Guide pour l’évaluation de la sécurité du traitement et de la délivrance des documents de voyage

Version 3.4 — septembre 2010

Sommaire

L'intégrité des passeports et autres documents de voyage est une composante clé des stratégies nationales et internationales de lutte contre la criminalité et le terrorisme. Étant donné qu'ils peuvent représenter de puissants outils dans les mains de criminels ou de terroristes, le contrôle de la sécurité des documents de voyage d'un pays et de leur processus de délivrance a des répercussions directes non seulement sur la sécurité nationale et internationale, mais également sur le respect international accordé à l'intégrité de ces documents.

Au cours des dernières années, le développement rapide de nouvelles technologies et de nouvelles techniques de sécurité a conduit à un déplacement de la fraude des documents de voyage. Les fraudeurs avaient l'habitude de concentrer leurs efforts en aval de la chaîne de production des documents de voyage. Aujourd'hui, ils sont à l'œuvre en amont de la chaîne de production, c'est-à-dire au niveau des systèmes de délivrance des documents et au niveau du registre des documents. Les pays doivent donc prêter une attention particulière à la sécurité du processus de traitement et de délivrance des documents de voyage pour éviter que des criminels ou des terroristes n'obtiennent des documents légitimes en recourant à de fausses identités.

À la 17e réunion du Groupe consultatif technique sur les documents de voyage lisibles à la machine (TAG/MRTD) de l'OACI, un projet a été approuvé relativement à la production d'un outil courant et pratique qui aiderait les pays membres de l'OACI, soit à évaluer eux-mêmes la sécurité de leur système de traitement et de délivrance de documents de voyage, soit à évaluer la sécurité du système de traitement et de délivrance d'un autre pays.

Le présent Guide est composé de deux parties :

1) la première partie recommande des pratiques exemplaires visant à prévenir ou à atténuer toute menace à chacune des étapes du processus de délivrance des passeports;
2) la seconde partie est un outil d'évaluation sous forme d'une liste de contrôle exhaustive permettant d'évaluer les vulnérabilités du processus de délivrance.

Les mesures et les pratiques mentionnées dans le présent document sont des pratiques recommandées et, en ce sens, aucun pays n'est tenu de les adopter en tout ou en partie.

Le présent Guide a été élaboré et sera entretenu par le Groupe de travail sur la mise en œuvre et le renforcement des capacités (ICBWG) de l'Organisation de l'aviation civile internationale (OACI). Les questions, commentaires et rétroactions doivent être acheminés au groupe de travail à ICBWG@icao.int.

Registre des modifications du document

Version	Date de parution	Brève description du ou des changements
1.1	7 janvier 2008	1ère version
1.2	18 janvier 2008	Modifications apportées à la structure (transmises au Groupe de travail des nouvelles technologies)
1.3	10 avril 2008	Version produite après les discussions de Christchurch et transmises au Groupe consultatif technique (TAG)
1.4	15 mai 2008	Mise à jour après la 18e réunion du TAG/MRTD
2.0	30 septembre 2008	Intégration des commentaires et modifications apportées à la structure (transmises au Groupe de travail sur la mise en œuvre et le renforcement des capacités — IBCWG))
3.0	10 mars 2009	Élaboration de la seconde partie — listes de vérification Révision et ajout de texte dans tous les chapitres de la Partie 1 Harmonisation des Parties 1 et 2
3.1	29 juin 2009	Modifications sur le plan de la forme
3.2	12 août 2009	Commentaires post-Tavira et La Haye
3.3	octobre 2009	Observations finales de l'ICBWG lors de la réunion au Cap-Vert
3.4	Janvier 2010	TAG/MRTD Commentaires d'Australie
3.4	Septembre 2010	Modification a la traduction d'une phrase

Table des matières

Introduction

A) Rôle des documents de voyage dans la sécurité nationale et internationale

Les passeports et autres documents de voyage sont des documents officiels, reconnus à l'échelle internationale, qui attestent l'identité et la citoyenneté d'une personne pour lui permettre de se rendre à l'étranger. Ils sont utilisés par les autorités frontalières et les autorités de l'immigration afin d'établir l'admissibilité et la légitimité des voyageurs qui souhaitent traverser des frontières internationales pour entrer dans le territoire d'un autre pays. Ces documents sont aussi utilisés par les pays de délivrance pour permettre aux voyageurs de revenir chez eux. Les titulaires d'un passeport peuvent demander un visa aux pays qui l'exigent pour être admis sur leur territoire. Les autorités frontalières des pays annotent les passeports des voyageurs et y inscrivent les dates d'entrée sur leur territoire et de sortie.

En plus d'être des documents de voyage, les passeports sont aussi des documents d'identité de plus en plus utilisés pour d'autres types de transactions avec les secteurs public et privé; par exemple pour ouvrir un compte bancaire, effectuer des transactions financières ou avoir accès à des prestations et des services gouvernementaux.

Les documents de voyage, obtenus en bonne et due forme ou non, falsifiés ou contrefaits, sont des outils de prédilection pour les groupes de criminels et de terroristes. Dans des mains criminelles, les documents de voyage peuvent être mal utilisés de manière organisée pour financer leurs activités, faciliter la migration illégale, le passage de clandestins, le trafic de personnes, de biens ou de drogues. Les passeports frauduleux peuvent servir à des fins d'espionnage ou de criminalité financière, ou encore permettre à des individus de s'enfuir d'un pays pour éviter des poursuites judiciaires ou commettre d'autres crimes. De tels documents peuvent aussi permettre à des terroristes de voyager, de faire du recrutement, d'établir des réseaux, de mobiliser des individus, de se financer et de s'organiser au plan international. S'ils ne peuvent pas voyager librement en utilisant des documents de voyage, les terroristes risquent davantage d'être repérés et, par conséquent, de voir leurs activités entravées, leurs finances minimisées ou même « mises en quarantaine », entraînant une diminution de leur portée et de leur capacité d'agir. En fait, un passeport ou un autre document de voyage peut être la mesure de sécurité qui empêche des terroristes d'atteindre leur but ultime.

Les criminels et leurs organisations sont prêts à verser d'importantes sommes d'argent pour obtenir illégalement des documents de voyage et avoir accès aux renseignements personnels qui sont recueillis, traités et stockés au cours du processus de délivrance des documents. Autrement dit, l'intégrité des documents de voyage et leur processus de délivrance peuvent être extrêmement vulnérables à la fraude, à la manipulation et à la commission d'actes illicites.

En raison du rythme accéléré des progrès technologiques récents, les documents de voyage deviennent de plus en plus sûrs, ce qui amène les fraudeurs à changer leur façon de faire : au lieu de contrefaire ou de modifier des passeports, ils cherchent maintenant à obtenir des documents de voyage authentiques en recourant à d'autres moyens illégaux. Il est généralement admis que les systèmes de délivrance des documents de voyage seront ciblés, comme tous les types de documents de base ou de registres authentiques (p. ex. registre de naissance). Par conséquent, les autorités de délivrance de documents de voyage (ADDV), de même que les organisations concernées par la production de documents de voyage devraient prêter davantage attention à la sécurité du processus de traitement et de délivrance. Un pays peut bien délivrer des passeports hautement sûrs, il n'empêche que, si l'identité d'une personne ne peut pas être établie au-delà de tout doute raisonnable, ou si un document valide est délivré à une personne non autorisée à en être le titulaire, alors la qualité des passeports importe peu.

Les menaces dirigées contre le processus de délivrance des documents de voyage peuvent être regroupées en plusieurs types principaux :

- le vol de documents vierges ou non personnalisés utilisés pour produire un document de voyage frauduleux, y compris l'accès non autorisé aux installations de production et de délivrance des documents ou aux systèmes de traitement des documents;

- la présentation d'une demande de document de voyage sous le couvert d'une fausse identité et d'un document de base falsifié ou d'un document de base authentique, mais volé;
- la présentation d'une demande d'un document de voyage en utilisant une fausse identité et une fausse preuve de nationalité ou d'identité;
- la demande de plusieurs documents de voyage permettant à un voyageur de ne pas déclarer un ou des voyages antérieurs suspects et d'obtenir des visas et des timbres d'entrée et de départ délivrés par des autorités frontalières;
- l'utilisation de documents de voyage non déclarés perdus ou volés ou faussement déclarés perdus ou volés;
- les méfaits commis par des employés;
- la demande d'un document de voyage dans l'intention de le donner ou de le vendre à un individu non autorisé à en être le titulaire et qui ressemble au véritable titulaire.

Le contrôle de la sécurité du processus de délivrance des passeports d'un pays a des répercussions directes non seulement sur la sécurité nationale et internationale, mais également sur le respect international accordé à l'intégrité de ces documents. L'intégrité des documents est particulièrement importante, quand ils sont présentés par des citoyens qui souhaitent obtenir des visas et franchir des frontières, et elle peut influer sur les exigences en matière d'entrée d'autres pays. De fait, le niveau de sécurité et la réputation des passeports délivrés par un pays influent considérablement sur la facilité ou la difficulté avec laquelle les citoyens de ce pays peuvent passer des frontières. L'intégrité des passeports et autres documents de voyage est une composante clé des stratégies nationales et internationales de lutte contre la criminalité et le terrorisme.

Bien qu'il soit reconnu que la sécurité des passeports est nécessaire à la sécurité aussi bien nationale qu'internationale, il faut admettre du même souffle que les autorités de délivrance sont confrontées à l'immense défi de trouver le juste équilibre entre la sécurité, les services, le respect de la vie privée et les coûts. Toutefois, il est incontestablement plus efficace et beaucoup moins coûteux de prévenir la fraude que de prendre des mesures à l'égard d'une fraude réussie.

Aucun pays n'est immunisé contre la fraude. Bien qu'il soit impossible d'éliminer entièrement les vulnérabilités d'un système de délivrance des documents de voyage et toutes les menaces auxquelles il peut être exposé, une combinaison de fonctions et de méthodes peut atténuer les risques en les ramenant à un niveau acceptable et dissuader suffisamment des intérêts criminels potentiels. Le présent Guide fournit aux organisations concernées par le processus de délivrance de documents de voyage de l'information sur les pratiques exemplaires de sécurité, ainsi qu'un outil d'auto-évaluation permettant de mesurer la performance d'un processus de délivrance de passeports sur le plan de la sécurité.

B) Organisation de l'aviation civile internationale (OACI)

La *Convention relative à l'aviation civile internationale* de 1944 a établi les fondements de l'Organisation de l'aviation civile internationale (OACI). Depuis longtemps, l'OACI joue un rôle majeur en établissant les normes, les pratiques recommandées et les spécifications relatives à la délivrance des documents ou titres de voyage. La section 3 de l'Annexe 9 [Facilitation] de la *Convention relative à l'aviation civile internationale* contient des normes et des pratiques recommandées relativement à la délivrance des passeports et autres documents de voyage.

En 1984, le secrétaire général de l'OACI a créé le Groupe consultatif technique sur les documents de voyage lisibles à la machine (TAG/MRTD), composé d'experts de divers États membres de l'OACI. Le TAG/MRTD élabore et adopte des spécifications relatives aux documents de voyage lisibles à la machine (DVLM) et aux documents de voyage électroniques lisibles à la machine (DVEVM), qui sont comprises dans le *Document 9303*. Le TAG/MRTD publie également des principes directeurs pour aider les États membres de l'OACI à mettre en œuvre ses spécifications, de même que des rapports techniques et des documents d'information. Sous la gouverne du TAG/MRTD, deux groupes de travail ont été créés : le Groupe de travail des nouvelles technologies (NTWG) et le Groupe de travail sur la mise en œuvre et le renforcement des capacités (ICBWG).

Lors de la 17e réunion du TAG/MRTD, en mars 2007, une proposition visant à élaborer un *Guide des normes de sécurité relatives au traitement et à la délivrance des documents de voyage* a été présentée et approuvée.

Ressources Web :

- ⇒ Programme des DVLM de l'OACI (anglais) : http://www2.icao.int/en/MRTD/Pages/default.aspx
- ⇒ Document 9303 (ce document doit être commandé auprès de l'OACI) : http://icaodsu.openface.ca/mainpage.ch2

C) But du Guide

L'importance de la sécurisation du processus de délivrance des documents de voyage est bien comprise. Toutefois, les lignes directrices sur les mesures de prévention et d'atténuation recommandées demeurent limitées. Notre système de délivrance est-il sûr? Quelles sont les mesures de sécurité les plus efficaces et les plus efficientes? Par où devrions-nous commencer? Voilà autant de questions que les pays et les organisations concernées par la délivrance des documents peuvent se poser. Le but du présent Guide est donc de fournir des références à la fois simples et détaillées sur la sécurité. Il présente des pratiques exemplaires visant à prévenir ou atténuer toute menace à chaque étape du processus de délivrance des documents de voyage, ainsi qu'un outil d'autoévaluation qui aide les organisations à établir leur degré de vulnérabilité.

Le présent guide a été rédigé dans la perspective de la délivrance des passeports dans les pays où il n'existe pas de carte d'identité nationale ou d'autres systèmes d'enregistrement universel de l'identité au niveau national. Dans les pays où les systèmes d'enregistrement des actes d'état civil comprennent un régime d'inscription universelle et/ou de cartes d'identité, la délivrance des passeports peut être gérée comme un processus rationalisé qui s'appuie sur l'intégrité de l'inscription antérieure pour l'obtention de la carte d'identité nationale. Dans ces situations, les contrôles décrits dans ce guide aux fins de la gestion de la délivrance des passeports demeurent essentiels, mais ils sont exercés avant la présentation d'une demande de passeport, dans le cadre d'un processus d'enregistrement des actes d'état civil distinct. Le contenu du guide demeure donc pertinent pour tous les systèmes de délivrance de passeports, bien que les sections relatives à l'enregistrement et à la vérification de l'identité puissent devoir être interprétées comme s'appliquant aussi bien à l'enregistrement des actes d'état civil qu'à la délivrance des passeports.

Bien que le Guide puisse être utilisé par les États pour évaluer la sécurité du traitement et de la délivrance de leurs documents de voyage et pour apporter des améliorations là où des faiblesses sont observées, l'ICBWG de l'OACI recommande vivement qu'on fasse appel à des évaluateurs qualifiés. L'ICBWG peut recommander des évaluateurs familiers avec le guide et qui ont de l'expérience dans tous les aspects pertinents du continuum des documents de voyage. Les évaluateurs effectuent une analyse interne objective et complète du processus de délivrance du document de voyage d'un État et rédigent un rapport confidentiel au gouvernement ayant fait la demande. La participation des évaluateurs qualifiés est essentielle lorsque l'État prévoit utiliser le rapport pour obtenir de l'aide au renforcement des capacités.

Diverses organisations nationales et internationales dans le monde se sont livrées à des activités de communication et de renforcement des capacités afin d'améliorer la sécurité des documents de voyage et de leur processus de délivrance. Le présent Guide reconnaît le travail de ces organisations et prend la mesure de leurs activités et de leurs réalisations. Sous les auspices du Sous-groupe d'experts sur la migration du G8, un document intitulé *Minimum Security Standards for the handling of MRTDs and other passports* (Normes de sécurité minimales pour le traitement des DVLM et autres passeports) a été produit, puis adopté en tant qu'Annexe III de la Section 3 du *Document 9303*. Ce document important, qui porte principalement sur la fraude à l'interne, sert de fondement au présent Guide.

Public cible

Le présent Guide vise les objectifs suivants :

- aider les décideurs des organisations qui délivrent des documents de voyage ou qui participent à la production de ces documents à évaluer leur propre situation;
- appuyer le Groupe de travail sur la mise en œuvre et le renforcement des capacités (IBCWG) de l'OACI ainsi que d'autres organisations internationales dans leurs activités de sensibilisation, de renforcement des capacités et de vérification;
- aider les gouvernements à évaluer d'autres États membres de l'OACI (p. ex. des États dont l'admissibilité à une mesure de dispense de visas est à l'étude).

Portée

Le présent Guide fournit des pratiques exemplaires et des recommandations relatives au processus de délivrance de passeports et d'autres documents de voyage. Ces pratiques s'appliquent à la fois aux gouvernements et aux organisations non gouvernementales concernées par toutes les étapes du processus de délivrance des passeports.

Les mesures et les pratiques présentées dans le document sont des pratiques recommandées et, en ce sens, aucun pays n'est tenu de les adopter. Il revient à chaque pays d'établir ses propres cadres juridique, administratif et stratégique. De même, tout pays peut adopter les coutumes culturelles, les traditions et les pratiques qui lui conviennent.

Le Guide est axé principalement sur la première étape du cycle de vie des passeports, à savoir le processus de délivrance des passeports, qui comprend les étapes suivantes :

- la réception d'une demande;
- le processus de prise de décisions et le processus administratif visant à établir l'identité, la citoyenneté et les restrictions relatives aux déplacements d'un individu;
- la production;
- la remise d'un document.

Il convient de noter que les mesures prises pour améliorer la sécurité du processus de délivrance peuvent avoir des répercussions directes ou indirectes sur les autres étapes du cycle de vie des passeports telles que l'authentification, la validation et la répudiation.

Structure

La Partie 1 — Pratiques exemplaires en matière de délivrance sûre des documents de voyage — recommande des pratiques exemplaires à chacune des étapes du processus de délivrance des passeports. La Partie 1 est divisée en 12 chapitres.

La Partie 2 — Guide d'évaluation — fournit un outil d'évaluation détaillé permettant d'évaluer les vulnérabilités du processus de délivrance. Il se trouve à la suite des recommandations et des organisations membres de la Partie 1.

Guide pour l'évaluation de la sécurité relative au traitement et à la délivrance des documents de voyage

PARTIE 1 : PRATIQUES EXEMPLAIRES EN MATIÈRE DE DÉLIVRANCE SÛRE DES DOCUMENTS DE VOYAGE

1. Autorité de délivrance des documents de voyage — Structure organisationnelle, sécurité interne et pratiques générales de sécurité
2. Processus de demande
3. Processus de détermination de l'admissibilité
4. Traitement des documents et des livrets vierges
5. Personnalisation et remise
6. Sécurité des documents
7. Sécurité des installations
8. Sécurité de la technologie de l'information
9. Intégrité interne et du personnel
10. Documents de voyage perdus et volés
11. Délivrance de documents de voyage à l'étranger
12. Intervenants nationaux et internationaux

1 Autorité de délivrance des documents de voyage — Structure organisationnelle, sécurité intérieure et pratiques générales de sécurité

1.1 Sommaire

En général, les autorités de délivrance de documents de voyage (ADDV) supervisent la réception et le traitement des demandes, l'établissement de l'admissibilité des requérants, ainsi que la production et la délivrance des documents de voyage.

Alors que chaque chapitre du présent Guide couvre un aspect, une étape ou une phase en particulier du continuum de la délivrance des documents de voyage, la présente section se penche sur la structure organisationnelle et le cadre stratégique dans lesquels se déroulent les activités de délivrance. Ce sont là les fondements mêmes d'un environnement organisationnel qui favorise la sécurité. Le présent chapitre aborde également certaines pratiques de sécurité qui doivent être appliquées à toutes les étapes du processus de délivrance : les évaluations courantes des menaces et des risques, de même que les vérifications.

1.2 Structure organisationnelle

1.2.1 Mandat, responsabilités et législations

Une ADDV devrait être une organisation (ou section) gouvernementale indépendante axée uniquement sur la délivrance des passeports, des autres titres de voyage et d'autres documents gouvernementaux d'identité. Il ne devrait y avoir qu'une seule ADDV chargée de tous les documents de voyage délivrés par l'État. Elle devrait relever d'un échelon administratif supérieur au sein du gouvernement qui devrait s'assurer que le mandat et les responsabilités de l'ADDV sont assumés adéquatement.

Des lois ou des règlements de mise en application sont nécessaires pour établir le mandat, les responsabilités et les limites d'une ADDV, de ses cadres supérieurs et de ses employés. De nombreux gouvernements traduisent les exigences générales de certaines lois en règlements particuliers ayant force de loi qui servent de lignes directrices à la fois aux requérants et au personnel de l'ADDV en ce qui a trait à ce qui est permis et aux règlements qui présentent une certaine flexibilité. Ces règlements établissent des limites quant à ce que les requérants peuvent s'attendre à recevoir et quant aux services que les membres du personnel peuvent légitimement fournir en vertu de leur autorité. Les pouvoirs, aux échelons local, régional et national, devraient être clairement définis. Les domaines devant être réglementés devraient comprendre :

- le pouvoir fondamental de délivrer, de révoquer, de refuser, de récupérer, d'annuler et de refuser des documents de voyage;
- les personnes qui peuvent présenter une demande de document de voyage;
- les exigences auxquelles les requérants doivent satisfaire pour obtenir un document;
- les droits associés aux services fournis par l'ADDV;
- les exigences relatives à la tenue des dossiers;
- la protection de la vie privée;
- la période de validité du document de voyage;
- les renseignements à fournir dans le document de voyage;
- des directives sur l'utilisation des documents de voyage;
- des mécanismes établis pour engager des poursuites lorsqu'il y a contrefaçon, utilisation abusive des documents de voyage, fausse représentation — utilisation d'un document de voyage d'une autre personne —, et mutilation du document de voyage.

En raison de ses implications en matière de sécurité et des interrelations avec le contrôle frontalier et l'immigration, la délivrance des documents de voyage devrait aussi être comprise dans le cadre de la sécurité nationale de tout pays et être reconnue comme ayant des effets considérables sur la sécurité nationale et internationale. L'ADDV et son personnel devraient être associés à la planification de la sécurité gouvernementale de façon générale et être conscients des répercussions de leurs responsabilités sur la sécurité à l'échelle mondiale. Un résultat souhaitable de cette reconnaissance est que les responsabilités en matière de sécurité de l'ADDV soient soutenues adéquatement par le gouvernement et par des ressources conséquentes.

1.2.2 Structure du processus de délivrance (centralisé ou décentralisé)

Chaque gouvernement doit tirer ses propres conclusions quant à la structure qui convient le mieux à son processus de délivrance (centralisé ou décentralisé), en tenant compte de nombreuses considérations, comme la charge de travail, la région géographie, la situation sociale, le niveau requis de service à la clientèle, etc.

Un processus uniforme de demande et de délivrance à tous les lieux de personnalisation et de délivrance des documents de voyage est hautement recommandé pour s'assurer de sa normalisation et de sa transparence. En utilisant des procédures, des configurations logicielles et matérielles, ainsi que des formulaires normalisés, il est plus facile de garantir un niveau minimal de qualité, de conformité, de sécurité et de contrôle. Peu importe la structure organisationnelle choisie, il doit y avoir une supervision et un contrôle centralisés de tous les aspects du processus de délivrance. Aussi, des examens et des vérifications de routine sont essentiels dans toutes les organisations et les installations concernées par le processus de délivrance des passeports.

1.2.3 Recours à des partenaires (publics ou privés)

Beaucoup de pays font appel à des partenaires gouvernementaux ou à des fournisseurs externes réputés pour l'exécution de certaines fonctions du processus de délivrance des documents de voyage, telles que :

- la production de livrets (ou de matériel utilisé dans la production des livrets);
- la réception des demandes de documents de voyage;
- l'impression;
- la délivrance.

Les décisions relatives à l'admissibilité des requérants ne doivent JAMAIS être confiées à une société extérieure.

Divers facteurs doivent être pris en considération lorsqu'il s'agit de décider de recourir à des partenaires publics ou privés. Chaque ADDV doit en venir à ses propres conclusions en fonction de sa situation particulière.

Facteurs	Commentaires
Coûts	Les coûts des fonctions peuvent varier, selon qu'elles sont exécutées à l'interne ou par une société extérieure.
Disponibilité des ressources	L'autorité de délivrance pourrait ne pas avoir les ressources internes (p. ex. ressources humaines, installations, équipement) requises pour exécuter certaines fonctions.
Accessibilité des services	Dépendant du territoire desservi par l'autorité de délivrance, les services pourraient être plus accessibles à la population, s'ils étaient fournis par des partenaires.
Contrôle des données, du matériel et des processus	L'externalisation peut se révéler moins souhaitable en ce qui concerne le contrôle des données, du matériel et des processus, à moins que ce contrôle soit réglementé en vertu d'une entente contractuelle.

Emplacement ou nationalité des sociétés extérieures dont on a retenu les services	Le contexte politique et économique ainsi que le contexte de sécurité doivent être pris en considération.
Questions de transport	La sécurité des documents de voyage ou du matériel lors de leur transport est cruciale.
Mesures de sécurité mises en place dans les installations	Toutes les installations concernées par le processus de délivrance doivent être munies de dispositifs de sécurité et de protection adéquats.

Avant de lancer un appel d'offres pour un nouveau système de production et de délivrance de documents de voyage ou d'autres services connexes, un pays devrait planifier soigneusement tous les aspects du projet. Dans bien des cas, le succès d'une telle démarche dépend du travail préliminaire exécuté lors de la phase de planification du projet et peut bénéficier grandement d'une recherche préalable au projet. Les pays devraient communiquer avec d'autres pays qui ont mis en œuvre le système ou le service considéré pour apprendre de leur expérience. Une autre bonne pratique consiste à effectuer une demande de renseignements (DR) afin d'établir quels types de systèmes et technologies sont disponibles actuellement pour mieux définir les besoins de l'autorité de délivrance. Avant de signer une entente avec un partenaire éventuel, une évaluation des menaces et des risques (EMR) de ce partenaire devrait être effectuée en vue d'assurer sa fiabilité. Une fois qu'un partenaire a été sélectionné, des vérifications régulières doivent être effectuées tout au long de la relation de travail.

Des contrats ou des protocoles d'entente doivent être mis en place pour définir les droits et les responsabilités de toutes les parties concernées, ainsi que les sanctions prévues s'ils ne sont pas respectés. L'ADDV doit procéder régulièrement à des examens et à des vérifications des partenaires pour s'assurer qu'ils disposent sur le terrain de tous les dispositifs de sécurité et de protection requis. Il est recommandé d'effectuer régulièrement des évaluations de risque dans toutes les installations.

1.3 Cadre de sécurité

Un cadre de sécurité comprend les stratégies, les politiques, les pratiques et les contrôles qui conduisent à un processus plus sûr de délivrance des documents de voyage. Le présent Guide a pour but d'évaluer le cadre de sécurité d'une autorité de délivrance de documents de voyage (ADDV). Un tel cadre favorise une meilleure coordination, la normalisation et la cohérence des pratiques et des concepts liés à la sécurité dans l'organisation et la chaîne de production des documents. Certains fondements doivent être mis en place pour s'assurer que le cadre de sécurité est efficace, mais aussi qu'il est connu et mis en application par les employés et la direction. La section 1.3 présente ces fondements, à savoir : une équipe ou une section spécialisée chargée de la sécurité; des politiques et des lignes directrices documentées; un appui de la direction et un soutien financier; ainsi que des outils et des activités de formation et de sensibilisation.

1.3.1 Équipe de sécurité (ou Section spécialisée chargée de la sécurité)

L' ADDV devrait avoir une équipe ou une section particulière chargée d'élaborer et de superviser le cadre stratégique de sécurité et de s'assurer de sa conformité. Ce groupe spécialisé chargé de la sécurité devrait être indépendant des opérations. Ses membres devraient recevoir les ressources appropriées et une formation à jour sur la sécurité. Les responsabilités et les activités de l'équipe de sécurité devraient être bien planifiées et relever de la haute direction. Ces responsabilités et activités devraient comprendre — sans toutefois s'y limiter — les suivantes :

- définir le cadre de la sécurité — les stratégies, les politiques, les pratiques et les contrôles;
- procéder à des examens documentés de la sécurité, des évaluations de risque et des vérifications dans toutes les installations et tous les processus, de même que chez les partenaires;
- assurer l'intégrité du processus de délivrance de documents de voyage;
- assurer la sécurité et la qualité des documents de voyage;
- fournir une expertise en matière de fraude;
- élaborer des programmes de formation et de sensibilisation à la sécurité;
- effectuer des enquêtes internes en cas d'incidents de sécurité;

- consulter les intervenants gouvernementaux (p. ex. organismes de contrôle frontalier, autorités de l'immigration et organismes d'application de la loi) à propos des questions liées à la sécurité.

1.3.1.1 Gestionnaires des contrôles internes

Tout changement organisationnel, toute mise à niveau de la technologie, toute modification au processus de demande et toute méthode opérationnelle peuvent avoir des répercussions sur la sécurité du processus de délivrance. Il est donc important que des gestionnaires soient désignés au niveau national (administration centrale) et à chaque lieu de production (bureau extérieur) afin de s'assurer que des considérations liées à la sécurité et aux contrôles internes sont prises en compte dans les décisions des gestionnaires.

Ces gestionnaires devraient être indépendants de la voie hiérarchique et relever du dirigeant de l'autorité de délivrance. La raison de cette indépendance est que la principale responsabilité du bureau des opérations est de délivrer des documents de voyage, de prévenir les arriérés et de s'assurer que le travail est fait. Bien que la direction des opérations puisse se soucier des contrôles internes, ils ne sont pas sa première préoccupation.

- Au niveau national, le gestionnaire désigné des contrôles internes devrait être un cadre supérieur qui participe aux processus de planification et de prise de décisions de l'organisation.
- Au niveau du bureau local, un cadre supérieur devrait être désigné comme responsable des contrôles internes, de préférence une personne qui connaît le travail en détail, mais qui n'a pas d'autorisation dans le processus de demande ou le traitement des documents. L'administration réussie du programme des contrôles internes sur place devrait constituer un élément crucial dans l'évaluation du rendement de ce cadre supérieur.

1.3.1.2 Équipe de lutte antifraude

Il est recommandé que toute ADDV crée une équipe axée principalement sur la prévention de la fraude. Il devrait y avoir au moins un représentant de cette équipe dans chaque bureau de délivrance de passeports. Les tâches de cette équipe antifraude devraient être notamment les suivantes :

- coordonner les activités de lutte contre la fraude;
- fournir des ressources de formation;
- fournir des conseils lors du traitement de dossiers difficiles;
- établir des liens avec d'autres entités gouvernementales qui produisent des documents de base, des documents principaux ou des documents justificatifs;
- assurer la liaison avec d'autres organismes gouvernementaux qui engagent des poursuites judiciaires en cas de fraude.

1.3.2 Politiques documentées en matière de sécurité

Les politiques, les pratiques, les lignes directrices et les stratégies de sécurité élaborées par l'équipe ou la section responsable de la sécurité, et qui forment le cadre de la sécurité organisationnelle devraient être rédigées et documentées. Elles devraient comprendre les procédures et les contrôles internes mis en place pour réduire la vulnérabilité de tous les aspects des opérations de l'ADDV. Elles devraient être mises en œuvre complètement et de façon uniforme dans toutes les installations et au sein de toute organisation partenaire qui participe à la délivrance des documents de voyage.

Les politiques, les pratiques et les lignes directrices devraient souligner les responsabilités de chaque personne relativement à la sécurité des biens et faire valoir le soutien de la direction au programme de sécurité. Elles devraient être communiquées à tous les employés de manière à être bien connues. Elles devraient être faciles à consulter et faciles à comprendre. La conformité aux politiques devrait être étroitement surveillée et les politiques devraient être rigoureusement appliquées.

Les renseignements figurant dans les différents chapitres qui suivent peuvent servir de base aux politiques et procédures de sécurité.

1.3.3 Appui de la direction et soutien financier

1.3.3.1 Appui de la direction

Aucun programme de sécurité ne peut fonctionner adéquatement sans l'appui de la haute direction. Les décideurs doivent être disposés à consacrer du temps et des ressources à l'élaboration, à la mise en œuvre et au maintien d'un système efficace de contrôles internes. La mise en œuvre d'un tel système pourrait nécessiter une réorganisation du déroulement du travail, des modifications apportées à la gestion du personnel ou à d'autres aspects des opérations, l'organisation de séances de formation et de sensibilisation, etc. Il est aussi essentiel que la haute direction donne l'exemple en suivant les politiques sur la sécurité et les autres mesures établies par l'équipe ou la section responsable de la sécurité, sans enfreindre les règles ni demander des faveurs particulières.

1.3.3.2 Soutien financier

Des ressources humaines et financières sont également requises pour protéger l'intégrité du processus de délivrance. Cette exigence peut poser des difficultés à une autorité de délivrance qui dispose d'un budget restreint. Toutefois, il est important de reconnaître que le défaut de fournir des ressources adéquates pour soutenir un programme efficace de contrôles internes peut, en dernier ressort, entraîner des coûts importants, parmi lesquels :

- la possibilité d'un embarras national, si un document de voyage d'un pays est utilisé pour commettre des actes terroristes;
- les difficultés que rencontreront les citoyens d'un pays au cours de leurs déplacements à l'étranger si leurs documents de voyage font l'objet d'un examen plus minutieux de la part des autorités frontalières et des autorités qui délivrent des visas;
- les coûts importants associés aux enquêtes, aux poursuites judiciaires et aux incarcérations découlant des activités criminelles facilitées par la fraude de documents de voyage.

Des documents de grande qualité délivrés avec un degré élevé d'intégrité sont de nature à prévenir ces types d'abus. Il est généralement moins coûteux de prévenir de tels événements en ayant un processus de délivrance hautement sûr et contrôlé que de prendre des mesures correctrices en raison d'un processus de délivrance qui n'est pas sûr.

Il est recommandé que le processus d'établissement des droits associés aux documents de voyage tienne compte des coûts réels des services fournis, y compris les coûts liés à la sécurité sous toutes ses formes (p. ex. le personnel, la formation, les logiciels, le matériel informatique, la sécurité physique, la papeterie, les brochures, les documents de communication, l'équipement d'entretien, etc.).

1.3.4 Création d'une culture de la sécurité (formation et sensibilisation)

L'organisation doit promouvoir la sécurité de son personnel afin de créer une culture organisationnelle propice à la mise en œuvre et au respect des politiques et des pratiques en matière de sécurité. Voici quelques exemples de techniques dont la haute direction pourrait se servir afin de créer une culture de la sécurité et d'améliorer la sensibilisation de son personnel à l'égard de la sécurité :

- tenir des séances régulières de formation et d'information sur la sécurité, de même que des programmes de mise à jour des connaissances;
- rappeler régulièrement aux individus leurs responsabilités en matière de sécurité;
- élaborer un code de déontologie ou des lignes directrices en matière de valeurs et d'éthique (Chapitre 9);
- organiser une campagne de communication ou de promotion des politiques en matière de sécurité;
- publier les résultats des évaluations et des vérifications de la sécurité;
- organiser des réunions mensuelles sur la sécurité;
- produire et distribuer des bulletins d'information;
- utiliser l'intranet;
- utiliser le renforcement positif et récompenser les bonnes pratiques de sécurité;

- imposer des sanctions et des mesures disciplinaires dans le cas d'un comportement non conforme ou négligent.

Il importe de fournir aux employés une formation régulière sur la sécurité afin de maintenir leur niveau de sensibilisation à la sécurité. Selon le poste qu'ils occupent, les employés devraient aussi recevoir une formation sur les mesures de sécurité particulières qui s'appliquent à leurs fonctions, par exemple sur l'utilisation abusive et la contrefaçon des documents de voyage et d'autres aspects de la fraude. Ils devraient être formés au traitement des renseignements personnels et confidentiels, ainsi qu'à la sécurité de la technologie de l'information. On devrait vérifier dans quelle mesure les employés comprennent les pratiques et les concepts liés à la sécurité, de même que les raisons sous-jacentes. S'ils manquent d'information ou ne comprennent pas la nécessité de toutes les mesures de sécurité à exécuter, ils pourraient être tentés d'utiliser des raccourcis dans les procédures afin de se faciliter la tâche. On devrait encourager également le personnel à faire des suggestions à propos des améliorations éventuelles à apporter aux pratiques de sécurité.

1.3.5 Normes de rendement

Les descriptions de postes de tous les employés devraient comporter une norme de rendement qui impose l'obligation de bien connaître les contrôles internes et de les respecter. L'évaluation de tous les employés devrait porter sur leur rendement par rapport aux contrôles internes et comporter des mesures disciplinaires, lorsque des responsabilités ou des obligations en matière de sécurité sont négligées.

1.3.6 Anticipation et planification de la charge de travail

L'ADDV devrait prévoir les périodes durant lesquelles les demandes de documents de voyage sont en forte hausse et affecter les ressources humaines et financières en conséquence. On peut faire des projections de la charge de travail en utilisant des données historiques et en tenant compte des éléments connus qui peuvent influer sur les demandes de production de documents (p. ex. la période des vacances et les périodes de relâche scolaire, des événements majeurs, les conditions économiques, et les exigences des autres pays en matière d'entrée, etc.).

L'ADDV devrait déployer tous les efforts requis pour établir un niveau de dotation en personnel adéquat et, ainsi, répondre aux besoins selon le volume projeté de travail. Elle devrait également préparer des plans d'urgence pour faire face à des éclosions de maladies telles que des pandémies. L'accroissement des capacités ne devrait pas être trop rapide, afin d'éviter d'avoir à former un nombre important de nouveaux employés en même temps. L'ADDV devrait maintenir un bassin de personnes disponibles sur appel, dont les antécédents ont été préalablement vérifiés, en cas de surcharge de travail ou dans des situations de manque de personnel.

Les contrôles internes sont plus importants que jamais quand il y a une augmentation de la charge de travail, puisque les employés affectés au service à la clientèle et concernés par les arriérés dans les demandes pourraient être tentés d'aller plus vite ou d'ignorer les procédures de contrôle interne alors perçues comme des entraves au déroulement du travail. Quand ils sont sujets aux pressions d'une charge de travail accrue, les gestionnaires doivent résister à la tentation d'ignorer les contrôles internes.

1.4 Pratiques générales de sécurité

Certaines pratiques de sécurité s'appliquent à tout le processus de délivrance de documents de voyage : les évaluations des menaces et des risques et les vérifications devraient être effectuées régulièrement à toutes les étapes et pour toutes les fonctions, les biens et les installations concernés par le processus de délivrance. Ces pratiques sont expliquées dans la présente section, *Pratiques générales de sécurité*, ce qui évite de répéter leur importance dans les chapitres subséquents.

1.4.1 Évaluations des menaces et des risques

Il est recommandé que toute ADDV prenne les mesures appropriées pour gérer les menaces à sa sécurité et la vulnérabilité de son système de délivrance. La gestion des risques est le processus au moyen duquel les ressources sont planifiées, organisées, orientées et contrôlées pour s'assurer que les risques associés au fonctionnement d'un système demeurent dans des limites acceptables à un coût optimal. Puisqu'il serait extrêmement coûteux et probablement impossible de protéger totalement les renseignements et les biens contre toute menace, les pratiques modernes de sécurité sont fondées sur l'évaluation des menaces et des vulnérabilités en raison du degré de risque présenté par chacune d'elles, ainsi que sur le choix des mesures de protection les plus appropriées et les plus efficientes.

Les évaluations des menaces et des risques sont importantes, car elles contribuent à déterminer les menaces actuelles qui pèsent sur le système de délivrance, de même que les biens et les secteurs les plus à risque à l'intérieur du processus. Ces évaluations conduisent à des recommandations de mesures de prévention et d'atténuation susceptibles de réduire les risques à des niveaux acceptables. Les évaluations des menaces et des risquent comportent les éléments suivants :

- l'établissement de la portée des évaluations;
- la détermination des menaces, l'évaluation de leur probabilité et des conséquences de leur apparition;
- l'évaluation des risques fondée sur l'adéquation des mesures de protection existantes et sur la vulnérabilité du système;
- la mise en œuvre de mesures de protection supplémentaires visant à réduire les risques à des niveaux acceptables.

Les menaces et les raisons sous-jacentes des tentatives de fraude peuvent différer considérablement d'un pays à l'autre, voire d'une région à l'autre. C'est pourquoi les évaluations des menaces et des risques doivent être faites dans toutes les installations de délivrance et à toutes les étapes du processus de délivrance, en collaboration avec les organismes d'application de la loi. Il est important de noter que des menaces proviennent également de sources internes et l'ADDV doit s'assurer que les processus et les systèmes de soutien du personnel et de gestion des risques relativement à l'inconduite et à la corruption sont pris en compte.

Les personnes qui travaillent avec les systèmes et les procédures sont celles qui en connaissent le mieux la vulnérabilité. Il est sage de demander périodiquement aux employés ce qu'ils pensent être des vulnérabilités du processus de délivrance et ce qui devrait être fait pour les minimiser. On devrait encourager le personnel à signaler toute préoccupation. Dans la même logique, les employés qui signalent des problèmes devraient faire l'objet d'une reconnaissance appropriée. Il est recommandé de conserver les statistiques sur les menaces ou les risques qui se concrétisent afin de concentrer les ressources sur les changements à apporter aux processus afin de prévenir de futurs incidents ou attaques d'un type particulier.

L'organisation doit surveiller continuellement tout changement dans l'environnement des menaces et prendre les mesures correctrices appropriées pour maintenir un niveau de risque acceptable en l'équilibre entre les besoins opérationnels et la sécurité. Pour de plus amples renseignements, veuillez consulter la norme de gestion des risques australienne et néo-zélandaise *(Australian and New Zealand Risk Management Standard* ASNZS 4360/2004), qui est en voie de devenir une norme ISO 31000 (http://www.iso.org/iso/catalogue_detail.htm?scnumber=43170).

Lorsqu'elle examine les risques et les vulnérabilités, l'ADDV devrait également mettre en place un plan de continuité des opérations pour s'assurer, dans l'éventualité où une importante menace ou attaque se concrétiserait, de la poursuite des opérations de délivrance de passeports. Ceci est particulièrement important pour les États qui possèdent un site principal de délivrance. Pour de plus amples renseignements sur le plan de continuité des opérations, veuillez consulter le matériel et les normes d'orientation des pratiques exemplaires de l'Institut de la continuité des opérations (Business Continuity Institute — http://www.the bci.org).

1.4.2 Vérifications

Un des moyens les plus efficaces de s'assurer de la conformité des employés et de leur compréhension des règles établies pour prévenir la fraude est d'avoir un système de vérifications prescrites officiellement. Il devrait y avoir des vérifications périodiques et ponctuelles à la fois internes et externes (réalisées par des organisations externes indépendantes).

1.4.2.1 Vérifications internes

Des vérifications officielles et ponctuelles devraient avoir lieu régulièrement dans toutes les installations et à toutes les étapes du processus de délivrance pour s'assurer que les politiques et les règles sont suivies.

Des vérifications internes officielles et des examens de conformité devraient être effectués par des cadres supérieurs afin de passer en revue la gestion des opérations et de s'assurer de l'adéquation du programme des contrôles internes. L'équipe d'inspection devrait produire un rapport officiel et acheminer ses recommandations d'amélioration au cadre supérieur dont l'ADDV relève. Un processus de conformité devrait être instauré pour s'assurer que les changements requis sont mis en œuvre.

Ces vérifications officielles devraient être accompagnées d'un examen intensif du travail en cours par les gestionnaires. Il devrait y avoir des vérifications du travail en cours faites au hasard pour s'assurer que les règles établies sont conformes en tout temps et, en particulier, lors des périodes de charge de travail accrue, lorsque les employés et les gestionnaires peuvent être tentés d'aller plus vite et d'ignorer certains contrôles internes. Les vérifications internes nécessitent la présence de cadres supérieurs dans toutes les installations pour établir un pourcentage des demandes les plus urgentes, les autres demandes en cours et les demandes de documents de voyage déjà livrés. Parallèlement, ces cadres doivent s'assurer que les procédures appropriées ont été suivies, que les documents justificatifs joints ou consignés sont adéquats, que les notations sont complètes, que les mesures prises peuvent être justifiées et que les droits appropriés ont été payés.

1.4.2.2 Vérifications externes

Une organisation externe indépendante, comme un bureau de vérification du gouvernement, devrait également pouvoir effectuer des vérifications du rendement afin d'évaluer les pratiques de sécurité mises en place par l'ADDV. Les organisations indépendantes formulent généralement des recommandations et ont la responsabilité de surveiller leur mise en œuvre. Les vérifications externes se révèlent très efficaces, puisqu'elles ne sont ni aveuglées par les « pratiques habituelles » au sein de l'organisation, ni influencées par les impératifs liés aux opérations, et qu'elles sont au courant des menaces à la sécurité et des mesures de sécurité efficaces instaurées dans d'autres organisations.

2 Processus de demande

2.1 Sommaire

Pour obtenir des documents de voyage, les requérants doivent suivre un processus de demande établi — remplir des formulaires, fournir des preuves documentaires, des photos et, dans certains cas, des identificateurs biométriques secondaires. Les renseignements et les documents présentés par les requérants permettent aux employés de l'autorité de délivrance d'établir leur admissibilité à un document de voyage.

Les renseignements des requérants doivent être protégés durant tout le processus de délivrance de documents de voyage et après leur délivrance. Le respect de la vie privée et la protection des données sont des éléments essentiels pour assurer la sécurité du processus de délivrance.

2.2 Processus de demande et exigences relatives aux demandes

2.2.1 Uniformité des processus

Peu importe la structure organisationnelle de l'ADDV (centralisée ou décentralisée) et les renseignements et les documents présentés par les requérants, toutes les demandes devraient être traitées uniformément dans l'ensemble de l'organisation. Tous les formulaires de demande devraient être normalisés, et les exigences relatives aux demandes devraient être uniformes à l'échelle du pays. Les politiques et les procédures concernant la manière de présenter les demandes et les endroits prévus à cette fin devraient être faciles à accès au public. Tout le processus de demande doit être transparent. Les politiques et procédures décrivant le mode de traitement des demandes devraient être documentées et faciles d'accès au personnel de l'ADDV.

2.2.2 Facteurs qui influent sur le processus

Le processus de demande et les exigences relatives aux demandes varient d'un pays à l'autre (p. ex. demandes en personne, par la poste, en ligne, etc.). En plus de la sécurité, divers facteurs doivent être pris en considération lors de l'établissement d'un processus de demande, dont ceux-ci :

Facteurs	Commentaires
Première demande ou renouvellement	Une première demande devrait être examinée plus minutieusement. Il est possible que le requérant qui a déjà eu un passeport ne soit pas tenu de se présenter en personne ou de présenter les mêmes documents (p. ex. des documents de base) qu'un nouveau requérant, mais il doit habituellement présenter son ancien passeport ou document de voyage avec sa demande. Toutefois, si le passeport antérieur a été délivré sous une fausse identité, le renouvellement automatique sans vérification supplémentaire perpétue le problème.
Accessibilité du service	Tout dépendant du territoire couvert par l'autorité de délivrance et du réseau des bureaux de délivrance, la possibilité d'acheminer la demande par voie postale ou de la présenter à un bureau d'un partenaire pourrait rendre le service plus accessible à la population.
Confirmation de l'identité	Une comparution obligatoire en personne devant un agent du gouvernement offre les meilleures possibilités d'une confirmation de l'identité pour la grande majorité des requérants. On peut ainsi confirmer que la personne est encore vivante, les photos peuvent être comparées à la véritable apparence de la personne, le requérant peut répondre directement aux questions, et son comportement peut être observé et jugé.
Antécédents de documents de voyage perdus ou volés	S'il a des antécédents de documents de voyage perdus ou volés, le requérant peut être tenu de présenter sa demande en personne (voir le Chapitre 10).
Collecte d'identificateurs biométriques secondaires	La collecte de données biométriques requiert la présence du requérant à au moins une occasion.
Sécurité du système postal	Si les services postaux publics ou privés ne sont pas fiables, le processus de demande devrait exiger du requérant qu'il présente sa demande en personne.
Technologie	Le développement de nouvelles technologies peut permettre qu'une partie du processus de demande soit faite en ligne ou à distance (p. ex. l'impression des formulaires, la

	transmission de photographies numériques, des entrevues par téléphone ou par téléconférence).
Service urgent ou service express	Lorsqu'une une demande doit être traitée en urgence, le requérant peut être tenu de se présenter en personne à un bureau de l'autorité de délivrance.

Beaucoup de pays exigent la comparution en personne pour toutes les demandes de document de voyage, y compris les demandes de renouvellement. Cependant, la question à savoir si cela est nécessaire dépend des mesures de protection mises en place dans les processus de demande et de délivrance. Certains pays exigent la comparution en personne seulement dans le cas des nouveaux requérants, des enfants mineurs et des personnes qui ne peuvent pas présenter leur plus récent document de voyage. On peut établir l'identité des adultes dont l'identité a déjà été authentifiée en comparant leur ancien passeport avec de nouvelles photos (ou des identificateurs biométriques). Ces derniers pourraient alors ne pas être tenus de se présenter en personne. Dans la perspective de la sécurité, la présentation de la demande en personne contribue à accroître la sécurité du processus. Néanmoins, d'autres moyens de vérifier l'identité des requérants peuvent réduire efficacement les risques à la sécurité à un niveau acceptable.

Les agents réceptionnaires de demandes de documents de voyage, le cas échéant, doivent être formés et devraient recevoir des directives écrites détaillées sur la manière d'établir l'identité des requérants, de noter les documents d'identité sur la demande de passeport et sur ce qu'ils doivent faire lorsqu'ils ne sont pas convaincus que les documents présentés satisfont aux exigences. Les employés doivent recevoir une formation leur permettant d'acquérir d'autres compétences qui les aideront à reconnaître d'autres signes ou indicateurs d'une demande frauduleuse, par exemple des techniques d'entrevue, des techniques de reconnaissance du langage corporel, des techniques de vérification des documents de base et l'aptitude à déceler des incohérences dans les demandes et l'ensemble des documents présentés par les requérants.

Dans de nombreux pays, les demandes de documents de voyage sont reçues par des partenaires externes de l'autorité de délivrance. Un partenaire externe peut simplement agir en tant que boîte aux lettres en procédant à des vérifications très élémentaires pour s'assurer, par exemple, que le formulaire de demande a été dûment rempli, que les droits exigibles ont été payés et que les preuves documentaires requises ont été jointes à la demande. Si elle n'est pas exécutée par l'autorité de délivrance, il est recommandé que cette fonction soit confiée à des institutions gouvernementales qui connaissent bien les procédures légales et le travail de bureau, comme les tribunaux, la police ou les bureaux de poste, ou à d'autres bureaux qui ont l'habitude de traiter avec le public, comme les bureaux d'impôt ou les bibliothèques gouvernementales. Les partenaires d'une ADDV doivent être formés pour procéder à la vérification des documents de base et disposer d'une formation de base pour reconnaître ou détecter les caractéristiques de la fraude. En cas de doute, ils doivent acheminer les dossiers à l'autorité de délivrance.

2.3 Photographies

Pour obtenir un document de voyage, le requérant doit présenter des photos prises par un photographe commercial, un partenaire de confiance ou un fonctionnaire du pays. Seules les photos conformes aux spécifications de l'OACI contenues dans le *Document 9303* devraient être acceptées par l'autorité de délivrance. La conformité à ces spécifications facilite la vérification de l'identité du titulaire par l'ADDV et aux postes frontaliers et permet l'utilisation de la technologie de reconnaissance faciale. Afin d'aider à assurer la conformité aux spécifications des photos de l'OACI, on devrait rendre ces spécifications accessibles aux photographes commerciaux ainsi qu'au public.

Voici quelques exemples de spécifications de photos publiées :

États-Unis : http://travel.state.gov/passport/guide/guide_2081.html
Nouvelle-Zélande : http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Passports-Photographic-Requirements
Canada : http://www.pptc.gc.ca/cdn/photos.aspx?lang=fra

En raison du développement des nouvelles technologies, certains pays pourraient commencer à accepter des demandes en ligne et des photographies numériques ou électroniques. Ces photos devraient être prises par un partenaire de confiance ou un fonctionnaire et transmises de manière sûre du point de saisie à l'autorité de délivrance, sans aucune possibilité qu'elles soient modifiées. Pour minimiser le risque qu'une photo puisse être modifiée aux diverses étapes du processus de demande, une photographie sur support papier devrait être exigée, en plus de la photographie numérique.

2.4 Identificateurs biométriques secondaires

Nombreux sont les pays qui exigent ou exigeront la collecte d'empreintes digitales dans le cadre du processus de délivrance de documents de voyage. La collecte de données biométriques, y compris les empreintes digitales et l'iris, peut être réalisée par une autorité de délivrance, d'autres agents gouvernementaux, des tiers agents de confiance désignés par le gouvernement, ou par d'autres moyens sûrs et fiables. Il reviendra à chaque pays de décider de la manière de traiter la collecte et l'inscription des données biométriques. Peu importe la méthode choisie, il est impératif de toujours s'assurer qu'elle est conforme au respect de la vie privée, sûre et fiable. Le pays doit décider s'il exigera la collecte de données biométriques seulement lors d'une première demande ou pour toute demande de documents de voyage, y compris les renouvellements.

2.5 Traitement et protection des renseignements personnels

Pour bien remplir son mandat, l'ADDV traite et stocke de grandes quantités de renseignements personnels sur les requérants. Ces renseignements doivent être protégés rigoureusement, puisque les criminels cherchent à y accéder et à les utiliser à des fins illégales, comme l'usurpation d'identité, des gains financiers ou d'autres types de fraude d'identité. Ces types de fraude sont de plus en plus courants et suscitent beaucoup de préoccupations dans nos sociétés.

Les formulaires de demande de documents de voyage, une fois remplis, contiennent des renseignements personnels. Ces renseignements sont généralement protégés par des lois sur la protection de la vie privée et ne doivent en aucun cas être divulgués à des tiers sans une autorisation appropriée. Les employés d'une ADDV doivent recevoir une formation et une documentation relatives aux diverses lois sur la protection de la vie privée en vigueur dans leur pays, et les gestionnaires doivent veiller à leur application. Outre les considérations liées au respect de la vie privée, la divulgation non autorisée de ces renseignements à des tiers externes peut conduire à la fraude d'identité.

Chaque demande de document de voyage doit être enregistrée dès sa réception, et son état doit être mis à jour à chaque étape du processus de traitement. Les noms de tous les individus concernés par les différents stades du processus de traitement des demandes devraient apparaître dans les dossiers consignés et être approuvés lorsque la demande passe à l'étape suivante. Une telle démarche permet une surveillance étroite des personnes qui ont eu accès au dossier de la demande, ainsi qu'un contrôle de l'état de la demande en tout temps. Cela vaut particulièrement dans le cas des dossiers relatifs à des personnalités de marque. Tous les formulaires et les documents présentés devraient être stockés dans des classeurs verrouillés adéquats ou, à tout le moins, dans un endroit sûr en tout temps, y compris pendant le traitement de la demande. En dehors des heures normales de travail, il est essentiel que le travail en cours soit mis sous clé de manière à ce que les surveillants de nuit, les employés préposés au nettoyage ou d'autres membres du personnel ne puissent pas avoir accès aux renseignements personnels des requérants. Les membres du personnel devraient toujours être en mesure de rendre des comptes sur tous les documents relatifs aux demandes et leurs copies. Ces documents ne devraient jamais sortir des installations de l'ADDV.

Les renseignements personnels contenus dans une demande et conservés dans des dossiers informatisés doivent être protégés par des normes relatives à la sécurité de la technologie de l'information (voir le Chapitre 8). Ces renseignements détaillés ne devraient jamais être enregistrés ou partagés sur un réseau non protégé, des connexions Internet ou des ordinateurs portables qui pourraient être retirés des installations de l'ADDV. Des registres électroniques doivent servir à contrôler l'accès aux fichiers. Pour une

plus grande sécurité, des caractéristiques telles que les contrôles biométriques et les cartes d'identité personnalisées peuvent être utilisées pour accéder à un système ou une base de données.

Une fois le traitement d'une demande terminé, tous les documents relatifs à la demande qui contiennent des renseignements personnels sur le requérant (le formulaire de demande, les documents connexes, les dossiers informatiques, les images des documents de base et les données connexes, les images de la page de renseignements, le contenu de la puce du passeport électronique, etc.) devraient être stockés minutieusement et en toute sécurité aux fins de consultation future dans un classeur verrouillé de manière appropriée ou dans une salle protégée et dans une base de données protégée. L'accès aux dossiers archivés devrait faire l'objet d'un contrôle, d'un protocole et d'un suivi stricts. Lorsque les renseignements ne sont plus requis, ils devraient être déchiquetés ou détruits à l'aide d'un appareil de destruction de documents, conformément aux lois applicables et aux politiques de l'autorité de délivrance.

2.5.1 Systèmes automatisés

Le recours à la technologie pour automatiser les processus de délivrance des passeports peut accroître la sécurité de ces processus et leur précision. Les processus concernant l'entrée de données, la numérisation par balayage, l'impression, l'archivage, les envois postaux et les rapports de gestion peuvent tous être automatisés à un certain degré. L'automatisation limite la manipulation manuelle des données et peut permettre la détection plus rapide des renseignements frauduleux ou suspects. Les systèmes automatisés peuvent comprendre une fonction de vérification aléatoire de la sécurité : la demande doit alors être vue par un superviseur avant que l'autorisation de délivrance soit accordée.

3 Processus de détermination de l'admissibilité

3.1 Sommaire

Dans la plupart des pays, il existe trois éléments essentiels qu'un gouvernement doit établir avant de délivrer un document de voyage : la preuve de l'identité du requérant (l'identité est réelle et le requérant est bien la personne qu'il prétend être); la preuve de citoyenneté; et la preuve que le requérant n'est sujet à aucune restriction relative aux déplacements (par exemple, un casier judiciaire, des antécédents de documents de voyage perdus ou volés, le défaut de verser une pension alimentaire pour enfants, etc.). L'utilisation de tels outils et techniques sont utilisés varie d'un pays à l'autre. Il n'y a pas une seule méthode pour établir fermement l'identité d'un requérant, mais divers moyens sont utilisés pour établir avec une certitude raisonnable l'authenticité d'une identité. Une ADDV exige habituellement des preuves documentaires pour vérifier l'identité et la citoyenneté des requérants. Parmi les autres stratégies, mentionnons la collecte de données biométriques, la vérification de « l'empreinte sociale », le recours à un répondant et des références, les entrevues, etc.

Les restrictions qui limitent ou interdisent les déplacements de certains individus sont généralement vérifiées en comparant les demandes avec des bases de données, y compris des listes de surveillance contenant des renseignements recueillies par l'autorité de délivrance et les diverses organisations qui sont ses partenaires.

L'ADDV devrait posséder des politiques et des procédures documentées liées à la vérification de l'identité et à la détermination de l'admissibilité à un passeport. Ces politiques et procédures devraient être faciles d'accès au personnel de l'ADDV et la conformité aux politiques et aux procédures devrait être surveillée.

Toutes les décisions d'admissibilité devraient être prises par le personnel approprié de l'ADDV.

3.2 Traitement des premières demandes par rapport aux renouvellements

Dans certains pays, le processus de demande et de détermination de l'admissibilité n'est pas le même pour une première demande que pour un renouvellement. L'information et les documents requis, de même que les vérifications entreprises, peuvent différer. Les pays qui utilisent un processus différent pour les demandes de renouvellement devraient avoir une politique qui définit clairement dans quelles conditions une demande de renouvellement peut être présentée (p. ex. le passeport précédent a expiré moins d'un an avant la demande de renouvellement).

(Exemple : Processus de renouvellement simplifié à www.passportcanada.gc.ca/cdn/ren.aspx?lang=fra)

Les premières demandes devraient être examinées plus minutieusement. Les pays qui permettent la présentation de demandes de renouvellement longtemps (c.-à-d. plus de deux ans) après l'expiration du document de voyage précédent devraient examiner soigneusement et de plus près ces demandes. Dans tous les cas de renouvellements, les données de la demande soumise devraient être comparées aux renseignements contenus dans les documents de voyage précédemment délivrés à cette personne. De même, en ce qui a trait aux renouvellements, si le document de voyage antérieur a été délivré sous une fausse identité, son renouvellement automatique perpétue le problème. Une vérification supplémentaire comme les vérifications des bases de données et les vérifications de référence, devrait être effectuée pour s'assurer que cela ne se reproduise plus.

3.3 Demandes pour enfants

Une demande de document de voyage pour un enfant devrait être présentée par au moins l'un des parents ou une autre personne titulaire de l'autorité parentale à l'égard de l'enfant. La preuve de naissance et d'une empreinte sociale devraient être fournie, en plus d'une comparaison éventuelle à d'autres documents d'appui si l'enfant est assez âgé pour y être admissible. Le parent (les parents) ou

l'autre personne titulaire de l'autorité parentale qui présente une demande doit établir son identité. Les enfants ne doivent pas être inscrits dans un passeport d'adulte. Un passeport doit plutôt être délivré à chaque enfant, y compris aux nouveau-nés.

3.4 Preuves documentaires

La confirmation de l'identité de la personne qui présente une demande de document de voyage est essentielle à l'intégrité de ce document. Pour établir son identité, le requérant utilise un ou plusieurs documents. Les preuves documentaires doivent démontrer à la fois l'identité et la citoyenneté du requérant.

Il est crucial d'établir clairement que l'identité déclarée est l'identité réelle d'une personne, et non celle d'une personne décédée ou d'une personne fictive. L'identité de personnes décédées peut être utilisée abusivement par des imposteurs pour présenter des demandes de documents de voyage frauduleuses. Des mesures doivent être prises pour s'assurer que l'identité déclarée appartient à la personne vivante qui la revendique.

Les preuves documentaires servant à établir l'admissibilité en vertu des exigences relatives à l'identité et à la citoyenneté peuvent être combinées dans une seule pièce d'identité ou un seul document :

- Acte de naissance
- Acte de mariage
- Certificat de citoyenneté
- Certificat de naturalisation
- Passeport ou autre document de voyage existant
- Carte d'identité nationale

Ces documents sont appelés « documents de base » ou « documents primaires ». Les documents de base fournissent des renseignements détaillés sur l'identité et la nationalité des requérants. Ils sont délivrés par un gouvernement ou une autre autorité officielle. Ils ont déjà fait l'objet d'un niveau de vérification suffisamment élevé par des personnes de confiance. Ces documents devraient contenir des caractéristiques de sécurité de base, notamment un numéro unique et éventuellement un identificateur biométrique ou une photographie claire. Sans ces caractéristiques, l'autorité de délivrance est vulnérable au vol de la carte ou de l'identité d'une personne vivante ou décédée. Un document qui ne contient pas une photographie ou un identificateur biométrique ne sont généralement pas acceptables en tant que preuves d'identité quand ils sont présentés isolément. Cependant, utilisés conjointement avec d'autres types de documents, ils peuvent aider à établir l'identité du requérant. Dans de tels cas, on pourrait alors demander au requérant de présenter des documents à l'appui pour confirmer, par exemple, qu'il est une personne vivante qui réside à une adresse précise. Voici des exemples de documents à l'appui :

- Carte d'identité
- Liste électorale
- Données de recensement
- Dossier médical
- Numéro d'assurance ou de sécurité sociale et dossier d'impôt
- Relevé d'emploi
- Permis de conduire
- Dossier de propriété d'un véhicule motorisé
- Dossier financier

Des procédures particulières devraient être définies dans le cas des requérants qui présentent des documents de base et des documents à l'appui limités (qui présentent de vieux actes de naissance, qui n'ont pas de permis de conduire, etc.). En pareils cas, d'autres techniques ou moyens de validation de l'identité revêtent une importance particulière.

Tout requérant doit présenter ses preuves documentaires en même temps que sa demande. Les documents originaux devraient être remis, numérisés par balayage par l'autorité de délivrance et conservés dans la base de données centrale de manière à pouvoir être vérifiés sans préavis à n'importe quel moment durant les processus de détermination de l'admissibilité et de délivrance, ou lors d'un renouvellement. Les documents sont ensuite retournés au requérant, en même temps que le document de voyage délivré. Dans le cas des renouvellements, certains pays ne demandent pas aux requérants de présenter à nouveau tous leurs documents, à l'exception de leur passeport antérieur (ou d'un autre document de voyage). La vérification se fait à l'aide des renseignements et des documents numérisés par balayage figurant déjà dans la base de données de l'ADDV.

Dans beaucoup de pays, les preuves documentaires (documents de base et documents à l'appui) sont délivrées, stockées et extraites séparément; souvent elles sont délivrées par des autorités locales ou régionales sans faire l'objet d'une normalisation ou d'un contrôle au niveau national (ou avec une normalisation ou un contrôle limités). Ces preuves documentaires contiennent peu de dispositifs de sécurité. Les personnes qui obtiennent des documents de voyage en utilisant une fausse identité peuvent recourir à de nombreuses méthodes pour mettre la main sur des documents de base : le vol d'identité en tirant avantage de procédures de demande relâchées; la création de fausses identités à partir de celle d'une personne décédée; la contrefaçon de reproductions acceptables, en les remplissant et en les présentant comme étant authentiques. Une attention particulière devrait être accordée à la vérification de l'authenticité des documents présentés par toute personne qui présente une demande de document de voyage.

Il est recommandé de vérifier l'identité du requérant à l'aide des actes de décès en version papier ou en version électronique.

La norme d'authentification de l'identité du gouvernement de la Nouvelle-Zélande est une référence utile : http://www.e.govt.nz/services/authentication/standards/index.html

3.4.1 Vérification de l'authenticité des documents

3.4.1.1 Vérification des dispositifs de sécurité

Les employés qui reçoivent les demandes et qui établissent l'admissibilité des documents de voyage devraient suivre une formation sur les dispositifs de sécurité des documents authentiques et le dépistage des faux documents. Les documents de base, souvent des actes de naissance, existent probablement sous différentes formes dans le pays — ce qui complique singulièrement le processus d'établissement de l'identité lié à la délivrance des documents de voyage.

Idéalement, la vérification est effectuée par les employés mêmes de l'ADDV, qui ont reçu une formation à cet égard et qui ont une cote de sécurité appropriée. Toutefois, plus le pays est vaste, plus il y a de bureaux de demande et plus il y a de chances pour que l'ADDV établisse des partenariats avec des organisations bien représentées localement. Les employés des partenaires de l'ADDV devraient donc aussi être formés pour vérifier les documents de base. En cas de doute, ils devraient montrer les demandes au personnel de l'ADDV pour obtenir des conseils ou des directives. À des fins d'examen ou de vérification, il pourrait être nécessaire au personnel des partenaires de transmettre automatiquement aux superviseurs ou à l'unité de lutte antifraude les demandes accompagnées de preuves d'identité ou de citoyenneté moins fiables. Les limites minimales de sécurité prescrites devraient être fournies à tous les examinateurs.

3.4.1.2 Bases de données de documents

Des bases de données disponibles, gouvernementales ou commerciales, contiennent des exemples de divers documents de base ou documents de voyage authentiques. Elles peuvent servir à vérifier l'authenticité des documents présentés par les requérants. La base de données DISCS pour les documents de base et la base de données EDISON sont des exemples de propriétés du gouvernement pour les passeports accessibles à toutes les autorités de délivrance du monde, moyennant des frais.

3.4.1.3 Consultation de dossiers officiels

Autant que possible, on devrait privilégier l'accès électronique direct aux dossiers ou registres protégés du gouvernement par rapport à l'examen de documents sur support papier.

Des vérifications automatisées de chaque demande peuvent contribuer grandement à la détection et à la prévention de la fraude. Parmi les outils automatisés utilisés, mentionnons la vérification en ligne auprès d'organismes possédant des sources primaires comme des dossiers de naissance ou de citoyenneté; des bases de données sur les dossiers de naissance et de décès; des registres de permis commerciaux; des listes électorales; des registres de dossiers de propriété résidentielle; des registres de dossiers de propriété de véhicules motorisés. De telles vérifications contribuent à confirmer la légitimité des documents et à repérer rapidement ceux qui sont frauduleux.

En l'absence de liens électroniques, il est recommandé à l'ADDV de communiquer avec les entités de délivrance de documents primaires ou de base de façon régulière, de façon aléatoire ou en cas de doute, afin de vérifier l'intégrité des documents présentés par les requérants.

3.5 Autres moyens d'établir l'identité des requérants

L'utilisation de plusieurs moyens d'établir l'identité des requérants est recommandée car elle accroît la confiance en la confirmation de leur identité.

3.5.1 Entrevues en personne

Si l'autorité de délivrance de documents de voyage (ADDV) exige que le requérant se présente en personne, ou s'il subsiste des doutes quant à l'intégrité de l'information et de la documentation qu'il a fournie, il peut être utile de l'interviewer. Les agents de l'ADDV devraient avoir la formation requise pour établir à première vue l'identité du requérant, juger ses moyens d'expression et la confiance qu'il inspire. La similarité de l'apparence du physique du requérant et de la photo peut être vérifiée. Les agents de l'ADDV peuvent aussi poser des questions personnelles au requérant afin de vérifier s'il y a des incohérences entre sa demande et les réponses qu'il fournit lors de l'entrevue.

3.5.2 Répondant

À défaut ou dans l'impossibilité d'une entrevue avec un requérant, certains pays utilisent avec succès une méthode qui consiste à accepter que des professionnels (médecins, avocats, etc.) ou d'autres personnes de confiance, comme des membres du clergé, contresignent des demandes pour confirmer l'identité du requérant. Si un professionnel connaît personnellement un requérant depuis de nombreuses années, il peut s'agir d'un moyen efficace d'établir son identité. Les professionnels choisis pour contresigner une demande de document de voyage doivent être membres d'associations reconnues, dont l'adhésion doit pouvoir être vérifiée par l'ADDV. L'inconvénient est qu'il peut être difficile pour une ADDV de suivre à la trace toutes les personnes autorisées à contresigner des demandes de documents de voyage.

Certains pays permettent qu'un requérant puisse recourir à un répondant qui n'est pas membre d'une association professionnelle, mais qui est titulaire d'un document de voyage. Il est alors facile pour l'ADDV de vérifier les renseignements personnels du répondant, puisqu'ils sont contenus dans sa base de données. Un tel répondant doit connaître personnellement le requérant depuis longtemps et accepter d'attester l'identité du requérant par écrit ou sous serment, sous peine de sanction pour parjure.

Le répondant ne doit percevoir aucune rémunération du requérant. Cette politique devrait être inscrite sur tous les formulaires de demande de documents de voyage et devrait porter la signature du répondant. Chaque répondant devrait signer et dater une des photos du requérant pour confirmer qu'elle est une représentation fidèle de l'apparence du requérant.

Pour vérifier la confirmation de l'identité d'un requérant par son répondant, l'ADDV devrait communiquer avec le répondant régulièrement, ou en cas de doute quant à l'identité du requérant. Pour des raisons de sécurité, il n'est pas recommandé que les répondants aient un lien étroit avec les requérants (par exemple, frères ou sœurs, parents ou enfants).

3.5.3 Références

En outre, ou en l'absence d'un répondant, on peut faire appel à des personnes agissant à titre de références personnelles (personnes indépendantes sans lien de parenté avec l'intéressé), qui connaissent le requérant depuis longtemps. Il est recommandé au requérant de recourir à au moins deux connaissances personnelles. L'ADDV pourrait communiquer avec ces personnes pour vérifier l'identité déclarée par le requérant.

3.5.4 Empreinte sociale

L' « empreinte sociale » est une trace que chaque individu laisse dans la collectivité par sa participation à des événements ou ses interactions avec la société dans son ensemble. Même les personnes qui vivent de manière discrète ou sans grande visibilité laissent des marques dans la société. De tels renseignements, qui se dévoilent habituellement sur une longue période et par le biais de sources variées, sont difficiles à falsifier. Dans la mesure du possible, une ADDV devrait chercher à établir les marques laissées dans la société par tout requérant. La technologie facilite de plus en plus l'utilisation de renseignements fiables disponibles pour corroborer le contexte sous-jacent à une identité déclarée, comme les renseignements détenus par les agences d'évaluation du crédit, d'autres renseignements ou dossiers financiers, des renseignements sur le statut de parent, des dossiers médicaux ou scolaires, de l'information sur l'emploi actuel ou des emplois antérieurs, des dossiers d'impôt, de l'information sur le lieu de résidence actuel ou des lieux de résidence antérieurs, etc.

3.5.5 Identificateurs biométriques

Les technologies biométriques confirment les caractéristiques physiques d'une identité déclarée par une personne pour qui des identificateurs biométriques sont utilisés, que cette identité déclarée soit authentique ou non. En fait, l'utilisation de la biométrie établit l'identité singulière d'un individu et restreint sa capacité de voyager ou d'obtenir d'autres documents de voyage de l'État de délivrance en recourant à de multiples identités. L'authentification de l'identité est donc particulièrement importante avant de joindre à cette identité toute information biométrique que ce soit. Lors de la mise en place d'un processus d'inscription des identificateurs biométriques, il est important de garder à l'esprit qu'il devrait y avoir des mesures de protection adéquates pour s'assurer que l'identité de la personne inscrite est établie de manière appropriée et très bien documentée, avant de l'enregistrer définitivement dans une base de données biométriques.

3.5.5.1 Reconnaissance faciale

La technologie de reconnaissance faciale (RF) peut être utilisée par l'ADDV comme moyen d'éliminer la possibilité de demandes présentées par une même personne sous différents noms. Cette technologie peut aussi se révéler très efficace quand elle est utilisée avant la délivrance d'un document en conjonction avec une « liste de surveillance » ou une galerie de personnes « indésirables » ou de fraudeurs connus. La comparaison avec la galerie existante d'images ou de modèles biométriques peut donc empêcher un imposteur potentiel d'obtenir plus d'un document. Comme il a été mentionné au Chapitre 2, pour que cette technologie fonctionne à un niveau optimal, il est important que les images utilisées lors de la demande d'un document satisfassent aux spécifications d'interopérabilité internationale établies par l'OACI.

3.5.5.2 Autres données biométriques

La collecte d'autres données biométriques (empreintes digitales ou iris) peut également faire partie du processus de délivrance. Dans le cas du renouvellement d'une demande de document de voyage, les

données biométriques du requérant peuvent être comparées à celles prélevées antérieurement afin de vérifier si l'identité utilisée est la même.

3.5.6 Vérifications à partir de la base de données

Les requérants devraient faire l'objet d'une vérification fondée sur la base de données de l'ADDV (ou sur les archives à défaut d'une base de données électroniques) pour s'assurer qu'ils n'ont pas obtenu d'autres documents de voyage sous des identités différentes. La base de données doit servir à rechercher des noms ou des orthographes similaires et des données biographiques.

Le système devrait être conçu de manière à pouvoir effectuer deux types de recherches sur les données du requérant : les concordances et les concordances potentielles. Une concordance potentielle a lieu lorsqu' il y a une correspondance étroite entre quelque chose dans la base de données (p. ex. des noms courants) et une entrée.

Les paramètres des systèmes électroniques d'autorisation des noms doivent être configurés de manière à ce qu'ils fournissent des correspondances avec des concordances étroites plutôt que des concordances parfaites. Par exemple, il arrive que des requérants fournissent leur second prénom ou l'initiale de leur second prénom, alors que d'autres requérants ne fournissent ni leur second prénom, ni l'initiale de leur second prénom. Si la base de données cherche à obtenir seulement une forme, l'une ou l'autre des deux autres formes peut faire en sorte que la correspondance n'apparaisse pas dans le système d'acceptation des noms. Certains fraudeurs ont appris à changer leur nom, leur date de naissance, leur numéro d'assurance sociale ou d'autres données cruciales. Il est aussi recommandé d'effacer les anciens noms lorsque des noms ont été changés par suite d'une ordonnance d'un tribunal, d'un mariage, etc.

La translittération des noms de langues ou d'alphabets étrangers suscite des préoccupations. Il importe d'avoir un logiciel de translittération fiable et de grande qualité. L'utilisation d'algorithmes de vérification des noms qui peuvent repérer les caractéristiques de différentes langues et de différents alphabets, et qui sont conçus pour vérifier divers types de noms, améliore la précision de la vérification des noms.

La résolution de la correspondance (y compris l'annulation des correspondances vérifiées) devrait faire partie intégrante du processus de détermination de l'admissibilité ou d'arbitrage. Le système de délivrance devrait être conçu de manière à enregistrer le nom ou le numéro d'identification de l'employé qui annule une correspondance. Un certain nombre de ces annulations devraient être examinées de façon aléatoire par le personnel de supervision. Toutes les vérifications des bases de données devraient être effectuées, les correspondances vérifiées et effacées avant de délivrer le passeport. Pour cette raison, les vérifications des bases de données devraient être terminées le plus tôt possible au cours du processus afin de ne pas retarder la délivrance du passeport.

3.6 Restrictions relatives aux déplacements

Le nom, la date et le lieu de naissance de chaque requérant devraient être vérifiés par rapport à une base de données contenant les noms des personnes qui ne sont pas admissibles à un document de voyage pour diverses raisons — par exemple des individus qui se sont déjà livrés à la fraude de passeport, qui sont recherchés par la police en raison d'activités criminelles, qui ont manqué à leur obligation de verser une pension alimentaire pour enfants, etc. Les données contenues dans cette base devraient provenir des partenaires de l'autorité de délivrance et de divers autres intervenants — comme les organismes de contrôle frontalier, les autorités de l'immigration, les organismes d'application de la loi, les services correctionnels, les fonctionnaires des Affaires étrangères, les agences de sécurité nationale, Interpol et diverses autres sources internationales. D'autre part, si ces renseignements peuvent être vérifiés à l'aide des bases de données des partenaires, il n'est pas nécessaire de les ajouter à la base de données de l'ADDV. La reconnaissance faciale et d'autres applications biométriques peuvent aussi être utilisées par rapport à des bases de données sur les restrictions relatives aux déplacements qui contiennent des photos

ou des identificateurs biométriques d'individus connus ou recherchés. Ces bases de données doivent être mises à jour régulièrement.

3.7 Mesures à prendre lorsqu'on détecte des anomalies

Si l'ADDV détecte des anomalies lors du processus de détermination de l'identité (p. ex. la preuve d'identité ou les renseignements demeurent invérifiées ou certaine forme de fraude est découverte), on devrait enquêter sur ces anomalies avant de poursuivre le processus de délivrance. L'enquête devrait comprendre les procédures suivantes :

- À moins qu'il soit clair qu'il s'agit d'une fraude (qui, en pareil cas, devrait être renvoyée directement au personnel spécialisé chargé des enquêtes), on devrait d'abord chercher à obtenir une explication de la part du requérant. Si cette explication n'est pas satisfaisante, le personnel responsable des enquêtes devrait mener une enquête plus approfondie sur la demande.
- S'il y a une divergence valable qui nécessite la modification ou le remplacement des documents de base ou d'appui, le requérant devrait être redirigé vers l'autorité qui a délivré ces documents.
- Les documents présumés frauduleux devraient être saisis jusqu'à ce que l'identité du requérant soit clairement établie.
- Si l'identité ou les justificatifs d'identité du requérant s'avèrent frauduleux, les détails de la fraude devraient être inscrits dans une base de données où l'on pourra effectuer des recherches lors de demandes futures afin d'empêcher que soient commises d'autres fraudes au moyen de cette identité ou de ces justificatifs d'identité.

4 Traitement du matériel et des livrets vierges

4.1 Sommaire

Le matériel et les documents de voyage vierges comprennent les livrets vierges, les vignettes d'identification, les vignette d'observation et les plastifiés de sécurité. La protection et la gestion sûre des documents de voyage vierges et des matières premières sont essentielles à l'intégrité du programme de production et de délivrance, puisque s'ils sont volés ou perdus, ils peuvent être utilisés pour créer des documents personnalisés contrefaits très convaincants.

L'ADDV devrait se doter de politiques et de procédures documentées liées au traitement du matériel et des livrets vierges. Les renseignements qui se trouvent dans ce chapitre peuvent être utilisés pour élaborer des politiques et des procédures. La conformité aux politiques et aux procédures devrait être étroitement surveillée.

4.2 Production des livrets

Dans de nombreux pays, les livrets des documents de voyage sont produits par une entreprise privée ou un tiers dans des installations indépendantes. L'ADDV devrait s'assurer que les documents vierges sont produits et entreposés dans des installations sûres qui sont conformes aux pratiques exemplaires utilisées pour les zones de sécurité et de haute sécurité (voir le Chapitre 7). Les pratiques de sécurité mises en place pour l'expédition, l'entreposage, la comptabilisation et la destruction doivent être aussi strictes ou rigoureuses dans le cas des documents vierges utilisés par le fabricant que dans le cas des livrets vierges utilisés par l'ADDV.

4.3 Numérotation

Les documents de voyage vierges devraient être produits à l'aide d'un système de numérotation de manière à ce que tout document puisse être reconnu à chacune des étapes du processus de délivrance. Cette exigence est de nature à faciliter la comptabilisation et le suivi pendant que les documents sont produits, expédiés, entreposés et personnalisés. Il est fortement recommandé que le numéro d'un

document vierge soit le numéro attribué au document de voyage pour faciliter le suivi des livrets perdus ou volés. Dans d'autres cas, les dossiers de comptabilisation (numérotation) des documents de voyage devraient être conservés durant leur période de validité, à tout le moins. Le numéro du livret ou du document de voyage devrait apparaître sur chacune des pages intérieures du livret (c.-à-d. imprimé, perforé au laser, etc.), et chaque page devrait être numérotée en séquence (1, 2, 3, 4…). Les documents peuvent également contenir des numéros de version pour en faciliter la vérification. Des techniques de sécurité, telles la perforation au laser pour le numéro du livret et l'encre à séchage ultraviolet (UV) pour les numéros de page, devraient aussi être utilisées afin d'atténuer le risque que le livret soit modifié ou que du matériel soit utilisé pour la création d'un nouveau document. D'autres dispositifs de sécurité peuvent également être utilisés.

4.4 Expédition et entreposage

Le matériel et les livrets vierges devraient être entreposés dans un dépôt hautement sûr, comme une chambre forte ou un coffre-fort, et leur accès devrait être limité à des personnes de confiance ayant un pouvoir de surveillance. L'accès à l'entreposage du matériel et des livrets vierges devrait être limité au plus petit nombre de personnes possible. L'accès à la chambre forte ou au coffre-fort devrait être contrôlé au moyen de cartes d'identité, d'identificateurs biométriques, de mots de passe, etc. Les installations contenant le matériel et les livrets vierges devraient faire l'objet d'une surveillance 24 heures par jour, sept jours par semaine, au moyen d'un système de télévision en circuit fermé. En outre, la zone de sécurité devrait être pourvue de mesures de protection contre les incendies ou d'autres sinistres catastrophiques. Il devrait y avoir des lieux d'entreposage de secours pour assurer le déroulement des opérations en cas de destruction du matériel et de tous les livrets (voir le Chapitre 7).

Lorsqu'ils sont expédiés depuis les installations du fabricant vers l'autorité de délivrance, les documents vierges et les matières consommables devraient être transportés de façon sécuritaire (c.-à-d. dans des véhicules blindés utilisés pour le transfert de fonds et en présence d'agents ou de gardiens de sécurité). Le transport devrait être étroitement surveillé. Aussi, le matériel et tous les livrets devraient pouvoir être retracés et comptabilisés en tout temps. L'expéditeur et le destinataire doivent signer des bordereaux attestant l'expédition et la réception des lots de documents reçus.

La distribution des livrets vierges au personnel de la production devrait être effectuée par au moins deux employés, en vertu du « principe des quatre yeux », avec deux signatures. Les livrets devraient être protégés, même quand ils sont distribués au personnel de la production, et mis sous clé en toute sécurité, peu importe qu'un employé doive s'absenter de son poste de travail pour une courte période (par exemple, lors des pauses-repas). Les livrets vierges non utilisés devraient être retournés au dépôt sûr à la fin de chaque journée ou de chaque quart de travail.

4.5 Comptabilisation

Les numéros de contrôle de stock apposés dans les livrets vierges au moment de la production devraient faire l'objet d'un suivi dès l'expédition des livrets par le fabricant et ce suivi devrait continuer jusqu'à ce que chacun des livrets soit comptabilisé comme document de voyage complété ou comme livret abîmé. Les dossiers de suivi devraient être conservés tout au long de la période de validité des documents de voyage. Cela implique la comptabilisation et l'enregistrement des documents vierges chaque fois qu'ils changent de main, par au moins deux employés.

Les livrets vierges devraient être comptés hors du dépôt verrouillé chaque matin, et les passeports non utilisés devraient y être recomptés chaque nuit, ou à la fin de chaque quart de travail, par deux employés. Le compte réel de documents de voyage vierges devrait faire l'objet d'un rapprochement à la fin de chaque journée pour s'assurer que le compte manuel correspond aux données du système de contrôle automatisé. Si le compte est maintenu à la main, le rapprochement est encore requis. Les dossiers devraient être conservés durant la période de validité des documents, à tout le moins. Ils devraient être inspectés par un tiers chaque jour ou à chaque quart de travail.

Les membres du personnel à qui des documents de voyage vierges sont confiés, et qui ont accès à leur entreposage ou à leur production, devraient faire l'objet d'une vérification chaque fois qu'ils quittent les installations de l'autorité de délivrance, ou faire l'objet de vérifications aléatoires ou ponctuelles, pour s'assurer qu'aucun livret vierge n'a été subtilisé.

4.6 Destruction

La destruction des livrets vierges abîmés, défectueux ou excédentaires, ainsi que des documents de voyage partiellement complétés, devrait se faire en présence de deux membres du personnel responsables, en vertu du « principe des quatre yeux ». La destruction des livrets devrait être faite chaque jour pour éviter une trop grande accumulation. Ces livrets devraient être comptabilisés aux fins de la correspondance à l'inventaire principal.

5 Personnalisation et remise

5.1 Sommaire

La personnalisation d'un document de voyage fait référence aux données variables ajoutées au livret vierge. Dans un passeport, la personnalisation comprend les renseignements personnels du titulaire (y compris sa photo) imprimés sur la page des renseignements et les renseignements encodés dans la puce.

Une fois personnalisé, le document de voyage peut être remis au requérant de diverses façons : retrait en personne seulement (ou remise à un tiers); courrier sûr; ou services de messagerie. Tout dépendant de la méthode ou des méthodes choisies, certaines techniques peuvent être utilisées pour atténuer le risque qu'un document de voyage soit remis à une personne qui se fait passer pour le véritable requérant ou qui utilise une fausse identité.

5.2 Personnalisation

La fonction de personnalisation doit être exécutée dans un endroit hautement sûr, comme une chambre forte, auquel seules des personnes autorisées ont accès. Le contrôle de l'accès à la chambre forte peut être sécurisé au moyen de diverses technologies, comme des cartes d'identité, des identificateurs biométriques, etc. De l'information détaillée est présentée au Chapitre 7.

Puisque le processus de personnalisation requiert la manipulation de matériel et de livrets vierges, toutes les pratiques exemplaires présentées au Chapitre 4 doivent être suivies, y compris la présence de deux personnes tout au long du processus de personnalisation. La transmission des renseignements personnels du requérant à l'imprimeur ou au partenaire responsable de l'encodage doit aussi être protégée par les pratiques exemplaires en matière de sécurité de la TI, comme il est mentionné au Chapitre 8.

5.2.1 Contrôle de la qualité

Une fois personnalisé, le document de voyage doit faire l'objet d'un processus d'assurance de la qualité pour s'assurer qu'il ne contient aucune erreur ou imperfection qui pourrait assujettir son titulaire à des examens minutieux de la part des autorités frontalières lors de ses déplacements.

Dans le cas d'un document de voyage lisible à la machine (DVLM) « régulier », la zone de lecture automatique (ZLA) devrait pouvoir être lue par un lecteur semblable à ceux utilisés aux frontières; les renseignements contenues dans la ZLA devraient pouvoir être comparés à la page de renseignements, aux renseignements personnels sur le requérant contenus dans la base de données de l'autorité de délivrance, ainsi qu'aux formulaires et autres documents à l'appui originaux présentés par le requérant. La page de renseignements devrait aussi être examinée, particulièrement la finition, la couture et la plastification. Quelques dispositifs de sécurité devraient également être vérifiés (au hasard).

Dans le cas d'un document de voyage électronique lisible à la machine (DVELM), les données que contient la puce (y compris la photo) devraient également pouvoir être lues par les lecteurs utilisés aux frontières et comparées aux données contenues dans le document de voyage, la ZLA, la base de données de l'autorité de délivrance et tous les documents présentés par le requérant. La validité et l'intégrité de la signature numérique utilisée pour protéger la puce devraient aussi être vérifiées.

5.3 Remise

5.3.1 Retrait en personne

Il est suggéré que les requérants viennent chercher en personne leur document de voyage nouvellement délivré. Toutefois, cette formule n'est pas toujours pratique pour des raisons qui tiennent à la géographie, ou dans des situations où le retrait en personne pourrait causer une grande affluence aux bureaux. Si le retrait en personne est utilisé, une fiche de retrait peut être fournie au requérant au moment de la demande.

Lors de la remise d'un document de voyage en personne, l'employé devrait comparer la photo apparaissant dans le document de voyage (y compris dans la puce) à celle contenue dans la base de données et au visage du requérant. Pour s'assurer que la personne qui vient chercher le document de voyage en est le titulaire légitime, d'autres techniques peuvent être utilisées : l'employé peut demander au requérant de lui montrer une pièce d'identité supplémentaire avec photo; l'employé peut lui poser des questions personnelles, comme son adresse, le nom de jeune fille de sa mère, etc.; l'employé peut utiliser des identificateurs biométriques (p. ex. technologie de reconnaissance faciale ou empreintes digitales). Le requérant devrait signer un reçu attestant que le document de voyage lui a été remis en main propre (la date et l'heure devraient être précisées), et l'« état du retrait » devrait être indiqué dans la base de données.

Il n'est pas recommandé de permettre la remise d'un document de voyage à un tiers, comme un agent ou un membre de la famille du requérant. Toutefois, si cela est permis, une autorisation écrite devrait être fournie et l'identité de la personne devrait être établie à l'aide de documents d'identité avec photo. Un reçu devrait être signé par la personne à qui le document de voyage est remis.

L'ADDV pourrait utiliser un système d'alerte pour vérifier si le délai normal prévu, une fois qu'un document de voyage est prêt pour le retrait en personne, est expiré. Si le document de voyage n'est pas réclamé au terme d'une certaine période, on devrait entrer en contact avec le requérant. Les cas de documents de voyage non réclamés devraient faire l'objet d'une enquête visant à vérifier s'il n'y a pas fraude.

5.3.2 Service postal

Si un document de voyage personnalisé est livré par la poste au requérant, un service de distribution du courrier fiable est nécessaire. En l'absence d'un service postal public fiable, un autre service de courrier ou un service privé de messagerie peut être utilisé. Dans tous les cas, une signature du requérant ou d'une autre personne vivant à la même adresse devrait être requise lors de la remise d'un document de voyage. La confirmation de la remise devrait être consignée dans la base de données de l'autorité de délivrance. Si le service du courrier ne requiert pas une signature sur réception, d'autres moyens pourraient être envisagés pour confirmer la réception du document de voyage, comme l'envoi d'un mot codé ou d'un reçu à l'autorité de délivrance. Encore une fois, l'ADDV pourrait utiliser un système d'alerte pour confirmer la réception du document de voyage dans la période de temps normale.

Parmi les raisons pour lesquelles un document de voyage expédié n'a pas été reçu par le requérant, mentionnons celles-ci :

- le document a été expédié à une mauvaise adresse par suite d'une erreur de l'autorité de délivrance;
- le document a été perdu par suite d'une erreur de la poste ou du service de messagerie;
- le document a été expédié à une mauvaise adresse par suite d'une erreur du requérant;
- la possibilité d'une fraude.

Le fait qu'un document de voyage ayant été expédié à la bonne adresse soit retourné à l'autorité de délivrance avec la mention « non distribuable » pourrait indiquer la possibilité d'une fraude. Il s'agit alors de vérifier les renseignements contenus dans les formulaires de demande. Si l'adresse est bonne, on devrait entrer en communication avec le requérant, qui viendra chercher son document de voyage en personne. Autrement, le dossier pourrait être transféré aux responsables des enquêtes sur les fraudes.

Si le requérant signale qu'il n'a pas reçu un document de voyage envoyé par l'autorité de délivrance, le cas devrait être traité de la même façon que les documents de voyage perdus ou volés. Le document devrait

être déclaré immédiatement non valide et inscrit dans la base de données des passeports perdus ou volés. Le requérant doit être avisé qu'il ne devrait pas utiliser le document de voyage si ce dernier est trouvé ou reçu subséquemment. Le document devrait être retourné à l'ADDV aux fins de sa destruction en toute sécurité.

6 Sécurité des documents

6.1 Sommaire

Le présent chapitre porte sur les caractéristiques physiques des documents de voyage et les techniques utilisées pour renforcer leur sécurité ou les rendre moins vulnérables aux attaques et aux utilisations abusives. L'accès généralisé à des technologies peu coûteuses, comme la numérisation par balayage de grande qualité, les photocopieurs couleur, le traitement des images et l'impression de photos de qualité, a entraîné une croissance exponentielle de la capacité des individus de produire des documents de voyage contrefaits convaincants et d'apporter des modifications très trompeuses. Voici quelques-unes des menaces physiques aux documents de voyage :

- contrefaçon d'un passeport ou d'un autre document de voyage complet;
- substitution de photo;
- suppression ou modification de texte dans la zone de lecture automatique de la page de renseignements d'un document de voyage lisible à la machine (DVLM);
- création d'un document frauduleux ou de parties frauduleuses d'un document à partir de documents légitimes;
- suppression ou remplacement d'une page ou de pages entières ou de visas;
- suppression d'entrée dans les pages de visas et la vignette d'observation;
- vol et personnalisation de documents vierges authentiques;
- falsification de la puce (le cas échéant) physiquement ou électroniquement.

Le présent document donne un aperçu des principaux développements enregistrés dans la technologie des DVLM, ainsi que des concepts associés à leur sécurité. La sécurité des documents de voyage est largement abordée dans l'« annexe informative » du *document 9303* (volume 1, section III) sur les normes de sécurité pour les documents de voyages lisibles à la machine, intitulée ***Informative Annex of Document 9303 Volume 1 Section III: Security Standards for Machine Readable Travel Documents***.

6.2 Documents de voyage lisibles à la machine (DVLM)

Un document de voyage lisible à la machine (DVLM) contient, dans un format standard, des détails sur l'identité du détenteur, dont une photographie ou une image numérique, ainsi que des éléments d'information obligatoires reproduits dans une zone de lecture automatique (ZLA) de deux lignes imprimées dans en format de reconnaissance optique de caractères. Les spécifications des DVLM sont fournies dans le ***Document 9303*** **(partie 1, volume 1) de l'OACI**.

Ce type de document de voyage a été conçu pour améliorer à la fois l'interopérabilité internationale et la sécurité. Il offre des avantages importants à tous les intervenants, y compris les gouvernements, les transporteurs aériens et les voyageurs, à des coûts relativement peu élevés. La conception uniformisée des DVLM améliore la capacité d'authentification visuelle. Les données normalisées, qui peuvent être lues optiquement, permettent la connexion avec des bases de données et le partage de renseignements avec les divers intervenants en détectant mieux les documents de voyage faux, volés ou frauduleux et, donc, améliorent les processus de contrôle frontalier. Les DVLM simplifient aussi l'utilisation des systèmes d'information préalable sur les voyageurs (IPV).

Les DVLM permettent la saisie automatique des données, ce qui représente une nette amélioration par rapport à la saisie manuelle des données. La saisie des données plus rapide comportant moins d'erreurs

compte parmi les avantages offerts par les DVLM. L'amélioration de la saisie des données, l'interopérabilité internationale et la sécurité apportées par les DVLM ont conduit à l'adoption de la **Norme 3.10 de l'OACI**, qui exige que tous les États membres commencent à délivrer seulement des passeports lisibles à la machine (PLM) à compter du 1er avril 2010, puis à retirer graduellement de la circulation tous les passeports non lisibles à la machine avant le 24 novembre 2015.

Le Groupe de travail sur la mise en œuvre et le renforcement des capacités (ICBWG) a été créé pour aider le secrétariat de l'OACI à réaliser des activités de communication sur le renforcement des capacités afin d'aider les pays à respecter l'échéance de 2010. Les pays qui ont besoin d'aide pour mettre en œuvre leur programme de PLM peuvent communiquer avec le Programme des DVLM du secrétariat de l'OACI.

6.3 Documents de voyage électroniques lisibles à la machine

Les travaux effectués par l'OACI depuis 1998 ont mené à l'élaboration d'une nouvelle génération de documents de voyage : les documents de voyage électroniques lisibles à la machine (DVELM). Un DVELM est un DVLM qui contient un circuit intégré sans contact, dans lequel la page de renseignements du document de voyage et une mesure biométrique du titulaire du passeport sont stockées. Les données encodées dans la puce sont protégées par la technologie cryptographique appelée « infrastructure à clés publiques » (ICP). Les spécifications relatives aux DVELM sont contenues dans le ***Document 9303*** **de l'OACI (partie 1, volume 2)**. Quoique l'OACI ait établi que l'image faciale est l'identificateur biométrique de prédilection pour atteindre l'interopérabilité internationale, les empreintes digitales et l'iris peuvent aussi être utilisés comme identificateurs biométriques secondaires. Le contrôle d'accès de base (CAB) ou le contrôle d'accès élargi (CAE) peuvent servir à protéger les données contre les accès non autorisés.

Les DVELM constituent la plus importante amélioration apportée à la sécurité des documents de voyage depuis l'apparition des DVLM. Ils améliorent l'intégrité des documents de voyage en fournissant la capacité de faire correspondre les renseignements contenues dans la puce aux données imprimées dans le document et aux traits physiques du titulaire (vérification en trois volets). Les DVELM permettent aussi la vérification assistée par la machine des données biométriques et biographiques du voyageur, en indiquant qu'il est le titulaire du document de voyage. Ils permettent aussi de vérifier en même temps les renseignements par rapport à des listes de surveillance ou des bases de données.

Bien qu'ils ne représentent pas la solution miracle à toutes les fraudes, les DVELM offrent une plus grande protection contre les utilisations abusives et la falsification. Ils réduisent également le risque de fraude sur l'identité lors des mouvements frontaliers en permettant une meilleure détection des imposteurs.

La pratique 3.9 recommandée par l'OACI en vertu de l'Annexe 9 de la Convention de Chicago préconise l'intégration, par les États membres de l'OACI, de données biométriques dans leurs passeports lisibles à la machine, visas et autres documents de voyage officiels.

⇒ Pour de plus amples renseignements sur le passeport électronique : *APEC, a Guide to Biometric Technology in MRTDs* (anglais) (http://www.apec.org/apec/publications/free_downloads/2007.html).

Répertoire de clés publiques (RCP) de l'OACI
Une couche de sécurité est ajoutée lorsque l'authenticité des données contenues dans la puce d'un DVELM est validée aux frontières à l'aide de l'infrastructure à clés publiques (ICP). La validation du DVELM est faite pour confirmer que :

- le document du titulaire a été délivré par une autorité de bonne foi;
- les renseignements biographiques et biométriques avalisés dans le document lors de sa délivrance n'ont pas été modifiés par la suite.

Le Répertoire de clés publiques a été créé par l'OACI pour agir en tant que courtier central et gérer l'échange des certificats de l'infrastructure à clés publiques des passeports électroniques et les listes de

révocation. Ce rôle est essentiel pour réduire le volume de certificats échangés entre les pays, garantir des téléchargements en temps opportun et gérer l'adhésion à des normes techniques pour s'assurer que l'interopérabilité est atteinte et maintenue.

En avril 2009, le Conseil de l'OACI a adopté une pratique recommandée liée au RCP de l'OACI (consulter la section 6.4.2 sur les normes et les pratiques recommandées de l'OACI).

⇒ Pour de plus amples renseignements sur le RCP et sur la façon d'en devenir membre (anglais) : http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx.

6.4 Normes de l'OACI, pratiques recommandées et spécifications

6.4.1 Spécifications du Document 9303

Pour atteindre l'interopérabilité internationale et améliorer la sécurité, les documents de voyage doivent être conformes aux spécifications techniques de la partie appropriée du *Document 9303* :

- **Partie 1 :** Passeports lisibles à la machine
  - **Volume 1 —** Passeports contenant des données lisibles à la machine grâce à la technologie de reconnaissance optique des caractères
  - **Volume 2 —** Spécifications pour des passeports électroniques pourvus d'identificateurs biométriques
- **Partie 2 :** Visas lisibles à la machine
- **Partie 3 :** Documents de voyage officiels lisibles à la machine

⇒ *Pour commander le Document 9303 :* http://icaodsu.openface.ca/documentItemView.ch2?ID=7990

Historiquement, le *Document 9303* n'a pas formulé des recommandations propres aux dispositifs de sécurité devant être compris dans les documents de voyage. À partir de ses évaluations des risques, chaque État doit établir la combinaison de dispositifs de sécurité qui répond à ses besoins.

Toutefois, en raison du besoin d'accroître la sécurité des documents, l'OACI a publié un document d'orientation sur les **Normes de sécurité relatives aux documents de voyage lisibles à la machine** sous forme d'**Annexe informative de la Section III du Volume 1 du *Document 9303***. Les recommandations contenues dans ce document couvrent la sécurité du matériel utilisé dans la fabrication des documents, les techniques d'impression de sécurité et de protection contre la copie, ainsi que les processus utilisés dans la production des documents vierges. Afin de prévenir les différentes formes de menaces potentielles à la sécurité des documents de voyage, il est recommandé d'utiliser une combinaison adéquate de ces dispositifs et de ces techniques lors de la production des documents et au moment de leur personnalisation. En dernier ressort, l'autorité de délivrance devrait diriger, et être responsable de l'approbation de la conception des documents de voyage, du choix du matériel utilisé pour les produire et de leurs dispositifs de sécurité.

6.4.2 Normes et pratiques recommandées de l'OACI

Certaines normes et pratiques recommandées contenues au Chapitre 3 de l'Annexe 9 de la Convention de Chicago concernent plus particulièrement la sécurité des documents de voyage. L'ADDV doit se conformer à ces normes et suivre, dans toute la mesure du possible, les pratiques recommandées.

Sécurité des documents

Norme 3.8 — Les États contractants établiront des contrôles sur la création et la délivrance licites des documents de voyage pour se prémunir contre le vol de leurs stocks et le détournement de documents de voyage nouvellement délivrés.

Norme 3.7 — Les États contractants actualiseront régulièrement les caractéristiques de sécurité des nouvelles versions de leurs documents de voyage, pour se prémunir contre leur usage indu et pour faciliter la détection de cas dans lesquels de tels documents ont été illicitement modifiés, reproduits ou délivrés.

Puisque les caractéristiques de sécurité d'un document peuvent être compromises à n'importe quel moment après leur mise en place, une bonne pratique de sécurité consiste à changer la conception de ces dispositifs de sécurité à tous les cinq ans. L'introduction périodique de versions mises à jour et plus sûres des documents de voyage est de nature à entraver le travail des faussaires. Des technologies de pointe et plus sûres devraient être incorporées à chaque nouvelle version d'un document de voyage et communiquées en toute sécurité et en toute confiance aux agents responsables de son examen. Pour favoriser cela, dans chaque document de voyage, il devrait y avoir une mention de la version dans laquelle il a été délivré.

Période de validité des passeports
Norme 3.4 — Les États contractants ne prolongeront pas la période de validité de leurs documents de voyage lisibles à la machine.

Pratique recommandée 3.16 — Il est recommandé que (…) ces passeports aient normalement une durée de validité d'au moins cinq ans (…) Note 1 — Comme les documents ont une durabilité limitée et que l'apparence du titulaire change avec le temps, il est recommandé que la période de validité de ces documents ne dépasse pas dix ans.

Des études démontrent que les dispositifs de sécurité dans un document de voyage commencent à être compromis dans les cinq ans suivant sa délivrance. Il est donc recommandé de remplacer le document après cinq ans. Cependant, le service, le volume et les conséquences financières sont des éléments importants à prendre en considération lors de l'établissement de la période de validité des passeports.

Un passeport, une personne
Norme 3.15 — Les États contractants délivreront un passeport individuel à chaque personne, indépendamment de son âge.

En 2002, l'OACI a adopté la norme « un passeport, une personne » afin de maximiser les avantages des passeports lisibles à la machine et de lutter contre l'enlèvement et la traite des enfants dans le monde.

Passeports lisibles à la machine
Norme 3.10 — Les États contractants commenceront à délivrer uniquement des passeports lisibles à la machine conformément aux spécifications du Doc 9303, 1ère Partie, au plus tard le 1er avril 2010.

Norme 3.10.1 — Les États contractants s'assureront que les passeports délivrés après le 24 novembre 2005, et qui ne sont pas lisibles à la machine, expireront avant le 24 novembre 2015.

Documents de voyage biométriques
Pratique recommandée 3.9 — Les États contractants incorporeront des données biométriques dans leurs passeports lisibles à la machine, visas et autre documents de voyage officiels, en utilisant une ou plusieurs des technologies facultatives de stockage de données pour compléter la zone de lecture automatique, comme le spécifie le Document 9303…

Répertoire des clés publiques de l'OACI
Pratique recommandée 3.9.1 — [Il est recommandé que] Les États contractants (a) qui émettent ou qui ont l'intention d'émettre des passeports électroniques et/ou (b) qui appliquent des mesures de vérification

automatiques aux postes de contrôle frontaliers adhèrent au Répertoire des clés publiques (RCP) de l'OACI.

6.5 Types de documents de voyage

Il est vivement recommandé que des caractéristiques de sécurité minimales (mentionnées à la section 6.4.1 — Doc 9303) soient incorporées dans tous les types de documents de voyage, y compris les passeports diplomatiques, officiels, spéciaux et, tout particulièrement, dans les passeports temporaires ou d'urgence. On devrait utiliser, pour les passeports diplomatiques et les passeports officiels (spéciaux), les mêmes livrets vierges et le même matériel (à l'exception de la couleur de la couverture des livrets) que pour les passeports réguliers.

Les passeports temporaires ou les passeports d'urgence sont délivrés à l'étranger dans des situations d'urgence ou en raison d'exigences en matière de résidence. La validité d'un passeport d'urgence ou d'un passeport temporaire est limitée pour satisfaire aux exigences relatives aux déplacements du requérant qui, la plupart du temps, ne souhaite que revenir dans son pays d'origine. Il est recommandé que ces documents de voyage, qui constituent présentement des risques élevés pour la sécurité, contiennent certains dispositifs de sécurité minimums afin d'éviter la suppression ou la modification des données.

7 Sécurité des installations

7.1 Sommaire

La sécurité des installations (ou la sécurité physique) comprend les moyens utilisés pour prévenir l'accès non autorisé aux installations et aux zones d'accès restreint des individus, à l'interne et à l'externe, et pour protéger les biens et les renseignements. Il existe un grand nombre de stratégies et de technologies pour sécuriser les installations. L'ADDV devrait utiliser une variété de ces dernières jugées appropriées en fonction des menaces, des vulnérabilités, des coûts, de la protection de la vie privée et des inconvénients pour les opérations.

7.2 Politiques en matière de sécurité physique

Une politique détaillée relative à la sécurité physique (ou matérielle) devrait couvrir toutes les installations et tous les lieux utilisés dans le cadre du processus de délivrance des documents de voyage, comme les locaux à bureaux, les zones de production, les aires du service à la clientèle, les salles d'ordinateurs, etc. Cette politique devrait être conforme aux normes et aux lignes directrices nationales et à des normes acceptables à l'échelle internationales.

Bien qu'il s'agisse essentiellement d'une norme de l'Organisation internationale de normalisation (ISO) sur les technologies de l'information, ISO/IEC 27002:2005 — Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information est une référence idéale pour améliorer la sécurité de la gestion de l'information dans les organisations. La norme fournit les pratiques exemplaires recommandées liées, entre autres, à la sécurité physique et environnementale. Elle prévoit des mesures de protection et des contre-mesures en vue de l'atténuation des risques en matière de sécurité ainsi qu'un soutien à la mise en œuvre adéquate du contrôle d'entrée physique, de la sécurisation des salles et des installations, du travail dans une zone protégée, de l'accès public et des zones de livraison et de chargement, lesquels sont tous applicables aux installations de l'ADDV.

La norme ISO 27007 est étroitement liée à la norme ISO/IEC 27001:2005, laquelle fournit des procédures et directives pour concevoir, mettre en œuvre et entretenir un système de gestion de la sécurité de l'information. On peut consulter les deux normes à l'adresse http://www.iso.org/iso/store.htm.

Il est recommandé que toutes les installations d'une autorité de délivrance, ou du moins les zones de sécurité et de haute sécurité (voir le tableau ci-dessous) appartiennent au gouvernement afin qu'on puisse assurer le contrôle complet et la flexibilité de la mise en œuvre des mesures de sécurité physique. Les installations des partenaires publics et privés concernés par le processus de délivrance devraient aussi satisfaire aux normes de sécurité établies par l'ADDV.

Tous les employés devraient recevoir une formation sur les politiques et les pratiques en matière de sécurité physique. Des sanctions devraient être imposées à ceux qui ne les respectent pas, par exemple qui n'escortent pas les visiteurs, qui ne portent pas leur insigne ou qui permettent à des employés non autorisés d'avoir accès à des zones restreintes.

- Voir un exemple de politique en matière de sécurité — *Norme opérationnelle sur la sécurité matérielle (2004)*, à l'adresse Web : http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329.

7.3 Zones de sécurité

Toutes les installations et aires de travail de l'autorité de délivrance devraient être définies comme des zones de sécurité physique dont la protection devrait varier selon la nature des activités qui s'y déroulent, la valeur des biens et l'importance des données stockées :

Zones	Activités ou fonctions	Sécurité physique
Zones d'accès non restreint		
Aire publique	• Autour des installations • Escaliers mécaniques	• Aucun contrôle d'accès • Peut être surveillée pour détecter les activités suspectes
Zone d'accueil	• Aire du service à la clientèle • Endroit où ont lieu les premiers contacts entre les visiteurs et l'organisation	• Accès limité à certains moments de la journée • Détection d'intrus • Zone surveillée aux points d'entrée (personnel de sécurité) • Protection contre la violence reliée au travail • Autres mesures utilisées pour protéger les employés
Zones d'accès restreint		
Zones de travail	• Locaux à bureaux • Traitement des demandes et fonction de détermination de l'admissibilité	• Accès contrôlé • Détection d'intrus • Zone surveillée • Classeurs verrouillés et sûr (pour le travail en cours ou les données)
Zones de sécurité et de haute sécurité	• Personnalisation des documents de voyage • Entreposage des livrets vierges • Aire de manutention d'argent comptant • Salle des réseaux • Entreposage des dossiers des requérants/archives	• Accès contrôlé et hautement restreint • Détection d'intrus • Surveillance 24 heures par jour, sept jours par semaine • Spécifications particulières en matière de sécurité physique (chambre forte ou coffre-fort)

7.3.1 Zone d'accueil (aire du service à la clientèle)

La sécurité physique est nécessaire pour assurer la santé et la sécurité des employés, ou pour les protéger contre la violence liée au travail. Étant donné la nature de la production et de la délivrance des documents de voyage, il se peut que des employés reçoivent des menaces en raison de leurs fonctions ou en raison de situations dans lesquelles ils se trouvent.

L'aire du service à la clientèle, où les gens viennent demander ou chercher des documents de voyage, doit être aménagée de façon à ce qu'ils ne puissent pas avoir facilement accès aux sommes d'argent payées pour les services au nom de la sécurité du personnel et de celle des livrets vierges et du matériel. En cas de problème, la sécurité pourrait ajouter des avertisseurs individuels, des vitres pare-balles, des instruments servant à détecter la présence d'armes sur des visiteurs, etc. Il est recommandé que des

agents de sécurité soient présents dans l'aire du service à la clientèle durant les heures d'ouverture pour calmer les visiteurs qui pourraient être agités et les escorter jusqu'à la sortie, s'ils deviennent turbulents.

Il pourrait y avoir une salle sûre où des agents responsables de l'application de la loi pourraient interroger les fraudeurs pris en flagrant délit lorsqu'ils font une demande de document de voyage ou qu'ils viennent chercher un document de voyage. Il serait préférable, dans certaines circonstances, que ces agents amènent les contrevenants ailleurs pour les interroger.

7.3.2 Traitement des demandes et fonction de détermination de l'admissibilité (zones de travail)

L'accès aux zones de travail devrait être limité aux employés autorisés, et non à tout le personnel. L'accès aux bureaux de traitement des demandes doit être contrôlé et limité aux employés autorisés de par leurs fonctions et qui ont fait l'objet d'une présélection. Des visiteurs ou des fournisseurs peuvent avoir accès à certaines zones, mais ils devraient être escortés en tout temps. Les employés affectés au nettoyage et les gardiens de sécurité doivent aussi être acceptés au contrôle sûr. L'accès des employés aux zones de travail devrait aussi être limité à certains moments (c.-à-d. uniquement durant leurs quarts de travail).

7.3.3 Personnalisation des documents de voyage (zones de sécurité et de haute sécurité)

Les zones de sécurité et de haute sécurité abritent une chambre forte ou un coffre-fort, où le matériel et les livrets vierges sont entreposés, et les documents de voyage sont personnalisés. Leur accès devrait être hautement restreint, ce qui implique l'utilisation de divers moyens de contrôle d'accès. Il est recommandé d'utiliser une authentification à deux facteurs, comme des cartes à puce, des clés électroniques, des numéros d'identification personnelle (NIP) et des identificateurs biométriques. La zone où la personnalisation des documents de voyage a lieu doit être verrouillée de manière sûre à la fin de chaque journée de travail. Des systèmes de surveillance et des dispositifs de détection d'intrus devraient être utilisés pour minimiser les probabilités de vol. Afin de prévenir le vol à l'interne, une politique devrait être mise en place pour empêcher des employés de se retrouver seuls dans des zones de sécurité. Puisqu'un complot impliquant plus d'une personne est plus complexe et requiert une planification très rigoureuse, les probabilités de crimes spontanés sont réduites (voir les Chapitres 4 et 5).

7.4 Contrôle d'accès et surveillance

Le contrôle d'accès est une composante importante de toute approche en matière de sécurité physique. Bien entendu, la capacité d'un tel contrôle de réduire efficacement une menace dépend de la nature de cette menace. Un contrôle d'accès fournit une protection minimale contre les individus ayant déjà accès aux installations. Des contrôles internes, comme ceux présentés au Chapitre 9, devraient donc être mis en place. Un équipement de surveillance et de détection d'intrus se révèle utile pour surveiller à distance des zones à partir desquelles des individus peuvent accéder aux installations, de même que certaines zones qui nécessitent un niveau de sécurité plus élevé.

Il existe diverses méthodes de contrôle d'accès, de détection d'intrus et de surveillance, chacune fournissant différents niveaux de protection à différents coûts. Une combinaison de stratégies et de technologies devrait être utilisée. Une attention particulière devrait être prêtée au degré auquel chaque option perturbe les activités courantes, de même qu'à ses répercussions sur le respect de la vie privée des employés et du public. Le contrôle d'accès devrait favoriser le plus possible l'exécution des activités courantes. Voici certaines stratégies, fondées sur le niveau de sécurité requis et les évaluations des risques, qui pourraient être utilisées dans toutes les installations d'une autorité de délivrance de documents de voyage (ADDV) :

- **Gardiens de sécurité** ayant pour tâches de fournir une sécurité sur place et de surveiller toutes les installations, 24 heures par jour, sept jours par semaine.

- **Insigne d'accès** que chaque employé doit porter en tout temps dans les zones restreintes (zones de travail, de sécurité et de haute sécurité). Chaque insigne devrait comporter une photo claire de son titulaire, ainsi qu'un code de couleur ou un autre code visuel indiquant les privilèges d'accès du titulaire. Les droits d'accès de tout le personnel devraient faire l'objet d'une vérification régulière. Lors d'une cessation d'emploi, l'insigne d'accès de tout employé doit être réclamé par l'organisation. Dès leur arrivée, les visiteurs et les fournisseurs se font remettre par le personnel de sécurité un insigne d'accès temporaire en échange d'une pièce d'identité à photo acceptable. Le personnel s'assure que les visiteurs et les fournisseurs signent un registre en entrant, et leur pièce d'identité ne leur est remise que lorsqu'ils remettent l'insigne d'accès temporaire.

- **Accompagnateurs** — Les visiteurs doivent être accompagnés en tout temps par des employés dans les zones d'accès restreint. Cela s'applique également aux employés de l'ADDV dont l'autorisation de sécurité ou le poste leur interdit l'accès à certaines zones.

- **Obstacles électroniques ou physiques aux point d'entrée** (portes, tourniquets, barrières, etc.).

- **Verrous de sécurité** utilisant des clés de distribution limitée, des numéros d'identification personnelle (NIP), des cartes à puce, des clés électroniques ou des identificateurs biométriques. Les NIP devraient être changés régulièrement. Même durant les heures de travail, les portes extérieures des zones d'accès restreint devraient restées verrouillées et accessibles seulement aux employés ayant les clés, les combinaisons ou les cartes à puce qui permettent de les ouvrir. Les autres qui ont besoin d'entrer dans ces zones devraient être surveillés et admis à l'aide d'écrans à reconnaissance visuelle aux portes et d'un mécanisme de déverrouillage des portes à distance.

- **Détection d'intrus** (alarmes et détecteurs de mouvement).

- **Surveillance** (écrans, caméras et système de télévision en circuit fermé). Les dossiers de la vidéosurveillance devraient être conservés durant des périodes appropriées ou plus de trois mois.

7.5 Autres pratiques de sécurité physique et de protection

Certaines aires ou zones requièrent des mesures de sécurité particulières. Par exemple, les zones de sécurité et de haute sécurité nécessitent des aménagements spéciaux, comme une chambre forte ou un coffre-fort. L'aire du service à la clientèle pourrait exiger un équipement de détection d'armes et des systèmes de protection des employés, comme des vitres pare-balles et des avertisseurs individuels.

Le courrier, y compris les demandes de documents de voyage et le matériel reçu, devrait être inspecté dans une salle de courrier bien située. Les employés de la salle de courrier devraient recevoir une formation pour inspecter les documents suspects à l'aide de rayons X ou d'autres méthodes et mettre en marche un protocole, lorsqu'ils détectent un colis suspect.

La protection des installations, des biens et des données contre l'incendie et d'autres sinistres catastrophiques devrait également être prise en considération. Des dispositions pour occuper d'autres lieux et utiliser des lieux d'entreposage de secours devraient être mises en place pour assurer la continuité des opérations, si les installations de délivrance n'étaient pas accessibles ou si des données ou des documents étaient détruits.

L'information organisationnelle et les renseignements personnels des requérants doivent être protégés. L'utilisation de classeurs sûrs et verrouillés et de salles protégées est requise pour stocker et protéger l'information. Lorsque les renseignements ne sont plus requis, ils devraient être déchiquetés ou détruits à l'aide d'un appareil de destruction de documents (voir le Chapitre 2).

8 Sécurité des technologies de l'information

8.1 Sommaire

La sécurité des technologies de l'information (STI) est l'ensemble des mesures prises pour préserver la confidentialité, l'intégrité, l'accessibilité, l'utilisation envisagée et la valeur des renseignements stockés, traités ou transmis électroniquement. Par le passé, il était possible de protéger les renseignements en contrôlant simplement leur accès physique. Aujourd'hui, à l'heure des réseaux, la protection des données constitue un défi de taille, puisque beaucoup de renseignements confidentiels sont stockés dans des réseaux de systèmes informatiques souvent interconnectés.

Cette question est préoccupante pour les ADDV, qui sont devenues de plus en plus automatisées et qui recourent aux technologies de l'information (TI) afin d'améliorer l'efficacité, la sécurité et la prestation de leurs services. Parallèlement, le nombre et la gravité potentielle des menaces, la vulnérabilité des mesures mises en place et les incidents augmentent sans cesse. Puisqu'une ADDV doit recueillir divers renseignements personnels détaillés, parfois même des données biométriques, la protection et la sécurité des systèmes de TI et des bases de données sont cruciales.

8.2 Politiques et pratiques en matière de STI

Une politique détaillée en matière de STI devrait être mise en place, qui serait en phase avec les technologies et les pratiques actuelles et engloberait tous les systèmes de TI, les bases de données, le flux de l'information, etc. Cette politique devrait se fonder sur des normes internationales et les incorporer, comme la norme ISO/IEC 27002:2005 — Technologie de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information : http://www.iso.org/iso/store.htm (voir chapitre 7).

Cette norme ISO fournit une ligne directrice pour élaborer des normes de sécurité et des pratiques de gestion de la sécurité concernant toutes les formes d'information. Les politiques et pratiques de sécurité jouent un rôle majeur dans cette norme, laquelle traite de l'ensemble des aspects de la gestion de la sécurité. Elle est divisée en onze secteurs de gestion, allant de la gestion des politiques de sécurité jusqu'à la gestion de la continuité des opérations.

Les évaluations, qui permettent d'identifier les risques et les besoins de protection, constituent l'un des éléments importants de cette norme. Elles comprennent les évaluations de la vulnérabilité du système, de la confidentialité des données de la TI, de la perte de renseignements dans les bases de données, de l'accès à des données non autorisées, et toutes les autres évaluations connexes qui devraient être effectuées régulièrement pour mettre en œuvre des mesures de protection de la sécurité, de prévention et d'atténuation des risques.

Les politiques et les pratiques en matière de STI devraient porter sur les éléments suivants :

- Des classifications appropriées de la **confidentialité** des bases de données et de l'information connexe, comme des listes de surveillance, des données biométriques et d'autres produits d'information. Des moyens technologiques et autres devraient être mis en place pour éviter que des individus non autorisés aient accès à ces renseignements, les interceptent, les copient ou les obtiennent électroniquement.
- La **protection appropriée de l'intégrité des données** des bases de données et de l'information connexe, de manière à ce que ces renseignements ne puissent pas être modifiés ou supprimés, sauf en conformité avec des processus définis adéquatement.
- L'**accessibilité appropriée des données** des bases de données et de l'information connexe, de manière à ce que ces renseignements ne puissent pas être bloqués ou cachés aux utilisateurs légitimes, quand elles sont requises.
- Un **permis approprié d'accès** aux bases de données et à l'information connexe, de manière à ce que ces renseignements ne puissent être accessibles qu'aux **utilisateurs visés autorisés**.

L'efficacité et le rendement de toutes ces politiques, pratiques, technologies et méthodologies devraient avoir été évalués par des vérificateurs professionnels de la TI.

Tous les produits de la technologie, comme les progiciels de bases de données, les serveurs, les installations de communication, les modules matériels de sécurité et les autres produits commerciaux utilisés, devraient être certifiés à un niveau d'assurance EAL (*Evaluation Assurance Level*) approprié. Les dispositifs de cryptographie utilisés devraient être certifiés au niveau approprié à l'aide de normes internationales, comme la norme FIPS 140-2 ou une norme équivalente.

8.3 Sécurité des utilisateurs

8.3.1 Contrôle d'accès

L'accès au système de technologie de l'information et aux bases de données de l'autorité de délivrance doit être restreint. L'accès à l'équipement devrait être limité au moyen d'identificateurs biométriques, de noms d'usagers et de mots de passe uniques permettant aux employés autorisés d'ouvrir des sessions dans le système. Tous les individus devraient être limités par des permissions d'accès et de traitement à certaines bases de données, applications et tâches. Les mots de passe utilisés devraient être composés de chiffres et de lettres aléatoires qui ne peuvent pas être devinés. Par exemple, les dates d'anniversaire et les noms des parents ne devraient pas être utilisés, parce qu'ils pourraient être connus. Les ouvertures de session et les mots de passe devraient être changés régulièrement par le système. Toutes les ouvertures de session devraient être fermées automatiquement après de courtes périodes d'inactivité et nécessiter automatiquement une nouvelle procédure d'entrée en communication de la part de l'utilisateur. Les droits d'accès des employés devraient être évalués de façon régulière et les comptes des TI des personnes qui ne travaillent plus pour l'ADDV devraient être annulés immédiatement. Le système devrait empêcher l'accès aux employés en dehors des heures de travail normales sans la permission du superviseur.

L'équipement devrait être pourvu d'un mécanisme de surveillance et d'historique d'expertise permettant de savoir quels utilisateurs ont accédé au système et quels renseignements ils ont consultés. Les dossiers informatisés des ouvertures de session devraient être conservés durant une période de temps raisonnable. Ces dossiers devraient être examinés par le personnel de gestion pour établir les irrégularités dans l'accès aux ordinateurs, et tout accès injustifié devrait faire l'objet d'une sanction précise. Cela est encore plus important dans le cas des dossiers des personnalités de marque. L'organisation doit rappeler régulièrement à ses employés de la STI leurs responsabilités et leur offrir une formation. En cas d'incident de sécurité lié à la TI, une enquête devrait être menée et des sanctions imposées, s'il est prouvé qu'il y a eu faute professionnelle ou négligence.

8.3.2 Utilisation d'Internet et du courrier électronique

L'accès à Internet devrait être refusé au personnel ou aux fournisseurs à partir de n'importe quel ordinateur ou terminal d'utilisateur dans le cadre du processus de délivrance des documents de voyage. De tels appareils devraient être séparés physiquement et technologiquement : ils devraient être utilisés soit pour le traitement des demandes de documents de voyage, soit pour le courrier électronique interne et externe ou pour Internet.

Un programme devrait être mis en place pour surveiller, de manière aléatoire mais régulière, les courriels et l'accès aux applications Internet par tous les employés et les fournisseurs afin de détecter les questions ou les communications qui pourraient être préoccupantes. Ce processus devrait être très bien protégé par des politiques et des pratiques internes strictes en matière de respect de la vie privée, de manière à ce que les renseignements personnels anodins appris lors de la surveillance ne soient jamais divulgués pour

quelque raison que ce soit. Tous les renseignements découlant de cette surveillance, qui ne présentent aucun intérêt sur le plan de la sécurité, devraient être régulièrement supprimés des dossiers.

8.4 Personnel responsable de la TI

Le personnel de la TI devrait avoir des droits d'accès spéciaux pour entrer dans les installations de TI, comme les salles d'équipement informatique, les bases de données, les réseaux, les installations de communication et les centres auxiliaires. Ces privilèges d'accès devraient exiger l'utilisation d'une authentification à deux facteurs et la présence en tout temps de deux individus autorisés ou plus.

On ne devrait pas confier à une seule personne toutes les responsabilités associées à un système de TI, car cela rendrait le système vulnérable aux utilisations abusives non détectées. Les responsabilités devraient être partagées et définies clairement. L'infrastructure de TI devrait être établie de manière à ce que personne, peu importe son niveau hiérarchique, n'ait le droit d'annuler des politiques ou des pratiques, de prendre des décisions arbitraires, de faire des copies de bases de données ou d'autres fichiers d'information, ou ne puisse, de quelque façon que ce soit, compromettre le système de délivrance des documents de voyage et ses renseignements confidentiels.

Le personnel de la TI devrait se faire rappeler régulièrement les politiques en matière de sécurité. Des examens et des vérifications devraient être menés régulièrement, et des sanctions devraient être imposées, s'il est prouvé qu'il y a eu faute professionnelle ou négligence.

9 Protéger et promouvoir l'intégrité du personnel et de l'organisation

9.1 Sommaire

Pour assurer la prestation de ses services à la population, l'ADDV dépend des actes, de la fiabilité et des décisions de son personnel. Ces éléments dont il dépend constituent aussi des vulnérabilités. Il est donc d'une importance capitale pour l'ADDV d'avoir des employés compétents et fiables ou dignes de confiance. L'authenticité des documents de voyage dépend de l'intégrité des individus qui les délivrent, et un programme efficace de sécurité du personnel est nécessaire pour assurer la plus haute intégrité dans le processus de délivrance des documents de voyage.

La satisfaction des employés, l'organisation du travail et les contrôles internes ont une grande incidence sur la prévention et la détection des fraudes à l'interne. Si une fraude est soupçonnée ou détectée, des mécanismes doivent être mis en place pour mener une enquête interne et, le cas échéant, imposer des sanctions.

Le *Western Australia Corruption and Crime Commission's Misconduct Resistance Integration Guide (*Guide d'intégration sur la résistance à la mauvaise conduite de la Commission sur le crime et la corruption de l'Australie occidentale) est une référence utile : http://www.ccc.wa.gov.au/pdfs/CCC-MR-GUIDE.pdf.

9.2 Autorisations de sécurité et séances d'information en matière de sécurité

9.2.1 Vérifications des antécédents et de la fiabilité

L'autorité de délivrance doit s'assurer que les individus qui ont accès aux installations et aux systèmes de délivrance sont fiables. Cette démarche débute bien avant l'embauche des employés : l'organisation doit d'abord vérifier que chaque candidat à un poste est fiable et non susceptible à la corruption. Avant d'embaucher un employé, l'ADDV doit procéder à des vérifications de ses antécédents et de sa fiabilité.

Les fournisseurs devraient également faire l'objet de telles vérifications. L'étendue des enquêtes devrait dépendre du poste occupé, des responsabilités assumées, de l'accès au système et du niveau de prise de décisions du candidat. Un niveau de sécurité doit être attribué à chaque poste, et l'employé qui occupe le poste doit avoir obtenu avec succès une habilitation ou une autorisation de sécurité à ce niveau.

Les vérifications doivent être réalisées en collaboration avec les organismes d'application de la loi, la police ou des agences de sécurité nationale. En ce qui concerne les postes d'un niveau de sécurité élevé, comme des postes de gestion et d'autres postes qui nécessitent des décisions quant à l'admissibilité des documents de voyage, les vérifications devraient être plus approfondies. Elles pourraient comprendre des entrevues avec des membres de la famille des candidats, des amis et des employeurs précédents, de même qu'un examen des antécédents financiers (pour éviter le risque d'une vulnérabilité financière). Il est recommandé que les responsables de la détermination de l'admissibilité soient des citoyens du pays.

La culture et les traditions des candidats devraient toujours être examinées pour s'assurer qu'elles n'annulent ou ne contournent ni la probité entourant les vérifications des antécédents et de la fiabilité, ni l'embauche de tout individu.

9.2.2 Contrôles de sécurité réguliers et vigilance constante

Des dettes difficiles à rembourser peuvent rendre des employés vulnérables à la corruption. L'avidité ne constitue qu'un des motifs qui puissent inciter des employés à commettre une fraude. Il est recommandé de surveiller attentivement les signes pouvant indiquer qu'un employé « vit au-dessus de ses moyens ». Les gestionnaires doivent rester vigilants, une fois qu'une habilitation de sécurité est accordée, et être à l'écoute de toute nouvelle information pouvant remettre en question la fiabilité ou la loyauté d'un individu. Les vérifications de sécurité des employés devraient être effectuées régulièrement selon un horaire préétabli durant la période d'emploi. Bien qu'il n'y ait pas un mécanisme définitif permettant d'évaluer le potentiel de faute de commission ou de méfait d'un employé, des vérifications périodiques peuvent mettre en lumière certains risques à la sécurité.

9.2.3 Obstacles aux risques d'opportunisme

Une autre menace qu'il faut garder à l'esprit est que des employés n'ayant aucun casier judiciaire connu, ou qui sont en apparence au-dessus de tout soupçon, peuvent obtenir facilement des habilitations de sécurité régulières, mais cela ne garantit pas qu'ils demeurent fiables. Il peut arriver que des employés soient sujets à diverses pressions extérieures qui les amènent à commettre des actes frauduleux. Il importe donc de limiter les risques d'opportunisme et de s'assurer de la fiabilité et de la loyauté indéfectibles des employés. Pour décourager et découvrir les fautes de commission parmi le personnel, il convient de délimiter les zones de sécurité et d'instaurer des contrôles internes qui limitent l'autorité des employés, à la fois matériellement et électroniquement. Cela s'applique aussi aux employés des partenaires qui participent à la production et à la délivrance des documents de voyage et des documents d'identité. Il est important de noter qu'une habilitation de sécurité ne confère pas en soi à son titulaire le droit d'accéder à des renseignements protégés ou à des zones de sécurité. Même les individus ayant une autorisation de sécurité ne devraient pas avoir accès à une zone de sécurité ou à des données protégées, sauf si leurs fonctions requièrent un tel accès. En limitant le nombre d'employés autorisés à accéder à des zones de sécurité, on réduit ainsi les risques d'opportunisme.

9.2.4 Personnel temporaire

Beaucoup d'autorités de délivrance embauchent des employés temporaires durant les périodes de pointe, ce qui représente une importante menace à la sécurité, s'ils ne sont pas évalués adéquatement en raison de contraintes de temps. Il est donc crucial que les employés temporaires soient soumis aux mêmes vérifications des antécédents que les employés permanents. L'ADDV devrait maintenir un bassin d'employés temporaires, dont les antécédents ont été préalablement vérifiés, en cas de surcharge de

travail ou dans des situations de manque de personnel (voir le Chapitre 1).

9.2.5 Sensibilisation à la sécurité et codes de conduite

Lorsqu'un nouvel employé ou un fournisseur se présente au travail, il doit recevoir des directives orales sur la sécurité et des lignes directrices écrites sur les contrôles internes et les politiques en matière de sécurité en vigueur. Tous les nouveaux employés et les fournisseurs doivent connaître leurs privilèges d'accès et les interdictions associées à leur niveau d'habilitation de sécurité. Dès leur première journée de travail et aussi longtemps qu'ils travaillent pour l'ADDV, les employés doivent participer à des séances régulières d'information et de formation visant à maintenir leur sensibilisation à l'égard de la sécurité (Chapitre 1).

Dès leur entrée en fonctions, les employés devraient recevoir de l'information sur les normes de conduite et les valeurs de l'organisation. Ces lignes directrices communiquent les actes et les comportements que l'autorité de délivrance considère comme acceptables ou inacceptables. Elles contiennent des clauses sur les conflits d'intérêt, notamment sur l'interdiction pour les employés d'accepter des cadeaux ou des pourboires de la part de fournisseurs qui font affaire ou cherchent à faire affaire avec l'ADDV, ou de la part de demandeurs de documents de voyage, alors qu'ils ne font qu'exécuter normalement leurs tâches, ou alors qu'on s'attend à recevoir des faveurs particulières de leur part. Les employés devraient avoir tout le temps nécessaire pour lire ces lignes directrices et poser des questions. Les gestionnaires devraient s'assurer que les employés comprennent les lignes directrices et les inviter à signer une lettre dans laquelle ils reconnaissent les avoir reçues et comprises.

9.3 Organisation du travail

9.3.1 Répartition des tâches

Les fonctions professionnelles doivent être établies de telle sorte qu'un employé ne puisse pas accomplir toutes les tâches associées à la détermination de l'admissibilité et à la délivrance des documents de voyage. Cela signifie que plusieurs employés participent à la délivrance d'un document de voyage à un individu qui souhaiterait l'acheter ou l'obtenir au moyen de la subversion. Puisqu'il est plus difficile de se livrer avec succès à un méfait en groupe qu'individuellement, l'autorité de délivrance a plus de chances de découvrir une conspiration impliquant plusieurs employés que des fautes de commission d'employés agissant seuls.

9.3.2 Délégation aléatoire des tâches

Afin de réduire la possibilité de méfaits à l'interne, il est recommandé que les procédures de déroulement du travail empêchent un requérant de choisir l'employé à qui il souhaiterait présenter sa demande. Par exemple, quand plus d'un employé accepte des demandes de documents de voyage en même temps, le déroulement du travail et le flux des requérants devraient être tels que les choses se passent ainsi : tous les guichets au comptoir s'alimentent à partir d'une seule et même file d'attente, et le préposé au premier guichet qui se libère demande au requérant suivant, le premier dans la file d'attente, de venir lui présenter sa demande. Ainsi, les requérants n'ont pas le loisir de choisir un employé en particulier en étant dans une file d'attente donnant accès au guichet de cet employé.

Le même principe s'applique à la détermination de l'admissibilité du travail. Le travail devrait être distribué aux employés selon leur disponibilité dans l'ordre des tâches à accomplir. Cela réduit la possibilité que des membres du personnel puissent avoir accès ou traiter des demandes en particulier. Pour la même raison, il devrait y avoir une rotation du personnel entre les différentes fonctions — p. ex. traiter avec le public, la détermination de l'admissibilité des demandes acheminées par la poste en vue de leur traitement, la saisie de données, la vérification de documents de base, etc.

Les employés et les gestionnaires ne doivent pas traiter ou approuver des demandes provenant de connaissances, d'amis ou de membres de leur famille. Une méthode visant à accélérer les dossiers des demandes ne devrait être permise que dans des situations exceptionnelles (par exemple, dans le cas des personnalités de marque). Ces services exceptionnels devraient être documentés minutieusement et supervisés par un cadre supérieur qui ne pourrait pas agir seul dans le processus de délivrance de tout document de voyage.

9.3.3 Transparence du processus

La transparence est essentielle à toutes les étapes du processus de délivrance. Il importe d'enregistrer toutes les décisions cruciales prises durant le processus de délivrance, même pendant les arriérés dus à la surcharge de travail. Des annotations adéquates dans les dossiers des demandes et les bases de données relativement aux preuves reçues ou aux mesures prises doivent pouvoir justifier toutes les décisions prises par le personnel responsable de la détermination de l'admissibilité. Grâce à des justifications écrites adéquates, les mesures prises pourront être examinées plus tard lors de vérifications aléatoires, ou si des questions se posent quant aux raisons pour lesquelles une décision a été prise dans le dossier d'une demande en particulier. Les procédures claires relatives aux annotations devraient faire partie d'un programme de formation.

9.4 Moral des employés [Satisfaction au travail]

Toute ADDV ferait bien de prêter attention au moral de ses employés. Des employés au moral élevé se sentent valorisés parce que leur contribution est appréciée, sont plus productifs ou plus efficaces et éprouvent un sentiment de loyauté à l'égard de l'organisation au sein de laquelle ils travaillent. Par contre, des employés malheureux peuvent devenir vulnérables et risquent davantage de répondre positivement à une invitation à participer à un méfait.

Le moyen le plus efficace de lutter contre les méfaits à l'interne est de bâtir un sentiment d'estime de soi et de fierté parmi les employés à l'égard de leurs accomplissements au sein de l'organisation. La satisfaction au travail est un des facteurs les plus déterminants pour obtenir la loyauté des employés. Divers éléments influent sur le moral des employés ou sur leur satisfaction au travail, entre autres :

- un contrat écrit;
- une paie régulière ou garantie;
- une équité salariale;
- des conditions de travail raisonnables;
- un milieu exempt de conflits;
- une bonne supervision, une bonne gestion et de bonnes communications;
- une participation aux décisions;
- des possibilités de formation et d'expériences pour obtenir des promotions;
- des absences autorisées et d'autres avantages liés à l'emploi;
- la possibilité de formuler des griefs auxquels l'organisation se montre réceptive.

Ce sont là les meilleures pratiques de gestion pour toutes les organisations, à plus forte raison pour celles dont le mandat et les activités peuvent avoir des répercussions sur la sécurité nationale et internationale. Les ressources financières et le temps consacrés à la formation des superviseurs et des gestionnaires, pour les aider à acquérir de bonnes compétences en leadership et de bonnes pratiques de gestion, sont de précieux investissements dont on ne soulignera jamais assez l'importance. Des gestionnaires compétents peuvent à la fois améliorer la productivité et dissuader les employés de participer à une fraude à l'interne.

Le climat de travail doit refléter le fait que l'organisation se soucie réellement de ses employés et de leur travail. Les systèmes de reconnaissance des employés y sont pour beaucoup. On peut reconnaître leurs efforts, leur rendement et leur contribution de diverses manières : une appréciation publique et organisationnelle, des prix ou des récompenses, des congés payés, etc.

Une bonne façon pour les cadres supérieurs de mesurer la satisfaction des employés et de repérer les situations problématiques consiste à mener régulièrement des enquêtes ou des sondages et d'analyser les résultats. Cette pratique fournit également aux employés l'occasion d'exprimer, en toute confidentialité, leur niveau de satisfaction à l'égard de leur travail et de donner leurs points de vue sur les pratiques de gestion mises de l'avant par l'organisation.

9.5 Enquêtes internes et sanctions

9.5.1 Signalement des incidents de sécurité

Il est important de rappeler périodiquement aux employés l'importance de rester aux aguets et de prêter attention aux infractions commises par un employé et à la fraude interne, y compris le vol de documents, de matériel et d'argent. On devrait exiger des employés qu'ils signalent tout incident ou toute menace. Les employés devraient également être encouragés à informer la direction chaque fois qu'une personne les incite à commettre une fraude.

L'ADDV devrait avoir une politique documentée concernant le signalement des incidents de sécurité, laquelle exige que tous les incidents soient signalés, plus particulièrement ceux liés à l'inconduite et à la négligence. Cette politique devrait également exposer les responsabilités des employés et de la direction en ce qui a trait au traitement des rapports. Les procédures liées au signalement des incidents devraient refléter l'obligation de documenter tous les incidents. Elles devraient comprendre des directives claires sur la façon de traiter les rapports, y compris des orientations quant à l'organisation responsable des enquêtes ou l'unité appropriée de l'ADDV, distincte des opérations, à laquelle on devrait les acheminer. Selon la nature et la gravité de l'incident, les enquêtes peuvent être de nature administrative ou criminelle. Les rapports devraient demeurer confidentiels. L'employé qui fait une telle déclaration doit être protégé contre toute réaction négative, peu importe la nature de la violation alléguée ou la personne soupçonnée.

Grâce à des méthodes efficaces d'enquête et de signalement des incidents, les points vulnérables peuvent être repérés et le risque qu'un incident se reproduise peut diminuer.

9.5.2 Enquêtes

Une législation rigoureuse devrait stipuler clairement quel est l'organisme gouvernemental ayant la responsabilité de faire enquête dans les cas de fraude de documents de voyage. Il arrive souvent que la responsabilité soit partagée : un organisme peut être responsable des fraudes à l'externe, et un autre, responsable des fraudes à l'interne. Quoi qu'il en soit, il est primordial que le directeur de l'autorité de délivrance rencontre régulièrement les responsables des enquêtes sur les fraudes, pour être informé des enquêtes en cours et s'assurer que l'ADDV collabore pleinement aux enquêtes.

Les conclusions des enquêteurs sur les fraudes à l'interne devraient être transmises à l'ADDV, y compris la nature de la fraude, la façon dont elle a été commise et les améliorations qui pourraient être apportées pour empêcher que de tels événements se reproduisent. Tout cela est important parce que l'ADDV doit tirer des leçons de chaque cas de fraude à l'interne et prendre rapidement des mesures correctrices pour prévenir toute récurrence.

9.5.3 Sanctions

L'autorité de délivrance doit s'assurer qu'il existe des lois adéquates permettant de porter des accusations et de poursuivre les employés soupçonnés de fraude, et que ces lois prévoient des sanctions ou des peines graves. Des sanctions devraient aussi être prévues pour les incidents de sécurité dans les cas de mauvaise conduite ou de négligence.

Les individus cernés par les enquêteurs comme ayant commis une fraude à l'interne devraient être congédiés et perdre leurs avantages, que la fraude soit majeure ou mineure. En commettant un acte frauduleux, indépendamment de sa nature, un employé enfreint délibérément les règles. S'il y a lieu, il devrait être poursuivi en justice dans la mesure autorisée par la loi, y compris au criminel.

L'autorité de délivrance devrait insister pour que les peines soient importantes non seulement en tant que mesures punitives, mais aussi en tant qu'éléments dissuasifs qui indiquent aux employés, de manière non équivoque, que toute participation à une fraude à l'interne ne sera pas tolérée et que les sanctions seront lourdes. Les résultats de chaque enquête (déclaration de culpabilité, renvoi ou démission) devraient être rendus publics pour que les employés qui auraient pu se sentir trahis par leur ancien collègue de travail sachent que cette personne a été punie, comme il se devait.

10 Documents de voyage perdus et volés

10.1 Sommaire

L'utilisation abusive de documents de voyage authentiques obtenus dans des circonstances illicites crée des risques importants pour la sécurité nationale et nécessite la mise en place de mesures correctrices. Qu'ils soient modifiés ou laissés intacts et utilisés par des imposteurs, ces documents peuvent, s'ils ne sont pas détectés, permettre à des terroristes, à des criminels ou à des migrants en situation irrégulière de voyager pratiquement incognitos.

En dépit de tous les efforts déployés en matière de sécurité, des pertes et des vols de documents de voyage se produisent dans chaque pays. Ces documents de voyage peuvent être volés isolément ou plusieurs à la fois. De même, il peut s'agir de livrets vierges ou de documents dûment personnalisés. Le résultat est qu'il peut y avoir un nombre élevé de documents de voyage perdus, volés ou annulés en circulation, utilisés par des personnes qui n'en sont pas les titulaires légitimes. Dans certains cas, des documents de voyage sont déclarés perdus ou volés, mais ils continuent d'être utilisés par leurs titulaires légitimes, après avoir été retrouvés.

Des mesures de prévention doivent être prises pour réduire le nombre de documents de voyage perdus et volés. Une fois que des documents de voyage sont déclarés perdus ou volés, des mesures d'atténuation peuvent réduire les risques qu'ils posent pour la sécurité.

10.2 Mesures de prévention

Parmi les mesures de prévention visant à limiter le nombre de documents de voyage perdus ou volés, on peut citer : les techniques de sensibilisation du public, visant à encourager les gens à prendre soin de leurs documents de voyage et à déclarer immédiatement leur perte ou leur vol; l'adoption de politiques plus strictes dans les cas où des demandeurs de documents de voyage ont un antécédent de documents perdus ou volés.

10.2.1 Sensibilisation du public

10.2.1.1 Mise en lieu sûr d'un document de voyage

L'ADDV devrait élaborer et mettre en œuvre une stratégie de communication afin d'encourager les gens à prendre soin de leurs documents de voyage, en les mettant en lieu sûr ou en les protégeant du vol en tout temps. Les campagnes de sensibilisation du public sont utiles pour informer les citoyens et leur expliquer que le remplacement des documents de voyage est une démarche difficile et onéreuse. Les autorités de délivrance devraient s'assurer que les titulaires de documents de voyage sont bien informés de leurs responsabilités et des conséquences possibles de la perte ou du vol de leurs documents.

10.2.1.2 Déclaration d'un document de voyage perdu ou volé

Des stratégies de sensibilisation du public devraient être utilisées pour informer les gens sur ce qu'ils devraient faire, si leurs documents de voyage sont perdus ou volés. Les gens devraient savoir qu'ils ont l'obligation de déclarer à l'autorité de délivrance, à la police ou à un organisme d'application de la loi, la perte ou le vol d'un document de voyage aussitôt qu'ils en font la découverte.

Des moyens simples de déclarer des documents de voyage perdus ou volés devraient être mis en place, et les gens devraient pouvoir y recourir facilement (p. ex. en utilisant une ligne téléphonique sans frais, un numéro de télécopieur, en ligne ou en personne). Les citoyens qui perdent leur passeport à l'étranger devraient avoir accès facilement à des conseils. Une fois qu'il a été déclaré perdu ou volé, un document de voyage est annulé, n'est plus valide et ne doit plus être utilisé pour voyager. Une nouvelle demande pour remplacer le document sera nécessaire. Si le document est retrouvé par la suite, il ne peut pas être validé à nouveau; le titulaire doit le retourner à l'autorité de délivrance qui en fera l'annulation physique ou la destruction.

Quand un passeport est déclaré perdu ou volé, un rapport doit être rempli par la personne qui a fait la déclaration de perte ou de vol, et l'autorité de délivrance doit s'assurer que les questions posées permettent d'établir que cette personne est, sans l'ombre d'un doute, le titulaire légitime du document.

Dans certains pays, ne pas déclarer la perte ou le vol d'un passeport le plus tôt possible est une infraction, tout comme le fait d'utiliser un passeport annulé pour voyager, même s'il s'agit du titulaire.

Exemples d'outils de sensibilisation du public à l'égard de la déclaration des documents de voyage déclarés perdus ou volés

- États-Unis : http://travel.state.gov/passport/lost/us/us_848.html
- Canada : http://www.ppt.gc.ca/planification/203.aspx?lang=fra
- Australie : https://www.passports.gov.au/Web/LostStolenInfo.aspx
- Nouvelle-Zélande : http://www.passports.govt.nz/diawebsite.nsf/wpg_URL/Services-Passports-Lost-or-Stolen-Passports

10.2.2 Politiques plus strictes à l'égard des nouvelles demandes

L'adoption de politiques plus strictes à l'égard des demandeurs qui ont un antécédent de documents voyage perdus ou volés incite les titulaires à bien prendre soin de leurs documents. Les mesures recommandées comprennent — sans toutefois s'y limiter — les suivantes :

- le requérant devrait être considéré comme un nouveau requérant de document de voyage (lorsque le pays possède également un processus de renouvellement simplifié);
- l'obligation de se présenter en personne lors de la demande de passeport de remplacement;
- une entrevue personnelle;
- des frais de remplacement élevés;
- la mention obligatoire sur le document indiquant qu'il s'agit d'un document de remplacement — ce qui est de nature à attirer davantage l'attention des agents des services frontaliers et des agents d'immigration;
- une période d'attente obligatoire à des fins d'enquête entre le moment de la nouvelle demande et celui de la délivrance du document de voyage;
- l'imposition d'une limite de la validité des documents de voyage de remplacement;
- (si la loi l'autorise) le refus de délivrer un autre document de voyage après un deuxième document perdu, ou si la preuve a été établie que le document déclaré perdu a été vendu ou prêté.

Les demandes de remplacement de passeports ou autres documents de voyage perdus ou volés représentent une menace potentielle; elles devraient faire l'objet d'une enquête rigoureuse sur la fraude menée par les responsables de l'arbitrage ou de la détermination de l'admissibilité. S'il y a eu plusieurs déclarations de perte, une entrevue personnelle avec la personne qui a fait ses déclarations et une

enquête policière pourraient être nécessaires. Divers motifs peuvent inciter une personne à déclarer faussement la perte ou le vol d'un document de voyage pour en obtenir un nouveau, dont ceux-ci :

- des restrictions de passage aux postes frontaliers ou douaniers ont été entrées dans le document;
- le requérant tente de maintenir un statut de résident temporaire à l'encontre d'un règlement d'un pays en obtenant un nouveau passeport où n'apparaît aucun timbre d'entrée;
- le requérant tente de contourner la loi sur l'immigration ou d'autres lois d'un autre pays;
- le document de voyage contient des pages munies de visas suspects.

10.3 Mesures d'atténuation

Diverses mesures visent à atténuer les risques pour la sécurité que posent les documents de voyage déclarés perdus ou volés, comme leur annulation immédiate et leur entrée dans une base de données nationale, ainsi que le partage de ces renseignements avec des partenaires nationaux et internationaux.

10.3.1 Annulation des documents de voyage perdus ou volés

Une fois qu'un passeport ou un autre document de voyage a été déclaré perdu ou volé, il doit être immédiatement annulé et ne doit plus être utilisé pour voyager. Cette mesure s'applique aussi bien aux documents personnalisés (passeports réguliers, diplomatiques, spéciaux, temporaires, etc.) qu'aux documents vierges. Une nouvelle demande de remplacement du document par le titulaire est nécessaire.

Dans bien des cas, les documents de voyage déclarés perdus ou volés sont retrouvés subséquemment par leurs titulaires. Ces documents ne sont plus valides, ne doivent pas être utilisés et doivent être retournés à l'autorité qui les a délivrés pour qu'elle en fasse l'annulation physique ou la destruction. L'utilisation d'un document de voyage déclaré perdu ou volé par son titulaire légitime peut lui causer des problèmes importants et des dépenses supplémentaires, puisque ses déplacements en avion et son entrée dans les pays de destination pourraient lui être refusés.

10.3.2 Inscription dans une base de données nationale des documents de voyage perdus ou volés

Les documents perdus ou volés devraient être déclarés non valides et être immédiatement signalés dans une base de données nationale sur les documents de voyage perdus ou volé durant la période de validité de ces documents, à tout le moins. Il est recommandé que chaque gouvernement s'assure qu'une telle base de données est conservée et accessible aux postes frontaliers. Les données sur les documents de voyage perdus ou volés devraient être téléchargées régulièrement, de préférence chaque jour. Une attention particulière devrait être prêtée à l'exactitude et à l'intégrité des données pour éviter des désagréments aux voyageurs légitimes qui n'ont pas déclaré un document de voyage perdu ou volé. Si une erreur est confirmée, l'autorité de délivrance devrait prendre toutes les mesures nécessaires pour extraire de la base de données les renseignements relatifs au document.

L'utilisation de numéros de série dans chaque livret vierge et chaque document de voyage personnalisé facilite l'annulation du document, s'il est déclaré perdu ou volé. Si un document de voyage est déclaré perdu ou volé, son numéro doit être annulé. Si le numéro est réutilisé dans le document de voyage ou les livrets (durant toute la vie d'un individu), il sera plus difficile de retracer le document perdu ou volé, et le titulaire risque d'avoir des problèmes lorsqu'il se présentera à des postes frontaliers.

L'échange de renseignements sur les documents de voyage perdus ou volés est une stratégie d'atténuation importante en ce qui concerne le contrôle frontalier, l'immigration et le vol d'identité. En ce sens, il est important pour les autorités frontalières et les autorités de l'immigration, à tous les points d'entrée, de comparer tous les passeports nationaux et les autres documents de voyage qui leur sont présentés avec la base de données afin de vérifier s'ils ont été déclarés perdus ou volés. Ces renseignements devraient être accessibles en temps réel. La base de données sur les documents de voyage perdus ou volés devrait être accessible à la police ou aux agents d'application de la loi afin de

détecter les cas de vol d'identité, ainsi qu'aux personnes autorisées à délivrer des visas pour éviter que des visas soient apposés dans des documents de voyage déclarés perdus ou volés.

Les bases de données nationales sur les documents de voyage perdus ou volés peuvent également fournir des renseignements pouvant être analysés et utilisés pour évaluer les menaces qui pèsent sur les documents de voyage nationaux et le processus de délivrance. Afin de pouvoir utiliser la base de données à cette fin, celle-ci devrait contenir des renseignements précis sur les circonstances entourant la perte de ces documents, qu'il s'agisse de perte individuelle ou collective.

10.3.3 Partage des renseignements avec des partenaires internationaux

Grâce à leur base nationale de données, les pays sont maintenant en mesure de déterminer l'utilisation qui est faite de leurs documents de voyage perdus ou volés quand ces derniers sont présentés à leurs frontières. Toutefois, pour déterminer si un document de voyage étranger présenté aux frontières a été signalé perdu ou volé, les pays doivent partager des renseignements avec des partenaires internationaux. En plus de permettre le partage de données régionales ou bilatérales, les partenariats internationaux facilitent l'échange de données sur les documents de voyage perdus ou volés; c'est le cas de la base de données sur les documents de voyage volés ou perdus (SLTD) d'Interpol et du Système régional d'alerte sur les déplacements (RMAS) mis en place par la Coopération économique Asie-Pacifique (APEC).

L'échange de renseignements sur les documents de voyage perdus ou volés entre les pays améliore l'intégrité des frontières et contribue à réduire le vol d'identité, aux postes frontaliers ou dans d'autres situations, lorsque ces documents sont présentés en tant que pièces d'identité.

10.3.3.1 Base de données d'Interpol sur les documents de voyage volés

Interpol gère une base de données sur des passeports, des cartes d'identité et des visas déclarés perdus ou volés par des pays du monde entier, la base de données sur les documents de voyage perdus et volés (SLTD). Cette base de données permet aux agents des services frontaliers et aux agents d'immigration de vérifier instantanément si un document de voyage qui leur est présenté a été déclaré perdu ou volé.

Toutes les ADDV devraient divulguer le plus tôt possible à Interpol les renseignements relatifs aux documents de voyage perdus et volés, idéalement dans les 24 heures. Cela comprend les livrets de passeport vierges et les documents personnalisés. Les bases de données nationales peuvent transmettre les renseignements requis à la SLTD d'Interpol.

Un bureau central d'autorités clairement désignées dans chaque pays devrait avoir la responsabilité de transmettre ces renseignements à Interpol pour s'assurer que les organismes d'application de la loi savent où faire la déclaration des documents perdus ou volés et que ces données sont transmises régulièrement à Interpol. Les pays doivent s'assurer que leur bureau central national (BCN) d'Interpol connaît les procédures de déclaration, de mise à jour et de vérification de l'information sur les documents de voyage perdus ou volés auprès d'Interpol.

Les renseignements qui doivent être acheminés à la SLTD d'Interpol comprennent — sans toutefois s'y limiter — les suivantes :

a) le numéro du document tel qu'il apparaît dans la zone de lecture automatique (ou le numéro de série dans un livret vierge);
b) le type de document (passeport ou autre);
c) le pays de délivrance (code de l'OACI);
d) s'il s'agit d'un document délivré ou d'un livret vierge;
e) s'il s'agit d'un document perdu ou d'un document volé;
f) la date et l'endroit de délivrance;
g) la date et l'endroit du vol ou de la perte.

Il convient de prêter une attention particulière à la qualité, à l'exhaustivité et à l'exactitude des données, en particulier le numéro du document de voyage. Toute erreur de saisie peut avoir des conséquences pour les voyageurs légitimes et se révéler coûteuse pour l'autorité de délivrance, si le voyageur cherche à obtenir un dédommagement et que l'autorité de délivrance est fautive. Si une erreur est confirmée, l'autorité de délivrance devrait prendre toutes les mesures nécessaires pour extraire de la base de données les renseignements relatifs au document.

Chaque pays devrait s'efforcer de rendre la SLTD d'Interpol accessible en temps réel à ses agents des services frontaliers et à ses agents d'immigration, quand ils veulent vérifier l'identité de voyageurs qui se présentent à leurs points d'entrée. Cette base de données devrait aussi être accessible aux personnes autorisées à délivrer des visas pour éviter que des visas soient délivrés dans des documents de voyage perdus ou volés, ainsi qu'aux agents d'application de la loi afin de détecter les cas de vol d'identité. Il est recommandé que l'autorité de délivrance rende disponible à Interpol, 24 heures par jour et sept jours par semaine, une personne-ressource pouvant confirmer l'état des documents déclarés et traiter les cas de correspondance dans la SLTD en temps opportun.

Pour aider les pays à se connecter facilement à sa SLTD, Interpol a élaboré deux solutions intégrées, la base de données en réseau fixe (*Fixed Interpol Network Database* ou FIND) et la base de données en réseau mobile (*Mobile Interpol Network Database* ou MIND). Ces deux bases de données peuvent s'intégrer au système de vérification assistée par ordinateur d'un pays. De plus, la base de données MIND peut être utilisée dans un pays qui ne possède pas un système de vérification assistée par ordinateur. L'accès aux données internationales et l'intégration à des systèmes de vérification existants sont les deux principaux avantages de l'utilisation de MIND et de FIND.

⇒ Site Web d'Interpol sur MIND et FIND : http://www.interpol.int/Public/FindAndMind/DefaultFR.asp

La SLTD d'Interpol est fortement appuyée par divers forums internationaux, dont l'OACI, le G8, l'Union Européenne (UE), l'Organisation pour la sécurité et la coopération en Europe (Décision n° 4/04 sur la déclaration des passeports perdus ou volés aux installations de recherche automatisée d'Interpol ou à la SLTD) et l'Organisation des Nations Unies (Résolution 1617 du Conseil de sécurité).

⇒ Documents d'orientation élaborés par le Sous-groupe d'experts Rome-Lyon du G8 sur la migration :
  - *Processing Travellers who Present Lost and Stolen Travel Documents* (Traitement des voyageurs qui présentent des documents de voyage perdus ou volés)
  - *G8 Best Practices on Quality Control of Reporting on Lost and Stolen Travel Document Data* (Pratiques exemplaires du G8 relatives au contrôle de la qualité lors du signalement des données de documents de voyage perdus ou volés)

⇒ Décision n° 4/04 de l'Organisation pour la sécurité et la coopération en Europe (OSCE) (*anglais*): http://www.osce.org/documents/mcs/2004/12/3907_en.pdf

⇒ Résolution 1617 du Conseil de sécurité de l'Organisation des Nations Unies (ONU) : http://daccessdds.un.org/doc/UNDOC/GEN/N05/446/61/PDF/N0544661.pdf?OpenElement

Le Système régional d'alerte sur les déplacements (RMAS) est une initiative de l'APEC qui permet une validation positive des passeports. Le RMAS permet aux économies participantes de vérifier l'état des passeports en temps réel à la source et informe les organismes concernés si des mesures sont nécessaires. En plus de vérifier les passeports perdus, volés ou non valides, RMAS peut établir si un passeport est reconnu par le pays de délivrance comme ayant été délivré de manière valide.

⇒ Site Web du RMAS de l'APEC : http://www.businessmobility.org/RMAL/RMAL.html

11 Délivrance de documents de voyage à l'étranger

11.1 Sommaire

Les documents de voyage d'un pays délivrés à l'étranger sont généralement délivrés en moins grand nombre que ceux délivrés au pays et relèvent souvent d'un autre ministère. Néanmoins, il est important que la sécurité du processus de délivrance soit la même pour tous les documents de voyage, qu'ils soient délivrés à l'étranger ou au pays, conformément aux nombreuses pratiques exemplaires mentionnées dans le présent guide. L'administration centrale de l'autorité de délivrance devrait superviser le travail réalisé dans chaque mission à l'étranger afin de s'assurer que les pratiques exemplaires de sécurité sont suivies en tout temps.

Pour assurer l'uniformité et la sécurité du processus de détermination de l'admissibilité et du processus de personnalisation des documents de voyage, certains pays rapatrient un de ces deux processus ou les deux processus dans leur administration centrale. Bien sûr, une telle décision est de nature à prolonger le temps requis pour la délivrance et la remise des documents de voyage et peut avoir une incidence sur le nombre de documents de voyage temporaires ou d'urgence délivrés. Le présent chapitre porte sur des situations où les processus de détermination de l'admissibilité et de personnalisation qui se déroulent dans des missions à l'étranger.

11.2 Aperçu du travail

Souvent, le personnel recruté localement s'acquitte de certaines fonctions associées à la délivrance à l'étranger. Il est donc important que ces employés aient fait l'objet d'une enquête sur la sécurité aussi approfondie que celle ayant servi lors de l'embauche des employés affectés aux documents de voyage dans le pays d'origine. Les activités du personnel recruté localement dans le cadre du processus de délivrance devraient faire l'objet du même niveau de surveillance que les activités des employés affectés à la délivrance des documents de voyage dans le pays d'origine. Les employés affectés aux documents de voyage dans les missions à l'étranger reçoivent la même formation (séances de formation, d'information et de sensibilisation à l'égard de la sécurité) que les employés affectés aux documents de voyage dans le pays d'origine. Les politiques, les critères d'admissibilité, les preuves documentaires de citoyenneté et d'identité, les exigences relatives aux demandes, etc. devraient, dans toute la mesure du possible, être les mêmes dans les missions à l'étranger et dans le pays d'origine.

Il devrait y avoir des communications constantes entre l'administration centrale de l'autorité de délivrance et les missions pour s'assurer que les politiques et les pratiques en matière de délivrance sont connues et bien comprises. Des vérifications, des examens et des contrôles de la qualité devraient être effectués de façon régulière par l'administration centrale pour s'assurer que toutes les politiques et les pratiques sont mises en application dans toutes les missions à l'étranger. De bonnes communications entre le pays et les missions, ainsi que des conditions de travail agréables contribuent à créer un sentiment d'appartenance parmi le personnel recruté localement et favorisent la loyauté à l'égard du pays.

11.3 Admissibilité

Lorsque le processus de détermination de l'admissibilité est confié au personnel recruté localement, un superviseur (citoyen du pays) devrait toujours approuver le travail réalisé au niveau des demandes (par exemple, l'examen des preuves documentaires fournies par le requérant, l'empreinte sociale du requérant, la vérification du répondant, le contrôle des références, etc.). Le personnel consulaire devrait fournir l'autorisation finale de toute décision relative à l'admissibilité d'un document de voyage.

Autant que possible, les missions à l'étranger qui délivrent des documents de voyage devraient avoir un accès en ligne aux mêmes bases de données, habilitations (ou autorisations), listes de surveillance, information sur les restrictions relatives aux déplacements, etc. que les bureaux qui délivrent des

documents de voyage dans le pays d'origine. En cas de doute quant à l'intégrité des renseignements ou des documents fournis par un requérant, ou quant à la manière d'interpréter les politiques en matière d'admissibilité, le dossier devrait être acheminé à l'administration centrale de l'ADDV. Une fois délivré par une mission à l'étranger, tout document de voyage doit être entré dans toutes les bases de données nationales pertinentes.

11.4 Personnalisation

Les livrets personnalisés à l'étranger devraient utiliser la même technologie d'impression, les mêmes caractéristiques de sécurité et les mêmes stocks que les livrets personnalisés dans le pays d'origine.

Le contrôle des livrets vierges devrait être encore plus rigoureux que celui des livrets vierges dans le pays d'origine. Les mêmes pratiques exemplaires, décrites aux Chapitres 4 et 5, devraient s'appliquer au processus de délivrance à l'étranger. Les documents vierges devraient être conservés dans une aire de sécurité de chaque mission, et seuls les responsables de la délivrance des documents de voyage devraient y avoir accès. Si le personnel recruté localement participe à la personnalisation des documents de voyage, un cadre dirigeant de la mission, citoyen du pays d'origine, devrait toujours superviser le travail et s'assurer du contrôle de la qualité. Comme c'est le cas à l'administration centrale de l'autorité de délivrance, la comptabilisation des livrets vierges devrait toujours être faite par au moins deux employés, dont un citoyen du pays d'origine, au début et la fin de chaque journée de travail.

12 Intervenants nationaux et internationaux

12.1 Sommaire

Les documents délivrés par l'autorité de délivrance de documents de voyage (ADDV) sont utilisés et vérifiés par divers intervenants nationaux et internationaux. De manière réciproque, l'ADDV doit être en communication constante et consulter les divers partenaires nationaux, internationaux et privés pour s'assurer de la sécurité de ses documents et de son processus de délivrance. La présent chapitre énumère les principaux partenaires et intervenants avec lesquels l'ADDV devrait être en communication, de même que les types de renseignements et de données qui devraient faire l'objet de communications bilatérales.

12.2 Intervenants nationaux

L'ADDV devrait établir des partenariats avec des organisations nationales, des intervenants dans la délivrance et l'utilisation des documents de voyage. Ces organisations comprennent— sans toutefois s'y limiter — les suivantes :

- les organismes de contrôle frontalier;
- les autorités de l'immigration;
- les organismes d'application de la loi ou la police;
- les laboratoires judiciaires de documents;
- les diverses organisations qui participent à l'élaboration de listes de surveillance et de restrictions relatives aux déplacements aux fins de détermination de l'admissibilité aux documents de voyage;
- les bureaux de l'état civil (qui délivrent des documents de base ou primaires et des documents à l'appui);
- tout autre partenaire qui participe au processus de délivrance des documents de voyage (p. ex. les missions à l'étranger qui délivrent des passeports diplomatiques, spéciaux, officiels, temporaires; les organisations qui reçoivent les demandes).

Toutes ces organisations peuvent contribuer à l'élaboration des caractéristiques physiques des documents de voyage, influencer les décisions relatives à l'admissibilité, avoir des répercussions sur la sécurité du processus de délivrance ou être touchées par des changements apportés ou des décisions prises par l'ADDV en ce qui concerne les documents de voyage et le processus de délivrance.

12.2.1 Organismes de contrôle frontalier et autorités de l'immigration

Les organismes de contrôle frontalier et les autorités de l'immigration sont les partenaires les plus proches de l'ADDV. À partir des renseignements contenus dans les documents de voyage, ces organisations déterminent quels voyageurs peuvent ou ne peuvent entrer sur un territoire national. Les agents frontaliers et de l'immigration connaissent les dispositifs de sécurité qui sont les plus efficaces et qui sont plus facilement vérifiés lors des inspections primaires et secondaires.

En tant qu'utilisateurs de première ligne des documents de voyage, les organismes de contrôle frontalier et les autorités de l'immigration sont également témoins de l'incidence et des tendances de la fraude de documents de voyage et compilent les données à ce sujet. Les autorités de délivrance devraient communiquer régulièrement avec ces organisations et établir des partenariats pour échanger des renseignements sur la fraude et influencer l'élaboration, la conception et l'intégration de dispositifs ou de caractéristiques de sécurité dans les documents de voyage. L'autorité de délivrance devrait prendre toutes les mesures requises pour s'assurer que les caractéristiques techniques ou physiques qu'elle incorpore dans ses documents de voyage sont non seulement élaborées en collaboration avec les organismes de contrôle frontalier et les autorités de l'immigration, mais aussi qu'ils satisfont aux exigences relatives au contrôle frontalier et à l'immigration.

Lorsque de nouveaux dispositifs de sécurité, de nouvelles versions ou spécifications sont incorporés dans un passeport, les agents des services frontaliers et les agents d'immigration nationaux et internationaux devraient en être informés dans un délai raisonnable. La coopération et la communication avec les organismes de contrôle frontalier et les autorités de l'immigration est aussi essentielle pour s'assurer que l'incorporation de nouvelles versions ou de mises à jour dans les documents de voyage, comme l'introduction des passeports électroniques, est interopérable avec les systèmes de contrôle frontalier, actuels et futurs, et les infrastructures (p. ex. le contrôle frontalier informatisé).

Les organismes de contrôle frontalier et les autorités de l'immigration peuvent contribuer à l'élaboration de listes de surveillance utilisées par les autorités de délivrance durant le processus de détermination de l'admissibilité aux documents de voyage. De leur côté, les ADDV fournissent aux organismes de contrôle frontalier et aux autorités de l'immigration certains renseignements sur les passeports déclarés perdus ou volés et annulés. Des mécanismes de communication bilatérale devraient également être en place pour confirmer la validité des données fournies par les deux organisations.

12.2.2 Organismes d'application de la loi, police et laboratoires judiciaires de documents

Les organismes d'application de la loi, la police et les laboratoires judiciaires de documents sont également bien conscients des menaces à la sécurité des documents de voyage et des tendances de la fraude. Ils enquêtent sur des cas de fraude de documents de voyage et sur les techniques utilisées pour les contrefaire. Ces renseignements sont d'une valeur inestimable pour les autorités de surveillance; elles les aident à élaborer, à concevoir et à intégrer des dispositifs de sécurité dans les documents de voyage, de même qu'à intégrer des mécanismes de sécurité et des contrôles internes dans le processus de délivrance.

Les organismes d'application de la loi et la police fournissent également des données qui contribuent à l'élaboration de listes de surveillance que les autorités de délivrance peuvent utiliser durant le processus de détermination de l'admissibilité.

12.2.3 Bureaux de l'état civil

Dans une large mesure, les décisions relatives à l'admissibilité aux documents de voyage nécessitent la vérification de l'identité et de la citoyenneté à l'aide de documents primaires ou de documents de base et de documents à l'appui souvent délivrés par des organismes gouvernementaux distincts. Toute autorité de délivrance devrait avoir des communications fréquentes avec les bureaux de l'état civil pour obtenir des renseignements sur les différentes versions de documents utilisées et les dispositifs de sécurité de ces documents, ainsi que sur des renseignements relatifs à la fraude. Un mécanisme devrait aussi être mis en place afin de vérifier régulièrement l'intégrité des documents présentés par les requérants. Comme il a été mentionné au Chapitre 4, il est recommandé d'avoir un accès électronique direct aux dossiers et aux registres appropriés.

12.2.4 Autres organisations

Autorités qui contribuent à l'élaboration des listes de surveillance et de restrictions relatives aux déplacements

Les données que contiennent les diverses listes de surveillance et listes de restrictions relatives aux déplacements, utilisées pour prendre des décisions en matière d'admissibilité, varient selon les États. Les organismes de contrôle frontalier, les autorités de l'immigration, les organismes d'application de la loi et la police devraient contribuer à l'enrichissement de ces listes. En outre, le ministère de la Justice, les Services correctionnels, le ministère des Affaires étrangères, les services de perception des impôts, etc. peuvent également être appelés à fournir un apport.

Partenaires qui participent au processus de délivrance

Toutes les organisations qui participent au processus de délivrance des documents de voyage — y compris la délivrance à l'étranger et la délivrance de passeports diplomatiques, officiels et spéciaux — et les organisations qui reçoivent les demandes au nom de l'ADDV devraient prendre part et être tenus au courant de toute modification des politiques et des processus mis en place par l'ADDV qui peuvent avoir des répercussions sur la sécurité du processus de délivrance.

12.3 Partenaires internationaux

L'ADDV devrait établir des associations ou des partenariats avec d'autres pays, participer à des forums internationaux et à des groupes de travail pour partager de l'information sur les normes relatives aux documents de voyage, les spécifications, les tendances et la fraude; partager des données pertinentes sur les documents de voyage; et chercher de l'aide aux fins du renforcement des capacités. Ces organisations devraient ou pourraient comprendre — sans toutefois s'y limiter — les suivantes :

- l'Organisation de l'aviation civile internationale (OACI);
- Interpol;
- la Coopération économique Asie-Pacifique (APEC);
- l'Organisation internationale pour les migrations (OIM);
- l'Organisation pour la sécurité et la coopération en Europe (OSCE);
- l'Organisation des États américains (OEA);
- tout autre forum régional ou international axé sur les documents de voyage, la sécurité frontalière, la migration, etc.

12.3.1 Organisation de l'aviation civile internationale (OACI)

L'OACI établit les normes et les pratiques recommandées relativement à la délivrance des passeports et des autres documents de voyage (Section 3 de l'Annexe 9 de la Convention de Chicago). Le Groupe consultatif technique sur les documents de voyage lisibles à la machine (TAG/MRTD) élabore et adopte des spécifications relatives aux documents de voyage lisibles à la machine (DVLM) et aux documents de

voyage électroniques lisibles à la machine (DVELM), qui sont comprises dans le *Document 9303*. Le TAG/MRTD publie également des principes directeurs pour aider les États membres de l'OACI à mettre en œuvre ses spécifications, de même que des rapports techniques et des documents d'information. Dans le cadre du TAG/MRTD, deux groupes de travail ont été créés :

Groupe de travail des nouvelles technologies (NTWG)
En partenariat avec l'Organisation internationale de normalisation (ISO), le NTWG élabore des stratégies, des politiques et des documents d'orientation relatifs à la fabrication, à la sécurité, aux tests, à la délivrance, au déploiement et à l'interopérabilité internationale des documents de voyage lisibles à la machine (DVLM) et des documents de voyage électroniques lisibles à la machine (DVELM), sous forme matérielle ou électronique.

Groupe de travail sur la mise en œuvre et le renforcement des capacités (ICBWG)
Ce groupe de travail aide le secrétariat de l'OACI à réaliser des activités de communication sur le renforcement des capacités afin d'aider les pays à délivrer des DVLM et à améliorer la sécurité de leur processus de délivrance.

Le programme MRTD (Machine Readable Travel Document) du secrétariat de l'OACI offre des possibilités de financement et une expertise relativement à la délivrance de documents d'identité et de documents de voyage.

⇒ Programme MRTD (anglais) : http://www2.icao.int/en/MRTD/Pages/default.aspx
⇒ Pour commander le *Document 9303* : http://icaodsu.openface.ca/mainpage.ch2

12.3.2 Partage de renseignements et de données à l'échelle internationale

Comme il a été mentionné au Chapitre 10, il est recommandé que les renseignements sur les documents de voyage déclarés perdus ou volés soient partagées avec des partenaires internationaux. Le partage de ces données permet aux pays d'établir le niveau d'utilisation abusive de leurs passeports déclarés perdus ou volés et des documents de voyage délivrés dans d'autres pays.

La base de données d'Interpol sur les documents de voyage volés (SLTD) permet aux agents des services frontaliers et aux agents d'immigration de vérifier instantanément si un document de voyage qui leur est présenté a été déclaré perdu ou volé.

En plus de vérifier les passeports perdus, volés ou non valides, le système régional d'alerte sur les déplacements (RMAS) de l'APEC peut établir si un passeport est reconnu par le pays dont il provient comme ayant été délivré de manière valide.

Plusieurs partenariats bilatéraux régionaux et internationaux ont été créés partout dans le monde pour améliorer la coopération et le partage de données et faciliter les passages aux frontières entre pays voisins, comme Shengen Area, MERCOSUR, ECOWAS, CARICOM, etc.

12.3.3 Coopération internationale et renforcement des capacités

En plus de l'OACI, diverses organisations régionales et internationales offrent des programmes sur les capacités, de l'expertise, du financement et des ressources disponibles pour aider et travailler de concert avec les pays qui cherchent de l'aide dans le domaine de la délivrance des documents de voyage. L'OIM, l'OAE et l'OSCE sont des organisations actives dans ce domaine.

Organisation internationale pour les migrations (OIM) — Coopération technique sur la gestion des migrations et le renforcement des capacités
L'OIM est une organisation intergouvernementale qui regroupe 122 membres. Les activités de la Division de la coopération technique sur les migrations aident les gouvernements à se donner les politiques, les lois, les structures administratives, les systèmes opérationnels et les ressources humaines nécessaires

pour aborder divers problèmes de migration. L'OIM offre des services-conseils, une assistance technique et des activités de formation.

⇒ Site Web de l'IOM TCM (anglais): http://www.iom.int/jahia/Jahia/pid/749

Organisation des États américains (OEA) — Comité interaméricain contre le terrorisme (CICTE)
Le but premier du Comité interaméricain contre le terrorisme (CICTE) de l'OEA est de promouvoir la coopération parmi les États membres afin de prévenir, de combattre et d'éliminer le terrorisme. Le programme de sécurité des documents et de prévention de la fraude du Comité a pour objectif d'accroître, dans des pays cibles, la capacité des employés des douanes, de l'immigration et de l'application de la loi de mieux contrôler la délivrance des documents de voyage et des documents d'identité et de mieux détecter les documents frauduleux afin de prévenir leur utilisation, la contrefaçon ou la falsification.

⇒ Site Web du CICTE de l'OEA (anglais/espagnol): http://www.cicte.oas.org/Rev/En/

Organisation pour la sécurité et la coopération en Europe (OSCE) — Unité Action contre le terrorisme
Créée en 2002, l'unité Action contre le terrorisme coordonne et facilite les initiatives et les programmes de renforcement des capacités de l'OSCE en matière de lutte contre le terrorisme. Le programme de sécurité des documents de voyage de l'OSCE fournit une aide pratique et une orientation dans la mise en œuvre des engagements en matière de lutte au terrorisme. L'OSCE a réalisé diverses activités de renforcement des capacités au cours des dernières années, dont des ateliers sur la sécurité, le traitement et la délivrance des documents de voyage, ainsi que des séances d'information sur la falsification des documents.

⇒ Site Web de l'OSCE ATU (anglais) : http://www.osce.org/atu/

12.4 Partenaires privés

En plus des partenaires nationaux et internationaux, la communication constante et le partage de renseignements sont à l'avantage de l'ADDV et des entreprises privées partenaires.

12.4.1 Transporteurs aériens

Puisque les gouvernements sollicitent de plus en plus l'aide des transporteurs aériens — par exemple en leur demandant de vérifier l'intégrité des documents de voyage, de stocker et de leur transmettre des renseignements sur les passagers — il est important pour une autorité de délivrance de rester en contact avec des compagnies et des associations aériennes, comme l'Association du transport aérien international (IATA). Cela permet de partager des renseignements sur les caractéristiques des documents de voyage, notamment leurs dispositifs de sécurité.

12.4.2 Entreprises privées

L'Organisation internationale de normalisation (ISO) et d'autres entreprises actives dans les domaines des documents de voyage, des lecteurs, des puces électroniques, des identificateurs biométriques, des imprimantes, etc. sont d'excellentes sources d'information sur les nouveaux systèmes, technologies et processus. Pour toute autorité de délivrance, présenter régulièrement des demandes de renseignements (DR) est une bonne pratique pour se tenir au courant des plus récentes recherches et innovations.

Documents de référence

1. *Security Standards for Machine Readable Travel Documents* — Annexe informative du Document 9303
2. *Minimum Security Standards for the handling of MRTDs and other passports* — Annexe informative de la Section III du Document 9303
3. *ICAO-New Technologies Working Group (IEC JTC1 SC17 WG3/TF1), "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation"*, version 1.4, 7 mars 2007, TAG-MRTD/17-WP/16
4. *Recommended Standards for Secure Proof of Status and Nationality Documents to Facilitate Cross-Border Travel, Security and Prosperity Partnership Deliverable* 1.1.3
5. *A Guide to Biometric Technology in Machine Readable Travel Documents*, APEC Business Mobility Group
6. *G8 Best practice for the processing of travellers who present lost of stolen travel documents*
7. *G8 Best practices on quality control of reporting on lost and stolen travel document data*

Sigles et acronymes

ADDV	Autorité de délivrance de documents de voyage
APEC	Coopération économique Asie-Pacifique
BCN Interpol	Bureaux centraux nationaux d'Interpol (*Interpol National Central Bureaus*)
CAB	Contrôle d'accès de base
CAE	Contrôle d'accès élargi
DR	Demande de renseignements
DVELM	Document de voyage électronique lisible à la machine
DVLM	Document de voyage lisible à la machine
FIND	Base de données en réseau fixe d'Interpol (*Fixed Interpol Network Database*)
ICBWG	Groupe de travail sur la mise en œuvre et le renforcement des capacités (*Implementation and Capacity Building Working Group*)
ICP	Infrastructure à clés publiques
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
MIND	Base de données en réseau mobile d'Interpol (*Mobile Interpol Network Database*)
NTWG	Groupe de travail des nouvelles technologies (*New Technology Working Group*)
OACI	Organisation de l'aviation civile internationale
OEA	Organisation des États américains
OIM	Organisation internationale pour les migrations
OSCE	Organisation pour la sécurité et la coopération en Europe
PLM	Passeport lisible à la machine
RCP	Répertoire des clés publiques
RMAS	Système régional d'alerte sur les déplacements (*Regional Movement Alert System*)
SACF	Système automatisé de contrôle frontalier
SD	Signataire du document
SLTD	Base de données d'Interpol sur les documents de voyage volés (*Stolen and Lost Travel Documents*)
TAG	Groupe consultatif technique (*Technical Advisory Group*)
UE	Union européenne
ZLA	Zone de lecture automatique