AWARE

L'utilisation de la biométrie et de la détection du caractère vivant pour l'intégration et l'authentification mobiles

Les opérateurs de téléphonie mobile, les banques et les organismes gouvernementaux doivent pouvoir établir la preuve de l'identité d'un nouveau client ou citoyen lors de son intégration, de manière à enregistrer une identité fiable et éviter la fraude. Après l'intégration, ils pourront identifier et habiliter cette personne lors des rencontres suivantes. Dans le secteur bancaire, ce processus est appelé KYC (Know Your Customer, c'est-à-dire la connaissance du client), et il est exigé par de nombreuses réglementations internationales concernant les services bancaires et la lutte contre le blanchiment d'argent.

L'intégration devient considérablement plus complexe quand les registres et les preuves d'identité sont limités ou de mauvaise qualité. Certaines personnes n'ont jamais eu le besoin de confirmer leur identité auparavant, et ne disposent d'aucun extrait de naissance ni de documents validant une rencontre avec un gouvernement central.

L'absence d'identité prouvable constitue un obstacle majeur pour l'obtention d'avantages gouvernementaux et la possibilité de jouer un rôle dans le système financier. Elle peut affecter la participation politique, l'emploi, l'enseignement et l'accès au crédit.

La biométrie mobile est la meilleure solution pour les problèmes d'intégration dans les régions où les registres d'identité sont disparates ou absents. La téléphonie est suffisamment répandue pour que, souvent, le propre appareil de l'individu puisse servir à établir son identité, lui donnant ainsi la possibilité d'interagir avec son gouvernement et ses institutions financières.

La confirmation de l'identité mobile exploite la puissance d'un smartphone pour fournir des services sans qu'il soit nécessaire de se déplacer jusqu'à une succursale bancaire, un bureau ou un point de vente. Les smartphones et la couverture haut débit sont de plus en plus répandus, y compris dans les régions les plus rurales, et, même si la pénétration n'est pas universelle, le recours aux informations biométriques en association avec d'autres processus de confirmation de l'identité peut permettre d'étendre l'accès à l'identification et aux services qu'elle autorise.

Faciliter l'acquisition de clients

Les opérateurs de téléphonie mobile, les banques et les organismes gouvernementaux ont tous besoin d'une identification sécurisée. Sans elle, il est impossible de procéder à des transactions sécurisées ou de verser des allocations de manière fiable. Mais une grande partie de la population n'est pas en mesure de se rendre aux bureaux situés dans les grandes agglomérations, souvent éloignées. Par conséquent, ces personnes ne peuvent pas participer au système.

En 2017, plus de la moitié des Africains n'avaient pas de compte bancaire . En plus d'être un handicap pour les individus, cela affecte également les petites et moyennes entreprises, qui sont la clé de la croissance économique et qui ont du mal à accéder aux services financiers.

En donnant la possibilité d'établir leur identité aux personnes qui en ont le plus besoin, la confirmation d'identité et l'authentification peuvent les intégrer au système. Une fois qu'une personne est identifiée de manière fiable, elle peut accéder à une gamme de services plus étendue. Cette étape d'intégration initiale est la plus importante.

Les exigences de l'identité

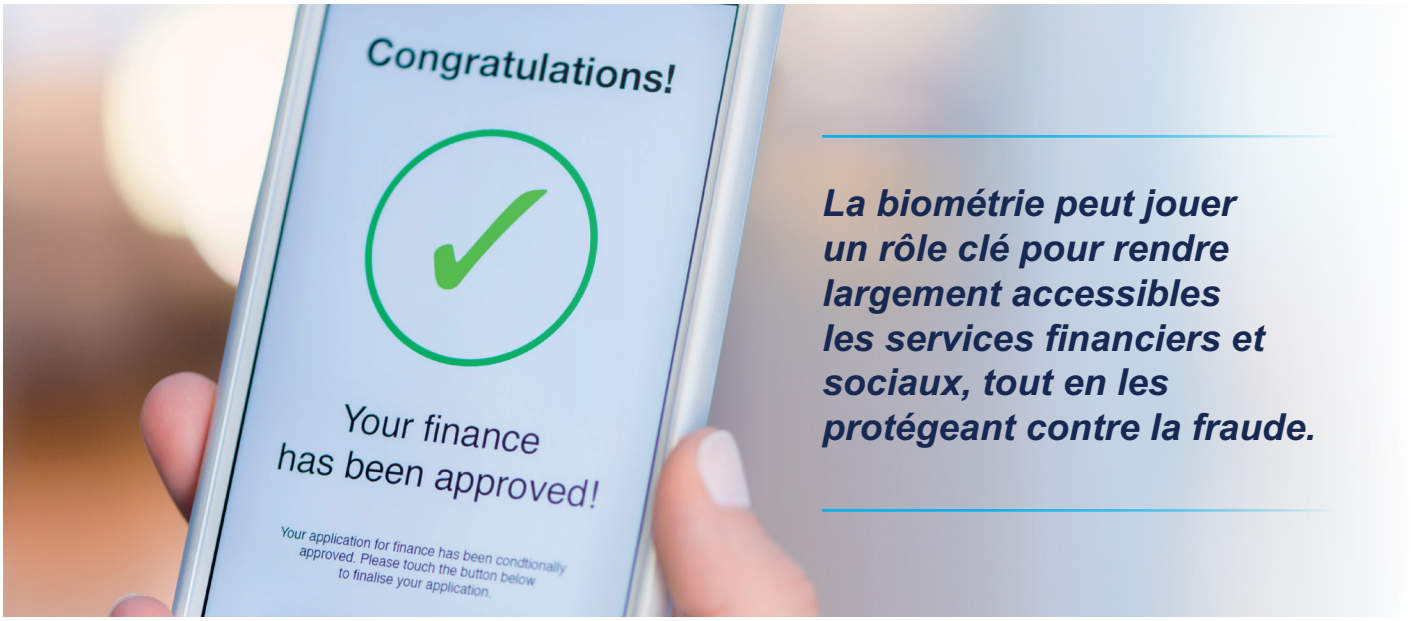
L'intégration par enregistrement biométrique implique de capturer les données biométriques et biographiques du candidat, en s'appuyant sur des preuves d'identité fiables telles que des extraits de naissance, des certificats de mariage, des diplômes, des contrats de travail, des certificats de service militaire, et même des factures de services publics.

Les personnes dénuées d'identité sécurisée ont du mal à accéder aux services sociaux, à envoyer de l'argent à leur famille et à participer à la vie politique. De leur côté, les gouvernements ont davantage de mal à recueillir des données sur la progression des divers programmes de développement. Et sans identité sécurisée, les problèmes de fraude et d'identités multiples sont bien plus fréquents.

Mais l'établissement d'une identité doit être accomplie systématiquement et de manière fiable afin que cette identité soit considérée comme sûre. Au début du processus, des erreurs peuvent persister.

Biométrie et détection du caractère vivant

La biométrie est un puissant outil pour l'intégration mobile sécurisée, et ce pour plusieurs raisons. Tout d'abord, elle permet de confirmer l'authenticité d'une session d'intégration, ce qui rend la fraude plus difficile. Elle permet également d'authentifier les interactions futures à l'aide des données biométriques collectées lors de la session d'intégration fiabilisée. Enfin, elle peut servir à empêcher un individu d'effectuer de multiples transactions au sein d'un système.



La biométrie peut jouer un rôle clé pour rendre largement accessibles les services financiers et sociaux, tout en les protégeant contre la fraude.

Les empreintes digitales sont notre donnée biométrique la plus traditionnelle, et, même si elles sont sans doute plus précises que la reconnaissance faciale (avec plusieurs empreintes digitales), cet avantage se réduit. En outre, la nécessité de prendre plusieurs empreintes de doigts la rend moins pratique et plus susceptible aux erreurs de capture. Bien que les smartphones disposent de lecteurs d'empreintes digitales, ils ne donnent pas accès aux données d'empreintes digitales brutes qui seraient exploitables par des applications tierces.

Des avancées spectaculaires dans les algorithmes de reconnaissance faciale ont rendu cette modalité biométrique plus fiable, plus économique et plus facile à mettre en œuvre, en particulier dans des conditions environnementales raisonnables. La plupart des smartphones sont désormais équipés d'appareils photo de grande qualité qui peuvent servir à collecter des images du visage de qualité biométrique.

Lors d'une session d'intégration, la reconnaissance faciale peut servir à comparer directement une image de visage à une preuve d'identité officielle, à condition que l'image de la pièce d'identité soit d'assez bonne qualité. À l'avenir, les cartes d'identité en papier et en plastique seront de plus en plus complétées, avant d'être finalement remplacées, par des identifiants numériques mobiles. Les gens ont en effet tendance à moins oublier leur téléphone que leurs papiers d'identité. Le transfert de ces identifiants vers l'univers numérique entraînera une foule d'avantages.

La reconnaissance faciale est une modalité biométrique unique, car les humains sont naturellement doués dans ce domaine. Cela signifie que les données biométriques faciales jouent un rôle prépondérant dans les applications d'identification, même sans le recours à des algorithmes biométriques (ce qui explique évidemment que les visages soient imprimés sur les preuves d'identité). Ainsi, contrairement aux empreintes digitales et autres modalités, il est possible d'implémenter des flux de travail qui utilisent les comparaisons de visages à la fois par des humains et des algorithmes.

La détection du caractère vivant est un aspect essentiel de l'intégration biométrique et de l'authentification mobile, en particulier la reconnaissance faciale. Elle empêche les fraudeurs de tenter d'ouvrir un compte par usurpation, par exemple avec des photos ou vidéos d'une autre personne. Sans détection du caractère vivant, un fraudeur pourrait établir un nombre illimité de comptes frauduleux en utilisant simplement des images numériques ou papier, ou des vidéos d'autres personnes, évitant ainsi la soumission de ses propres données biométriques, qui permettraient autrement de détecter la fraude.

Il existe différentes solutions technologiques pour détecter le caractère vivant et les usurpations, que l'on classe généralement en deux catégories : actives et passives. Une approche active nécessite une certaine interaction avec l'utilisateur : une question et une réponse. Une approche passive, transparente du point de vue de l'utilisateur, s'appuie sur une image ou un flux d'images afin de détecter la preuve que la source de l'image est numérique, papier, ou même un masque 3D.

Conclusion

Tout comme la téléphonie mobile a rendu les télécommunications accessibles à des milliards d'individus mal desservis, les smartphones permettent aujourd'hui de procurer des services financiers et gouvernementaux tout aussi essentiels, et ce sans qu'il soit nécessaire de recourir à des infrastructures physiques. Mais les services de valeur nécessitent une confirmation d'identité et une authentification solides. La biométrie peut jouer un rôle clé pour rendre largement accessibles les services financiers et sociaux, tout en les protégeant contre la fraude.