Façonner l'avenir des titres de voyage numériques (digital travel credentials)

Enseignements tirés du premier projet pilote transatlantique DTC-1 au monde.

IDENTITÉ

POSTÉ LE 12.05.24

Peu de sujets ont été abordés lors des récents événements du secteur de l'identité aussi souvent que les Titres de voyage numériques (DTC). Cependant, les présentations et les articles viennent rarement des personnes concernées et sont peu souvent rédigés par une personne réellement impliquée dans un pilote en conditions réelles d'exploitation. La plupart des informations et des conseils proviennent toujours de fournisseurs qui n'ont pas ou très peu d'expérience en dehors de leur bulle de R&D.

Nous devons changer cette situation ! Tout récemment, au nom d'IDEMIA Smart Identity, j'ai eu l'honneur de présenter ce que l'on a pu apprendre du premier projet pilote transatlantique DTC-1 lors du **symposium TRIP de l'OACI** à Montréal, au Canada.

Voici ma présentation :

Fait marquant 1 : Les DTC représentent des avantages concrets pour les utilisateurs et les gouvernements

Cela ne surprendra pas les acteurs du secteur qui travaillent sur ce sujet depuis un certain temps, mais il est tout de même important de mentionner que les résultats du projet pilote auquel IDEMIA Smart Identity a participé ont prouvé ces avantages. Un DTC, même « simplement » de type 1, garantit une expérience de voyage plus sûre et plus pratique. L'optimisation des procédures de contrôle aux frontières et l'amélioration du flux de passagers permettent de réduire les coûts de la police des frontières.

Fait marquant 2 : Les enseignements tirés du premier projet pilote transatlantique sont encourageants

IDEMIA Smart Identity a été le fournisseur de technologie du premier projet pilote transatlantique DTC-1, réalisé par un consortium néerlandais et cofinancé par la Commission européenne. L'ensemble des acteurs s'attendaient à ce que ce projet ne se déroule pas bien. Il y a évidemment eu des obstacles à surmonter, sur lesquels nous nous concentrerons davantage dans nos projets à venir. Dans l'ensemble, il est apparu très rapidement que nous étions confrontés à un « triangle de fer », visant à obtenir la meilleure expérience pour les voyageurs, la sécurité des données et la protection de la vie privée, de manière égale et sans compromis. C'est certainement le cas dans de nombreux cas d'exploitation de

l'identité, mais lorsqu'il s'agit de voyages internationaux, ce défi prend une toute autre dimension.

Voici nos principales recommandations pour les prochains projets DTC :

1. **Mettre le voyageur au cœur du process pour l'inciter à adopter le projet**
   Aucun projet d'identité numérique ne sera jamais couronné de succès s'il n'est pas conçu en fonction de l'utilisateur final. Une expérience utilisateur complexe, ou simplement les plus petits obstacles à franchir, conduiront le public cible à abandonner l'innovation et à revenir aux anciennes méthodes fiables – dans notre cas, le passeport physique.
   Nous devons garder en tête l'ensemble du trajet. Lors d'un voyage international, de nombreux acteurs et systèmes différents entrent en jeu. Tous les systèmes doivent fonctionner les uns avec les autres, offrir la même expérience pratique et inclusive à l'utilisateur et avancer avec différentes versions de la technologie (différentes générations de smartphones, de systèmes d'exploitation, etc.). Si un seul élément est défaillant à cet égard, c'est toute la chaîne qui est affaiblie. Cela implique, aussi simple que cela puisse paraître, de mettre l'accent sur le UX Design, les guides d'utilisation et les tutoriels destinés à l'utilisateur final.
2. **Atteindre le plus haut niveau de sécurité demande de se concentrer sur les systèmes sous-jacents**
   L'adoption des identités numériques est motivée par l'expérience utilisateur et les avantages qui en découlent (voir le point ci-dessus), mais seulement si l'utilisateur final peut compter sur le processus. La confiance est fondée sur le plus haut niveau de sécurité des systèmes concernés. La biométrie joue sans aucun doute un rôle essentiel dans la délivrance et l'utilisation des identités numériques, mais elle va plus loin. L'authentification multifactorielle n'est qu'un exemple des mesures de protection à intégrer dans l'ensemble du processus. La gestion du Répertoire des Clés publiques de l'OACI, le répertoire central pour l'échange des informations nécessaires à l'authentification des passeports électroniques, demeure particulièrement importante, même dans le cas d'un DTC.
3. **Protéger les données implique de ne faire aucun compromis**
   Une solution DTC induira inévitablement le stockage et le transfert de données personnelles sensibles, telles que des informations biométriques et des documents de voyage. La conformité avec la réglementation en matière de protection des données est indispensable : la protection des données est non négociable. Nous devons avoir la certitude que les individus ont une complète maîtrise de leurs données personnelles. Il s'agit notamment d'obtenir un consentement explicite pour la collecte des données, d'assurer la transparence de l'utilisation des données et de donner aux utilisateurs le droit de révoquer leur consentement ou de demander la suppression de leurs données.
   La minimisation des données est évidemment une réponse fiable à ce défi. Une solution DTC ne collecte et ne stocke que le minimum de données nécessaires à la vérification de l'identité et aux voyages, et ce pour une durée limitée, ce qui reste conforme aux principes de minimisation des données énoncés dans les réglementations relatives à la protection de la vie privée.
   Étant donné qu'il s'agit de voyages internationaux, dans notre cas entre les Pays-Bas et le Canada, les données seront transférées au-delà des frontières. Le respect des réglementations est donc nécessaire dans tous les pays concernés.

Pourquoi est-ce que j'affirme que ces enseignements sont encourageants ?

Effectivement, ces sujets ne sont pas nouveaux dans l'écosystème de l'identité. En effet, la complexité est extrapolée dans le monde des voyages internationaux par rapport à la création d'un régime national. Ces problèmes ne sont toutefois pas insolubles. L'élément clé reste qu'une identité numérique n'est pas « simplement » une version numérique d'un titre d'identité physique, mais qu'elle dépend entièrement de la performance et de la sécurité des systèmes sous-jacents. Un travail permanent sur les systèmes biométriques nécessaires et une expérience en la matière sont la seule manière de mettre en œuvre un projet avec succès.

Fait marquant 3 : Les DTC ne sont pas prêts de disparaître

Dans ce contexte, le retour d'information sur le projet pilote le confirme : les DTC sont là pour durer. Les avantages escomptés ont été confirmés et les voyageurs sont prêts à adopter une telle innovation. Comme souvent, c'est le cadre réglementaire qui est à la traîne, mais même dans ce cas, la concrétisation d'un tel projet pilote a accru la pression politique et a donné lieu à des discussions intéressantes.

Plus de projets pilotes, et de plus grande envergure, sont déjà prévus, ce qui, espérons-le, renforcera la confiance générale dans ce changement révolutionnaire dans notre façon de voyager. Chez IDEMIA Smart Identity, nous sommes assurément prêts à mettre nos connaissances en pratique.

À propos de l'auteur : Sahy Rabarimeriarijaona est Responsable produit Mobile ID chez IDEMIA Smart Identity.