

Data Passport

The minimal digital identity

Le problème

Aujourd'hui, pour prouver une chose simple sur Internet : être majeur, étudiant, résident, on nous demande une identité complète.

Ces données sont stockées, copiées, revendues ou piratées, créant des risques énormes pour les utilisateurs et une complexité inutile pour les services.

⇒ ***Le système actuel collecte trop de données pour des usages très simples.***

De plus, l'actualité récente de l'Union Européenne nous montre que ce type de problème devient de plus en plus dominant et qu'il faut à tout prix éviter la censure excessive des médias/réseaux sociaux

L'idée

Data Passport inverse la logique.

Plutôt que de partager toute son identité, un utilisateur doit pouvoir **prouver uniquement ce qui est nécessaire**, une seule fois, sans révéler le reste.

Exemples :

→ prouver qu'on est majeur, **sans donner sa date de naissance**

→ prouver qu'on est étudiant, **sans révéler son école**

→ prouver qu'on est résident d'un pays, **sans adresse**

La solution

Data Passport est un **wallet d'identité minimal**, sur le téléphone de l'utilisateur.

Il permet de prouver des attributs simples (âge, statut, droits, abonnements) de manière sécurisée, **sans que les données personnelles ne quittent l'appareil.**

Pour les services, la vérification est :

- rapide
- simple
- respectueuse de la vie privée

Pour l'utilisateur :

- aucune création de compte complexe
- aucune base de données centrale
- contrôle total sur ses informations

Pourquoi maintenant ?

- Explosion des besoins de vérification (apps +18, e-commerce, lieux physiques, services en ligne)
- Rejet croissant des systèmes KYC lourds et intrusifs
- Pression réglementaire forte autour de la protection des données surtout au sein de l'UE via la RGPD ou d'autre norme bureaucratique freinant la tech

⇒ **Le besoin est là, mais la bonne solution n'existe pas encore.**

Ce que nous construisons

Data Passport vise une expérience :

- aussi simple qu'un QR code
- aussi fluide qu'un paiement mobile
- sans compromis sur la sécurité ou la confidentialité

L'objectif n'est pas d'ajouter une couche de complexité, mais de **supprimer le superflu**.

⇒ Permettre d'incorporer ce système au sein des sites web craignant la censure pour pouvoir empêcher leurs interdiction aus ein de l'Europe

La vision

À terme, Data Passport peut devenir :

- un standard de fait pour la preuve d'attributs
- une brique d'infrastructure utilisée par des milliers de services
- une alternative crédible à l'identité numérique centralisée

Moins de données. Plus de confiance.

Concrètement comment ça marcherait ? Modèle one-shot

1. L'utilisateur installe Data Passport

Data Passport est une application mobile.

Elle permet de stocker des **preuves cryptographiques**, et non des documents ou des données personnelles lisibles.

Aucune information n'est centralisée.

Tout se passe sur le téléphone de l'utilisateur.

2. Vérification unique ("one-shot")

Lors de la première utilisation, l'utilisateur effectue une **vérification ponctuelle** de l'information réelle.

Exemples :

- vérification de l'âge (+18)
- vérification d'un statut spécifique (étudiant, résident, etc.)

Cette vérification peut se faire :

- soit directement via Data Passport
- soit via un prestataire de vérification existant (KYC, identité, documents)

⇒ Cette étape a lieu **une seule fois**.

Une fois l'information vérifiée :

- **aucune donnée personnelle n'est conservée**
- **aucun compte n'est créé**
- **aucune base de données n'est constituée**

Le système génère uniquement une **preuve numérique minimale**, par exemple :

“Cette personne est majeure”

Cette preuve est :

- signée cryptographiquement
- stockée **uniquement sur le téléphone**
- inutilisable hors de Data Passport

3. Accès à un service

Lorsqu'un service a besoin d'une vérification :

Exemples :

- site +18
- abonnement étudiant
- entrée dans un lieu
- service en ligne

Le service demande simplement :

“Prouve que tu es majeur”

4. Présentation de la preuve (sans données)

Depuis Data Passport :

- l'utilisateur accepte la demande
- l'application affiche un QR code ou envoie une preuve numérique

Le service ne reçoit **aucune donnée personnelle** :

- pas de nom
- pas de date de naissance
- pas d'identifiant
- rien à stocker

Il reçoit uniquement une réponse binaire et vérifiable :

⇒ Oui, cette personne est majeure
ou Non

5. Fin de l'échange

Une fois la preuve vérifiée :

- aucune information n'est conservée par le service
- aucune trace n'est laissée
- aucune corrélation possible entre usages

Pas de compte.

Pas de tracking.

Pas de réutilisation des données.

Pourquoi ce système est sécurisé et infalsifiable ?

- Les preuves sont générées à partir d'une vérification réelle
- Elles sont signées cryptographiquement
- Toute modification invalide automatiquement la preuve
- Sans la clé cryptographique, il est impossible de copier ou de falsifier une preuve

⇒ La confiance repose sur **une vérification unique**, pas sur une surveillance permanente.

Business Model Data Passport

1. Proposition de valeur clé

Pour l'utilisateur :

- Preuves numériques fiables d'attributs (âge, statut, droits) sans divulguer ses données personnelles.
- Expérience simple, rapide et sécurisée.
- Contrôle total de ses informations.

Pour les services / entreprises :

- Vérifications rapides et fiables.
- Réduction du risque juridique lié au stockage et traitement de données personnelles.
- UX améliorée, adoption plus facile de leurs services.

2. Sources de revenus potentielles

A. B2B – Paiement par vérification (primary MVP model)

- Chaque vérification demandée par un service (ex. site +18, abonnement étudiant, accès à un lieu) est **facturée au service**.
- Le service paie **une micro-frais par transaction**, par exemple 0,50€–2€ selon le type de vérification et le volume.
- Avantage : modèle **scalable dès le MVP**, facile à expliquer et justifiable légalement.

B. B2B – Abonnement SaaS pour services

- Offrir un **SDK / API** aux services qui veulent intégrer Data Passport de manière fluide.
- Deux options :
 1. **Abonnement mensuel** : accès illimité aux vérifications et au dashboard admin.
 2. **Freemium** : quelques vérifications gratuites, puis abonnement pour usage professionnel.
- Permet un **revenu récurrent** et fidélise les services partenaires.

C. B2B – Licensing / white-label

- Les institutions (universités, opérateurs, entreprises) peuvent intégrer **leur propre version “white-label”** de Data Passport pour leurs utilisateurs internes.
- Revenue via licence annuelle ou forfait par utilisateur.
- Utile pour bâtir des partenariats stratégiques.

D. B2C – éventuellement, premium pour utilisateurs

- Pour un MVP, pas prioritaire.
- À terme, possibilité d'ajouter **fonctionnalités avancées** pour les utilisateurs :
 - gestion multi-preuves
 - intégration avec plusieurs services
 - récupération sécurisée des preuves perdues

3. Coût d'acquisition et marge.

- **Marge** : très élevée par preuve (coût marginal proche de zéro), ce qui permet un modèle B2B très rentable si le volume croît rapidement.

4. Stratégie de déploiement (go-to-market)

1. **MVP ciblé** : un premier cas simple et critique (ex : preuve d'âge +18 pour services web et lieux physiques).
 - Facile à expliquer aux services
 - Permet un paiement par vérification immédiat
 - Teste la traction utilisateurs
2. **Phase expansion** : ajouter d'autres preuves (étudiant, résident, abonnement, droits spécifiques).
 - Commence à bâtir un réseau d'émetteurs et services intégrés
3. **Phase long terme** : licence / API / white-label pour institutions.
 - Vision : Data Passport comme **standard de facto pour la preuve d'attributs**, utilisé par des milliers de services

5. Scalabilité

- Chaque nouvelle preuve ou service intégré **augmente la valeur sans augmenter les coûts proportionnellement**.
- Une fois que le réseau d'émetteurs et services est établi, les revenus deviennent largement **récurrents et prévisibles**.

⇒ *Fort revenues car les logiciels/réseaux sociaux sensibles seront fortement dépendant à notre système face aux restrictions nationales ou européennes*

De qui j'aurais besoin ?

Ce projet nécessite une conciliation entre exécution technique et protection juridique/qualité de design

Pour que **Data Passport** devienne un produit fiable, auditable et utilisable dès le lancement, le rôle le plus critique est celui du **CTO / Lead Engineer**.

CTO / Lead Engineer

Le CTO sera **le moteur technique du projet** et responsable de l'architecture, de la sécurité et de la qualité du produit.

Responsabilités principales :

- Concevoir l'**architecture globale** de Data Passport, simple, robuste et évolutive
- Implémenter les **preuves cryptographiques** sécurisées et infalsifiables
- Arbitrer les **choix entre sécurité et expérience utilisateur** de manière pragmatique
- Construire le **MVP fonctionnel** et garantir sa fiabilité dès le lancement
- Superviser l'intégration avec les prestataires de vérification et garantir la conformité aux standards privacy

Je m'occuperais personnellement grâce à ma formation juridique actuelle de tous les **aspects juridiques, médiatiques et publicitaires**, du projet dont les démarches pour effectuer des **levées de fond** grâce à mon réseau parisien