SECURE IDENTITY ALLIANCE

Tendances de la Fraude sur les Passeports et Comment les Combattre

Version publique
2021

Mentions

Secure Identity Alliance (SIA)
www.secureidentityalliance.org

Design
Design Motive Ltd

Crédits photo
Shutterstock

Traduction
Oriane Duboz

Nous tenons tout d'abord à remercier les nombreux contributeurs de ce document. Sans leur aide précieuse, il aurait été impossible de réaliser une analyse aussi détaillée des documents sécurisés qui existent aujourd'hui, des menaces auxquelles ils sont confrontés et des dispositifs de sécurité mis en place afin d'atténuer les risques.

Production
Ce rapport a été produit par le groupe de travail « Sécurité des documents » de la SIA :

Joachim Caillosse (Président du groupe de travail et auteur principal)
IN Groupe

Christophe Duriez, Aimane Ait El Madani et Thomas Poreaux
IDEMIA

Françoise Daniel et Philippe Jung
IN Groupe

Renaud Laffont-Leenhardt et Petri Viljanen
Thales

Michael Ruhland-Bauer et Tobias Rosati
Veridos

Christophe Halopé et Cosimo Prete
CST

Claudia Schwendimann et Andreas Zechmann
OSD

Frank Smith
Observateur consultant pour la SIA et ancien Directeur Adjoint au 'Home Office' du Royaume-Uni

Patrick Butor
Consultant indépendant, président du groupe de normalisation international de la sécurité publique et privée ISO TC 292 WG 6

Merci
Nous adressons également nos remerciements à la Division de l'Expertise en Fraude Documentaire et à l'Identité (DEFDI), au sein de la Direction Centrale de la Police Aux Frontières (DCPAF) française, ainsi qu'à l'Unité Contrefaçon de Monnaie et Documents de Sécurité d'INTERPOL, pour leur examen approfondi de ce rapport.

SECURE IDENTITY ALLIANCE

Contenus

1. Assurer l'intégrité des documents sécurisés actuels

L'intégrité des documents sécurisés actuels étant menacée par des contrefacteurs et des fraudeurs de plus en plus sophistiqués, il est aujourd'hui primordial de constamment faire évoluer et intégrer de nouveaux éléments de sécurité. Comme nous le verrons dans ce document, un travail considérable concentré sur le cas du passeport est en cours, document pour lequel ce constat s'applique tout particulièrement.

Ce document a été rédigé par le groupe de travail « Sécurité des documents », groupe de travail intersectoriel de la Secure Identity Alliance (SIA) chargé de guider la conception, la fabrication, la délivrance et la vérification de documents sécurisés. Ce rapport fournit une analyse globale du paysage de la fraude documentaire, assortie de lignes directrices et de recommandations utiles sur la façon de renforcer un passeport contre les attaques.

Le but de ce document n'est pas de montrer des exemples réels de fraude ; les organisations autorisées ont déjà accès à ces exemples via des canaux restreints.

Il est constructif de discuter publiquement des principes généraux de la sécurité des documents et de quelques exemples choisis. Cependant, dans un souci de maximiser la sécurité, la version publique de ce document évite de traiter en détails de certains exemples, en particulier des techniques les plus avancées, qui pourraient être d'un grand intérêt pour les faussaires et les contrefacteurs.

La version restreinte de ce rapport, plus explicite, est réservée aux agences et autorités chargées de l'application de la loi. Elle est accessible sur la page web du Centre INTERPOL de référence des documents de voyage et d'identité, dont l'accès est régi par des règles et des règlements stricts. Pour plus de détails, si vous travaillez pour la police, une agence de contrôle aux frontières, pour l'immigration ou une autre autorité gouvernementale compétente, veuillez contacter l'Unité Contrefaçon de Monnaie et Documents de Sécurité d'INTERPOL: CCSD@interpol.int

2. Introduction

La fraude documentaire, en particulier la contrefaçon et la falsification de documents de voyage tels que les passeports, représente une menace importante tant pour l'identité personnelle que la sécurité nationale. Elle s'inscrit surtout dans un contexte beaucoup plus large, comme le souligne le rapport SOCTA 2017 d'Europol qui établit un lien clair entre la fraude documentaire et la criminalité internationale. La Plateforme Pluridisciplinaire Européenne contre les Menaces Criminelles (EMPACT) cite cette question comme l'une de ses priorités stratégiques.

La fraude documentaire est également un défi croissant, conduisant certains commentateurs à dénoncer une croissance « épidémique » de la fraude au passeport[1] . En 2020, près de 100 millions de documents de voyage étaient signalés perdus ou volé[2] – suggérant le que marché noir des documents d'identité volé se porte toujours bien.

Les conséquences de la modification ou reproduction illégale de documents de voyage sont nombreuses et variées. Qu'il s'agisse de l'atteinte à la réputation du pays émetteur et du fabricant du document, ou des incessantes possibilités de détournement telles que la criminalité financière, le trafic de drogue et le terrorisme, la création et l'utilisation de faux documents de voyage peuvent avoir un impact qui va bien au-delà des désagréments personnels.

L'usurpation d'identité reste cependant un problème grave, qui peut entraîner de sérieuses conséquences pour les personnes concernées. Les autorités de délivrance ont la responsabilité de protéger les citoyens, ainsi que les frontières nationales.

Sur un plan plus positif, les autorités de délivrance ont désormais accès à un arsenal de moyens de dissuasion et de contre-mesures plus important que jamais. Les passeports peuvent aujourd'hui être équipés d'une série d'éléments de sécurité qu'il aurait été pratiquement impossible de mettre en œuvre il y a seulement quelques décennies. Des puces biométriques aux éléments physiques, l'innovation continue dans les composants des documents a permis de créer tout un panel de possibilités d'empêcher ou de mettre en évidence les modifications illicites.

Un document sécurisé bien conçu repose aujourd'hui sur une collaboration entre diverses compétences et domaines d'expertise. Cet esprit d'unité concerne :

- Les experts en matière de fraude et de vérification de documents, tels que les organismes chargés de l'application de la loi.
- Les experts en conception et en fabrication de documents sécurisés, tels que la SIA.
- Les autorités de délivrance, qui peuvent ou non disposer d'une expertise interne, et qui sont responsables à la fois de la création et de la délivrance de documents sécurisés.

Bien sûr, en pratique, de nombreux pays disposent de ressources limitées dédiées à la détection, l'analyse et la lutte contre la fraude documentaire ; ils ont en conséquence un fort besoin de soutien.

En tant qu'organisme consultatif mondial à but non lucratif sur l'identité et les services numériques sécurisés, le partage de conseils et de bonnes pratiques est l'un des rôles fondamentaux qu'exerce la Secure Identity Alliance (SIA).

Nos membres et nous-mêmes sommes profondément investis dans l'aide aux gouvernements et aux organismes émetteurs afin de faire face à la menace permanente de fraude documentaire, autant que nous le pouvons. Notre groupe de travail focalisé sur la sécurité des documents a été créé spécifiquement dans le but de fournir des recommandations et lignes directrices pour la conception de documents sécurisés.

Ce rapport est un exemple de notre engagement continu en faveur de l'application de bonnes pratiques en matière de sécurité des documents. Vous y trouverez une analyse approfondie des dernières tendances qui influencent à la fois la prévention et la détection de la fraude aux passeports. Nous cherchons à mettre en évidence le besoin toujours présent d'équilibrer la simplicité d'utilisation et la sécurité, ainsi que le nombre croissant de moyens que les émetteurs peuvent mettre en œuvre pour garder une longueur d'avance sur les dernières menaces.

Nous espérons que ce document vous sera utile.

[1] EU's passport fraud 'epidemic' – Politico, 28th January 2016

[2] https://www.INTERPOL.int/How-we-work/Databases/Stolen-and-Lost-Travel-Documents-database

3. Un aperçu des livrets de passeport et de la fraude

3.1
Une définition du passeport

L'objectif premier d'un passeport est de servir de document de voyage, donnant à son détenteur le droit de franchir des frontières géographiques. Les contrôles stricts qui entourent la délivrance des passeports leur ont toutefois permis d'acquérir la seconde fonction de document d'identité, permettant à leurs détenteurs d'effectuer toutes sortes d'opérations comme ouvrir un compte bancaire ou voter. Dans certains pays, par exemple, le passeport tient lieu de carte nationale d'identité.

Si leur utilisation est régie par une série de restrictions et d'exigences, les passeports sont aujourd'hui également conçus pour être pratiques et interopérables entre différentes autorités. Cela est rendu possible grâce aux normes et pratiques recommandées définies par l'Organisation de l'Aviation Civile Internationale (OACI) dans son bien connu Doc 9303, entre autres documents fournissant des indications. Dans ce document, l'OACI définit également les éléments de sécurité « de base » (c'est-à-dire obligatoires) et « supplémentaires » (c'est-à-dire facultatifs) des passeports.

Ces dispositifs de sécurité doivent désormais se défendre contre les menaces tant physiques que numériques. Empêcher la modification d'une photo d'identité demeure important, tout comme la capacité à garantir qu'une puce électronique intégrée ne puisse être altérée ou contrefaite. Ces dangers ne se limitent pas seulement aux passeports - d'autres types de documents de voyage, tels que les Laissez-Passer, sont soumis à des risques similaires.

Naturellement, la mise en œuvre de ces mesures défensives doit également tenir compte du coût de production. En règle générale, ces documents de voyage sûrs et pratiques doivent être rentables sur le plan économique, ce qui demande de sélectionner de manière judicieuse des caractéristiques techniques ayant un bon rapport coût/performance.

Le design continue lui aussi de jouer un rôle essentiel. Une identité visuelle forte, qui met en valeur le pays et sa culture à travers ses symboles souverains, est un élément clé du passeport moderne. Il en va de même pour la durabilité, une condition indispensable pour un document qui doit rester actif et sûr pendant dix ans d'utilisation normale.

3.2
Comment les livrets de passeport sont-ils fabriqués

Grâce au Doc 9303 de l'OACI, les passeports sont aujourd'hui des documents standardisés dont les caractéristiques de base sont communes et universelles. La plupart des passeports vierges sont fabriqués puis personnalisés à l'aide de techniques similaires, maîtrisées par des entreprises publiques ou privées de renommée mondiale.

3.3
Les principaux composants d'un livret de passeport

Les passeports suivent aujourd'hui un design général commun comprenant les éléments suivants :

- **La couverture** (avant et arrière)
  Elle constitue le premier niveau d'identification du document. La couverture peut comprendre un inlay électronique intégré (contenant une antenne et une puce sécurisée sans contact).
- **La couverture intérieure** (faces avant et arrière)
  Elle comporte une impression de fond sécurisée ainsi qu'une numérotation.
- **La page de données**
  Elle est habituellement positionnée comme la première page intérieure, bien que certains passeports utilisent encore la couverture interne à cet effet (ce qui est fortement déconseillée par l'OACI et la plupart des experts). La page de données peut être :
  - » En papier, toujours avec un film de sécurité, généralement holographique.
  - » En matière synthétique, faite principalement de polycarbonate. Celui-ci peut être électronique ou non, selon le choix de l'autorité chargée de sa délivrance.
- **Pages internes**
  Destinées aux observations et aux visas, ces pages sont fabriquées en papier de sécurité et comptent entre huit et soixante-quatre pages au total.

Un passeport présente également d'autres caractéristiques de fabrication essentielles, toutes étroitement liées à la sécurité :

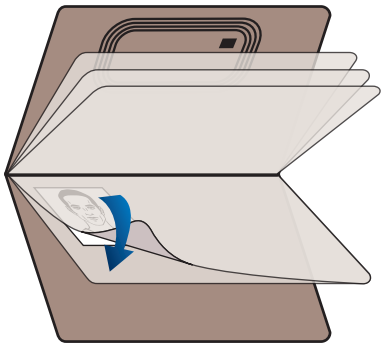
- Une charnière reliant une page de données en polycarbonate au reste du livret. Ce composant clé peut également comporter des éléments de sécurité.
- Un fil de couture fluorescent sous UV, appliqué selon une méthode spécifique, pour lier les composants du livret.
- Une ou des méthode(s) de numérotation permettant à chaque livret d'avoir son propre numéro de document, unique (il s'agit généralement d'une impression typographique combinée à une perforation au laser).
- Des techniques de personnalisation graphique contenant les données du titulaire. On les trouve sur la page de données, mais parfois aussi sur d'autres pages (une image du portrait supplémentaire immédiatement après la page de données, par exemple).
- Une couche de protection (généralement un film de sécurité très mince, aussi appelé « lamina ») utilisée pour protéger les informations personnalisées de la page de données, surtout si elle est en papier.
- Une personnalisation électronique de la puce sans contact, comprenant l'intégration de mécanismes de sécurité. Ceux-ci sont expliqués plus en détail dans la suite de ce rapport.

La position du composant électronique (antenne et puce) dans un passeport est laissée à l'appréciation des autorités de délivrance. Diverses solutions techniques sont disponibles, et les fabricants de dispositifs de lecture de passeports ont adapté leurs produits pour répondre à ces configurations.

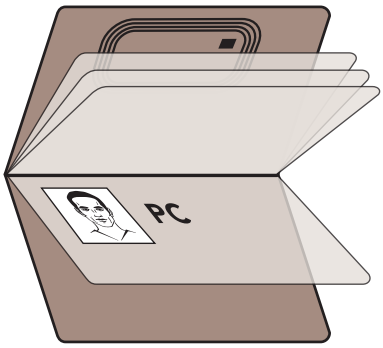
[1] Il peut être relativement facile de d'opérer un délaminage de la couverture d'un passeport, permettant aux faussaires de dissimuler une attaque sur une page de données.

3.4
Les formats de passeport les plus courants

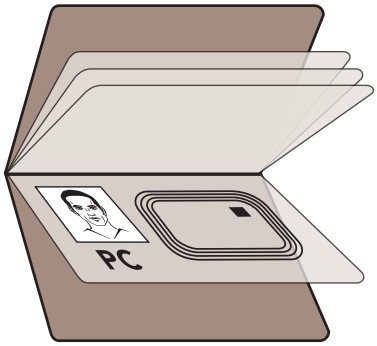
De nos jours, les passeports se présentent généralement dans l'un de ces trois formats (configurations):



1. Passeports avec une page de données en papier laminée, avec élément électronique dans la couverture arrière du livret



2. Passeports avec une page de données en polycarbonate, avec électronique dans la couverture arrière (ou avant) du livret



3. Passeports avec une page de données électronique en polycarbonate

Il existe quelques rares exceptions, comme des passeports dont la puce est intégrée au milieu du livret.

3.5
Entités clés du processus de fabrication

De manière générale, les organismes impliqués dans la fabrication de passeports peuvent se diviser en trois catégories. Certaines entreprises peuvent être impliquées dans ces trois domaines à la fois en raison de la diversité de leurs activités et par le biais de filiales.

i. **Fabricants publics et privés de documents sécurisés vierges**
Responsable de l'impression et de la finition d'un passeport vierge une fois que tous les composants sécurisés ont été assemblés. Ces entreprises sont les principaux fournisseurs des États souverains.

ii. **Fabricants de composants de sécurité**
Les composants de sécurité comprennent les papiers sécurisés, les pages en polycarbonate, les hologrammes, les encres, les fils de couture, les composants électroniques, etc. Les entreprises opérant dans ce domaine jouent un rôle majeur dans le renforcement de la sécurité des passeports.

iii. **Fabricants de machines de personnalisation**
Les machines dédiées à la personnalisation comprennent des imprimantes à jet d'encre, des imprimantes à transfert thermique, des toners laser, des dispositifs de gravure laser, des équipements d'impression UV, des laminateurs de films de sécurité, etc. Ces fournisseurs aident à créer le lien entre un passeport vierge et son titulaire.

3.6
Fraudes : types, techniques et objectifs

Lorsque des attaques physiques et électroniques sont menées contre des passeports, la fraude est très certainement l'objectif final. Qu'il s'agisse de tenter d'utiliser l'identité d'une autre personne ou d'en créer une nouvelle, fausse, la fraude au passeport est toujours orchestrée dans la poursuite d'activités illégales.

Le rapport SOCTA 2017 d'Europol identifie huit menaces criminelles prioritaires, énumérées ci-dessous. La fraude documentaire est l'une des trois « menaces criminelles transversales » qui, selon SOCTA, « permettent ou renforcent tous les types de criminalité grave et organisée ».

- La cybercriminalité
- La production, le trafic et la distribution de drogues
- Le trafic de migrants
- Le crime organisé touchant à la propriété
- Le trafic d'êtres humains
- La criminalité financière et le blanchiment d'argent
- La fraude documentaire
- Le commerce en ligne de biens et de services illicites

Le dernier rapport SOCTA, publié en avril 2021, ne fait que reconfirmer cette réalité : « La fraude documentaire est un catalyseur pour la plupart des activités criminelles… Sa prévalence est en partie due au fait qu'elle ne nécessite pas nécessairement d'outils sophistiqués ou d'investissement financier excessif. »

> *Europol recommande de se concentrer sur trois menaces criminelles transversales ayant un impact important sur l'ensemble de la grande criminalité organisée - la fraude documentaire, le blanchiment d'argent et le commerce en ligne de biens et services illicites.*
>
> **Quoted from SOCTA report 2017, Internal only**

Une fraude documentaire s'explique bien sûr de manière différente d'un incident à l'autre. De la « simple » criminalité financière, telle que l'ouverture d'un faux compte bancaire, à des fins plus graves comme le terrorisme, les faux documents tout comme les documents authentiques peuvent être utilisés pour un large éventail d'activités illégales. Compte tenu de l'omniprésence des passeports, tout le monde - des citoyens aux organisations privées et publiques – court le risque d'être victime de telles fraudes.

Quatre techniques principales sont utilisées dans la fraude touchant les passeports :

1.
La contrefaçon

La contrefaçon est la reproduction non autorisée d'un document authentique. Des matériaux et/ou des méthodes d'impression de substitution sont utilisés pour une partie ou la totalité du livret.

2.
La falsification

La falsification consiste à modifier un document authentique, à l'altérer frauduleusement pour fournir des informations trompeuses sur le porteur ou la validité du passeport. Cette menace touche aux éléments de sécurité et aux données du titulaire, comme sa photo d'identité. Certains documents falsifiés sont fabriqués à partir de matériaux provenant de documents légitimes[3].

Les documents volés vierges puis illégalement personnalisés entrent également dans cette catégorie. Ces documents sont authentiques, volés sur le site de fabrication, ou plus généralement à l'endroit où les documents sont personnalisés. Ces documents peuvent ensuite être personnalisés par le fraudeur en utilisant la même technologie que celle utilisée par un organisme légitime (ou d'autres technologies produisant un résultat similaire). Le résultat est une identité frauduleuse sur un document d'apparence authentique.

[2] Rapport SOCTA 2017 - https://www.europol.europa.eu/socta-report

[3] OACI - Documents de voyage lisibles à la machine, Huitième édition, 2021 – partie 2: Spécifications pour la sécurité de la conception, de la fabrication et de la délivrance des DVLM - https://www.icao.int/publications/pages/publication.aspx?docnum=9303

3.
La fraude à l'identité

La fraude à l'identité implique l'utilisation illégale de documents authentiques, et entre dans deux catégories : l'usurpation d'identité et l'obtention frauduleuse de documents.

L'usurpation d'identité (parfois appelée « fraude par ressemblance ») consiste en l'utilisation d'un document authentique par un imposteur qui prétend en être le titulaire. L'usurpateur peut utiliser un document qui a été perdu, volé ou emprunté à un complice.

Les documents obtenus frauduleusement proviennent de l'exploitation de failles potentielles dans le processus de délivrance. Cela peut inclure l'utilisation de "documents sources" qui sont soit faux, soit contrefaits, ou appartiennent à quelqu'un d'autre. Les fraudes de ce type sont parfois réalisées en coopération avec un fonctionnaire corrompu.

INTERPOL a découvert des cas où des organisations criminelles ont été capables d'obtenir frauduleusement des documents de voyage authentiques auprès de fonctionnaires impliqués dans le processus de délivrance des documents, par le biais d'un abus de position présumé.

Bien que nous ne couvrions pas la fraude à l'identité dans ce rapport, nous soulignons l'importance des listes de surveillance et des contrôles biométriques, y compris ceux utilisés dans le processus de délivrance.

4.
Pseudo documents

Il s'agit de documents qui semblent légitimes, mais qui ne cherchent pas réellement à reproduire des documents authentiques.

Les pseudo-documents prennent généralement la forme de :

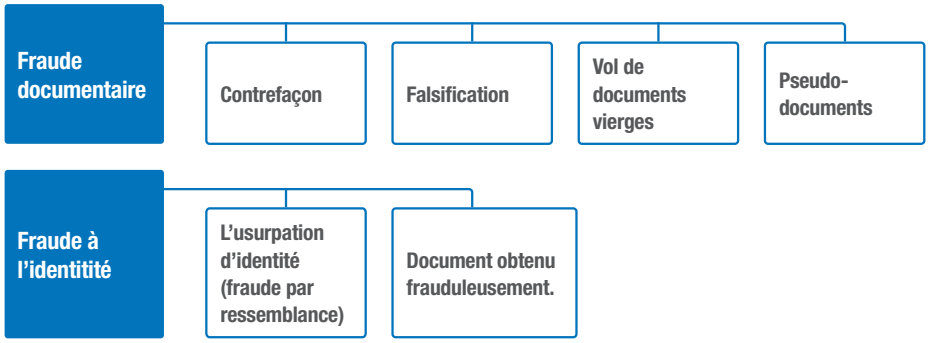
- Documents exotiques ou fantaisistes émis par un État ou une organisation imaginaires.
- Documents de camouflage d'un État qui n'existe plus ou qui a été renommé.
- Documents fictifs qui utilisent le nom d'un État ou d'une organisation réelle mais qui ne sont pas authentiques et n'ont pas d'équivalent légitime.

Bien que nous ne traitions pas des pseudo-documents dans ce rapport, il convient de noter que ce type de fraude peut être facilement détecté en consultant les listes fournies par le Registre Public En Ligne de Documents Authentiques d'Identité et de Voyage (PRADO) dans l'Union Européenne. Les lecteurs de documents modernes sont également capables de détecter de tels documents en utilisant les codes pays de l'OACI.

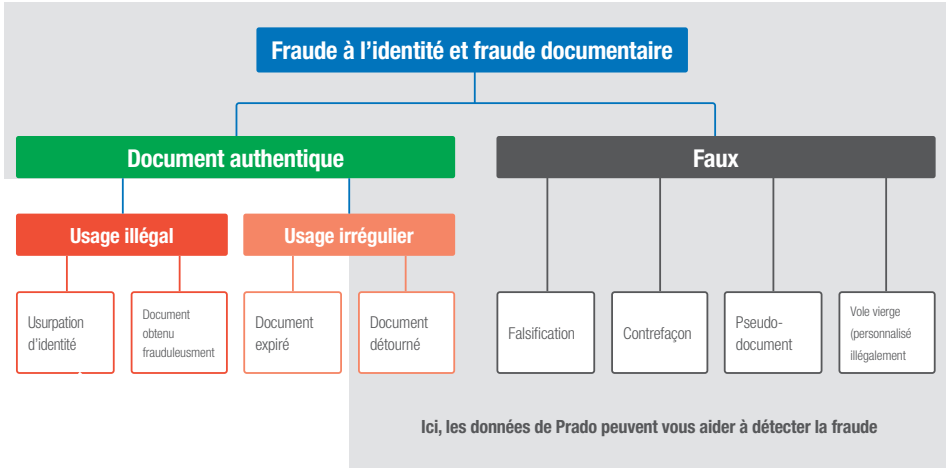
Le présent rapport se concentre principalement sur la contrefaçon et la falsification, communément appelées la « fraude documentaire ». La fraude à l'identité n'est pas couverte dans ce document car elle est principalement liée aux systèmes de délivrance et de contrôle, notamment des documents sources. Les pseudo-documents sont omis en raison de leur relative rareté.

3.7
Classification des fraudes

Le diagramme ci-dessous présente un schéma simplifié de classification des fraudes. Notez que l'utilisation irrégulière de documents authentiques (qu'ils soient expirés ou valides) n'est pas représentée.



Ce diagramme propose un résumé général des types de fraude, mais il existe d'autres façons de classer la fraude liée aux documents d'identité et de voyage. Par exemple, le modèle « Fraude à l'identité et fraude documentaire » a été adopté par le « European Union Document Fraud Risk Analysis Network », le réseau de l'Union européenne pour l'analyse des risques en matière de fraude documentaire (EDF-ARA 2012 Réf. R023) et est également utilisé par Frontex. Ce modèle est disponible publiquement et peut être trouvé dans le glossaire proposé par le PRADO[4].



Le registre PRADO se réfère au règlement de l'Union Européenne et aux recommandations de l'OACI.

INTERPOL propose un autre schéma, qui présente la fraude liée aux documents de voyage de manière relativement simple. Leur approche est similaire à celle utilisée par Frontex.

Les différents types de fraude documentaire[5]

Les criminels et terroristes utilisent souvent des documents d'identité et de voyage authentiques et frauduleux dans le cadre de leurs activités illégales.

Faux documents
- Contrefaçon : reproduction non autorisée d'un document authentique.
- Falsification : altération d'un document authentique.
- Pseudo-document : document non officiellement reconnu.

Documents authentiques
- Documents authentiques obtenus de manière frauduleuse.
- Usage frauduleux de documents authentiques par un imposteur.

[4] https://www.consilium.europa.eu/prado/en/prado-glossary.html

[5] Termes utilisés par INTERPOL. Sources ici https://www.INTERPOL.int/Crimes/Counterfeit-currency-and-security-documents/Identity-and-travel-document-fraud

3.8
La fraude documentaire en chiffres

Il est difficile de trouver des statistiques précises sur la fraude documentaire : rares sont celles qui sont a la fois accessibles au public et suffisamment fiables pour être dignes de confiance. Il existe bien sûr des exceptions, et celles recueillies par l'Agence Européenne de garde-frontières et de garde-côtes (appelée communément Frontex) donnent un bon aperçu de la situation globale relative à la fraude documentaire.

L'analyse de risques – publiée annuellement par Frontex – se base sur des statistiques mensuelles échangées par les États membres au sein du « Frontex Risk Analysis Network » (FRAN), le Réseau Frontex d'Analyse des Risques. Celui-ci met en lien Frontex avec des experts en analyse de risques et en renseignement des États membres. La détection de documents frauduleux est l'un des neuf indicateurs clés recueillis chaque trimestre.

En 2019, le nombre de documents frauduleux détectés aux frontières extérieures[6] était de :

- **Passeports**
  3582 sur les 7536 documents frauduleux détectés.

- **Passeports authentiques utilisés par des imposteurs**
  27 % (2019) ; autres types de fraude documentaire sur les passeports = 73 %.

Comme les années précédentes, la majorité des documents frauduleux ont été détectés aux frontières aériennes. En moyenne, ce sont sept détections sur dix qui se font sur ces itinéraires selon Frontex[7].

Bien entendu, ces statistiques ne représentent qu'un faible pourcentage des documents frauduleux saisis au total. Les faux documents ne sont pas seulement utilisés pour franchir les frontières, mais aussi pour un certain nombre d'autres entreprises criminelles.

Annex Table 10. Fraudulent documents used

Detectections on entry at the external borders, by country of issuance of the document and type of document

	2016	2017	2018	2019	Share of total	% change on prev. year	Highest share
Country of issuance							**Type of Document**
Spain	862	989	1 107	895	12	-19	ID Cards (37%)
France	783	1 030	944	817	11	-13	Passports (34%)
Italy	875	860	711	649	8.6	-8.7	Visas (29%)
Germany	469	504	412	443	5.9	7.5	Residence Permits (37%)
Turkey	69	117	276	315	4.2	14	Passports (95%)
Poland	886	740	404	272	3.6	-33	Visas (79%)
Greece	272	296	283	251	3.3	-11	ID Cards (34%)
Belgium	293	253	239	203	2.7	-15	Residence Permits (32%)
Senegal	78	91	75	192	2.5	156	Passports (98%)
Ghana	43	57	88	181	2.4	106	Passports (97%)
All Other	3 659	3 289	3 439	3 318	44	-3.5	Passports (68%)
Type of Document							**Type of Fraud**
Passports	2 764	2 885	3 130	3 582	48	14	AUTH-IMPOSTOR (27%)
Visa	2 124	1 856	1 454	1 179	16	-19	FALSE-COUNTERFEIT (47%)
ID Cards	1 166	1 309	1 461	1 163	15	-20	FALSE-COUNTERFEIT (45%)
Residence Permits	1 193	1 227	1 138	956	13	-16	FALSE-COUNTERFEIT (43%)
Stamps	832	710	602	496	6.6	-18	FALSE-COUNTERFEIT (85%)
Other	210	239	193	160	2.1	-17	FALSE-COUNTERFEIT (61%)
Total	**8 289**	**8 226**	**7 978**	**7 536**	**100**	**-5.5**	

[5] Indicateurs: détections de franchissement illégal de frontière entre points de passage frontaliers (PPF) ; détections de franchissement illégal de la frontière aux PPF ; détections de facilitateurs présumés ; détections de séjour illégal ; refus d'entrée ; demandes d'asile ; détections de faux documents ; décisions de retour de ressortissants de pays tiers en séjour irrégulier ; retours de ressortissants de pays tiers en séjour irrégulier. Plus d'informations sur : https://knowledge4policy.ec.europa.eu/dataset/ds00034_en

[6] Les « frontières extérieures » désignent les frontières extérieures de l'UE et des pays associés à l'espace Schengen. Source: Frontex Analyse de risques 2020

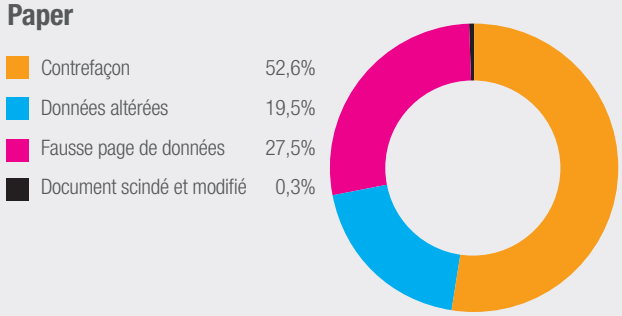
[7] Source : Frontex Risk Analysis 2020

3.8
La fraude documentaire en chiffres (suite)

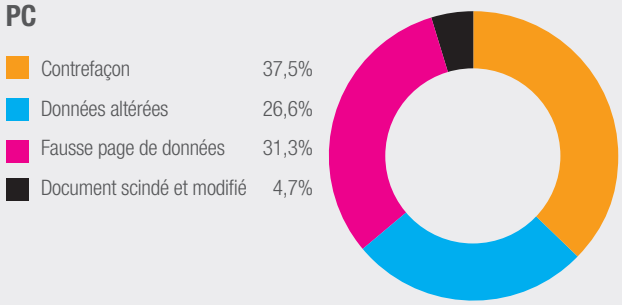
Keesing Technologies[8] a eu l'amabilité de bien vouloir nous fournir quelques statistiques supplémentaires. Celles-ci s'appuient sur les solutions de vérification d'identité Authentiscan - habituellement utilisées par des organisations non répressives, publiques ou privées. Par conséquent, les statistiques couvrent bien les cas de contrefaçon et de falsification de documents et elles sont principalement liées à des objectifs de connaissance du client (KYC – « Know Your Customer »), plutôt qu'au contrôle des frontières.

Passeports frauduleux – détail par type de page de données et de fraude documentaire

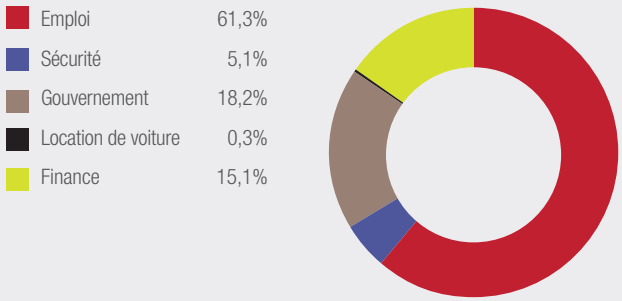
Paper



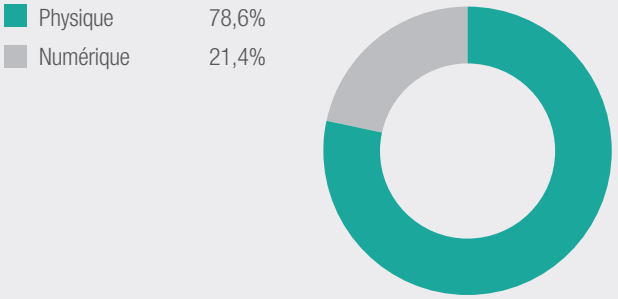
PC



Passeports frauduleux – détail par type d'industrie



Passeports frauduleux – détail par type d'image



Les attaques « numériques » concernent les images envoyées par un utilisateur (le détenteur du document télécharge des images - potentiellement modifiées - dans le système de vérification d'identité). Les attaques « physiques » portent sur des images prises dans un environnement réel. Cela peut se faire à distance par l'utilisateur avec un smartphone ou avec des scanners sur place. Il est plus difficile d'évaluer l'authenticité d'un document à partir d'images envoyées par un utilisateur plutôt que générées par un dispositif de confiance.

L'impact de la Covid-19

Alors que l'impact évident de la Covid-19 sur les voyages internationaux a contribué à ralentir le taux d'utilisation de documents frauduleux – « seulement » 3 885 documents frauduleux ont été détectés en 2020, selon Frontex.[9]

[8] https://keesingidacademy.com/product/study/

[9] Frontex - 'Frontex 2020 in brief' – Février 2021, https://frontex.europa.eu/publications/2020-in-brief-lrbE0G

3.9
Les faussaires de documents

Les faussaires de documents, qu'il s'agisse de contrefaçon ou falsification, peuvent être décrits principalement comme des entrepreneurs criminels proposant des produits et/ou services illégaux. On peut cependant les classer en plusieurs catégories, selon leur niveau d'investissement, leurs compétences et la qualité de leurs produits.

Voici la catégorisation proposée. Certains experts remarqueront des similitudes avec une classification possible des faussaires de billets de banque.

- **Non-professionnels**
  Personnes physiques qui falsifient des éléments de documents tels que des données biographiques ou des informations sur les pages de visa, souvent de manière grossière et non sophistiquée, ou qui produisent des documents sans tenter d'en simuler les éléments de sécurité.
- **Semi- professionnels**
  Individus utilisant des équipements d'impression à petite échelle (numériques et traditionnels) et des matériaux achetés dans le commerce, avec l'ambition de simuler des éléments de sécurité et la capacité de produire des documents trompeurs.
- **Professionnels**
  Individus et réseaux ayant accès à des équipements d'impression et de marquage haut de gamme et possédant des compétences techniques avancées, souvent capables de produire ou de se procurer des modèles et des imitations d'éléments de sécurité. Capables de produire des documents contrefaits trompeurs en grandes quantités.
- **Sophistiqués**
  Réseaux capables de produire des documents contrefaits particulièrement trompeurs et d'une grande sophistication.

Il reste difficile de proposer une classification précise et exhaustive - en raison notamment de la démocratisation de la contrefaçon de documents. Les particuliers peuvent aujourd'hui acheter des modèles Photoshop et des matériaux contrefaits tels que des hologrammes. Cela leur permet de passer de la catégorie semi-professionnelle à professionnelle.

Comme indiqué précédemment, il existe diverses motivations à la production de faux documents d'identité. Ceux-ci peuvent en effet être utilisés pour toutes sortes de démarches, comme l'ouverture d'un compte en banque ou d'une ligne téléphonique, mais aussi pour permettre le trafic d'êtres humains et de drogues, le blanchiment d'argent ou des actes de terrorisme. Par conséquent, la « qualité » d'un document frauduleux peut varier considérablement en fonction des intentions des fraudeurs.

En fait, s'il y a une chose commune aux faussaires c'est leur créativité. Préférant se faciliter la tâche, ils cherchent généralement à ne remplacer que des éléments tels que les photos d'identité et les numéros de documents, tout en conservant intacts les éléments de sécurité d'un document authentique.

Le même type de comportement peut être observé dans la contrefaçon de billets de banque. Le document ne subissant souvent qu'un rapide contrôle, il n'est guère nécessaire que l'ensemble soit falsifié. Par conséquent, la fraude documentaire est généralement un mélange de contrefaçon et de falsification (un livret authentique avec une fausse page de données, par exemple).

Comme dans beaucoup d'autres réseaux illégaux, les faussaires chercheront à établir le même type de systèmes de production que ceux auxquels les organismes autorisés ont accès. Aujourd'hui, la fraude documentaire est facilitée par des criminels qui se spécialisent dans la fourniture de faux composants, les faux documents vierges et la personnalisation non autorisée.

Les capacités que démontrent les faussaires ne font que souligner l'importance du travail effectué par les organismes de police dans le but d'étudier et neutraliser les réseaux partout où ils existent. Plus spécifiquement, certaines initiatives récentes des services de sécurité se sont focalisées sur ce que l'on appelle le "profilage de documents frauduleux". Cette approche vise à trouver des similitudes entre divers documents frauduleux saisis à différents endroits et à différents moments, et à déterminer s'ils peuvent provenir d'une seule source de production ou d'un seul fournisseur de composants.

3.9
Les faussaires de documents
(suite)

Comme le souligne Europol, « les documents contrefaits de haute qualité sont principalement produits par des contrefacteurs hautement spécialisés »[10], et les fraudeurs sont décrits comme des « criminels spécialisés proposant la fraude documentaire comme un service »[11], appartenant souvent à des réseaux criminels fluides.

À propos de la distribution de documents frauduleux

Pour s'en référer une fois encore à Europol, l'agence européenne spécialisée dans la répression de la criminalité note que « les documents frauduleux font de plus en plus l'objet d'un commerce en ligne et d'un trafic via les services postaux et les colis », une tendance qui s'est « accélérée durant la pandémie de COVID-19 ».

L'un des canaux fréquemment utilisés par les organisations criminelles pour la distribution de documents frauduleux est le « dark web ». Les services de répression sont bien déterminés à démanteler ces réseaux, mais c'est un nombre croissant d'affaires que l'on voit aujourd'hui être lié à l'Internet public. Parmi elles figurent de pures fraudes (escroqueries), dans lesquelles les fraudeurs sont payés à l'avance et n'envoient jamais aucun document - authentique ou non.

[13] Rapport SOCTA (2017)

[14] Rapport SOCTA (2021)

4.
Examen des catégories de fraude

Dans ce chapitre, nous examinons plus en profondeur les types de fraude documentaire les plus courants ; en regardant la typologie et la fréquence des attaques, comment la fraude se produit et les contre-mesures recommandées.

Afin de maximiser la sécurité, une grande partie du détail de cette section est exclu de ce document public. Ce détail se trouve dans la version restreinte réservée aux agences et autorités chargées de l'application des lois, et disponible pour le personnel autorisé en contactant CCSD@interpol.int

4.1
La contrefaçon

4.1.1 Le Passeport

Il est très rare qu'un passeport soit reproduit en partant de zéro tout en étant d'assez bonne qualité pour paraître authentique. La plupart du temps, plutôt que d'essayer de reproduire un original avec précision, les contrefacteurs en font une imitation capable de tromper les autorités et les non-spécialistes.

Les passeports les plus visés sont généralement ceux qui permettent d'accéder à des pays sans nécessiter de visa. C'est également le cas de ceux dont le design renferme un niveau de sécurité plus faible, étant plus faciles à imiter.

Les documents ayant une longue période de circulation (plus de 10 ans) sont également des cibles privilégiées. Les faussaires auront en effet plus de temps pour étudier et expérimenter diverses techniques de falsification du document, et pourront plus facilement réussir leur attaque. Même lorsqu'un document fait l'objet d'une modernisation, des tentatives de fraude se poursuivront tant que les anciennes versions continueront d'être utilisées.

> *Lorsque de nouvelles versions de documents d'identité sont émises, les fraudeurs peuvent choisir la voie la plus simple en s'attaquant à son ancien modèle, valide et en circulation pendant encore de nombreuses années. Ce phénomène peut être difficile à éviter. Lorsqu'ils le jugent nécessaire, certains émetteurs tentent d'atténuer ce problème en réduisant la durée de validité des passeports, par rapport à la durée maximum de 10 ans fixée par l'OACI (certains choisissent 5 ans) ; ou par exemple en introduisant une amélioration intermédiaire des éléments de conception et de sécurité après seulement 5 ans, plutôt que d'attendre la fin du cycle complet de 10 ans.*
>
> **Frank Smith**
> Ancien Directeur Adjoint au 'Home Office' du Royaume-Uni

Pour vérifier l'authenticité d'un document, les autorités de contrôle peuvent à la fois vérifier et contribuer à plusieurs bases de données, comme :

- PRADO (Public Register of Authentic Identity and Travel Documents Online, ou Registre Public En Ligne de Documents Authentiques d'Identité et de Voyage), une base de données accessible au public créée par le Conseil de l'Union Européenne
- iFADO (Faux Documents et Documents Authentiques En Ligne), également mis en place par le Conseil de l'Union Européenne. L'accès est strictement limité à certains organes d'application de la loi.
- Edison TD (Travel Documents), une base de données de référence en matière de documents de voyages et autres ressources liées aux voyages - développée par les autorités néerlandaises en coopération avec plusieurs autres autorités dont INTERPOL. Ce registre comporte trois niveaux d'accès : Public, LEA (« Law Enforcement Agencies » ou agences spécialisées dans l'application de la loi) et Expert (une sélection de laboratoires d'analyse), chacun fournissant des détails supplémentaires sur le document authentique. Les 194 pays membres d'INTERPOL sont connectés à cette base de données via son réseau de communication sécurisé appelé I-24/7.
- Documentchecker, une base de données de référence développée par Keesing Technologies (Pays-Bas), utilisée par des organisations publiques et privées afin de remplir leurs obligations légales : Know Your Customer (KYC) et Customer Due Diligence (CDD) – soit des obligations de connaissance du client.
- Dial-Doc, La Bibliothèque numérique INTERPOL d'alerte sur les documents, est une initiative conjointe du G8 et INTERPOL, permettant aux pays de partager dans le monde entier des alertes d'origine nationale sur les nouvelles méthodes de contrefaçon ou falsification des documents de voyage. En comparant des images et des descriptions de documents frauduleux en provenance du monde entier, le système permet de renforcer la coopération policière internationale en matière de contrôle d'identité et de lutte contre les faux documents.
- Il existe de nombreuses autres initiatives portées par les organismes de répression afin de collecter, produire et partager les alertes nationales, et qui mettent l'accent sur les principaux points de détection.

Certaines de ces bases de données de référence (PRADO et Edison TD en particulier) ont été rendues largement accessibles grâce à Internet, afin que chacun puisse tenter de déterminer l'authenticité d'un document avec de meilleures chances d'y parvenir. Les images de haute qualité et les informations complémentaires sur les éléments de sécurité authentiques ne sont toutefois accessibles qu'aux organismes autorisés.

> *Par contraste avec la longue tradition de stricte confidentialité autour des éléments de sécurité des documents, [ces] initiatives visent à sensibiliser le public à la fraude documentaire et à aider toute personne ayant à vérifier un document. Certains observateurs craignent que ces références publiques et ouvertes n'aident les faussaires dans leur entreprise, mais elles ne fournissent pas d'images de haute qualité des documents ni de descriptions détaillées des éléments de sécurité. Seuls des faussaires de piètre niveau pourraient potentiellement apprendre quelque chose de ces sites Internet* [11].
>
> **Simon Baechler**
> Docteur en science forensique, Université de Lausanne
> Chef du Domaine Traces et Analyse criminelle, Police neuchâteloise

Afin de soutenir la lutte contre la fraude, l'OACI recommande aux autorités qui émettent les passeports de partager des spécimens physiques et informations de base relatives aux éléments de sécurité avec les principales organisations qui gèrent les bases de données de référence, ainsi qu'avec les fabricants de lecteurs de documents : « En plus d'envoyer des spécimens aux États destinataires, il est bon d'en envoyer aux organisations qui proposent une base de données de référence sécurisée et qui fournissent des images de passeports ainsi que leurs éléments de sécurité[16]. »

Les autorités émettrices ont une responsabilité sociale dans le fait de faciliter les vérifications d'identité. Cela est en effet plus pratique pour les citoyens et stimule l'utilisation des services numériques. Un meilleur accès aux bases de données de référence offre divers avantages, comme par exemple :

- Une meilleure connaissance des éléments de sécurité à vérifier sur un document (grâce à des images de haute qualité) et leur rapide identification. Il y a même des contrôles automatiques qui peuvent être effectués en utilisant des modèles, par exemple.
- Une réduction du temps d'attente aux points de contrôle et un onboarding numérique (au sens, enregistrement en amont) plus simple pour les voyageurs.

Les tentatives de contrefaçon classiques peuvent être classées en deux catégories : l'une visant les matériaux sécurisés utilisés dans la création du passeport (les composants de base), et l'autre impliquant l'imitation des techniques de fabrication et les éléments de sécurité associées (par exemple, l'impression sécurisée).

[11] Baechler, S. Document Fraud: Will Your Identity Be Secure in the Twenty-first Century?. Eur J Crim Policy Res 26, 379–398 (2020). https://doi.org/10.1007/s10610-020-09441-8

[12] Guide OACI sur la diffusion des spécimens de documents de voyage / ICAO Guide for Circulating Specimen Travel Documents, Version: Release 2 - April 2019

4.1
La contrefaçon (suite)

Matériaux de substitution

La reproduction complète d'un passeport nécessite des matériaux de substitution. Il s'agit notamment du papier, du polycarbonate, des encres et films de sécurité, de fil de couture, de matériaux pour les charnières (pour les pages de données en polycarbonate) et du matériau de base nécessaire à la couverture.

Certains faussaires (très peu) tenteront de reproduire la plupart des composants ou des matériaux. D'autres auront des connaissances limitées et peu de moyens leur permettant de tenter une contrefaçon totale. Il existe ainsi de nombreux cas de contrefaçon différents, et l'aperçu ci-dessous est plus indicatif qu'exhaustif. Veuillez le considérer comme un guide général, et non comme une analyse précise.

Il convient de noter que les meilleures contrefaçons ne sont pas toujours détectées, même par des contrôleurs hautement qualifiés et expérimentés. Avec seulement quelques secondes pour analyser la validité d'un passeport, il arrive que des contrefaçons bien produites réussissent à passer les contrôles.

Voici un examen de certains des matériaux utilisés pour la production de contrefaçons.

Papier	**Filigrane** Étant l'un des premiers éléments de sécurité contrôlés, les contrefacteurs ont tendance à utiliser des filigranes à deux tons avec un design simple, ou à simuler le filigrane par impression. Il en résulte un manque de détails. S'il est réalisé par impression, un faux filigrane peut être visible sous lumière UV, ce qui n'est pas le cas d'un vrai. Assez souvent, les contrefacteurs utilisent des filigranes génériques, avec un design non-personnalisé ne correspondant pas aux filigranes authentiques.
	Fibres de sécurité Très souvent, la contrefaçon des fibres de sécurité est réalisée par impression. Les fibres visibles ont alors toutes la même apparence (aucune variation dans l'épaisseur), et peuvent se trouver au même endroit sur des pages différentes. Cela n'est pas le cas des fibres authentiques qui sont réparties de manière aléatoire, ce qui rend les contrefaçons relativement faciles à repérer. Certains fraudeurs ont toutefois trouvé le moyen d'imprimer des motifs de fibres de sécurité aléatoires.
	Fil de sécurité Les fils de polyester transparents et micro-imprimés sont le plus souvent contrefaits par impression. Les tentatives de fraude de cette nature sont assez faciles à identifier car, comme pour les fibres de sécurité, un fil de sécurité authentique est intégré au support papier et non sur sa surface, où il est visible sans lumière transmise.
Polycarbonate	Bien que certaines cartes en polycarbonate contrefaites (format ID-1) aient été trouvées sur le terrain, il n'existe actuellement aucune contrefaçon complète et significative de pages de données en polycarbonate. Les matériaux en polycarbonate sont bien sûr disponibles sur le marché public et pourraient donc être considérés comme moins sûrs que le papier de sécurité. Les polycarbonates spécialement conçus pour la gravure au laser sont toutefois plus difficiles à contrefaire, et certains permettent désormais des contrôles plus poussés, comme la fluorescence à réponse contrôlée sous UV. Cette dernière est différente de la fluorescence par ajout d'azurants optiques.
Couverture	Fabriquée en papier ou en textile, la couverture doit offrir un haut niveau de durabilité. Le matériau utilisé pour la couverture d'un passeport est très similaire à celui utilisé dans l'industrie de l'édition. Par conséquent, on peut rarement compter sur elle seule pour authentifier sereinement un document. Certains experts lui accordent toutefois une grande attention, car elle constitue le premier contact avec le document pour les agents de première ligne. Le passeport doit normalement être pris fermé avant toute inspection. Par conséquent, le toucher de la couverture ainsi qu'une vérification rapide des côtés du livret peuvent aider à détecter un problème avant d'inspecter l'intérieur.
Fil de couture	Cet élément de sécurité est rarement contrefait. Lorsque des reproductions sont utilisées, une coloration bleue sous lumière UV, voire une absence totale de fluorescence, permettent de les identifier. La plupart des fils de couture authentiques utilisent des couleurs fluorescentes aux UV moins disponibles, comme le rouge.
Film de sécurité (laminas pour les pages de données en papier)	Les films de sécurité modernes étant des matériaux très complexes, les contrefacteurs ont tendance à ne pas essayer de les reproduire de manière authentique, mais à créer de faux équivalents suffisamment bons pour passer auprès des autorités et des citoyens. Si les techniques holographiques ont rendu la contrefaçon de pages de données papier plus difficile, l'efficacité de ces méthodes repose sur l'intégration de nouveaux éléments hautement sécurisés. Cela nous amène à souligner l'importance d'une communication claire avec les services de contrôle au sujet des contrefaçons courantes et la manière de les reconnaître. L'OACI recommande d'utiliser un film de sécurité sur toute la page de données personnelles (papier).
Marques Optiques variables	Les contrefacteurs préfèrent garder les éléments de sécurité à la surface des pages de données en polycarbonate, et ce pour une bonne raison. Les hologrammes sont aujourd'hui un élément optique variable très répandu. Lorsqu'ils sont contrefaits, la mauvaise qualité qui les caractérise généralement risque de ne pas passer un contrôle effectué par un professionnel. Les faussaires tentent ainsi d'extraire directement la couche qui présente une marque optique variable afin de réutiliser ce matériau authentique. La première génération d'encres optiques variables - disponibles en dehors du marché de la sécurité (par exemple, le marché des cosmétiques) - constitue un autre angle d'attaque.

Techniques d'imitation

Reproduire un passeport signifie également recréer les techniques utilisées lors de fabrication. Cela va du fond de sécurité (c'est-à-dire les éléments de sécurité imprimés) aux différentes techniques de fabrication et éléments de sécurité utilisés sur les documents authentiques.

Les scanners, les logiciels de modification d'images et les technologies d'impression (jet d'encre, laser et sublimation) jouent ici un rôle. Les technologies grand public proposent en effet des résolutions toujours plus élevées et offrent ainsi aux faussaires un arsenal plus complet que jamais pour simuler des documents d'identité.

Voici un examen de quelques-unes des techniques utilisées.

Couverture	L'estampage à chaud est une technique disponible dans le commerce. Elle est principalement utilisée pour l'identification et l'embellissement des couvertures de livrets de documents de voyage. Elle n'est cependant pas toujours maîtrisée par les contrefacteurs : un estampage de film de dorure de mauvaise qualité (avec une mauvaise définition et/ou une mauvaise adhérence) devrait suffire à déclencher la vérification approfondie du document. Le gaufrage ou l'impression fluorescente aux UV sont moins fréquemment utilisés sur la couverture, et ne seront pas nécessairement reconnus par un contrôleur.
Impression et encres de sécurité	Les technologies de haute résolution étant de plus en plus disponibles, la contrefaçon devient plus facile. Un grossissement minimal de x15 est désormais nécessaire pour voir la différence entre une impression de sécurité et une contrefaçon.
Méthode de couture	La méthode de couture utilisée pour la reliure des livrets de passeport n'est pas complexe en soi. Elle n'est toutefois pas totalement maîtrisée par tous les contrefacteurs, et une qualité moindre risquera de déclencher un contrôle plus approfondi.
Perforation Laser	La perforation mécanique (sans utilisation de technologie laser) peut être reproduite, mais son utilisation est de plus en plus rare. En revanche, la contrefaçon par perforation laser conique est en augmentation, mais elle est beaucoup plus difficile à reproduire lorsque la perforation n'est pas uniforme (c'est-à-dire lorsqu'elle utilise des formes différentes comme des cercles et des carrés).
Personnalisation	Les contrefacteurs utilisent souvent les technologies d'impression à jet d'encre et d'impression au laser pour fabriquer de fausses pages de données papier.

4.1
La contrefaçon (suite)

Contre-mesures recommandées

Les fraudeurs ont tendance à employer les techniques qu'ils connaissent le mieux, surtout à mesure que les matériaux et les moyens de les utiliser deviennent plus largement disponibles. Par conséquent, des éléments de sécurités qui sont nouveaux, innovants et surprennent les fraudeurs jouent un rôle majeur en rendant certaines caractéristiques beaucoup plus difficiles à reproduire.

Certains éléments de sécurité très complexes sont utilisés depuis des décennies, bien sûr, et n'ont pas encore été contrefaits. Chacun d'entre eux a un cycle de vie, et certains nécessitent une évolution plutôt qu'une réinvention.

Des organisations comme l'OACI sont en constante recherche d'éléments de sécurité plus récents et les utilisent pour élaborer les recommandations qu'elles fournissent aux gouvernements à travers le monde. Aucun élément de sécurité n'étant sans faille ou fonctionnant à tous les coups, cette démarche est vitale.

Une bonne sécurité repose sur une combinaison de plusieurs éléments qui interagissent les uns avec les autres. La bonne combinaison de technologies peut rendre la fraude documentaire très complexe, tout en répondant aux besoins de l'utilisateur final - un document facile à utiliser, mais difficile à reproduire.

Afin de déterminer si un nouvel élément doit être, ou non, appliqué à un document, les experts impliqués doivent tenir compte de certains points essentiels (ceux-ci ne sont pas classés par ordre d'importance) :

- Le niveau de sécurité, et si l'élément peut être détecté à l'œil nu. Certains éléments peuvent être contrôlés sous le prisme de plusieurs niveaux de sécurité, jusqu'à trois selon la classification traditionnelle.
- S'il peut être contrôlé via une authentification par lecture optique (OMA, pour Optical Machine Authentication). Cette technologie en développement aide à la vérification de documents, et certains éléments de sécurité sont adaptés ou conçus spécifiquement pour elle.
- La facilité avec laquelle il est possible de contrôler l'élément de sécurité. Certains experts estiment que pour être efficace, il doit être :
  - » Facile à expliquer (certaines caractéristiques sont très intuitives et ne nécessitent pratiquement aucune formation).
  - » Facile à comprendre et à mémoriser.
  - » Facile à localiser, à reconnaître et à contrôler (authentification) - l'aspect le plus critique étant le temps total de ce processus.
- Dans quelle mesure il permet de résister à la fraude. Un bon élément de sécurité, en général, est :
  - » Difficile à imiter (avec des technologies alternatives).
  - » Difficile à reproduire (contrefaçon totale).
  - » Difficile à se procurer (le fraudeur devra trouver le même produit auprès d'un fournisseur spécialisé). Certains sont difficiles à obtenir parce que la quantité minimale à commander est élevée, augmentant ainsi l'investissement.
- Les aspects visuels, et en particulier l'impact sur la lisibilité des données de personnalisation graphique. La facilité avec laquelle l'élément s'intègre et se combine avec le design d'ensemble du document est également importante.
- La sécurité de la chaîne d'approvisionnement, de la production au transport.
- L'impact sur le coût total du document. Il n'existe pas de règle générale dans ce domaine, car chaque technologie possède son propre modèle de coût. En général, le lien entre le coût et la quantité varie beaucoup d'un élément de sécurité à l'autre - et même d'un fournisseur à l'autre.
- L'exclusivité, ou la disponibilité sur le marché. L'élément de sécurité est-il fourni par une seule entreprise ou peut-on trouver des alternatives équivalentes auprès d'autres fournisseurs de confiance ? Une offre limitée est synonyme de sécurité accrue, du moins en théorie.

La classification des éléments de sécurité

Bien qu'il n'existe pas de norme internationale en matière de classification des éléments de sécurité, un système à trois niveaux est généralement accepté comme une base pour leur évaluation. Ces niveaux sont les suivants :

- **Niveau 1 :** Les contrôles peuvent être effectués avec les sens humains, à la lumière du jour, et sans utilisation d'un outil spécialisé. Le contrôleur pourra être amené à toucher, regarder ou incliner l'élément pour l'authentifier.

- **Niveau 2 :** Contrôlable à l'aide d'un outil de vérification simple et largement disponible. Le plus souvent, il s'agira d'une lampe UV (UV-A 365nm) ou d'une loupe (x10).

- **Niveau 3 :** La vérification exige un outil spécifique et/ou d'analyse scientifique (laboratoire) - typiquement, un microscope et/ou un comparateur vidéo spectral.

Icônes créées par Secure Identity Alliance afin de représenter les trois niveaux de sécurité

Certains experts considèrent qu'il existe un quatrième niveau, relatif aux éléments gardés secrets par le fabricant du document ou du composant en tant que niveau de sécurité supplémentaire. De plus, les téléphones portables étant désormais dans les mains de la quasi-totalité des individus, certains classent en niveau « 1,5 » les éléments de sécurité pouvant être vérifiés avec ce type d'outil . Les trois niveaux décrits ci-dessus doivent être considérés comme une ligne directrice, plutôt que comme une règle.

Les contrôles peuvent être effectués soit en "première ligne" (avec généralement seulement quelques secondes disponibles), soit en "deuxième ligne" (pour une analyse plus approfondie qui demande plus de temps). Par conséquent, certains éléments de sécurité ne sont pas adaptés aux contrôles de première ligne. Il est important que les professionnels qui conçoivent les directives de vérification des documents tiennent constamment compte de la différence entre ces deux cas.

La disponibilité des éléments de sécurité

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 pour la sécurité des documents, cela signifie également que certaines technologies exclusives ne peuvent être trouvées qu'auprès d'un seul fournisseur, entrainant un risque de devenir client captif, risque qui doit être évalué et géré.

Conscientes de cette question, les autorités de délivrance savent qu'il est de leur responsabilité de consulter les fournisseurs sur les technologies qui font l'objet de brevets actifs. Le fait qu'un élément de sécurité soit exclusif – spécifique à un fournisseur - n'est pas nécessairement une raison suffisante pour éviter d'utiliser cette technologie.

Lors de la modernisation d'un document, un juste équilibre doit être trouvé entre la sécurité globale et l'utilisation de technologies propriétaires. En évaluant les options qui s'offrent à eux, les gouvernements trouvent grand avantage à travailler avec des organismes certifiés ; les membres de la SIA, par exemple, détiennent « une ou plusieurs certifications de sécurité et une ou plusieurs certifications de sécurité des technologies de l'information, reconnues par les États membres de l'Union Européenne[14] ».

[14] https://secureidentityalliance.org/about-secure-identity-alliance/join-us/types-of-membership

4.1
La contrefaçon (suite)

Analyse des éléments de sécurité, des matériaux et des techniques de fabrication.

Élément de sécurité	Niveau	Leur contribution à la prévention de la fraude
Supports sans fluorescence sous UV	**2**	« Papier sans fluorescence sous UV, ou support à réponse sous UV contrôlée, tel qu'il présente, lorsqu'il est exposé au rayonnement UV, une fluorescence dont la couleur se distingue de la luminescence bleu-blanc utilisée dans les matériaux généralement disponibles sur le marché contenant des azurants optiques. » Ceci est la définition donnée par l'OACI. Cet élément de base est une mesure efficace contre les contrefaçons de faible qualité.
Filigrane (papier)	**1**	Filigranes multi-tons (parfois appelés filigranes « en forme ronde » ou filigranes "ombrés") présentant de subtils changements de ton (plus de deux) et des zones claires et obscures. Il n'est pas possible de reproduire ce type de filigrane par impression, et il n'est pas aussi disponible sur le marché que le papier filigrane à deux tons (produits sur machines dites de Fourdrinier ou « table plate »). Éléments de sécurité supplémentaires : » Filigrane spécifique pour la page de données » Électrotype fin avec numérotation des pages
Fibres de sécurité (papier)	**1-2**	Fibres de sécurité multicolores, visibles et/ou invisibles, fluorescentes aux UV, dispersées de manière aléatoire dans le papier. Impossible à réaliser par impression.
Fil de sécurité (papier)	**1-2**	Plus facile à identifier à la lumière transmise, il est idéalement placé sur le côté de la page. On peut aussi le placer près de la charnière pour faciliter l'authentification lors de la vérification du filigrane. Les fils métalliques clairs sont plus complexes à imiter, et la fluorescence d'une ou plusieurs couleurs accroît la difficulté de reproduction. Les fils fenêtrés - rarement utilisés dans les passeports - sont parmi les fils de sécurité les plus difficiles à imiter. En effet, ils sont intégrés en partie dans le papier et apparaissent également en surface. Des propriétés optiques supplémentaires sont parfois présentes. Remarque : s'il est incorporé, un fil fenêtré doit généralement être positionné sur la page trois ou les pages de couverture intérieures.
Fenêtre transparente sur la page de données en polycarbonate, avec marque optique variable	**1-2-3**	Les pages de données sont le plus souvent fabriquées en fusionnant des couches de polycarbonate. Une façon de rendre ces structures plus difficiles à falsifier et plus rapides à authentifier consiste à inclure une ou plusieurs zones transparentes dans l'épaisseur de la structure. Il s'agit souvent d'une fenêtre, de taille et de forme variables, qui peut parfois être asymétrique. Une sécurité supplémentaire est conférée par un fond imprimé avec une encre à optique variable ou métallique et/ou une personnalisation gravée au laser (par exemple, les données personnelles du titulaire, une image).
Polycarbonate de sécurité	**1-2-3**	Les polycarbonates spécialement conçus pour la gravure au laser sont plus difficiles à contrefaire, et il existe maintenant des matériaux en polycarbonate permettant des contrôles supplémentaires du niveau de sécurité.
Impression Offset	**1-2**	Un fond de haute qualité et détaillé utilisant des guillochis, du micro texte et d'autres éléments graphiques complexes uniquement disponibles via un logiciel spécifique.
Impression taille-douce	**1-2-3**	Présente sur les couvertures internes à l'avant et/ou l'arrière d'un livret de passeport, l'impression en taille-douce peut inclure des motifs cachés (par exemple, des images latentes), des éléments tactiles et des micro-textes.

Security features	Level	How they aid fraud prevention
Encres à propriétés optiquement variables	**1-2-3**	Imprimées sur les zones transparentes d'une page de données en polycarbonate, les encres à propriétés optiquement variables permettent une authentification simple à effectuer en première ligne.
Estampage à chaud sur la couverture	**1**	L'estampage à chaud de bonne qualité et constitué d'un design de haute définition est difficile à reproduire. Toutefois, en raison de l'accès aisé à cette technique, certains ne considèrent pas l'estampage à chaud comme un élément de sécurité.
Gaufrage (embossage réalisé lors de la lamination du polycarbonate) avec un effet optique et/ou un micro texte	**1 -2**	Difficile à reproduire, et dont l'absence est facile à détecter au toucher ou à la lumière oblique (angle rasant). Des outils spéciaux sont toutefois nécessaires pour vérifier la présence de micro textes.
Gaufrage lié à une couleur optiquement variable	**1-2-3**	Une combinaison d'embossage tactile avec un type de polycarbonate de sécurité, et/ou des encres optiquement variables sécurisées dans des zones transparentes (par exemple, une fenêtre transparente).
Fil de couture	**1-2-3**	Il est recommandé d'utiliser un fil à coudre fluorescent sous UV comportant jusqu'à trois brins de couleurs UV différentes (l'utilisation d'une fluorescence bleue seule est à éviter). Certains fils peuvent intégrer des éléments de sécurité de niveau 3 si nécessaire.
DOVID (pour les pages de données papier et PC)	**1-2-3**	Les DOVIDs (pour « Diffractive Optically Variable Identification Devices », en français « dispositifs optiquement variables diffractifs ») sont l'un des éléments les plus couramment contrôlés lors de vérifications d'identité.
Perforation laser (numérotation du livret)	**1**	Les trous perforés au laser et adoptant différentes formes (des cercles, des carrés et des triangles) sont beaucoup plus difficiles à contrefaire que les trous perforés de manière mécanique, ou bien perforés au laser (conique) avec une seule forme.

4.1
La contrefaçon (suite)

Éléments de sécurité spécifiquement liées à la personnalisation

Des machines spéciales sont utilisées pour renforcer la sécurité des passeports vierges lors de leur personnalisation. La page de données étant le composant du passeport le plus souvent attaqué, ce procédé est en effet essentiel. Les technologies de personnalisation sont spécialement adaptées aux pages en papier ou en polycarbonate, et seule leur combinaison minutieuse offre le plus haut niveau de sécurité.

Il est fortement recommandé d'inclure plusieurs images du portrait du détenteur dans le livret de passeport, de préférence en utilisant différentes technologies. Elles doivent être suffisamment grandes pour faciliter le contrôle. Cela peut être facilité par des Images Laser Multiples (disponibles pour les pages de données en polycarbonate) ou par un portrait supplémentaire obtenu par gravure laser ou perforation. Ces dernières machines ne sont disponibles que pour les fabricants de documents sécurisés certifiés.

De nombreuses solutions peuvent être utilisées pour intégrer des photographies en couleur sur des pages en polycarbonate. Une gravure laser ou une impression couleur peut être appliquée au cœur de la structure. Une combinaison de gravure laser noire et d'impression couleur peut également être utilisée en surface de la page de données.

Une autre possibilité de personnalisation consiste à imprimer un portrait supplémentaire en couleur sur la page 3 (après la page de données). Ce procédé est nativement protégé par le fond de sécurité (avec des éléments offset visibles et invisibles). La sécurité peut être renforcée par des mesures de sécurité supplémentaires telles que :

- Des portraits holographiques transparents et colorés (élément de sécurité de niveau 1).
- Portraits réalisés à partir de micro-textes (élément de niveau 2, nécessitant une vérification à la loupe).
- Protection du portrait par technologie numérique (une garantie de l'authenticité du portrait, les données étant scellées par un Cachet Electronique Visible interopérable).
- Informations cachées intégrées dans le portrait (Niveau 3 de sécurité, vérifié avec un filtre spécifique).

Les portraits en couleur sont utiles contre la fraude documentaire dans son ensemble (contrefaçon ou falsification), et plus particulièrement contre la fraude à l'identité. La couleur peut également aider la police à authentifier la personne en comparant la photo du document au porteur.

Élément de sécurité	Niveau	Leur contribution à la prévention de la fraude
Combinaison de différentes techniques de personnalisation	**1-2**	L'utilisation de différentes technologies pour imprimer le portrait rend la contrefaçon plus difficile. Par exemple, il est possible d'utiliser la gravure au laser pour le portrait principal sur une page de données en polycarbonate, et de la combiner avec une impression en couleur et/ou fluorescente sous UV sur la page 3.
Portrait en couleur pour la page de données en polycarbonate	**1-2**	Les portraits en couleur pour le polycarbonate sont dans leur ensemble des technologies relativement nouvelles, qui ne sont pas encore maîtrisées par les contrefacteurs.
Gravure laser tactile (pour les pages de données en polycarbonate)	**1**	Les éléments tactiles servent généralement à personnaliser les numéros de documents ou les dates d'expiration, des données susceptibles d'être modifiées par les contrefacteurs.
Personnalisation dans les zones transparentes	**1-2**	Positionner le portrait dans une fenêtre transparente est l'élément de sécurité le plus couramment utilisé. Cela permet une authentification facile (très intuitive), et renforce la sécurité apportée par la zone transparente.
Personnalisation dans une structure lenticulaire	**1**	L'élément le plus couramment utilisé ici est une Image Laser Multiple (ou MLI pour « Multiple Laser Image »), intégrant une image du portrait et une donnée clé (par exemple, la date d'expiration).

4.1.2 Passeports biométriques

Certains rapports d'alerte font état de l'utilisation de fausses puces dans des passeports contrefaits. Il est difficile de quantifier ce phénomène, mais ces alertes suggèrent l'existence de fausses puces (plus ou moins) avancées qui simulent le comportement des puces officielles. « Plus ou moins » signifie ici que, logiquement, avec un solide dispositif de contrôle standard, la fraude sera détectée par signalement (l'authentification passive n'aura pas fonctionné, par exemple).

Comme nous l'a souligné un expert en fraude documentaire et à l'identité travaillant en contrôle aux frontières, « le problème est que de nombreux gardes-frontières ne sont pas du tout conscients de la menace. Par conséquent, s'ils ont été inondés de faux positifs auparavant, ils auront tendance à ignorer les messages envoyés par le système. Un travail de vulgarisation est donc indispensable."

Pendant ce temps, des documents avec des puces contrefaites continuent de circuler. Ceux-ci ne contiennent parfois qu'un BAC, DG1 et DG2 mais pas de EF.SOD (c'est-à-dire pas de signature). D'autres documents de voyage avec puce contenant des données en DG1 et DG2 et signée « UTOPIA » ont également été observés. Naturellement, ils ne correspondent à aucun pays réel.

L'utilisation de ces documents reste peu fréquente et, si l'appareil de lecture est aux normes, le problème sera signalé. Leur existence doit tout de même être prise en compte.

Comme nous l'a expliqué notre interlocuteur des services de contrôle aux frontières lors de la rédaction de ce rapport, il est donc important que :

- Les dispositifs développés réduisent autant que possible le taux de faux positifs afin que la police puisse avoir une confiance totale dans le système et agisse en fonction des messages qui lui sont envoyés. Des messages clairs relatifs aux anomalies détectées devraient être délivrés afin de s'assurer que les agents de police restent actifs dans la détection de la fraude et/ou la levée de doute.
- Les agents reçoivent une meilleure formation quant aux défis que représente le contrôle de la composante électronique des Documents de Voyage Lisibles à la Machine électroniques (DVLM-e).

Comme on peut le déduire des exemples ci-dessus, la contrefaçon potentielle de la partie électronique d'un passeport est directement liée à l'âge de ses composants sécurisés : son logiciel, son système d'exploitation (OS ou 'Operating System') et son circuit intégré (IC ou 'Integrated Circuit').

De ce fait, le respect des normes et recommandations en matière de sécurité électronique est le moyen le plus sûr de préserver l'intégrité des puces. Par exemple, les Etats qui mettent en place des passeports biométriques avec contrôle d'accès étendu (EAC ou 'Extended Access Control') tels que définis par l'OACI garantissent à leurs citoyens le plus haut niveau de sécurité. Les différents mécanismes de sécurité recommandés par l'OACI pour les composants électroniques sont détaillés dans une autre section.

Afin de s'assurer que seuls des documents dignes de confiance sont délivrés, le système d'exploitation et le circuit intégré contenus dans un passeport électronique doivent faire l'objet d'une certification de sécurité (les Critères Communs) avant l'émission. Les certificats de sécurité Critères Communs (CC ou 'Common Criteria') démontrent seulement qu'un produit répond aux exigences au moment de la certification, et n'ont aucune signification quant à leur sécurité effective à une date ultérieure.

Le passeport électronique a généralement une longue période de validité, la plupart du temps de dix ans. Les durées de vie d'un logiciel intégré et d'une puce sont toutefois plus longues que la période de validité du document d'identité lui-même.

Afin de garantir à tout moment la sécurité effective des composants des systèmes d'exploitation et des circuits intégrés, certains pays mettent en œuvre des processus de surveillance qui permettent de contrôler le logiciel et la puce intégrés. La dégradation potentielle du niveau de sécurité de ces composants peut ainsi être vérifiée tout au long de leur durée de vie.

Ce type de surveillance peut fournir des informations pour les plans de gestion des risques. Il permet aux autorités émettrices d'anticiper la fin de vie d'un système d'exploitation ou d'un circuit intégré, et d'ordonner la migration vers de nouvelles générations. En outre, elle permet aux autorités de délivrance de définir différents plans d'urgence adaptés au niveau de violation de sécurité pouvant être rencontré.

[15] EF « Elementary File » – Dossier élémentaire / SOD « Document Security Object » - Objet de sécurité du document

4.2
Falsification

4.2.1 La couverture

Remplacement de la couverture

Certains faussaires tentent de transformer la couverture d'un passeport ordinaire en passeport diplomatique afin d'éviter de devoir présenter un visa lors du passage d'une frontière. Pour ce faire, ils se contentent d'ajouter une nouvelle couverture ou de retirer la couverture existante pour la remplacer.

Ce type de fraude peut d'abord être détecté en prêtant attention aux marques d'identification qui caractérisent le livret de passeport diplomatique. En général, une mention indiquant clairement qu'il s'agit d'un document diplomatique est imprimée sur la page de données, au recto et au verso.

En prévention, les autorités de délivrance doivent rendre le retrait de la couverture aussi complexe que possible en utilisant les matériaux et méthodes de collage appropriés. Le papier des couvertures internes doit être suffisamment fragile pour rendre toute manipulation évidente.

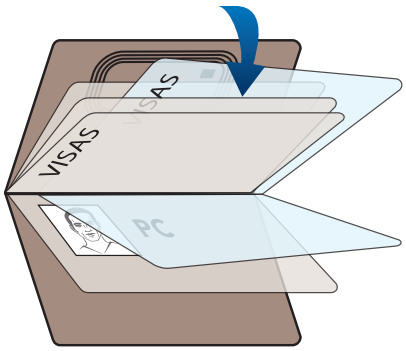
4.2.2 Le livret

La suppression ou le remplacement (substitution) de pages de visa entières

Dans les livrets de passeport, les pages de visa sont sujettes à deux catégories de fraude :

i. La page de visa est découpée et repositionnée à un autre endroit du même livret ou dans un autre. Cette opération a généralement pour but de dissimuler le fait qu'une page a été découpée, car elle contient - par exemple - un visa périmé délivré par le pays dans lequel le voyageur séjourne. La page manquante est ensuite remplacée par une autre page du même livret ou d'un autre livret.

ii. La page de visa est divisée en deux fines feuilles. Le but de cette opération est d'éviter de devoir réinsérer une page complète dans le livret de passeport.



Exemple de remplacement d'une page de visa (Feuillet de quatre pages complet)

Si le fraudeur décide de remplacer un feuillet de quatre

Retrait/remplacement (substitution) de visa autocollant

Il arrive que les faussaires retirent des visas autocollants d'un livret de passeport pour les apposer dans un autre, dans le but d'accéder à un territoire.

Les visas collés dans le passeport sont généralement autocollants. Les fraudeurs utilisent la chaleur (ou des produits chimiques) pour ramollir la colle, afin de soulever et de retirer plus facilement la vignette, à condition de le faire lentement et soigneusement.

Il existe trois façons de prévenir ce type de manipulation :

i. La vignette de visa peut être prédécoupée dans plusieurs directions afin de la rendre plus fragile.

ii. Des agents réactifs aux produits chimiques peuvent être inclus dans le papier servant aux pages de visa et dans l'autocollant lui-même.

iii. Des encres de sécurité peuvent être utilisées pour imprimer des motifs de fond.

Suppression de tampons

Les fraudeurs tentent généralement de supprimer les tampons présents sur les pages de visa en utilisant des produits chimiques ou une gomme, voire en grattant. Pour prévenir ces menaces, les mesures suivantes peuvent être employées :

i. Imprimez le motif de fond avec des encres sensibles aux solvants qui réagiront aux produits chimiques ou à l'eau.

ii. Des agents peuvent être intégrés au papier des pages de visa. Ils réagiront aux produits chimiques en produisant un effet de coloration.

iii. Utilisez une encre qui disparaît lorsqu'on la frotte. Une partie du fond de sécurité disparaîtra en cas d'altération du tampon.

iv. Faites en sorte que le support papier soit suffisamment fragile pour créer des dommages visibles si un fraudeur tente de gratter les données personnalisées.

4.2.3 Page de données papier

A. Substitution de la page de données entière

En bref, la page de données est supprimée et remplacée par une fausse page contenant des données frauduleuses. Du faux fil de couture peut également être utilisé dans cette opération. Les faussaires cherchent à imiter l'aspect original de la page de données et du papier, même si les motifs imprimés holographiques ne sont pas tout à fait exacts.

La falsification de pages de données peut venir d'une série de facteurs :

- Pages de données vierges d'un faible niveau de sécurité, faciles à contrefaire.
- Films ou couches de protection de faible niveau de sécurité.
- Films de protection volés à la suite d'un stockage non sécurisé.
- Méthodes de couture et/ou fil de couture de faible niveau de sécurité.
- Méthodes de numérotation de faible niveau de sécurité, notamment pour les pages internes.
- Absence de puce électronique dans la couverture (contenant une photo d'identité numérique authentique et protégée par des mécanismes de cryptographie de pointe).
- Un livret trop facile à démonter et réassembler sans laisser de traces d'effraction.

Contre-mesures recommandées

Éléments de sécurité non liés à la personnalisation

Éléments de sécurité	Niveau	Leur contribution à la prévention de la fraude
Page de données **1. Motif unique** **2. Un filigrane unique (différent de celui utilisé sur les pages intérieures)**	**1-2**	1. Un motif unique rend impossible l'utilisation d'une page intérieure en remplacement ; l'une des recommandations de base est d'utiliser une impression offset irisée. 2. Comme ci-dessus, un filigrane unique empêche l'utilisation des pages intérieures ; l'utilisation d'un filigrane à deux tons est une recommandation de base.
Film sécurisé, avec au moins un dispositif de sécurité de niveau 1 très résistant à la contrefaçon	**1**	L'authentification est rapide et facile, et les contrefacteurs ne peuvent pas facilement l'imiter.
Couture **1. Méthode de couture programmable (point noué, avec retour de fil aux extrémités)** **2. Fil de couture fluorescent sous lumière UV**	**1 - 2**	1. Lorsque le livret est réassemblé, un retour de fil à la fin est encore plus difficile à reproduire en utilisant les mêmes trous. Ces derniers peuvent ainsi être agrandis, les rendant faciles à détecter. 2. Un fil de couture fluorescent sous lumière UV est une recommandation de base ; ils sont difficiles à trouver ou à imiter, en particulier des fils complexes (par exemple, rouge sous une lumière UV 365nm).
Numérotation des pages intérieures **1. Perforation laser conique** **2. Perforation laser géométrique**	**1**	1. Lorsque le livret est réassemblé, les pages intérieures ne peuvent pas être parfaitement alignées. Par conséquent, les trous perforés au laser sur les différentes pages intérieures ne seront pas non plus parfaitement alignés, ce qui est assez facilement détectable. 2. Les perforations géométriques au laser (trous de formes différentes) sont plus difficiles à imiter avec des aiguilles chauffées.
Papier fin pour les pages de couverture intérieures	**1**	Le papier fin doit être résistant et durable mais suffisamment fragile pour être partiellement détruit s'il est séparé de la couverture.

Éléments de sécurité liés à la personnalisation

Éléments de sécurité	Niveau	Leur contribution à la prévention de la fraude
Portrait(s) supplémentaire(s) après la page de données	**1-2**	Toute tentative de modification de cette image peut activer des dispositifs de sécurité spécifiques intégrés dans ou sur le papier.
Puce électronique avec photographie authentique protégée par des mécanismes cryptographiques	**2**	Ce portrait numérique authentique est presque impossible à modifier, et un faux portrait (imprimé sur la page de données) peut être détecté. Si la puce est endommagée ou détruite pour tenter de la contourner, cela peut susciter des doutes sur l'intégrité du passeport et la légitimité de son titulaire.
Technologie de personnalisation supplémentaire	**1-2**	La plupart des pages de données papier sont personnalisées avec des méthodes d'impression à jet d'encre ou au laser. L'ajout de certaines données au moyen d'une technologie de personnalisation supplémentaire (par exemple, l'impression invisible par fluorescente sous UV) rendra le remplacement d'une page plus susceptible d'être détecté.

4.2
Falsification (suite)

B. Modification ou remplacement de la photo d'identité (portrait)

Plusieurs techniques peuvent être utilisées pour falsifier une photo d'identité sur la page de données d'un passeport. Vous trouverez ci-dessous les principales techniques observées sur le terrain, ainsi que les contre-mesures de base.

- **Surimpression directe sur le film de sécurité (sans suppression de la photo authentique)**
  Il s'agit d'une falsification assez simple, mais qui peut être très difficile à détecter pour les non-experts. La fausse photo étant ajoutée par-dessus le film, certains éléments optiques protégeant la zone de portrait n'apparaîtront pas authentiques. Cela peut être détecté en regardant le document sous un angle rasant avec une lumière oblique, et en vérifiant si le film repose sur le portrait comme il le devrait. Par conséquent, la qualité des éléments optiques du film sécurisé est essentielle pour détecter de telles attaques.

  En outre, un fond de sécurité bien conçu (à la fois visible et fluorescent aux UV) protégeant la zone de portrait facilitera la détection.

- **Retrait et/ou réutilisation du film**
  Les faussaires procèdent généralement à des attaques chimiques ou physiques dans l'espoir d'ôter le film de sécurité et d'accéder aux données de personnalisation en ne lui infligeant qu'un dégât mineur. Il arrive qu'ils essaient ensuite de réutiliser ce film, qui est la plupart du temps détruit en raison de sa finesse (quelques microns d'épaisseur seulement).

- **Attaque chimique et remplacement (après un accès direct à la photo)**
  Pour les pages de données papier, la recommandation de base est d'utiliser un réactif chimique approprié. Au cas où la photo se trouverait accessible (ce qui est pratiquement impossible avec un film de sécurité fin et bien conçu), les réactifs chimiques rendront l'attaque évidente.

C. Cas supplémentaires non-étudiés dans ce rapport

- **Utilisation d'une page de visa pour falsifier une page de données**
  Bien que ce genre de cas ait été observé par le passé, les pages de données sont aujourd'hui conçues pour être très spécifiques, notamment en ce qui concerne le fond de sécurité imprimé. Il est recommandé que le filigrane ait également un motif spécifique, qui peut être aussi simple que le fait d'orienter différemment l'image centrale (par exemple, des armoiries).

- **Film ou couche transparent(e) avec un faux portrait**
  Cette technique est similaire à celle utilisée pour falsifier des données sur une page en polycarbonate dans le cas de la surimpression directe, un examen attentif des éléments optiques (notamment avec une lumière oblique) permet de détecter plus facilement ce type de tentative de fraude.

- **Abrasion depuis le verso du papier**
  Dans ce cas, le filigrane serait probablement en partie détruit. Les attaques de ce type - et les contre-mesures à prendre - sont examinées plus en détails ci-dessous.

- **Séparation en couches et remplacement partiel avec une fausse page de données (face avant seulement)**
  Ici, les fraudeurs séparent la page de données. Dans ce cas, les contre-mesures classiques sont les plus efficaces : un filigrane avec certaines zones fines (laissant une trace d'effraction lorsqu'elles sont divisées), des fonds de sécurité de haute qualité et des films hautement sécurisés.

- **Remplacement du film par un faux**
  Dans ces attaques, les faussaires tentent d'imiter les véritables films de sécurité grâce aux techniques holographiques disponibles. Cela se traduit parfois par l'utilisation de films holographiques non personnalisés.

  L'utilisation d'un film contrefait n'est généralement qu'une reproduction brute des principaux éléments du motif. Par conséquent, il manque de certains détails et est dépourvu des éléments de sécurité les plus résistants et spécifiques, tels que les reliefs simulés (virtuels), le changement d'image et/ou les permutations entre deux couleurs.

  Les éléments cachés tels que les micro-textes ne sont pas non plus parfaitement reproduits, et peuvent parfois être totalement absents.

4.2.4 Page de données en polycarbonate et page de données électroniques

A. Retrait de la page de données et remplacement par une fausse page de données, une fausse charnière, et un faux fil de couture

Causes

Plusieurs circonstances peuvent expliquer la falsification de pages de données en polycarbonate, notamment en démontant et remontant le passeport sans laisser de traces d'effraction, et/ou en retirant la puce électronique

Éléments de sécurité non liés à la personnalisation

Éléments de sécurité	Niveau	Leur contribution à la prévention de la fraude
Pages de données vierges	-	Veuillez vous référer aux recommandations destinées à limiter la contrefaçon.
Eléments optiquement variables	1-2-3	Un élément optiquement variable hautement sécurisé avec au moins un élément de sécurité de niveau 1 très résistant à la contrefaçon.
Charnières	1-2	Les charnières bien conçues sont difficiles à séparer du corps de la page de données sans laisser de traces de manipulation.
Méthodes de couture et/ou fil de couture	1-2	
1. Méthode de couture programmable (point noué, avec retour de fil aux extrémités)		1. Lorsque le livret est réassemblé, un retour de fil aux extrémités est encore plus difficile à reproduire en utilisant les mêmes trous. Ces derniers peuvent ainsi être agrandis, les rendant faciles à détecter.
2. Fil de couture fluorescent aux UV		2. Un fil de couture fluorescent aux UV est une recommandation de base ; ils sont difficiles à trouver ou à imiter, en particulier les fils complexes (par exemple, rouge sous une lumière UV 365nm).
Numérotation utilisant une perforation laser conique ou géométrique des pages intérieures	1	Lorsque le livret est réassemblé, les pages intérieures ne peuvent pas être parfaitement alignées.
Papier fin pour les pages de couverture intérieures (90gr, par exemple)	1	Ce papier est résistant et durable mais assez fragile pour que le retrait de la couverture l'abîme au moins partiellement.

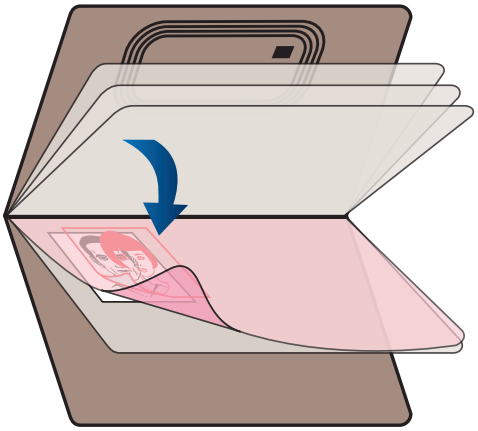
Éléments de sécurité liés à la personnalisation

Éléments de sécurité	Niveau	Leur contribution à la prévention de la fraude
Éléments de sécurité relatifs à la personnalisation de la page de données	-	Plusieurs approches permettent de rendre la falsification de la page plus difficile, comme : » La personnalisation utilisant des structures lenticulaires » Les informations cachées (généralement dans le portrait). » La personnalisation tactile » Une fenêtre avec personnalisation. » La perforation laser.
Portrait supplémentaires imprimées après la page de données	1-2	La photo authentique peut ne pas être modifiée, ou la tentative de modification peut être détectée grâce à des éléments de sécurités spécifiques intégrés dans ou sur le papier.
Puce électronique avec portrait authentique protégé par des mécanismes de cryptographie	2	Ce portrait électronique authentique est presque impossible à modifier, et le comparer au faux portrait (imprimé sur la page de données) permettra de détecter la fraude. Si la puce est rendue non fonctionnelle (elle peut être détruite de manière intentionnelle), le doute est permis quant à l'intégrité du passeport et la légitimité de son titulaire.

4.2
Falsification (suite)

B. Modification des données et/ou de la photo d'identité

La modification des données ou des images se fait généralement par l'application d'un film transparent contenant de fausses informations.



Exemple de film transparent utilisé afin de modifier un portrait

Contre-mesures recommandées

Éléments de sécurité non liés à la personnalisation

Éléments de sécurité	Niveau	Leur contribution à la prévention de la fraude
Fond de sécurité imprimé visible et invisible (fluorescent aux UV) couvrant la zone de portrait	**1-2**	Il peut être moins visible (ou du moins paraître différent) une fois recouvert par la couche transparente, et sera beaucoup moins visibles sous la fausse photo.
Encre optiquement variable près de la zone de portrait	**1**	Peut être moins visible une fois recouverte par la couche transparente.
Hologramme/DOVID par-dessus la zone de portrait, incluant des variations optiques (par exemple mat / brillant)	**1-2-3**	Une fois recouverts par la couche transparente, ils peuvent être moins visibles et les variations optiques peuvent disparaître.
Éléments d'embossage tactiles (gaufrage)	**1**	Peut être moins évident au toucher une fois recouvert par une couche transparente ; peut perturber l'application de la fausse couche.
Éléments de lamination (gaufrage) comprenant des variations optiques (par exemple mat / brillant)	**1**	Les variations optiques peuvent disparaître une fois recouvertes par la couche transparente.

Éléments de sécurité liés à la personnalisation

Éléments de sécurité	Niveau	Leur contribution à la prévention de la fraude
Images laser multiples (MLI) ou images laser changeantes (CLI), éléments tactiles pouvant contenir un portrait supplémentaire	**1**	Peuvent être moins efficaces une fois recouvertes par une couche transparente ; peuvent perturber l'application de la couche transparente ; l'image authentique peut ne pas être modifiée.
Gravure laser tactile de données clés (par exemple le numéro de passeport ou sa date d'expiration)	**1**	Peut être moins évidente à percevoir au toucher une fois recouverte par une couche transparente ; peut empêcher l'application de la couche transparente contrefaite.
Portrait(s) supplémentaire(s) gravé(s) ou perforé(s) au laser dans la structure de la page de données et/ou imprimée(s) sur une page intérieure (papier).	**1-2**	Le portrait authentique peut ne pas être modifié, ou la tentative de modification peut être détectable grâce aux éléments de sécurité spécifiques intégrés dans ou sur le papier (réactifs chimiques, fond de sécurité, informations liées au passeport intégrées dans le portrait authentique).
Technologies de personnalisation sécurisées	**1-2-3**	Certaines nouvelles technologies intègrent des éléments visibles qu'il est difficile d'imiter avec une fausse photo sur un film de sécurité. Ces éléments peuvent être liés à la couleur, à la résolution ou à la combinaison du laser et du gaufrage sur la zone du portrait, par exemple.

4.2
Falsification (suite)

C. Surimpression directe par-dessus la page de données en polycarbonate

La fausse photo étant placée par-dessus la photo authentique, certains éléments optiques n'apparaîtront plus comme ils le devraient.

Grâce à eux, la détection par lumière coaxiale laisse peu de place au doute. Sans accès à un tel outil – ce qui est une réalité pour la majorité du personnel de première ligne - les experts recommandent au personnel chargé du contrôle aux frontières de vérifier la zone de portrait en observant le document de biais. C'est généralement le meilleur moyen de remarquer que le portrait principal n'est pas personnalisé là où il devrait l'être.

Contre-mesures recommandées

éléments de sécurité les plus efficaces contre la surimpression directe sont les fonds de sécurité (surtout visibles) ou des DOVIDs intégrés au-dessus de la zone du portrait (en recouvrant une partie). Ceci est assez complexe à concevoir de manière efficace car les éléments de sécurité ne doivent pas non plus cacher le portrait.

Des portraits supplémentaires contribueront également à faciliter la détection de la fraude, surtout s'ils sont assez grands et protégés contre toute manipulation. La troisième page du livret de passeport (qui suit généralement la page de données) dispose de l'espace nécessaire et est de plus en plus considérée comme une "deuxième" page de données.

D. Abrasion depuis le verso de la page de données

Ce type de falsification concerne généralement les documents synthétiques (en polycarbonate). Le document est poncé depuis le verso afin d'enlever certaines des couches de sécurité et d'accéder à la zone de portrait (la couche personnalisée).

Contre-mesures recommandées

En plus des fonds de sécurité imprimés offset (visibles et invisibles), plusieurs éléments peuvent rendre les tentatives de fraude plus difficiles à effectuer et plus faciles à détecter. Les éléments suivants sont relativement faciles à intégrer dans la conception :

- L'ajout d'éléments de lamination (embossage) tactiles et/ou optiques au verso
- Une encre optiquement variable derrière la zone de portrait (généralement imprimée uniquement sur le recto)
- Des éléments de sécurité sur une couche à l'intérieur de la structure de la page de données.
- Une lentille de type MLI au recto. Si le portrait supplémentaire a lui-aussi été effacé et remplacé, il est peu probable qu'on puisse observer un quelconque mouvement en inclinant le document.
- Une fenêtre transparente avec un portrait supplémentaire. L'attaque de cette image depuis l'envers laisserait des traces d'effraction.
- Des portraits supplémentaires en page 3 ou derrière la principale zone de portrait (au verso). Dans les deux cas, il est nécessaire de prévoir un équipement spécial et un temps de personnalisation plus long.

Il est bien sûr fortement recommandé aux contrôleurs d'inspecter le verso d'une page de données chaque fois que cela est possible.

4.2.5 Passeport biométrique (falsification des puces sans contact)

Désactivation intentionnelle, dommage, ou remplacement de puce

La falsification d'un livret de passeport inclut la modification de détails clés afin que le document corresponde à son nouveau titulaire. Souvent, cela implique de désactiver le microcontrôleur pour empêcher les agents aux frontières de faire correspondre le contenu de la puce avec le document, et donc de repérer des incohérences dans le portrait ou autres données.

Les fraudeurs peuvent parfois ajouter un microcontrôleur avec les données du "nouveau titulaire" signées par une fausse autorité de délivrance. Cette méthode peut s'avérer efficace lorsque les contrôles aux frontières ne vérifient pas le Répertoire de Clés Publiques (RCP) de l'OACI, ou lorsque l'autorité émettrice ne publie pas ses certificats dans le RCP. Cette méthode est la même que celle utilisée pour la contrefaçon complète du livret de passeport (décrite plus haut).

Le précédé de remplacement d'une puce sans contact par une fausse s'appuie sur les faiblesses d'un système susceptible de ne pas vérifier et croiser les éléments de sécurité physiques et les données personnalisées physiquement. Ce type d'attaque était le plus courant dans les années 2010.

Aujourd'hui, des mécanismes de sécurité résistants sont présents dans les puces des passeports. Les faussaires visent rarement à les modifier ou à les remplacer, et préfèrent tenter de les détruire ou désactiver afin de rendre les données personnelles impossibles à vérifier. Là encore, les fraudeurs visent généralement à se faire passer pour le véritable porteur ou à éviter que le portrait sur la puce ne soit vérifié alors qu'un portrait falsifié a été apposé sur la page de données.

Désactiver le microcontrôleur demande de séparer le câblage qui le relie à l'antenne, ou de couper une partie de l'antenne. Cela se fait généralement en retirant les couches de sécurité de la couverture afin d'accéder à l'inlay (dans le cas d'une puce sans contact située dans la couverture), en utilisant un four à micro-ondes, ou même en percutant le microcontrôleur pour le désactiver.

Nous recommandons que les puces qui ne fonctionnent pas soient toujours considérées comme suspectes. Il revient aux agents aux frontières de vérifier que le document ne présente aucun signe de falsification, par exemple aucune entaille sur la couverture (qui laisserait un vide clairement visible en regardant à la lumière). Le passage au four à micro-ondes pourrait laisser des traces de brûlure visibles, un signe de dommage que peuvent rechercher les examinateurs.

Les puces doivent être systématiquement et minutieusement vérifiées lors d'une inspection, et contrôlées avec tous les dispositifs de sécurité possibles.

Il est également fortement recommandé de sécuriser les puces en suivant les directives établies dans le Doc 9303 de l'OACI, en particulier les parties 9, 10 et 11. Il encourage l'utilisation des techniques suivantes :

- **L'Authentification Passive (PA) :** en permettant la vérification des signatures numériques et des certificats de pays, ce mécanisme garantit qu'un passeport a été délivré par un gouvernement légal et n'a pas été manipulé.
- **L'Authentification Active (AA) :** un algorithme crypté vérifie que la puce n'a pas été clonée grâce à un mécanisme de défi/réponse.
- **Le Contrôle d'Accès de Base (BAC) :** empêche le piratage et atténue le risque d'interception de données circulant entre la puce et les systèmes d'inspection en utilisant un canal de communication sécurisé. Ce protocole est toutefois affaibli par l'utilisation des algorithmes SHA-1 et 3DES.
- **Le Contrôle d'Accès Supplémentaire (SAC) :** ce mécanisme est similaire au BAC dans la mesure où il protège les échanges de données entre la puce et le terminal, et permet au terminal d'accéder aux groupes de données qui ne sont pas biométriques. Le SAC est fortement recommandé car il se base sur des mécanismes cryptographiques plus récents et plus résistants que le BAC.
- **Le Contrôle d'Accès Étendu (EAC) :** ce mécanisme permet au terminal d'accéder au groupe de données stockant les données biométriques du titulaire (son empreinte digitale et son scan rétinien). La photo d'identité, parfois considérée comme une donnée biométrique, est stockée dans le groupe de données 2 et ne nécessite que le BAC ou le SAC pour être accessible.

Comme indiqué précédemment, la fraude touchant à la partie électronique du passeport est directement liée à l'âge de ses composants sécurisés. Afin de s'assurer que seuls des documents dignes de confiance sont délivrés, les logiciels intégrés et les puces contenues dans les passeports électroniques sont certifiés conformes aux Critères Communs de sécurité avant leur délivrance.

Il est néanmoins fortement recommandé de mettre en œuvre un processus de surveillance de sécurité qui assure le suivi de la puce pendant toute sa durée de vie et garantit une sécurité efficace.

4.3 Le cas spécifique du morphose

Le morphose représente une menace très sérieuse pour la sécurité des pièces d'identité, un élément clé de la sécurité nationale et internationale. En mélangeant les traits du visage de deux personnes, les fraudeurs sont en mesure de produire une photo combinée qui pourrait potentiellement tromper des agents hautement qualifiés et des systèmes de reconnaissance faciale sophistiqués.

Des études ont prouvé que les agents formés ainsi que les machines ont du mal à détecter les photos modifiées avec un niveau de confiance élevé. Celles-ci risquent donc de ne pas être détectées lors de la procédure de demande de documents d'identité, ce qui se traduit par des passeports et des cartes d'identité authentiques obtenus frauduleusement (Fraudulently Obtained but Genuine, FOG, en anglais) que deux personnes pourraient utiliser pour faire des demandes frauduleuses de services et prestations, ou pour voyager dans le monde entier.

En outre, de nombreuses mesures actuellement utilisées pour protéger les photos d'identité contre le morphing sont insuffisantes, ce qui constitue une source de préoccupation majeure pour les autorités chargées de la délivrance de documents d'identité. Afin de lutter contre cette menace permanente et en constante évolution, les gouvernements doivent rester agiles et ouverts à des mesures de prévention, de protection et de détection qui soient nouvelles et innovantes.

La meilleure façon de se protéger de manière fiable contre le morphing est d'adopter une approche à trois volets : empêcher la délivrance de documents authentiques obtenus frauduleusement, protéger les photos d'identité contre toute manipulation et détecter les discordances entre les images réelles et les photos d'identité modifiées à l'aide des meilleurs algorithmes biométriques disponibles.

La première étape consiste à interdire l'utilisation de photos imprimées, pour plutôt prendre le contrôle de la prise de photos et empêcher les photos modifiées de s'infiltrer dans les demandes de documents d'identité. Ensuite, pour protéger les photos des cartes d'identité existantes contre de potentielles attaques par morphing, il est essentiel d'utiliser les techniques les plus avancées afin de les sécuriser.

Enfin, pour appuyer ces solutions et renforcer la sécurité nationale et internationale, les gouvernements doivent également déployer des systèmes biométriques de pointe sur les lieux de contrôle de sécurité et d'identification. À mesure que les algorithmes biométriques évoluent, ces systèmes aideront de plus en plus les agents frontaliers, les forces policières ainsi que les autres autorités à mettre la main sur les fraudeurs, criminels et terroristes avant qu'ils ne puissent mettre leurs plans à exécution.

En résumé, la meilleure défense contre les attaques par morphing consiste à combiner les solutions suivantes :

- Bannir les photos imprimées, et prendre des photos sur place, directement ou par l'intermédiaire de photographes et de cabines contrôlés et connectés.
- Protéger les photos contenues dans les documents d'identité en mettant en place des dispositifs de sécurité résistants à la fraude.
- Déployer des systèmes de reconnaissance biométrique de pointe sur les lieux de contrôle d'identité.

5. Divers facteurs de terrain à prendre en compte

La fraude est en constante évolution, et les autorités de délivrance se doivent de suivre de près les dynamiques changeantes qui la façonnent. Nous examinerons ci-dessous quelques-unes des questions clés qui risquent d'influencer l'avenir de la fraude documentaire.

Les facteurs favorisant la fraude

- **La professionnalisation (les capacités grandissantes des fraudeurs et leur accès aux technologies)**
  Les impressions à jet d'encre et par sublimation ont été largement maîtrisées et sont désormais régulièrement utilisées pour la contrefaçon de documents. L'impression offset et la gravure laser peuvent également être utilisées, généralement par des faussaires "professionnels" qui participent probablement aussi à la production de faux billets de banque.

- **Accès à des matériaux sécurisés standard ou sophistiqués**
  Les rapports de fraude documentaire ont commencé à mentionner certaines encres ou papiers de sécurité d'entrée de gamme, ainsi que de faux films de sécurité holographiques (créés principalement par la technologie dot matrix).

- **Accès à des informations confidentielles.**
  Chaque personne impliquée dans la chaîne de sécurité a son rôle à jouer afin d'assurer la sécurité des informations dans les zones à accès restreint, en tenant compte du niveau d'information nécessaire au destinataire avant de partager quoi que ce soit. Tous les membres de la SIA sensibilisent leurs organisations à l'importance de la gestion des informations confidentielles. Ils sont régis par les cadres de certification les plus élevés en matière de sécurité, tant pour les sites de production que pour les technologies de l'information utilisées. Ces certifications sont reconnues par les États membres de l'Union européenne.

- **Documents à faible niveau de sécurité**
  L'objectif de ce rapport est de souligner l'importance de la sécurité des documents, en se concentrant sur les principaux risques identifiés.

- **Accès aux équipements et produits sur le Dark Web et l'Internet public**
  On peut même y trouver des documents "finis" en vente.

Les Facteurs diminuant les chances de détecter la fraude

- **Trop d'éléments de sécurité**
  Certains experts ont comparé les passeports trop compliqués à un sapin de Noël surchargé ; ils peuvent paraître impressionnants, mais sont aussi totalement impraticables. Trop de vérifications à effectuer peut s'avérer contre-intuitif.

- **Temps limité pour précéder aux vérifications en première ligne**
  C'est la principale raison pour laquelle les experts en matière d'examen de documents réclament des éléments de sécurité qui peuvent être authentifiés intuitivement en quelques secondes et sans outils.

- **Trop peu d'outils permettant de faciliter les contrôles (limitant donc la possibilité de procéder à des vérifications dans le détail)**
  Le personnel de première ligne ne devrait pas avoir à être découragé par un manque de technologie. Même les smartphones, qui permettent de zoomer, d'agrandir, d'éclairer et de scanner des puces sans contact, pourraient servir d'outil de contrôle supplémentaire, par exemple.

- **Manque de connaissances et de formation des contrôleurs quant à la vérification des documents.**
  En général, les documents frauduleux présentent quelques similitudes entre eux. C'est pourquoi certains organismes policiers diffusent des alertes mettant en évidence certains éléments clés permettant la détection de la fraude. Même quelques sessions de formation de base peuvent donner la confiance nécessaire aux contrôleurs afin de détecter la majorité des tentatives de falsification.

- **De faibles niveaux de standardisation (certains documents spécifiques nécessitent des contrôles différents)**
  Les recommandations de l'OACI proposent l'introduction de normes permettant d'accroître l'interopérabilité et de faciliter les voyages. Des initiatives localisées permettent également une standardisation supplémentaire de documents qui sont similaires (par exemple, les règlements de l'UE concernant des documents comme le titre de séjour). Cela reste cependant assez disjoint, notamment dans le cas des passeports.

6. Recommandations générales et mesures supplémentaires

Outre les mesures de sécurité spécifiques aux composants et aux techniques décrites dans le chapitre précédent, les bonnes pratiques générales relatives à la prévention de la fraude jouent un rôle essentiel dans la sécurité des documents.

Nous présenterons ci-dessous quelques recommandations générales et mesures supplémentaires qui devraient être prises en compte par les fabricants de documents lors de la conception de nouveaux livrets de passeport. (NB : les points ne sont pas classés par ordre d'importance).

- Ne vous fiez pas à un élément de sécurité seul. Les passeports modernes offrent de nombreuses techniques de validation différentes, et celles-ci sont plus efficaces lorsqu'elles sont utilisées en se combinant les unes avec les autres. Comme l'OACI l'indique clairement dans le Doc 9303 (Partie 2), « certains éléments peuvent offrir une protection contre plusieurs types de menace, mais il n'en existe aucun qui puisse, à lui seul, protéger contre tous ces types de menaces. De même, aucun élément de sécurité n'est efficace à 100 % pour éliminer une catégorie quelconque de menace."
- Utilisez les matériaux, les techniques d'impression et de fabrication, et le personnel les plus sûrs possibles, dans le respect de votre budget. Veillez à ce qu'il y ait un équilibre entre tous les facteurs concernés.
- La meilleure protection vient d'une combinaison de plusieurs éléments de sécurité. La clé est de trouver un équilibre entre la protection et la lisibilité des pages de données, en particulier. De nombreuses options doivent être envisagées ici, notamment les combinaisons suivantes :
  - » Impressions offset (irisées), repères visibles et invisibles, imprimés en registre.
  - » Impression en taille-douce avec une encre optiquement variable (par exemple pour la face interne de couverture en début de livret).
  - » Filigranes, qui sont plus faciles à contrôler si chaque page intérieure comporte une zone vierge d'impression (une sorte de fenêtre), comme c'est le cas sur les billets de banque.
  - » Films de sécurité (sur les pages de données en papier) ou surfaces laminées (avec embossage) intégrant plusieurs éléments de sécurité (pour les pages de données en polycarbonate).
  - » Gaufrage lié à une couleur optiquement variable
- S'il est conseillé de combiner plusieurs éléments de sécurité, un trop grand nombre peut rendre la vérification peu intuitive. L'équilibre et le bon sens sont essentiels. Sur le terrain, seuls quelques éléments de sécurité (quatre ou cinq selon certains experts) sont nécessaires pour vérifier l'authenticité du livret de passeport et l'intégrité du portrait principal.
- Tirez le meilleur parti de chaque élément de sécurité en optimisant la manière dont il est intégré dans la conception globale du passeport. Les éléments tactiles doivent être intégrés là où les doigts vont naturellement tenir ou prendre le document, par exemple. C'est un domaine dans lequel l'expérience du fabricant de documents peut s'avérer très utile, tout comme une collaboration étroite entre les experts en vérification de documents et les fabricants de passeports.
- En général, en ce qui concerne la répartition des éléments entre les trois niveaux de sécurité, il est recommandé de procéder comme suit :
  - » Les autorités de délivrance doivent se concentrer sur les éléments de sécurité de niveau 1, car ils représentent plus de 90% des contrôles effectués en première ligne. Seuls quelques-uns sont susceptibles d'être vérifiés, ils doivent donc être suffisamment résistants et intuitifs pour permettre un examen superficiel par quiconque sait quoi chercher. Les examinateurs hautement qualifiés et bien équipés sont une minorité, et les spécialistes en analyse documentaire appartiennent à un groupe qualifié encore plus réduit.
  - » Intégrer quelques fonctionnalités de niveau 2 telles que les micro-textes et l'impression irisée UV. Celles-ci doivent être conçues pour apporter confiance et facilité aux inspections de deuxième ligne.
  - » Utilisez les éléments de sécurité de niveau trois avec parcimonie ; un ou deux suffisent généralement. Ils ne seront utilisés que dans des cas très particuliers et nécessitent des outils spécifiques pour les vérifier. Pour déclencher leur inspection, il faudrait avoir un doute important sur l'authenticité du document, ou besoin d'apporter une preuve incontestable de contrefaçon ou de falsification devant une autorité judiciaire. Faites en sorte qu'ils restent hautement confidentiels.

6
Recommandations générales et mesures supplémentaires (suite)

- La répartition des éléments sur le livret nécessite d'établir des priorités. Il est fortement recommandé aux autorités de délivrance de protéger avant tout la page de données, la zone de portrait principal et les portraits supplémentaires. Certaines données clés devraient également être dupliquées et intégrées à l'aide d'éléments spéciaux (par exemple, le numéro du document ou la date d'expiration présentés de manière personnalisée en page trois, dans une lentille MLI et/ou avec une gravure laser tactile).
- Certains éléments de sécurité permettent d'intégrer plusieurs niveaux de sécurité en même temps, et nombre d'entre eux permettent aux autorités de lutter à la fois contre la contrefaçon et la falsification. Les éléments doivent être sélectionnés de manière à permettre un large éventail de moyens de protection. Cela facilite leur intégration tout en limitant le nombre d'éléments à vérifier.
- Les documents doivent être conçus pour être contrôlés à la fois par les humains et par les machines qui les assistent. Certains éléments de sécurité sont hybrides et peuvent être contrôlés à la fois par des humains et des machines, généralement en comparant un document donné à un modèle sous lumière VIS/UV/IR (les fonds imprimés fluorescents UV et IR font partie du champ d'application).
- L'intégration des mêmes éléments et composants de sécurité principaux dans les passeports ordinaires et autres documents de voyage au format ID-3 (par exemple, les passeports diplomatiques ou de service) facilite la vie des contrôleurs. Moins de spécificités à gérer leur demanderont moins de formation, et les agents seront ainsi en mesure d'effectuer des contrôles plus rapides et plus fiables. Un certain niveau d'homogénéité pour les éléments de sécurité dès la conception permet également aux fabricants de documents de proposer de meilleurs prix et délais de livraison tout en maintenant la barre suffisamment haute pour dissuader les contrefacteurs . À titre d'exemple, bien qu'un passeport diplomatique de 48 pages (au lieu des 32 que l'on trouve dans un passeport "ordinaire") puisse être utile, si celui-ci exige également un filigrane électrotype avec numérotation des pages, alors il faudra produire deux versions d'un papier de sécurité personnalisé (32 + 48 pages intérieures). Cela peut représenter un surcoût important. Certaines exceptions ont toutefois un sens, comme les passeports d'urgence, qui peuvent ne pas présenter tous les éléments de sécurité d'un passeport standard.
- En ce qui concerne la numérotation unique de passeports vierges :
  - » Les livrets de passeport vierges ne doivent jamais quitter le site de production sans un numéro unique.
  - » Les éléments de sécurité doivent être appliqués après la personnalisation. À défaut, la personnalisation doit être un processus complexe utilisant des éléments de sécurité qui nécessitent un équipement spécialisé de niche.
  - » Utilisez une puce dans le document et vérifiez ses données.
  - » Gardez le contrôle du processus de demande de document et sa délivrance.
  - » Stockez les documents de manière sécurisée et appliquez les mesures appropriées ainsi que le principe des « quatre yeux » pour accéder aux documents vierges.
  - » Connectez-vous aux bases de données MIND/FIND et SLTD d'INTERPOL, et signalez les numéros de tout document volé afin d'invalider immédiatement leur utilisation lors des voyages internationaux.

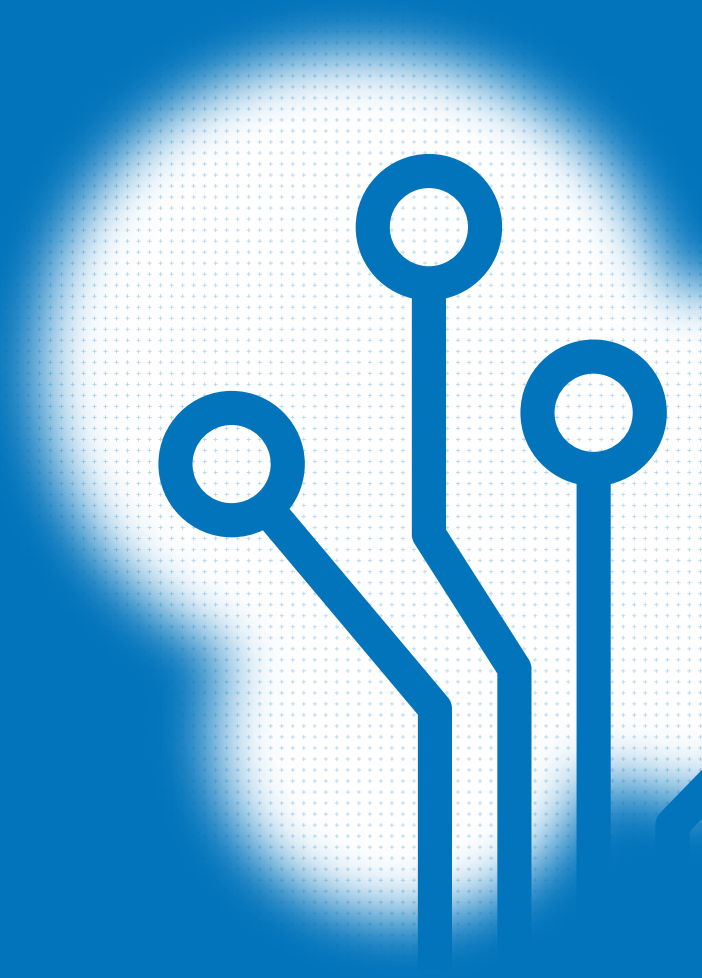
7. Conclusion

Le monde de la fraude documentaire est de plus en plus complexe et il convient d'adopter une vision d'ensemble pour en comprendre les rouages. Le succès des contrôles dépend désormais d'une variété de facteurs en évolution rapide, allant des méthodes d'exploitation des fraudeurs à une technologie nouvelle et parfois très complexe.

Ce document a été conçu pour aider les lecteurs à mieux comprendre ces facteurs, ainsi que pour leur rappeler les enjeux liés à la fraude documentaire. Quand les fraudeurs gagnent, nous sommes tous perdants.

Les recommandations formulées ici sont tirées de sources et d'experts en sécurité de documents parmi les plus réputés au monde, et nous encourageons toute personne impliquée dans la délivrance, le contrôle ou la conception de livrets de passeport et autres formes d'identification à tenir compte de leurs conseils. Comme nous l'avons vu plus haut, le nombre d'éléments de sécurité importe moins que l'art de la conception sécurisée dans son ensemble. Une quantité moindre peut être la clé du succès lorsqu'elle est appliquée efficacement.

Un outil qui peut s'avérer utile pour évaluer l'efficacité des éléments de sécurité inclus dans vos propres documents est le « eSecurity Evaluation Model » (eSEC) de la SIA. Lancé pour la première fois en 2017, eSEC fournit aux organisations un moyen de mieux évaluer comment les éléments de sécurité, tels que les pages de données et les photos, devraient être répartis entre les différentes sections d'un livret de passeport. Une version actualisée et optimisée d'eSEC est prévue pour 2022.



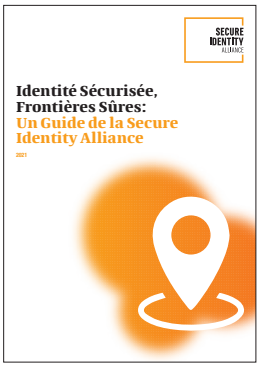
Les autres rapports de la Secure Identity Alliance:

https://secureidentityalliance.org/ressources/publications

(Disponibles aussi en anglais)

L'Expression des Identités Numériques dans le Monde

Offrant des perspectives et des retours de terrain sans précédent, l'étude réalisée en partenariat avec onepoint donne une voix unique aux parties prenantes de 25 systèmes d'identification numérique souverains innovants. Leurs apprentissages partagés mettent en évidence les principes directeurs et les bonnes pratiques qui sont essentiels pour favoriser l'utilisation, l'adoption et le succès, quel que soit le modèle d'identification numérique adopté.



Identité Sécurisée, Frontières Sûres

Explorant les principaux facteurs qui façonneront l'avenir du contrôle aux frontières, illustré par de nombreux exemples de réussites et d'enseignements tirés de l'expérience terrain d'agences du monde entier, ce rapport examine la nécessité d'équilibrer sécurité et protection avec des expériences passagers efficaces et sans friction.

Il examine aussi le rôle vital - et complexe - joué par la gestion de l'identité, en soulignant certaines des technologies évolutives, notamment l'automatisation et intelligence artificielle, la biométrie et le mobile.

La biométrie dans l'identité: Construire un avenir inclusif et protéger les libertés civiles

Ce rapport vise à aider les décideurs politiques lors de la planification et de la mise en œuvre de programmes d'identité biométriques et des services associés. Adoptant une vision holistique du paysage biométrique sophistiqué d'aujourd'hui, il identifie les principaux problèmes et moteurs de l'identité biométrique, donne un aperçu des projets actuels et à venir en Europe et au-delà, et présente un ensemble de bonnes pratiques et de recommandations communes pour soutenir les politiques qui souhaiteraient tirer parti de l'identité biométrique pour stimuler et accélérer l'économie numérique à travers le monde.

SECURE IDENTITY ALLIANCE