'authentification physique et à distance. Cela aurait pour but d'améliorer la sécurité et l'expérience utilisateur grâce à un facteur supplémentaire moins encombrant qu'un mot de passe, ou un OTP par SMS, par exemple.

Le service de reconnaissance faciale est actuellement testé dans différentes agences de services publics, comme le centre des impôts. L'une des plus grandes banques de Singapour l'utilise également pour valider l'inscription à leur plateforme mobile. Les organisations qui utilisent ce service mis à disposition par GovTech Singapore ne seront averties que de la correspondance de l'individu, et n'auront accès à aucune donnée personnelle identifiable. Les premiers résultats de l'essai pilote sont encourageants et un plus grand nombre d'organisations sont en passe d'adopter ce système.

DIFFÉRENTES STRATÉGIES EN FONCTION DES IDENTITÉS NUMÉRIQUES :

1. **Dans les pays où l'identité numérique est facultative, et où l'expérience utilisateur déterminera le taux d'adoption, il est essentiel de fournir des options faciles d'utilisation et d'adapter progressivement le niveau de sécurité.**

2. **Lorsque l'identité numérique est partiellement obligatoire, certains pays (dont l'Azerbaïdjan) ont trouvé qu'il était plus facile de commencer directement avec des niveaux de sécurité élevés pour tous les services, afin de « casser les habitudes des utilisateurs »**

3. **Dans les pays à haut niveau de maturité numérique, adoptez une approche qui dépend du cas d'usage en attribuant à chaque cas un niveau de sécurité qui lui est adapté, comme en Estonie ou à Singapour.**

OBSERVATION #4

INTÉGRER L'UTILISATEUR FINAL DANS LE PROCESSUS DE DÉVELOPPEMENT & MISE EN PLACE DE L'ID NUMÉRIQUE

La proposition de valeur pour l'utilisateur final de l'identité numérique est essentielle pour son adoption et son diffusion à grande échelle par les citoyens et les entreprises. Les utilisateurs - ou plutôt les clients - doivent percevoir un intérêt et une valeur immédiats dans le cas d'usage proposé, que ce soit en termes de gain de temps, de réduction des coûts ou simplement de plus grande flexibilité. L'expérience utilisateur doit être sans encombre, avec une interface simple d'utilisation.

Les gouvernements et les porteurs de projet d'ID numérique acceptent de remettre en question l'idée qu'ils se faisaient d'abord de leurs «clients». Ils cherchent des moyens de mieux comprendre les nouvelles attentes de ces derniers, afin de les transposer à leurs propres services et expériences. Les façons de penser, les outils et les méthodes évoluent vers une plus grande «centralité du citoyen» pour s'assurer que les besoins et les attentes des utilisateurs sont pris en compte dès la conception de la solution jusqu'à son développement et sa mise en œuvre.

« La co-conception est l'un des moyens d'obtenir l'adhésion de vos citoyens. »

Christopher Goh, Manager Général, Modernisation des Permis et Immatriculations – Département des Transports et Routes Principales, Queensland, Australie

QUE PENSENT-ILS DE LA CENTRALITÉ DE L'UTILISATEUR ?

Christopher Goh, Manager Général, Modernisation des Permis et Immatriculations – Département des Transports et Routes Principales, Queensland, Australie

« Nous avons dû repenser nos clients. Nous nous sommes rendu compte qu'il y avait tant de choses que nous n'avions pas comprises. Nous avons délivré notre premier permis de conduire en 1910 : aujourd'hui, nos clients sont différents. »

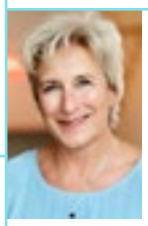
« Mettez en place un véritable processus de co-création : ne vous contentez pas d'envoyer une enquête, d'attendre un retour, faites en sorte que vos clients viennent, touchent, ressentent et travaillent sur les cas d'usage de manière relationnelle. Nous avons vu qu'il y avait tellement de choses que nous ne comprenions pas des aspects culturels car nous n'étions pas dans un dialogue, une véritable co-conception ».

Valérie Péneau, Directrice du Programme Interministériel France Identité Numérique

« Recruter des Designers UX dès le départ permet de combiner systématiquement la recherche d'une ergonomie optimale avec les exigences de sécurité ».

Lionel Fouillen, Responsable des Relations Partenaires, FranceConnect

« Afin de garantir une connexion simplifiée aux services publics, nous soutenons nos partenaires en leur proposant des recommandations UX afin de créer un parcours utilisateur de qualité. Avant la mise en production, nous vérifions le parcours utilisateur et sa mise en œuvre. Nous examinons les aspects techniques, sécuritaires et UX du service. »



Charlotte Jacoby, Cheffe de service de la Division pour le Développement de l'Infrastructure, Danemark

« A chaque fois que nous développons quelque chose, nous prenons réellement en compte les groupes de population spécifiques dès la conception - afin de nous assurer que les exigences qui sont importantes pour eux sont bien prises en compte dans nos offres et notre développement ».

CAS D'USAGE #1

UN PROCESSUS DE CO-CRÉATION D'IDENTITÉ NUMÉRIQUE DANS LE QUEENSLAND, AUSTRALIE

Le programme CORAL (« Customer Orientated Registration and Licensing ») est chargé de la conception, du développement et du déploiement de l'application de Permis Numérique dans le Queensland. L'équipe a conçu un manuel numérique expliquant les différentes étapes nécessaires à la conception d'une solution centrée sur l'utilisateur. Dès le début du projet, l'État a impliqué une grande variété de clients et parties prenantes (populations indigènes, entreprises, groupes de réglementation et de lobbying) pour co-concevoir, collaborer et prioriser les résultats obtenus, et ainsi créer l'application. Ces groupes ont permis d'assurer une bonne expérience utilisateur ainsi qu'une plus grande inclusivité et accessibilité pour les populations spécifiques. Enfin, ils ont participé à l'évaluation et à la sélection des distributeurs.

L'application est testée début 2020 dans la région de la Côte Fraser, où les utilisateurs ont été invités à prioriser de nouvelles fonctionnalités pour les versions futures.

CAS D'USAGE #2

LE DANEMARK RÉUNIT PERSONNES ÂGÉES ET MALVOYANTES DANS LA CONCEPTION DE TITRES D'IDENTITÉ

Le département du Gouvernement Danois chargé de développer la solution MitID (troisième génération de l'identité numérique nationale) travaille aux côtés d'associations pour concevoir des solutions adaptées et les faire participer à des tests utilisateurs. Ils concevront un jeton spécifique pour les personnes âgées ou malvoyantes, où le code sera lu à haute voix et auquel sera attaché un casque audio. Le jeton est également un peu plus grand et plus facile à manipuler.

Pendant la phase de mise en œuvre, ils s'appuient également sur un réseau d'enseignants par le biais des municipalités, afin d'apprendre aux personnes âgées à utiliser l'ensemble de l'infrastructure numérique et les services publics en ligne.

« Si vous voulez que votre solution numérique soit à la base de toute numérisation publique, vous devez penser aux groupes de la société qui auront du mal à y adhérer, et leur proposer des solutions. »

Charlotte Jacoby, Cheffe de service de la Division pour le Développement de l'Infrastructure, Danemark

LES CITOYENS DEVRAIENT ÊTRE INTÉGRÉS À CHAQUE ÉTAPE DU PROJET NATIONAL D'IDENTITÉ NUMÉRIQUE

1. La gouvernance du projet doit inclure une vision centrée sur le citoyen (souvent traduite par la présence de Designers UX dans l'équipe) pour valider les nouvelles intégrations ou nouveaux services.
2. Changez votre manière de voir les citoyens en interagissant avec eux, lors de groupes de travail mais aussi directement sur le terrain, dans les centres de services publics, afin de mieux comprendre leur parcours client, leurs difficultés, besoins, préférences, etc.
3. Impliquez les citoyens dans un véritable processus de co-conception : de la définition du cas d'usage à la conception de l'interface de solution numérique, ou au choix du facteur de forme de l'identité numérique. Ce processus centré sur l'utilisateur permettra également de définir les niveaux de sécurité pertinents pour chaque cas d'usage /service, et de garantir que les solutions correspondent aux préférences locales et culturelles et s'adressent à tous les citoyens.
4. Impliquez les citoyens dans la mise en œuvre et le déploiement de la solution, en ayant avec eux un flux de communication clair et fort.

OBSERVATION #5

FAVORISER LA COLLABORATION ENTRE LES SECTEURS PUBLIC ET PRIVÉ POUR UNE STABILITÉ FINANCIÈRE

« Il faut en moyenne cinq ans pour pénétrer le marché et modifier le comportement du client, avant que les choses ne commencent à réellement changer. Il est ensuite plus facile de développer de nouveaux modèles commerciaux car les acteurs comprennent les avantages de ces services et sont prêts à en payer le prix. »

Jana Krimpe, Représentante du consortium Public/Privé d'Azerbaïdjan

Dans de nombreux pays et cultures, l'identité numérique est considérée comme une prérogative de l'État. Beaucoup d'entre elles sont encore initiées, financées et gérées par des entités gouvernementales, comme c'est le cas en Autriche, à Singapour, à Oman, etc. Mais comprendre sa valeur ajoutée par rapport aux lourds investissements qu'elle nécessite reste un défi pour de nombreux gouvernements, notamment dans les pays en développement où ces investissements demandent souvent de mettre de côté d'autres besoins essentiels (infrastructures, santé, éducation, etc.). La récente pandémie COVID-19 a contribué à modifier les points de vue en démontrant «in situ» les avantages de l'identité numérique afin d'accéder à des services publics et aides sociales essentielles.

Gardant à l'esprit que l'accès aux services publics en ligne doit rester gratuit et accessible à tous, les gouvernements ont commencé à créer diverses formes de partenariats et de modèles de partage des revenus avec le secteur privé afin d'affiner leurs modèles commerciaux et capacités d'investissement. Dans des pays tels que le Danemark, le secteur financier a joué un rôle déterminant dans le succès des identités numériques. Dans les pays en développement, des opportunités prometteuses de retour sur investissement ont commencé à attirer des fournisseurs d'identité et fourisseurs de services, pour lesquels les modèles commerciaux peuvent être basés sur des volumes considérables de transactions.

Les avantages de cette collaboration public-privé sont notamment la réduction du temps de développement et de mise en œuvre de solutions, le partage des coûts d'investissement, la mise en place de services privés qui améliorent l'adoption via des cas d'usage populaires tels que la banque en ligne... Elle permet aussi un partage de compétences entre le privé et le public, un soutien dans l'authentification à distance de clients, etc.

QUE PENSENT-ILS D'UN CO-FINANCEMENT DES SECTEURS PUBLIC ET PRIVÉ ?

Mory Camara, Président du Conseil sur l'Identité (CII), ID4Africa

« Les ressources sont toujours un problème. Dans des pays comme la Guinée où tout est prioritaire - que ce soit la santé, les infrastructures, l'agriculture, le logement - la technologie en général n'est pas oubliée mais juste une priorité parmi tant d'autres. Il y a un problème de positionnement et il doit y avoir une volonté politique pour un réel développement du secteur numérique en Afrique. »

Quek Sin Kwok, Directeur Principal, Plateforme et Produits de l'Identité Numérique Nationale, GovTech Singapour

« Pour qu'une plate-forme numérique soit durable, il est important d'en identifier et démontrer d'abord clairement sa valeur. De cette valeur générée, nous pouvons ensuite en déduire un modèle commercial. Le défi de toute plate-forme numérique est d'obtenir une masse considérable de consommateurs et de fournisseurs pour former un effet de réseau, avant que le modèle commercial ne puisse décoller. »

Jana Krimpe, Représentante du consortium Public/Privé d'Azerbaïdjan

« Pour l'Afrique et l'Asie, un PPP fonctionnera parfaitement en raison du modèle commercial et de la complexité des infrastructures. Si on prend seulement le secteur financier, les services seront limités - mais si vous voulez créer un véritable service 24/7, vous devez impliquer l'ensemble du pays et motiver le gouvernement. Il est préférable de commencer immédiatement à impliquer tout le monde en créant un PPP. »

Eric A. Caprioli, Avocat à la Cour, Représentant France de la CNUDCI/UNCITRAL

« Il faut garder en tête que l'État n'a plus d'argent. Si les acteurs privés n'étaient pas capables de dépenser des millions, voire des dizaines de millions, en partenariat avec les acteurs publics, nous n'aurions pas d'identité numérique. Si l'État ne s'était pas ouvert au secteur privé, nous serions restés les bras croisés. Ce n'est pas un problème pour la souveraineté de l'État car il sera toujours là pour contrôler, auditer et sanctionner si nécessaire, et dans le cas des pays Européens, faire respecter le règlement eIDAS»

CAS D'USAGE #1

UN MODÈLE PROGRESSIVEMENT PAYANT EN INDE

La création du programme Aadhaar, le plus grand programme d'État basé sur la biométrie au monde, a été entièrement financée par le gouvernement Indien.

L'UIDAI (« Unique Identification Authority of India »), responsable du programme, a initialement proposé à tous et gratuitement tous les services d'authentification afin de minimiser les barrières à l'entrée. Elle n'a commencé à faire payer les parties utilisatrices qu'en 2019. Depuis, les organisations privées doivent payer 0,007 $US pour une authentification Aadhaar (par oui ou non), et 0,3 $US pour les transactions e-KYC.

CAS D'USAGE #2

LE SECTEUR FINANCIER CO-FINANCE ET CO-DÉTIENT L'IDENTITÉ NUMÉRIQUE DU DANEMARK

La troisième génération d'eID Danoise, appelée MitID, est co-financée et co-détenue par le gouvernement et le secteur financier.

Les fournisseurs de services qui voudront l'utiliser devront payer des frais par transaction. Cette redevance, calculée sur la base des coûts de fonctionnement, devrait être moins chère pour la plupart des fournisseurs de services que la version précédente NemID.

«Il est assez coûteux de construire une telle infrastructure pour seulement 5 millions de personnes. Donc, plutôt que d'en construire une pour le secteur public, une pour le secteur privé et une pour le secteur financier, en construire une qui puisse être utilisée dans tous les secteurs a plus de sens. Et je pense que c'est aussi la raison pour laquelle il a été intéressant pour toutes les parties de s'y associer»

Charlotte Jacoby, Cheffe de service de la Division pour le Développement de l'Infrastructure, Danemark

CAS D'USAGE #3

9 IDPS PRIVÉS FINANCENT LE PROGRAMME NATIONAL D'IDENTITÉ NUMÉRIQUE EN ITALIE

Le système public italien d'identité numérique (SPID) est un écosystème public ouvert permettant aux IdPs privées accréditées de fournir une identité numérique aux citoyens et aux entreprises. Le programme est financé à 100 % par ces IdPs privés, qui croient fermement en sa rentabilité à long terme.

Ce partenariat offre un système sûr et fiable aux services publics italiens, en déléguant les lourdes procédures d'identification (délivrance et gestion des titres d'identité) et en économisant en ressources humaines et financières.

SPID est gratuit pour les citoyens et les fournisseurs de services publics pour tous les niveaux de sécurité, à l'exception du plus haut niveau d'assurance (utilisé principalement par les professionnels) - les prestataires de services privés sont soumis à un modèle de paiement à l'usage.

AFFINER LE MODÈLE COMMERCIAL SUIVANT LA MATURITÉ NUMÉRIQUE ET LA PROPRIÉTÉ DE LA BASE DE DONNÉES

1. Avec un système centralisé détenu et financé par le gouvernement, et des services publics en ligne facultatifs (et non obligatoires), privilégiez une approche gratuite pour tous pendant les premières années (5-6) afin de favoriser son utilisation et adoption. Une fois le taux d'adoption plus ou moins stabilisé, de nouveaux modèles commerciaux (freemium, paiement à l'usage, etc.) peuvent être explorés avec des services privés et parties prenantes pour un ROI à long terme.

2. Un système d'identité numérique ayant un historique solide de stratégie publique de numérisation et de services publics en ligne obligatoires garantissant des niveaux élevés d'adoption peut opter pour un modèle de paiement à l'usage dès le départ. Toutefois, la qualité et le volume des services disponibles doivent être élevés et apporter une réelle valeur ajoutée aux utilisateurs.

3. Afin de faciliter le financement initial et les coûts opérationnels de l'identité numérique, les gouvernements peuvent s'associer au secteur financier dès le début du projet. Il contribuera également à assurer l'utilisation et l'adoption si la numérisation n'est pas obligatoire, en proposant un accès aux services bancaires en ligne, qui ont une fréquence d'utilisation élevée.

4. Si les bases de données ne sont pas établies ou détenues et centralisées par les gouvernements, ceux-ci peuvent privilégier un modèle fédéré avec financements privés de la part d'IdPs, à condition qu'ils soient régis par des cadres et des mécanismes de gouvernance gouvernementaux clairs. Les modèles fédérés constituent une alternative au financement public, sont flexibles et faciles d'utilisation pour les clients et les entreprises qui peuvent sélectionner l'IdP de leur choix.

OBSERVATION #6

CRÉER UN GROUPE DE TRAVAIL INTERGOUVERNEMENTAL ET PLURIDISCIPLINAIRE POUR DIRIGER L'IDENTITÉ NUMÉRIQUE

Les gouvernements ont souvent du mal à saisir les aspects techniques, de sécurité et de confidentialité des projets d'identité numérique et sont tentés de confier le projet à des équipes techniques et experts. Il en résulte souvent des équipes de projet en sous-effectifs et sous-représentées, qui manquent de fort soutien politique - pourtant vital à une gestion de projet efficace et fluide. L'identité numérique se situant à l'intersection de l'identité juridique et de l'accès aux services publics essentiels, il s'agit d'un projet national stratégique et politique qui doit être suffisamment doté en personnel, mais aussi représenté et géré comme tel.

> Avoir les ressources nécessaires pour gérer le projet, c'est à la fois avoir les ressources adéquates et en quantité suffisante. Les équipes sont trop souvent en sous-effectif et manquent de compétences clés telles que la communication, le marketing, l'UX/UI.
> Pour gagner en temps et en efficacité, la collaboration au sein de l'écosystème public (ministères, administrations, municipalités) et privé (fournisseurs d'identité, prestataires de services, parties prenantes, fournisseurs de solutions, etc.) de l'identité numérique dès le début est essentielle pour une conception, une gestion, une mise en œuvre et une adoption réussies.

«Aborder FranceConnect d'un point de vue purement technique est une erreur. La mise en œuvre technique est simple et bien documentée. FranceConnect, c'est avant tout des choix métier et fonctionnels, des positionnements stratégiques. »

Lionel Fouillen, Responsable des Relations Partenaires, FranceConnect

QUELS DÉFIS RELATIFS À LA GESTION DE PROJET ET LA GOUVERNANCE DE L'ID NUMÉRIQUE ?

Michiel Van der Veen, Directeur Innovation & Développement au Bureau National des Données d'Identité, Pays-Bas

« Tout ce monde de l'identité numérique est très complexe. Cela demande des personnes capables de le comprendre, d'élaborer des stratégies et de faire des choix en matière de conception. Vous devez vous assurer que vous avez ces personnes au sein de votre équipe ou que vous avez accès à elles et leurs savoirs. »

Herbert Leitold, Secrétaire Général, Centre de Technologie de l'Information, Autriche

« Toutes les parties prenantes ont été impliquées dès le départ : différents ministères, les provinces, les représentants de municipalités, ainsi que le secteur privé représenté par la Chambre de Commerce. Ces groupes de travail collaboratifs ont probablement été l'un des facteurs de succès des services publics en ligne et de l'identité numérique. Cela prend plus de temps, mais une fois que les normes sont fixées, on évite des cloisonnements et on augmente les chances de succès. »

Mory Camara, Président du Conseil sur l'Identité (CII), ID4Africa

« Nous avons des experts de niveau doctorat, des consultants internationaux hautement compétents et des techniciens de niveau 1 et 2, mais entre les deux, il y a un fossé - au niveau de la gestion de projets, des superviseurs, des managers . Cela rend la mise en œuvre, le suivi et la maintenance du projet un problème constant.»

Christopher Goh, Manager Général, Modernisation des Permis et Immatriculations – Département des Transports et Routes Principales, Queensland, Australie

« Notre principal défi quotidien est la gouvernance : comment travailler en collaboration avec toutes nos parties prenantes ? Comment faire pour ne pas diluer ce qu'ils demandent, tout en nous permettant de hiérarchiser les idées et les fonctionnalités en fonction des fonds dont nous disposons ? »

CAS D'USAGE #1

COLLABORATION INTERGOUVERNEMENTALE PROPOSANT DES SERVICES NUMÉRIQUES EN COLOMBIE

Le Registre Civil National de Colombie (RNEC) est chargé d'émettre et de gérer l'identité des citoyens, tandis que le Ministère de la Technologie et des Télécommunications (MINTIC) dirige les utilisations de l'identité numérique dans le pays par le biais de son Agence Nationale du Numérique.

Le RNEC et le MINTIC, dans un effort intergouvernemental, visent à doter le pays d'un Dossier Numérique du Citoyen comprenant un système d'authentification interopérable avec les principaux services publics. Le Dossier Numérique du Citoyen se veut être un service d'hébergement de documents en ligne accessible aux citoyens et personnes morales autorisées grâce à l'identité numérique. Il facilitera l'échange de documents administratifs entre les entités publiques et autres parties prenantes. Les services numériques seront également étendus au secteur financier et au système de vote électronique.

Cette approche intergouvernementale apporte des avantages importants en termes de sécurité, d'efficacité, de transparence et de respect de la vie privée.

CAS D'USAGE #2

UN GROUPE DE TRAVAIL INDÉPENDANT DIRIGE ET GÈRE L'eID AU NIGERIA

Dans de nombreux pays africains, les registres nationaux d'identité sont hébergés dans différents ministères ou organismes publics. Au Nigeria, cependant, le Gouvernement a créé la Commission Nationale de Gestion de l'Identité (NIMC) pour gérer les multiples parties prenantes impliquées dans la conception du programme d'identité numérique. La NIMC est une agence indépendante et autonome dirigée par un conseil d'administration composé de 18 personnes, représentant différentes agences gouvernementales du pays et son secteur privé.

Les avantages de cette organisation comprennent une meilleure coordination des parties prenantes, avec plus de fluidité et de coopération. Elle permet également de tirer parti des possibilités d'innovation du secteur privé grâce aux partenariats public-privé (PPP), dans le cadre desquels des entreprises privées fournissent des fonds en échange de flux de revenus dans le cadre du futur système d'identité numérique.

CAS D'USAGE #3

PROCESSUS COLLABORATIF MULTI-ACTEURS POUR LA CONCEPTION ET LE MANAGEMENT EN FRANCE

Lorsque le projet fédérateur d'identités numériques FranceConnect a démarré en 2015, la DINUM (Direction Interministérielle du Numérique) comptait 5 personnes à plein temps. 5 ans plus tard, environ 30 personnes travaillent pour FranceConnect, avec une majorité de développeurs et 6 fonctions de support.

Gérée par la DINUM, l'Identité numérique a été co-construite avec une quinzaine d'administrations publiques pour la gestion des données et le fonctionnement quotidien.

METTRE EN PLACE LA BONNE ÉQUIPE DE TRAVAIL POUR LA GESTION DE PROJET :

1. **Dès le départ, identifiez le projet d'identité numérique comme une priorité politique, juridique, stratégique et nationale - et non seulement technique - pour gagner une légitimité immédiate au sein des différents ministères et administrations et bénéficier d'un portage politique fort.**

2. **Mettez en place une équipe intergouvernementale avec un certain degré d'autonomie et d'indépendance pour une approche transversale et éviter les cloisonnements au sein des différents ministères. Soyez aussi présent que possible dans les organes stratégiques de gouvernance interministérielle.**

3. **Constituez une équipe multidisciplinaire solide, dotée à la fois de solides compétences en gestion de projet et d'experts en technique, construction, réglementation, UX et communication. Pour être agile, il est essentiel de disposer d'une expertise en interne dont on peut tirer des enseignements, et de travailler en parallèle avec une expertise externe.**

4. **Collaborez régulièrement avec les acteurs publics et privés. Intégrez-les dans des ateliers de co-conception, en mettant en avant les bons cas d'usage et en représentant les intérêts majeurs. Les méthodologies et outils de collaboration aident les parties prenantes à prioriser et à converger efficacement, bien qu'il s'agisse d'un défi quotidien pour bon nombre d'équipes porteuses de projet interrogées.**

OBSERVATION #7

S'IMPLIQUER DANS LES ORGANISMES INTERNATIONAUX DE RÉGULATION & STANDARDISATION

Les gouvernements qui prévoient de lancer un nouveau programme d'identité mobile doivent d'abord établir un cadre juridique complet pour qu'elle soit reconnue et soutenue par la loi, et pour garantir la confidentialité des données, la sécurité et les droits des utilisateurs.

Il est essentiel qu'ils s'appuient sur les normes internationales existantes telles que l'ISO, l'OACI, l'OSIA, le NIST ou sur des cadres tels que eIDAS pour garantir l'interopérabilité et proposer une compréhension et un langage communs entre les responsables politiques et les techniciens, mais aussi permettre la comparabilité entre régions en interne, et avec d'autres pays au niveau régional / international.

Les normes assurent la mise en place de protocoles universellement compris nécessaires au fonctionnement, à la compatibilité et à l'interopérabilité, choses essentielles au développement et à l'adoption des produits. Participer à la définition de nouvelles normes peut également permettre aux gouvernements un accès rapide aux informations relatives à l'industrie, de donner leur avis sur l'élaboration des normes et de contribuer à maintenir ouvert l'accès au marché.

« Lorsque nous avons rédigé notre décret au Vietnam, nous nous sommes inspirés de différents supports ; le premier, bien sûr, étant eIDAS. Nous avons également lu le cadre d'identité numérique d'Australie et avons également appris des États-Unis. Ces trois sources sont nos principales références.»

Lã Hoàng Trung, Directeur du Centre National d'E-Authentification, Ministère de l'Information et des Communications, Vietnam

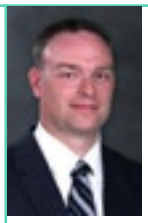
LEUR VISION DES ORGANISMES INTERNATIONAUX DE RÉGULATION ET STANDARDISATION

Valérie Péneau, Directrice du Programme Interministériel France Identité Numérique

« La question de la standardisation est colossale pour d'identité numérique. C'est un enjeu pour l'industrie et pour l'Etat, qui doit garantir sa représentation à long terme et au niveau adéquat dans les bonnes instances, afin d'anticiper les évolutions et les ruptures technologiques attendues dans les années à venir ».

Lionel Fouillen, Responsable des Relations Partenaires, FranceConnect

« Pour FranceConnect, eIDAS est très rassurant et permet deux choses : il définit clairement les niveaux de sécurité, et instaure les modalités d'interopérabilité européenne ».



Eric Jorgensen, Directeur de la Division des Véhicules Automobiles au Département des Transports de l'Arizona, USA

« Que ce soit d'État à État ou de pays à pays, la coopération et les normes telles que la norme ISO pour le Permis Numérique Mobile sont très utiles ».

« Nous allons même au-delà et cherchons à savoir quelles autres normes doivent être mises en place, non seulement d'un point de vue technologique, mais aussi du point de vue de la vérification, de l'acceptation et de la politique. Nous travaillons avec des groupes pour comprendre à quoi ressembleraient ces normes pour nous. Les normes internationales sont importantes pour l'avenir de l'identité ».

CAS D'USAGE #1

INTEROPÉRABILITÉ DU PERMIS DE CONDUIRE MOBILE (MDL) EN AUSTRALIE ET ARIZONA

La norme ISO/IEC 18013-3 définit les protocoles de communication permettant à une Application de Permis de Conduire Numérique de procéder à l'authentification et la validation d'une identité. La reconnaissance internationale et l'interopérabilité sont particulièrement essentielles étant donné la nature du permis de conduire, utilisé dans le monde entier. Les applications de vérification de permis de conduire et d'identité ne sont souvent pas assurées par le même fournisseur, en particulier à un niveau international d'interaction. Cependant, un engagement fluide entre ces deux dispositifs doit pouvoir permettre une expérience sans encombre.

De nombreuses autorités de transport public ont été impliquées très tôt dans la définition de la norme ISO, comme le département des transports (TMR) du Queensland en Australie et les autorités AMVA aux États-Unis. Elles ont pu exprimer leurs difficultés afin de les résoudre au mieux, ainsi que gagner en visibilité sur les dernières caractéristiques et protocoles pour mieux anticiper les prochaines étapes.

CAS D'USAGE #2

VERS UN CADRE INTEROPÉRABLE EN AMÉRIQUE LATINE

CLARCIEV, le Conseil d'Amérique-Latine pour l'Inscription, l'identification et l'organisation des Statistiques de l'Etat Civil travaille à la normalisation et à l'interopérabilité des registres nationaux et des solutions d'identification de chacun des pays.

Leur but final est de construire un cadre inspiré de eIDAS, mais basé sur la biométrie, ce qui n'est pas le cas actuellement en Europe. En effet, des pays d'Amérique latine tels que la Colombie, l'Argentine, l'Équateur, le Pérou et le Chili ont commencé à construire leurs programmes d'identité numérique autour de bases de données biométriques.

CAS D'USAGE #3

AU NIGERIA, DES NORMES OUVERTES POUR CAPITALISER SUR LES INFRASTRUCTURES EXISTANTES

Le Nigeria construit son cadre d'identité numérique sur des normes ouvertes telles que les spécifications ISO/ICAO pour l'agencement des données, FIPS Niveau 2 et NIST pour la PKI et le cryptage, et OSIA et la RGPD pour la conformité aux API.

L'écosystème d'Identité Mobile du Nigéria sera basé sur un système très robuste, avec tokenisation, non-répudiation, authentification biométrique par reconnaissance faciale, horodatage et audit par blockchain, et bien sûr, des interfaces API REST compatibles avec OSIA.

RAISONS VARIÉES D'INTÉGRER DES ORGANISMES INTERNATIONAUX DE RÉGULATION ET STANDARDISATION

1. **Assurez-vous que le cadre juridique reconnaisse l'identité numérique et réglemente la protection des données des citoyens.**
2. **Utilisez des normes ouvertes et assurez-vous de la neutralité des fournisseurs et de la technologie.**
3. **Prenez part aux travaux des organismes internationaux de réglementation et de normalisation, soyez intégré dans la définition des normes afin de garder une longueur d'avance.**
4. **Cherchez l'inspiration dans des cadres de confiance d'identité à succès.**

OBSERVATION #8

PENSER MOBILE AVANT TOUT

« Nous pensons que l'avenir sera mobile. L'argument principal pour soutenir notre choix de passer à l'identité mobile est la facilité d'utilisation. »

Sylvan Fux, Chef du Consulting Commerce Finance/Justice et E-Gouvernement, Liechtenstein

« Progressivement, les titres d'identité numériques ou mobiles seront dominants, dès qu'il y aura plus de confiance en leur sécurité»

Mory Camara, Président du Conseil sur l'Identité (CII), ID4Africa

Ces dix dernières années, les systèmes d'identité numérique sont progressivement passés **de formes physiques à des formes mobiles**, une tendance qui se reflète dans tous nos entretiens L'identité mobile peut prendre plusieurs formes : solutions 100 % dématérialisées, solution basée sur une carte SIM et application mobile, ou encore applications de portefeuille d'identité numérique.

Dans leurs appels d'offres, les gouvernements demandent désormais de leur fournisseur de solutions une forte **composante mobile** pour garantir une **meilleure adoption**. Cette exigence est en phase avec divers éléments : la pénétration mondiale des téléphones mobiles et smartphones, la **protection des données** lors du partage d'attributs nécessaires à l'identification des utilisateurs, **la simplicité d'inscription** et de délivrance des titres d'identité, la **résilience** lors de la mise à jour en direct d'attributs d'identité, et un remplacement simple, sûr et rentable des titres de connexion en cas de perte. Les applications mobiles tirent également parti de la pléthore de fonctionnalités offertes par les appareils mobiles, comme le sans contact avec le NFC, le Bluetooth ou les caractéristiques biométriques. Les identités numériques qui ont commencé au début des années 2000 avec des jetons physiques sont maintenant toutes en train d'évoluer vers des stratégies mobiles.

La technologie et les appareils d'identité mobiles sont **de plus en plus sûrs, grâce à des mécanismes de crypto-graphie en boîte blanche, à des Trusted Execution Environment (environnements fiables pour l'execution de l'application) ou à des eSIMs.** Pour un niveau d'assurance plus élevé et dans les cas d'usage sensibles, des alternatives physiques intelligentes restent nécessaires. À l'avenir, les titres d'identité mobiles et les titres physiques intelligents devraient continuer à coexister.

LEUR OPINION SUR L'IDENTITÉ MOBILE

Margus Arm, Député Directeur Général, Autorité du système d'informations Estonien, Directeur Branche système d'information de l'Etat

«Je pense que si je repartais de zéro aujourd'hui, je ne ferais plus de carte d'identité. Cela devrait être basé sur le téléphone portable, car distribuer une carte n'est pas simple, et il faut mettre à jour les logiciels. Il est impossible de couvrir tous les citoyens. Je pense que les nouveaux systèmes doivent être basés sur le téléphone portable et la biométrie parce que vous l'avez toujours sur vous.»

Jana Krimpe, Co-Présidente de GANMI – Alliance Mondiale des Identité Nationales Mobiles

« Nous considérons la eSIM (carte SIM virtuelle) comme une alternative de confiance aux solutions basées sur le cloud en termes de cryptographie, alors que la sécurité et le contrôle des signatures dans le cloud suscitent encore beaucoup d'inquiétudes. La eSIM a le potentiel d'être plus sûre grâce à la possibilité d'y intégrer plusieurs types de cryptographie et de passer à une autre technologie si l'une d'entre elles est compromise. Le seul défi est la standardisation. »

Joni Brennan, Présidente du Conseil canadien de l'identification & authentification numériques (CCIAN)

« Dans les années à venir, les citoyens pourraient avoir à la fois une carte à puce physique à la maison et un titre intelligent stocké dans leur portefeuille numérique, un réseau ou un système de confiance. »

Christopher Goh, Manager Général, Modernisation des Permis et Immatriculations – Département des Transports et Routes Principales, Queensland, Australie

« La COVID a montré l'importance de notre application, avec une validation sans contact de l'identité via notre permis numérique, mais aussi la possibilité d'enregistrer facilement qui était dans une boîte de nuit ou une fête en cas de contamination. C'est mieux qu'une carte d'identité en plastique, ou que de partager un stylo et d'écrire les noms sur une liste de présence. Nous sommes sur le point d'étendre ce service aux restaurants. »

CAS D'USAGE #1

UNE ID MOBILE POUR PLUS DE FLEXIBILITÉ AU LIECHTENSTEIN

Lancée en avril 2020, eID.li est la nouvelle application d'identité numérique de la Principauté du Liechtenstein avec laquelle les citoyens et les résidents ainsi que les ressortissants étrangers peuvent s'identifier et se connecter en toute sécurité aux services publics électroniques et s'authentifier grâce à la biométrie.

Le gouvernement du Liechtenstein a décidé de remplacer ses cartes à puce d'origine par une identité mobile pour plusieurs raisons :
> plus de flexibilité et de réactivité en cas de problèmes techniques ou de sécurité
> vérification en direct des attributs.

« Les solutions mobiles nous permettent de vérifier en direct les attributs des utilisateurs sur notre base de données. Cela ne se base plus sur une signature de la carte à puce, car l'identité mobile ne stocke aucune donnée sur le téléphone. Il récupère toujours les informations les plus récentes dans la base de données. Si quelqu'un se marie ou déménage, il n'est pas nécessaire d'émettre une nouvelle carte »

Sylvan Fux, Chef du Consulting Commerce Finance/Justice et E-Gouvernement, Liechtenstein

CAS D'USAGE #2

L'AZERBAÏDJAN A OPTÉ POUR UNE SOLUTION BASÉE SUR LA CARTE SIM

L'identité mobile d'Azerbaïdjan, appelé Asan İmza, est une carte SIM connectée à 3 certificats différents (citoyens, entreprises, fonctionnaires), ce qui équivaut à une carte d'identité physique dans un environnement électronique.
L'Identité mobile peut être utilisée comme une forme d'identité électronique sécurisée pour prouver son identité et signer des documents. L'utilisateur ne dispose que d'un seul code PIN, quel que soit le certificat utilisé, pour s'authentifier et signer.

« Tout le monde sait utiliser un téléphone portable, même s'il a un faible niveau d'alphabétisation. Une solution basée sur la carte SIM a l'avantage de fonctionner dans tous les types de réseau, à partir de la 2G. La pénétration des smartphones sur le marché n'est pas aussi rapide que nous voulons l'admettre. Internet est encore assez cher et l'accessibilité à un bon réseau haut débit est également une grande question. Une solution basée sur les SMS fonctionne beaucoup mieux, en particulier pour les marchés en développement.»

Jana Krimpe, Représentante du consortium Public/Privé d'Azerbaïdjan

CAS D'USAGE #3

UNE STRATÉGIE 100% SANS DISPOSITIF POUR LE PROGRAMME ITALIEN SPID

Le SPID, le Système Public Italien d'Identité Numérique, est géré par l'»Agenzia per l'Italia Digitale» (AgID) et financé par 9 fournisseurs d'identité privés accrédités.

Le SPID est la première identité numérique à avoir passé la procédure de notification eIDAS sans carte ni jeton. Il a été conçu pour être 100% sans dispositif, à l'exception du smartphone. Certaines alternatives sont possibles pour des niveaux d'authentification plus élevés, pour lesquels un HSM (Hardware Security Module) est requis.

« SPID est également compatible avec les cartes à puce telles que la carte d'identité électronique, pour obtenir un plus haut niveau d'assurance, mais cela n'est pas souvent utilisé car il faut acheter un lecteur de carte à puce, ou au moins un smartphone avec la technologie NFC, ce qui n'est pas évident pour les populations âgées, n'ayant pas toujours les compétences nécessaires. »

Andrea Spallacci , Chef de Projet, Agenzia per l'Italia Digitale (AgID)

QUE VEUT DIRE « PENSER MOBILE AVANT TOUT » ?

1. Profitez des fonctionnalités mobiles et des dernières technologies embarquées (NFC, Bluetooth, biométrie) pour offrir une expérience utilisateur améliorée avec des fonctionnalités avancées telles que l'inscription à distance, l'authentification biométrique, les mécanismes de confidentialité, les nouvelles possibilités de l'IoT, etc.

2. Offrez une expérience utilisateur fluide avec une approche mobile et combinez à la fois des titres d'identité physiques intelligents tels que les cartes à puce avec des justificatifs mobiles chaque fois que cela est nécessaire pour atteindre un niveau de sécurité plus élevé lorsque des cas d'usage sensibles l'exigent.

3. Les identités mobiles basées sur des logiciels sont indépendantes des opérateurs de réseaux mobiles, ce qui peut être un facteur de décision important pour certains pays.

4. Profitez d'une grande flexibilité de mise sur le marché avec les applications mobiles, évolutives par nature, permettant aux gouvernements d'y ajouter plus de fonctionnalités au fur et à mesure (ex : les fonctionnalités covid ont été intégrées dans les portefeuilles d'identité numérique).

OBSERVATION #9

METTRE EN PLACE DES PROCÉDURES AGILES ET ITÉRATIVES – DE MANIÈRE EXPLICITE

Le développement et les processus de mise en œuvre d'identité numérique du monde entier évoluent en fonction de l'évolution rapide des technologies et des usages. Agile est une nouvelle vision et méthodologie visant à délivrer de la valeur le plus rapidement possible, et suivant des étapes successives – chacune d'entre elles apportant des améliorations ou des fonctionnalités supplémentaires. Plusieurs gouvernements ont adopté cette approche pour développer leurs projets d'identité numérique, en publiant des versions préliminaires (appelées MVP, ou Produit Minimal Viable) afin **d'intégrer les retours des utilisateurs et des parties prenantes.**

Les porteurs de projet d'identité numérique et les responsables gouvernementaux ont identifié **l'approche Agile comme facteur clé de succès**, pour plusieurs raisons :
> Agile intègre plus fréquemment les retours des utilisateurs et des tests techniques, évitant ainsi un gros **effet tunnel lors du développement**, qui pourrait mener à des problèmes techniques non anticipés et un risque d'être obsolète dès la sortie.
> **Les pilotes et les «Produits Minimums Viables»** permettent d'identifier non seulement les problèmes techniques, mais aussi les **difficultés juridiques, politiques et culturelles.**
> **Les pilotes sont des preuves fortes** des cas d'usage réussis et de la satisfaction client aux futurs partenaires et parties prenantes.

« Ce sera un défi de faire comprendre que, traitant d'une application numérique, il y aura forcément des mises à jour, des versions successives. Ce n'est pas facile à comprendre, ni pour l'usager, ni pour les commanditaires publics, qui sont habitués à décliner une offre pour un besoin dans une approche plus traditionnelle et stable. »

Valérie Péneau, Directrice du Programme Interministériel France Identité Numérique

LEURS CONVICTIONS SUR LES PROCÉDÉS AGILES

Michiel Van der Veen, Directeur Innovation & Développement au Bureau National des Données d'Identité, Pays-Bas

« Aux Pays-Bas, la législation est telle qu'il est très difficile de faire des essais, ce qui entrave l'innovation. L'identité numérique n'est pas quelque chose que l'on peut développer depuis une tour d'ivoire. Du point de vue de la politique, il est aussi important de tester et apprendre suivant son développement.»

Herbert Leitold, Secrétaire Général, Centre de technologie de l'Information, Autriche

« La principale conclusion du projet pilote mené sur l'identité numérique et les services transfrontaliers est qu'au-delà du défi technique, nous devons anticiper tous les autres problèmes auxquels nous serons confrontés : questions juridiques, protection des données, etc. Ensuite, nous saurons sur quoi travailler. »

Quek Sin Kwok, Directeur Principal, Plateforme et Produits de l'Identité Numérique Nationale, GovTech Singapour

« Il y a trois ans, je n'aurais pas pu vous dire exactement quels services de confiance nous allions proposer et qui allait les utiliser. Nous avions une vision générale, une idée, une intuition. Mais nous devons accepter que l'avenir est imprévisible et que nous n'avons pas toutes les réponses. Nous avons donc dû être très agiles - cela signifie être capable d'écouter, de comprendre les lacunes, problèmes et inefficacités par rapport au marché cible, être réceptif à leurs besoins et en saisir rapidement les opportunités. Cela a été une aventure passionnante pour nous. »

« Il n'est pas facile d'être agile, tous nos processus doivent l'être : la gouvernance, l'approvisionnement, la manière dont nous finançons et développons le produit. Par exemple, il y a cinq ans, GovTech Singapour a commencé à renforcer ses capacités d'ingénierie en interne, au lieu de s'appuyer sur l'externalisation de nos projets. Nous maîtrisons désormais mieux nos processus de gestion et de développement de produits, et sommes plus réactifs aux besoins de nos citoyens et de nos entreprises. »

CAS D'USAGE #1

LE QUEENSLAND ADOPTE UNE APPROCHE AGILE

En 2016, le Ministère des Transports et des Routes Principales du Queensland (TMR) a publié son plan stratégique numérique 2016-2020, qui accorde une priorité claire notamment à la connexion des clients.

Elle est l'une des premières entités publiques à adopter la méthodologie Agile et à la placer au cœur de son processus d'appel d'offres pour l'identité numérique. L'Application de Permis Numérique a été développée en utilisant un processus de co-conception et un sprint de 4 semaines avec différents fournisseurs de technologie. La méthodologie Agile-SCRUM a permis de développer un logiciel complexe de type portefeuille, qui héberge divers documents numériques dans une application simple d'utilisation, grâce à une approche itérative basée sur les commentaires réguliers des clients.

Des tests avec des panels d'utilisateurs finaux ont été effectués à la fin de chaque sprint et tout au long du cycle de développement du logiciel afin d'évaluer et améliorer son intérêt et utilisation. Il est essentiel d'adapter les procédures d'appel d'offres et d'approvisionnement à une approche agile afin de proposer aux citoyens des services publics efficaces, transparents et rentables. De nombreux gouvernements adoptent ces nouvelles méthodes.

CAS D'USAGE #2

L'APPLICATION MOBILE ALICEM EN FRANCE, UNE EXPERIENCE INTERNE

L'application mobile Alicem est une expérience novatrice lancée en 2019 avec des fonctionnalités et une portée limitées. Cette expérience a permis de recueillir des informations sur les moyens techniques (sous le contrôle de la CNIL[1] et de l'ANSSI[2]), les retours des utilisateurs et les cadres juridiques, ainsi que lancer un débat de société sur les données biométriques, la reconnais-sance faciale, les préjugés discriminatoires et l'inclusion.
Les retours ont servi à adapter les appels d'offres et à confirmer l'évolution vers une application mobile permettant l'identification et l'authentification sécurisées, avec une future version bureau.

« Choisissez un mode de développement agile, permettant de gagner en réactivité et d'être dans une perspective d'amélioration constante de la solution, en lien très étroit avec les retours des utilisateurs et ceux de la communauté. »

Valérie Péneau, Directrice du Programme Interministériel France Identité Numérique

[1]CNIL: Autorité publique française chargée de la protection des données à caractère personnel
[2]ANSSI: Agence Nationale de Sécurité des Systèmes d'Information en France

CAS D'USAGE #3

PROJET PILOTE MYINFO, UNE PLATEFORME DE PARTAGE DE DONNÉES, À SINGAPOUR

Le pilote MyInfo, une plateforme de partage de données au sein du NDI, le projet d'Identité Numérique Nationale de Singapour, a été lancé en 2018 avec plusieurs banques, principalement pour les cas d'usage d'eKYC. **Deux ans après le succès du projet pilote,** plus de 300 services du secteur privé s'appuient désormais sur MyInfo pour uniformiser l'inscription des utilisateurs et renforcer la confiance des clients.

« Ces projets pilotes transfrontaliers n'ont pas pour but d'explorer des approches de mise en œuvre technique - cette partie est généralement assez simple. Mais grâce à ces pilotes, nous espérons apprendre à connaître les différences de législation, de normes et d'autres contextes, afin de voir comment lier ces différences et parvenir à une reconnaissance mutuelle. »

Quek Sin Kwok, Directeur Principal, Plateforme et Produits de l'Identité Numérique Nationale, GovTech Singapour

ÊTRE AGILE SIGNIFIE TESTER MAIS AUSSI CHANGER LES MENTALITÉS, EN COMMENÇANT EN INTERNE

1. Réorganisez les capacités d'ingénierie internes (gestion et développement de produits, architecture, etc.) au sein même de l'équipe de travail sur l'Identité Numérique, afin d'être plus réactif et plus agile, en complément des partenaires externes.
2. Quand vous travaillez avec des partenaires externes, assurez-vous que vos équipes internes soient présentes afin de favoriser une réelle co-construction, et que chacun apprenne des compétences et aptitudes des autres.
3. Adoptez une approche agile pour l'approvisionnement, les processus et la mise en œuvre en testant et en réalisant des projets pilotes - Faites de la pédagogie et communiquez à ce sujet - non seulement envers le public (citoyens et entreprises) mais envers toutes les parties prenantes (services publics, partenaires, parties tierces, etc.). Agile est une nouvelle façon de voir, changer les habitudes prend du temps.
4. Choisissez une technologie régie par des normes afin d'assurer son interopérabilité et gagner en flexibilité et réactivité.

OBSERVATION #10

METTRE EN PLACE DES INFRASTRUCTURES ADAPTABLES & MODULAIRES QUI FONT LE LIEN ENTRE PASSÉ ET FUTUR

L'héritage informatique et ses débuts sont différents pour chaque pays, ce qui explique la diversité des systèmes d'identité numérique, centralisés ou fédérés. Alors que certains peuvent s'appuyer sur des systèmes d'identité régaliens, qui inclut un Registre National de Population numérique, d'autres qui commencent seulement à enregistrer leur population choisissent de passer directement à des modèles plus décentralisés.
Indépendamment de ces contextes initiaux, l'objectif de chaque pays reste le même : créer des **écosystèmes d'identité numérique** robustes et fiables. Cette approche holistique de l'identité représente un défi mais est nécessaire à bien des égards. La difficulté consiste à passer d'une base de données fermée et sécurisée à une infrastructure ouverte, flexible et évolutive, **capable d'intégrer facilement de nouveaux services privés et publics, de nouveaux titres d'identité et de nouveaux modèles émergents,** tels que le Self Sovereign Identity (SSI)

Les gouvernements auront un rôle essentiel dans la mise en place d'un tel écosystème en émettant de manière sécurisées les identités et titres d'identité, en créant un espace réglementaire pour l'innovation et en fournissant des cadres et des normes juridiques.

« Nous avons hérité de systèmes que nous devons gérer, nous ne commençons pas notre système du début. Nous devons le faire d'une manière qui fonctionne avec l'ancien, en créant des liens vers le nouveau et en faisant de la place pour ce qui viendra ensuite, dans une perspective d'économie numérique globale. »

Joni Brennan, Présidente du Conseil canadien de l'identification & authentification numériques (CCIAN)

LEURS CONVICTIONS RELATIVES AUX INFRASTRUCTURES D'IDENTITÉ NUMÉRIQUE

Michiel Van der Veen, Directeur Innovation & Développement au Bureau National des Données d'Identité, Pays-Bas

«L'innovation avance tellement rapidement que la technologie dont vous disposez aujourd'hui sera dépassée dans cinq ans. En tant que gouvernement, nous ne souhaitons pas seulement développer un système mais un écosystème d'identité numérique, avec les limites et conditions qui lui sont nécessaires».

« Notre gouvernement se veut une source fiable d'information faisant autorité, afin d'apporter une confiance dans l'économie numérique. Aux Pays-Bas, nous avons introduit la notion d' « identité numérique source » : une information légale, qui permet une identification secondaire, des applications et ses systèmes. C'est un élément de base de l'économie numérique. »

Margus Arm, Député Directeur Général, Autorité du système d'informations Estonien, Directeur Branche système d'information de l'Etat

« Ce qu'il est important de voir dans notre programme, c'est que nous n'avons pas qu'une seule grande base de données centralisée, mais des milliers. Si une tierce partie veut rejoindre l'écosystème, elle n'a qu'à acheter la plateforme X-Road et utiliser le protocole, sans avoir besoin de remplacer son système informatique et ses bases de données existants.»

« Intégrer la plateforme X-Road était trop lourd pour les startups. Nous recherchons des solutions alternatives - les startups ont besoin d'une alternative à X-Road qui soit sécurisée et standardisée.»

Eric Jorgensen, Directeur de la Division des Véhicules Automobiles au Département des Transports de l'Arizona, USA

« Avant, notre architecture était basée sur un système mainframe, qui avait ses avantages mais n'était pas assez flexible pour s'adapter aux changements et demandes modernes. Nous avons décidé de passer à une architecture modulaire. Lors de la construction de notre système, nous avons sans arrêt pensé à comment ajouter la prochaine brique technologique, même sans savoir de quoi il s'agirait. C'est un changement de philosophie. »

CAS D'USAGE #1

UNE PLATEFORME D'INTERMEDIAIRES AU DANEMARK POUR ÊTRE PLUS MODULAIRE

Pour sa troisième génération d'identité numérique (MitID), le Danemark et le secteur financier ont co-financé une infrastructure à sécurité renforcée en limitant son accès aux intermédiaires certifiés. Ils géreront l'interface technique et vendront leurs services aux prestataires de services.

Cette infrastructure devrait permettre de résoudre les problèmes d'intégration et de sécurité grâce à sa modularité inhérente. Les titres d'identité peuvent être branchés ou débranchés en fonction des besoins des utilisateurs et de l'évolution de la technologie, et les petits fournisseurs de services pourront intégrer MitID sans avoir de compétences informatiques en internes.

« Il est plus logique d'avoir quelques intermédiaires qui ont la capacité de gérer la sécurité et l'intégration de l'infrastructure technique ».

« Nous voulions pouvoir moderniser et mettre à jour l'infrastructure en permanence : il y aura probablement pas mal de changements techniques au fil des années ».

Charlotte Jacoby, Cheffe de service de la Division pour le Développement de l'Infrastructure, Danemark

CAS D'USAGE #2

L'ID NUMÉRIQUE, UN OUTIL MODULAIRE PERMETTANT AU SECTEUR PRIVÉ DE STIMULER L'ÉCONOMIE NUMÉRIQUE EN INDE

Aadhaar a été conçu dès le départ avec des services et des protocoles ouverts qui peuvent s'étendre au secteur privé et stimuler l'économie numérique. Différentes fonctions se basent sur le programme, avec une API ouverte permettant aux entreprises de procéder à des vérifications eKYC via la base de données Aadhaar (pour un justificatif de domicile ou d'autres attributs biographiques ou biométriques). Le partage de données se fait toujours avec le consentement de l'individu.

Depuis mars 2019, les organisations privées doivent payer 0,007 USD pour l'authentification Aadhaar (pour une réponse par oui/non), et 0,3 USD pour les transactions eKYC. En 2018, un total de 4,9 milliards de transactions e-KYC ont été effectuées via Aadhaar.

CAS D'USAGE #3

UN CADRE AGNOSTIQUE POUR ASSURER UNE CONFIANCE NUMÉRIQUE AU CANADA

LE DIACC, le Conseil Canadien pour l'Identité et l'Authentification Numériques, élabore actuellement un cadre de confiance pancanadien, (Pan Canadian Trust Framework) avec la collaboration d'acteurs publics et privés.

L'objectif de ce cadre est de cartographier et d'identifier les points d'intersection entre les technologies et les politiques juridiques. Il est conçu comme agnostique et sera applicable à tout modèle existant (fédération, plateforme d'intermédiaire, etc.) ou émergent (Registre Distribué et Blockchain, Identité Auto-Souveraine (SSI)).

« La portabilité des titres d'identité de multiples écosystèmes deviendra essentielle, tout comme l'interopérabilité basée sur différentes technologies, mais s'appuyant sur des normes identiques telles que celles du W3C».

Joni Brennan, Présidente du Conseil canadien de l'identification & authentification numériques (CCIAN)

FACILITEZ L'INTÉGRATION TECHNIQUE EN CRÉANT UN ENVIRONNEMENT FAVORABLE :

1. Adoptez une architecture modulaire pour accroître la flexibilité de l'écosystème et simplifier l'intégration technique pour les prestataires de services. Par exemple, déléguez l'intégration grâce à une plateforme d'intermédiaires.
2. Atteignez une véritable interopérabilité qui fonctionne autour de technologies multiples. Pour les titres d'identité et fournisseurs d'identité, adoptez une approche «plug-n-play» afin de suivre les besoins des utilisateurs et assurer une modernisation et mise à jour constantes de l'infrastructure.
3. Soyez neutre sur le plan technologique et suivez les recommandations en termes d'exigences minimales, ainsi que les normes internationales.
4. Créez un environnement favorable à l'innovation, en matière de politiques et de réglementations, pour créer un réel écosystème : assurez l'adéquation entre le cadre politique et règlementaire, et des avancées technologiques qui soient sécurisées et pragmatiques.

OBSERVATION #11

FOURNIR DES SERVICES UTILES ET RÉCURRENTS EN S'APPUYANT SUR LE SECTEUR PRIVÉ

Le retour d'expérience des identités numériques nationales qui ont progressivement ouvert leur accès aux fournisseurs de services privés est unanime : fournir des services en ligne utiles et récurrents (2 à 3 fois par mois) aux citoyens est essentiel pour créer une dynamique d'adoption - et les services du secteur privé sont un accélérateur essentiel.
La plupart des identités numériques, lancées et financées par les gouvernements dans le cadre d'un accès aux services publics en ligne, avait pour objectif initial de fournir des services publics en ligne gratuits aux citoyens, tels que la déclaration d'impôts, l'accès au service des retraites, etc. Au fil des années, et plus encore pendant la pandémie COVID-19, des services publics plus récurrents et plus rapides ont été rendus disponibles en ligne, comme les portails éducatifs sur lesquels les parents peuvent se connecter régulièrement pour accéder aux notes de leurs enfants. L'identié numérique a progressivement ouvert l'accès aux services du secteur privé.

Les services bancaires en ligne se sont révélés très efficaces pour susciter l'adhésion, les visites récurrentes, et l'adoption. Encouragés par ces résultats, de nombreuses identités numériques - à Singapour, en Australie et en France - intègrent de nouveaux acteurs privés, à différents niveaux (banques nationales, Assurances, Opérateurs mobiles, ou encore restaurants, bars et boîtes de nuit locales). Cette tendance a pris une telle ampleur que les organismes de réglementation internationaux tels que eIDAS en Europe mènent actuellement des consultations publiques pour étendre l'interopérabilité au secteur privé et améliorer l'usage et l'adoption des solutions d'identités numériques.

« Si nous n'avions pas eu la diffusion que nous avons eu en travaillant avec les banques, nous n'aurions jamais osé rendre la numérisation obligatoire. »

Charlotte Jacoby, Cheffe de service de la Division pour le Développement de l'Infrastructure, Danemark

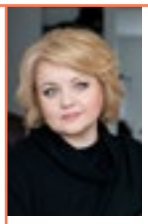
QUE PENSENT-ILS DE L'OUVERTURE AUX SERVICES DU SECTEUR PRIVÉ ?

Quek Sin Kwok, Directeur Principal, Plateforme et Produits de l'Identité Numérique Nationale, GovTech Singapour

« Fournir à chacun une identité numérique n'est pas seulement un moyen d'atteindre notre but. L'important est le cas d'usage - comment l'identité numérique peut-elle apporter des avantages directs aux consommateurs et aux entreprises. Nous travaillons en partenariat étroit avec l'industrie pour identifier ces cas d'usage et en faire une réalité, je pense que c'est ce dont nous sommes le plus fiers ».

Andre Vasconcelos, Conseiller eID du Comité de Direction, Agence pour la Réforme des Services Publics, Portugal

« Nous avons créé des partenariats avec des associations et des mouvements pour pousser la numérisation de la société et présenter la Clé Numérique Mobile (CMD). Cela nous a aidés à forger un lien et une confiance avec le secteur privé. Cependant, le principal moteur de l'adoption par le secteur privé n'a pas tant été la promotion de la CMD que sa valeur ajoutée. C'est pour cela qu'ils ont décidé d'investir et de modifier leurs systèmes, ils y voient un retour sur investissement. »



Jana Krimpe, Représentante du consortium Public/Privé d'Azerbaïdjan

« Il est trop difficile de créer de nouveaux comportements d'utilisateurs vis-à-vis des services numériques s'ils n'accèdent aux services qu'une fois par an. Il est important qu'il y accèdent au moins plusieurs fois par mois ».

Margus Arm, Député Directeur Général, Autorité du système d'informations Estonien, Directeur Branche système d'information de l'Etat

« L'une des nos meilleures incitations pour l'adoption a été l'impôt : en faisant leur déclaration sur papier, les citoyens devaient attendre trois mois pour leur remboursement d'impôts, contre 10 jours avec une déclaration en ligne utilisant la carte d'identité. De nombreux utilisateurs n'ont pas réfléchi longtemps.

« Coopérer et impliquer les banques est essentiel, les gens se connectent à leur banque en ligne au moins une fois par mois voire une fois par semaine pour payer leurs factures, etc. En Estonie, près de 75% des transactions proviennent du secteur financier : banques et compagnies d'assurance ».

CAS D'USAGE #1

UNE STRATÉGIE GAGNANT-GAGNANT POUR LES SECTEURS PUBLIC ET PRIVÉ AVEC LA CMD AU PORTUGAL

La CMD, la Clé Numérique Mobile lancée en 2014 par le gouvernement Portugais, s'est ouverte au secteur privé dès la date de son lancement. Cependant, un réel intérêt a été observé dès lors que l'adoption a atteint 1 million de Portugais - 10% de la population.

La principale valeur ajoutée de l'utilisation de la CMD pour le secteur privé fut le service d'authentification et la signature électronique qualifiée, d'autant plus que ces services sont actuellement gratuits pour toutes tierces parties (sauf coûts des SMS pour l'OTP). Lors des épidémies de COVID-19, les banques et opérateurs de télécommunications ont pu identifier et inscrire de nouveaux clients, ainsi qu'authentifier les clients existants.

Habitués à des processus d'authentification sécurisés depuis la création en 2007 de la Carte de Citoyen électronique pour accéder aux services publics en ligne, les citoyens demandent maintenant les mêmes niveaux de sécurité de la part du secteur privé.

CAS D'USAGE #2

DE NOUVEAUX SECTEURS D'ACTIVITÉ BIENTÔT DISPONIBLES PAR FRANCECONNECT

FranceConnect, fédérateur d'identité numérique, met en relation les utilisateurs avec 800 services publics et privés, via le fournisseur d'identité de leur choix.

Pour favoriser l'adoption, des services à usage plus fréquent seront intégrés dans l'écosystème de FranceConnect d'ici 2021, comme les aides au logement (CAF), les allocations chômage (Pôle Emploi) ou l'accès aux bulletins scolaires en ligne. L'intégration de nouveaux services privés avec des réglementations sectorielles spécifiques telles que les consultations médicales en ligne, les plateformes de covoiturage ou les agences immobilières est à la fois un défi à relever et une priorité pour l'avenir de FranceConnect.

« Nous lançons actuellement un essai visant à intégrer de nouveaux secteurs d'activité qui ne sont pas actuellement éligibles à FranceConnect (transport de personnes, médico-social, location immobilière, location de voitures, etc.)

Lionel Fouillen, Responsable des Relations Partenaires, FranceConnect

CAS D'USAGE #3

PARTENARIAT AVEC LES BANQUES POUR UNE DIFFUSION ÉTENDUE DU NEMID AU DANEMARK

NemID, une carte ou application à code (bientôt MitID) a été lancée en 2010 grâce à une coopération unique entre l'Agence Danoise de Numérisation et le secteur bancaire Danois (Finans Denmark) afin de permettre aux citoyens d'utiliser leur carte d'identité numérique pour les opérations bancaires en ligne. Proposer ces services a été déterminant afin de favoriser la diffusion et la fréquence d'utilisation du service auprès des citoyens Danois. Cette étape a été nécessaire avant de rendre NemID obligatoire. Aujourd'hui, le taux d'adoption est proche de 100 %.

« Le principal intérêt de s'associer au secteur financier est certainement d'avoir cette diffusion et la fréquence d'utilisation - sans cette dernière, la numérisation n'aurait pas pu être rendue obligatoire. »

Charlotte Jacoby, Cheffe de service de la Division pour le Développement de l'Infrastructure, Danemark

PROPOSEZ DES SERVICES RÉCURRENTS ET UTILES AFIN DE STIMULER L'ADOPTION :

1. Proposez des services en ligne qui soient utiles aux citoyens et font une réelle différence pour l'usage quotidienne, l'efficacité et les économies de temps et d'argent. D'autre part, évitez de donner la priorité aux cas d'usage intrusifs et limités qui ne concerneraient qu'une petite partie de la population.

2. Privilégiez l'accès aux services qui ont une fréquence d'utilisation élevée, tels que les services de banque en ligne, qui sont utilisés plusieurs fois par mois voire par semaine.

3. Travaillez conjointement les différentes parties utilisatrices, elles connaissent leurs clients, encouragez-les à parler des cas d'usage qu'ils ont eux-mêmes identifiés.

OBSERVATION #12

FOURNIR UNE PROCÉDURE D'INSCRIPTION SÛRE, SIMPLE ET MULTIPLE

« Les citoyens italiens sont très contents de ces procédures à distance. Il n'y a pas d'opposition. Il y a eu une forte augmentation des demandes d'authentification à cause de la pandémie. Personne ne souhaite se rendre dans une entreprise privée ou un service public pour faire la queue et obtenir une identité».

Andrea Spallacci, Chef de Projet, Agenzia per l'Italia Digitale (AgID)

La procédure d'inscription consiste à capturer et enregistrer les attributs d'identité de la personne qui la revendique, ce qui peut inclure des données biographiques (ex : nom, date de naissance, sexe, adresse, courriel), des données biométriques (ex : empreintes digitales, scan de l'iris) et un nombre croissant d'autres attributs («Technical Standards for Digital Identity», ID4D, 2017). L'inscription est la clé de la création d'une identité numérique fiable.

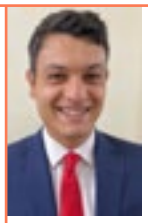
Un processus d'inscription sûr, pratique et rapide est essentiel pour la mise sur le marché et l'adoption à grande échelle de l'identité numérique, tant pour les citoyens que pour les entreprises, en particulier dans un contexte où les services en ligne ne sont pas obligatoires. Il s'agit d'un moment décisif qui établit une certaine confiance entre l'utilisateur, le fournisseur de solution et le gouvernement.

Aujourd'hui, la plupart des procédures d'inscription exigent une présence physique pour plus de sécurité. Certains pays comme l'Italie, les États-Unis ou les Pays-Bas proposent cependant des options d'inscription à distance, et de plus en plus de pays testent des technologies de vérification à distance par reconnaissance faciale.
Pour autoriser l'identification à distance et contre-attaquer la fraude de documents contrefaits ou falsifiés, de manipulation vidéo ou d'absence de vérification de l'identité d'un utilisateur par un agent, eIDAS travaille actuellement à améliorer les recommandations, la normalisation, et les pratiques d'évaluation de la conformité dans l'utilisation de ces technologies («eIDAS COMPLIANT eID SOLUTIONS, Security Considerations and the Role of ENISA», mars 2020).

CE QU'ILS PENSENT DES PROCESSUS D'INSCRIPTION

Margus Arm Député Directeur Général, Autorité du système d'informations Estonien, Directeur Branche système d'information de l'Etat

« Notre sécurité se base sur un processus d'inscription sécurisé. Une grande partie de la confiance repose sur ce processis en face à face. À l'avenir, il sera peut-être possible de le faire à distance. Cependant, nous exigeons actuellement une inscription en personne car nous pensons que c'est la seule façon de garantir le plus haut niveau de sécurité requis pour des cas d'usage tels que le vote en ligne. »



Andrea Spallacci, Chef de Projet, Agenzia per l'Italia Digitale (AgID)

« SPID a été le premier programme notifié en Europe à disposer d'un processus d'inscription à distance. Notre point de vue était différent de celui d'autres États membres. eIDAS exigeait initialement la présence physique du citoyen lors de l'inscription/l'enregistrement. Nous croyons fermement que la présence physique est garantie même si elle se fait par le biais d'un dispositif, car la présence physique ne signifie pas la possibilité de toucher le demandeur. »

Jana Krimpe, Représentante du consortium Public/Privé d'Azerbaïdjan

« Pendant la crise COVID, nous avons augmenté le nombre de lieux d'inscription physique - les banques peuvent maintenant émettre des identités mobiles - afin que les gens puissent obtenir leur carte SIM et certificats au même endroit. Nous avons repensé l'ensemble du processus et l'avons simplifié, grâce à une convention d'une seule page, évitant les lourdeurs administratives d'une autre époque. Bientôt, nous mettrons en place le processus complet d'inscription en ligne à distance. »

Aziz Aliyu, Chef de la Commission de Management de l'Identité Nationale (NIMC), Nigéria

« Nous espérons que plus de 90 % de la population sera inscrite d'ici 2023. Pour atteindre cet objectif ambitieux, nous avons élaboré un cadre juridique autour du processus d'inscription en 2017, avec plusieurs recommandations qui permettront à de nombreuses entreprises privées d'être certifiées et devenir des centres d'inscription, et toucher l'ensemble de la population ».

CAS D'USAGE #1

ALICEM, UNE INSCRIPTION SÉCURISÉE BASÉE SUR LA RECONNAISSANCE FACIALE

En 2019, le gouvernement français a lancé la phase de test de l'application Alicem, une nouvelle méthode d'authentification pour FranceConnect, le programme Français d'identité numérique.

Le test Alicem a permis d'expérimenter une technologie de reconnaissance faciale basée sur un dispositif pour faciliter l'inscription. Les utilisateurs pouvaient utiliser le NFC (« Near-field Communication ») de leur téléphone portable pour lire leur passeport biométrique ou un permis de séjour. Alicem compare l'image stockée dans la puce avec une vidéo «challenge», filmée par l'utilisateur. La vidéo est immédiatement supprimée après le processus et la comparaison est effectuée sur l'appareil de l'utilisateur. Aucune donnée personnelle n'est envoyée sur Internet.

Une fois l'inscription terminée, Alicem fournira un accès simple et sécurisé à l'écosystème FranceConnect, via un téléphone portable et ses codes de sécurité associés pour s'authentifier. Pour certains cas d'usage sensibles, une lecture NFC du passeport biométrique pourrait également être requise. En 2021, la nouvelle application mobile pourra également s'appuyer sur la lecture NFC de la nouvelle carte nationale d'identité électronique (CNIe) pour l'authentification.

CAS D'USAGE #2

L'ITALIE INSTAURE UN PROCESSUS UNIQUE D'INSCRIPTION VIDÉO & AUDIO A DISTANCE

SPID a été le premier système notifié eIDAS à disposer d'un processus audio et vidéo à distance pour l'inscription des citoyens (par opposition à une présence physique) avec une validation en direct par un opérateur qui prend environ 20 minutes. Les taux de satisfaction de cette procédure sont extrêmement élevés, avec une forte augmentation des demandes de procédures d'authentification lors de l'épidémie de COVID-19.

Une mise à jour est en cours de conception, améliorant le temps et le processus d'inscription (10 secondes pour l'enregistrement audio et vidéo sans opérateur en direct). Les citoyens effectueront des actions aléatoires demandées par l'application et l'opérateur décidera plus tard de valider ou non l'inscription.

CAS D'USAGE #3

LES MULTIPLES CANAUX D'INSCRIPTION ENTRAÎNENT UN BOND DANS L'ADOPTION AU PORTUGAL

L'inscription à la Clé Numérique Mobile (CMD) lancée en 2014 par le gouvernement portugais a fait un bond impressionnant en 2018 lorsque l'Agence de Modernisation Administrative du Portugal (AMA) décide de créer des canaux d'inscription multiples. En plus du traditionnel face à face ou de la Carte de Citoyen électronique avec lecteur de carte à puce (obligatoire depuis 2007 pour tous les citoyens portugais), deux nouveaux canaux sont désormais disponibles :

> Inscription à la CMD lors du renouvellement de la Carte de Citoyen

> Inscription à la CMD lors de l'utilisation du mot de passe lié au service des impôts. Les codes sont envoyés au citoyen par courrier physique à l'adresse enregistrée.

> L'AMA envisage une future inscription à la CMD via les distributeurs automatiques de billets ou en utilisant la biométrie sur applications mobiles.

« Ces deux dernières années, nous avons changé de niveau, en passant de 1 000 inscriptions par mois à 4 000 par jour. Notre investissement dans la communication a fait peu de différence. Il est clair que la plus grande différence que nous avons remarquée est le passage aux trois nouveaux canaux d'inscription ».

Andre Vasconcelos, Conseiller eID du Comité de Direction, Agence pour la Réforme des Services Publics, Portugal

LE PROCESSUS D'INSCRIPTION, UN ÉLÉMENT CLÉ DE L'ADOPTION DU SYSTÈME D'IDENTIFICATION NUMÉRIQUE

1 **Appuyez-vous sur l'écosystème public et privé existant (administration publique, banques, opérateurs mobiles, etc.) et proposez une certification permettant d'augmenter le nombre de centres d'inscription et d'enregistrer une grande partie de la population. Si ce système est correctement organisé et réglementé par un cadre juridique et des directives techniques obligatoires claires, il peut augmenter considérablement l'efficacité de la procédure d'inscription et réduire ses coûts.**

2 **Pensez à une procédure de préinscription et/ou d'inscription en ligne simple et rapide, utilisant l'audio et la vidéo, pour accélérer l'ensemble du processus et offrir une meilleure expérience utilisateur. Gardez en tête que certains cas d'usage sensibles, comme le vote électronique, peuvent nécessiter un niveau d'assurance plus élevé.**

OBSERVATION #13

CONCEVOIR UNE CAMPAGNE PERSONNALISÉE AUX PARTIES PRENANTES AFIN DE STIMULER L'ADOPTION

Le taux d'adoption est l'indicateur clé le plus suivi, **révélant l'accessibilité, l'inclusion et le succès** - ou l'absence des succès - d'une identité numérique dans un pays. Bien sûr, l'adoption peut être nuancée par d'autres indicateurs, tels que les utilisateurs actifs, le nombre de transactions, la satisfaction client, etc.

Les facteurs favorisant l'adoption sont très différents selon les pays : certains ont rendu leur identité numérique obligatoire, atteignant un taux d'adoption proche de 100 %, tandis que d'autres sont confrontés à des défis supplémentaires, notamment quand posséder une forme d'identification nationale ne fait pas partie de la culture du pays, ou quand les bases de données nationales ne sont pas encore consolidées.

L'adoption entre en jeu bien avant le déploiement et la mise sur le marché de l'identité numérique. La conception de l'interface et de l'expérience utilisateur, le choix des titres d'identité, la pertinence des cas d'usage , la simplicité du processus d'enregistrement et d'authentification - **tous ces choix auront un impact sur le niveau d'adoption et doivent être analysés en profondeur au préalable.** Une fois l'identité numérique conçue et prête à être déployée, les stratégies de mise sur le marché réussies définissent différents groupes cibles de consommateurs et d'acteurs clés, et adaptent la stratégie de communication et d'adoption en conséquence.

«Les initiatives marketing pour l'identité numérique, par des spots télévisés et dans les journaux, créent une adoption continue mais aucun impact mesurable».

Herbert Leitold, Secrétaire Général, Centre de technologie de l'Information, Autriche

CE QU'ILS PENSENT DES STRATÉGIES DE COMMUNICATION ET D'ADOPTION

Margus Arm, Député Directeur Général, Autorité du système d'informations Estonien, Directeur Branche système d'information de l'Etat

« Près de 70% de la population utilise la carte d'identité électronique et je pense que c'est le maximum que nous pouvons atteindre. Il y aura toujours des gens qui n'y auront pas accès et qui ne voudront pas l'utiliser. Il est impossible d'atteindre 100 % ».

Sarah Kirk-Douglas, Vice-Présidente, Marketing & Communications Mondiales, SecureKey Technologies Inc. (Candada)

« Nous avons créé une équipe marketing avec les sept institutions financières qui ont développé Verified.Me avec nous. En travaillant avec les marques de confiance faisant partie du réseau, nous avons pu mettre en place des campagnes de marketing ciblées pour éduquer, sensibiliser et faire adopter le produit par les consommateurs. L'approche a inclu plusieurs phases intégrant des participants différents et via différentes tactiques (événements, relations publiques, réseaux sociaux, vidéos, publicité, etc.) »

Andre Boysen, Directeur d'Identité, SecureKey Technologies Inc.

« La stratégie de mise sur le marché de Verified.Me se base sur le modèle à succès des cartes de crédit, avec un côté émetteur (banques, gouvernement, opérateurs mobiles, etc.) et un côté acquéreur (les parties utilisatrices). Nous avons travaillé ensemble pour permettre aux partenaires d'ajouter de nouveaux services et de rejoindre le réseau. Cela nous a permis de nous développer plus rapidement, et de créer maintenant des relations commerciales grâce auxquelles les partenaires signent des accords avec des parties utilisatrices pour nous ».

Lionel Fouillen, Responsable des Relations Partenaires, FranceConnect

« Il y a un véritable travail à accompagner le grand public dans sa compréhension des concepts de RGPD, fournisseur d'identité, transit de données, sécurité, protection des données, etc. »

CAS D'USAGE #1

COMPTER SUR LES PROVINCES POUR BOOSTER L'ADOPTION AUX PAYS-BAS

Aux Pays-Bas, le service d'authentification DigID permet aux citoyens de se connecter en toute sécurité au portail de services publics.

Pour garantir l'adoption, le gouvernement néerlandais a commencé par une approche progressive en limitant le nombre de fournisseurs de services et en attendant un nombre critique d'utilisateurs actifs avant d'ouvrir le programme à un plus large éventail de services publics.

En outre, un programme de partenariat entre le Ministère des Affaires Intérieures et des Relations au sein du Royaume, l'Association des Municipalités Néerlandaises, les associations professionnelles et les organisations de lobbying a été mis en place pour toucher les citoyens des différentes provinces et stimuler l'adoption. Pour aider les citoyens à utiliser la DigID, des cours en ligne et en face à face (4 sessions de 2 heures chacune) sont dispensés par des enseignants spécialement formés, dans les bibliothèques de chaque province afin de faciliter l'accès pour tous au niveau local.

CAS D'USAGE #2

DES PÉTITIONS POPULAIRES POUR FAVORISER L'ADOPTION EN AUTRICHE

Le premier programme d'identité numérique a été lancé en 2003, avec trois grandes étapes pour son adoption :

> Les portails de services publics en ligne ont introduit un processus d'inscription facile d'utilisation
> Une stratégie du numérique par défaut pour accéder aux dossiers de retraite et de sécurité sociale. Le gouvernement a envoyé une lettre aux ménages autrichiens et a invité les citoyens à créer une identification électronique pour accéder à leurs dossiers de retraite en ligne, même si l'alternative hors ligne était toujours active.
> utiliser leur identification électronique pour signer des pétitions populaires (interdiction du tabac, ou augmentation des droits des femmes). L'inscription est passée de 2 000 à 10 000 par jour.

CAS D'USAGE #3

UNE STRATÉGIE DE MISE SUR LE MARCHÉ BILATERALE À SINGAPOUR

Pour favoriser l'adoption de la NDI, l'Identité Numérique Nationale, l'Agence Gouvernementale pour la Technologie de Singapour GovTech doit envisager une stratégie d'adoption bilatérale :

> la stratégie d'adoption par les citoyens a dû être aussi inclusive que possible pour favoriser l'adoption, et être menée en collaboration avec de multiples agences et médias tout en organisant des présentations destinées à accroître les compétences numériques des personnes âgées et des familles à faibles revenus.

> la stratégie d'adoption par les entreprises consiste d'abord à rendre l'inscription aussi simple et facile à développer que possible, mais aussi à présenter les cas d'usage à succès afin de démontrer la valeur et le potentiel du programme à d'autres entreprises.

LES STRATÉGIES D'ADOPTION ET DE COMMUNICATION À METTRE EN PLACE :

1. **Déployez progressivement l'identité numérique en commençant par un groupe cible prioritaire (citoyens, grandes entreprises, petites et moyennes entreprises, fonctionnaires, etc.), montrez les résultats positifs et poursuivez le déploiement.**
2. **Ciblez les stratégies et la campagne en fonction des acteurs clés - pas seulement les cibles de consommateurs mais aussi les industries clés et principaux acteurs politiques, juridiques et de conformité**
3. **Introduisez des stratégies du «numérique par défaut» dans les services populaires (pétitions, retraites, impôts, etc.) une fois que les services en ligne sont opérationnels.**
4. **Choisissez avec soin les éléments et angles de communication : un axe sécurité et protection des données n'est peut-être pas le plus efficace, communiquez plutôt sur l'utilité et les avantages pour l'utilisateur.**

PROGRAMMES D'IDENTITÉ NUMÉRIQUE DES PAYS INTERROGÉS

PAYS-BAS - DigID

87%

en action depuis 2003 - Programme centralisé dirigé par le gouvernement
Les citoyens et résidents peuvent s'identifier facilement et en toute sécurité en utilisant l'application DigID pour accéder aux services publics en ligne tels que les établissements d'enseignement secondaire, de soins de santé ou de retraite. DigID fait partie d'un programme d'identité numérique plus large, un écosystème de marché ouvert, où le gouvernement agit comme une source d'information fiable faisant autorité.

BELGIUM - itsme®

20%

en action depuis 2017 - Programme fédéré interprofessionnel
La solution d'identité mobile itsme® est détenue et financée par le consortium privé «Belgium Mobile ID», qui regroupe 4 banques et 3 opérateurs de téléphonie mobile, offrant un accès sécurisé à leurs propres services. En 2018, le gouvernement Belge a certifié Itsme et l'a rendu interopérable avec le programme d'identité régalienne nationale, basé sur la Carte d'identité électronique. Itsme donne désormais accès à plus de 700 services électroniques publics et privés.

UNITED KINGDOM - Gov.UK Verify

en action depuis 2017 - Programme fédéré dirigé par le gouvernement
Initialement lancé par le gouvernement britannique, Gov.UK Verify permet aux citoyens et aux résidents de s'authentifier auprès du fournisseur d'identité de leur choix lorsqu'ils se connectent à des services en ligne. Le contrat initial du gouvernement ne permettait pas au secteur privé de l'utiliser, et l'adoption était très lente. Un nouveau système d'identité numérique britannique est en cours de définition, dans lequel les sources de données gouvernementales peuvent être utilisées pour vérifier les détails de l'identité.

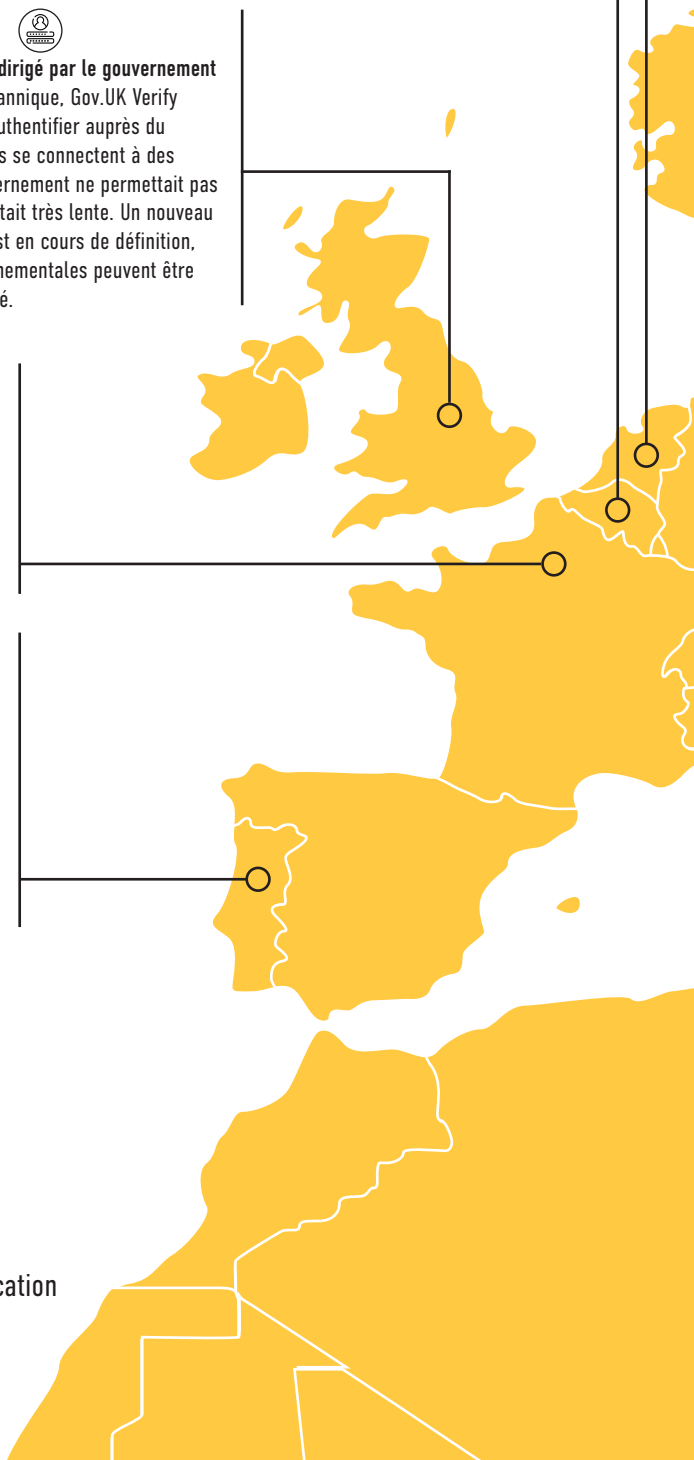
FRANCE - FranceConnect

en action depuis 2016 - Programme fédéré dirigé par le gouvernement
Lancé par le gouvernement, FranceConnect est un fédérateur d'identité numérique qui maintient et réglemente un écosystème pour les utilisateurs, les fournisseurs d'identité et les prestataires de services. Les utilisateurs peuvent choisir leur fournisseur d'identité lorsqu'ils accèdent à l'un des 800 services publics et privés disponibles.

PORTUGAL - Chave Móvel Digital

14,5%

en action depuis 2014 - Programme centralisé dirigé par le gouvernement
Sept ans après le lancement de sa carte d'identité électronique, le gouvernement portugais a lancé la clé mobile numérique ou «Chave Móvel Digital» (CMD), un programme d'identité mobile centré sur l'utilisateur, qui offre simplicité et commodité aux citoyens et aux résidents. Il permet une authentification sécurisée sur divers sites web publics et privés, ne nécessitant qu'un téléphone portable, un code PIN à 4 chiffres et un OTP ou une reconnaissance biométrique.



LÉGENDE

- carte à puce
- numéro / nom d'utilisateur / mot de passe
- identité mobile via carte SIM
- identité mobile via téléphone portable ou application

DANEMARK - NemID et MitID

100%

en action depuis 2010 - Programme centralisé dirigé par le gouvernement et les banques
NemID a été lancé par une coopération entre le secteur financier et le gouvernement Danois. Le programme propose une carte nationale d'identité électronique gratuite pour tous les citoyens, ainsi qu'un accès aux services en ligne via de multiples méthodes d'authentification telles qu'une application mobile et différents types de jetons physiques. En 2021, la troisième génération d'identification numérique «MitID» sera disponible.

ESTONIE - e-identity

98%

en action depuis 2002 - Programme centralisé dirigé par le Gouvernement
Lancé grâce à la participation du secteur privé, le programme e-Estonia propose aux citoyens et entreprises de multiples titres d'identité moyens d'authentification : classique carte nationale d'identité à puce, identité mobile via carte SIM et PKI ou application Smart-ID. En 2020, 99 % des service publics sont en ligne, y compris le vote électronique.

LETTONIE - eParaksts

40%

en action depuis 2018 - Programme centralisé dirigé par le gouvernement
En plus de la carte d'identité électronique délivrée par le gouvernement (obligatoire d'ici 2023), le Centre National de Radio et de Télévision de Lettonie (LVRTC), fournisseur national de services de confiance, a lancé les solutions eParaksts («e-signature» en letton) : une application mobile et différentes cartes à puce, entièrement financées par le gouvernement, qui permettent aux utilisateurs de procéder à une authentification sécurisée et à la signature électronique qualifiée à partir d'un téléphone portable, éliminant ainsi la nécessité d'une connectivité physique par carte à puce.

AUTRICHE - Carte de Citoyen & ID Mobile

17%

en action depuis 2003 - Programme centralisé dirigé par le gouvernement
Pionnier européen, le programme d'identité numérique autrichien financé par le gouvernement est basé sur une Carte de Citoyen virtuelle (CC) qui peut être installée sur plusieurs appareils selon une approche technologique neutre (cartes à puce ou téléphones portable) et donne accès à plus de 300 services publics en ligne ainsi qu'à des services privés (banques, chambre de commerce ou opérateurs mobiles).

ITALIE - SPID

17%

en action depuis 2016 - Programme fédéré dirigé par le gouvernement
Le SPID, Système Public Italien d'Identité Numérique, est géré par l'»Agenzia per l'Italia Digitale» (AgID) et financé par des fournisseurs d'identité privés accrédités. Le SPID fournit une identité numérique sans dispositif à tous les citoyens italiens et aux entreprises, afin de leur permettre d'accéder facilement et gratuitement aux services électroniques privés et publics.

LIECHTENSTEIN - EID.LI

en action depuis 2020 - Programme centralisé dirigé par le gouvernement
Avec moins de 40 000 habitants, le Liechtenstein a développé un système d'identité numérique basé sur sa Carte Nationale d'Identité Electronique. En avril 2020, le gouvernement a lancé l'identité mobile eID.li. Comme la carte à puce, la nouvelle application permet aux citoyens et aux résidents de s'identifier et de se connecter en toute sécurité à près de 200 services publics en ligne.

AZERBAÏDJAN - ASAN IMZA

en action depuis 2014 - Programme centralisé dirigé par le gouvernement
L'identité mobile Asan Imza, qui s'appuie sur une carte SIM et PKI, est financée et exploitée par un partenariat public-privé entre le gouvernement, les opérateurs mobiles et un fournisseur de solutions privé. Elle est utilisée par les citoyens, les entreprises et les fonctionnaires pour l'authentification en ligne (plus de 1000 services électroniques sont actuellement disponibles) et la signature électronique.

OMAN - OMANUMA

100%

en action depuis 2014 - Programme centralisé dirigé par le gouvernement
Le gouvernement Omanais a entièrement financé le programme d'identité numérique Omanuna. Les citoyens, résidents et entreprises d'Oman peuvent accéder en ligne à plus de 36 fournisseurs de services publics et privés, en utilisant soit leur Carte Nationale d'Identité/de Résidence électronique, soit leur application d'identité mobile pour s'authentifier et signer des documents en ligne.

LÉGENDE

- carte à puce
- numéro / nom d'utilisateur / mot de passe
- identité mobile via carte SIM
- identité mobile via téléphone portable ou application

INDE - AADHAAR

98%

en action depuis 2009 - Programme centralisé dirigé par le gouvernement
Aadhaar est un programme d'identité numérique sans titre d'identité physique, ce qui en fait le plus grand programme d'État basé sur la biométrie au monde. Les citoyens et les résidents peuvent accéder à un large éventail de services en face à face et en ligne, comme les programmes alimentaires subventionnés dans des lieux physiques proposés par le gouvernement. Aadhaar s'est avéré favoriser l'inclusion et accroître la transparence, entre autres avantages.

SINGAPOUR NATIONAL DIGITAL IDENTITY (NDI)

98% pour SingPass
50% pour IDMobile

en action depuis 2003 - Programme centralisé dirigé par le gouvernement
À Singapour, le gouvernement a étendu le service SingPass, plateforme d'accès aux services publics. Elle fait partie d'un programme national d'identité numérique (NDI) qui vise à fournir une identité numérique unique aux utilisateurs et aux entreprises d'ici 2021. SingPass Mobile et CorpPass, disponibles depuis 2018, permettent aux utilisateurs et aux entreprises de s'authentifier en ligne pour accéder à des services publics et privés ainsi qu'à un large éventail d'autres cas d'usage , tels que le partage d'attributs en face à face ou pour remplir des formulaires via la plateforme de données MyInfo.

QUEENSLAND, AUSTRALIE - APPLICATION PERMIS DE CONDUIRE NUMÉRIQUE

en action depuis 2020 - Programme centralisé dirigé par le gouvernement
En 2020, le Ministère des Transports et des Routes Principales du Queensland a financé une application de permis numérique, actuellement en phase pilote. Elle sert de portefeuille d'identité numérique, stockant sur une seule plateforme sécurisé un large éventail de documents numériques et d'immatriculations de véhicules et d'embarcations, afin de permettre aux citoyens d'avoir le contrôle de leurs titres d'identité, permis et biens enregistrés, et de leur donner accès à toute une gamme de services publics en lignes et options de paiement.

CANADA - Réseau d'identité Verified.Me

15M

en action depuis 2012/2019

Programme fédéré intersectoriel dirigé par le gouvernement

Lancé en 2012, Government Sign-in par Verified.Me, anciennement appelé Concierge, est un système fédéré d'authentification unique (ou Single Sign On) qui relie les fournisseurs de services publics à des partenaires de connexion tels que les banques, qui fournissent des titres d'identité appuyant l'authentification. Cette solution a été adoptée par plus de 18 millions de Canadiens en 2020. Secure Key Technologies Inc, la société qui a conçu le Government Sign-in par Verified.Me, a lancé en 2019 un nouveau produit Verified.Me pour le secteur privé, basé sur la technologie des Blockchains.

ARIZONA, USA - MVD SOLUTIONS

en action depuis 2018/2020

Programme centralisé dirigé par le gouvernement

Dans un pays où le permis de conduire est la preuve d'identité la plus courante, le Ministère des Transports de l'Arizona (ADOT) a mis en ligne un large éventail de services publics gratuits grâce à une authentification renforcée sur son site web. Une nouvelle version d'application de permis de conduire numérique devrait être lancée en 2021, et un nouveau super-portail permettra à d'autres agences gouvernementales d'utiliser les capacités d'authentification de l'ADOT.

COLOMBIE - Nouvelle Carte d'Identité électronique et Identité Mobile

en action depuis 2020

Programme centralisé dirigé par le gouvernement

Dans le cadre des politiques du gouvernement sur le numériques définies en 2017, la nouvelle carte d'identité électronique a été lancée en novembre 2020. D'autres services d'identité numérique sont en cours de développement, tels qu'une application d'identité mobile liée à la carte d'identité électronique, un dossier en ligne où chaque citoyen peut stocker ses documents administratifs, et une plateforme de services publics. À long terme, l'ambition du gouvernement est de lutter contre la fraude électorale et l'abstention en proposant le vote électronique.

LÉGENDE

- carte à puce
- numéro / nom d'utilisateur / mot de passe
- identité mobile via carte SIM
- identité mobile via téléphone portable ou application

NIGÉRIA - NIN et Application d'Identité Mobile

en action depuis 2007 -
Programme centralisé dirigé par le gouvernement

Afin de créer une base solide pour un futur système d'identité numérique, le Gouvernement Fédéral a mis en place la Commission Nationale de Gestion de l'Identité [NIMC] pour saisir les données dans une base de données centrale, sécurisée et harmonisée et fournir un numéro national d'identité (NIN) à tous les citoyens. Ceux-ci peuvent utiliser leur carte à puce pour s'authentifier, procéder à des signatures électroniques, paiements, virements ou pour retirer de l'argent aux distributeurs automatiques de billets. Le taux de pénétration est très faible (moins d'1 million de cartes ont été émises). Un nouvel écosystème d'identité mobile est en cours de lancement.

BRÉSIL - Application de portefeuille numérique CPF

en action depuis 2020
Programme centralisé dirigé par le gouvernement

Après avoir mis en place le cadre juridique de son programme national d'identité numérique en 2017, le Brésil a deux objectifs principaux : centraliser toutes les données biométriques des citoyens dans une base de données, et finaliser la mise en œuvre de son identité mobile d'ici 2020. L'application «CPF ID Wallet» permettra de stocker des titres d'identité (permis de conduire, etc.) et sera dans un premier temps réservée aux prestataires de services publics. Le gouvernement augmentera progressivement les cas d'utilisation et créera un portail en ligne unique.

APPLICATION DE PERMIS DE CONDUIRE NUMÉRIQUE

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

APP MOBILE (PORTEFEUILLE) *incluant permis de conduire, cartes d'identification avec photo et permis bateau de plaisance*

PHASE PILOTE, LANCEMENT PRÉVU EN **2021**

IDENTIFICATION *en ligne & hors ligne*

PARTAGE D'ATTRIBUTS D'IDENTITÉ

> Identification en face à face pour les vérifications d'identité dans le commerce, se faisant d'un dispositif à un autre via code QR et partage de données par Bluetooth à basse consommation (chez le pharmacien, revendeurs d'alcool, voitures de location, etc.) en mode non-connecté (localement de téléphone à téléphone) et en mode connecté (avec une vérification sur le serveur).
> Preuve d'âge
> Code QR inversé pour un accès sécurisé par téléphone / skype (phase POC)

AUTHENTIFICATION

L'authentification en ligne des utilisateurs pour l'accès aux services publics et privés est prévue dans un second temps

SIGNATURE ÉLECTRONIQUE

L'application propose un PDF à signature électronique qui peut être envoyé par message, e-mail ou Airdrop.

RECONNAISSANCE TRANSFRONTALIÈRE

Basé sur les normes ISO 18013-5 pour l'interopérabilité et l'utilisation transfrontalière.

CONTEXTE & OBJECTIFS

Le Ministère des Transports et des Routes Principales du Queensland a lancé une nouvelle Application de Permis Numérique actuellement à l'essai dans la région de la côte Fraser avant son lancement en 2021.

L'objectif principal était d'abord de moderniser le système de permis de conduire du Queensland en ajoutant un compagnon mobile à la carte pour faire face à la fraude et à la perte de documents physiques. Plus qu'une preuve du droit de conduire, le permis est également un élément clé d'identification, largement utilisé par le secteur privé. Le projet a également été motivé par l'ambition de proposer une identité numérique fiable aux habitants du Queensland afin de préserver la dignité des personnes, de leur permettre d'accéder aux services essentiels de la vie quotidienne et bien plus encore.

PROPOSITION DE VALEUR

L'Application de Permis Numérique du Queensland est une application mobile qui sert également de portefeuille d'identité numérique stockant un large éventail de documents numériques, d'immatriculation de véhicules et d'embarcations dans une seule plateforme sécurisé. Elle est destinée à donner à tout citoyen du Queensland, quelle que soit son origine ou sa communauté, le contrôle de ses titres d'identité, permis et biens enregistrés, et à lui donner accès à toute une série de services publics en ligne et options de paiement.

AUTRES SERVICES SPÉCIFIQUES ET CAS D'USAGE :
> Confirmer l'éligibilité à l'aide en cas de catastrophe naturelle (feux de forêt, inondations) et son paiement
> Respect des normes COVID dans les boîtes de nuit et restaurants
> Des fonctions de paiement sont attendues prochainement (notamment pour les entreprises)
> L'immatriculation sera disponible pour une large gamme de véhicules et d'embarcations

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Le financement gouvernemental est considéré comme le modèle le plus efficace, permettant d'éviter une majoration de 30 % des coûts en cas de sous-traitance par le secteur privé. Cette dernière induirait également des difficultés réglementaires et de protection de la vie privée.
> Seuls les organismes publics peuvent ajouter des titres d'identité et autres informations numérisées à l'application de portefeuille numérique
> Le secteur privé peut être une tierce partie - l'application servirait d'outil de validation pour ses propres services
> Le ROI du projet se mesure en termes de rentabilité et évitement de la fraude, une fois qu'un certain nombre de titres d'identité gouvernementaux sont intégrés à la plate-forme unique

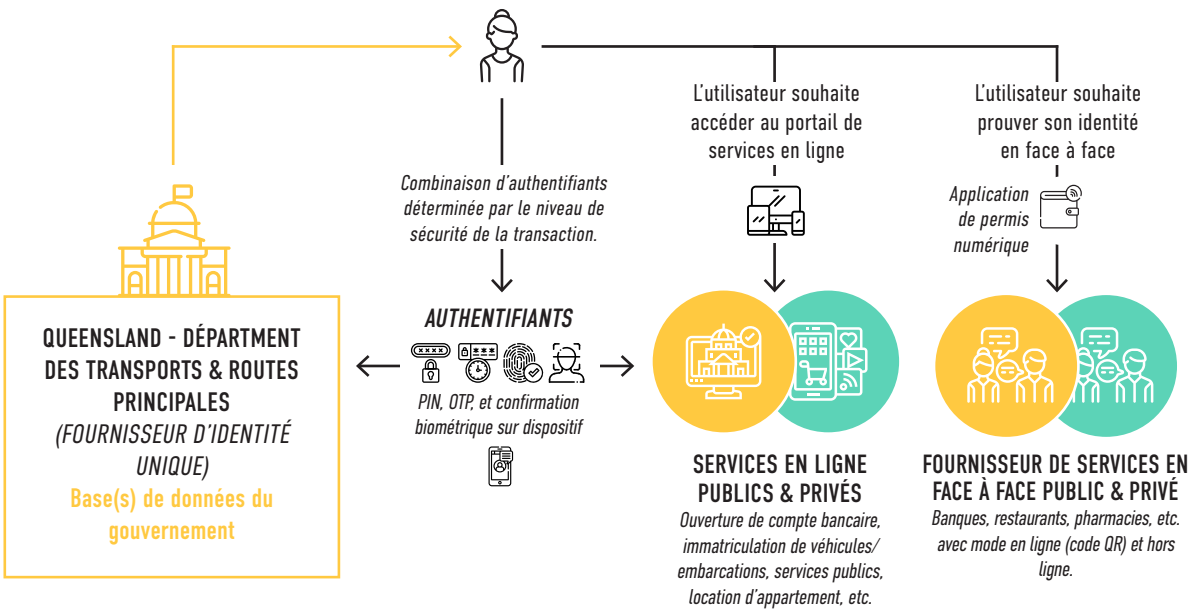
CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> L'application de permis numérique et celle de lecture (Reader App) sont toutes deux conformes à la loi sur la protection de la vie privée et aux dispositions spécifiques de confidentialité de la législation sur les transports.
> Le modèle s'appuie sur le consentement du partage de données
> L'application s'appuie sur des mécanismes de sécurité à plusieurs niveaux et a été testée au moyen d'un Test d'Intrusion (Pentest)

ÉTAPES CLÉS DU PROJET

Nov. 2018	Été 2019	2020	2021
Début du prototype & co-conception	Pré-pilotage avec une grande participation de la communauté, programme ambassadeur numérique, actions sur le terrain, etc.	lancement du pilote Accepté comme forme officielle d'identité	Lancement du portefeuille d'identité numérique du Queensland

APPLICATION DE PERMIS DE CONDUIRE NUMÉRIQUE DU QUEENSLAND - ÉCOSYSTÈME



CADRE JURIDIQUE

> Une évaluation des incidences sur la vie privée (PIA) a été validée de manière indépendante

> La Loi sur les Informations Personnelles oblige les organismes gouvernementaux du Queensland à se conformer aux Principes relatifs aux Informations Personnelles (les IPP). Les IPPs concernent la collecte, le stockage, l'utilisation et la divulgation d'informations personnelles.

AUTRES INITIATIVES D'IDENTITE NUMÉRIQUE DANS LE PAYS

> Initiatives en matière de permis de conduire mobiles en Australie-Méridionale et en Nouvelle-Galles du Sud

> La poste australienne a lancé une identité mobile visant à proposer à ses clients des services d'authentification en ligne

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

Un conseil de gouvernance avec 3 groupes de référence (Expérience Client, Architecture, Politique & Législation) dirigé par un groupe de travail interdépartemental, chargé de valider toute nouvelle intégration à l'application.

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

> Portefeuille d'identité numérique unique contenant divers documents d'identité (permis de conduire, cartes d'identification avec photo, permis bateau de plaisance, etc.) et servant de preuve d'identité en ligne et hors ligne, permettant également le partage d'attributs.

> Procédé de co-conception centré sur l'utilisateur intégrant un panel de 120 utilisateurs finaux qui ont influencé le choix des distributeurs.

MISE EN ŒUVRE TECHNOLOGIQUE

Confidentialité des données basée sur le consentement - les citoyens gardent le contrôle sur la divulgation des leurs données et peuvent personnaliser leur choix.

MISE SUR LE MARCHÉ & PROMOTION

> Une approche à 4 parties prenantes pour l'adoption : campagne médiatique classique pour les villes, approche spécifique pour les industries (pharmaciens, buralistes, etc.) et les communautés telles que les soignants, et campagnes spécifiques pour embaucher des chômeurs longue durée et les transformer en ambassadeurs actifs.

> Une stratégie de gamification liée à la jeune génération : le programme Ambassadeur Numérique organise des concours régionaux - les lycéens soumettent des vidéos promotionnelles de l'application célébrant leur région et le permis de conduire numérique.

8,8 MILLION D'HABITANTS
18% TAUX D'ADOPTION

CARTE DE CITOYEN ET IDENTITÉ MOBILE

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

CARTE À PUCE (CARTE D'ASSURANCE MALADIE) + ID MOBILE (SMARTPHONE & INTERNET)

EN ACTION DEPUIS 2003

IDENTIFICATION *en ligne et hors ligne*
Utilise des identifiants spécifiques au secteur et non connectés entre eux.

PARTAGE D'ATTRIBUTS D'IDENTITÉ
Pour les autorités publiques si une base légale existe

AUTHENTIFICATION
Cadre à technologie neutre définissant les exigences minimales en termes de titres d'identité permettant l'authentification en ligne et hors ligne

SIGNATURE ÉLECTRONIQUE

RECONNAISSANCE TRANSFRONTALIÈRE
Pilote des services transfrontaliers pour les entreprises en collaboration avec d'autres pays européens.

300 **SERVICES PUBLICS EN LIGNE**
notamment portail pour les services des impôts, sécurité sociale, assurance maladie, retraites et quelques services privés.

NOTIFICATION EIDAS PREVUE POUR 2021

CONTEXTE & OBJECTIFS

L'Autriche a été l'un des premiers pays européens à mettre en œuvre un système national d'identité basé sur une carte d'identité électronique - fortement porté par un projet de services publics en ligne.

Si l'inscription au Registre Central des Résidents (CRR) est obligatoire pour tous les citoyens et résidents, la carte d'identité physique reste optionnelle. En revanche, l'Autriche dispose d'une Carte de Citoyen virtuelle (CC) qui peut être installée sur plusieurs dispositifs, et s'appuie sur une approche de technologie neutre : cartes à puce ou téléphones portables.
L'objectif principal est de réduire les coûts et efforts du gouvernement, ainsi que de faire gagner du temps et de l'argent aux citoyens et aux entreprises.

PROPOSITION DE VALEUR

La Carte de Citoyen virtuelle donne actuellement accès aux services publics en ligne ainsi qu'à plusieurs services privés (banques, chambre de commerce ou opérateurs de téléphonie mobile).

Elle est accessible à tous les Autrichiens, aux résidents et à certains étrangers tels que les frontaliers et les expatriés.

AUTRES SERVICES SPÉCIFIQUES ET CAS D'USAGE :
> Représentation électronique : le titulaire peut effectuer des opérations juridiques au nom d'une autre personne.
> Des cas d'usage pour les entreprises sont à l'étude : le programme d'identité numérique est relié aux bases de données relatives aux entreprises (comme le portail de Services aux Entreprises) pour les cas comme la signature électronique, le paiement des impôts ou la représentation.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> L'identité mobile est gratuite pour les citoyens et les prestataires de services publics et privés (intégration de la carte d'identité électronique dans le service) afin d'encourager l'adoption et l'utilisation.
> Certains services, comme le portail de service des impôts, sont obligatoires pour les entreprises, mais jamais pour les citoyens.

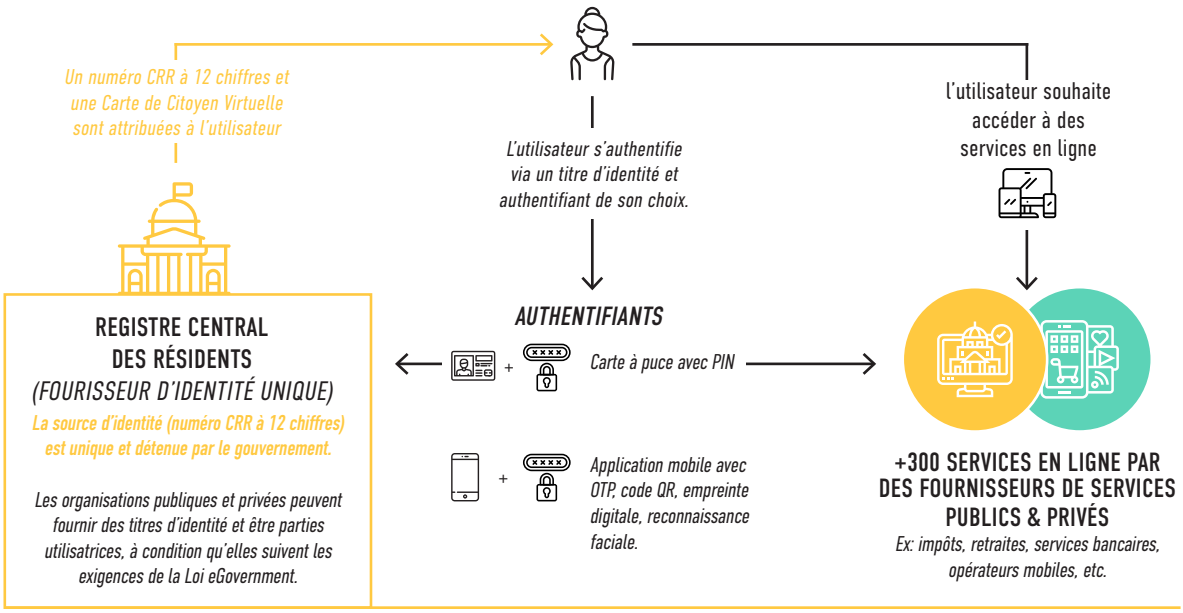
CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Des exigences de sécurité strictes liées au règlement eIDAS pour les signatures électroniques qualifiées
>Des identifiants spécifiques aux secteurs, dérivés du numéro CRR : pour une même personne, chaque secteur gouvernemental ou fournisseur de services privé utilise un identifiant différent, dérivé cryptographiquement du numéro CRR. Cela empêche la mise en correspondance des individus dans leur utilisation des services.
> Le GovCERT autrichien, géré par le département de la Stratégie Fédérale pour les Techniques d'Information et de Communication de la Chancellerie fédérale, s'occupe des failles de sécurité de l'infrastructure.

ÉTAPES CLÉS DU PROJET

2003	2005	2008	2009	June 2021	2021
Lancement du programme d'Identité Numérique	Lancement des cartes à puces & identité mobile	Reconnaissance des identités numériques étrangères	Signature par identité mobile	1,5 Million d'utilisateurs actifs e-ID Mobile	Passage à une stratégie mobile en priorité. Nouvelle interface standard pour intégration de fournisseur de service Objectif notification eIDAS

IDENTITÉ NUMÉRIQUE AUTRICHIENNE - ÉCOSYSTÈME



CADRE JURIDIQUE

> Loi sur la Protection des Données (Datenschutzgesetz, DSG) (2000)
> Loi eGovernment (2004) établissant un cadre général, définissant l'identité mobile, et fixant des exigences de haut niveau : Identité unique, signatures électroniques qualifiées et représentation «au nom de».
> L'Autorité indépendante qui gère le registre source des numéros personnels d'identification (Personal Identification Numbers - PINs) en assure le traitement
> Acceptation unilatérale de l'identité numérique d'autres pays depuis 2008, notification eIDAS prévue pour 2021

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

Une nouvelle approche «zéro empreinte» où les citoyens n'ont besoin que d'un navigateur et d'un smartphone

MISE EN OEUVRE TECHNOLOGIQUE

> Un système d'interopérabilité « by design » pour intégrer d'autres pays si les exigences sont respectées. Des projets pilotes sont en cours avec d'autres pays européens sur la sémantique de la représentation électronique transfrontalière et du mandat électronique (projet SEMPER avec les Pays-Bas, la Slovénie et l'Espagne)
> Des identifiants spécifiques aux secteurs pour la protection de la vie privée et le partage des données quand c'est légitime

MISE SUR LE MARCHÉ & PROMOTION

> Fort taux d'adoption atteint quand les portails ont introduits des procédés d'inscriptions simples à appréhender.
> Une campagne par courrier de la sécurité sociale a annoncé la numérisation par défaut pour l'accès aux dossiers de retraites en 2008/2009
> L'utilisation de la carte d'identité électronique pour signer des pétitions populaires en 2018 (interdiction de fumer, droits des femmes)

ASAN IMZA

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

ID MOBILE (VIA SIM ET PKI) SUR TÉLÉPHONE PORTABLE STANDARD & SMARTPHONE

EN ACTION DEPUIS 2014

- ✓ IDENTIFICATION *en ligne & hors ligne*
- ○ PARTAGE D'ATTRIBUTS D'IDENTITÉ
- ✓ AUTHENTIFICATION
- ✓ SIGNATURE ÉLECTRONIQUE — *Signature électronique à valeur juridique. Possibilité de procéder à une signature électronique sans connexion internet et sur un téléphone portable type feature phone.*
- ✓ RECONNAISSANCE TRANSFRONTALIÈRE — *a ratifié en 2020 la Convention sur l'Harmonisation des Contrôles aux Frontières en Asie et Pacifique, adopté par l'UN ESCAP.*

1000+ services publics et financiers en ligne

CONTEXTE & OBJECTIFS

Depuis 2003, l'Azerbaïdjan accorde une grande importance au développement de son secteur des TIC. La maturité numérique du pays est très élevée pour les entreprises (environ 100 %), mais beaucoup plus faible pour les citoyens, bien que la crise COVID ait augmenté la pénétration du marché - notamment grâce à l'utilisation des services financiers en ligne.

En créant une identité numérique, le gouvernement souhaitait en premier lieu simplifier l'accès aux services, et rendre les processus plus transparents en résolvant des problèmes profonds de bureaucratie et de corruption. Il espérait également améliorer l'éducation numérique de la population globale en rendant certains services obligatoirement numériques. Aujourd'hui, la plupart des services numérisés concernent les entreprises.

PROPOSITION DE VALEUR

L'identité mobile Asan Imza est une carte SIM connectée à 3 certificats différents (citoyen, entreprise, fonctionnaire), équivalente à une carte d'identité physique dans l'environnement électronique et de même valeur qu'une carte manuscrite. Elle est connectée à un code personnel unique tiré du registre de la population. L'identité mobile peut être utilisée comme forme d'identité électronique sécurisée afin de prouver une identité ou procéder à une signature électronique. Quand cela est possible, les services électroniques sont obligatoires. Pour plus de commodité, l'utilisateur ne dispose que de deux codes PIN quel que soit le certificat utilisé : le PIN1 pour l'authentification et le PIN2 pour la signature.

Après avoir obtenu une carte SIM auprès d'un Opérateur de Réseau Mobile, les citoyens peuvent activer leurs certificats dans un centre des impôts, un centre ASAN ou une banque. Cela peut également se faire à distance (depuis 2020 en raison de l'épidémie de COVID) via le portail Asan Imza, en utilisant les données biométriques (reconnaissance faciale).

AUTRES SERVICES SPÉCIFIQUES ET CAS D'USAGE :

> 9 services basés sur une solution verbale, actuellement alimentés par un humain, mais l'Intelligence Artificielle est explorée pour l'avenir. Ces services sont populaires dans les zones rurales pour la déclaration d'impôts.

> Les programmes E-Residency et M-Residency fournis par le Digital Trade Hub pour les entrepreneurs locaux et étrangers afin de créer et de gérer, en Azerbaïdjan, une entreprise qui est indépendante d'un lieu d'implantation, grâce à une identité numérique délivrée par le gouvernement.

UN MODÈLE ÉCONOMIQUE BASÉ SUR UN PPP

La technologie et le service sont fournis par un fournisseur de solutions privé, tandis que l'Autorité Fiscale relevant du Ministère de l'Économie assure la mise à disposition des services de confiance (stockage des clés, délivrance et activation des certificats, etc.). Le processus et le coût d'émission de la carte SIM sont décidés par les Opérateur de Réseau Mobile, en fonction de leur réglementation et de leur modèle commercial.

> Les certificats sont gratuits pour les citoyens, les entreprises paient des frais de service (environ 9€ pour un certificat de 3 ans.)
> Les citoyens et les entreprises paient une redevance mensuelle (1€) par carte SIM, quel que soit le nombre de certificats. Les bénéfices sont répartis entre les Opérateur de Réseau Mobile et le fournisseur de solution.
> Pour des raisons d'efficacité du service, les SMS autrefois tous payants sont maintenant illimités pour tous lors des transactions.

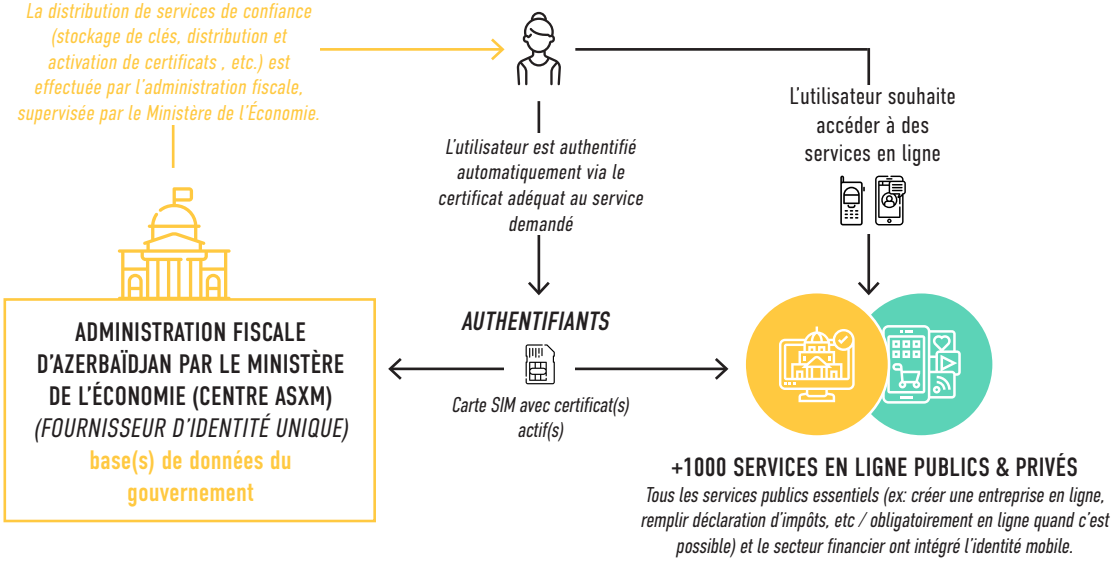
CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> L'Identité Mobile suit les réglementations internationales telles que la RGPD et est conforme à eIDAS grâce à sa solution basée sur la PKI (la clé privée est stockée sur le matériel appartenant au client).
> Suit les normes US NIST et eIDAS High (UE) : actuellement, tous les niveaux d'assurance sont supportés par le système d'identité numérique.

ÉTAPES CLÉS DU PROJET

2014	2016	2017	2018	2019	2020	2021/2022
Lancement d'Asan Imza	Plus de 650 services en ligne et 25 banques connectées	Lancement du Digital Trade Hub d'Azerbaïdjan pour la validation des e-Signatures et e-Services transfrontaliers	1er programme m-Residency au monde. Disponbile dans 79 ambassades dans le monde.	Récompense NIST pour la technologie carte SIM d'Asan Imza. L'OCDE a reconnu Asan comme exemple d'innovation d'excellence.	Plus de 90 millions de transactions enregistrées et plus de 1000 services électroniques disponibles.	Nouvelle génération d'ID Mobile : fonctionne hors ligne avec license Mobile Drivers et passeport, Authentification par blockchain, e-SIM avec cryptographie post-quantique. Reconnaissance bilatérale mutuelle avec l'UE pour les e-signatures.

IDENTITÉ NUMÉRIQUE ASAN IMZA DIGITAL - ÉCOSYSTÈME



CADRE JURIDIQUE

> Des lois fondamentales réglementent l'environnement numérique en Azerbaïdjan : la signature électronique, les documents électroniques et la protection des données.

AUTRES INITIATIVES D'IDENTITE NUMÉRIQUE DANS LE PAYS

> Carte d'identité physique avec signature
> E-signature avec jetons
> Nouveau type de cartes d'identité avec photo stockant la signature électronique

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

Un modèle de partenariat public-privé entre le gouvernement, un fournisseur de solutions privé et les Opérateur de Réseau Mobile a permis de construire l'écosystème en 6 mois (comparé à une procédure traditionnelle gérée par le gouvernement - en moyenne 2 ans). Le système de PPP a donné des résultats clairs, rapides et concrets qui ont convaincu les principaux décideurs et parties prenantes (en particulier le gouvernement).

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

> La solution via carte SIM convient à tous les types de réseaux (2G) et à tout type de téléphone portable, ce qui en fait un choix pertinent pour les marchés en développement.
> L'accès gratuit aux services en ligne pour les citoyens lors de l'épidémie de COVID -19, afin d'atteindre une nombre critique d'utilisateurs et booster l'éducation numérique des citoyens.

MISE EN OEUVRE TECHNOLOGIQUE

Le fournisseur de solution a fait un benchmark des normes et réglementation internationales afin de proposer le meilleur niveau d'assurance. Cette approche a été essentielle pour établir une forte confiance en interne et permettre un développement des transactions transfrontalières ainsi que le commerce en ligne avec d'autres pays.

MISE SUR LE MARCHÉ & PROMOTION

Une collaboration étroite et un partenariat entre le gouvernement et le secteur privé, y compris les banques et les opérateurs de réseau mobile, afin d'accroître l'utilisation et promouvoir Asan Imza auprès des particuliers et des entreprises. Des campagnes publicitaires ou des consultations sur le terrain ont notamment été menées.

+18M UTILISATEURS *pour Governement.Sign-In par Verified.Me*

37.6 MILLION D'HABITANTS

RÉSEAU D'IDENTITÉ VERIFIED.ME

MENÉ PAR :
LE GOUVERNEMENT POUR
Governement Sign-In par Verified.Me
INTERSECTORIEL pour verified.Me

DEPUIS **2012** *pour Government Sign-In par Verified.Me*
2019 *pour Verified.Me*

269 SERVICES DU GOUVERNEMENT FÉDÉRAL *disponibles sur Governement.Sign In par Verified.Me*

PROGRAMME FEDERE

- **IDENTIFICATION** *seulement en ligne*
- **PARTAGE D'ATTRIBUTS D'IDENTITÉ** *Partage d'attributs clair et basé sur le consentement à chaque connexion à un fournisseur d'identité, grâce au réseau Verified.Me sur téléphone portable ou navigateur.*

CONNECTION VIA TITRE D'IDENTITÉ BANCAIRE

- **AUTHENTIFICATION**
- **SIGNATURE ÉLECTRONIQUE** *Vérification accrue de la personne signataire du document*

VALIDATION SUR APPLICATION ET NAVIGATEUR

- **RECONNAISSANCE TRANSFRONTALIÈRE** *Verified.Me est conçu pour être exportable vers d'autres pays et compatible avec d'autres écosystèmes : développé par Test CEM pour le modèle d'identité, en utilisant les normes ouvertes W3C - se voulant technologiquement agnostique - d'après le cadre CCIAN*

CONTEXTE & OBJECTIFS

En 2012, le gouvernement fédéral canadien a lancé un appel d'offres pour développer un service d'authentification permettant aux citoyens canadiens d'accéder aux services publics en ligne. SecureKey Technologies Inc. a développé Government Sign-in par Verified.Me (anciennement Concierge), un service de SSO fédéré qui agit comme un opérateur de réseau de confiance, reliant les fournisseurs de services à un fournisseur de titres d'identité, et qui utilise les titres financiers existants (numéros de carte, noms d'utilisateur et mots de passe) pour authentifier les utilisateurs en ligne.

En 2019, SecureKey Technologies Inc. a lancé Verified.Me pour le secteur privé en collaboration avec un consortium de sept des principales institutions financières du Canada.

PROPOSITION DE VALEUR

Verified.Me simplifie les processus de vérification d'identité en permettant aux utilisateurs de partager leur identité et d'attribuer des informations provenant de sources fiables (institutions financières, opérateurs de téléphonie mobile, bureau de crédit ou gouvernement) aux services auxquels ils souhaitent accéder.

Pour s'inscrire, les utilisateurs doivent connecter un compte existant et actif d'au moins une des institutions financières participantes sur la plateforme Verified.Me (web et mobile). Au Canada, entre 85 et 90 % des adultes possèdent un tel compte.

Aujourd'hui, des dizaines de services du gouvernement canadien, mais aussi des services des secteurs de la finance, de la santé ou des télécommunications, sont intégrés à l'écosystème.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE SECTEUR PRIVÉ

> Initialement financé par les membres du consortium.
> Gratuit pour les utilisateurs finaux
> Modèle de paiement à l'usage pour les prestataires de services.

> Une importante économie d'argent pour les prestataires de services et leur processus d'inscription[1] avec une réduction de 50%.
> De 2012 à 2018, Government Sign-in par Verified.Me a permis de baisser les coûts d'authentification du gouvernement à 200 millions de dollars (par rapport aux 970 millions de dollars dépensés de 2004 à 2012)[2].

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

La protection des données est au cœur de la conception de Verified.Me. Le service adopte l'approche «privacy by design» et vise à dépasser les exigences en matière de protection des données.

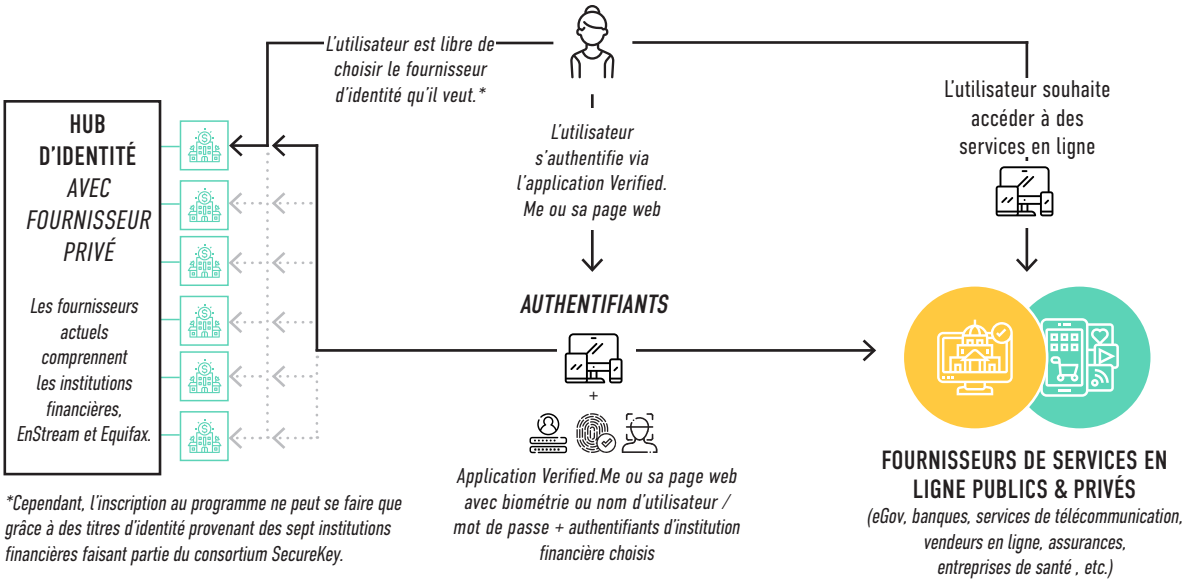
> Dans le système, aucun attribut d'information explicite n'est collecté ou partagé par Verified.Me entre les fournisseurs d'identités ou de services : les titres d'identité (contenant les attributs) sont cryptés de bout en bout avec des clés cryptographiques générées dynamiquement, qui sont communiquées indépendamment à la transmission des titres. La Blockchain est également un facteur clé pour assurer la confiance, la protection des données et la sécurité.
> L'architecture garantit que les sujets ont un contrôle total sur les titres d'identité partagés tout en maintenant le principe du Triple Blind®, ce qui signifie qu'aucun des participants au réseau, y compris l'opérateur, ne peut avoir une vue complète des transactions des utilisateurs.

ÉTAPES CLÉS DU PROJET

2012	2014	2019	2020
Lancement de Concierge	+1M transactions par mois	Lancement de Verified.Me	Enorme augmentation de 100 à 800 transactions par seconde durant la pandémie : 18 millions d'utilisateurs sur Government Sign-In par Verified.Me

1. How to Make Digital Identity a Success: Insights and Learnings from Seven Digital ID Schemes, Groupe d'Experts en identité numérique de Mobey Forum, 2020
2. Andre Boysen, SecureKey Technologies Inc. Directeur d'Identité, 2020

IDENTITÉ NUMÉRIQUE VERIFIED.ME -ÉCOSYSTÈME



*Cependant, l'inscription au programme ne peut se faire que grâce à des titres d'identité provenant des sept institutions financières faisant partie du consortium SecureKey.

CADRE JURIDIQUE

> Autorité indépendante de protection des données : Commissariat de Protection de la Vie Privée du Canada ...
> Plusieurs lois provinciales et sectorielles sur la protection de la vie privée, ainsi que plusieurs règlements fédéraux : la Loi sur la Protection des Renseignements Personnels (1983), La Loi sur la Protection des Renseignements Personnels et Documents Électroniques (2000) pour le secteur privé, modifiée par la Loi sur la Protection des Renseignements Personnels Numériques (2015).
> Le Conseil d'Identification et d'Authentification Numériques du Canada (DIACC ou CCIAN) a élaboré le Cadre de Confiance Pancanadien avec des intervenants des secteurs public et privé. L'objectif de ce cadre est de cartographier et d'identifier les points d'intersection entre les technologies et les politiques juridiques. Il se veut agnostique et sera applicable à tout modèle (fédération, hub d'utilisateurs, etc.).

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

Une approche de consortium public et privé avec un écosystème basé sur le consentement distribué et une responsabilité structurée et documentée.

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

MISE EN OEUVRE TECHNOLOGIQUE

Utilisation du blockain pour Verified.Me pour mettre en œuvre le protocole Triple Blind. Le réseau de confiance Verified.Me et le hachage crypté garantissent que les données proviennent d'une source fiable, qu'elles n'ont pas été altérées et que les données sont présentées par la personne à laquelle elles appartiennent.

MISE SUR LE MARCHÉ & PROMOTION

Une stratégie d'adoption inspirée du modèle des cartes de crédit, en séparant le côté émetteur du côté acquéreur. D'une part, il s'agit de créer des partenariats avec les banques qui émettent des cartes de crédit et, d'autre part, d'inscrire des partenaires qui les acceptent en créant une acceptation universelle. Verified.Me est construit sur le même exemple. Du côté de l'émission, Verified.Me s'appuie sur les bureaux de postes, banques, des agences de crédit (credit scoring), le gouvernement et les opérateurs de télécommunications. Côté acquéreur (côté commerçant), l'effort commun permet aux partenaires d'inscrire de nouveaux services. Cette stratégie a permis d'accélérer l'expansion en établissant des relations commerciales dans lesquelles des partenaires peuvent inscrire des parties utilisatrices pour Verified.Me.

49,65 MILLIONS D'HABITANTS

NOUVELLE CARTE D'IDENTITÉ ÉLECTRONIQUE ET IDENTITÉ MOBILE

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

CARTE À PUCE (DÉPLOIEMENT EN 2021) + ID MOBILE (DÉPLOIEMENT EN 2021)

EN ACTION DEPUIS 2020

IDENTIFICATION *en ligne et hors ligne*

L'identification hors ligne avec la nouvelle carte d'identité électronique permet d'accéder à de nombreuses données comme l'historique médical ou l'état civil.

PARTAGE D'ATTRIBUTS D'IDENTITÉ

AUTHENTIFICATION

SIGNATURE ÉLECTRONIQUE

191 services d'entités publiques seront connectées grâce au portail citoyen GOV.CO dès 2022.

RECONNAISSANCE TRANSFRONTALIÈRE

Les discussions continuent concernant les normes et l'interopérabilité en Amérique Latine : grâce aux normes ICAO la nouvelle carte d'identité électronique devrait être acceptée comme document de voyage par les autres pays.

CONTEXTE & OBJECTIFS

Depuis 2015, le Registre National d'État Civil de Colombie (RNEC) - constitutionnellement chargé de l'identification des citoyens - permet aux organisations publiques et privées d'utiliser sa base de données biométriques pour proposer des services d'identification et d'authentification par des mécanismes d'interopérabilité, atténuant la fraude à l'identité.

Grâce à une étroite collaboration avec le gouvernement, l'identité numérique fournie par le RNEC sera l'accès clé à différents services (santé, services publics, services sociaux et services financiers). Ce modèle d'identification numérique unique sera basé sur des données biographiques et biométriques, ainsi que sur un numéro d'identification unique.

Outre la RNEC, d'autres initiatives existent actuellement en Colombie autour de trois axes : le Dossier Électronique du Citoyen, l'Authentification Electronique, et la Plateforme d'Interopérabilité dirigés par le gouvernement.

PROPOSITION DE VALEUR

La nouvelle identité nationale prendra deux formes : une carte d'identité électronique physique traditionnelle (lancement prévu en décembre 2020) et une identité numérique mobile, dématérialisation de la carte d'identité électronique. Cette dernière sera légalement reconnue comme l'équivalent du document physique et comme identification logique pour les transactions à distance.

Les nouveaux services apportés par les outils d'identité numérique permettront aux citoyens d'accéder facilement aux services publics, en évitant les formulaires encombrants et les mots de passe multiples. Ils apporteront également des avantages importants en termes de sécurité, d'interopérabilité, d'efficacité, de transparence et de respect de la vie privée.
Le processus d'authentification pour l'application mobile utilise la biométrie, y compris la reconnaissance faciale avec détection en direct. Le niveau d'assurance (par exemple, l'authentification forte) sera adapté au service.

L'identité numérique ouvre la voie à de nouvelles possibilités comme le vote électronique afin de lutter contre l'abstention électorale, d'optimiser le processus et en assurer la transparence. Cet objectif est ouvertement désigné comme le but à long terme des politiques colombiennes. Le Registre National de l'État Civil et le Conseil National Électoral (CNE) mettent déjà en place un cadre pour le nouveau système de vote, avec quatre modalités de vote : manuel, électronique mixte, électronique à distance et anticipé.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Le gouvernement a financé la mise en place de l'infrastructure fournissant l'identité numérique, ainsi qu'un pourcentage du coût du document numérique.
> Pour les Colombiens qui n'ont jamais eu d'identité, la nouvelle carte à puce et l'identité mobile associée sont gratuites. Pour ceux qui en avaient déjà une et qui désirent avoir la nouvelle, ils doivent payer 12-13 dollars US (comme pour l'actuelle Carte Nationale d'Identité).
> Les services publics peuvent utiliser gratuitement l'identité numérique afin d'identifier et authentifier l'identité des citoyens.
> Coût fixe par transaction pour les fournisseurs de services privés. Cette redevance sera réinvestie dans l'infrastructure et les outils de sécurité pour améliorer le système d'identité numérique.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Numéro d'identification unique délivré au hasard à tous les citoyens de Colombie.
> La biométrie permet l'identification et l'authentification avec un haut niveau de confiance.
> Tout le système est basé sur la PKI-CSC. Le vote électronique doit être effectué par le biais de la blockchain.

ÉTAPES CLÉS DU PROJET

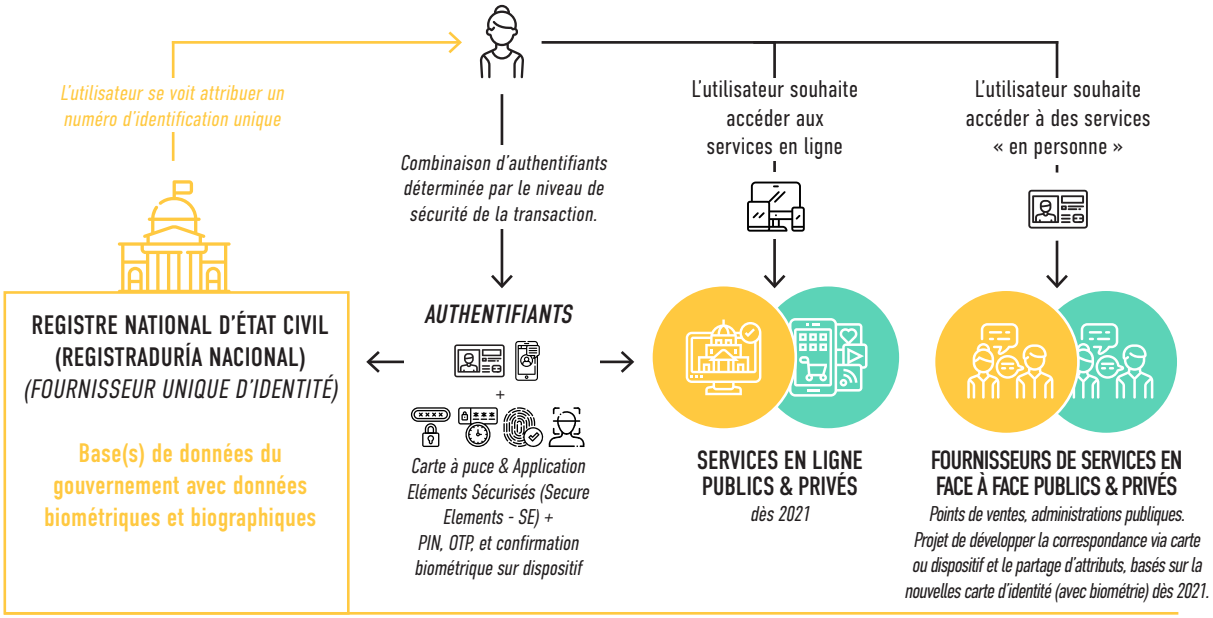
1948
Création du Registre National d'État Civil

2012
Le RNEC permet aux institutions publiques de vérifier des informations via la base de données

2017
Une loi définit les 3 axes de l'identité numérique : le Dossier Électronique du Citoyen, l'Authentification Électronique et la plateforme d' Interopérabilité.

2020
99,98% des citoyens Colombiens sont enregistrés sur la base de données.
50 000 cartes d'identité électroniques sont distribuées.
En Dec. 2020, législation du Congrès en faveur de l'utilisation de l'identité numérique comme moyen d'authentification pour le vote électronique.

IDENTITÉ NUMÉRIQUE - ÉCOSYSTÈME ⟶ OPÉRATIONNEL EN 2021



CADRE JURIDIQUE

Au cours des deux dernières décennies, de nombreux décrets ont été signés concernant le gouvernement numérique, la transparence, la protection de la vie privée ou l'identité. Parmi les plus importants et les plus récents, on peut citer :

2017 : Le décret 1413 comprenant les lignes directrices relatives à l'identité numérique des trois projets : l'authentification, le dossier du citoyen et l'interopérabilité.

2018 : La Loi sur le Gouvernement Numérique, encourageant l'utilisation des outils numériques pour stimuler l'économie et les innovations grâce à la confiance numérique.

2020 : Le décret 620, principalement basé sur le règlement eIDAS, définissant les aspects transversaux de la Politique de Gouvernement Numérique : définition, coût, sécurité, protection de la vie privée, accessibilité et autres.

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

> **Gouvernance indépendante et collaborative :** Le Registre National d'État Civil (RNEC) en charge de la gestion de l'identité numérique et des élections collabore étroitement avec le Ministère des Technologies de l'Information et de la Communication afin d'accéder au Dossier Numérique du Citoyen

> **Choix supposé d'utiliser la reconnaissance faciale dans l'avenir:** l'agence RNEC tente d'ouvrir sa base de données biométriques faciales et d'instaurer la reconnaissance faciale en complément de la base de données d'empreintes digitales qui est déjà utilisée dans plusieurs secteurs en Colombie (secteur financier, notarial ou des télécommunications).

NEMID & MITID

5,8 MILLIONS D'HABITANTS
PRESQUE 100% DE TAUX D'ADOPTION

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT ET LES BANQUES

POUR NEMID: NOM D'UTILISATEUR ET MOT DE PASSE avec une carte clé ou application utilisées comme second facteur d'authentification (technologie PKI)
POUR MITID: NORME EID AVEC SOLUTION DE SIGNATURE ÉLECTRONIQUE BASÉE SUR LA PKI (avec connexion NEM) avec un large choix de titres d'identité

IDENTIFICATION *en ligne*

EN ACTION DEPUIS 2010

PARTAGE D'ATTRIBUTS D'IDENTITÉ

La solution NemLogin propose l'administration des droits des utilisateurs pour les services publics

+800 services connectées publics & privés

AUTHENTIFICATION

Solutions d'authentification multiples: *application mobile, jeton type clé, puce MitID (jeton FIDO, un jeton type puce utilisé pour niveaux d'assurance élevés), jetons accessibles spécifiques aux personnes âgées et malvoyantes, etc.*

SIGNATURE ÉLECTRONIQUE

RECONNAISSANCE TRANSFRONTALIÈRE

NOTIFICATION EIDAS (NIVEAU SUBSTANTIEL) POUR NEMID

CONTEXTE & OBJECTIFS

Le Danemark a une longue tradition d'identité numérique et passe actuellement à sa troisième génération (MitID), codétenue par le secteur financier.

En 2003, la principale priorité était de permettre l'accès aux services publics en ligne en fournissant une identification électronique aux citoyens. En 2010, grâce à une coopération avec le secteur financier, les citoyens ont pu commencer à utiliser leur identité numérique pour effectuer des opérations bancaires en ligne. Aujourd'hui très largement diffusée dans la population danoise, la NemID fournit une identité numérique gratuite et nationale pour tous.

Pour la nouvelle solution MitID, le gouvernement a mobilisé un partenariat public-privé avec le secteur financier, qui en sera copropriétaire.

PROPOSITION DE VALEUR

NemID est une connexion internet sécurisée qui peut être utilisée pour les opérations bancaires en ligne, la recherche d'informations par les autorités publiques ou la collaboration avec l'une des nombreuses entreprises utilisatrices.

Du point de vue de l'utilisateur, il n'y aura pas de différence entre NemID et MitID, si ce n'est qu'elle offrira une meilleure expérience utilisateur, en particulier avec la solution Nemlogin destinée à la gestion des identités des employés.

La principale différence se situe au niveau de l'infrastructure : elle offrira plus de fiabilité, de sécurité et de flexibilité. Avec MItID, seuls les intermédiaires MitID certifiés seront autorisés à dialoguer directement avec le système central. Le rôle des intermédiaires sera de rejoindre l'infrastructure MitID, de réaliser les interfaces techniques et de vendre ensuite leurs services aux fournisseurs qui souhaitent utiliser MitID pour leurs services.

MODÈLE ÉCONOMIQUE

NEMID
> Le secteur public a un contrat avec le fournisseur d'identité numérique et fournit gratuitement NemID pour tous les citoyens - ainsi que 3 certificats employés gratuits par entreprises.
> Les entreprises privées paient pour la validation des NemIDs reçues.

MITID
> Le nouveau modèle est financé et co-détenu par le gouvernement et le secteur financier. Il est toujours gratuit pour les citoyens, ainsi que 3 certificats employés pour toutes les entreprises.
> Il y aura une redevance par transaction pour les fournisseurs de services qui voudront utiliser MitID. Le prix, calculé selon les frais de fonctionnement, devrait être plus bas pour la plupart des prestataires de services.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

La MitID s'appuie sur une infrastructure d'intermédiaires. Cela réduira le niveau de risque auquel le système est exposé. Les fournisseurs de services accéderont à l'infrastructure par le biais d'un intermédiaire et chaque secteur (public, financier, privé) aura le sien:
> Le secteur public n'aura qu'un seul intermédiaire : NemLogin
> Le secteur financier aura plusieurs intermédiaires
> Les intermédiaires privés pourront rejoindre l'infrastructure afin de la rendre accessible aux prestataires de services privés.

ÉTAPES CLÉS DU PROJET

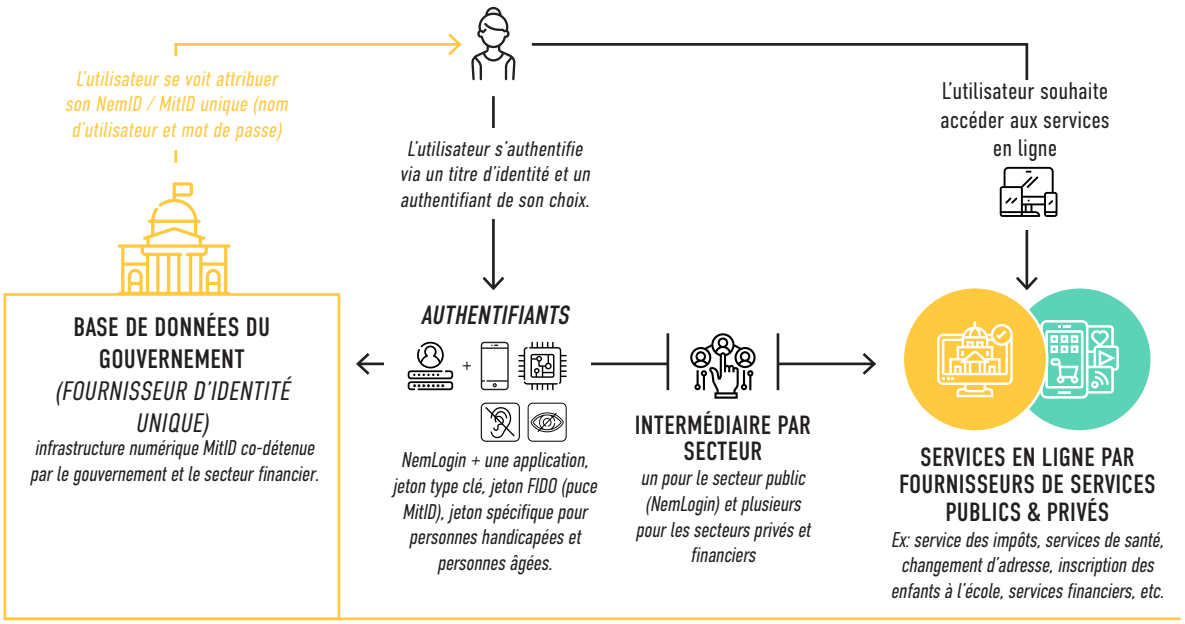
2003
Première infrastructure de services publics en ligne

2010
Lancement de la solution nationale NemID

2020
5.6 millions de NemIDs distribuées aux citoyens Danois et résidents de plus de 15 ans.
1.5M entreprises utilisent l'infrastructure NemID.

Q2 2021
Lancement MitID

IDENTITÉ NUMÉRIQUE MITID - ÉCOSYSTÈME



CADRE JURIDIQUE

> Normes nationales
> Une loi est en cours d'élaboration sur l'infrastructure de MitID et NEM Login, régulant l'accès à l'infrastructure et le respect des utilisateurs.

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

Une grande variété de titres d'identité afin de s'adapter à tous les pans de la population (y compris des titres spécifiques pour les personnes handicapées et les personnes âgées).

MISE EN OEUVRE TECHNOLOGIQUE

> Une infrastructure d'intermédiaires afin d'augmenter le niveau de sécurité en limitant l'accès de l'infrastructure à ces seuls intermédiaires
> Une infrastructure modulaire permettant de suivre l'évolution de la technologie et de connecter/déconnecter les titres d'identité en fonction des besoins des utilisateurs.
> Un accès inclusif et simple pour les petits fournisseurs de services sans grandes compétences informatiques afin de pouvoir utiliser MitID - l'intégration est prise en charge par les intermédiaires

MISE SUR LE MARCHÉ & PROMOTION

> Un partenariat avec le secteur financier depuis le lancement de NemID pour augmenter la fréquence d'utilisation et l'adoption de la solution d'identité.
> Une implication forte et un processus de test avec toutes les parties prenantes, y compris les entreprises et les différentes industries, les associations représentant les personnes âgées, les personnes handicapées, etc.
> Un solide réseau d'enseignants sur lequel s'appuyer pour aider les personnes âgées à utiliser l'identité numérique et à accéder aux services publics en ligne

E-IDENTITY

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

600+ e-services publics pour les citoyens
2400+ e-services publics pour les entreprises
99% services bancaires par identité numérique.

4 TITRES D'IDENTITÉ DISPONIBLES

- **CARTE D'IDENTITÉ : CARTE NAT. D'IDENTITÉ À PUCE**
- **DIGI-ID: CARTE À PUCE COMPLÉMENTAIRE** (qui propose les mêmes fonctionnalités que la carte d'identité mais sans photo, ou identification physique)
- **MOBIIL-ID: SOLUTION BASÉE SUR LA PKI**
- **APPLICATION SMART-ID: SOLUTION BASÉE SUR LA PKI** (utilisant les éléments sécurisés et méthodes de clés partagées d'iOS et Android)

EN ACTION DEPUIS 2002

NOTIFIÉ EIDAS POUR PLUSIEURS NIVEAUX D'ASSURANCE (DONT HAUT ÉLEVÉ) SELON LA SOLUTION CHOISIE

IDENTIFICATION *en ligne & hors ligne*

PARTAGE D'ATTRIBUTS D'IDENTITÉ

AUTHENTIFICATION

Les titres d'identité auront toujours 2 certificats numériques : l'un pour l'authentification de utilisateur et l'autre pour signer des documents de manière électronique. L'accès y est sécurisé par un PIN.

SIGNATURE ÉLECTRONIQUE

Les 3 solutions sont notifiées par le règlement eIDAS pour la signature électronique qualifiée.

RECONNAISSANCE TRANSFRONTALIÈRE

X-road est la première plateforme d'échange de données. Cette plateforme a aussi été mise en oeuvre en Finlande, Azerbaïdjan, Namibie et dans les Îles Féroé.
Pour une interopérabilité transfrontalière au sein de l'UE (entre identités notifées), 2 services centraux d'eIDAS-Node :
> Le node service, pour une authentification avec la carte d'identité électronique estonienne notifiée pour les e-services d'un autre État membre.
> Le node connecteur, pour une authentification dans le secteur public estonien avec une identité numérique émanent d'un autre État membre.

CONTEXTE & OBJECTIFS

L'Estonie est l'une des sociétés les plus intégrées numériquement au monde. On peut accéder aux services numériques via trois solutions d'identité numérique interopérables

> Une carte à puce d'identité (ID-Kaart – pour la Carte Nationales d'Identité et Carte de Résident). La principale agence gouver-nementale impliquée est le Ministère de l'Intérieur, qui supervise le registre de la population. Il est obligatoire pour tout citoyen estonien de plus de 15 ans d'avoir cette carte d'identité.
> Mobiil-ID, proposée par les opérateurs de téléphonie mobile estoniens et le gouvernement. Ce système permet d'effectuer des transactions en ligne sans avoir besoin d'un ordinateur ou d'un lecteur de carte.
> La Smart-ID, proposée par le secteur privé, est également une carte d'identité électronique basée sur une application liée aux éléments sécurisés des smartphones.

L'ID-Kaart a longtemps été la plus populaire mais la tendance s'est récemment arrêtée, donnant l'avantage à la Smart ID (500 000 utilisateurs).

PROPOSITION DE VALEUR

99 % des services publics sont disponibles en ligne en Estonie (y compris le vote en ligne avec 44 % des votants lors des dernières élections). Seuls quelques actes nécessitant une présence physique ne peuvent être effectués par Internet, comme le mariage ou l'achat d'une maison.
De nouveaux services sont disponibles comme le stationnement, la banque en ligne et les transports publics, les services de sécurité sociale (y compris les ordonnances médicales en ligne), les programmes de fidélité intégrés par les commerçants.

MODÈLE ÉCONOMIQUE

> La carte d'identité électronique est obligatoire, financée par le gouvernement, et distribuée par le secteur privé, dans le cadre d'un partenariat public-privé. Les citoyens paient un montant initial de 25€ pour obtenir une nouvelle carte d'identité valable 5 ans.
> L'identité mobile est facultative et cofinancée par le gouvernement et le secteur privé. Les citoyens paient environ 1€ / mois aux opérateurs de réseaux mobiles pour la nouvelle carte SIM, les SMS, etc.
> La Smart ID est facultative, financée et fournie par le secteur privé, et est totalement gratuite pour les citoyens. Comparé à l'identité mobile, les fournisseurs de services en ligne doivent payer deux fois plus cher pour les services de signature en ligne et d'authentification.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Les données sont échangées par le biais d'un système de bases de données connectées au moyen d'un protocole appelé X-Road.
> L'Inspection Estonienne de la Protection des Données, une autorité de contrôle fondée en 1999, protège les droits des citoyens estoniens (utilisation des données personnelles, droit d'acquérir des informations, droit d'accéder aux données...).
> Des données minimales sont partagées, l'Estonie suit le principe «une seule fois» stipulant que les citoyens ne partagent une même donnée qu'une seule fois avec les fournisseurs d'identité et de services.
> Le portail citoyen fournit aux utilisateurs des outils pour superviser et contrôler l'accès à leurs données.
> En 2017, l'Estonie a dû reprogrammer des milliers de cartes à puce parce qu'elles présentaient un problème de sécurité lié aux clés privées PKI stockées sur la puce. Connue sous le nom de «vulnérabilité ROCA», les cartes étaient exposées à des vols d'identité.

ÉTAPES CLÉS DU PROJET

2002
Première carte d'identité électronique distribuée et e-signature

2005
Premier vote par Internet pour les élections locales. 2% des votants par Internet

2006
90% de la population a une ID-kaart

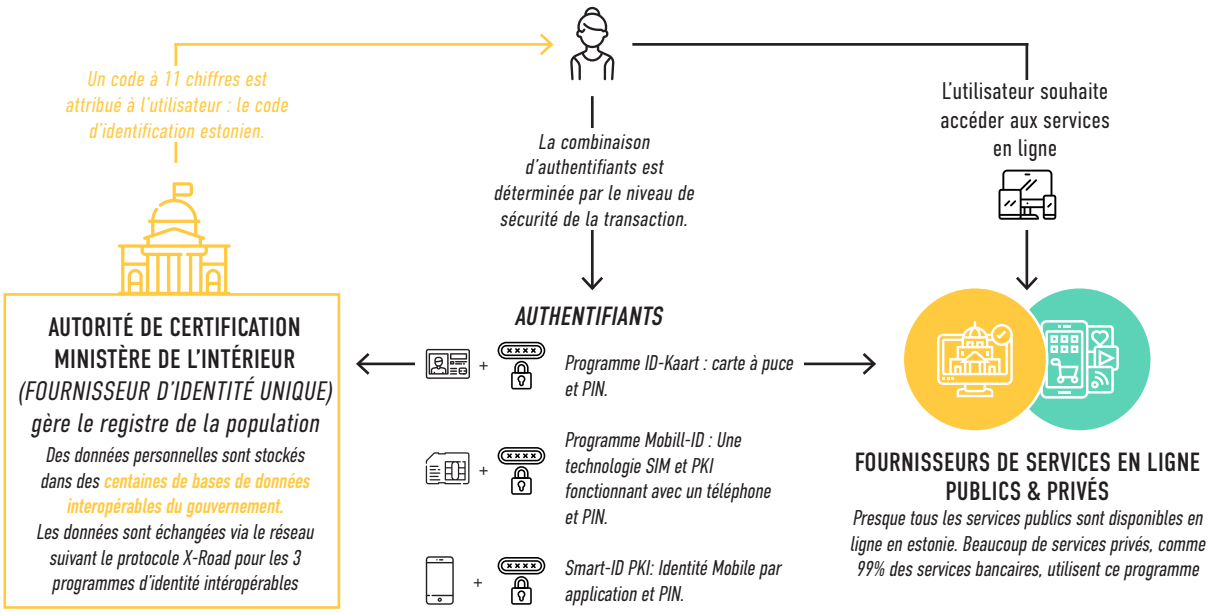
2007
Lancement des services d'identité mobile avec SIM PKI

2011
intégration du programme d'ID Mobile aux services publics

2017
Sortie du service Smart-ID basé sur la plateforme d'identité numérique SplitKey. Crise ROCA (vols d'identité)

2020
98% citoyens ont carte eID
67% l'utilisent régulièrement
250,000 utilisateurs identité mobile
500,000 utilisateurs smart-ID
900,000 utilisateurs actifs ID-kaart

IDENTITÉ NUMÉRIQUE ESTONIENNE - ÉCOSYSTÈME



CADRE JURIDIQUE

> L'Inspection Estonienne de la Protection des Données, fondée en 1999, est une autorité de contrôle dont l'objectif est de protéger les droits des citoyens estoniens (utilisation des données personnelles, droit d'obtenir des informations, droit d'accéder à vos données...).
> Le RIA, l'Autorité des Systèmes d'Informaton, définit les cadres réglementaires pour les différentes parties prenantes.

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

> Cas d'usage faisant gagner du temps aux citoyens : le vote en ligne a réduit la nécessité de se déplacer, un réel avantage pour les personnes de zones rurales. En 2017, il a permis de gagner 11 000 jours de travail pour les élections.
> Une efficacité et une précision accrues du système de santé du pays, avec une réduction de la bureaucratie et la mise en place de nouveaux services : 99 % des ordonnances médicales sont traitées par voie électronique.
> Un programme de résidence en ligne qui place l'Estonie comme pionnière du modèle « country-as-a-service» (ou pays-service). Il permet aux non-citoyens et aux non-résidents d'obtenir une carte de résidence virtuelle, avec un nombre limité d'actions telles que l'ouverture d'un compte bancaire ou l'enregistrement d'une entreprise dans le pays.

MISE EN OEUVRE TECHNOLOGIQUE

> Plateforme open source X-Road, un exemple pionnier d'interopérabilité nationale et internationale, permettant le principe «une seule fois» pour la fourniture de services publics en ligne et la collecte de données.
> Technologie innovante pour l'inscription à la SMART-ID, comme la reconnaissance faciale, comparée avec la photo du passeport.

MISE SUR LE MARCHÉ & PROMOTION

> Une démarche de formation et de soutien pour favoriser l'adoption : une formation spécifique pour la population et une ligne téléphonique de soutien sont toujours disponibles pour les utilisateurs en cas de problème.
> Des incitations à utiliser les services numériques : Transport public sans billet, remboursements d'impôts plus rapides, plafonds plus élevés pour les virements bancaires.

FRANCE CONNECT

67 MILLIONS D'HABITANTS

18 MILLIONS D'UTILISATEURS

GÉRÉ PAR LE GOUVERNEMENT

PROGRAMME FÉDÉRÉ

Titres d'identité et procédés d'authentification dépendent du fournisseur d'identité : nom d'utilisateur, mot de passe + PIN, Application mobile, etc.

- ✓ IDENTIFICATION *en ligne & hors ligne*
- ✓ PARTAGE D'ATTRIBUTS D'IDENTITÉ
- ✓ AUTHENTIFICATION
- ○ SIGNATURE ÉLECTRONIQUE
- ○ RECONNAISSANCE TRANSFRONTALIÈRE

EN ACTION DEPUIS 2016

800 services publics et privés en ligne connectés à FranceConnect (dont 50 privés)

AMBITION D'ÊTRE NOTIFIÉ EIDAS EN 2021

CONTEXTE & OBJECTIFS

Au cours des 15 dernières années, plusieurs tentatives ont été menées par le gouvernement pour développer un écosystème d'identité numérique en France avant FranceConnect. Contrairement à d'autres pays européens, aucune des grandes institutions financières françaises ou des opérateurs de téléphonie mobile n'a choisi d'investir dans le développement d'un service d'identité numérique.

L'objectif initial de FranceConnect était de garantir un accès sécurisé à un maximum de services en ligne sans avoir à multiplier les mots de passe. Grâce à un fort soutien politique, le service a maintenant pour objectif de devenir un système d'identité numérique pleinement fonctionnel, compatible avec le plus haut niveau d'assurance défini par eIDAS.

PROPOSITION DE VALEUR

FranceConnect est un fédérateur d'identités numériques qui maintient et réglemente un écosystème pour les fournisseurs d'identité, les prestataires de services et les utilisateurs. Sa particularité est que l'utilisateur peut sélectionner le fournisseur d'identité de son choix pour accéder à un service.

Afin de favoriser la pénétration, de nouveaux services quotidiens seront intégrés dans l'écosystème d'ici 2021, comme les aides au logement (CAF), les allocations chômage (Pôle Emploi) ou l'éducation (bulletins de notes en ligne).

D'ici 2021, une carte à puce (Carte Nationale d'Identité Électronique - CNIE) sera liée à une application mobile du gouvernement.

AUTRES SERVICES SPÉCIFIQUES ET CAS D'USAGE :
> Réception de lettres recommandées électroniques pour la poste nationale (La Poste).
> Trois extensions innovantes de FranceConnect prévues :
- Une dédiée aux entreprises : ProConnect
- Une consacrée aux personnes handicapées/n'ayant pas accès aux outils numériques, qui permettra une représentation électronique : AidantsConnect
- Une pour les fonctionnaires : AgentConnect.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Les services de FranceConnect sont entièrement financés par le gouvernement.
> Le service est gratuit pour les utilisateurs, les fournisseurs de services et les fournisseurs d'identité publics / privés.
> Les fournisseurs d'identité privés peuvent faire payer leurs services d'authentification aux fournisseurs de services privés, mais doivent les offrir gratuitement pour les services publics.

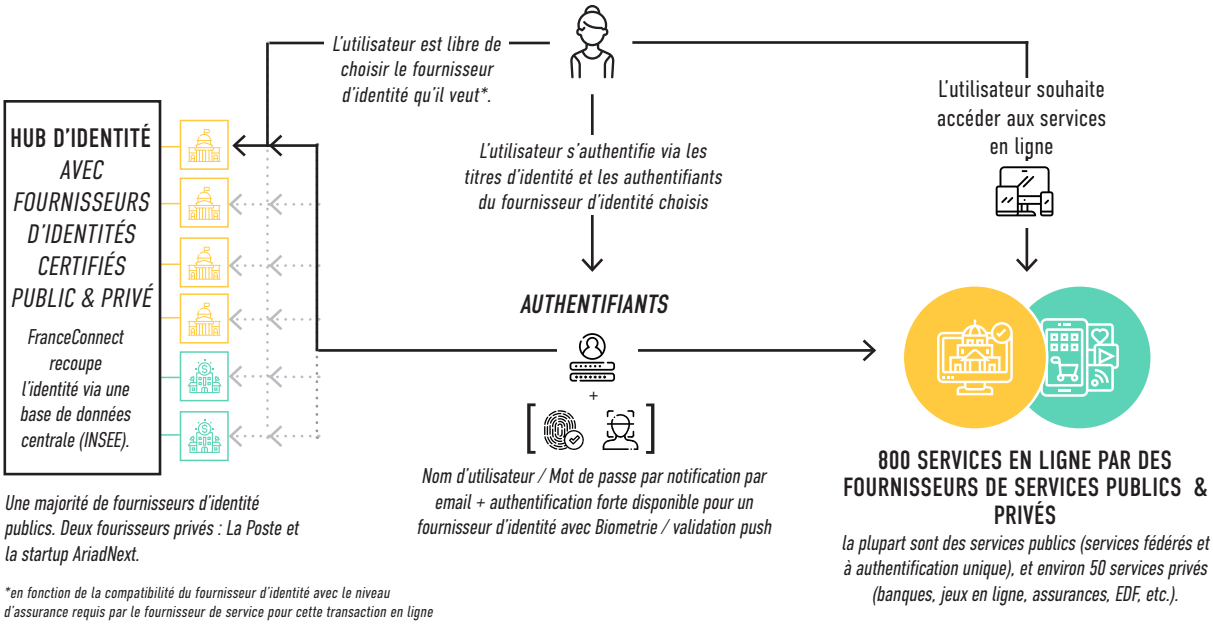
CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> FranceConnect ne stocke aucune information récupérée chez les fournisseurs d'identité, une clé de hachage unique garantit le caractère unique de l'identité.
> La majorité des fournisseurs d'identité de FranceConnect requièrent un nom d'utilisateur et un mot de passe pour l'authentification. La Poste a été approuvée par eIDAS comme niveau substantiel.
> FranceConnect garantit un cadre solide de confidentialité pour les utilisateurs : les fournisseurs de services ne savent pas quel fournisseur d'identité l'utilisateur a choisi et vice versa.
> Conformément aux exigences de la CNIL, il n'y a pas de centralisation des données au sein de l'écosystème de FranceConnect et la propriété de toutes les identités est partagée entre les fournisseurs d'identités.
Ce choix a été fait très tôt et s'est confirmé au fil des années.

ÉTAPES CLÉS DU PROJET

2015	2016	Sept. Oct. 2020	June 2021	2021	2022
Démonstration de faisabilité de FranceConnect	Lancement de FranceConnect	18M d'utilisateurs en France - environ 30 personnes dans l'équipe FranceConnect.	Objectif notification eIDAS	Ajout de nouveaux services fréquemment utilisés. Lancement de la carte à puce CNIE.	Objectif de 30M d'utilisateurs. Ouverture à de nouveaux services privés.

IDENTITÉ NUMÉRIQUE FRANCECONNECT - ÉCOSYSTÈME



Une majorité de fournisseurs d'identité publics. Deux fourisseurs privés : La Poste et la startup AriadNext.

**en fonction de la compatibilité du fournisseur d'identité avec le niveau d'assurance requis par le fournisseur de service pour cette transaction en ligne*

CADRE JURIDIQUE

> Réglementations strictes et contrôle par la CNIL (Commission Nationale de l'Informatique et des Libertés), organisation indépendant chargée de protéger la vie privée des citoyens français.
> Vide juridique quant à l'ajout de nouveaux services privés en ligne tels que les agences immobilières : la future réglementation devrait être adaptée pour intégrer ces nouveaux services.

AUTRES INITIATIVES D'IDENTITE NUMÉRIQUE DANS LE PAYS

> ALICEM: L'identité mobile détenue par le gouvernement a passé la phase pilote et devrait être lancée en 2021.
> En parallèle, le gouvernement français va lancer sa nouvelle génération de Carte d'Identité électronique (CNIE), qui sera liée à une application mobile du gouvernement. Ce service devrait être intégré à FranceConnect.

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

> **Une gouvernance interministérielle** - un des facteurs clé du succès de FranceConnect - avec des comités représentant les parties prenantes (Ministère de l'Intérieur, des Finances, de l'éducation Nationale, de la Santé, etc.) et l'Agence Nationale de Sécurité des Systèmes d'Information
> **Un programme dirigé par le gouvernement :** Contrairement à d'autres programmes fédérés, FranceConnect ne dépend pas d'acteurs privés comme les banques ou les opérateurs de téléphonie mobile.

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

Choix du fournisseur d'identité par l'utilisateur : Il peut choisir de s'authentifier auprès du fournisseur d'identité de son choix, parmi plusieurs organismes publics et privés largement utilisés. Un seul titre d'identité est nécessaire pour accéder à l'écosystème.

MISE EN OEUVRE TECHNOLOGIQUE

> **Un système interopérable « by design »** utilisant des normes telles que OAuth 2 et Open ID Connect.
> **Une solution à technologie agnostique:** les fournisseurs d'identité sont libres d'utiliser n'importe quelle technologie tant qu'elle respecte le cadre réglementaire.

MISE SUR LE MARCHÉ & PROMOTION

SPID

60 MILLIONS D'HABITANTS

26% TAUX D'ADOPTION

GÉRÉ PAR LE GOUVERNEMENT	PROGRAMME FÉDÉRÉ	NOM D'UTILISATEUR & MOT DE PASSE + OTP ou app en fonction du Niveau d'assurance	EN ACTION DEPUIS 2016

IDENTIFICATION *en ligne & présentiel*	PARTAGE D'ATTRIBUTS D'IDENTITÉ	AUTHENTIFICATION	SIGNATURE ÉLECTRONIQUE	RECONNAISSANCE TRANSFRONTALIÈRE
100% **des services publics en ligne sont connectés de droit au SPID.** Beaucoup de services privés sont déjà connectés ou prévoient de l'être.	*La fédération SPID supervise une autre entité, qui s'appelle Attribute Authority et qui fournit des attributs certifiés basés sur l'utilisateur authentifié. Aucun attribut n'est partagé entre fournisseurs d'identité.*	*Authentification Unique (Single Sign-On) - seulement pour certains services qui requièrent un faible niveau d'assurance.*	*Le procédé dépend du fournisseur d'identité choisi. Depuis Mars 2020, le SPID peut aussi être utilisé pour signer des documents et des contrats de manière électronique, ayant la même valeur qu'une signature manuelle.*	**NOTIFIÉ EIDAS DEPUIS 2018** POUR PLUSIEURS NIVEAUX D'ASSURANCE (Y COMPRIS ÉLEVÉ) SUIVANT LA SOLUTION CHOISIE.

CONTEXTE & OBJECTIFS

Le Système Public Italien d'Identité Numérique (le SPID) est géré par l' « Agenzia per l'Italia Digitale » (AgID) et est financé par des fournisseurs d'identité privés accrédités.

L'objectif principal du SPID est de fournir à tous les citoyens et entreprises une identité numérique sans dispositif (à l'exception du smartphone) et de leur permettre d'accéder facilement et gratuitement aux services publics. Avec plus de 10 millions d'identités délivrées, le programme est considéré comme un succès en Italie. De plus en plus de fournisseurs de services privés souhaitent rejoindre l'écosystème et se font progressivement accréditer par l'AgID.

PROPOSITION DE VALEUR

SPID est un écosystème public ouvert permettant aux fournisseurs d'identité privés accrédités de fournir une identité numériques aux citoyens et entreprises. Actuellement, chaque citoyen peut choisir jusqu'à 9 fournisseurs d'identité gratuits, même si la plupart des utilisateurs n'en ont qu'un. Les professionnels et entreprises peuvent aussi s'abonner à un type d'identité payant spécifique aux entreprises.

SPID permet aux citoyens d'avoir accès à des services publics et privés avec un même titre d'identité, sûre, simple à garder en tête, et disponible sur ordinateur, tablette ou smartphone. Pour accéder à des services qui demandent un plus haut niveau de sécurité, l'utilisateur choisit un nom d'utilisateur et un mot de passe, et un code d'accès temporaire est généré. D'autres facteurs d'authentification peuvent être disponibles en utilisant une application mobile (smartphone) ou la biométrie.

SPID fournit également un système fiable et sécurisé à l'administration publique italienne, qui délègue maintenant les procédés d'identité trop lourds (distribuer et gérer les titres d'identité, etc) et économise ses ressources en termes de main d'œuvre et de coûts financiers.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE SECTEUR PRIVÉ

> Le programme fédéré est financé par des fournisseurs d'identité privés qui attendent un retour sur investissement important dans les années qui viennent (certains d'entre eux ont payé plus d'1M € par an pour les SMS de mot de passe OTP)
> SPID est gratuit pour les citoyens et les fournisseurs de services publics pour tous les niveaux de sécurité, à l'exception du plus haut, utilisé principalement par les professionnels et lié à un certificat électronique qualifié
> Les fournisseurs de services privés suivent un modèle de paiement à l'usage et paient une redevance par utilisateur et par an au fournisseur d'identité (0.40€ à 7€, suivant le nombre d'informations et le niveau d'assurance requis).
> Le SPID va également proposer de nouveaux types d'identité numériques payantes aux professionnels et entreprises, ce qui fera partie intégrante du modèle économique.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

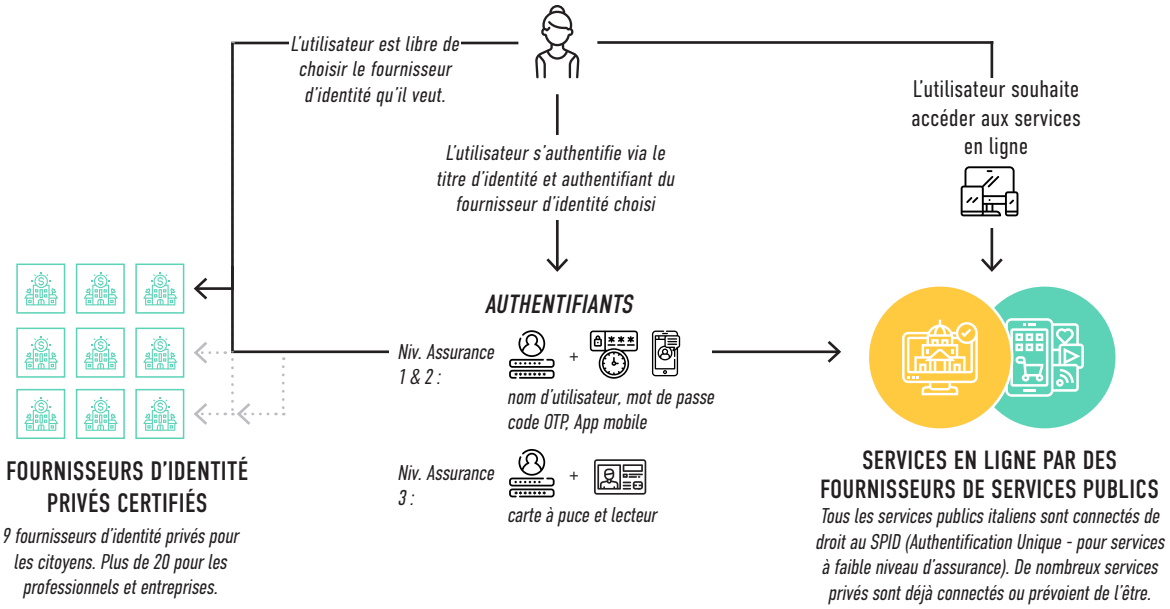
> AgID se veut le superviseur de la protection et gestion des données. Les organismes d'évaluation de la conformité et de la sécurité évaluent un fournisseur candidat avant son accréditation par l'AgID.
> Les niveaux d'assurance du SPID sont fidèles aux normes ISO-IEC 29115 et eIDAS. A la différence d'autres pro-grammes d'identité numérique avec une passerelle nationale connectant fournisseurs d'identité et fournisseurs de service, le SPID autorise le partage direct des données (seulement celles qui sont nécessaires au service demandé) entre fournisseur d'identité et fournisseur de service, après consentement du citoyen. Si cela peut paraître in choix peu optimal en termes de protection des données, d'autres stratégies techniques et organisationnelles rendent le SPID tout à fait respectueux du principe de « privacy by design »[1].

ÉTAPES CLÉS DU PROJET

2016	Fin 2017	2018	2019	2020	2021
Lancement du SPID avec 3 fournisseurs d'identité	Les 600 services publics seront disponbiles d'ici 2018.	2.5M d'identités numériques SPID distribuées. Notification eIDAS	5.5M d'identités numériques SPID distribuées	15M d'identités numériques SPID distribuées	Objectif de 20M d'identités numériques SPID distribuées et nombre de fournisseurs de services privés x2

1. «privacy by design» principe énoncé dans le Règlement EU 2016/679 du Parlement européen et du Conseil du 27 Avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

IDENTITÉ NUMÉRIQUE SPID - ÉCOSYSTÈME



NB: Pas de Hub d'identité – Les fournisseurs d'identité envoient directement les données aux fournisseurs de services publics & privés

CADRE JURIDIQUE

> Le cadre Légal National stipule que l'adhésion au SPID est obligatoire pour le secteur public.
> Le SPID est réglementé par le Code de l'Administration Numérique via un décret législatif d'application (communément appelé CAD) et par plusieurs directives et règles techniques émises par l'Agence Numérique Italienne (AgID).

AUTRES INITIATIVES D'IDENTITE NUMÉRIQUE DANS LE PAYS

> La Carte Nationale d'Identité (CIE) a reçu la notification eIDAS pour sa version antérieure (Carta d'identità elettronica (CIE 3.0) lancée en 2016) en 2019. Ce programme à fort taux d'adoption (en 2020, 13,6M nouvelles cartes d'identité ont déjà été délivrées) s'appuie principalement sur la carte d'identité électronique physique, sortie en 2001.

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

Un modèle économique et une gouvernance publique et privée avec un programme géré par le gouvernement, mais financé entièrement par les fournisseurs d'identité privés.

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

Une stratégie 100% mobile avec une diversité de choix pour accéder à des services à niveaux d'assurance substantiels : les utilisateurs peuvent choisir entre la Carte Nationale d'Identité Électronique (CIE), une signature électronique qualifiée, ou une signature qualifiée à distance plus simple d'utilisation, où le HSM est la plupart du temps hébergé par le fournisseur d'identité.

MISE EN OEUVRE TECHNOLOGIQUE

OpenID Connect comme choix de standard pour le SPID, au lieu de SAML (utilisé par la plupart des programmes notifiés par l'UE). Cette solution permet, entre autres, une meilleure UX lors de l'utilisation sur téléphone portable.

MISE SUR LE MARCHÉ & PROMOTION

Un processus unique d'inscription des citoyens à distance via audio et vidéo (par opposition à la présence physique) avec une validation en direct par un opérateur - qui prend environ 20 minutes. SPID a été le premier programme à être notifié avec une procédure d'inscription à distance. Les taux de satisfaction concernant ce processus sont extrêmement élevés, car il a été et reste très utile durant l'épidémie de COVID-19. Récemment, l'AgID a autorisé une nouvelle procédure destinée à améliorer le temps d'inscription (10 secondes pour l'enregistrement audio et vidéo sans opérateur en direct) : les citoyens effectuent des actions aléatoires demandées par l'application, puis l'opérateur décide de la valider ou non.

EID.LI

38,7 MILLE HABITANTS
5% TAUX D'ADOPTION

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

ID MOBILE SUR APP SMARTPHONE (APP EID.LI) AVEC AUTHENTIFICATION VIA PIN OU BIOMÉTRIE

EN ACTION DEPUIS 2020

- IDENTIFICATION *en ligne & hors ligne*
- PARTAGE D' ATTRIBUTS D'IDENTITÉ
- AUTHENTIFICATION *L'ancienne carte à puce et l'identité mobile proposent des fonctions électroniques avancées facilitant une authentification sécurisée (protocole FIDO).*
- SIGNATURE ÉLECTRONIQUE
- RECONNAISSANCE TRANSFRONTALIÈRE

presque 200 services publics en ligne *disponibles, incluant la déclaration d'impôt, les formulaires pré-remplis, service de poste, immatriculation de véhicule, etc.*

NOTIFICATION EIDAS PRÉVUE POUR 2021

CONTEXTE & OBJECTIFS

Avec une population de moins de 40 000 habitants, le Liechtenstein est un petit pays européen ayant développé une stratégie et un réel agenda numérique pour le développement des services en ligne.

En 2008, le Liechtenstein a mis au point un programme d'identité numérique reposant sur sa Carte Nationale d'Identité électronique. Basée sur un certificat PKI intégré, la carte à puce est utilisée par les citoyens, les résidents et les entreprises pour accéder aux services publics en ligne.

La carte est délivrée par l'Office National de l'Immigration et des Passeports du Liechtenstein ; tandis que l'Office des Technologies de l'Information est chargée de développer le programme d'identité numérique.

En avril 2020, la Principauté du Liechtenstein a lancé une nouvelle carte d'identité électronique sur téléphone portable : eID.li. Elle prévoit de supprimer progressivement sa carte à puce dans les mois à venir.

PROPOSITION DE VALEUR

eID.li est la nouvelle identité numérique avec laquelle les citoyens et résidents du Liechtenstein ainsi que les ressortissants étrangers peuvent s'identifier et se connecter aux services électroniques en toute sécurité. Elle présente de nombreux avantages : une inscription et des mises à jour plus faciles, une expérience utilisateur solide (ex : les formulaires sont automatiquement préremplis avec les attributs personnels enregistrés, et envoyés simplement au gouvernement).

L'application eID.li est liée - grâce des mesures cryptographiques - à l'appareil mobile utilisé lors de l'inscription. Les utilisateurs peuvent ensuite utiliser leur application eID.li pour se connecter à un service et s'authentifier en utilisant la biométrie.

L'ambition actuelle de l'Office des Technologies de l'Information du Liechtenstein est d'étendre le système d'identité numérique au secteur privé et d'être notifié eIDAS dans les années à venir. Un projet visant à développer l'identé numérique mobile pour les entreprises est également en cours : les employés pourraient représenter leur entreprise/société en utilisant le système d'identité numérique et télécharger des déclarations fiscales.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Le gouvernement finance le programme d'identité numérique à 100 %.
> L'accès à l'identité numérique est gratuit pour les citoyens, les résidents et les entreprises.
> Le projet visant à étendre l'écosystème aux fournisseurs de services privés comprend l'introduction de modalités de paiement à l'usage.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Tests de pénétration et audits réguliers des systèmes.
> Pour la protection des données, l'Office des Technologies de l'Information du Liechtenstein suit la réglementation générale de l'UE et du Liechtenstein en matière de protection des données.
> l'Office des Technologies de l'Information du Liechtenstein poursuit ses démarches de notification eIDAS pour les niveaux substantiel et élevé.

ÉTAPES CLÉS DU PROJET

2008 – Lancement de l'identité numérique

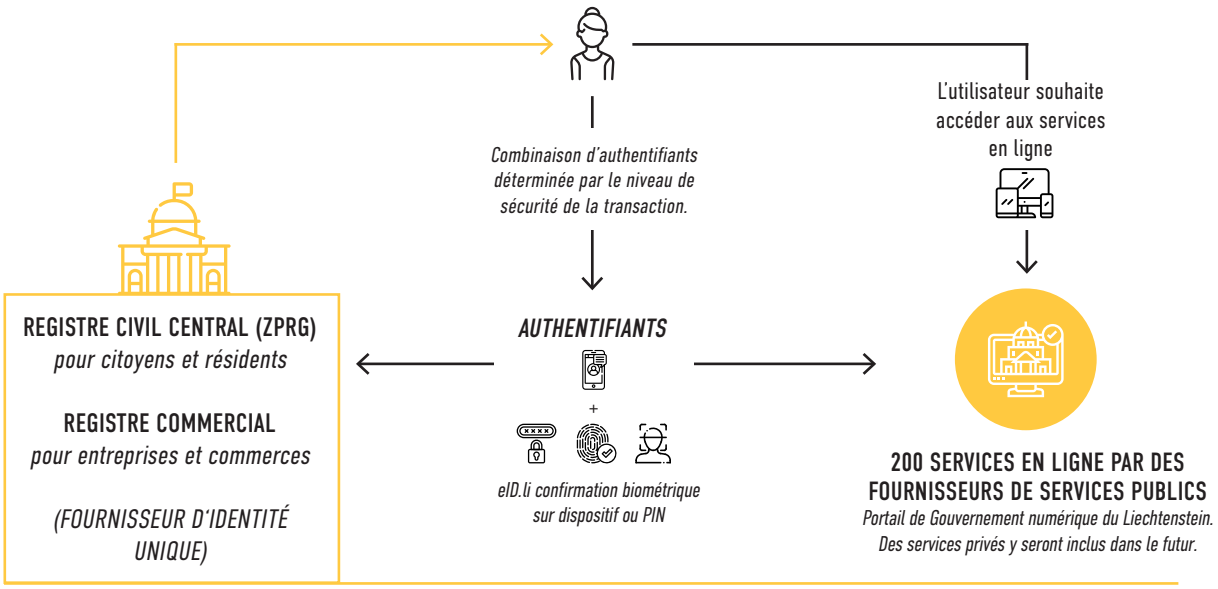
2018 – 5000 identités numériques par cartes à puces délivrées

2020 – Lancement d'une nouvelle identité numérique basée sur téléphone portable en Avril. 500 identités mobiles distribuées en Octobre.

2021 – Objectif d'être notifié eIDAS pour des niveaux d'assurance élevé et substantiel - afin d'ouvrir au secteur privé et mettre en place l'inscription à distance par vidéo.

2023/2027+ – Objectif de numériser toutes les démarches pour les entreprises et adopter une politique du tout numérique pour tous les citoyens et résidents, conformément à la feuille de route du gouvernement numérique.

IDENTITÉ NUMÉRIQUE LIECHTENSTEIN DIGITAL ID ECOSYSTEM



CADRE JURIDIQUE

Le gouvernement a adopté en Juillet 2019 le Rapport de Consultation relatif à l'adoption d'une loi instaurant le règlement eIDAS, concernant les signatures électroniques et les services de confiance.

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

> Ambition de devenir 100% mobile en remplaçant la carte à puce et ses services par le nouveau programme d'identité mobile afin d'apporter plus de flexibilité. Le système utilise les dernières technologies et les mécanismes de sécurité les plus récents pour sécuriser l'identité de leurs citoyens : l'application eID.li est fortement liée à l'appareil mobile des utilisateurs

> Un processus d'inscription très rapide pour la nouvelle identité mobile afin de stimuler l'adoption des utilisateurs : le processus d'inscription à eID.li se déroule au bureau de l'immigration et des passeports et dure entre 2 et 5 minutes. La prise en main de l'application eID.li est très simple. En outre, le Liechtenstein organise régulièrement des événements et des webinaires pour promouvoir la nouvelle solution d'identité numérique.

DIGID

17,4 MILLIONS D'HABITANTS
87% TAUX D'ADOPTION (2015)

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT	**NOM D'UTILISATEUR & MOT DE PASSE** AVEC VERIFICATION SMS ET IDENTITÉ MOBILE (APP), NFC	EN ACTION DEPUIS 2003

✓ IDENTIFICATION *en ligne*	○ PARTAGE D'ATTRIBUTS D'IDENTITÉ	✓ AUTHENTIFICATION	○ SIGNATURE ÉLECTRONIQUE	✓ RECONNAISSANCE TRANSFRONTALIÈRE

615 organisations publiques et semi-publiques connectées	**NOTIFICATION EIDAS DEPUIS 2020** AVEC NIVEAUX D'ASSURANCE SUBSTANTIEL ET ÉLEVÉ

CONTEXTE & OBJECTIFS

Les Pays-Bas bénéficient d'un système d'identité régalien très solide, avec un registre de population numérique et centralisé depuis 1994, attribuant un numéro d'identité unique (BSN) à chaque citoyen.
Les documents légaux qui servent à vérifier l'identité d'une personne sont la carte d'identité, le passeport et le permis de conduire.
En 2003, la DigID a été mise en place par l'Unité ICT, créée en 2001 par le Ministère de l'Intérieur et l'Association des Municipalités Néerlandaises, afin d'accéder aux services publics.

Plutôt que de développer leur propre système d'identité, les Pays-Bas créent un écosystème de marché ouvert, dans lequel des parties privées peuvent également fournir des services d'identité numérique, grâce à une nouvelle législation (Loi Digital Government – Février 2020). L'objectif est triple : bénéficier des innovations du marché, renforcer la compétitivité des prix, et rester fort en disposant de plusieurs services d'identité fiables en cas d'échec. Le gouvernement agira comme une source d'information fiable faisant autorité.

En outre, le gouvernement lancera sa nouvelle carte à puce le 1er janvier 2021, et travaille sur une version mobile de la carte d'identité et du passeport.

PROPOSITION DE VALEUR

Lorsque des citoyens ou des résidents demandent une DigiD, ils entrent un nom d'utilisateur et un mot de passe qu'ils utiliseront ensuite pour s'identifier. En général, les procédures d'authentification nécessiteront l'utilisation de l'application DigID ou la vérification par SMS. Pour les transactions d'informations particulièrement sensibles (ex : vérification ou mise à jour des informations de santé), une vérification unique de documents physiques peut être requise (effectuée avec l'application DigiD sur les smartphones équipés d'un lecteur NFC). La DigiD est liée au Numéro de Service au Citoyen (BSN).

DigID permet aux citoyens et aux résidents de s'identifier facilement et en toute sécurité et d'accéder aux services publics numériques (gouvernement, établissements d'enseignement, institutions de santé ou fonds de retraite). En 2006, Il est devenu obligatoire d'effectuer toute déclaration d'impôt en ligne.

eHerkenning, qui a remplacé DigID pour les entreprises, est construit sur un réseau public-privé d'organisations, et leur fournit des services d'authentification.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Le gouvernement finance le programme d'identité numérique à 100 %.
> Gratuit pour les citoyens et les prestataires de services publics.
> Nouvel écosystème de marché ouvert avec des fournisseurs d'identité privés, encadré par la nouvelle Loi Digital Government de Février 2020

Les principaux piliers de cette Loi sont :
- Il est obligatoire pour les fournisseurs de services publics de demander le niveau d'assurance substanciel ou élevé
- Ouverture à des IdP multiples (avec DigID) – les fournisseurs de services publics doivent accepter ces nouvelles solutions d'authentification
- Potentiellement ouvrir aux fournisseurs de services du secteur privé.
- Traitement du BSN (Numéro d'Identité Unique) licite régi par la Loi.

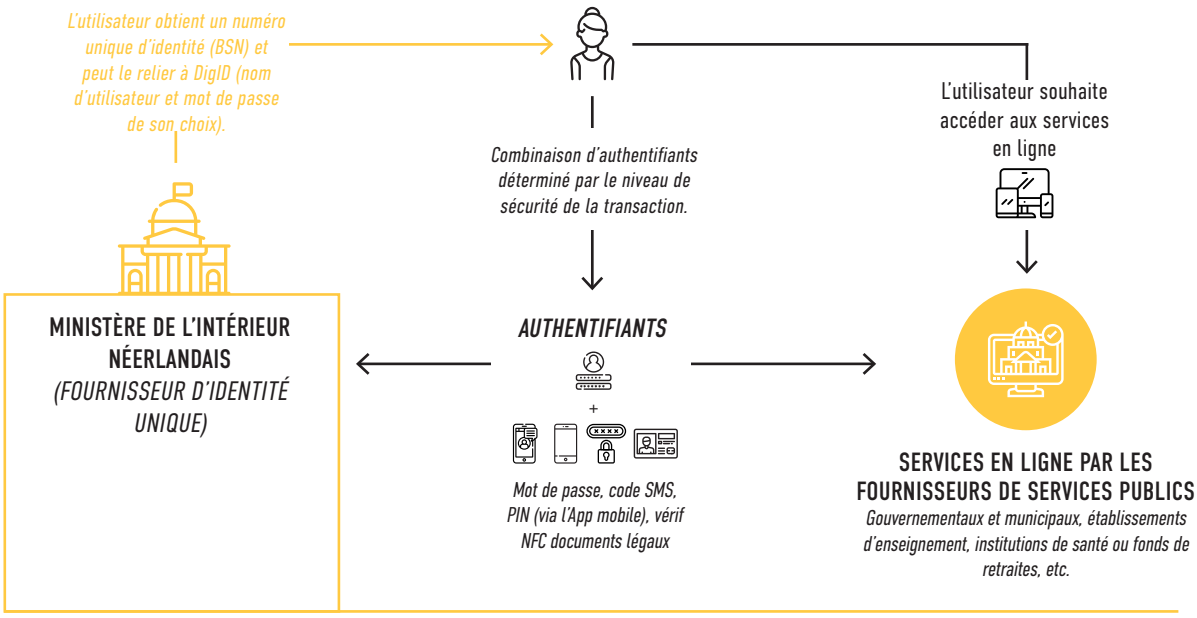
CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Respecte la réglementation RGPD.
> Un Numéro d'Identité Unique - le BSN - est utilisé pour établir le caractère unique d'une identité. Il était auparavant imprimé sur la carte d'identité, mais il sera supprimé pour améliorer la protection de la vie privée.
> Adoption de jetons destinés à rendre le numéro anonyme pour les différents fournisseurs de services. Il sera également inclus dans la carte d'identité électronique.

ÉTAPES CLÉS DU PROJET

2003	2005	2011	2015	2020	2021
Lancement de DigID	Lancement de DigID pour les entreprises Tous les services publics sont connectés à DigID	Remplacement de DigID pour les entreprises par eHerkenning	87% des citoyens néerlandais de plus de 16 ans utilisent DigID	Notification eIDAS pour DigID	1er Janvier, nouvelle carte d'identité électronique

DIGID - ÉCOSYSTÈME



CADRE JURIDIQUE
Recommandations de l'OACI pour les titres d'identité

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

> **Un gouvernement qui se positionne** comme constructeur d'écosystème plutôt que fournisseur de système d'identité, et agissant comme une source d'information fiable faisant autorité. Son objectif est d'insuffler une confiance dans l'économie numérique. Il délivre l'identité source et l'estampille comme une «identité numérique de confiance délivrée par le gouvernement». D'autres fournisseurs de services et fournisseurs d'identité peuvent ensuite s'en servir pour soutenir d'autres moyens d'identification.
> **Un groupe de travail ouvert :** le gouvernement néerlandais travaille en étroite collaboration avec le secteur privé mais également avec les universités et instituts de recherche sur les questions d'identité numérique.

> **Un processus d'inscription à distance :** DigID est l'un des rares programmes d'identité numérique notifié par eIDAS à avoir une procédure d'inscription à distance. Celle-ci prend plusieurs jours : les utilisateurs doivent remplir un formulaire de demande, ils recevront ensuite un courrier contenant un code d'activation dans les trois jours ouvrables. Ils peuvent alors activer leur DigiD en utilisant ce code, ainsi que leur nom d'utilisateur et mot de passe. Ils pourront ensuite se connecter.

NIN & APPLICATION D'IDENTITÉ MOBILE

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

CARTE À PUCE (OU REÇU NIN IMPRIMABLE) + ID MOBILE (SUR APPLICATION - PHASE D'ESSAI)

EN ACTION DEPUIS 2014

IDENTIFICATION *en ligne & hors ligne*

PARTAGE D'ATTRIBUTS D'IDENTITÉ

AUTHENTIFICATION

> La carte à puce peut être utilisée pour l'authentification, combinée avec la biométrie ou un PIN (mais manque de points de vente connectés hors-ligne)
> L'App mobile utilisera les authentifiants Google, entre autres titres d'identité, pour l'authentification en ligne

SIGNATURE ÉLECTRONIQUE

> Fonctionne avec la carte à puce
> L'application d'identité numérique permettra la signature électronique de documents. Des certificats et clés privées seront également stockés dans les éléments sécurisés des smartphones, avec une sauvegarde stockée de manière sécurisée sur les HSM.

RECONNAISSANCE TRANSFRONTALIÈRE

En Juin 2021, discussions bilatérales avec les pays de la CEDEAO et de l'EAC pour une reconnaissance transfrontalière

CONTEXTE & OBJECTIFS

Historiquement, la majorité des Nigérians n'a aucune forme d'identification légale et le pays le plus peuplé d'Afrique est très fragmenté en termes d'identité. De multiples bases de données privées et publiques non-interopérables coexistent (permis de conduire, opérateurs de téléphonie mobile, banques, bases de données des électeurs) nécessitant chacune des attributs différents.

Afin de créer une base solide pour un futur système d'identité numérique, le gouvernement a mis en place la Commission Nationale de Gestion de l'Identité [NIMC]. Son principal objectif pour les années à venir est de saisir les données dans une base de données d'identité centrale, sécurisée et harmonisée afin de distribuer un Numéro National d'Identité (NIN) à tous les citoyens Nigérians, ainsi qu'aux réfugiés et aux déplacés internes (IDP)

Le programme d'identité numérique devrait améliorer l'inclusion financière - la population adulte non bancarisée au Nigeria est estimée entre 40 et 60 millions de personnes - mais aussi accroître la sécurité et la transparence, stimuler le développement économique et réduire les coûts de gouvernance.

PROPOSITION DE VALEUR

Le Numéro National d'Identité (NIN) se compose de 11 numéros non intelligibles choisis au hasard et attribués aux citoyens nigérians lors de leur inscription, au cours de laquelle sont saisies les données démographiques, la biométrie (10 empreintes digitales), une photo de la tête aux épaules, et la signature numérique.

Les Nigérians peuvent utiliser leur Carte Nationale d'Identité pour l'authentification et la signature numérique. Elle peut également être utilisée par les banques pour les procédures d'inscription de nouveaux clients (KYC), peut servir aux paiements, transferts ou aux distributeurs automatiques de billets.

De nouveaux services seront disponibles ultérieurement, tels que le vote, les retraites, les prestations de santé, le permis de conduire, les impôts, etc.

À ce jour, la pénétration de la carte à puce reste faible - seulement 1 million de cartes d'identité ont été émises jusqu'à présent - en raison du manque de services disponibles. Un nouvel écosystème d'identité mobile est prêt à être lancé.

MODÈLE ÉCONOMIQUE

> Le gouvernement fédéral bénéficie du soutien de prêts de la Banque Mondiale, de l'Agence Française de Développement (AFD) et de l'Union Européenne (UE) pour financer son système d'identité numérique.
> L'enregistrement de la carte à puce est gratuit pour les citoyens et les résidents, le remplacement de la carte est payant (10$US).
> L'application d'identité mobile sera gratuite pour tous les détenteurs du NIN. Les revenus seront générés par l'achat préalable de crédits, pour toute personne souhaitant payer une vérification d'identité pour accéder à un service.

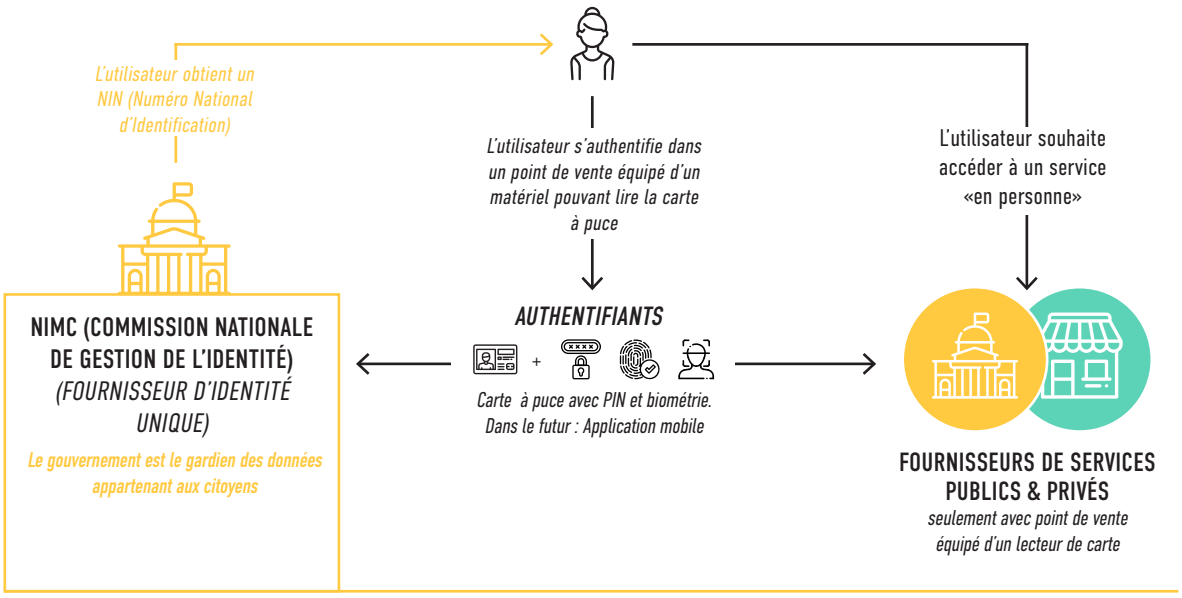
CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Le NIMC délivre un numéro généré de manière aléatoire (Numéro National d'Identité, NIN) à tous les citoyens.
> Le NIMC met l'accent sur la sécurité : cryptage, serveurs de secours, générateurs diesel. Il a reçu la certification ISO pour sa procédure de stockage de données et ses installations de récupération de données après sinistre.
> Le Gouvernement Fédéral a l'intention de prolonger sa volonté de protéger l'identité personnelle des citoyens en leur délivrant des titres d'identité virtuels sûrs, qui seront limités dans le temps et émis par le détenteur de l'identité à un commerçant ou personne vérificatrice.
> Aucune organisation n'est mandatée pour protéger les données personnelles et de la vie privée des citoyens.

ÉTAPES CLÉS DU PROJET

2007	2014	2015	2016	2017	2020	2021
Création du NIMC à partir de la Loi NIMC.	Lancement de la carte à puce	7M Nigérians enregistrés dans la base de données	14M Nigérians enregistrés dans la base de donnés	28M Nigérians enregistrés dans la base de donnés	Lancement de l'application mobile 41M Nigérians enregistrés	Objectif de 90% de Nigérians inscrits au numéro NIN

IDENTITÉ NUMÉRIQUE - ÉCOSYSTÈME → De nouveaux services (y compris en ligne) seront disponibles dans les années à venir.



CADRE JURIDIQUE

> Loi sur la Protection des Données Personnelles (2010)
> "Ébauche de Règlement sur la Protection des Données" (2013): évaluation privé et définition des politiques relatives à la protection des données qui ont été adoptées par le gouvernement
> Nouvelle Loi de Protection des Données (2019) inspirée des conventions européennes. La loi a été ratifiée par les deux parlements mais n'a pas été signée à temps par le Président, avant le changement de gouvernement.

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

Agence indépendante et autonome (NIMC) dirigée par un conseil d'administration de 18 personnes représentant différentes agences gouvernementales et parties prenantes. Parmi les avantages de cette organisation, citons la coordination entre les différentes parties prenantes et l'effet de levier sur l'innovation du secteur privé grâce aux partenariats public-privé : les entreprises privées apportent les fonds en échange d'un flux de revenus dans le futur programme d'identité numérique.

Inscription des partenaires publics et privés afin de renforcer et accélérer le taux d'enregistrement (banques, opérateurs de téléphonie mobile et agences gouvernementales).

10,3 MILLIONS D'HABITANTS
1.5M D'UTILISATEURS ACTIFS

CHAVE MÓVEL DIGITAL

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

CARTE DE CITOYEN (CARTE À PUCE) + TÉLÉPHONE PORTABLE + PIN + OTP (SMS OU EMAIL) OU APP MOBILE

EN ACTION DEPUIS 2014
(2007 POUR LA CARTE DE CITOYEN

IDENTIFICATION *en ligne & hors ligne*
L'utilisateur peut s'identifier hors ligne via sa carde de citoyen mais aussi une application de portefeuille d'identité numérique depuis 2019.

PARTAGE D'ATTRIBUTS D'IDENTITÉ
L'utilisateur peut décider de sélectionner un ou plusieurs attributs à partager pour chaque authentification

AUTHENTIFICATION
La Carte d'e Citoyen et la Clé Mobile Numérique assurent des fonctions électroniques avancées facilitant une authentification sécurisée (protocole FIDO).

SIGNATURE ÉLECTRONIQUE
Signature électronique qualifiée par HSM

RECONNAISSANCE TRANSFRONTALIÈRE

NOTIFICATION EIDAS (ÉLEVÉE) POUR LA CARTE DE CITOYEN ET LA CLÉ MOBILE NUMÉRIQUE

+200 services en ligne accessibles depuis le portail de gouvernement numérique

CONTEXTE & OBJECTIFS

Le Portugal a été l'un des pionners dans la mise en œuvre de certificats numériques avec sa Carte de Citoyen électronique, lancée en 2007. La carte à puce obligatoire contient 5 cartes différentes en une (Carte d'Identité Civile, Carte Fiscale, Carte Électorale, Carte de Sécurité Sociale, Carte de Santé), et comprend une signature électronique qualifiée pour une authentification sécurisée. Cette dernière permet aux citoyens de réaliser des transactions et de signer des documents de manière électronique.

La Carte de Citoyen ayant rarement été utilisée par les citoyens pour accéder à des services en ligne, l'AMA (Agence de Modernisation Administrative du Portugal) à créé une identité mobile plus pratique et plus simple d'utilisation, la Clé Mobile Numérique ou «Chave Móvel Digital» (CMD) en 2014. Aujourd'hui, la Carte de Citoyen est principalement utilisée par des publics spécifiques, comme les entreprises ou les utilisateurs de prescriptions médicales, pour son service de signature électronique.

PROPOSITION DE VALEUR

La Clé Mobile Numérique permet une authentification sécurisée sur divers sites web publics et privés, ne nécessitant qu'un téléphone portable, un code PIN de 4 à 8 chiffres et un mot de passe OTP (code temporaire envoyé par SMS ou e-mail). Depuis 2020, un système de reconnaissance biométrique utilisant le téléphone portable peut également être utilisé pour remplacer les seconds facteurs d'authentification tels que l'OTP.

Pour les citoyens portugais, la clé mobile numérique relie leur numéro d'identification civile à leur numéro de téléphone portable, et au numéro de passeport ou de titre / carte de séjour pour les citoyens étrangers.
Contrairement à la Carte de Citoyen, la Clé Mobile Numérique n'est pas obligatoire, mais son activation est importante, puisque pratiquement tous les sites web proposant des services publics - y compris ePortugal - ont adopté ce système d'authentification.

Depuis 2019, les citoyens peuvent également télécharger leur Permis de Conduire, leur Carte de Citoyen, ainsi que d'autres cartes sur une application de portefeuille d'identité numérique (ID.gov.pt) disponible sur téléphone portable.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Le gouvernement finance le projet d'identité numérique à 100 %.
> Les processus d'authentification et de signature numérique sont gratuits pour les citoyens, les résidents et les entreprises.
> Pas de frais pour les fournisseurs des secteurs public et privé, à l'exception des coûts des SMS OTP envoyés.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Mêmes exigences de sécurité pour la Carte de Citoyen et la Clé Mobile Numérique.
> La Carte de Citoyen et la Clé Mobile Numérique sont toutes deux notifiées eIDAS avec un niveau d'assurance élevé. Les fournisseurs de services définissent le niveau d'assurance de chaque application spécifique.
> Des audits annuels des plateformes d'identité numérique afin de maintenir leur qualification autorisant la délivrance de la signature numérique et de certificats qualifiés.
> Les principes de « Privacy by Design » sont appliqués. Les utilisateurs peuvent vérifier l'historique de leurs authentifications et signatures sur le site web Authenticao.gov.

ÉTAPES CLÉS DU PROJET

2007
Lancement de la Carte de Citoyen

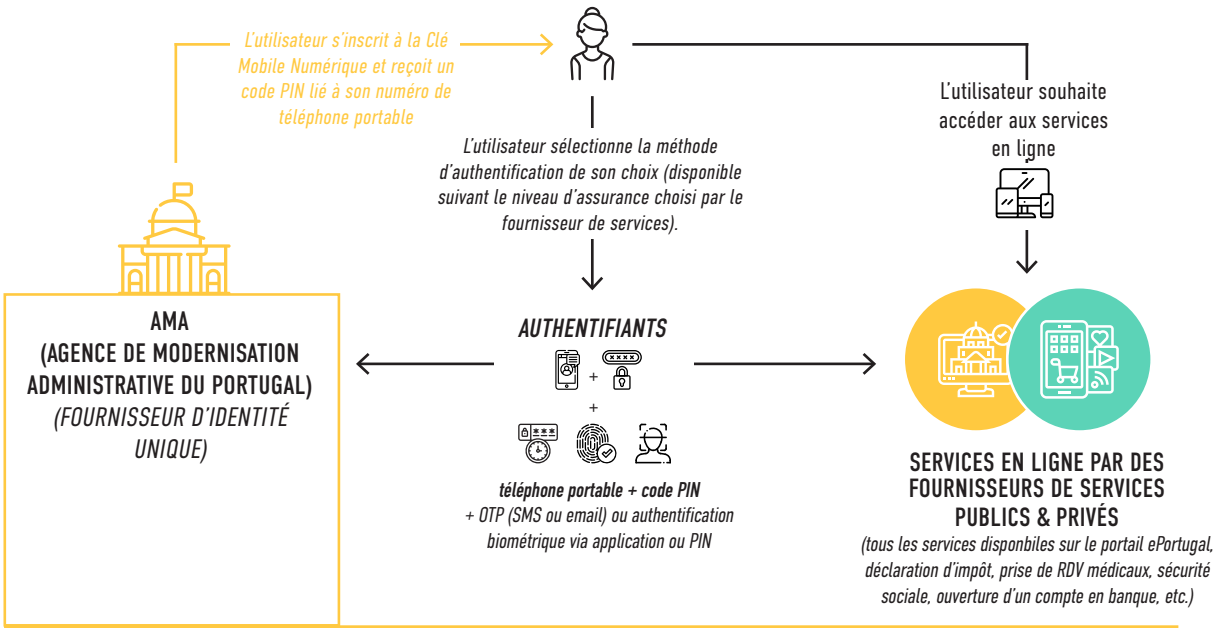
2014
Lancement de la Carte Mobile Numérique (CMD)

2018
160,000 utilisateurs actifs de la CMD.
Signature électronique qualifiée possible via CMD

2019
La Loi autorise la numérisation du Permis de Conduire, de la Carte de Citoyen et autres cartes sur l'application mobile de portefeuille d'identité numérique.

2020
1.5M d'utilisateurs actifs (2M de comptes créés)
Environ 4,000 inscirptions à la CMD par jour.

CLÉ MOBILE NUMÉRIQUE - ÉCOSYSTÈME



CADRE JURIDIQUE

> L'autorité publique du GNS (Gabinete Nacional de Segurança – National Security Office) est responsable de la sécurité.
> Il existe deux organismes de sécurité nationale : GNS and CNCS (Centro Nacional de Cibersegurança - National Cybersecurity Centre)
> Pour la protection de la vie privée, l'autorité CNPD (Commission Nationale de Protection des Données) se rapporte au Parlement

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

ÉCOSYSTÈME & GOUVERNANCE

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

> Un système d'identité mobile inclusif et fortement centré sur l'utilisateur, offrant simplicité et commodité à tous les citoyens et résidents (pas seulement par smartphones - la CMD est liée à un numéro de téléphone) sans négliger le niveau de sécurité. L'option de la biométrie comme facteur d'authentification pour remplacer le mot de passe OTP augmente également l'ergonomie de la solution. Le gouvernement Portugais continue de mettre l'utilisateur au centre de ses intentions - ses 600 commerces du citoyen (comptoirs physiques avec assistance d'un médiateur compétent) avaient déjà marqué les esprits, tout comme le récent chatot SIGMA offrant son aide en ligne aux citoyens.

MISE EN OEUVRE TECHNOLOGIQUE

MISE SUR LE MARCHÉ & PROMOTION

> Canaux multiples pour l'inscription à la Clé Mobile Numérique (CMD) : un grand bon a été fait lorsque l'AMA a décidé de créer plusieurs canaux d'inscription.
En plus du traditionnel face à face ou en utilisant la Carte de Citoyen électronique avec un lecteur de carte à puce, deux nouveaux canaux sont désormais disponibles:
> S'inscrire à la CMD lors du renouvellement de la Carte de Citoyen
> S'inscrire à la CMD lors de l'utilisation du mot de passe lié au service des impôts. Les codes sont envoyés par courrier à l'adresse liée au citoyen.
> L'AMA réfléchit également à permettre aux utilisateurs de s'inscrire à la CMD sur les distributeurs automatiques de billets, ou alors via la biométrie sur téléphone portable.

5,6 MILLIONS D'HABITANTS

95-50% TAUX D'ADOPTION (SINGPASS / ID MOBILE)

IDENTITÉ NUMÉRIQUE NATIONALE

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

FACTEURS D'AUTHENTIFICATION MULTIPLES
y compris identité mobile cryptographique via une application, reconnaissance faciale via le Cloud (physique et à distance), PIN et mots de passe

EN ACTION DEPUIS 2003

IDENTIFICATION *en ligne & hors ligne*
"Verify with SingPass" permet à l'utilisateur de procéder à une vérification d'identité sécurisée en face à face et à un transfert de données par scan de code QR ou NFC.

PARTAGE D'ATTRIBUTS D'IDENTITÉ
Adoption de principes de protection des données, comme la spécificité de l'objet, l'accès basé sur le consentement et le partage des données et la minimisation des données

AUTHENTIFICATION
SingPass et SingPass mobile utilisent une authentification unique securisée (single sign-on) pour les services du gouvernement.

SIGNATURE ÉLECTRONIQUE
Signature numérique via scan de code QR lancée en Octobre 2020.

RECONNAISSANCE TRANSFRONTALIÈRE
Des discussions sont en cours entre plusieurs pays afin d'envisager des projets pilotes bilatéraux.

+1000 services gouvernementaux *sont connectés à SingPass*

+300 services *sont connectés à CorpPass*

+100 services en ligne *s'appuient sur MyInfo Business*

CONTEXTE & OBJECTIFS

Depuis 2003, les Singapouriens utilisent SingPass pour accéder aux services publics en ligne. Avec l'augmentation du nombre de transactions en ligne, l'Agence Gouvernementale de Technologie de Singapour (GovTech) est en train de transformer SingPass en un programme d'Identité Numérique Nationale (NDI). L'objectif est de fournir un service de gouvernement-plateforme pour les utilisateurs et les entreprises, grâce à un programme d'identité numérique universel servant à effectuer des transactions avec le gouvernement et le secteur privé de manière plus sûre et transparente.

La plateforme d'Identité Numérique Nationale (NDI) a été introduite progressivement depuis 2017, permettant aux secteurs privé et public de développer davantage de services à valeur ajoutée sur cette plateforme de confiance commune et universelle.

PROPOSITION DE VALEUR

Le projet rassemble divers outils numériques offrant un plus grand confort et une meilleure sécurité transactionnelle en ligne. Du côté des consommateurs, le principal produit disponible est SingPass Mobile. Du côté des entreprises, les principaux produits sont :
> Login with SingPass, service d'authentification auquel les entreprises peuvent s'abonner.
> MyInfo / MyInfo Business, plateforme de données où les citoyens/entreprises peuvent donner leur consentement aux entreprises qui récupèrent des données auprès de sources gouvernementales
> Verify with SingPass, service de vérification d'identité en personne.
> SingPass Face Verification, service de vérification d'identité par biométrie faciale.
> Sign with SingPass, permettant la signature crypto numérique sécurisée.
L'écosystème du NDI présente plusieurs avantages : pour les citoyens et les résidents, il fournit une identité numérique unique plus sécurisée, plus efficace, et avec une meilleure expérience utilisateur.
Pour les entreprises, la plateforme NDI offre notamment une plus grande sécurité ou encore une meilleure expérience utilisateur pour les clients et les employés. Elles sont également encouragées à tirer parti de la plateforme NDI en utilisant des fonctionnalités telles que la signature numérique afin de créer des services à valeur ajoutée.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> La NDI est entièrement financée par le gouvernement, qui en a la propriété.
> Gratuit pour les citoyens et les entreprises pendant la période initiale d'adoption. Des modèles de Freemium sont en cours d'exploration pour l'avenir.
> Les entreprises ont déclaré des économies de plus de $50 par transaction et une réduction de 80 % du temps de transaction quand leurs clients utilisent MyInfo pour pré-remplir des formulaires avec des informations provenant de sources gouvernementales. Les entreprises signalent également un taux d'approbation des transactions jusqu'à 15% plus élevé en raison de la meilleure qualité des données saisies avec MyInfo.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> La gouvernance de la cybersécurité est dirigée par l'Agence de Cybersécurité de Singapour (« Cybersecurity Agency of Singapore ») (CSA).
> Adoption d'une approche de sécurité «by-Design» pour assurer la conception de la sécurité, l'assurance et les tests à chaque étape du développement et de l'exploitation du produit.
> Possibilité d'effectuer une authentification renforcée - à plusieurs facteurs - pour les transactions jugées plus sensibles.
> Pour la Vérification faciale, aucune donnée personnelle n'est partagée avec les parties utilisatrices ; seul un résultat de correspondance sera retourné après le test de correspondance. Ce service supprime la charge que représentent pour les entreprises la collecte, le stockage et la protection des données.

ÉTAPES CLÉS DU PROJET

2003
Lancement de SingPass

2015
Lancement de nouvelle version SingPass avec plusieurs facteurs d'authentification, améliorations UX

2016
3,3M d'utilisateurs (66% de la population)
57M transactions
350 e-services et 64 Agences du Gov connectées

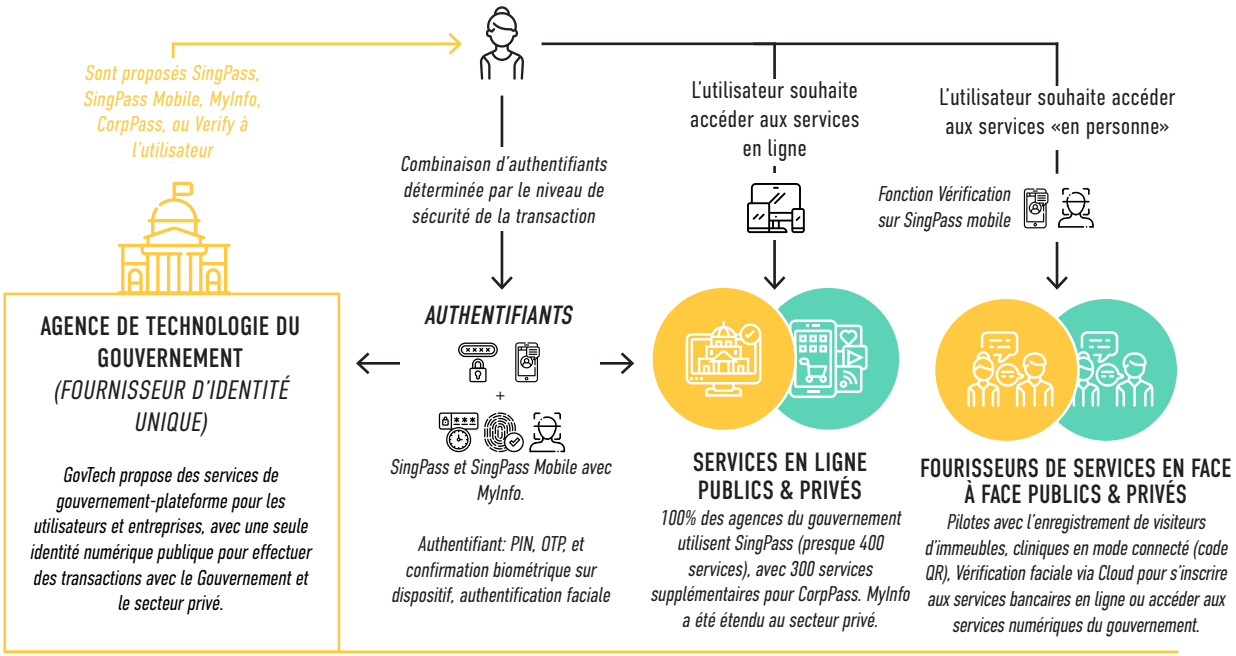
2017
Lancement du programme NDI
Lancement pilote de MyInfo avec le secteur bancaire

2018
Lancement de l'app SingPass Mobile. 100% des agences du gov utilisent SingPass.

2019
Lancement des pilotes pour Verify with SingPass et Notify

2020
4M de citoyens utilisent SingPass (95% des utilisateurs éligibles). 2.2M utilisateurs pour SingPass Mobile.
Lancement du pilote pour SingPass Face verification et Sign with SingPass

IDENTITÉ NUMÉRIQUE NDI - ÉCOSYSTÈME



CADRE JURIDIQUE

> Loi sur la Protection des Données Personnelles
> Loi sur la Gouvernance du Secteur Public
> Loi sur les Transactions Électroniques
> Loi sur l'Enregistrement Civil National
> Loi sur l'Utilisation Abusive de l'Ordinateur

APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

> Un accès sûr et pratique aux services privés et ceux du gouvernement
> Un accès aux données personnelles et un contrôle sur le partage des données en donnant son consentement lors de transactions via services numériques, tant en ligne que dans un cadre physique. Cela apporte plus de transparence, et permet un gain de temps et d'argent.

ÉCOSYSTÈME & GOUVERNANCE

> Une équipe d'ingénieurs en interne permettant l'innovation et des réponses plus rapides, surtout durant une crise comme celle de la COVID-19.

MISE EN OEUVRE TECHNOLOGIQUE

Vérification de l'identité en comparant le visage à une image stockée dans une base de données gouvernementale. La reconnaissance faciale sera disponible pour les services du gouvernement et des entreprises. Ceux-ci devront se conformer aux exigences de gouvernance, comme celle de demander obligatoirement le consentement de la personne avant de procéder à la vérification de son visage.

MISE SUR LE MARCHÉ & PROMOTION

> Une stratégie de communication holistique déployée pour favoriser l'adoption par les citoyens, peu importe leur niveau de connaissances technologiques.
> Exploitation de diverses plateformes d'engagement présentes dans l'industrie, à la fois en ligne et physiques, pour favoriser l'adoption des entreprises
> Portail de développeurs et partenaires permettant aux entreprises de s'intégrer facilement à la plateforme nationale d'identité
> Se préintègre avec les solutions et plateformes du secteur privé existantes telles qu'Adobe Sign, DocuSign et autres.

SOLUTIONS MVD

5,8 MILLIONS DE CONDUCTEURS

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

APPLICATION MOBILE ET NAVIGATEUR WEB *AVEC RECONNAISSANCE FACIALE, OTP VOCAL, KBA*

EN ACTION DEPUIS **2020**
pour portail en ligne

IDENTIFICATION *en ligne & hors ligne*
Identification en face à face disponible début 2020 via l'application de Permis de Conduire numérique.

PARTAGE D'ATTRIBUTS D'IDENTITÉ
Les permis de conduire mobile permettent le partage des attributs requis à l'accès à un service.

AUTHENTIFICATION
Authentification sur le site internet de l'ADOT pour accéder à une large gamme de services en ligne. Ouverture de la plateforme à d'autres services publics et privées prévue sur la feuille de route.

SIGNATURE ÉLECTRONIQUE
La MDV accèpte les signatures électroniques sur tous les documents si elles sont authentifiées par connexion sur le portail et sont effectuées sur celui-ci.

RECONNAISSANCE TRANSFRONTALIÈRE

40 services MVD
disponibles sur le portail

CONTEXTE & OBJECTIFS

Dans un pays où le permis de conduire est la preuve d'identité la plus utilisée, le Ministère des Transports de l'Arizona (ADOT) a été un pionnier dans la fourniture de services en ligne innovants à ses clients. Actuellement, 65 % des renouvellements d'immatriculation de l'État se font sur son site web, un taux beaucoup plus élevé que dans la plupart des autres États.

En 2018, l'agence a lancé un nouveau portail pour les consommateurs, AZ MVD Now, avec des fonctions innovantes d'authentification à plusieurs facteurs, dont une application mobile destinée à l'authentification.
La prochaine étape pour le MVD (Motor Vehicle Division) est de passer à une application numérique mobile entièrement déployée en 2021. Elle permettra de délivrer en toute sécurité des titres d'identité publics (permis de conduire, carte d'identité avec photo) au format numérique. Ensuite, l'objectif du MVD est d'étendre le Super Portail eAZ Identity, qui permettra aux citoyens de l'Arizona d'accéder à des services en ligne d'autres organismes publics participants d'Arizona.

PROPOSITION DE VALEUR

Le portail AZ MVD Now permet aux citoyens de l'Arizona l'accès à la plupart des services MVD (renouvellement du permis de conduire, immatriculation des véhicules, etc.) en libre-service, sans avoir à se rendre dans une agence MVD.

Dans les années à venir, la stratégie de MVD est d'étendre les capacités d'identité du permis de conduire au-delà du simple droit de conduire grâce au Super Portail eAZ Identity. Les premiers pilotes ont intégrés plusieurs agences publiques pour des cas d'usage tels que l'enregistrement d'animaux de compagnie, les permis d'élimination des déchets dangereux ou le système de déclaration de financements de campagnes.
La démocratisation de la vérification d'identité dans l'État d'Arizona ouvrira la voie à l'utilisation généralisée de l'identité numérique, surtout pour l'immatriculation des entreprises qui est complexe en Arizona. Les candidats doivent en effet passer par un long processus et remplir des formulaires pour environ 7 organismes d'État. Le super-portail AZ Identity devrait faciliter ce processus et stimuler le dynamisme de l'économie.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Actuellement gratuit pour les citoyens.
> À l'avenir, des outils seront disponibles gratuitement pour les parties utilisatrices comme les entreprises.
> Au total, un investissement de 60 millions de dollars par l'ADOT depuis 2015 pour la refonte de leur système informatique, y compris le portail en ligne et la mise en place d'une identité mobile.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Pour assurer un niveau de sécurité optimal sans dégrader l'expérience utilisateur, le Ministère des Transports a mis en place un processus d'enregistrement simple et adaptable. L'agence n'exige que des informations basiques, posant des questions simples à ses utilisateurs. Des vérifications sont ensuite menées sur le dispositif et la connexion, entre autres facteurs. Après avoir attribué une note aux utilisateurs, ils décident quels authentificateurs seront nécessaires pour accéder au service, avec, par exemple, la reconnaissance faciale sur application mobile ou navigateur web.

Bien que chaque connexion soit évaluée, la création initiale du compte (l'inscription) et certaines autres transactions spécifiques et sensibles, notamment le remboursement des fonds et le transfert de propriété, sont plus surveillées que d'autres et peuvent nécessiter des actions d'authentification supplémentaires de la part du client.

ÉTAPES CLÉS DU PROJET

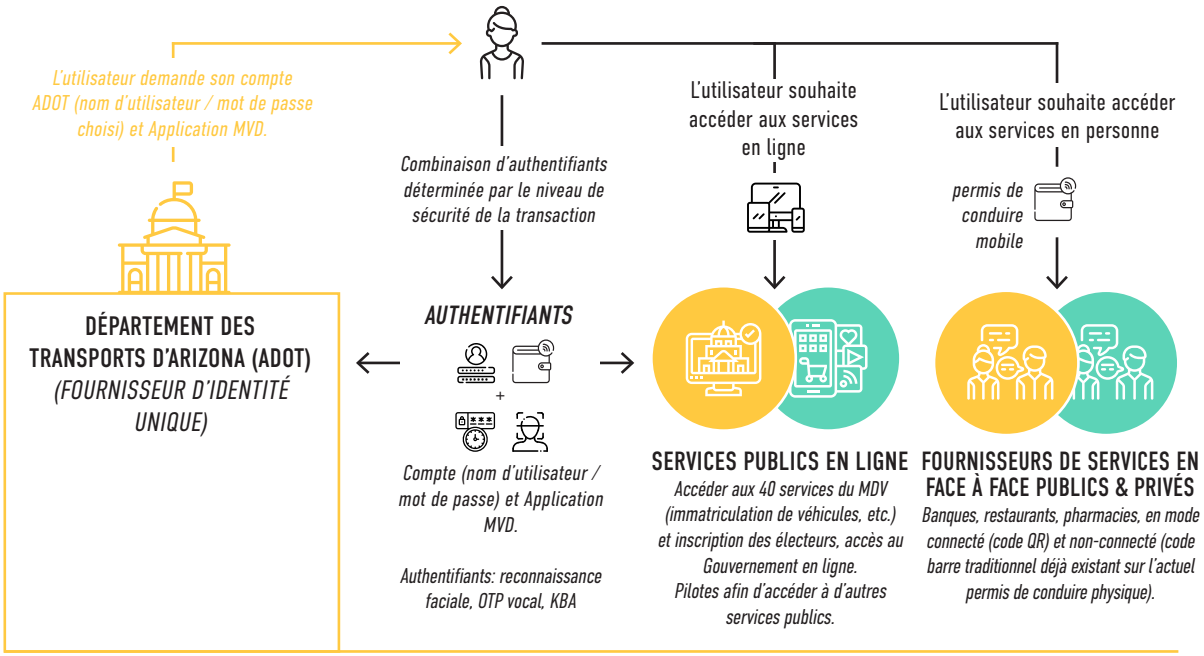
2018
Lancement du portail en ligne AZ MVD Now.

April 2020
Lancement de la plateforme.
200.000 comptes enregistrés sur le portail AZ MVD Now.

November 2020
1.5m comptes créés - ils n'ont pas tous l'application.

2021
Nouvelle version du permis de conduire mobile.

IDENTITÉ NUMÉRIQUE ADOT - ÉCOSYSTÈME



APPROCHE INNOVANTE DE L'IDENTITE NUMÉRIQUE EN TERMES DE...

> Un organisme spécifique pour s'appuyer sur la meilleure expertise tout en conservant la propriété intellectuelle des solutions développées : Il peut être difficile d'avoir la bonne ressource en interne car les projets de transformation nécessitent une expertise spécifique. Pour construire leurs solutions comme projets internes, l'ADOT a externalisé l'expertise (mais pas le contrat) et a engagé 60 à 70 prestataires individuels. Ils ont donc l'entière propriété intellectuelle, sont propriétaires des solutions et bénéficient de plus de flexibilité et de contrôle sur la gestion de projet.

ÉCOSYSTÈME & GOUVERNANCE

MISE EN OEUVRE TECHNOLOGIQUE

> Reconnaissance faciale sur navigateur Internet permettant l'accès au service en ligne pour une méthode d'authentification renforcée.

PROPOSITION DE VALEUR POUR L'UTILISATEUR FINAL

MISE SUR LE MARCHÉ & PROMOTION

LES PAYS SUIVANT N'ONT PAS FAIT L'OBJET D'ENTRETIENS INDIVIDUALISÉS. LES PROGRAMMES D'IDENTITÉ NUMÉRIQUE DÉCRITS SONT LE RÉSULTAT DE RECHERCHES DOCUMENTAIRES ET D' EXPÉRIENCES MENÉES PAR LES ÉQUIPES DE ONEPOINT ET DE LA SIA.

ITSME®

11,46 MILLIONS D'HABITANTS
20% TAUX D'ADOPTION

DIRIGÉ PAR PLUSIEURS INDUSTRIES (BANQUES ET OPÉRATEURS DE TÉLÉPHONIE MOBILE)

PROGRAMME FÉDÉRÉ

APP MOBILE ancré dans les application de banques en ligne

EN ACTION DEPUIS **2017**

IDENTIFICATION *seulement en ligne*
Identification en ligne pour la création d'un nouveau compte ou pour appliquer un procédé «Know-Your-Customer» (Carte d'Identité électronique et Itsme)

PARTAGE D'ATTRIBUTS D'IDENTITÉ

AUTHENTIFICATION
Permet aux utilisateurs de se connecter en utlisant Itsme et Carte d'ID électronique Belge.

NOTIFICATION EIDAS (ÉLEVÉE) POUR LA CARTE D'ID. ÉLECTRONIQUE ET APP ITSME

SIGNATURE ÉLECTRONIQUE
Signature Électronique Qualifiée avec Carte d'Identité électronique (règlement eIDAS) largement utilisée dans la sphère professionnelle.

RECONNAISSANCE TRANSFRONTALIÈRE
Itsme sera bientôt testé au Luxemburg avec l'ambition de toucher d'autre marchés de l'UE.

700+ SERVICES EN LIGNE PUBLICS ET PRIVÉS ACCESSIBLES SUR ITSME®

34% des accès sont pour les services gouvernementaux
66% des accès sont pour les services privés

CADRE NATIONAL DE RÉGULATION : DÉCRET ROYAL SUR L'IDENTITÉ NUMÉRIQUE EN 2004 - LOI SUR L'ACCÈS AUX DONNÉES PERSONNELLES EN 2012.

CONTEXTE & OBJECTIFS

Itsme a été créé et est détenu par un consortium privé (Identité Mobile de Belgique) composé de quatre banques et de trois opérateurs de réseaux mobiles. Il a pour but d'offrir une solution d'identité mobile unique qui serait utilisée pour sécuriser l'accès à leurs propres services, augmenter la satisfaction des utilisateurs et monétiser la solution de sécurité pour les fournisseurs de services tiers.

En janvier 2018, le gouvernement belge a reconnu itsme comme identité numérique officielle pour sécuriser l'accès aux services publics et l'a donc fait notifier par la Commission Européenne, entraînant une reconnaissance transfrontalière.

PROPOSITION DE VALEUR

L'application mobile Itsme complète le programme d'identité numérique existant, qui s'appuie sur la carte d'identité électronique. Elle apporte un nouveau niveau de commodité nécessaire, et répond à la demande de mobilité.
Itsme s'articule autour d'une application mobile intuitive permettant un moyen d'identification portable et omniprésent, soutenu par un code secret à cinq chiffres ou un scan d'empreintes digitales. Il permet ainsi de résoudre de nombreux problèmes qui compromettent actuellement l'expérience utilisateurs dans les domaines numériques, comme la fatigue des mots de passe, la vulnérabilité aux cyber-attaques et le manque de contrôle sur les informations personnelles.

Pour les fournisseurs de services, le programme permet un procédé KYC simple, ainsi qu'une inscription des utilisateurs basée sur des données d'identité vérifiées et exactes à 100 %. Ils bénéficient également de solutions de sécurité haut de gamme pour leurs services en ligne à une fraction du coût et ne paient qu'en fonction du volume d'utilisateurs, du type de transactions et du niveau de services (identification, authentification, signature numérique). Plus de 140 fournisseurs de services privés ont adhéré au programme afin d'utiliser Itsme pour sécuriser leurs activités en ligne.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE SECTEUR PRIVÉ

> Le consortium "Identité Mobile de Belgique" a lancé et exploite l'identité mobile Itsme.
> Le programme s'appuie sur des principes de protection de la vie privée sans monétisation des données.
> Itsme est gratuit pour les citoyens. Les fournisseurs de services supportent les coûts avec un plan personnalisé pour répondre à chaque besoin. Un coût par transaction a d'abord été testé, puis abandonné car cela dissuadait de s'engager. Il a été remplacée par un modèle d'abonnement annuel basé sur le volume d'utilisateurs et le type de services (connexion simple, contrôle complet avec données vérifiées, tout numérique y compris l'approbation de transactions).

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Respect stricte de la PSD2, la RGPD et eIDAS, certifié ISO/IEC 2700.
> Itsme permet à l'utilisateur final de créer un compte sans partage de données d'identité, ou de lier un compte existant à itsme.
> L'inscription à Itsme peut se faire par la lecture en ligne de la carte d'identité électronique ou via une identité vérifiée provenant des banques et opérateurs de téléphonie mobile.

ÉTAPES CLÉS DU PROJET

2002
Déploiement de la Carte Nationale d'Identité électronique : La Belgique est pionnière dans les système de gouvernement numérique.

2017
100% de la population possède la carte nationale d'identité électronique.

2017
Le Consortium Belge pour l'identité mobile lance l'application mobile Itsme.

2018
400.000 utilisateurs Itsme. La carte d'identité électronique est reconnue par e-IDAS au niveau d'assurance élevé

2020
Itsme et FAS (Service Fédéral d'Authentification du Gouvernement Belge) notifié par la Comission Européenne. 2 Millions d'utilisateurs Itsme en Juin 2020. Plus de 8 millions de transactions itsme effectuées chaque mois.

210 MILLIONS D'HABITANTS

APPLICATION PORTEFEUILLE D'IDENTITÉ CPF

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT	APPLICATION DE PORTEFEUILLE NUMÉRIQUE AVEC AUTHENTIFICATION BIOMÉTRIQUE	EN ACTION DEPUIS 2020

✓ IDENTIFICATION *en ligne & hors ligne*	○ PARTAGE D'ATTRIBUTS D'IDENTITÉ	✓ AUTHENTIFICATION *par biométrie (reconnaissance faciale)*	○ SIGNATURE ÉLECTRONIQUE	○ RECONNAISSANCE TRANSFRONTALIÈRE

CONTEXTE & OBJECTIFS

Le programme national d'identité numérique du Brésil (« Identificaçao Civil Nacional » - ICN) a été annoncé par le gouvernement en 2017. Le Tribunal électoral Supérieur (TSE) du Brésil gère ce programme qui a été spécialement conçu pour réduire la fraude électorale et la fraude des électeurs.

Il comprend la centralisation de toutes les données biométriques (photos et empreintes digitales) collectées lors des élections dans les 27 états différents et provenant de l'IRS (« Registre Individuel du Contribuable »), dans une **base de données nationale biométriques et centralisée.**

Le projet est mené par le gouvernement, avec l'intention de privatiser diverses entreprises technologiques publiques contribuant au développement de l'identité numérique :
- Serpro, le service fédéral de traitement des données, qui a développé l'application d'identité numérique,
- Dataprev, une entreprise de technologie de la sécurité sociale,
- L'entreprise brésilienne de télécommunications Vivo, chargée de l'enregistrement biométrique pour le pays.

En parallèle, la stratégie de gouvernement numérique du pays (2020-2022) consolidera et rassemblera 1500 sites internet publics en un seul portail. Il s'attend à une plus grande adoption du cloud et un accès plus large aux données ouvertes du gouvernement.
En 2020, **le gouvernement brésilien a lancé une nouvelle application (L'Application de Portefeuille Numérique CPF) qui réunit la carte de sécurité sociale et le permis de conduire.** L'objectif est de proposer les documents les plus utilisés, comme la carte d'identité ou le certificat de naissance, dans une seule application.

PROPOSITION DE VALEUR

Les versions numériques des documents sont disponibles sur la nouvelle application de portefeuille numérique CPF et sont validées par un Code QR. L'application permet aux citoyens d'accéder à plusieurs services liés à leur CPF via le Service Fédéral des Impôts, le Ministère de l'Économie et le Gouvernement Fédéral. Depuis 2019, les Brésiliens peuvent accéder aux services publics en utilisant leur numéro de sécurité sociale.

L'inscription se fait sur l'application mobile en utilisant la biométrie et en effectuant un contrôle de validation en personne auprès d'un agent du gouvernement dans des lieux dédiés.
Seuls les pouvoirs publics (pouvoirs Exécutif et Législatif de l'Union, des États, du District Fédéral et des Municipalités) ont accès à la base de données ICN. Ils peuvent créer leur propre base de données à partir du contenu de l'ICN (à l'exception de la biométrie).

AUTRES SERVICES SPÉCIFIQUES ET CAS D'USAGE :
> Accès au programme d'aide d'urgence pour les citoyens financièrement vulnérables.
> Comprend un chatbot pour aider à soumettre la déclaration annuelle d'impôt sur le revenu.

ÉTAPES CLÉS DU PROJET

2008	2017	2019	2020	2022
Déut de l'enregistrement biométrique des électeurs	Mise en place du cadre légal pour le programme d'identité numérique national	Environ 50% des Brésiliens sont enregistrés de manière biométrique	Finalisation de la mise en oeuvre du programme d'identité numérique	Objectif: 40 millions d'identités numériques attribuées

AADHAAR

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT	NUMÉRO AADHAAR (à 12 chiffres) et biométrie	EN ACTION DEPUIS 2010

IDENTIFICATION *en ligne & hors ligne*

PARTAGE D'ATTRIBUTS D'IDENTITÉ

Le eKYC est sans papier, privé, basé sur le consentement, non répudiable et instantané. Par conséquent, des données CDD (Customer Due Diligence) / vigileance à l'égard de la clientèle) précises et fiables sont partagées avec l'entité déclarante en temps réel.

AUTHENTIFICATION

> L'authentification se fait à l'aide du numéro et de la biométrie (généralement une empreinte digitale), avec un dispositif de Point de Vente (POS).
> Les banques et les opérateurs de réseaux de paiement ont intégré l'authentification Aadhaar dans des micro-DAB afin d'offrir des services bancaires sans guichet partout dans le pays, en temps réel, de manière évolutive et interopérable.

SIGNATURE ÉLECTRONIQUE

Basée sur une API ouverte, une nouvelle fonction de signature électronique est prévue afin d'éliminer les signatures manuelles. Une demande en ligne de signature électronique entraînera un contrôle eKYC sur la base de données Aadhaar, ainsi qu'une vérification de l'identité et de l'adresse via Aadhaar. L'authentification se fera soit par biométrie, soit par mot de passe à usage unique.

RECONNAISSANCE TRANSFRONTALIÈRE

CARDE: LA LOI AADHAAR, ADOPTÉE EN 2016 (7 ANS APRÈS LE LANCEMENT D'AADHAAR) PAR LA CHAMBRE BASSE DU PARLEMENT INDIEN LUI FOURNIT UN CADRE LÉGAL ET RÈGLEMENTAIRE.

CONTEXTE & OBJECTIFS

Aadhar est le plus grand programme d'État basé sur la biométrie au monde. Il a été créé dans un but d'inclusion par le gouvernement Indien afin de délivrer à chaque citoyen une identité qui lui permet d'accéder aux services de base, lui donnant ainsi les moyens de devenir un acteur économique. Aadhaar renforce l'inclusion sociale et financière ainsi que la dignité : chaque citoyen peut faire valoir ses droits.

Le programme est géré par l'UIDAI (l'Autorité Indienne relative à l'Identification Unique), une entité autonome qui dépend du Ministère de l'Électronique et des Technologies de l'Information.

PROPOSITION DE VALEUR

Aadhaar est une identité numérique sans justificatif d'identité physique. Après une inscription chargée de capturer les données biographiques et biométriques, l'UIDAI est mandatée pour délivrer à tous les résidents du pays un numéro aléatoire à 12 chiffres, facilement vérifiable, qui devient leur Identité Unique. Chaque citoyen reçoit un document contenant son numéro Aadhaar, dont les références peuvent être croisées avec les données biométriques contenues dans la base de données.

De nombreux services et transactions en ligne et hors ligne sont désormais accessibles, simplifiées et sûres grâce à Addhaar. Par exemple, l'accès aux aliments subventionnés dans les magasins de rationnement est désormais protégé : les demandes sont authentifiées par Aadhaar avec un système d'identité numérique à distance, plutôt que laissé à la discrétion des fonctionnaires locaux. Le programme a également contribué à la lutte contre le travail et le mariage des enfants, en fournissant une preuve d'âge.

MODÈLE ÉCONOMIQUE

> Initialement financé par le gouvernement, l'inscription et l'utilisation sont gratuites pour les citoyens.
> Les partenaires gérant les inscriptions sont engagés par le gouvernement à un coût fixe d'environ la moitié de 1$ US (à ce jour, plus de 300 millions de dollars US payés par le gouvernement à ces fins) alors que l'UIDAI fournit seulement les directives techniques obligatoires.
> Afin de garantir une adoption rapide par les parties utilisatrices, l'UIDAI a initialement maintenu les services d'authentification gratuits pour tous afin d'abaisser la barrière à l'entrée et n'a commencé à les facturer qu'en 2019. Depuis, les organisations privées doivent payer 0,007 USD pour l'authentification Aadhaar et 0,3 USD pour les transactions e-KYC. Les services publics restent quant à eux gratuits.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Les données sont cryptées et signées numériquement : toute modification rend la signature numérique invalide. Utilisation étendue de la PKI/HSM pour le cryptage des données pendant la transmission et le stockage, et pour la protection de l'accès à l'API.
> Seules les données KYC (les données démographiques et une photographie) sont partagées par l'UIDAI, après consentement de l'utilisateur - aucune donnée n'est transmise pendant le processus d'authentification : seule une réponse OUI/NON à la demande d'authentification est donnée aux fournisseurs de services. Les données biométriques ne sont jamais partagées avec qui que ce soit.
> Les citoyens peuvent accéder à leur historique d'authentification comprenant des journaux horodatés et signés numériquement de toutes les transactions. Ils peuvent les contester ou mettre à jour leurs informations en ligne.
> Il n'existe pas de loi exhaustive ni d'autorité indépendante pour la protection des données. Un projet de Loi sur la Protection des Données Personnelles est en discussion depuis des années.

ÉTAPES CLÉS DU PROJET

2009	2015	2016	2018	2019	2020
Création de l'UIDAI et lancement d'Aadhaar	L'UIDAI est rattachée au Ministère de l'Électronique et des Technologies de l'Information (au lieu de la Commission d'Aménagement)	Adoption de la Loi Aadhaar qui fournit un cadre légal et règlementaire	339M d'Aadhaar ont été liées à des comptes bancaires. 1.7 milliards de demandes d'authentification en 3 ans.	+27 milliards de demandes d'authentification. 1.2 milliards de numéros Aadhaar distribués.	95% des adultes possède Aadhaar, avec un taux de satisfaction de 92%.

EPARAKSTS

1.9 MILLIONS D'HABITANTS
40% TAUX D'ADOPTION

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

eParaksts mobile (sur app) + carte nat. d'identité électronique et carte à puce eParaksts

EN ACTION DEPUIS 2018

- IDENTIFICATION *en ligne*
- AUTHENTIFICATION
- PARTAGE D'ATTRIBUTS D'IDENTITÉ

eParaksts permet de ne fournir que des attributs spécifiques inscrits dans le registre (ex : l'âge de l'utilisateur) aux fournisseurs de services en ligne, qui doivent répondre à des conditions spécifiques afin de fournir le service.

- SIGNATURE ÉLECTRONIQUE
- RECONNAISSANCE TRANSFRONTALIÈRE

+90 **fournisseurs de services publics et privés** intégrés aux services eParaksts

NOTIFIÉ EIDAS DEPUIS 2019 POUR PLUSIEURS NIVEAUX D'ASSURANCE (DONT ÉLEVÉ) EN FONCTION DE LA SOLUTION CHOISIE.

CONTEXTE & OBJECTIFS

Afin de promouvoir l'utilisation de l'administration en ligne et de réduire les frais générés par les documents et services physiques, le gouvernement letton a lancé sa première carte d'identité électronique incluant la signature électronique en 2012. Elle est actuellement facultative mais deviendra obligatoire en 2023.
En 2018, le Centre National de Radio et de Télévision (LVRTC) du pays, un fournisseur national de services de confiance, a lancé eParaksts :
Des services de Signature Cloud Qualifiée permettant aux utilisateurs de s'authentifier de manière sécurisée et d'utiliser une signature électronique qualifiée (QeS) à partir d'appareils mobiles, éliminant ainsi la nécessité d'une connectivité physique par carte à puce.

PROPOSITION DE VALEUR

Avec les solutions eParaksts, les utilisateurs peuvent accéder à des services publics et privés en ligne. Comme elles comprennent une QeS, il est possible d'envoyer des demandes signées - même pour des services hors ligne comme des certificats ou autres documents légaux.
L'application eParaksts mobile (fonctionnant sur Smartphone iOS et Android) permet aux particuliers de signer électroniquement des documents, de s'identifier et de s'authentifier sur divers portails en libre-service pour les institutions et les entreprises : services municipaux, gestion de logement, prestataires de services médicaux, assurance, etc.
Les utilisateurs peuvent toujours utiliser leur carte d'identité électronique ou eParaksts pour accéder à des services en ligne et signer numériquement des documents, mais cela nécessite des lecteurs de cartes à puce ainsi qu'un logiciel informatique gratuit eParakstītājs.

Les solutions eParaksts ont rendu quasi obsolète la nécessité de se rendre dans un lieu dédié pour accéder à un service. Elles sont devenus essentielles au maintien de l'activité des entreprises et du Parlement pendant l'épidémie de COVID-19.

Le processus d'inscription à eParaksts mobile peut se faire à distance avec une carte d'identité électronique (ou carte eParaksts) ou en personne par le biais d'un coursier pour les personnes qui ne peuvent pas utiliser de carte d'identité numérique ou de carte à puce. Cette dernière solution s'appuie sur une authentification par lien bancaire. Pour faciliter l'inscription à eParaksts, l'État letton parraine les services de coursier. En 2021, 116 notaires nommés par l'État deviendront des Autorités d'Enregistrement. Six mois après le lancement, les notaires factureront aux clients une redevance unique pour couvrir le coût du service d'inscription.
Le LVRTC délivre également des certificats de sceau électronique sur les cartes ou les logiciels des organisations. Le LVRTC facilite l'intégration de ses solutions pour les entreprises en organisant des démonstrations destinées à présenter les APIs disponibles aux intégrateurs de systèmes. L'intégration des APIs ne prend que quelques minutes.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Le gouvernement a entièrement financé le programme d'identité numérique.
> La carte d'identité numérique et les solutions eParaksts sont gratuites pour les utilisateurs finaux (à l'exception des frais d'inscription via les notaires à partir de la mi-2021).
> eParaksts est gratuit pour les fournisseurs de services privés et publics, y compris les solutions d'APIs intégrées prêtes à l'emploi (sauf pour les services qui ne font pas partie du Programme d'Identification Nationale, tels que les qSeals, le site internet qAuthCert et les certificats NQC).

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Niveau d'assurance élevé pour la carte nationale d'identité électronique, la carte à puce eParaksts et l'application eParaksts mobile
> Niveau d'Assurance substanciel pour les modèles de smartphones non pris en charge
> Certificats qSeals, qAuth Websites

ÉTAPES CLÉS DU PROJET

2012 — Lancement de la carte nat. d'identité électronique, avec e-signature

2018 — Lancement des solutions eParaksts Service des impôts,portail d'État et 68 services publics en ligne intégrés à eParaksts en Mars.

2019 — Notification eIDAS pour le programme d'identité numérique national

2020 — Amélioration d'eParaksts au niveau QeS

2021 — Lancement de la nouvelle application apportant plus de fonctionnalités et une meilleure expérience utilisateur

2023 — La carte d'identité électronique devient obligatoire pour les citoyens Lettons.

OMANUNA

2,8 MILLIONS D'HABITANTS
100% DE LA POPULATION EST ÉQUIPÉE

SYSTÈME CENTRALISÉ DIRIGÉ PAR LE GOUVERNEMENT

CARTE EID + ID MOBILE (VIA SIM)

EN ACTION DEPUIS 2014

IDENTIFICATION *en ligne & hors ligne*

Identification hors ligne seulement par lecture de carte d'identité électronique et correspondance avec l'identification par carte

PARTAGE D'ATTRIBUTS D'IDENTITÉ

61 fournisseurs de services publics et privés disponibles

AUTHENTIFICATION

Authentification à deux facteurs via une approche multi-modale (carte d'identité électronique ou identité mobile). Niveau d'assurance le plus élevé, conformément aux normes US NIST - atteint le niveau élevé de eIDAS (UE).

SIGNATURE ÉLECTRONIQUE

Signature Électronique Qualifiée (QeS), atteignant le niveau le plus élevé de la signature électronique à valeur légale. Utilisée par toutes les parties prenantes (citoyens, résidents, entreprises et fonctionnaires).

RECONNAISSANCE TRANSFRONTALIÈRE

CADRE : LOI SUR LES TRANSACTIONS ÉLECTRONIQUES (2008) PASSÉE PAR DÉCRET - DÉFINIT LE CADRE LÉGAL DU PROGRAMME D'IDENTITÉ NUMÉRIQUE DONNE VALEUR LÉGALE À LA SIGNATURE ÉLECTRONIQUE

CONTEXTE & OBJECTIFS

Pour mettre en place son programme national d'identité numérique, l'ITA (Autorité de l'Information & Technologie) était prête à s'appuyer sur les cartes d'identité et de résident électroniques déjà en circulation, ainsi qu'à profiter de la forte pénétration des téléphones portables à Oman (189%) pour lancer une identité mobile accompagnant ces cartes. Oman a été le tout premier pays du Moyen-Orient à compléter sa carte nationale d'identité électronique d'un système d'identité mobile - pour plus de commodité. Tout le monde est équipé et la solution est totalement inclusive, s'adressant à tout profil d'utilisateur.

Au total, 61 entités différentes ont rejoint le programme à succès, dont des banques, opérateurs de téléphonie mobile, ainsi que des entités publiques de tous niveaux (Ministères, Municipalités et Chambres de Commerce), afin de mettre en place un puissant système informatique centralisé. Un accord avec les opérateurs de réseaux mobiles a été signé pour gérer l'inscription des citoyens sur l'identité mobile nationale.

Omanuna est une initiative publique dont l'ambition est de
> Lisser la prestation des services publics
> Accroître l'efficacité et la satisfaction des citoyens
> Améliorer les interactions Goverment-2-Consumer
> Réduire les coûts opérationnels en mutualisant les coûts de sécurité des services publics en ligne et de gestion des accès.

PROPOSITION DE VALEUR

Les citoyens et les entreprises d'Oman peuvent accéder de manière fluide aux services en ligne publics et privés, communiquer avec les autorités publiques par le biais d'une interface simple d'utilisation, et signer des formulaires à valeur légale sans avoir à se rendre physiquement dans des lieux dédiés. Cela représente un gain de temps et d'énergie.
Les prestations du service public sont optimisées - les utilisateurs peuvent se connecter en toute sécurité au portail du gouvernement Omanuna en utilisant soit leur carte nationale d'identité/de résidence électronique avec un lecteur de carte à puce connecté à un PC et un code PIN, soit en utilisant simplement leur application d'identité mobile pour s'authentifier et signer en ligne.

Les principaux services en ligne utilisés par les citoyens, résidents et entreprises d'Oman sont : l'enregistrement d'une entreprise, la prise de rendez-vous médicaux, les formalités privées, les permis de construire, l'enregistrement de plaintes, la candidature d'emploi, etc.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Le gouvernement a entièrement financé le programme d'identité numérique afin de soutenir au mieux la transformation numérique du pays.
> Gratuit pour l'utilisateur final et pour les prestataires de services publics souhaitant l'utiliser pour sécuriser leurs services en ligne.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Oman a opté pour le plus haut niveau de sécurité et atteint le niveau 3 d'Assurance d'Identification (IAL3) pour son inscription ainsi que le niveau 3 d'assurance d'authentification (AAL3) pour son accès, selon les normes NIST.
> S'appuyant sur les élements sécurisés (carte à puce et carte SIM), les programmes d'identité numérique d'Oman atteignent également le niveau élevé de l'e-IDAS de l'UE.

ÉTAPES CLÉS DU PROJET

2002
e Registre National centralise la base de données des citoyens

2003
Déploiement des cartes d'identité électroniques

2008
Loi sur les transactions électroniques

2009
Lancement du portail de services publics en ligne d'Oman

2011
Service d'authentification des électeurs ajouté à la carte d'identité électronique

2014
Lancement du programme d'identité numérique et de la plateforme IDP avec carte d'eID et ID Mobile pour sécuriser les transactions en ligne

GOV.UK VERIFY

66,65 MILLIONS D'HABITANTS
7,4M D'UTILISATEURS

MENÉ PAR LE GOUVERNEMENT
(bientôt mené par le secteur privé)

PROGRAMME FÉDÉRÉ

Titres d'identité et procédés d'authentification dépendent de l'IDP : authentification à 2 facteurs avec la plupart des IDPs, par téléphone portable

EN ACTION DEPUIS 2014

- ○ IDENTIFICATION
- ✓ PARTAGE D'ATTRIBUTS D'IDENTITÉ
- ✓ AUTHENTIFICATION
- ○ SIGNATURE ÉLECTRONIQUE
- ✓ RECONNAISSANCE TRANSFRONTALIÈRE

CADRE : **LOI SUR LA COMMUNICATION ÉLECTRONIQUE (2000)** - DÉFINISSAIT LE CADRE LÉGAL SUIVI PAR LES FOURNISSEURS D'IDENTITÉ DU SECTEUR PRIVÉ POUR ACCÉDER AUX SERVICES PUBLICS NUMÉRIQUES. **LE RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES (2016)** - SOUS LEQUEL L'«INFORMATION COMMISSIONER'S OFFICE» (ICO) A LE RÔLE D'AUTORITÉ INDÉPENDANTE POUR LA PROTECTION DES DONNÉES.

Authentification avec un niveau de sécurité équivalent à Bas et Subtantiel (non-certifiée par eIDAS)

22 **services publics disponibles**

Le gouvernement du Royaume-Uni espèce exporter son modèle vers d'autres pays via la standardisation. Par exemple, les principaux atouts techniques de son programme ont été mis à disposition sous license «open-source» au bureau Australien de Transformation Numérique, qui a pour but de créer un écosysème similaire en Australie.
L'alignement du Royaume-Uni sur eIDAS n'est pas encore définit dans le contexte du Brexit - mais les avantages d'une interopérabilité continue sont clairs.

CONTEXTE & OBJECTIFS

Le Royaume-Uni ne dispose pas d'une base de données d'identité unique - un large éventail de titres d'identité est utilisé par la population pour affirmer son identité (permis de conduire, passeports, certificats de naissance, relevés bancaires, etc.)
En 2014, le gouvernement britannique a lancé GOV.UK Verify, un programme d'identité numérique permettant aux citoyens et résidents britanniques de s'authentifier via le fournisseur d'identité de leur choix pour accéder aux services numériques des secteurs public et privé.
L'objectif du gouvernement était d'établir un marché privé de services d'identité certifiée, fidèle aux normes définies par le gouvernement.

À ce jour, plus de 7 millions d'identités numériques ont été délivrées. L'initiative n'a pas eu le succès escompté. En conséquence, le gouvernement britannique a été contraint de lancer une consultation publique à la suite de laquelle le nombre de fournisseurs d'identité a baissé. Cependant, l'épidémie de COVID-19 a provoqué une pic de demandes de crédit universel (Universal Credit) (faibles revenus ou allocations de chômage) par l'intermédiaire de Gov.UK Verify. La demande a dépassé la capacité de la plateforme, obligeant le gouvernement à investir davantage dans le service et à garder le contrôle de la plateforme pendant au moins 18 mois supplémentaires.

Fin 2020, le gouvernement du Royaume-Uni a lancé un pilote du Service de Vérification de Documents par lequel les informations d'identité peuvent être comparées à la base de données liée aux passeports.

PROPOSITION DE VALEUR

Pour s'enregistrer puis s'authentifier en ligne, les utilisateurs peuvent choisir entre 5 fournisseurs d'identité privés, chacun offrant des processus d'inscription différents pour tous types d'utilisateurs. Ils peuvent ensuite utiliser leur compte d'identité pour se connecter facilement à d'autres services (y compris publics) utilisant GOV.UK Verify.

MODÈLE ÉCONOMIQUE : FINANCÉ PAR LE GOUVERNEMENT

> Initialement financé par le gouvernement
> Gratuit pour les citoyens.
> Les services des secteurs public et privé paient pour la confirmation d'identité
> Les services publics paient le Service Numérique du Gouvernement (GDS – « Government Digital Service ») à l'utilisation. Le GDS paie le fournisseur d'identité choisi par le citoyen.

CHOIX EN MATIÈRE DE SÉCURITÉ & PROTECTION DES DONNÉES

> Le système a été conçu dans le but de protéger la vie privée : éviter de «traquer» les comportements et éviter que le choix du fournisseur d'identité ne porte préjudice à l'individu.
> Les fournisseurs d'identité ne peuvent pas voir à quels fournisseurs de services les données d'identité sont envoyées et les fournisseurs de services ne peuvent pas voir quel fournisseur d'identité a assuré l'identité.
> Les fournisseurs d'identité privés ont accès au Service de Vérification de Documents, par lequel ils peuvent demander une validation «oui/non» des données biographiques du passeport. Cela n'a été rendu possible pour le secteur privé que depuis le nouveau projet pilote de ce service, lancé par le gouvernement fin 2020.

ÉTAPES CLÉS DU PROJET

2012
Politique annoncée par le Ministre du Bureau du Cabinet

2014
GOV.UK Verify lancé en Beta test

2016
9 entreprises ont rejoint le programme en tant que fournisseurs d'identité.
Vote Brexit

2020
Projet pilote d'un Service de Vérification de Documents lancé par le gouvernement du Royaume-Uni - permettant le secteur privé de comparer les informations liées au passeport à la base de données nationale.
Programme d'identité numérique actuellement en redéfinition

REMERCIEMENTS

Cette recherche a été menée conjointement par Marie-Alice Manderscheid, Hélène Le Héricy et Corentin Marsily, sous la direction de Yannick Ragonneau de onepoint, de Stéphanie de Labriolle de la Secure Identity Alliance (SIA) et de et Kristel Teyras, Responsable marché identité numérique, plateformes et services, de Thales. De plus, Vincent Rémon et Corina Fontaine de onepoint et Pavlina Navratilova (Idemia), Marie-Sophie Bellot (Idemia), Eric Piroux (Entrust), Fabian Bahr (Giesecke+Devrient), Olivier Dussutour (INGroupe), Michael Edwards (Veridos), Sebastian Zehetbauer (Youniqx), Andreas Zechmann (OSD) ont contribué à l'analyse.

Cette initiative indépendante de la SIA et de onepoint s'appuie sur le retour d'expérience de ces deux organisations, des sources analytiques officielles et documentées, ainsi que sur une analyse croisée de 25 entretiens avec des acteurs internationaux clés et les représentants des pays étudiés.
Nous devons une profonde reconnaissance à :

Australie (Queensland)
Christopher J Goh, Manager Général, Modernisation des Permis et Immatriculations – Département des Transports et Routes Principales du Queensland
Autriche
Herbert Leitold, Secrétaire Général, Centre de technologie de l'Information
Azerbaïdjan
Jana Krimpe, Représentante du consortium Public/Privé d'Azerbaïdjan et Co-Présidente de GANMI – Alliance Mondiale des Identité Nationales Mobiles
Canada
Joni Brennan, Présidente du Conseil Canadien de l'identification & authentification numériques (CCIAN)
Sarah Kirk-Douglas, Vice-Présidente, Marketing & Communications Mondiales, SecureKey Technologies Inc.
Andre Boysen, Directeur d'Identité, SecureKey Technologies Inc.
Colombie
Didier Alberto Chilito Velasco, Directeur National de l'Identification du Régistre National de l'État Civil, Colombie
Sofía Romero Mondragón, Coordinatrice de l'équipe juridique.
Danemark
Charlotte Jacoby, Cheffe de service de la Division pour le Développement de l'Infrastructure
Estonie
Margus Arm, Député Directeur Général, Autorité du Système d'Information Estonien, Directeur Branche systèmes d'information de l'Etat
France
Valérie Péneau, Directrice du Programme Interministériel France Identité Numérique
Lionel Fouillen, Responsable des Relations Partenaires, FranceConnect
Italie
Andrea Spallacci, Chef de Projet, Agenzia per l'Italia Digitale (AgID)
Service des Accréditations / Membre du FESA, le «Forum of European Supervisory Authorities for Electronic Signatures.»
Lettonie
Edmunds Belskis, Président du Conseil d'Administration, LVRTC.
Liechtenstein
Sylvan Fux, Chef du Consulting Commerce Finance/Justice et E-Gouvernement.
Pays-Bas
Michiel Van der Veen, Directeur Innovation & Développement au Bureau National des Données d'Identité, Ministère de l'Intérieur et des Relations au sein du Royaume
Nigéria
Aziz Aliyu, Président Directeur Général de la Commission de Management de l'Identité Nationale (NIMC)
Olatunji Durodola, Consultant Senior en Technique & Intégration Systèmes (NIMC)
Portugal
Andre Vasconcelos, Conseiller eID du Comité de Direction, Agence pour la Réforme des Services Publics
Claudia Barroso, Chef de l'Unité chargée des Relations Internationales de l'AMA - Agence pour la Réforme des Services Publics
Singapour
Quek Sin Kwok, Directeur Principal, Plateforme et Produits de l'Identité Numérique Nationale, GovTech Singapour
USA (Arizona)
Eric Jorgensen, Directeur de la Division des Véhicules Automobiles au Département des Transports de l'Arizona
Vietnam
Lã Hoàng Trung, Directeur du Centre National d'E-Authentification

ORGANISATIONS INTERNATIONALES

Conseil de l'Europe
Sophie Kwasny, Cheffe de l'Unité de Protection des Données du Conseil de l'Europe
Peter Kimpian, Unité de Protection des Données, Conseil de l'Europe.
eIDAS
GANMI
Jana Krimpe, Co-Présidente de GANMI – Alliance Mondiale des Identité Nationales Mobiles
IIC, ID4Africa
Mory Camara, Président du Conseil sur l'Identité (CII), ID4Africa
UNCITRAL
Eric A. Caprioli, Avocat à la Cour, Représentant France UNCITRAL/CNUDCI

SECURE IDENTITY ALLIANCE

onepoint.
beyond the obvious