

Biométrie au porteur : clé d'une authentification sécurisée et respectueuse des données personnelles

La sécurité et la protection des données personnelles sont des priorités pour les citoyens, les États et les entreprises qui les exploitent.

Le développement des usages numériques, la généralisation des applications mobiles, et des services en ligne facilitent le quotidien de chacun. À mesure que ces services se personnalisent et offrent davantage de valeur ajoutée, il devient nécessaire de renforcer les moyens d'authentification.

Ainsi, la personnalisation des services nécessite le traitement de données sensibles concernant l'identité et le profil des utilisateurs. Cette évolution rend encore plus essentielle la vérification de l'identité de chaque utilisateur : il faut s'assurer que chaque utilisateur est bien celui qu'il prétend être.

L'usage de la biométrie s'est imposé en tant que facteur d'authentification fiable, plus particulièrement en mobilité sur téléphones portables et tablettes. Par extension, elle est également utilisée en ligne pour les transactions financières et dans le secteur de la santé, mais aussi en face à face pour les contrôles d'accès en entreprises ou dans le secteur des transports.

Dans ce cadre, IN Groupe garantit une authentification de confiance basée sur une biométrie au porteur, entièrement sous le contrôle des individus. Cette solution s'intègre parfaitement dans le cadre réglementaire, notamment le règlement eIDAS 2.0, assurant une sécurité et une interopérabilité accrues.

La biométrie et ses usages au quotidien

Avec l'accélération de la numérisation de nombreux services, la biométrie est devenue une technologie facilement accessible pour garantir une vérification fiable. Son adoption s'explique par plusieurs facteurs :

- **Authentification fiable et simplifiée** : La reconnaissance faciale et les empreintes digitales permettent un accès rapide et sécurisé. Son usage s'inscrit dans la transformation numérique de notre quotidien.
- **Réduction des mots de passe** : La simplification des parcours d'authentification rend désormais l'expérience utilisateur plus simple et plus fluide.

L'ère numérique bouleverse nos interactions avec les services publics et privés transformant la manière de s'authentifier :

- **Contrôle d'accès** : Le contrôle d'accès automatisé, dans les entreprises, les bâtiments sécurisés et les infrastructures critiques, est utilisé de manière récurrente.

- Paiements sécurisés : Les institutions bancaires et les plateformes de paiement optent pour les paiements authentifiés par la biométrie pour réduire les risques de fraude.
- Secteur de la santé : La biométrie permet l'accès sécurisé aux dossiers médicaux, évitant ainsi les risques de vol d'information, ou de commettre des erreurs d'identité, notamment pour les prescriptions.
- Transports : Le contrôle d'embarquement dans les aéroports, les gares et les ports, grâce à la reconnaissance faciale, est devenu une modalité de plus en plus répandue.

Toutefois, certains fournisseurs de services, peut-être encore peu sensibilisés aux enjeux de la protection des données personnelles ou n'ayant jusqu'à présent pas eu d'autres options, effectuent des vérifications biométriques sur des données stockées dans des bases centralisées. A titre d'exemple, dans le cas d'une vérification en face-à-face, le visage de l'utilisateur, présenté devant une caméra, sera comparé avec des images d'utilisateurs stockées sur une base de données centralisée. Ces bases sont localisées sur des serveurs privés ou dans le cloud, exposant les utilisateurs à des risques des cybermenaces pouvant être massives. Ces bases constituent de véritables « pots de miel / honey pot » pour les cybercriminels. C'est ici que la biométrie au porteur apporte une réponse adaptée, sécurisée et garante de la protection des données personnelles.

La biométrie au porteur, définition et fonctionnement

La biométrie au porteur repose sur une logique d'authentification locale et de comparaison dite « un contre un ». Les données biométriques, telles que les empreintes digitales ou l'image du visage, sont directement conservées sur le support personnel sous le contrôle unique de l'utilisateur. Ce support peut être une carte à puce biométrique, un module cryptographique intégré dans son téléphone, ordinateur ou tablette (Trusted Platform Module - TPM), ou un titre d'identité biométrique dont la sécurité est garantie par l'État sur le niveau de sécurité de la puce qui contient les données (carte d'identité ou passeport). Ces supports sont généralement certifiés par une entreprise ou un fournisseur fiable.

Cette méthode évite la transmission de données sensibles, réduisant ainsi les risques de vulnérabilité réseau. De plus, elle empêche le stockage de données biométriques sur des serveurs distants ou dans le cloud, dont le niveau de sécurité peut être variable et difficile à vérifier.

La biométrie au porteur évite le stockage centralisé des données, réduisant ainsi le niveau de risques liés aux cyberattaques (compromission des données, usurpation d'identité). Les données restent sous le contrôle exclusif de l'utilisateur. Lorsqu'un individu souhaite s'authentifier, ses données biométriques sont comparées localement : les informations captées par le dispositif d'authentification (par exemple une caméra ou un lecteur d'empreinte) sont comparées avec celles enregistrées sur le support sous son contrôle (comparaison un contre un). Si elles correspondent,

l'accès est accordé. Il n'y a aucun transfert de données vers un système extérieur, ce qui limite le risque d'exposition des données biométriques hors du dispositif personnel de l'utilisateur.

La biométrie au porteur respecte le principe de minimisation des données imposé par le Règlement Général sur la Protection des Données (RGPD), du fait de l'absence de stockage centralisé. Aucune donnée biométrique ne transite sur un réseau ou un serveur distant, réduisant ainsi les risques de surveillance abusive et protégeant la vie privée de chacun.

La biométrie au porteur inclut toutes les populations, y compris celles ne disposant pas de smartphone ou vivant dans des zones à faible connectivité. Dans les zones rurales, les sites industriels, ce modèle permet de sécuriser l'authentification sans infrastructure réseau complexe.

Enfin, la simplicité d'usage et la rapidité d'authentification font de la biométrie au porteur une solution idéale pour tous les secteurs de la vie quotidienne, qu'ils soient publics ou privés.

Une solution conforme aux normes et réglementations

La biométrie au porteur s'appuie sur plusieurs standards internationaux garantissant un haut niveau de sécurité et d'interopérabilité :

- ISO/IEC 19794 : Norme de représentation et d'interopérabilité des données biométriques
- ISO/IEC 30107 : Norme sur la détection des attaques par présentation (PAD) pour éviter les fraudes biométriques
- Règlement eIDAS 2.0 : Réglementation européenne définissant les standards d'authentification électronique et d'identité numérique
- ICAO 9303 : Norme encadrant les documents de voyage biométriques, notamment les passeports électroniques
- RGPD, CNIL 1 : Exigences réglementaires en matière de protection des données personnelles

Fly'IN : la biométrie au porteur adaptée à la fluidification des voyages

Développée par IN Groupe, Fly'IN – Fast Track est une solution inclusive qui intègre la biométrie au porteur.

Le voyageur configure à son domicile son profil sur l'application mobile du transporteur en entrant ses données d'identité à l'aide de son passeport, sa carte d'identité, son titre de séjour, ou tout autre document officiel.

Ces informations d'identité, complétées des données de sa carte d'embarquement, sont encapsulées dans un QR code unique. Celui-ci permet au voyageur de se déplacer librement et rapidement dans l'aéroport.

Le voyageur est le seul propriétaire de ses données personnelles. Son identité et son titre de voyage peuvent être authentifiés sans besoin d'accès à une base de données externe. Unique détenteur de ses données personnelles, il peut à tout moment retirer son consentement depuis son smartphone, un site Web ou un formulaire.

La biométrie au porteur est aujourd'hui la solution la plus efficace pour allier sécurité, protection des données et expérience utilisateur fluide. Elle permet :

- Une sécurité accrue contre les fraudes.
- Une protection optimale des données personnelles pour prévenir les usurpations d'identité.
- Une solution universelle, adaptée à tous les aspects de la vie quotidienne, qu'ils relèvent du secteur privé ou du secteur public.

Cette solution, sécurisée et conforme aux réglementations, est essentielle pour une authentification respectueuse des données personnelles. L'adoption de Fly'IN représente une avancée stratégique pour garantir une authentification de confiance, entièrement sous le contrôle des individus.

À propos d'IN Groupe

Spécialiste européen des identités, des transactions sécurisées et des services numériques, IN Groupe est un partenaire de confiance des gouvernements et entreprises publiques et privées dans la gestion et la protection des données sensibles.

En maîtrisant l'ensemble de la chaîne de valeur de l'identité, IN Groupe étend son expertise de l'identité citoyenne aux solutions et services pour les identités professionnelles et des objets. IN Groupe est un acteur clé qui garantit le droit d'être soi dans l'espace physique et numérique.

Avec 2 000 collaborateurs répartis sur tous les continents, IN Groupe réalise un chiffre d'affaires d'environ 600 millions d'euros. Le groupe est un partenaire de confiance pour les gouvernements et ses clients du secteur privé et public dans plus de 130 pays.

Pour plus d'informations, visitez www.ingroupe.com

Contact Presse : Céline Fauvet celine.fauvet@ingroupe.com (06 43 85 06 43)