SECURE IDENTITY ALLIANCE

Authentification : Êtes-vous la personne que vous prétendez être ?

Comment l'Authentification Optique par Machine (OMA, pour Optical Machine Authentication), et notamment par téléphone (OPA, pour Optical Phone Authentication) peut améliorer l'authentification de documents.

2022

Mentions

Secure Identity Alliance (SIA)

La Secure Identity Alliance (SIA) est une association à but non lucratif représentant les acteurs, les organisations et les industries adjacentes, actifs dans l'écosystème de l'identité numérique. La mission de la SIA est d'unifier l'écosystème de l'identité et d'en libérer toute la puissance afin que les personnes, l'économie et la société prospèrent. L'association soutient le développement des activités de ses membres autour de quatre grands axes: "Identity for Good", sensibilisation, développement de normes ouvertes et services à l'industrie.

www.secureidentityalliance.org

Design

Design Motive Ltd

Crédits photo

CST, IDEMIA, Keesing, Shutterstock, Thales, WHO

Révision

Slingshot Communications

Traduction

Oriane Duboz

Production de ce rapport

Auteurs principaux

Frank Smith Observateur Consultant, SIA
(Ancien Directeur Adjoint du Bureau de l'Intérieur Royaume-Uni)

Thomas Poreaux IDEMIA

Contributeurs

IDEMIA
Aimane Ait El Madani
Patrick Guthmann

IN Groupe
Joachim Caillosse (Président du Groupe de Travail 'Document Security')
Amaury Chasseux
Françoise Daniel

Thales
Renaud Laffont-Leenhardt
Alejandro Leon Garcia
Roger Edwards

Veridos
Faten Ben Jemaa

Crime Science Technology
Cosimo Prete
Christophe Halope

OeSD (ÖSTERREICHISCHE STAATSDRUCKEREI)
Claudia Schwendimann

Remerciements

Nous adressons également nos remerciements à la Division Faux monnayage et documents de sécurité (CCSD) d'INTERPOL pour leur examen complet de ce guide.

SECURE IDENTITY ALLIANCE

Table des matières


VISA

Sommaire

Ce document

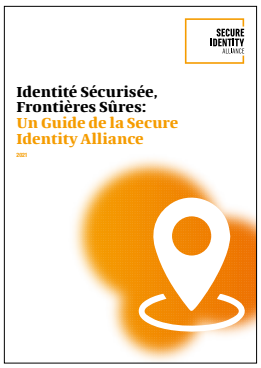
Ce guide examine les défis liés à l'authentification, y compris ses difficultés et les solutions disponibles. Il se penche sur l'automatisation, et plus particulièrement sur l'émergence de l'automatisation de l'analyse optique des documents d'identité notamment à l'aide de smartphones. Cette approche peut permettre de répondre à la question « Êtes-vous la personne que vous prétendez être ? ». L'authentification de documents sécurisés a toujours été cruciale pour le contrôle aux frontières, mais devient également de plus en plus importante dans d'autres contextes : échanges financiers, interactions en ligne et, de plus en plus, pour le grand public.

Ce guide étudie :

- **Les défis de l'authentification de l'identité.** La plupart du temps, les personnes présentant un passeport ou un autre document dans le but de prouver leur identité le font de bonne foi. Il arrive cependant que certaines personnes tentent de se présenter sous une fausse identité. Ce guide examine comment un document et une identité peuvent être attaqués et comment vous pouvez essayer d'authentifier un document pour prouver ou réfuter l'identité revendiquée par un individu.
  Page 4 »
- **Cas d'utilisation.** Comment mettre en pratique ces techniques.
  Page 22 »
- **Recommendations.** D'après l'analyse de ce document
  Page 28 »
- **Glossaire**
  Page 30 »
- **Références**
  Page 31 »

Les informations présentées dans ce guide ont été recueillies et validées en collaboration avec des experts de diverses organisations à travers le monde. Nous avons une fois encore travaillé avec la division Fausse Monnaie et Faux Documents de Sécurité d'INTERPOL (CCSD). Ce guide fait partie d'une large gamme de documents traitant de différents aspects de l'identité, publiée par Secure Identity Alliance (SIA). Plus spécifiquement, il créé un lien naturel entre les guides de la SIA traitant des documents sécurisés (« Tendances Récentes de la Fraude aux Passeports ») et des frontières (« Identité Sécurisée, Frontières Sûres »). Voir :

https://secureidentityalliance.org/ressources/publications



1. Le défi de l'authentification de l'identité

De nombreuses personnes cherchant à prouver leur identité sont de bonne foi et présentent des documents authentiques. Cependant, il existe également des individus cherchant à utiliser de fausses identités à des fins malhonnêtes comme la grande criminalité organisée, l'immigration, illégale le terrorisme ou la fraude.

Il peut donc être crucial de connaître la véracité de l'identité revendiquée par une personne, par exemple pour traverser une frontière, ouvrir un compte bancaire ou effectuer une transaction en ligne. L'examen d'un document d'identité tel qu'un passeport, une carte d'identité ou un permis de conduire représente ainsi une étape très importante.

Les défis auxquels l'authentification de l'identité fait face sont représentés dans la Figure n°1. Il y a une personne ; un document d'identité ; et une identité sous-jacente, dont la personne affirme qu'elle est sienne.

L'association de ces trois éléments est-elle authentique ou fausse ? Les différents éléments de cette identité correspondent-ils les uns aux autres ou la personne essaie-t-elle d'utiliser une fausse identité, peut-être par une tromperie sophistiquée ? Comment en être sûr ?

Figure n°1
Personne, passeport, identité… Correspondent-ils les uns aux autres ?

Notre souhait n'est pas de fournir un guide d'utilisation pour l'usurpation d'identité. Il existe cependant deux façons principales d'usurper une identité :

- **Usurpation d'une pièce d'identité ou d'un autre document.** Cela peut prendre diverses formes, notamment la création complète d'un faux document (contrefaçon) ou la modification d'un document authentique afin de lui faire délivrer de fausses informations. Il peut par exemple s'agir de remplacer la photo d'identité du document d'origine par celle d'une autre personne.
- **Tromperie de la part de la personne qui revendique l'identité.** Cela ne nécessite pas forcément une altération de la pièce d'identité. Par exemple, un individu peut tenter de passer le contrôle aux frontières avec un passeport authentique volé dont la photo présente une grande ressemblance avec l'usurpateur.

Bien entendu, une tentative de falsification d'identité peut impliquer ces deux types de tromperie. Par exemple, il peut arriver qu'un individu réussisse à faire une demande frauduleuse de nouveau passeport et à le présenter à une frontière (on parle alors de Documents Authentiques Obtenus de Manière Frauduleuse. (FOG, pour « Fraudulently Obtained but Genuine »).

La figure N°2 en pages 6 et 7 présente les différentes attaques potentielles et montre les principaux moyens de mitigation ou de défense contre celles-ci, ainsi que des exemples d'outils technologiques pouvant être utilisés.

Figure n°2
Risques et attaques potentielles…

FAUX DOCUMENT

Créer un faux document

- **Falsification :** modification d'un document authentique, par exemple en modifiant la photo de son détenteur ou en personnalisant un document volé vierge
- **Contrefaçon :** création d'un nouveau faux document, en utilisant par exemple du papier sécurisé volé, des éléments de sécurité ou des techniques d'impression de haute précision (usine de faux documents ?)
- **Un Document Authentique Obtenu de Manière Frauduleuse (FOG)**

Attaque de la puce

Le piratage du cryptage est considéré comme étant « au-delà de la faisabilité informatique », mais peut causer :

- **Une puce inactive :** « ça ne marche jamais ! »
- **Exécution ou inspection de la puce** pouvant être trop légère ou non-effectuée
- **Un utilisateur ressemblant** peut ne pas être détecté

PERSONNE FICTIVE OU MALHONNÊTE

Utilisation illégale d'un document authentique

Un document authentique utilisé par une personne n'étant pas son détenteur légitime. L'utilisateur peut ne pas correspondre à la photo mais toutefois réussir à utiliser le document, grâce à :

- Des documents perdus ou volés n'ayant pas été signalés aux autorités
- Un document expiré
- La permission du détenteur légitime

Attaque biométrique

Une attaque dite "par présentation" consiste à tenter' de déguiser les données biométriques de la personne et donc son identité. Cela peut par exemple impliquer l'utilisation d'un masque, d'une photo devant le visage, d'une combinaison de plusieurs visages (morphing), de fausses vidéos générées par ordinateur, de fausses empreintes digitales (gommes recouvrant les empreintes digitales). Dans de nombreux cas, il s'agit d'utiliser un objet inanimé en guise d'une personne vivante.

Malhonnêteté

Une personne déclarant sa réelle identité tout en la prouvant à l'aide de documents authentiques peut toutefois chercher à tromper autrui quant à ses intentions. Par exemple, elle peut déclarer entrer sur un territoire pour des « vacances » alors qu'elle cherche à fuir ses obligations après avoir contracté un emprunt bancaire. Il peut également s'agir d'un individu cherchant à cacher des événements de son passé.

… et les contre-mesures

Examen des documents

Examen détaillé du document afin de vérifier qu'il soit authentique. L'aspect et le toucher du document sont-ils corrects ? La qualité est-elle celle attendue ? Les éléments de sécurité sont-ils présents ? Peut-on observer une quelconque altération ?

- **(1) Contrôle effectué par une personne** : par le grand public, un spécialiste formé, un expert ayant accès à un laboratoire d'analyse en fraude documentaire ?
- **(2) Authentification Optique par Machine (OMA),** par exemple en utilisant un scanner de bureau, ou
- **(3) Authentification Automatisée par Téléphone (OPA),** par exemple en utilisant un appareil photo et en traitant l'image sur smartphone ou sur le Cloud

Entretien

S'entretenir avec un individu peut révéler des éléments utiles et renforcer ou non la confiance en la véracité du document

Système de référence en matière de documents, comme :

- **Liste de surveillance** : passeports perdus ou volés dans le pays
- **Listes de surveillance mondiales** : INTERPOL, documents de voyage volés ou perdus

Vérification électronique de la puce

Les passeports électroniques ainsi que d'autres documents contiennent une puce sécurisée protégée par signature numérique cryptée grâce aux PKI : Infrastructure à clés publiques

Tests biométriques, par exemple

- **La biométrie** est utilisée afin de vérifier la correspondance entre une personne et la photo d'une pièce d'identité ou d'un visa, les empreintes digitales etc.
- Une recherche **« One to Many »** permet de vérifier les différents noms qu'une seule personne peut avoir utilisé par le passé
- Les algorithmes avancés dédiés à la correspondance de données peuvent aider à la détection d'attaque par présentation (PAD, pour « Presentation Attack Detection »)
- En ligne, la détection du vivant - vérification qu'une vraie personne se présente - est très utile

Système de référence de personnes

- **Listes de surveillance** : Suspects potentiels, criminels connus, membres de groupes criminels organisés, terroristes...

Examen du document par un individu

Standard : toucher, regarder, incliner

Expert : différentes sources de lumière, de différents types, avec agrandissement

OMA = OSA et OPA

Inspection Automatisée :

Scanner ou smartphone

Répertoire des Clés Publiques (Le RCP, ou PKD pour « Public Key Directory »)

Répertoire des clés publiques de l'OACI, utilisé pour authentifier (= donner confiance) les puces sécurisées et les données qu'elles renferment (OACI)

Système d'Identification Biométrique Automatisé (ABIS, pour « Automatic Biometric Identification System »)

Base de données permettant de faire correspondre les données biométriques à une identité

1.1
Authentification de documents : trouver le juste équilibre entre l'humain et la machine

L'examen traditionnel d'un document d'identité s'effectue par un opérateur ayant reçu une formation adéquate. Une attention toute particulière est accordée aux agents aux frontières qui reçoivent une formation spécifique à divers aspects tels que : l'identification de faux documents et de contrefaçon, la comparaison de la puce ou de la photo imprimée avec la personne présentant le passeport, ou encore le fonctionnement des systèmes utilisés aux frontières. Un soutien supplémentaire peut également être apporté par des agents disposant d'un équipement de laboratoire, spécialement formés à la détection de fraudes évoluées.
La formation de base des opérateurs moins expérimentés n'est pas aussi efficace mais peut permettre d'insister sur la nécessité de comparer soigneusement les visages et les photos des documents, de prêter attention au comportement et à la façon de parler de la personne, d'être conscient des techniques de falsification les plus courantes et de leur détection, comme « TOUCHER, REGARDER, INCLINER ».

Un examen effectué par l'Homme, et non par une machine, présente divers avantages pouvant être résumés comme suit :

- **Authentification par l'Homme** : Capable de combiner l'examen du document avec une évaluation plus globale de toutes les interactions avec la personne, une connaissance des tendances actuelles en matière de falsification et une expérience significative dans ce travail.
- **Authentification par machine** : Pour les organisations commerciales, l'authentification par machine peut permettre au personnel de valider des documents qu'il ne voit pas souvent, ou de supprimer complètement la prise de décision d'un opérateur non formé. Pour la vérification d'identité à distance, qu'elle soit à des fins commerciales ou gouvernementales (par exemple des eGates, ou l'application mobile d'avant-vol aux États-Unis), la machine automatise l'authentification en cas d'absence d'un agent dédié. Elle fournit également un soutien actif au personnel chargé du contrôle aux frontières, surtout dans le cas d'opérateurs moins expérimentés et plus susceptibles de se fatiguer après une longue session de contrôle.

En fonction du cas d'utilisation, il convient de trouver le juste équilibre entre authentification par l'Homme et authentification par machine pour obtenir le niveau de confiance voulu. Dans certains cas d'utilisation (tels que le contrôle aux frontières ou la délivrance de documents sécurisés), l'authentification par machine ne pourra pas remplacer l'authentification par l'humain. Elle permettra cependant d'assister la personne en charge d'inspecter le document afin d'assurer une authentification plus rapide. L'agent pourra ainsi se concentrer sur les cas réellement difficiles et/ou suspects.

Bien qu'il soit assisté d'une solution automatisée, l'opérateur doit continuer à être vigilant afin d'être en mesure de détecter toute trace d'utilisation frauduleuse d'une identité. Les systèmes automatisés peuvent être très utiles mais, comme tout système, peuvent se tromper. Un opérateur peut repérer des anomalies que la solution automatisée ne voit pas. Celui-ci doit donc garder tous les facteurs nécessaires à l'esprit et ne pas considérer une mention « positive » ou « négative » comme une garantie.

1.2
Authentification Optique par Machine (OMA)

L'Authentification Optique par Machine consiste à effectuer un scan visuel d'un document à l'aide d'un appareil photo. Ce scan est ensuite analysé de diverses manières afin de vérifier son authenticité. Dans ce rapport, on considère les termes suivants :

- **L'OMA** : Couvre toute forme de scan et authentification par lecture optique. (Le guide OACI des meilleures pratiques pour l'authentification par lecture optique utilise le terme 'Optical Machine Authentication' ce qui équivaut à OMA dans le document).

Sscanner de documents (Thales)

- **L'OSA** : 'Optical Scanner Authentication' couvre l'authentification optique par scan, généralement par le biais d'un scanner de bureau. Ces scanners disposent de sources de lumière plus sophistiquées (visible, UV et IR), mais sont moins à même de contrôler les différents éléments de sécurité qui varient selon l'angle auquel on examine le document. L'OSA est particulièrement adaptée dans les cas suivants :
  - » Authentification entièrement automatisée par machine lors du contrôle aux frontière (e-Gates, bornes…) (page 15).
  - » Assister l'authentification effectuée par des opérateurs lors du contrôle aux arrivées / aux frontières (page 15) et dans le secteur privé pour les procédures KYC (page 17).

- **L'OPA** : 'Optical Phone Authentication' couvre l'authentification optique par téléphone, par le biais de smartphones. De par leur caractère complètement mobile, ils peuvent être orientés dans le but d'examiner le document sous plusieurs angles. Suivant le niveau de confiance nécessaire, l'OPA peut être adaptée aux cas suivants :
  - » Assister la personne en charge du contrôle dans la décision d'authentification, par exemple dans le cas des contrôles mobiles aux frontières (page 15) ou des services de police de première ligne (page 17).
  - » Vérification d'identité entièrement réalisée à distance : eKYC pour le secteur privé (page 17) et pour les gouvernements (page 18).

Optical Phone Authentication (IDEMIA)

1.2
Authentification Optique par Machine (OMA) (suite)

1.2.1 Ce qu'il faut savoir à propos de l'OMA :

- Parmi les documents pouvant être testés par l'OMA, on compte : les passeports, les Visas, les cartes d'identité, les permis de conduire et les billets de banque.
- L'authentification OMA des éléments peut être effectuée en ligne ou hors ligne selon la solution et les besoins spécifiques du pays (certaines solutions peuvent fonctionner dans les deux modes). Lorsqu'elle est effectuée hors ligne, la machine intègre un algorithme qui effectue l'authentification par elle-même. En ligne, l'image sera envoyée sur le Cloud où l'algorithme effectuera l'authentification. Une attention particulière doit être portée au choix du Cloud : public ou privé afin de respecter le niveau de sécurité, la confidentialité des données et les réglementations (par exemple la RGPD).
- Les avantages et les inconvénients d'une authentification en ligne et hors-ligne peuvent se résumer comme ceci :

En ligne

» Avantage : La solution peut accéder à la dernière version de l'algorithme et/ou de la bibliothèque de documents.

» Avantage : La procédure peut s'effectuer sur le Cloud, pour un résultat plus rapide effectué sur smartphone.

» Inconvénient : La solution n'est pas disponible sans connexion Internet.

» Inconvénient : La solution peut ne fonctionner que sur des appareils ou smartphones spécifiques.

Hors ligne

» Avantage : La solution est disponible à tout moment.

» Avantage : La solution est vendue avec l'appareil adéquat.

» Inconvénient : Des mises à jour doivent être faites fréquemment, la maintenance ainsi que la gestion de la solution sont plus difficiles à effectuer.

» Inconvénient : Limite les fonctionnalités et la quantité de données auxquelles vous pouvez accéder en utilisant un smartphone ou une tablette.

- L'OMA peut être utilisée dans de nombreux cas, comme : des services financiers, des services de location de véhicule, des contrôles d'accès, des services de sécurité, des services de commerce en ligne, des jeux vidéo, des services publics, des services de santé et l'hôtellerie.
- Suivant le cas d'utilisation, le niveau d'assurance attendu peut varier. Dans le cas d'une utilisation par le gouvernement, un niveau d'assurance élevé peut être nécessaire. Bien sûr, une solution pouvant proposer un niveau d'assurance élevé ainsi qu'une expérience utilisateur simple et agréable sera plus largement adoptée.
- Bien qu'une puce sécurisée intégrant des éléments biométriques apporte un niveau d'assurance plus élevé dans l'authentification de documents (eIDAS, mécanismes de sécurité PKI de l'OACI), intégrer certains éléments de sécurité dans les documents d'identité peut permettre à l'OMA de servir de solution de repli, de complément ou de remplacement de la puce.

Cela apporte également un niveau d'assurance élevé pour les quatre raisons suivantes :

1- Tous les documents n'intègrent pas une puce.

2- Pour des raisons techniques, il peut arriver que la puce ne fonctionne pas (qu'elle soit cassée, abimée ou défectueuse).

3- L'accès à la puce peut être interdit pour des raisons légales (ex : un contrôle d'identité dans le secteur privé).

4- La sécurité des puces n'est pas toujours vérifiée correctement à l'aide de certificats externes. La combinaison de l'authentification de la puce et de l'OMA rend la vie des fraudeurs beaucoup plus difficile.

Les solutions OMA peuvent être divisées en différentes catégories décrites ci-dessous. Il est important de noter que certaines technologies et éléments de sécurité ne sont disponibles qu'auprès de quelques fabricants de documents ou fournisseurs de composants certifiés. Bien que cela soit bénéfique à la sécurité des documents, cela signifie également que certaines technologies brevetées peuvent être exclusives à un seul fournisseur entrainant un risque de dépendance à celui-ci. Ce risque doit être évalué et géré. Ce n'est pas parce qu'un élément est exclusif à un fournisseur qu'il faille nécessairement l'éviter. Lors de la modernisation d'un document, il convient de trouver un juste équilibre entre la sécurité globale et le désir éventuel d'éviter d'utiliser une technologie brevetée.

- Deux points essentiels sont à retenir lors de l'intégration des fonctions de sécurité de l'OMA dans la conception d'un document : D'abord, fournir un niveau d'assurance élevé de l'authenticité du document (il ne s'agit pas d'une copie, par exemple) et ensuite, prouver que son propriétaire est bien la personne qui présente le document :

  » **Pour lutter contre la fraude touchant directement au document ou à la pièce d'identité** : La solution doit contrôler l'intégrité du document pour s'assurer qu'il est authentique, qu'il a été délivré par un organisme autorisé et qu'il n'a pas été modifié. Le meilleur moyen est d'intégrer dans la conception du document des éléments de sécurité contenant et protégeant les informations de son titulaire. Cela concerne tout particulièrement la photo d'identité, qui est à la fois la zone la plus attaquée (par le morphing, par exemple) et la plus examinée d'un document de voyage.

  » **Pour lutter contre la fraude touchant directement à la personne présentant le document ou la pièce d'identité** : Dans le cas d'une authentification à distance, la solution doit permettre de prouver que le document est correct et présenté par son titulaire légitime. Cela peut être réalisé de différentes manières, notamment grâce à un élément de sécurité OMA protégeant le portrait d'identité. Ce dernier peut ainsi être authentifié et comparé de manière fiable avec le visage de son titulaire.

1.2
Authentification Optique par Machine (OMA) (suite)

Les exemples suivants montrent différentes façons dont les technologies OMA peuvent être mises en œuvre…

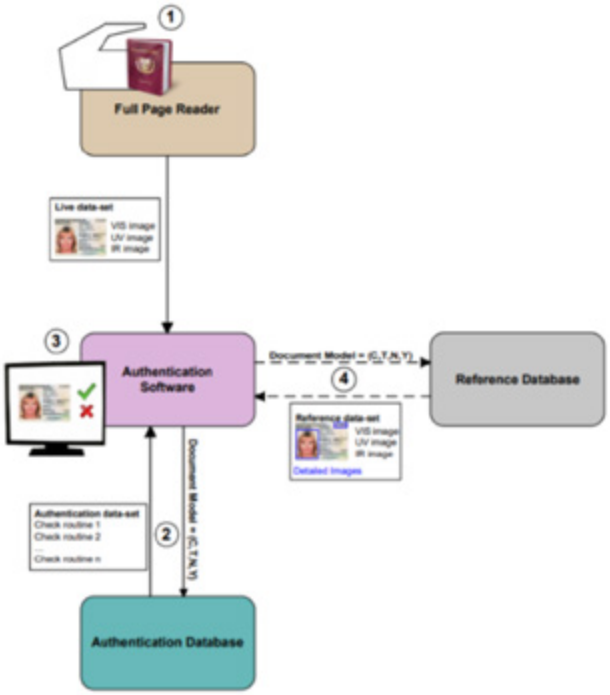
(1) Vérification du modèle : Il s'agit de scanner la partie essentielle d'un document de voyage (dans un passeport : la page de données personnelles) et de vérifier l'image du document par rapport à des modèles de documents connexes stockés dans une base de données de référence, ce qui peut inclure l'utilisation de lumière visible, UV et IR.

Il s'agit aujourd'hui du type de solution de vérification de document assistée par machine le plus largement déployé, car largement utilisé pour le contrôle aux frontières. L'authentification optique peut être réalisée en ligne ou hors ligne. Un algorithme effectue alors plusieurs tests : il vérifie la cohérence de la Zone de Lecture Automatique (ZLA), la compare à la zone d'inspection visuelle (ZIV) du DVLM (Document de Voyage Lisible à la Machine), effectue le test B900 (test de la visibilité sous IR de la ZLM), et bien d'autres encore, recommandés dans le document de l'OACI intitulé "Best Practice Guidelines for Optical Machine Authentication, Part 1- Recommendations" (disponible uniquement en anglais, voir références). Cette solution apporte un soutien à l'opérateur devant authentifier le document et lui permet, dans une certaine mesure, de lutter contre la fraude aux documents de voyage.

Cette solution présente certaines limites. En général, l'authentification par smartphone (OPA) ne permet pas le même niveau d'assurance que l'authentification par scanner (OSA) car un smartphone ne dispose habituellement que de lumière visible, mais pas de lumière UV ou IR. Cette solution n'est pas non plus en mesure de détecter automatiquement une substitution de portraits bien réalisée, ni une altération des éléments de sécurité (comme les hologrammes), les motifs de lignes fines ou les copies papier de qualité supérieure. Par conséquent, il n'est pas toujours possible d'établir le lien entre le titulaire et le document de voyage et donc de contrer l'attaque frauduleuse d'une personne revendiquant une identité.

Image n°22 : Guide OACI des meilleures pratiques pour l'authentification par lecture optique

Source: Keesing



Meilleures pratiques pour l'authentification par lecture optique d'un passeport électronique

Processus d'identification et de vérification des documents ; les chiffres indiquent l'ordre des étapes du processus.

Source: Guide OACI des meilleures pratiques pour l'authentification par lecture optique (Partie 1), Version 1.2, Février 2018

(2) Décodage et vérification des données intégrées, c'est-à-dire codées dans un cachet électronique visible (CEV), un code-barres ou d'autres éléments.

Ces éléments sont maintenant largement déployés dans la conception de documents de voyage. C'est par exemple le cas du code-barres 2D intégré dans le nouveau visa Schengen, qui peut facilement être lu et vérifié à l'aide d'un scanner/smartphone. Suivant sa mise en œuvre, un algorithme en extrait les données (soit en ligne ou hors ligne) qui peuvent être des informations personnelles et/ou biométriques. L'opérateur peut ensuite comparer les données décodées avec les données du document afin de l'authentifier.

En authentifiant les données du titulaire, cette solution permet de proposer un bon niveau d'assurance et de contrer la fraude aux documents de voyage lorsqu'elle est croisée avec les données imprimées et celles de la puce. Elle a cependant ses limites, comme celle de ne pas protéger le document contre la substitution de la photo d'identité. Par conséquent, elle ne permettra pas de faire le lien entre le document de voyage et son titulaire pour contrer une tentative de fraude de la part de la personne qui revendique l'identité.

Visa Européen avec cachet électronique visible (CEV)

(3) Vérification de l'intégrité du document physique : Utiliser les fonctionnalités de logiciels pour vérifier l'intégrité du document et d'autres éléments de sécurité spécifiques.

Dans ce cas, un scanner et/ou un smartphone capture une image ou une vidéo du document de voyage. Celle-ci est ensuite analysée par un algorithme spécifique, en ligne ou hors ligne, qui authentifie un élément de sécurité spécifique. Ce type de fonctionnalité est une tendance croissante dans la conception de documents de voyage et fournit aux opérateurs une réponse claire par « oui » ou « non » pour les guider dans leur prise de décision.

Ces fonctionnalités de l'OMA peuvent permettre l'authentification d'un document de voyage avec un niveau d'assurance élevé. De plus, elles sont souvent conçues dans le but de protéger les données du titulaire en utilisant le portrait pour vérifier l'intégrité du document. Elles assurent également une protection contre la substitution de photos et permettent l'identification à distance en comparant le portrait authentique du document au visage analysé en direct. Cette solution est efficace, tant contre les tentatives de fraude liées directement au document qu'à celles liée à la personne revendiquant l'identité.

Motif guilloché encodé, par Thales

Photometrix, par Surys

Authentification Lasink, par IDEMIA

1.2
Authentification Optique par Machine (OMA) (suite)

(4) Vérification renforcée de l'intégrité d'un document physique, qui peut inclure l'utilisation de l'OMA comme outil pour renforcer des éléments de sécurité plus basiques (connus comme étant de « niveau 1 », comme des dispositifs ou des encres optiquement variables).

Certains éléments de sécurité ont été spécifiquement conçus pour être vérifiés manuellement à l'aide d'un smartphone et facilitent ainsi la prise de décision. L'utilisateur peut par exemple utiliser la lampe torche pour révéler un effet optique spécifique, ce qui serait très difficile à contrefaire. Lier ces effets à une photo d'identité permet notamment d'éviter sa substitution.

Les solutions d'OMA permettent non seulement d'automatiser l'examen des documents de voyage, mais également de guider les opérateurs en leur donnant des astuces et conseils (en étant connecté à une bibliothèque de référence en ligne). Il peut par exemple s'agir du message suivant, pouvant aider l'opérateur dans l'authentification: « ce document est sensé contenir des éléments visibles qui changent d'apparence/de couleur lorsqu'il est examiné sous différents angles - regardez et inclinez le document pour voir si c'est le cas ». En outre, la combinaison de cette technologie avec (2) une solution de décodage et de vérification des données intégrées peut créer un concept amélioré, avec un niveau d'assurance renforcé. Les deux solutions présentent des avantages : l'intégrité du document physique peut être vérifiée manuellement et les données peuvent être décodées à l'aide d'un smartphone ou d'un scanner pour effectuer une authentification automatique ou assister le contrôleur dans l'authentification.

Solution OVM (« Optical Variable Material ») de CST

1.2.2 L'utilisation de l'OMA et autres techniques de vérification

Plusieurs solutions d'OMA peuvent être combinées pour fournir un niveau d'assurance élevé des concepts d'authentification. Par exemple, la combinaison d'une (1) vérification à partir d'un modèle (3) avec une vérification de l'intégrité du document physique renforcera le niveau de confiance et supprimera les inconvénients de la seule vérification à partir d'un modèle (substitution de la photo d'identité, copies…). On cumule ainsi les avantages de chaque solution.

Suivant le cas d'utilisation et le niveau d'assurance recherché, il est possible de coupler une solution d'OMA avec d'autres solutions d'authentification. Par exemple :

- Vérifier des données électroniques d'une puce sécurisée (comme dans le cas d'un contrôle aux frontières ou d'une relation entreprise / client)
- S'entretenir avec le détenteur du document (contrôle aux frontières, services de police de première ligne, vérification KYC…)
- Effectuer une capture biométrique et une recherche/mise en comparaison avec des archives biométriques (contrôle aux frontières, demande de visa…)
- Vérifier s'il s'agit bien d'un humain lorsque la personne utilise un système en self-service (vérification KYC numérique, e-Gates, bornes…)
- Et effectuer des contrôles et/ou mettre à jour les systèmes de référence tels que les listes de surveillance, les dossiers de cas passés et les fichiers d'historiques de voyages (vérification KYC numérique, demande de visa…)

1.2.3 Coopération entre la création et l'authentification de documents

Des éléments visuels peuvent être introduits lors de la fabrication ou personnalisation d'un document de voyage. Dans le cas d'un examen effectué par un individu, il peut s'agir d'éléments de sécurité qui changent d'apparence ou de couleur, comme une DOVID, (pour « Diffractive Optically Variable Image Device »), c'est-à-dire une structure diffractive changeant d'apparence selon l'inclinaison, ainsi que d'encres qui changent de couleur selon l'angle de vue. Dans le cas de l'OMA, le concepteur peut également inclure des éléments de sécurité des différentes catégories énumérées ci-dessus (la vérification à partir de modèles, le décodage et la vérification des technologies de données intégrées, la vérification de l'intégrité du document physique à l'aide d'une fonctionnalité logicielle, la vérification avancée de l'intégrité d'un document physique). Ils peuvent même être liés à un détenteur individuel, pour permettre au processus d'OMA d'authentifier le document de manière plus sûre et ainsi maximiser son efficacité.

1.3
Authentification Optique par Scanner (OSA)

Ce type d'OMA est généralement un scanner de bureau. Il peut s'agir d'une solution robuste pour une utilisation fréquente et à haut volume et peut inclure une gamme plus large de capteurs, comme des lumières ultraviolettes (UV), visibles (directe et oblique), infrarouges (IR) et autres. Chacun de ces capteurs peut potentiellement révéler des éléments de sécurité particuliers à un document donné. Ils seront toutefois plus lourds qu'un smartphone et n'offriront peut-être pas les mêmes avantages en termes de mobilité, de familiarité pour l'opérateur, de facilité de déploiement et d'accès au réseau.

1.4
Authentification Optique par téléphone (OPA)

Les dernières décennies ont vu une augmentation constante de la puissance et des capacités des smartphones et autres outils informatiques mobiles du même type (ordinateurs portables, tablettes, technologies embarquées), ainsi qu'une explosion des performances des infrastructures de communication mobile à haut débit (4G et 5G). Il est maintenant courant que les forces de l'ordre disposent de solutions mobiles ayant accès à un large éventail de fonctions et d'informations sur le terrain. Sans ces solutions, les outils d'information ne seraient accessibles que dans un bureau fixe ou par radio. Ils servent notamment aux contrôles d'identité, à la vérification de passeports et cartes électroniques, à la saisie de données biométriques, à la recherche de données de référence, à la saisie de transactions et aux contrôles mobiles aux frontières.

En plus d'un large éventail d'autres fonctions, l'authentification optique par téléphone (OPA) permet d'élargir les actions pouvant être effectuées par les forces de l'ordre lors de leurs déplacements. En outre, l'OPA peut permettre à des non-professionnels d'avoir accès à l'authentification automatisée de documents, par exemple pour s'assurer de l'identité d'une personne sur le terrain ou à distance comme lors de vérifications KYC (« Know Your Customer », processus de vérification d'identité du client).

Comparaison de l'OPA avec d'autres moyens de contrôle :

- **Avantages** : Contrôle simple et rapide qui demande moins de compétences et ne nécessite pas de connaissances ou de formation d'un spécialiste. Elle peut être utilisée par un large éventail d'utilisateurs, y compris des personnes non-expertes de l'authentification. Pour l'OPA, tous types de smartphones (même sans NFC) peuvent être utilisés pour vérifier les éléments optiquement variables ainsi que d'autres éléments de sécurités grâce à toute une gamme de fonctionnalités. Il s'agit d'un outil de petite taille, léger et facile à transporter.
  - » L'OPA est une solution efficace contre les risques et menaces dont font face les opérateurs n'ayant pas accès aux informations confidentielles des listes de surveillance (comme la falsification, la contrefaçon, les attaques biométriques, etc).
  - » Dans les cas d'utilisations tels que les vérifications KYC, les solutions OPA peuvent être particulièrement rentables et permettre une authentification simple et fiable. La procédure peut nécessiter qu'un opérateur effectue un contrôle manuel supplémentaire.
  - » Les solutions OPA sont durables et peuvent servir de sauvegarde si, par exemple, la puce d'un document de voyage ne fonctionne pas ou n'est pas accessible par le contrôleur.
  - » Les solutions OPA permettent d'obtenir une pièce d'identité numérique sécurisée à partir de documents physiques sans puce électronique.

- **Inconvénients** : Tous les éléments de sécurités ne peuvent être testés automatiquement (la plupart des appareils photos de smartphone sont incapables de contrôler les éléments visibles à la lumière UV ou IR). Il peut être peu pratique de tester plusieurs pages d'un document sous forme de livret (un passeport par exemple), et difficile de repérer les éléments de sécurité multipages. Risque que les utilisateurs ne s'attardent pas à détecter de faux documents, se contentant de vérifier si le témoin lumineux est rouge ou vert. Risque de faux positifs et faux négatifs.

1.5
Entretiens

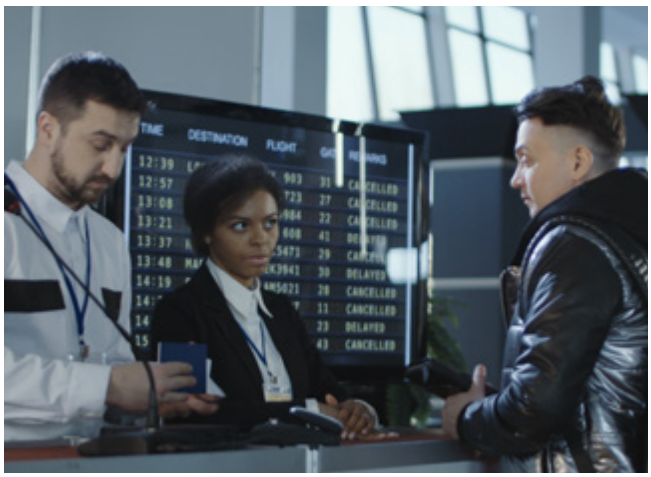
Les questions, en particulier celles posées par une personne formée et expérimentée, peuvent être une étape importante pour vérifier les dires et la crédibilité d'un individu. En faisant attention au « langage corporel », un expert peut sentir si quelqu'un dit la vérité ou cherche à détourner l'attention de l'enquêteur. Un entretien peut également permettre de répondre à des questions complexes allant au-delà de l'identité ou de l'authenticité d'un document, notamment relatives aux véritables intentions d'une personne cherchant à entrer sur un territoire ou à emprunter de l'argent.

Une formation différente peut être nécessaire suivant le type d'utilisateur. Par exemple, un agent de contrôle aux frontières qualifié aura besoin d'une formation importante sur la détection de faux documents et la mise en comparaison avec les passagers. Un expert en faux documents aura quant à lui besoin d'une formation encore plus poussée et devra apprendre à utiliser un équipement de laboratoire spécialisé. En revanche, une personne travaillant dans un magasin de vente au détail peut se contenter d'une formation plus simple, portant par exemple sur la reconnaissance d'un faux document, l'utilisation de l'équipement et des conseils pratiques sur la manière de réagir lorsque les tests d'authentification indiquent un problème.

Les compétences en matière de détection de fraude et de comparaison des visages sont importantes pour les agents aux frontières et peuvent être améliorées par la formation. Les contrôles automatisés se limitent normalement à la partie principale d'un passeport (page des données biographiques), mais un agent formé à la détection des fraudes peut repérer des signes de falsification ou de contrefaçon en se basant sur de nombreux autres éléments du document.

Les ressources et actions servant à soutenir et appuyer les entretiens de première ligne peuvent inclure une bonne formation initiale et continue ; des entretiens secondaires (prolongés) dans un lieu différent du contrôle aux frontières principal ; des agents spécialisés dans la détection de faux documents et dans les équipements de laboratoire ; des renseignements confidentiels, par exemple sur les techniques de falsification actuelles et les exemples récemment détectés.

- **Avantages** : Soumet la personne à une évaluation poussée effectuée par un autre individu, ce qu'un ordinateur ne pourrait pas faire. Peut donner le sentiment que « quelque chose ne va pas » dans ce que dit une personne et qu'il est nécessaire de procéder à un entretien plus long ou à un contrôle plus rigoureux du document.
- **Inconvénients** : Les ordinateurs sont capables de traiter beaucoup plus de données que les humains, qui se fatiguent et peuvent faire des erreurs.



1.6 Authentification Numérique

Les documents sécurisés tels que les passeports électroniques et les cartes bancaires peuvent contenir une puce spéciale contenant des informations concernant l'individu ainsi que des codes cryptographiques avancés (appelés « signatures numériques »). Ces informations peuvent être utilisées pour vérifier de manière concluante que les données de la puce sont authentiques, c'est-à-dire qu'elles proviennent bien de la source par laquelle elles sont censées avoir été émises, et qu'elles sont intègres, c'est-à-dire que personne n'a modifié les données qui ont été placées là par l'émetteur… et que les données sont donc fiables.

Les passeports électroniques (ou documents de voyage électroniques lisibles par machine (eMRDT)) sont définis dans la norme OACI 9303. Ils mobilisent une technologie d'infrastructure à clés publiques (PKI) utilisant des clés de chiffrement privées et publiques pour signer et authentifier les données.

Un passeport électronique contient une puce sécurisée contenant une copie de certaines informations imprimées sur le passeport. Plusieurs éléments de sécurité protègent les données de la puce plus fortement que sur un passeport traditionnel :

- **Accès** : On accède à la puce par une connexion radio localisée, mais seulement après avoir lu certaines données clés de la page de titre du document de voyage pour générer un code d'accès sécurisé. Cela sert à empêcher l'accès à la puce sans que le titulaire du passeport n'en soit informé.
- **Intégrité des données** : Des codes cryptographiques puissants, connus sous le nom de signatures numériques, sont utilisés pour « verrouiller » chaque bloc de données sur la puce, le reliant de manière sécurisée à la bonne personne. Toute modification, telle que le remplacement de la photo d'identité par une autre, sera rendue évidente car le faussaire ne sera pas en mesure de créer la signature numérique correcte correspondant aux nouvelles données.
- **Intégrité de la puce** : Un autre test permet de vérifier que la puce est bien la puce d'origine délivrée par l'autorité compétente, et non un « clone » d'une puce valide.
- **Les empreintes digitales** : Dans l'Union Européenne, une sécurité supplémentaire est utilisée pour protéger deux empreintes digitales du titulaire. Ces images peuvent être utilisées pour confirmer qu'il s'agit bien du titulaire du passeport, tout en protégeant sa vie privée.
- **Avantages** : Si elle est correctement appliquée et mise en œuvre, la technologie PKI apporte un niveau d'authentification des données extrêmement fort. Il s'agit du plus haut niveau d'authentification disponible à ce jour.
- **Inconvénients** : Spécialisée et complexe ; elle nécessite des systèmes spécifiques, notamment l'accès au répertoire mondial de clés publiques (RCP) de l'OACI, qui contient les certificats publics de données cryptées. Par conséquent, l'authentification électronique n'est pas accessible pour tous les cas d'utilisation. Des techniques supplémentaires telles qu'une OMA doivent être mises en place comme solution de repli.

1.7
Biométrie

Les caractéristiques durables ou permanentes d'une personne, telles que son visage, ses empreintes digitales, son iris et son ADN, peuvent être capturées et encodées dans un système informatique en guise de future référence. Cela peut par exemple servir à identifier la personne en recherchant une correspondance dans la base de données ou pour vérifier qu'elle est bien celle qu'elle prétend être en la comparant à son dossier existant.

Les systèmes biométriques ont considérablement progressé en termes de capacité, de sophistication et de performance au fil des ans. Ils sont utilisés dans les cas d'identification et afin de relier des systèmes différents entre eux. Par exemple, on peut citer comme systèmes biométriques multiples le système HART mis en place par le Ministère américain de la Sécurité Intérieure (le DHS) et le système sBMS (« shared Biometric Matching System ») mis en place par eu-LISA pour les États membres de l'Union Européenne.

Un grand nombre des techniques mentionnées précédemment peut être testé dans les cas d'identification biométrique. Les réponses seront du ressort des technologies de Détection des Attaques de Présentation (PAD, pour « Presentation Attack Detection »), qui peuvent impliquer des techniques avancées et efficaces de détection et de mise en correspondance, renforcées par des tests robustes chargés de tester un éventail d'attaques afin de voir si la mesure de protection permet de repérer la fraude.

- **Avantages** : Peut apporter une assurance solide concernant le lien entre un passeport authentifié de manière fiable et la personne qui le présente. La biométrie peut également établir un lien fiable entre un échantillon biométrique obtenu d'une personne et les enregistrements détenus dans un système d'identification biométrique automatique (ABIS). Elle permet d'établir un lien entre la personne et les enregistrements préexistants la concernant, même lorsque la personne a utilisé un nom différent à diverses occasions. Elle peut donc constituer une défense solide contre une personne cherchant à utiliser une identité illégitime.
- **Inconvénients** : Possible tentative de tromper le test biométrique en utilisant une reproduction d'une caractéristique biométrique, connue sous le nom d' « attaque par présentation », qui nécessite par exemple de vérifier que le sujet est bien une personne vivante pour la déjouer. Un système biométrique complet peut être vaste, complexe et coûteux à adopter et à intégrer à d'autres systèmes. La vérification du caractère vivant de l'individu et la détection des attaques de présentation (PAD) aident à contrer les attaques frauduleuses.

Source: Keesing

1.8
Systèmes de référence

Les systèmes de référence sont également importants et peuvent soulever des questions qui n'auraient pas été posées autrement. Les systèmes de surveillance peuvent inclure la base de données d'INTERPOL sur les documents de voyage volés et perdus (SLTD), l'historique des déplacements, les antécédents judiciaires, les renseignements généraux, les alertes (notamment criminelles) concernant des personnes recherchées pour toute une série d'infractions possibles, ou dont les données biométriques montrent qu'elles voyagent régulièrement sous de faux noms et documents de voyage.

- **Avantages** : Une liste de surveillance ou un autre système de référence peut mettre en évidence des problèmes qui seraient autrement passés inaperçus (par exemple, le document peut être authentique mais avoir été déclaré volé).
- **Inconvénients** : Coûts et complexité additionnels pour accéder à ces systèmes et assurer leur maintenance ; nécessité de protéger soigneusement les informations confidentielles.

1.9
Approches multiples

Les techniques déjà décrites présentent toutes des éléments très utiles pour prouver que les documents d'identité et de voyage sont authentiques (ou non) et qu'une personne est bien celle qu'elle prétend être. Cependant, quelle que soit la qualité de ces techniques, aucune d'entre elles ne peut à elle seule faire la totalité du travail dans chacune des situations. Un large éventail d'attaques possibles peut être tenté. Il est donc préférable de disposer de divers tests permettant de rechercher des preuves de fraude et maximiser les chances de détecter un faux document.

- **Avantages** : Il est essentiel d'utiliser plusieurs techniques plutôt qu'une seule pour tester les documents et contrôler l'identité d'une personne afin d'obtenir un niveau de confiance plus élevé dans l'authentification.
- **Inconvénients** : Coût supplémentaire / complexité… sans garantie de succès.

2.
Cas d'utilisation

2.1
Contrôle aux frontières

- **Guichet d'arrivée** : Contrôle aux frontières traditionnel avec un agent expérimenté qui peut : examiner visuellement le passeport et vérifier les signes de falsification ; scanner le passeport sur un lecteur spécialisé qui soumet les informations à une liste de surveillance listant les passeports déclarés perdus ou volés et authentifie les données de la puce en utilisant les clés de cryptage pertinentes détenues dans le répertoire des clés publiques (RCP) de l'OACI ; et qui parle au voyageur. Si la personne doit démontrer qu'elle répond à certains critères (par exemple, qu'elle peut subvenir à ses besoins pendant ses vacances et ne va donc pas travailler illégalement), l'agent évalue la validité globale de toutes les preuves. Ce voyageur et les preuves de son identité sont-ils crédibles et cohérents, ou y a-t-il des divergences qui nécessitent une discussion plus approfondie ?

Comment faciliter l'authentification avec l'OMA ?
L'OMA permet une authentification de repli lorsque l'authentification électronique ne peut être réalisée (puce inexistante dans le document ou qui ne fonctionne pas). En outre, elle permet aux gardes-frontières d'effectuer des vérifications préalables dans la file d'attente lorsque les frontières sont surchargées.

- **Contrôle Mobile aux frontières** : peut compter plusieurs exemples

  » Lecteur NFC et puces de passeport : de nombreux smartphones sont équipés d'une technologie de communication sans fil à courte portée et à haute fréquence (dite NFC : « Near-Field Communication ») pour lire les cartes et les passeports lorsqu'ils sont à proximité. En utilisant l'appareil photo embarqué pour lire la zone de lecture automatique d'un passeport ou d'une carte, il est possible de lire et authentifier les DVLMe (Documents de Voyage Lisibles à la Machine électroniques : passeports / cartes électroniques).

  » Appareils photos embarqués et capture biométrique : de petits lecteurs biométriques portables peuvent être connectés à un smartphone. Un logiciel peut également être configuré avec l'appareil photo d'un smartphone afin de lire les empreintes digitales et les confronter à un « système d'identification automatique par empreintes digitales » (AFIS). La capture et la vérification biométriques peuvent être nécessaires pour certains types de contrôle aux frontières, notamment le système européen d'entrée/sortie (EES).

  » Contrôle mobile aux frontières : certaines situations exigent qu'un contrôle aux frontières complet soit effectué en déplacement, par exemple à bord d'un train ou d'un bateau. Avec l'adoption croissante de la biométrie et de contrôles techniques rigoureux, les systèmes mobiles sont tenus d'être tout aussi capables que les systèmes fixes (tels les guichets de contrôle aux frontières d'aéroport). Par exemple, il devient aujourd'hui possible de créer un système mobile sur tablette ou smartphone : l'utilisation du NFC et de l'appareil photo décrite ci-dessus montre comment d'excellents moyens techniques peuvent être rendus disponibles en déplacement. Néanmoins, il est essentiel de s'assurer que le processus opérationnel complet puisse être exécuté de manière réaliste.

IDEMIA

2.1
Contrôle aux frontières (suite)

- **Une e-Gate ou porte automatisée de contrôle aux frontières** (ABC, pour « Automated Border Control ») est un équipement automatisé pouvant remplacer un agent frontalier à un poste de contrôle, comme décrit ci-dessus. En général, le passager entre dans l'espace de la porte puis présente son passeport au dispositif de lecture qui est similaire à celui utilisé par un agent frontalier et effectue les mêmes contrôles. Il est ensuite demandé au passager de regarder une caméra, qui prend une photographie du visage et vérifie sa correspondance avec la photo authentifiée dans la puce du passeport, en utilisant la technologie de reconnaissance faciale (RF). Si toutes ces étapes se déroulent correctement et sans encombre, le passager passe la porte et est admis dans le pays. Si ce n'est pas le cas, l'agent supervisant les portes examinera l'individu et pourra lui poser diverses questions. Un individu autorisé à passer la porte automatique n'aura pas à s'entretenir avec un agent. Généralement, les e-Gates sont réservées aux voyageurs ayant une autorisation d'entrée sur le territoire, comme un ressortissant du pays ou une personne inscrite dans un programme de « voyageurs dignes de confiance » qui a été autorisée à entrer sans entretien. Les e-Gates filtrent les passagers les « plus faciles » qui arrivent à la frontière, ce qui laisse aux agents qualifiés et expérimentés plus de temps pour examiner les passagers qui nécessitent plus d'attention.

  Comment faciliter l'authentification avec l'OMA ?
  Les solutions OMA (notamment celles qui luttent contre les fausses copies de documents de voyage), couplées à d'autres, permettront de renforcer l'authentification d'un document.

- **Bornes libre-service** : Une borne libre-service représente une solution alternative comportant certains des éléments d'une e-Gate. En voici l'utilisation classique : le voyageur arrive à la borne (complètement autonome, elle se compose d'un écran, d'un clavier et d'un lecteur de passeport, sans porte). Elle scanne le passeport que le système reconnaît grâce au système d'Information préalable sur les voyageurs (IPV), et répond à des questions telles que l'objet de la visite, le vol d'arrivée, les déclarations de douane, de santé, de nourriture, etc. Une fois ceci effectué, un billet codé est imprimé. Le voyageur le présentera ensuite à un agent du guichet des arrivées avec son passeport. Entre-temps, le système aura pu vérifier les informations présentées à l'agent.

2.2
Police de terrain

- La plupart des gens disposent aujourd'hui de smartphones puissants et performants qui font partie intégrante de leur vie quotidienne. La police et autres autorités chargées de l'application de la loi ne font pas exception. Des systèmes mobiles bien conçus permettent aux agents d'assumer un large éventail de fonctions lorsqu'ils traitent avec le public, tant dans l'espace public qu'en première ligne. Ils ont ainsi accès aux résultats en temps réel grâce à des systèmes auxquels ils ne pourraient autrement accéder qu'au poste de police, ou par communication radio. Il peut s'agir de contrôler une personne, divers types de documents ou un véhicule, de dresser des procès-verbaux, de transférer un contrôle au système central, ou encore d'intégrer le système mobile au système central de commande et de contrôle. Les deux questions fondamentales que se pose un agent face à une personne qui semble suspecte sont "Qui est cette personne ?" et "Que savons-nous de lui/d'elle ?". Une bonne solution mobile peut ôter de nombreux doutes en facilitant la détection des personnes recherchées et en évitant les arrestations inutiles.

An Garda Síochána (La Police Irlandaise)

2.3
Relations Entreprise / Client

Y compris l'authentification B2C (« Business to Customer », de l'entreprise au consommateur) et C2C (« Customer to Customer », échanges inter-consommateur)

- **Authentification assistée de documents — KYC (pour « Know Your Customer »)** : Les réglementations relatives aux services financiers exigent souvent des entreprises et des professionnels qu'ils fassent preuve de diligence raisonnable pour vérifier l'identité d'un client et les risques liés à une nouvelle relation commerciale avec celui-ci, dans le cadre de de la Lutte contre le Blanchiment de Capitaux (LCB).

  Comment faciliter l'authentification avec l'OMA ?
  Les solutions d'OMA permettent d'authentifier tous types de documents de voyage en utilisant seulement un smartphone (simple à utiliser). Pour une plus grande sécurité, celui-ci peut être couplé à un test permettant de déterminer s'il s'agit d'une personne réelle et vivante.

- **Contrôle d'identité et enregistrement à distance** : Il s'agit de la version numérique d'une procédure KYC, similaire à une demande de visa en ligne. Les informations fournies par le demandeur peuvent être vérifiées grâce à celles déjà détenues par l'institution financière ainsi qu'aux bases de données dont disposent les agences de notation de crédit. Ce processus est nécessaire aux banques et institutions financières devant vérifier l'identité et l'intégrité d'une personne souhaitant faire affaire avec elles (ouvrir un compte bancaire, par exemple). Le client potentiel fait généralement une demande en ligne pouvant nécessiter l'implication d'agences de notation de crédit, qui compilent alors les informations relatives à son historique financier et sa solvabilité. Dans ce cas, le principal défi est d'authentifier le document avec un bon niveau d'assurance, mais aussi de le relier à son détenteur pour éviter toute fraude de la part de son détenteur.

» **Enregistrements en libre-service** : Ils sont acceptées par de nombreux services d'immigration pour l'obtention de visas ou de dispenses de visa, ainsi que par les banques pour l'ouverture d'un compte bancaire. Il est ensuite possible de poser des questions supplémentaires, de scanner des papiers d'identité ou le passeport, d'en lire la puce, de saisir les données biométriques à l'aide de « selfies » et d'effectuer un test vérifiant le caractère vivant de la personne. Les données biométriques enregistrées peuvent ensuite être vérifiées lorsque la personne se présente à un entretien ou (dans le cas d'un visa) à la frontière pour entrer dans le pays.

» **Demande de Visa** : Dans de nombreux pays, un voyageur peut demander un visa en ligne et donner accès à son passeport (et à sa puce) via l'antenne NFC de son téléphone portable. Il fournit alors une photo « selfie », qui peut être comparée (RF) à la photo du passeport et/ou à une demande antérieure. Divers contrôles peuvent être effectués afin de vérifier que le « demandeur » est bien une personne vivante (détection d'attaque de présentation). Les informations fournies par le demandeur peuvent être comparées aux bases de données de référence détenues ou utilisées par l'agence. Les doutes pouvant subsister peuvent être vérifiés dans un second temps, par exemple lors d'un entretien approfondi (souvent nécessaire pour obtenir un visa) ou lorsque le titulaire du visa se présente à la frontière.

» **Carte d'embarquement** : permet au citoyen de télécharger un code barre, accepté à l'aéroport pour embarquer à bord d'un vol. Il est important de prendre en compte la sécurité de cette solution, entrée en service en 2007.

» **Identité Numérique dérivée d'un document de voyage physique** : Les identités numériques (disponibles via une solution mobile : le DTC (Digital Travel Credential), le permis de conduire numérique, le Digital NID) seront bientôt disponibles et adoptées par les citoyens. L'un des moyens (peut-être le plus complet) de créer ces identités

numériques (IN) sera de les dériver d'un document physique. Pour garantir la sécurité de ce processus, les documents devront intégrer des caractéristiques (électroniques ou physiques) permettant une communication et une authentification sécurisées par le dispositif mobile.

Comment faciliter l'authentification avec l'OMA ?

L'OMA permet d'authentifier tous types de documents en utilisant uniquement un scanner de bureau ou un smartphone. Pour lutter contre la fraude touchant directement aux documents et/ou à la personne revendiquant l'identité, il conviendrait d'intégrer à la conception du document une fonctionnalité d'OMA pouvant être authentifiée à l'aide d'un smartphone et d'un logiciel dédié. Elle devrait par exemple protéger les informations personnelles, et notamment la photo d'identité, élément le plus souvent attaqué. La photo d'identité représente en effet le meilleur moyen de lier le document à son titulaire, par exemple en la comparant au visage de la personne par correspondance biométrique. La solution permettrait ainsi d'empêcher les fraudeurs de présenter de faux documents de voyage, une photocopie ou une vidéo (à condition d'utiliser le bon dispositif de sécurité) et l'organisme effectuant l'authentification sera en mesure d'identifier la personne derrière l'écran.

Keesing

- **Le passeport sanitaire** : Conçu pour garantir la santé des passagers. Au vue de la récente pandémie de COVID-19, il peut devenir une nécessité (voir la description précédente sous la rubrique authentification électronique). Diverses formes de passeports sanitaires utilisant l'authentification électronique sont à l'étude pour permettre à un voyageur de prouver qu'il a récemment été vacciné contre la COVID-19, qu'il a effectué un test de dépistage négatif, ou qu'il s'est remis de la COVID-19 et est considéré comme étant immunisé. Le consensus sur la ou les solutions qui seront retenues n'a pas encore émergé. Il s'agira peut-être d'un mélange de solutions constituant une solution globale. Il se peut qu'une version papier (imprimée) comprenant un code-barres signé numériquement soit acceptée parallèlement à une solution sur smartphone. Dans les deux cas, la nécessité de lire et d'authentifier les données relatives à la santé peut se poser, en plus des autres formes de données codées/signées déjà décrites dans ce document.

Exemples de l'OMS représentant un passeport sanitaire physique et mobile.

3. Recommendations

Nous espérons que ce document vous sera utile. Pour conclure, voici quelques recommandations quant à une authentification efficace de documents de voyages et papiers d'identité, utilisant surtout des moyens automatisés :

- **Prenez ce sujet au sérieux !** : De plus en plus de transactions et de contrôles s'effectuent en ligne, ce qui multiplie le risque de fraude et le besoin de s'en protéger. Une enquête de l'Association américaine des examinateurs de fraudes certifiés (« US Association of Certified Fraud Examiners ») réalisée en novembre 2020 a révélé que 79 % des personnes interrogées avaient observé une augmentation de la fraude au cours des 12 mois précédents et que 90 % d'entre elles s'attendaient à une augmentation de la fraude au cours des 12 prochains mois : cyberfraude, fraude aux paiements et, en particulier, vol d'identité (www.acfe.com/covidreport.aspx). Il existe de nombreuses façons de tenter une fraude d'identité, comme le résume la section traitant des risques.
- **Une authentification par machine offre un moyen de protection supérieur qu'il est préférable d'envisager.** Ce document apporte plusieurs exemples d'authentification optique par machine (OMA), par le biais d'un scanner de bureau traditionnel (OSA) et, de plus en plus, d'un smartphone (OPA). Ces solutions offrent de réels avantages et devraient être sérieusement envisagées, explorées et étudiées afin d'être évaluées et testées par des projets pilotes et, le cas échéant, pour être déployées de manière opérationnelle.
- **Lorsque vous choisissez une solution, prenez en considération le fait que l'OMA est la solution la plus inclusive en matière d'authentification:** Elle peut être utilisée simplement et par tous (qu'il s'agisse des secteurs publics et privés ou des citoyens eux-mêmes); elle peut être déployée pour tous cas d'utilisation, même lorsque d'autres techniques de vérification ne sont pas disponibles. Cette solution est particulièrement adaptée aux cas d'utilisation ne nécessitant pas un accès à des informations confidentielles (comme par exemple à certaines formes d'authentification électronique et listes de surveillance).
- **Des considérations plus détaillées** sont également recommandées :
  - **La conception du document** : Peut inclure des éléments de sécurité qui facilitent l'authentification automatisée et la rendent plus efficace (l'aide de spécialistes des documents de voyage peut être utile).

    Y compris des éléments de sécurité permettant une authentification optique à l'aide d'un téléphone, ce qui constituerait la meilleure option étant donné les besoins d'authentification croissants des secteurs publics et privés.

    Pour lutter contre la fraude touchant directement au document de voyage et celle touchant à la personne qui revendique l'identité, il serait avantageux d'inclure dans la conception du document un dispositif de sécurité OPA qui protège les données personnelles du titulaire et authentifie son intégrité. Cela concerne surtout la photo d'identité principale, car il s'agit de l'élément le plus souvent attaqué mais aussi du meilleur élément permettant de lier le document de voyage à son titulaire.
  - **Infrastructure** : Solutions techniques et organisationnelles pouvant aider, en fournissant par exemple des modèles mis à jour de nouveaux types de documents et en faisant le lien avec le RCP, le répertoire des clés publiques, afin d'authentifier les MRTD ('Machine Readable Travel Documents') électroniques.
  - **Formation** : Elle doit être incluse et adaptée aux circonstances et aux utilisateurs dans n'importe quel contexte (par exemple, tant les gardes-frontières que les vendeurs au détail doivent savoir comment contrôler des documents, utiliser leur équipement d'authentification et réagir aux alertes, bien que leurs situations soient différentes). Une attention particulière doit également être accordée aux questions de protection de la vie privée.
- **Plusieurs moyens d'authentification valent mieux qu'un** : Il n'existe pas de solution unique qui puisse être efficace dans toutes les situations, comme nous avons tenté de l'expliquer dans ce document. L'authentification optique, les contrôles électroniques (RCP), les entretiens en face à face, les systèmes de référence et la biométrie peuvent jouer un rôle : il faut choisir la bonne solution pour chacun des cas.

4. Glossaire

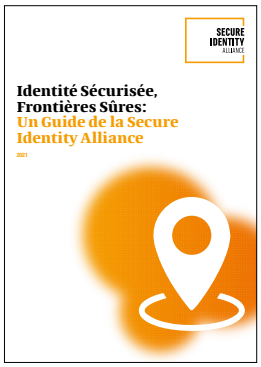
AFIS	Automated Fingerprint Identification System : Système d'identification automatique par empreintes digitales permettant de réaliser des identifications (authentifications, recherches ouvertes) basées sur les empreintes digitales.
CEV	Le Cachet Électronique Visible est un dispositif qui garantit l'origine et l'intégrité des données clés d'un document, quel que soit le support, électronique ou papier.
DHS	Department of Homeland Security (US) : Département de la sécurité intérieure des États-Unis.
DOVID	Diffractive Optically Variable Image Device : structure diffractive changeant d'apparence selon l'inclinaison.
DTC	Digital Travel Credential.
eu-LISA	Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice.
FOG	Documents authentiques obtenus de manière frauduleuse. (« Fraudulently Obtained but Genuine »).
FR	Facial Recognition.
IN	Identité Numérique.
IR	Infra-Rouge.
KYC	« Know Your Client / Customer » : Procédure de Connaissance du Client.
LCB	Le concept AML, par ses sigles en anglais « Anti-Money Laundering » , et PBC, par ses sigles en français "Prévention du Blanchiment de Capitaux", également connu sous le nom Anti Blanchiment de Capitaux ou Lutte Contre le Blanchiment de Capitaux (LCB).
MRZ	Machine Readable Zone - Zone de Lecture Automatique (ZLA).
NFC	Near Field Communication - technologie de communication sans fil à courte portée et à haute fréquence.
NID	National Identity Document – titre national d'identité.
OACI	Organisation de l'Aviation Civile Internationale.
OMA	Optical Machine Authentication - Authentification optique par machine.
OPA	Optical Phone Authentication - Authentification optique par téléphone.
OSA	Optical Scanner Authentication - Authentification optique par scanner.
PAD	Presentation Attack Detection - Détection d'attaque par présentation.
PKD	Public Key Directory - Répertoire des Clés Publiques (ou RCP).
RF	Reconnaissance Faciale.
SIA	Secure Identity Alliance.
SLTD	Stolen and Lost Travel Documents. La base de données SLTD d'Interpol contient des informations sur des documents de voyage et d'identité déclarés volés, perdus, révoqués, invalides ou volés vierges.
UE	Union Européenne.
UV	Ultra-Violet.
VIZ	Visual Inspection Zone : la « zone d'inspection visuelle » (ZIV) de la page de renseignements du passeport lisible à la machine.

Autres rapports publiés par la Secure Identity Alliance :

https://secureidentityalliance.org/ressources/publications

Tendances Récentes de la Fraude aux Passeports

L'objectif de ce rapport est d'établir un lien clair entre les problèmes de fraude documentaire et d'usurpation d'identité auxquels sont confrontés les autorités de délivrance et de contrôle de documents de voyage, et certaines organisations privées telles que les institutions de services financiers. Ce document explore également certaines des solutions techniques pouvant relever ces défis, telles que celles proposées par l'industrie mondiale de la gestion d'identité.



Identité Sécurisée, Frontières Sûres

Examine le besoin qu'ont les autorités frontalières d'assurer sécurité et protection tout en proposant une expérience efficace et sans encombre aux passager. En plus des principaux moteurs qui façonnent l'avenir des espaces de contrôle aux frontières, le rapport examine le rôle vital et complexe que joue la gestion des identités en soulignant certaines des technologies en pleine évolution, comme l'automatisation, la biométrie ou la mobilité des solutions. Il étudie également leurs applications par le biais d'études de cas tirées de diverses régions du monde.

L'Expression des Identités Numériques dans le Monde

Fournissant des observations et perspectives de terrain inédites, cette étude produite en partenariat avec onepoint donne la parole aux parties prenantes de 25 programmes souverains innovants en matière d'identité numérique. Leurs analyses mettent en évidence les bonnes pratiques et les principes directeurs essentiels à la bonne utilisation, l'adoption et le succès de l'identité numérique, quel que soit le modèle adopté.

SECURE IDENTITY ALLIANCE