L'enregistrement numérique des clients établi avec Aadhaar: une nouvelle ère pour l'industrie des télécommunications en Inde

IDENTITÉ

POSTÉ LE 17.05.17

Suite à la décision du gouvernement indien de rendre obligatoire l'enregistrement numérique de tous les clients des réseaux de téléphonie mobile, les opérateurs téléphoniques se sont mis en quête d'une solution pour remplacer l'ancien processus d'enregistrement manuel, fastidieux et peu sécurisé. Cette alternative dématérialisée et plus efficace devait renforcer la confidentialité des données personnelles et raccourcir considérablement les délais d'activation des cartes SIM. La réponse trouvée par l'Industrie des Télecoms consiste à lier l'identification numérique des clients au numéro d'identification national « Aadhaar ».

La plus vaste base de données d'identités numériques au monde

Le projet national de **numéros d'identification indien Aadhaar**, lancé en 2010 sous la gestion de l'autorité indienne d' **identification unique**, l'UIDAI, est le plus vaste programme d'**identités numériques** au monde. Chaque habitant se voit ainsi attribuer un **numéro d'identification unique** à douze chiffres afin de constituer une base de données de la population indienne unique et fiable. Pour cela, les citoyens suivent une procédure d'**enrôlement** durant laquelle une photo du visage, dix empreintes digitales et le scan des deux iris, sont enregistrés avec les données démographiques des résidents (nom, adresse, sexe et date de naissance). Une fois l'enregistrement terminé et les **informations biométriques vérifiées**, le **numéro Aadhaar** est attribué. Pour confirmer l'**identité** d'une personne, les fournisseurs de service peuvent ainsi soumettre le **numéro Aadhaar** et une **caractéristique biométrique** (telle que des empreintes digitales) de l'intéressé à l'UIDAI, qui valide ou invalide immédiatement son **identité**. En 2017, le programme a dépassé les **1,1 milliard de numéros Aadhaar** créés.

Un socle pour l'enregistrement numérique des clients des opérateurs de télécommunications

Safran Identity & Security a mis au point une **solution d'identification numérique des clients** répondant au besoin du secteur indien des télécommunications mobiles, en s'appuyant sur le **système Aadhaar.** Cela a été le début, pour les opérateurs de réseaux mobiles du passage à un enregistrement fluide et dématérialisé des abonnés. Lorsque les utilisateurs souhaitent obtenir une nouvelle carte SIM, leur **identité est vérifiée** en combinant leurs **données biométriques** (scan de l'iris/empreinte digitale) à leur **numéro Aadhaar**. Ces **données biométriques**, ici l'empreinte digitale par exemple, sont comparées à celles de la base de données de l'UIDAI et le résultat immédiatement envoyé à l'opérateur ainsi qu'au point de vente. L'abonnement peut ainsi être activé sans délai. La **solution d'enregistrement des clients** permet une inscription numérique des abonnés grâce aux lecteurs d'empreinte digitale de Safran Identity & Security et services associés, pris en charge par les terminaux mobiles **MorphoTablet** entièrement intégrés pour une interface utilisateur unique. Le Groupe a fourni aux opérateurs indiens une **solution d'enregistrement numérique des clients**

leur permettant de répondre efficacement à la résolution du gouvernement de mettre en place une identification des abonnés. En outre, le processus d'enregistrement très exhaustif assure aux opérateurs qu'ils peuvent s'appuyer sur des **identités fiables** de leurs abonnés pour développer davantage de services.

Une nouvelle ère pour l'enregistrement de la clientèle

Les opérateurs de réseaux mobiles sont entrés dans une nouvelle ère d'inscription de leurs clients. Airtel, premier opérateur mobile en Inde, a choisi la solution d'**enregistrement numérique des clients** proposée par Safran Identity & Security après une démonstration de faisabilité qui s'est déroulée à Lucknow, en Uttar Pradesh. Le nouveau **système d'enregistrement des utilisateurs** sera d'abord introduit dans les points de vente Airtel, puis dans ceux gérés par des revendeurs. *« L'enregistrement de la clientèle pour les lignes mobiles s'appuyant sur le système Aadhaar est une avancée historique pour l'industrie des télécommunications et représente une véritable amélioration de l'expérience client grâce à une inscription plus rapide. Maintenant, les clients peuvent ressortir d'un magasin Airtel avec une ligne mobile activée en quelques minutes seulement. Cette solution complète en outre la stratégie digitale du gouvernement indien et vient s'ajouter aux initiatives écologiques d'Airtel »*, déclare Ajai Puri, Directeur des Opérations (Inde & Asie du Sud) chez Bharti Airtel.

Vodafone, un autre opérateur de réseau mobile majeur en Inde, a également adopté la **solution d'enregistrement numérique des clients** de Safran Identity & Security. Sandeep Kataria, Directeur commercial de Vodafone India, explique: *« Nous déployons ce système d'enregistrement des clients à travers tout le pays. L'inscription numérique permettra de réduire considérablement les délais d'activation de nouvelles lignes mobiles dus à des problèmes d'infrastructure tels que les pannes de courant, le transport de kilos de papier et le manque de ressources en photocopiage et photographie. Cette solution renforcera de plus le processus de vérification en éliminant le risque d'erreur manuelle. »* Vodafone a mis en place le **système d'enregistrement de la clientèle** par étapes dans ses plus de 10000 magasins licenciés en zone urbaine comme rurale, ainsi que chez ses revendeurs à travers tout le pays.

Un enregistrement exhaustif des clients combiné au système Mobile Connect: l'opérateur comme passerelle de services pour ses abonnés

Une fois l'**identité** de leurs clients établie de manière fiable et sécurisée, les opérateurs mobiles sont à même d'offrir un large choix de nouveaux services. Durant le processus d'inscription, l'**identité de l'utilisateur** est enregistrée et associée à un identifiant déterminé par l'opérateur. Une fois la procédure terminée, l'identité de chaque abonné est ainsi établie de façon sûre.

La GSMA, l'association des opérateurs de réseaux mobiles, a mis au point une solution de connexion sécurisée universelle intitulée Mobile Connect, permettant aux abonnés d'accéder aux services mobiles simplement, avec leur téléphone, selon un processus sécurisé utilisant les cartes SIM comme moyen d'authentification protégé. Mobile Connect permet aux clients de créer et gérer leur **identité numérique universelle** au travers d'une seule identification. Mobile Connect vérifie et autorise l'accès en ligne en utilisant le numéro de téléphone unique de l'abonné, associé à un PIN unique pour un usage encore plus sécurisé. Comme ils sont automatiquement identifiés grâce à leur carte SIM, les utilisateurs n'ont plus à retenir leurs identifiant et mot de passe pour chaque service. Les réseaux mobiles sont chargés de comparer l'**identité des utilisateurs** avec l'identifiant lié à la carte SIM. De cette façon, les fournisseurs de service peuvent se fier à l'identité de l'utilisateur vérifiée, sans avoir à accéder à ses informations personnelles. En outre, Mobile Connect permet aux utilisateurs de décider quels éléments d'identité ils souhaitent communiquer à leurs fournisseurs de service, de manière à ce qu'ils contrôlent l'utilisation de leurs données. Cela signifie également que les fournisseurs n'ont pas à constituer d'importantes bases de données d'**identités numériques**, qui courent toujours le risque d'être la cible des hackeurs.

En Inde, Mobile Connect a déjà été adopté par:

- Aircel, Bharti Airtel, Idea, Tata Teleservices Ltd, Telenor et Vodafone.

Mobile Connect est également utilisé par un grand nombre de services tels que GaneshaSpeaks, GoIbibo, Trupay, Twigly, Zee Digital Group et Zomato, actifs dans le domaine commercial, banquier et financier, le secteur de la santé, les médias et le divertissement, ainsi que le voyage et l'hôtellerie. Enfin, les services B2B de Mobile Connect opérés par mXpresso ont été déployés par BuyHatke et Times Mobile Ltd pour empêcher les installations frauduleuses et le téléchargement de fausses applications.