Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/7
EX/4
5/7/19
(Note d'information)

ASSEMBLÉE — 40e SESSION

COMITÉ EXÉCUTIF

Point 14: Programmes de facilitation

AVANTAGES DE LA PARTICIPATION AU RÉPERTOIRE DE CLÉS PUBLIQUES (RCP)

(Note présentée par le Conseil de l'OACI)

RÉSUMÉ ANALYTIQUE

La présente note fournit de l'information sur le Répertoire OACI de clés publiques (RCP OACI), et fait ressortir les avantages que les États ont à y participer. Le RCP OACI a été établi afin de permettre aux États d'avoir accès aux renseignements sur les clés publiques qui sont nécessaires pour valider et authentifier les passeports électroniques. Il s'agit d'un volet essentiel de la stratégie du Programme OACI d'identification des voyageurs (TRIP), qui soutient d'une manière efficace et rentable les processus de lecture et de vérification des documents de voyage. La vérification des passeports électroniques à l'aide des certificats associés à l'infrastructure de clé publique peut fournir aux autorités chargées du contrôle frontalier l'assurance que les documents de voyage sont authentiques et non modifiés, ce qui authentifie alors les renseignements biométriques contenus dans les passeports électroniques et permet d'automatiser des aspects du processus de contrôle frontalier. La validation des passeports électroniques est un élément essentiel pour tirer profit de l'investissement consenti par les États en vue de mettre au point de tels titres de voyage, contribuer à renforcer la sécurité aux frontières, pour combattre le terrorisme et la criminalité, et promouvoir la sécurité des voyages aériens à l'échelle mondiale. Étant donné que le RCP OACI répond en même temps aux besoins de facilitation et de sûreté, son utilisation aidera à combler les failles dans la sûreté des mécanismes de contrôle frontalier d'un pays, tout en améliorant l'expérience des voyageurs. Le RCP compte actuellement 66 participants. L'OACI encourage tous les États membres à s'inscrire au RCP et à l'utiliser activement dans le but d'améliorer l'efficience et l'efficacité de la validation des passeports électroniques.

Objectifs stratégiques :	La présente note de travail se rapporte à l'Objectif stratégique : *Sûreté et facilitation.*
Incidences financières :	Nul besoin de ressources supplémentaires.
Références :	C- DEC 216/2 Doc 9303 (7e édition), *Documents de voyage lisibles à la machine* A40-WP/6, Faits nouveaux concernant le Répertoire de clés publiques (RCP) de l'OACI A40-WP/8, Faits nouveaux concernant la stratégie du Programme OACI d'identification des voyageurs (TRIP)

1. HISTORIQUE

1.1 Un passeport électronique est un passeport lisible à la machine (PLM) qui contient une puce électronique intégrée comportant des données chiffrées où sont stockés les renseignements d'identification indiqués sur la page 2 du passeport du titulaire. Une fois personnalisé par l'État émetteur, le passeport électronique est verrouillé et donc impossible à modifier, ce qui ajoute une couche de sécurité aux PLM.

1.2 Outre les renseignements servant à identifier le voyageur sur la page des données, le passeport électronique comporte une puce (Appendice A) dotée de fonctions de sécurité numériques propres à l'État émetteur, appelée la signature numérique de l'État. Cette signature numérique est propre à chaque État et est stockée de manière sûre dans la puce du passeport électronique en tant qu'objet de sécurité de document (OSD), et peut donc être vérifiée par l'intermédiaire d'une infrastructure de clé publique (ICP) de l'État émetteur. L'Appendice B présente les liens possibles entre la délivrance et la vérification d'un passeport électronique, et la façon dont l'authentification de celui-ci peut être confirmée à l'aide du Répertoire OACI de clés publiques (RCP). Lors du balayage d'un passeport et de la lecture de la puce, l'authentification de sa signature numérique indique aux autorités de contrôle aux frontières que les données stockées dans la puce sont authentiques, que le passeport a été délivré par l'État émetteur, et qu'il n'a pas été modifié.

1.3 Cette authentification, communément appelée validation du passeport électronique, constitue le processus de validation de l'authenticité et de l'intégrité d'un passeport électronique par la vérification de la signature numérique que contient la puce. Pour que les autorités de contrôle frontalier puissent authentifier le passeport électronique d'un voyageur arrivant de l'étranger, il faut que l'État récepteur ait accès à certains renseignements de l'État émetteur.

1.4 Il existe actuellement plus de 140 États et entités non étatiques, comme les Nations Unies, qui émettent des passeports électroniques ou des documents de voyage lisibles à la machine électroniques (DVLM-e), ce qui représente environ un milliard de passeports électroniques en circulation. Bien que les signatures numériques des États puissent être échangées bilatéralement, le nombre croissant d'États qui délivrent des passeports électroniques et le volume par conséquent élevé de passeports électroniques en circulation créerait un mécanisme hautement complexe et inefficace qui pourrait retarder le processus de facilitation et occasionner des erreurs. Le RCP OACI est un répertoire central pour l'échange de renseignements nécessaires à l'authentification des passeports électroniques. Il fournit donc aux États un moyen efficace de téléverser leurs propres renseignements et de télécharger ceux des autres États aux fins d'utilisation lors des contrôles aux frontières, en vue de renforcer la facilitation et la sûreté. Comme indiqué à l'Appendice C, tous les États émetteurs de passeports électroniques ne participent pas au RCP.

2. RÔLE DU RCP DANS LA STRATÉGIE DU PROGRAMME OACI D'IDENTIFICATION DES VOYAGEURS (TRIP)

2.1 La stratégie TRIP de l'OACI se fonde sur une approche comportant cinq éléments indissociables qui permettent aux États d'établir et de confirmer l'identité des voyageurs. Les cinq éléments se complètent et se renforcent mutuellement. L'établissement efficace de l'identité permet d'optimiser les avantages économiques, sociaux et politiques des voyages internationaux, et aide à gérer les risques pour la sûreté et à réagir aux menaces visant les frontières en permettant de mieux axer les ressources sur les personnes qui présentent un intérêt.

2.2 L'ensemble des éléments de la stratégie TRIP de l'OACI donne les moyens aux États d'établir l'identité des voyageurs et d'évaluer d'une manière ciblée les risques qu'ils présentent, notamment en reliant les systèmes et outils d'inspection (IST) et les applications interopérables (IA). L'obtention de renseignements sur les voyageurs complète le cycle TRIP de l'OACI en fournissant des preuves supplémentaires sur l'identité des étrangers arrivant dans un État.

2.3 Les systèmes et outils d'inspection permettent aux autorités frontalières de recueillir, de vérifier et d'enregistrer des données sur les voyageurs contenues dans les documents de voyage lisibles à la machine (DVLM). Les contrôles des détenteurs de ces documents peuvent être effectués lors des différentes phases du voyage, autrement dit avant le départ, avant l'arrivée, à l'entrée, pendant le séjour et à la sortie. Ces contrôles sont renforcés par le partage mondial, au moyen d'applications interopérables, de données sur les voyageurs et leurs documents de voyage. Ces deux éléments, qui font partie des cinq autour desquels s'articule la stratégie TRIP de l'OACI, sont directement liés à la gestion du contrôle aux frontières. Les systèmes de contrôle frontalier dont se servent les États intègrent des applications interopérables et des systèmes et outils d'inspection.

2.4 Les systèmes et outils d'inspection saisissent, vérifient, croisent et enregistrent les données contenues dans les DVLM et les données relatives aux voyageurs, tandis que les applications interopérables permettent d'échanger des données sur les voyageurs et leurs documents de voyage à l'échelle mondiale. L'intégration des IST et des IA au système de contrôle frontalier national permet d'évaluer les risques que présentent les voyageurs aux différentes étapes de leur parcours. L'évaluation s'appuie sur l'identification des voyageurs et utilise les nouveaux renseignements auxquels les États de transit et de destination ont accès à chaque étape du voyage. L'Appendice D décrit les éléments TRIP de l'OACI, certains des éléments que recouvrent les IST et les IA, et la façon dont ils influent sur les différentes étapes d'un voyage typique.

2.5 La gestion efficiente du contrôle aux frontières repose avant tout sur une lecture efficace des éléments des données DVLM, ce qui suppose l'utilisation de DVLM et de DVLM électroniques normalisés et interopérables, conformes aux spécifications techniques du Doc 9303 de l'OACI, *Documents de voyage lisibles à la machine*, que l'on peut consulter à https://www.icao.int/publications/pages/publication.aspx?docnum=9303. Les États devraient se conformer à la pleine application des spécifications techniques afin d'assurer l'interopérabilité et d'en retirer les avantages connexes en matière de sûreté et de facilitation.

3. AVANTAGES DE L'UTILISATION DU RCP AUX FRONTIÈRES

3.1 Pour l'État émetteur, l'utilisation des technologies de délivrance les plus récentes, assortie d'un réseau sécurisé et d'infrastructures ICP, renforce à la fois la confiance dans les passeports délivrés par l'État et la participation aux initiatives de sûreté internationales. De plus, elle offre de la souplesse vis-à-vis d'initiatives plus récentes telles que l'autorisation de voyage électronique (AVE), le contrôle frontalier automatisé (CFA) aux portes ainsi que tous les outils modernes disponibles basés sur la technologie des passeports électroniques. Pour que se concrétisent pleinement les avantages de l'adhésion au RCP, l'utilisation du Répertoire devrait aller de pair avec un renforcement des inspections aux frontières.

3.2 En 2014, le Conseil de sécurité de l'ONU (UNSC) a adopté la résolution 2178 stipulant notamment qu'il : « réaffirme que tous les États doivent empêcher la circulation de terroristes et de

groupes terroristes en effectuant des contrôles efficaces aux frontières, en surveillant de près la délivrance de documents d'identité et de voyage, et en prenant des mesures visant à empêcher la falsification de documents d'identité et de voyage, la fabrication de faux et l'utilisation frauduleuse de tels documents ». L'adhésion au RCP OACI et son utilisation peuvent aider les États membres à mettre en œuvre la résolution du Conseil de sécurité, car il s'agit d'une démarche dont l'utilité est reconnue et pour laquelle il n'existe pas de solution de rechange viable actuellement. En engageant cette démarche proactive, les États sont à même de contribuer à l'amélioration de l'expérience voyageur et à la lutte contre le terrorisme international.

3.3 À défaut de pouvoir valider, à la frontière, les données électroniques figurant dans un passeport électronique, le document de voyage doit être traité exactement comme un PLM et ne fournit pas un complément de sûreté. Le RCP OACI offre un moyen simple, rapide et économique de valider les passeports électroniques. L'utilisation d'un lecteur de passeports électroniques contenant déjà des données RCP aux points de contrôle frontaliers est le seul moyen de confirmer l'authenticité des données contenues dans la puce d'un passeport électronique. L'utilisation de l'outil RCP aux frontières permet donc de disposer de renseignements en temps utile pour établir l'authenticité des passeports électroniques. Ce processus, qui simplifie la validation des passeports électroniques aux frontières, assure la rapidité et la sûreté des mouvements transfrontaliers en permettant de déceler promptement les puces corrompues ou contrefaites.

3.4 Il est important, pour les États émetteurs, de s'assurer que les autorités frontalières du monde entier valident leurs passeports électroniques. Les frais d'inscription au RCP sont minimes, comparativement aux sommes nécessaires pour maintenir une infrastructure bilatérale permettant de relier tous les participants émetteurs de passeports électroniques. L'échange de données par l'intermédiaire du RCP réduit les coûts administratifs connexes d'une approche bilatérale. De plus, les frais d'inscription au RCP diminuent à mesure que le nombre de participants augmente.

3.5 L'utilisation du RCP aux frontières favorise une solide confiance dans la sûreté des passeports électroniques, aux niveaux matériel et numérique. Les données inscrites sur le passeport et celles contenues dans la puce peuvent être comparées au résultat de l'inspection visuelle, tandis que la reconnaissance faciale peut être appliquée à une photo du passager à l'arrivée. Si l'inspection est réalisée convenablement, les usurpateurs et les détenteurs de faux passeports doivent donc franchir de nombreux obstacles avant d'entrer sur le territoire d'un État.

3.6 La participation au RCP OACI procure un accès privilégié aux agences de contrôle frontalier des États émetteurs. La validation des passeports électroniques, conformément aux dispositions de la Partie 12 du Doc 9303, permet aux autorités frontalières de s'assurer que les documents de voyage inspectés ont été délivrés par les autorités compétentes et que les renseignements qu'ils contiennent n'ont pas été falsifiés. La Partie 12 du Doc 9303 décrit les spécifications de l'ICP, aspect important de la sûreté globale des MRTD, car elle énonce les exigences s'appliquant aux spécialistes des technologies de l'information qui sont chargés de développer le système d'ICP nationale pour les États et couvre, entre autres sujets, les rôles et les responsabilités, la gestion des clés, les mécanismes de distribution, la confiance à l'égard de l'ICP et sa validation. L'outil RCP OACI fournit un accès fiable et économique à l'ICP nationale publiée par d'autres États, ce qui permet une validation robuste des passeports électroniques.

3.7 Par ailleurs, un État émetteur de passeports électroniques qui participe au RCP peut partager ses expériences avec d'autres États et profiter des leurs, tout en bénéficiant de l'efficacité de l'échange de données multilatéral et en facilitant les voyages internationaux de ses ressortissants.

3.8 Enfin, il est intéressant de souligner que la Commission du RCP met la dernière main à une liste de contrôle qui devrait être disponible à la fin de 2019 et qui représentera un complément important aux services actuellement offerts par le RCP OACI.

4. CONCLUSIONS

4.1 La participation au RCP OACI devrait s'inscrire dans les efforts déployés pour renforcer la gestion globale de l'identité nationale. Il est indispensable d'empêcher des criminels de se procurer un passeport électronique authentique sous une fausse identité et il est essentiel de relier les mécanismes d'émission aux données de l'état civil.

4.2 L'introduction du RCP exige une bonne préparation, qui consiste, pour les États, à s'assurer dès le départ qu'ils se conforment aux spécifications de l'OACI. Ils doivent s'occuper des démarches administratives et des questions techniques nationales et internationales associées à l'intégration de leur système au RCP OACI. L'Appendice E présente en détail les étapes concrètes de la mise en œuvre du RCP OACI.

4.3 Grâce aux normes et pratiques recommandées, et aux spécifications de l'OACI, chaque État a aujourd'hui la possibilité de tirer parti de ce cadre, qui a créé un mécanisme vraiment interopérable à l'échelle mondiale pour lire et vérifier les passeports aux frontières.

4.4 Ce cadre non seulement contribue grandement à la sûreté mondiale, mais facilite aussi les processus d'immigration dans les aéroports, ainsi qu'aux frontières terrestres et maritimes. L'ajout de caractéristiques biométriques, comme les images faciales, à la puce sans contact que contiennent les PLM montre que le niveau de sûreté a considérablement augmenté. Il incombe à présent aux agences qui gèrent les frontières dans le monde de mettre à niveau leur infrastructure de façon à pouvoir lire ces éléments d'information et les utiliser dans leurs mécanismes de contrôle frontalier pour vérifier l'identité des détenteurs.

– – – – – – – – – – – –

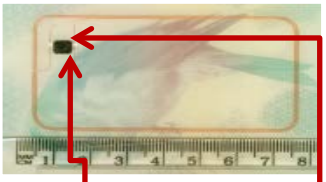
APPENDICE A

QU'EST-CE QU'UN PASSEPORT ÉLECTRONIQUE ?

Selon la définition de l'OACI, un passeport électronique est un passeport lisible à la machine (PLM) contenant une puce sans contact où sont stockées les données de la page de renseignements du PLM, un identifiant biométrique du détenteur du passeport et un objet de sécurité visant à protéger les données par cryptographie, et qui respecte les spécifications énoncées dans le Doc 9303-4.

PLM

Puce



<u>Structure de données logique (SDL)</u> **<u>Signature numérique de l'État</u>**

La SDL contient les données personnelles et les données biométriques obligatoires (visage) ainsi que d'autres informations.

DONNÉES ENREGISTRÉES PAR L'ÉTAT ou L'ORGANISME ÉMETTEUR

Détail(s) enregistré(s) dans la ZLA	DG1		Type de document
			État émetteur ou organisation émettrice
			Nom (du titulaire)
			Numéro de document
			Chiffre de contrôle - Numéro de document
			Nationalité
			Date de naissance
			Chiffre de contrôle - Date de naissance
			Sexe
			Date d'expiration ou valide jusqu'au
			Chiffre de contrôle - Date d'expir./valide jusqu'au
			Données optionnelles
			Chiffre de contrôle - Champ de données option.
			Chiffre de contrôle composite
Élément(s) d'identification codé(s)	Élément pour échanges mondiaux	DG2	Visage codé
	Élément(s) supplémentaire(s)	DG3	Doigt(s) codé(s)
		DG4	Œil (yeux) codé(s)
Élément(s) d'identification affiché(s)	DG5		Portrait affiché
	DG6		Réservé pour usage futur
	DG7		Signature ou marque habituelle affichée
Élément(s) de sécurité codé(s)	DG8		Élément(s) de données
	DG9		Élément(s) de structure
	DG10		Élément(s) de substance
	DG11		Détail(s) personnel(s) supplémentaire(s)
	DG12		Détail(s) supplémentaire(s) sur le document
	DG13		Détail(s) optionnel(s)
	DG14		Options de sécurité
	DG15		Info de clé publique d'authentification active
	DG16		Personne(s) à aviser

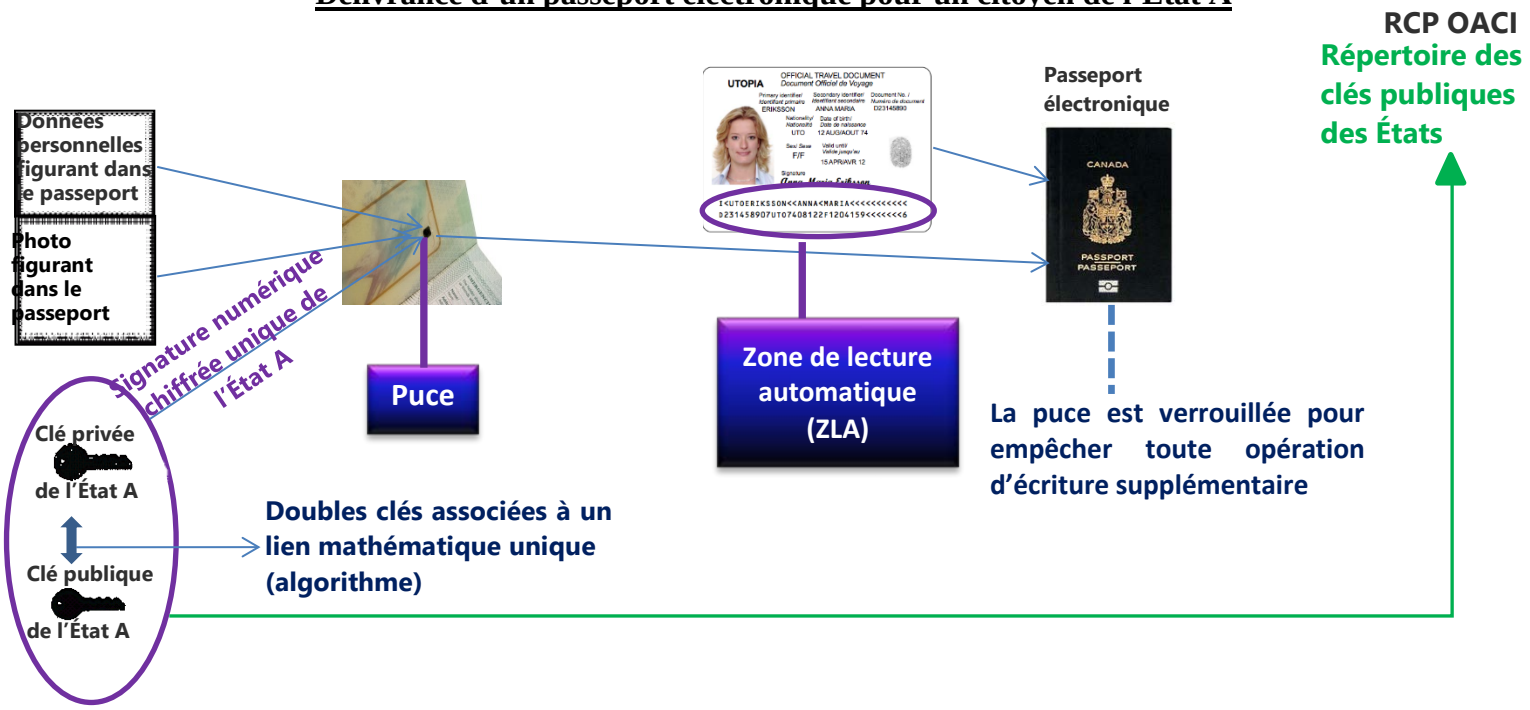
La validation en bonne et due forme de la signature numérique de l'État émetteur sur une puce de passeport électronique indique l'authenticité et l'intégrité des données stockées dans la portion de la SDL de la puce.

– – – – – – – – – – – –

APPENDICE B

DE LA DÉLIVRANCE D'UN PASSEPORT ÉLECTRONIQUE À SA VÉRIFICATION AUX FRONTIÈRES : LA CHAÎNE DE CONFIANCE

Délivrance d'un passeport électronique pour un citoyen de l'État A



Étapes de vérification à l'arrivée du citoyen de l'État A à la frontière de l'État B

Étape 1

Les données de la ZLA sont simplement une représentation de certaines des informations de la page de renseignements du passeport, ce qui permet aux ordinateurs de lire électroniquement, avec précision, les informations imprimées.

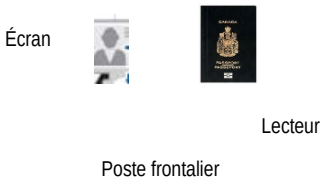
L'agent passe le passeport dans un lecteur pour détecter la ZLA, ce qui permet d'accéder à la puce du passeport électronique.

Parmi les composantes de la ZLA, une clé permet d'accéder à la puce ; le lecteur ne peut lire la puce que si la clé est la bonne.

Dans ce cas, les données et la photo sont récupérées et l'agent passe à l'étape 2 de la vérification.

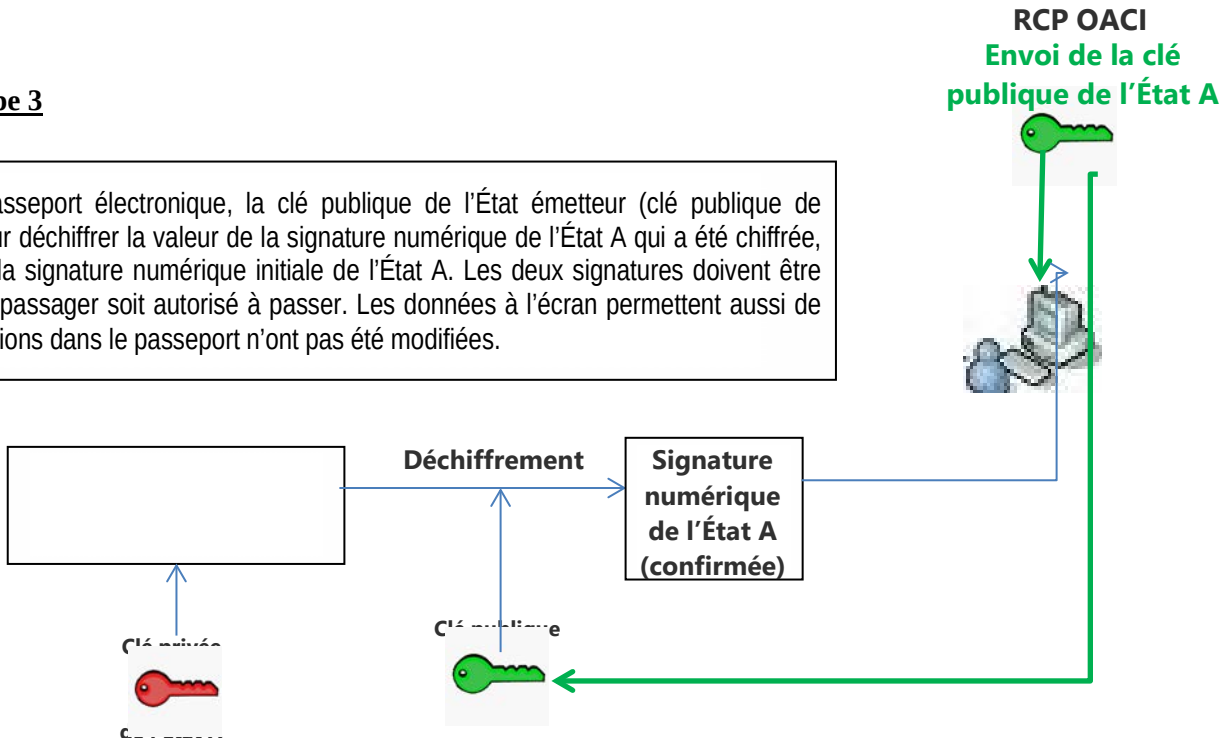
Étape 2

Après lecture de la puce, l'agent vérifie la correspondance entre le visage du détenteur du passeport et la photo figurant dans le document, ainsi que les données et la photo contenues dans la puce du passeport qui s'affichent à l'écran. L'étape suivante consiste à vérifier que le passeport a été délivré par une autorité compétente et qu'il n'a pas été modifié depuis.



Étape 3

Pour authentifier le passeport électronique, la clé publique de l'État émetteur (clé publique de l'État A) est utilisée pour déchiffrer la valeur de la signature numérique de l'État A qui a été chiffrée, et pour la comparer à la signature numérique initiale de l'État A. Les deux signatures doivent être identiques pour que le passager soit autorisé à passer. Les données à l'écran permettent aussi de vérifier que les informations dans le passeport n'ont pas été modifiées.

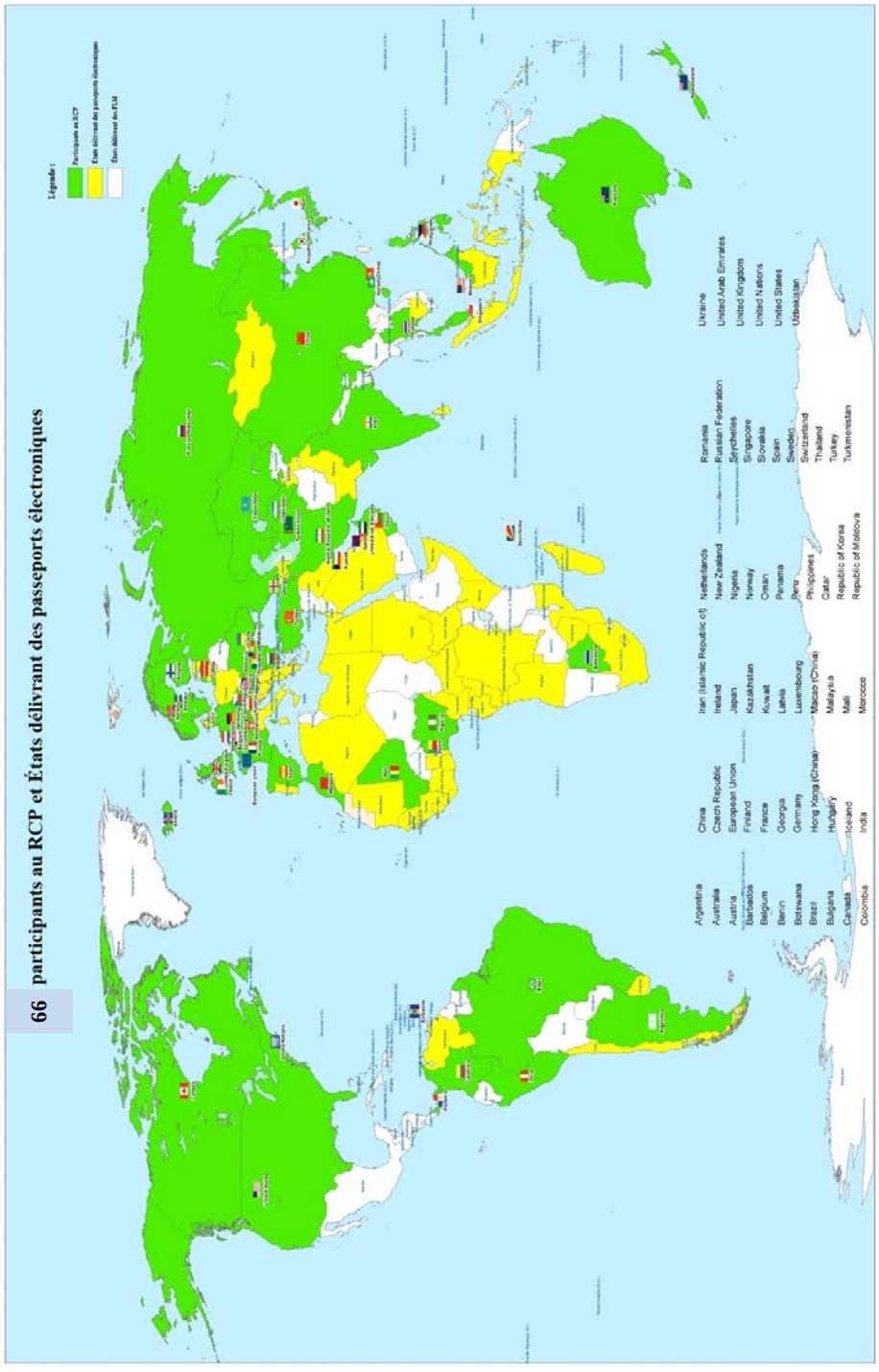


Le RCP OACI vise à valider l'authenticité de la clé publique de chaque État, sans laquelle toutes les données du passeport électronique pourraient être fausses. Ce rôle du RCP est confirmé par l'importation officielle de la clé publique de chaque participant au RCP. Toutefois, le RCP OACI ne garantit pas l'identité du détenteur du passeport, mais uniquement le fait que les données du passeport électronique n'ont pas été modifiées depuis la délivrance du passeport par une entité spécifique.

– – – – – – – – – – – –

APPENDICE C

ÉTATS ET ENTITÉS DÉLIVRANT DES PASSEPORTS ÉLECTRONIQUES ET PARTICIPANT AU RCP

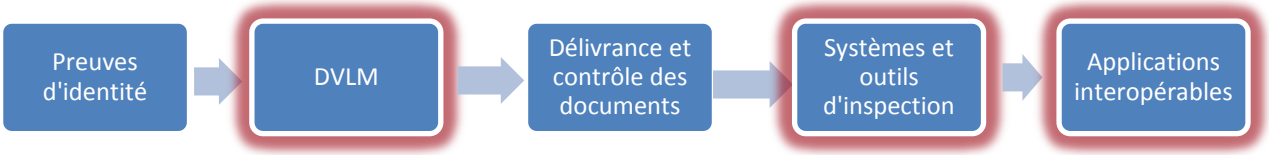


– – – – – – – – – – – –

APPENDICE D

STRATÉGIE TRIP DE L'OACI ET GESTION DU CONTRÔLE FRONTALIER

Les cinq éléments de la stratégie TRIP de l'OACI dont trois sont liés à l'utilisation du RCP

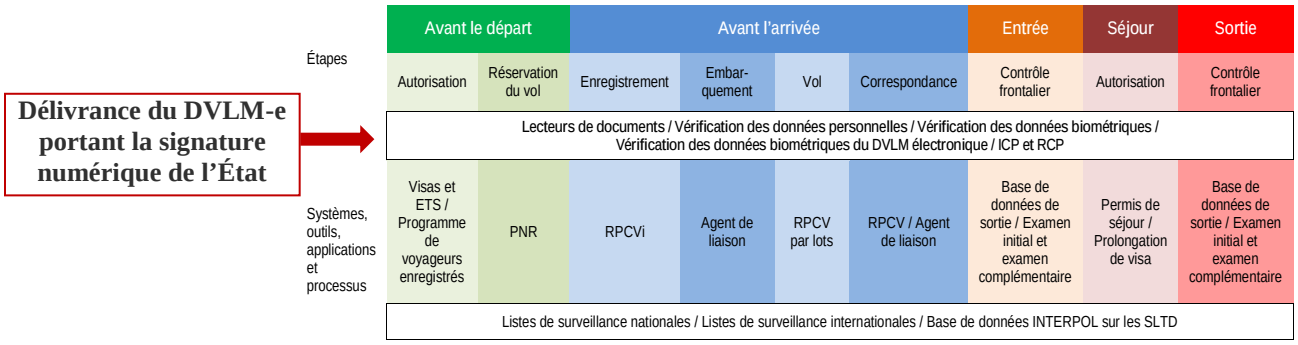


Le tableau ci-dessous énumère quelques exemples des différentes composantes des 4e et 5e éléments de la stratégie TRIP de l'OACI

SYSTÈMES ET OUTILS D'INSPECTION	APPLICATIONS INTEROPÉRABLES
Visas et Systèmes électroniques de voyage (ETS)	Renseignements préalables concernant les voyageurs (RPCV) et RPCV interactif (RPCVi)
Lecteurs de documents	Données du dossier passager (PNR)
Infrastructure de clé publique (ICP)	Infrastructure de clé publique (ICP)
Répertoire OACI de clés publiques (RCP)	Répertoire OACI de clés publiques (RCP)
Vérification des données personnelles	Vérification des données biométriques du DVLM-e
Vérification des données biométriques	Base de données INTERPOL sur les documents de voyage volés ou perdus (SLTD)
Listes de surveillance nationales	Listes de surveillance internationales
Bases de données d'entrée et de sortie	Contrôles frontaliers automatisés (CFA)
Contrôles frontaliers automatisés (CFA)	

Les différentes étapes d'un voyage

La préparation en vue de l'utilisation de l'outil RCP OACI devrait commencer à l'étape « avant le départ », au moment de l'émission du DVLM-e (2e élément TRIP). À l'étape « entrée », l'outil RCP OACI (4e élément TRIP) serait utilisé pour authentifier le DVLM-e, et son interopérabilité (5e élément TRIP) permettrait d'articuler le DVLM-e avec les autres applications interopérables.



<u>À TOUTES LES ÉTAPES DU VOYAGE</u> : Les lecteurs de documents sont utilisés pour la récupération fiable et efficace des données concernant l'identité des voyageurs. La vérification des informations personnelles est réalisée sur la base des données lues sur les documents de voyage. Lorsque cela est possible, la vérification des données biométriques et l'authentification ICP, à l'aide de l'outil RCP, contribuent à garantir l'identification des voyageurs. Une fois que l'identité du voyageur est établie à un niveau de certitude suffisant, un État peut consulter la base de données INTERPOL sur les documents de voyage volés ou perdus (SLTD), ainsi que les listes de surveillance nationales et internationales dans le cadre d'une évaluation des risques associés aux voyageurs.

– – – – – – – – – – – –

APPENDIX E

GUIDE PRATIQUE POUR ADHÉRER AU RCP OACI

1) Examen de la législation nationale : il est essentiel de réaliser un examen approfondi du cadre législatif national avant d'introduire les passeports électroniques et de participer au RCP OACI.

2) Définition des rôles et des responsabilités, et mise en œuvre d'un RCP national : les États ont la responsabilité de veiller à la qualité des données qu'ils partagent par le RCP OACI. Pour ce faire, les rôles et responsabilités des parties prenantes nationales doivent être clairement définis, et il est nécessaire que les normes techniques soient respectées et maintenues. Cela s'applique en particulier aux Répertoires de clés publiques nationaux (NPKD) qui téléverseront et téléchargeront des certificats dans et depuis le RCP OACI, ainsi qu'à l'ACSN.

3) Adhésion au RCP OACI : pour un État, la première étape consiste à signer avec l'OACI le protocole d'entente (MOU) relatif au RCP. S'ensuit alors une période de 15 mois pour apparier le NPKD avec le RCP OACI et commencer le téléversement et le téléchargement actifs. Les États souhaitant participer au RCP OACI devraient consulter le Secrétariat pour connaître les modalités du processus d'adhésion.

4) Intégration du NPKD au le RCP OACI : la dernière étape consiste en la pleine intégration du NPKD de l'État dans le RCP OACI, notamment par le téléversement et le téléchargement des certificats et des listes de révocation entre les NPKD et le RCP OACI.

— FIN —