

# L'identification numérique dans le secteur du transport aérien

Améliorer la sécurité, l'efficacité et  
la commodité, tout en réduisant les  
risques et la fraude.

Le point de vue d'Interac Corp.



« Les vols  
internationaux devraient  
se chiffrer à 1,8 milliard  
d'arrivées par année  
d'ici 2030. »

# Introduction

Avant la pandémie de COVID-19, le transport aérien international devait se chiffrer à 1,8 milliard d'arrivées par année d'ici 2030<sup>1</sup>. Même si la pandémie a sans aucun doute causé un choc sans précédent dans le secteur à court terme, il est toujours possible que ce dernier connaisse une croissance à long terme, mais elle pourrait survenir différemment.

La pandémie a non seulement soulevé des préoccupations évidentes en matière de santé qui doivent être prises en compte dans le cadre des questions de sécurité transfrontalière, mais les gouvernements, les aéroports et les compagnies aériennes doivent également tenir compte de la façon dont le transport aérien devra s'adapter aux changements démographiques plus généraux et des pressions qu'ils exerceront sur les infrastructures de transport existantes.

Au cours de la prochaine décennie, une grande partie de la population mondiale sera composée des générations post-numériques, soit les personnes qui utilisent la technologie en ligne

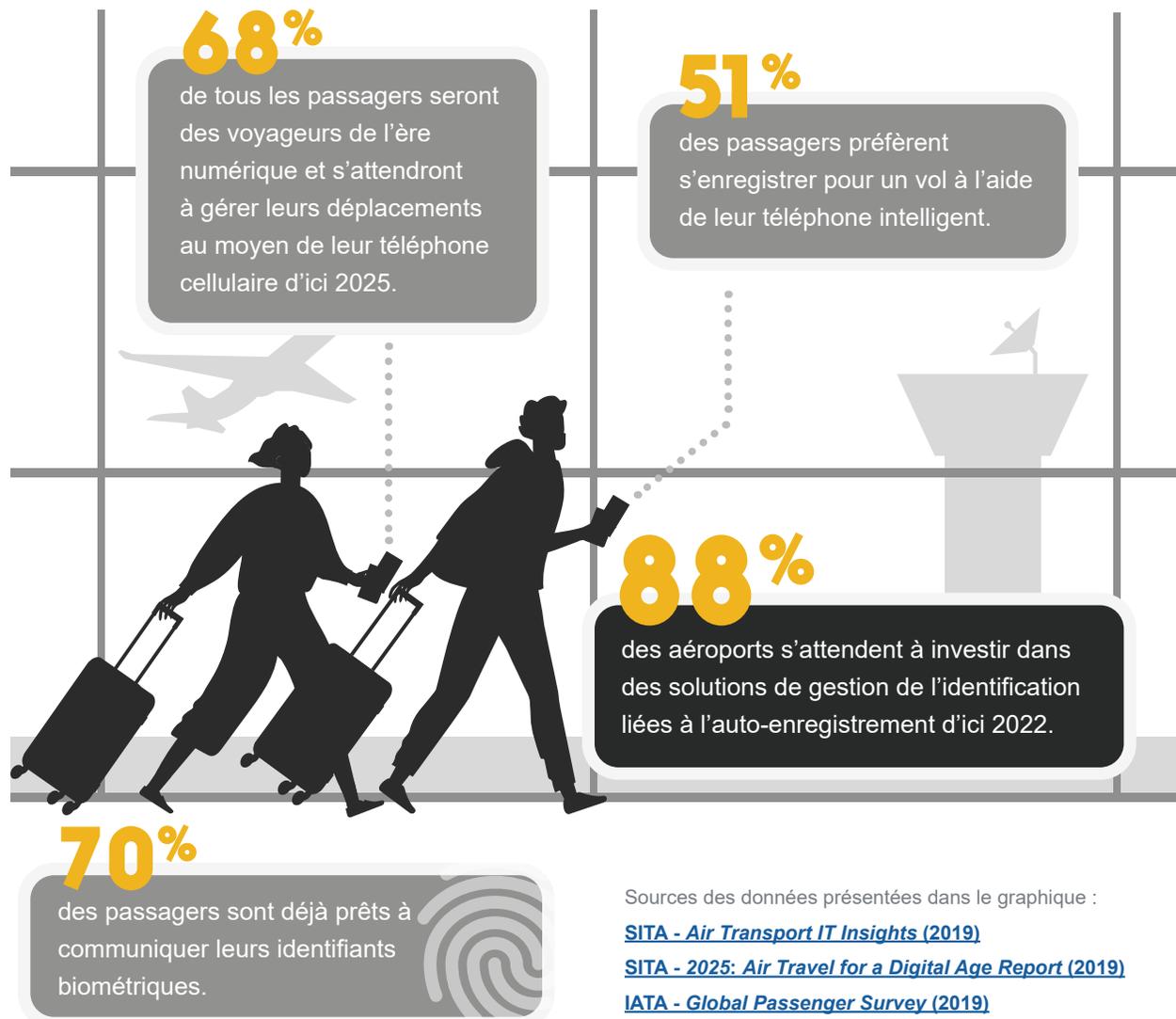
depuis leur enfance et qui s'en servent activement de diverses façons pour gérer leur vie. Les aéroports et les compagnies aériennes devront principalement effectuer une transformation numérique dans le but d'améliorer l'expérience des passagers pour les natifs de l'ère numérique, tout en réduisant les coûts. De leur côté, les gouvernements devront adopter des technologies fiables afin de faciliter les mouvements transfrontaliers légitimes, tout en repérant les mouvements illégaux et en réduisant la propagation des agents pathogènes nuisibles.

Parmi les tendances technologiques importantes qui façonnent l'avenir du transport aérien, l'identification numérique donne lieu à une expérience aéroportuaire nécessitant peu d'interventions, améliore la surveillance de la sécurité, accélère le traitement des passagers et réduit les ressources nécessaires pour gérer le parcours de ces voyageurs post-numériques.

<sup>1</sup> [Baromètre du tourisme mondial – OMT \(janvier 2017\)](#)

# Comment le secteur du transport aérien évolue-t-il?

Les voyageurs post-numériques s'attendent à un niveau de service plus personnalisé et à un moins grand nombre de points de friction pendant leur parcours. L'identification numérique tire parti des progrès des technologies émergentes, comme la biométrie (pour vérifier de façon sûre l'identité des voyageurs), les registres distribués (pour créer un réseau fiable) et la cryptographie (pour améliorer simultanément les capacités en matière de sécurité) sur lesquelles les gouvernements comptent, tout en uniformisant et en améliorant l'expérience de bout en bout du voyageur tout au long de son parcours.



# Quelle aide l'identification numérique peut-elle offrir?

## Gouvernements

**Renforcement de la sécurité** en passant d'étapes subjectives d'identification et d'autorisation à un processus d'authentification automatisé et fiable.

**Diminution des coûts** en réduisant le nombre d'employés nécessaires grâce à l'efficacité des technologies de numérisation et de vérification automatisées.

## Compagnies aériennes

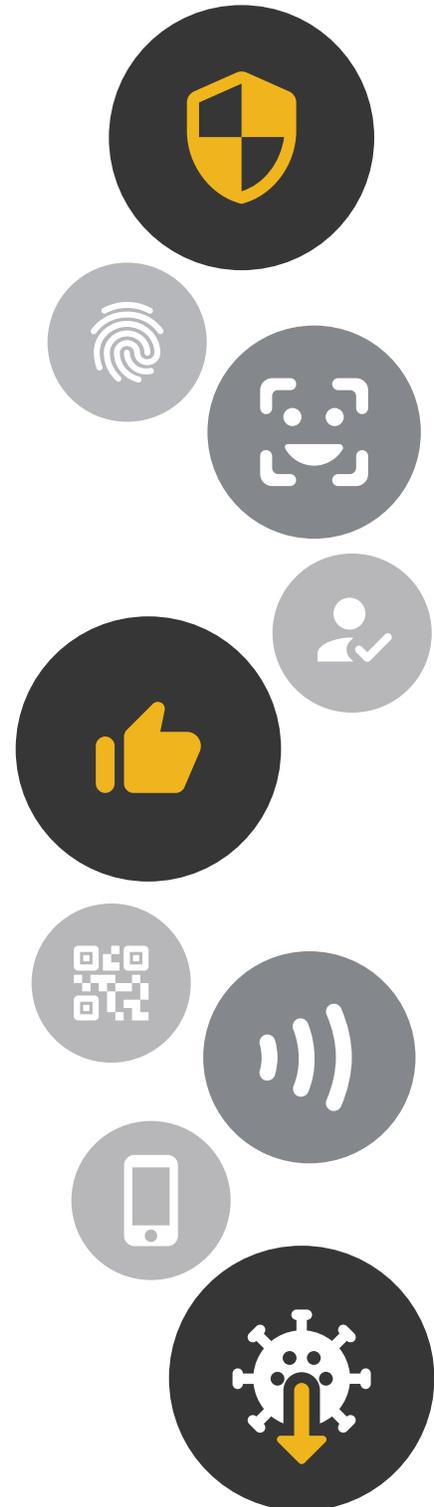
**Réduction de la fraude** en tirant parti d'une mesure d'authentification supplémentaire, afin de prévenir les contrepassations illégitimes liées à des achats légitimes et l'exploitation des programmes pour grands voyageurs.

**Accroissement de la capacité et l'efficacité** en éliminant les points de contrôle d'identification manuels qui exigent beaucoup de temps et en facilitant une rapidité accrue des autorisations pour les passagers à l'arrivée et au départ.

## Passagers

**Amélioration de la confidentialité et de la sécurité** en offrant aux passagers le contrôle et la transparence liés aux renseignements qu'ils communiquent.

**Plus grande commodité et réduction des risques** en permettant aux voyageurs d'utiliser leurs appareils tout au long de leur parcours et de passer de façon harmonieuse à chaque poste de contrôle au moyen de la fonction sans contact, tout en réduisant le risque de transmission d'agents pathogènes.



# Parcours de l'utilisateur

## Étape 1 :

### Ouverture du portefeuille numérique

Julian arrive à l'aéroport, enregistre ses bagages et se rend au poste de contrôle de sécurité. Il ouvre son portefeuille numérique et prépare ses identifiants de voyage numériques\* aux fins de vérification.



## Étape 2 :

### Option sans contact ou de numérisation d'un appareil

L'agent de sécurité indique le terminal à partir duquel Julian doit utiliser l'option sans contact de son appareil pour communiquer les renseignements nécessaires tirés de ses identifiants de voyage numériques et vérifier son identité.



## Étape 3 :

### Authentification et vérification

Au moment de l'authentification, Julian est invité à communiquer ses renseignements et à effectuer un test de détection du caractère vivant. Le terminal affiche une lumière verte clignotante une fois qu'il a utilisé l'option sans contact de son appareil et que la vérification a été effectuée.



## Étape 4 :

### Aller de l'avant

Au moment de la vérification, cet échange d'identifiants est enregistré dans le portefeuille numérique de Julian et il va de l'avant.

\* Voir la page suivante



## Identifiants de voyage numériques

Les identifiants de voyage numériques constituent un jeton biométrique sécurisé, mobile, vérifiable et unique qui contient l'image faciale du voyageur, des renseignements personnels et des caractéristiques de sécurité afin d'appuyer son authentification.

À moyen et à long terme, les identifiants de voyage numériques permettront aux gouvernements de se fier beaucoup plus aux données biométriques et biographiques qu'ils reçoivent directement des passagers, car ils confirmeront instantanément que les données sont authentiques, qu'elles ne sont pas contrefaites et qu'elles n'ont pas été modifiées de quelque façon que ce soit.

# Nos principes

Il est facile de discuter de l'identification numérique de manière théorique, mais il est beaucoup plus complexe de concevoir une architecture et de mettre en œuvre un système d'identification numérique complet, sécuritaire et durable. Pour ce faire, il faut suivre un ensemble de principes clairement définis. Selon nous, cinq principes sont essentiels :



## **Contrôle par l'utilisateur et commodité**

Personne ne veut confier ses renseignements personnels à un système si les données doivent être transférées et stockées par de nombreuses parties, surtout si cela se fait à l'insu de l'utilisateur et sans son consentement exprès. En plus de veiller au contrôle par l'utilisateur, un système d'identification doit être commode et facile à utiliser. Si ce n'est pas le cas, les gens, qui sont nombreux à être déjà habitués aux applications intuitives des appareils mobiles, ne voudront pas l'adopter.

## **Normes et ouverture**

Dans un système dynamique, il est difficile de prédire l'avenir. Il est donc important d'établir des solutions qui sont conformes à des normes acceptées de façon universelle. Non seulement cela permet-il d'éliminer des dépenses liées à l'établissement du système de base et à l'adaptation de solutions ou à la création de solutions ponctuelles par la suite, mais cela permettra aussi de relier à la solution initiale des solutions créées par d'autres à l'avenir. L'ouverture favorise l'adoption, l'innovation et la souplesse.

## **Omniprésence**

Lorsque les gens créent différents identifiants et mots de passe pour tous les services publics et privés auxquels ils doivent accéder, les menaces à la sécurité augmentent, car ils vont le plus souvent se limiter à un seul mot de passe facile à

mémoriser (et facile à deviner). De plus, un identifiant numérique ne donnant accès qu'à un nombre limité de services ne suscitera probablement pas une grande adhésion. Un système omniprésent sera donc plus commode et plus sécuritaire.

## **Marque de confiance**

Aucun utilisateur n'est susceptible d'adopter une solution d'identification conçue ou maintenue par une organisation en laquelle il n'a pas confiance. La question de l'identité est trop importante et les répercussions du vol d'identité sont trop grandes pour s'en remettre au hasard. De plus, l'établissement d'une solution à grande échelle (et omniprésente) exige la coopération et la coordination de nombreux intervenants, et ces derniers doivent pouvoir se faire confiance, et avoir confiance en l'organisation dirigeant cette initiative.

## **La sécurité par l'abstraction**

Même avec les meilleurs contrôles par l'utilisateur, certaines données d'identification doivent faire partie des transactions de tout écosystème. L'une des façons les plus efficaces de sécuriser ces données est de les rendre « abstraites » en remplaçant un identifiant privé par un identifiant public (comme l'adresse de courriel d'une personne), ou par un numéro aléatoire utilisé comme une sorte de jeton autorisé aux fins de l'opération, et utilisé à aucune autre fin.

# Conclusion

La pandémie de COVID-19 continuera sans aucun doute de décourager les déplacements par avion dans un proche avenir, mais les voyageurs afflueront vers de nouvelles destinations en plus grand nombre au cours de la prochaine décennie. Les gouvernements et les compagnies aériennes s'appuieront sur les technologies émergentes pour améliorer la capacité et l'efficacité des aéroports, tout en offrant aux voyageurs post-numériques l'expérience sécuritaire et harmonieuse à laquelle ils s'attendent.

Le processus d'approbation nécessitant beaucoup de main-d'œuvre et dans le cadre duquel les voyageurs font la file pour prouver leur identité en présentant des documents de voyage sera bientôt chose du passé. L'identification numérique offre de nombreux avantages par rapport à ces processus traditionnels, car elle donne lieu à une expérience aéroportuaire nécessitant peu d'interventions, tout en offrant un moyen d'authentification des voyageurs très sûr, résistant à la fraude et pratique pour les nombreux points de contrôle de leur parcours.

Si vous souhaitez collaborer avec *Interac* au sujet de l'avenir de l'identification numérique, écrivez-nous à [digitalid@interac.ca](mailto:digitalid@interac.ca)

« Les voyageurs post-numériques s'attendent à un niveau de service plus personnalisé et à un moins grand nombre de points de friction pendant leurs déplacements. »





**Pour en savoir plus sur ce sujet,  
visitez le site [innovation.interac.ca](https://innovation.interac.ca).**

**Publication : novembre 2020**

**Copyright © Interac Corp., 2020. Tous droits réservés.**

Le logo *Interac* est une marque déposée d'Interac Corp.

Sauf dans la mesure permise par la loi, le présent document ne peut être reproduit ou transmis, en tout ou en partie, sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris la photocopie, sans le consentement autorisé d'Interac Corp. Le présent document est fourni à titre indicatif uniquement, et Interac Corp., en le publiant, ne garantit aucunement que les renseignements qu'il contient sont ou resteront exacts. Interac Corp., y compris ses agents, ses dirigeants, ses actionnaires et ses employés, ne peut être tenue responsable envers toute partie de toute perte ou de tout dommage, quels qu'ils soient, se basant sur l'hypothèse de la fiabilité de l'information contenue dans le présent document.