SYSTÈMES D'IDENTITÉ DÉCENTRALISÉE

Un cadre stratégique pour la transformation numérique des administrations publiques

Livre blanc

TOPPAN
TOPPAN Security

QU'EST-CE QUE L'IDENTITÉ DÉCENTRALISÉE ?

L'identité décentralisée, dans le contexte de ce document, désigne l'identité numérique mise en œuvre au moyen de justificatifs vérifiables (Verifiable Credentials – VC). Ce modèle rompt avec les pratiques traditionnelles : là où les gouvernements et entreprises stockent et contrôlent les données des citoyens dans des bases centralisées, l'identité décentralisée remet l'individu au cœur de la gestion de sa propre identité. C'est le principe de l'identité auto-souveraine (Self-Sovereign Identity – SSI).

Les citoyens conservent leurs VC dans des portefeuilles numériques sécurisés, ou dans des super-applications (SuperApps), directement sur leurs appareils personnels. C'est eux qui décident quand partager leurs informations, avec qui, et jusqu'à quel niveau de détail.

Un système d'identité décentralisé s'articule autour de quatre composants essentiels:

1. Émetteurs: autorités de confiance telles que des agences gouvernementales qui créent et certifient des VC.

2. Portefeuilles numériques ou super-applications: applications sécurisées installées sur les appareils des citoyens, permettant de stocker et de présenter les VC.

3. Registres de confiance: référentiels faisant autorité qui permettent aux vérificateurs de contrôler la légitimité des émetteurs.

4.Vérificateurs (Relying Parties – RP) : services ou organisations qui acceptent et valident les VC comme un hôtel lors d'un enregistrement client.

Lorsqu'un citoyen doit prouver son identité ou ses qualifications, il ne communique que les informations strictement nécessaires, c'est le principe de divulgation sélective. Il peut ainsi attester résider dans une ville donnée sans en préciser l'adresse, ou confirmer être majeur sans révéler sa date de naissance. Cette minimisation des données protège la vie privée tout en maintenant un niveau élevé de confiance.

SYSTÈMES CENTRALISÉS: UN POINT DE DÉFAILLANCE UNIQUE

Les systèmes d'identité centralisés concentrent l'ensemble des données des citoyens dans des bases contrôlées par l'État. Si cette approche offre une certaine simplicité administrative, elle constitue aussi un risque majeur : ces bases de données, exposées à Internet et remplies d'informations personnelles, représentent des cibles de choix pour les cybercriminels faisant de ces systèmes un point de défaillance unique.

Assurer la haute disponibilité et la fiabilité qu'exigent les services publics et le secteur privé est par ailleurs coûteux, et ces charges ne font qu'augmenter à mesure que les usages se développent. À cela s'ajoute une concentration du pouvoir entre les mains d'une seule autorité, qui engendre des risques de surveillance, d'exclusion des populations les plus vulnérables, et de mauvaise utilisation, voire de commercialisation des données personnelles des citoyens.

DÉCENTRALISATION: CONÇUE POUR ÊTRE DISTRIBUÉE

Dans un système décentralisé, les citoyens peuvent prouver leur identité auprès d'un RP sans que l'État n'intervienne dans la transaction ce qui favorise une adoption plus large, à coûts maîtrisés. Cette architecture ouvre également la voie à de nouvelles sources de revenus.

L'État conserve bien les données dans un registre central, mais cette base n'est pas exposée à Internet : les citoyens reçoivent directement dans leur portefeuille numérique une copie signée de leurs informations.

Comme les données résident sur les appareils des citoyens plutôt que sur des serveurs centraux, il n'existe aucun point de concentration des données à cibler. La vérification s'effectue par preuve cryptographique et non par simple consultation d'une base centrale ce qui permet aussi son utilisation hors ligne dans les zones à faible connectivité. L'architecture distribuée élimine les points de défaillance uniques et allège les coûts d'infrastructure. Surtout, les citoyens restent maîtres de leurs données, ce qui renforce la confiance envers les institutions publiques tout en préservant leur vie privée.

	Centralisé	Décentralisé
Stockage des justificatifs	Stocké sur le serveur	Distribué dans les portefeuilles des utilisateurs
Point de défaillance unique	Oui	Non
Sécurité des données	★☆☆	★★★
Confidentialité des données	☆☆☆	★★★
Contrôle des donnée	★☆☆	★★★
Mode de vérification	En ligne uniquement	En ligne et hors ligne
Coûts	Coûteux	Efficace
Interopérabilité	Non interopérable	Normes internationales
Inclusivité	★☆☆	★★★

POURQUOI L'IDENTITÉ DÉCENTRALISÉE EST LE MEILLEUR CHOIX POUR LES GOUVERNEMENTS

Pour les gouvernements, les arguments en faveur de l'identité décentralisée sont convaincants.

McKinsey estime que les systèmes d'identité numérique pourraient générer une valeur économique équivalente à 3 à 13 % du PIB d'ici 2030 pour les économies émergentes.

Pour les gouvernements aux budgets limités, réduire les besoins en infrastructure est un enjeu de premier plan. Une architecture fondée sur des normes ouvertes internationales et indépendante de tout fournisseur permet d'éviter de coûteuses dépendances à des solutions propriétaires, tout en garantissant une interopérabilité durable au-delà des frontières comme entre les services.

VÉRIFICATION SANS DÉPENDANCE CENTRALE

Utilisable en ligne et hors ligne

Un écosystème SSI permet aux individus de justifier leur identité dans des contextes très variés. Les VC transitent directement du portefeuille numérique du citoyen vers le RP qui les demande. La vérification repose sur une preuve cryptographique, non sur la consultation d'une base de données centrale. Ce mécanisme fonctionne aussi bien en ligne qu'hors ligne, ce qui est particulièrement précieux dans les zones où l'accès à Internet reste peu fiable ou limité.

Pour qu'un tel système soit réellement inclusif, la question de l'accès doit être pensée avec soin dès la conception. Il doit fonctionner aussi bien pour les personnes possédant leur propre smartphone que pour celles qui en partagent un. Il doit répondre aux besoins des populations vivant dans des zones à faible ou nulle connectivité. Et les services doivent rester opérationnels même en l'absence d'Internet.

Les fonctionnalités hors ligne et les options flexibles de portefeuilles ne sont donc pas des ajouts optionnels, elles sont indispensables à tout déploiement équitable et inclusif.

Engagement du secteur privé

La participation du secteur privé est déterminante pour la viabilité de l'écosystème. Les banques et les opérateurs de services financiers mobiles peuvent s'appuyer sur les VC pour optimiser leurs processus de vérification d'identité (KYC) : l'expérience utilisateur lors de la capture de documents est considérablement simplifiée, et le temps d'enregistrement peut être réduit à quelques secondes. Les opérateurs télécoms peuvent, de leur côté, intégrer l'enregistrement des cartes SIM à la vérification d'identité numérique.

La clé du succès réside dans l'établissement de normes claires et de programmes de certification permettant à plusieurs fournisseurs de participer, tout en garantissant la sécurité et l'interopérabilité de l'ensemble.

Précisons enfin que le cadre des VC peut s'étendre bien au-delà de l'identité nationale: qualifications professionnelles, licences, attestations diverses… Ces usages s'appuient sur la même infrastructure, mais constituent des extensions naturelles de l'écosystème qui est à distinguer des composantes de l'identité à proprement parler.

UN LEVIER FISCAL

L'écosystème numérique entre les citoyens, les gouvernements et le secteur privé, rendu possible par l'identité décentralisée, offre également une opportunité de créer de nouvelles sources de revenus. En adoptant des standards reconnus à l'échelle internationale, les gouvernements peuvent faciliter davantage les transactions numériques transfrontalières, élargissant ainsi les opportunités commerciales offertes aux entreprises et, par extension, augmentant les recettes fiscales générées par l'accroissement de l'activité économique.
En prenant l'exemple du Portefeuille d'Identité Numérique Européen (EUDI), les gouvernements européens imposent au secteur privé des exigences réglementaires en matière de vérification de l'identité numérique des citoyens dans un large éventail de cas d'usage. Ceux-ci incluent l'accès aux plateformes de réseaux sociaux, réservé aux utilisateurs ayant atteint un âge minimum qui varie selon les pays, ainsi que l'achat en ligne de biens et services soumis à des restrictions d'âge, tels que l'alcool. La vérification de l'âge s'impose ainsi comme un cas d'usage à haute fréquence, obligeant les citoyens à prouver régulièrement leur identité.
Cette dynamique ouvre la voie à l'introduction, par les gouvernements, de structures tarifaires applicables aux entités du secteur privé se connectant au système, qu'il s'agisse d'un droit d'accès forfaitaire ou d'une facturation à la vérification potentiellement modulées selon le volume de transactions et encadrées par la réglementation.

Les gouvernements peuvent mettre en œuvre ces modèles de revenus par le biais de l'autorisation des vérificateurs. Tous les vérificateurs sont autorisés via un certificat d'authentification assorti d'une date d'expiration, offrant ainsi un mécanisme permettant d'activer et d'appliquer un système d'abonnement, sans suivi des transactions individuelles, mais garantissant des revenus récurrents grâce au renouvellement des licences. Par ailleurs, les gouvernements peuvent autoriser des technologies de vérification qui appliquent des limites de transactions prépayées et permettent de transmettre des rapports d'activité.

Les acteurs du secteur privé soumis à des obligations de vérification d'identité, comme lors de l'enregistrement d'une carte SIM ou de l'ouverture d'un compte bancaire, peuvent acquérir un nombre défini de vérifications à l'avance, selon un modèle similaire aux licences KYC existantes. Ces vérificateurs peuvent être désactivés, c'est-à-dire non renouvelés, en l'absence de transmission des rapports requis.

La transmission des rapports peut être structurée sous forme de synthèses quotidiennes ou mensuelles plutôt qu'en temps réel, conciliant ainsi les besoins de visibilité des gouvernements avec l'efficacité du système. Le respect des obligations peut être assuré par la désactivation automatique des vérificateurs ne soumettant pas les rapports requis, garantissant ainsi le respect des conditions d'utilisation autorisées tout en préservant les avantages décentralisés du système.

RECOMMANDATIONS
POUR LES GOUVERNEMENTS

Pour les gouvernements qui entament leur parcours de numérisation, nous recommandons de :

• Établir un cadre juridique solide et des règles de protection des données avant tout déploiement.

• Opter pour des solutions fondées sur des normes ouvertes internationales, afin de garantir l'interopérabilité et d'écarter toute dépendance à un fournisseur unique.

• Associer la société civile pour asseoir la confiance du public et s'assurer que les droits des citoyens sont intégrés dans la conception même du système.

• Privilégier une conception adaptée au mobile et capable de fonctionner hors ligne, pour maximiser l'inclusion numérique.

La transition vers l'identité décentralisée ne se résume pas à une mise à niveau technologique. C'est une réinvention profonde du lien entre les citoyens et l'État : un lien fondé sur la confiance, le respect de la vie privée et l'autonomie individuelle. individuelle.

TOPPAN

TOPPAN Security

www.toppansecurity.com
info@toppansecurity.com