OACI

Doc 9303

Documents de voyage lisibles à la machine

Huitième édition, 2021

Partie 9 : Déploiement de l'identification biométrique et stockage électronique des données dans les DVLM

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

OACI

Doc 9303

Documents de voyage lisibles à la machine

Huitième édition, 2021

Partie 9 : Déploiement de l'identification biométrique et stockage électronique des données dans les DVLM

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Publié séparément en français, en anglais, en arabe, en chinois, en espagnol et en russe par l'ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE
999, boul. Robert-Bourassa, Montréal (Québec) H3C 5H7 Canada

Le site http://www.icao.int/Security/FAL/TRIP permet de télécharger les documents et d'obtenir des renseignements supplémentaires.

Doc 9303, *Documents de voyage lisibles à la machine*
Partie 9 — *Déploiement de l'identification biométrique et stockage électronique des données dans les DVLM*

Commande nº : 9303P9
ISBN 978-92-9265-483-2 (version imprimée)
ISBN 978-92-9275-354-2 (version électronique)

AMENDEMENTS

La parution des amendements est annoncée dans les suppléments au *Catalogue des produits et services*. Le Catalogue et ses suppléments sont disponibles sur le site web de l'Organisation à l'adresse suivante : www.icao.int. Le tableau ci-dessous est destiné à rappeler les divers amendements.

RELEVÉ DES AMENDEMENTS ET DES RECTIFICATIFS

AMENDEMENTS		
N°	Date	Inscrit par
1	20/3/24	OACI

RECTIFICATIFS		
N°	Date	Inscrit par

Les appellations employées dans cette publication et la présentation des éléments qui y figurent n'impliquent de la part de l'OACI aucune prise de position quant au statut juridique des pays, territoires, villes ou zones, ou de leurs autorités, ni quant au tracé de leurs frontières ou limites.

TABLE DES MATIÈRES

1. PORTÉE

Les spécifications définies dans la Partie 9 du Doc 9303 s'ajoutent aux spécifications applicables aux DVLM de base définies dans les Parties 3, 4, 5, 6 et 7 du Doc 9303. Elles doivent être utilisées par les États ou les organisations qui souhaitent émettre un DVLM électronique (DVLM-e) utilisable par tout État récepteur ou organisation réceptrice convenablement équipé pour lire et authentifier les données concernant le DVLM-e lui-même et la vérification de son détenteur. Ces données comprennent des données biométriques obligatoires, interopérables à l'échelle mondiale et utilisables comme entrées dans des systèmes de reconnaissance faciale, et, de façon optionnelle, dans des systèmes de reconnaissance d'empreintes digitales ou de l'iris. Ces spécifications exigent que les données biométriques interopérables à l'échelle mondiale soient stockées sous forme d'images haute résolution sur un circuit intégré (CI) sans contact de grande capacité, qui contient aussi une reproduction codée des données de la zone de lecture automatique (ZLA). Les spécifications autorisent également le stockage de diverses données optionnelles, à la discrétion de l'État émetteur ou de l'organisation émettrice. L'utilisation de CI sans contact étant indépendante de la taille du document, les spécifications s'appliquent à tous les formats de DVLM dotés de fonctions électroniques. Les différences entre les formats de DVLM-e concernent la ZLA et ont des incidences sur le stockage de la ZLA dans le CI sans contact. Ces différences sont indiquées dans les spécifications relatives à la structure de données logique (SDL) énoncées dans le Doc 9303-10.

La Partie 9 doit être lue en parallèle avec les parties suivantes du Doc 9303 :

- Partie 1 — *Introduction*
- Partie 10 — *Structure de données logique (SDL) pour le stockage des données biométriques et d'autres données dans le circuit intégré (CI) sans contact*
- Partie 11 — *Mécanismes de sécurité pour les DVLM*
- Partie 12 — *Infrastructure à clés publiques pour les DVLM*

2. DVLM-e

Note.— Les termes DVLM et DVLM-e sont employés dans le présent document comme désignations génériques de tous les documents de voyage lisibles à la machine et s'appliquent respectivement aux documents à reconnaissance optique de caractères et aux documents électroniques. Les termes TD1, TD2 et TD3 désignent différents formats de DVLM. Tous les DVLM-e dont il est question dans la présente partie sont dotés de fonctions électroniques.

2.1 Conformité au Doc 9303

Un DVLM-e DOIT être conforme à tous égards aux spécifications énoncées dans le Doc 9303.

2.2 Période de validité d'un DVLM-e

La période de validité d'un DVLM-e est à la discrétion de l'État émetteur ou l'organisation émettrice ; toutefois, compte tenu de la durabilité limitée des documents et de l'évolution de l'apparence physique du détenteur au fil du temps, il est

RECOMMANDÉ qu'elle ne soit pas supérieure à 10 ans. Il est POSSIBLE d'opter pour une période plus courte afin de permettre la mise à niveau progressive du DVLM-e à mesure qu'évolue la technologie.

2.3 Symbole indiquant la présence d'une puce électronique

Le Partie 9 du Doc 9303 porte principalement sur la biométrie appliquée aux DVLM et utilise le terme DVLM-e pour désigner les DVLM dotés de fonctions biométriques et interopérables à l'échelle mondiale. Les DVLM qui ne sont pas conformes aux spécifications du Doc 9303 ne peuvent pas être appelés DVLM-e et ne doivent pas porter le symbole indiquant la présence d'une puce électronique à l'intérieur du document.

Tous les DVLM-e doivent porter le symbole suivant :

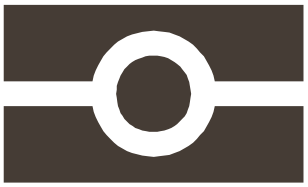


Figure 1. Symbole indiquant la présence d'une puce électronique

Un fichier électronique de ce symbole est disponible sur le site web de l'OACI. Le symbole DOIT figurer uniquement sur un DVLM-e qui contient un CI sans contact, d'une capacité de stockage suffisante pour contenir les éléments de données obligatoires, conformément à la SDL (Doc 9303-10), toutes les données entrées étant sécurisées par une signature numérique conforme aux spécifications du Doc 9303-11. Un DVLM-e NE DOIT PAS être décrit comme DVLM-e ni porter le symbole indiquant la présence d'une puce électronique s'il ne répond pas à ces exigences minimales. Le symbole doit figurer près du bord supérieur ou du bord inférieur de la couverture avant d'un DVLM-e en livret de format TD3 (PLM-e), ou au recto du DVLM-e s'il s'agit d'une carte (DVOLM-e).

Sur un PLM-e, le symbole doit être inséré dans l'estampage métallisé ou autre image figurant sur la couverture avant. Il est recommandé de l'imprimer aussi sur la page de renseignements, dans une couleur appropriée et à un endroit qui ne gênera pas la lecture d'autres données. L'État émetteur ou l'organisation émettrice peut aussi imprimer ce symbole sur la page intérieure ou la face intérieure de couverture du passeport en livret qui contient le CI sans contact ou, à sa discrétion, ailleurs dans le passeport.

Sur un DVOLM-e, le symbole DOIT figurer au recto du DVOLM-e, de préférence dans la zone 1.

L'image, représentée à la Figure 1, est un positif, ce qui signifie que la partie noire de l'image est celle qui doit être imprimée ou autrement reproduite. Il est RECOMMANDÉ que le symbole soit visible à l'œil nu et qu'il soit facilement reconnaissable.

La Figure 2 montre les dimensions RECOMMANDÉES du symbole tel qu'il doit figurer sur la couverture ou la page de renseignements d'un PLM-e ou sur un TD2 électronique.

Il est RECOMMANDÉ d'employer une taille plus petite, de 4,2 × 7,2 mm (0,17 × 0,28 in), réduite proportionnellement, pour un TD1 électronique.

Le symbole PEUT être redimensionné proportionnellement pour être utilisé, par exemple, dans des motifs de fond.

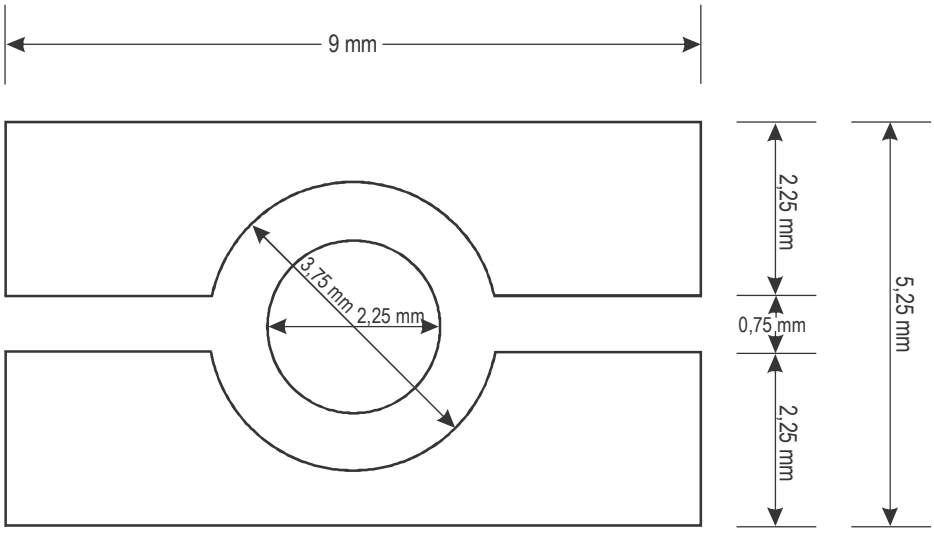


Figure 2. Dimensions du symbole

Note.— Les dimensions correspondantes en pouces sont : 9,0 mm (0,35 in), 5,25 mm (0,21 in), 3,75 mm (0,15 in), 2,25 mm (0,09 in), 0,75 mm (0,03 in).

2.4 Avertissement de manipuler le PLM-e avec soin

Il est suggéré de placer, à un endroit bien visible du livret, un avertissement invitant instamment le détenteur du PLM-e à prendre soin de ce document, par exemple :

« Ce passeport contient des éléments électroniques sensibles. Pour une performance optimale, ne pas le plier, le perforer ni l'exposer à des températures extrêmes ou à une humidité excessive. »

L'État émetteur ou l'organisation émettrice pourrait aussi indiquer sur la partie de la page contenant le CI, et sur les parties correspondantes de pages adjacentes, la mise en garde :

« Ne pas apposer de cachet à cet endroit. »

3. IDENTIFICATION BIOMÉTRIQUE

Le terme « identification biométrique » est un terme générique employé pour décrire des moyens informatisés de reconnaissance d'une personne vivante, qui utilisent la mesure de caractéristiques physiques ou comportementales distinctives.

Un « gabarit biométrique » est une représentation en code machine de caractéristiques distinctives créée au moyen d'un algorithme logiciel ; il permet de procéder à des comparaisons pour établir un score du degré de confiance avec lequel des enregistrements des caractéristiques créés séparément identifient (ou n'identifient pas) la même personne. En général, le volume de données d'un gabarit biométrique est relativement petit ; toutefois, chaque fabricant de système biométrique utilise son propre format de gabarit et les gabarits ne sont pas interchangeables entre systèmes. Pour qu'un État ou une organisation puisse choisir un système biométrique qui convienne à ses besoins, les données

doivent être stockées sous une forme qui permettra au système de cet État ou de cette organisation d'en tirer un gabarit. Il faut pour cela que les données biométriques soient stockées sous forme d'une ou de plusieurs images.

3.1 Vision de l'OACI en matière de biométrie

La vision de l'OACI en ce qui concerne l'application des technologies biométriques porte sur les aspects suivants :

- spécification d'une forme principale interopérable de technologie biométrique, à utiliser aux points de contrôle frontalier (vérification, listes de surveillance) ainsi que par les transporteurs et les émetteurs de documents, et spécification des technologies biométriques complémentaires convenues ;

- spécification des technologies biométriques à utiliser par les émetteurs de documents (identification, vérification et listes de surveillance) ;

- possibilité d'extraire les données pendant 10 ans, la période de validité maximale recommandée pour un document de voyage ;

- absence d'éléments propriétaires, pour que les États ou organisations qui investissent dans la biométrie soient protégés contre les changements d'infrastructure ou les changements de fournisseurs.

Le Doc 9303 ne prévoit que trois types de systèmes d'identification biométrique. En ce qui concerne le stockage des éléments biométriques dans le CI sans contact d'un DVLM-e, l'État émetteur ou l'organisation émettrice DOIT se conformer à la norme internationale applicable.

Les trois types d'identification biométrique sont :

- la reconnaissance faciale (REQUISE) ;

- la reconnaissance d'empreinte digitale (OPTIONNELLE) ;

- la reconnaissance d'iris (OPTIONNELLE).

La norme ISO/IEC 39794 a succédé à l'ISO/IEC 19794:2005 comme norme internationale pour le codage des données biométriques. Le calendrier de transition suivant a été défini :

- les systèmes d'inspection DOIVENT être en mesure de traiter les données ISO/IEC 39794 d'ici le 01-01-2026, après une période de préparation de six ans débutant le 01-01-2020 ;

- entre 2026 et 2030, les États et les organisations émetteurs peuvent utiliser les formats de données spécifiés dans la norme ISO/IEC 19794-X:2005 ou dans la norme ISO/IEC 39794-X pendant une période de transition de quatre ans. Pendant cette période de transition, les tests d'interopérabilité et de conformité seront essentiels ;

- à partir du 01-01-2030, les États et les organisations émetteurs DOIVENT utiliser la norme ISO/IEC 39794-X pour le codage des données biométriques.

Le Doc 9303, partie 10, Amendement nº1 fournit des orientations sur la transition de l'ISO/IEC 19794:2005 à l'ISO/IEC 39794.

Terminologie

Les termes suivants sont employés dans l'identification biométrique :

- « vérifier » signifie procéder à une comparaison individuelle (1:1) entre des données biométriques présentées, obtenues du détenteur d'un DVLM-e au moment de présenter les données, et un gabarit biométrique créé lorsque le détenteur s'est enrôlé dans le système ;

- « identifier » signifie procéder à une recherche un-à-beaucoup (1:N) entre des données biométriques présentées et un ensemble de gabarits représentant tous les sujets qui se sont enrôlés dans le système.

Des éléments biométriques peuvent être utilisés dans la fonction d'identification pour améliorer la qualité de la vérification d'antécédents effectuée dans le cadre du processus de demande de passeport, de visa ou d'un autre document de voyage et ils peuvent être utilisés pour établir une correspondance positive entre le document de voyage et la personne qui le présente.

Aux fins de la présente partie, les termes et définitions du vocabulaire biométrique donnés dans la norme ISO/IEC 2382-37:2017 s'appliquent.

3.2 Considérations essentielles

Les considérations essentielles suivantes doivent être prises en compte dans la spécification des applications biométriques pour les DVLM-e :

- *Interopérabilité mondiale.* Nécessité cruciale de spécifier un système de déploiement qui doit être utilisé d'une manière interopérable universellement ;

- *Uniformité.* Nécessité de réduire au minimum, dans la mesure du possible, par l'établissement de normes spécifiques les variations entre les différentes solutions susceptibles d'être déployées par les États émetteurs ou les organisations émettrices ;

- *Fiabilité technique.* Nécessité d'établir des lignes directrices et des paramètres pour faire en sorte que les États émetteurs ou les organisations émettrices déploient des technologies éprouvées assurant un haut niveau de confiance en matière de confirmation d'identité, et donner aux États ou organisations qui lisent des données codées par d'autres États émetteurs ou organisations émettrices l'assurance que les données qui leur sont fournies sont d'une qualité et d'une intégrité suffisantes pour permettre une vérification précise dans leurs propres systèmes ;

- *Fonctionnalité.* Nécessité de faire en sorte que les normes recommandées puissent devenir opérationnelles et être mises en œuvre par les États ou les organisations sans qu'ils aient à introduire une pléthore de systèmes et d'équipements disparates pour répondre à toutes les variations et interprétations possibles des normes ;

- *Durabilité.* Nécessité pour les systèmes mis en place de continuer à prendre en charge les documents de voyage pendant leur durée de vie maximale recommandée, qui est de 10 ans, et pour les mises à jour futures d'être rétro-compatibles.

3.3 Processus clés en biométrie

Les principaux processus d'un système biométrique consistent à :

- *Établir l'identité.* Faire en sorte que l'identité de la personne enrôlée soit connue sans aucun doute ;
- *Capturer.* Acquisition d'un échantillon biométrique brut ;
- *Extraire.* Conversion des données de l'échantillon biométrique brut en une forme intermédiaire ;
- *Créer un gabarit*. Conversion des données intermédiaires en gabarit ;
- *Comparer*. Comparaison avec les informations que contient un gabarit de référence conservé en mémoire.

Ces processus s'articulent comme suit :

- Le processus d'*enrôlement*, qui repose sur la *capture* d'un échantillon biométrique brut, est utilisé pour chaque nouvelle personne (titulaire potentiel de DVLM-e) et consiste à prélever des échantillons d'images biométriques qui seront stockés. Le processus de capture est l'acquisition automatisée de l'élément biométrique au moyen d'un dispositif tel qu'un scanneur d'empreintes digitales, un scanneur de photographies, un appareil photo numérique pour capture en direct ou une caméra avec zoom pour capture en direct de l'iris. Chacun de ces dispositifs nécessite la définition de certains critères et de certaines procédures pour le processus de capture — par exemple, pose normalisée face à l'appareil photo pour capture d'image destinée à la reconnaissance faciale ; capture des empreintes digitales à plat ou déroulées ; yeux bien ouverts pour capture de l'iris. L'image qui en résulte est comprimée, puis stockée pour une confirmation future de l'identité.

- Le processus de *création de gabarit* préserve les caractéristiques biométriques distinctes et reproductibles provenant de l'image biométrique capturée et utilise généralement un algorithme logiciel propriétaire pour extraire un gabarit de l'image stockée. L'image est définie de telle façon qu'elle pourra par la suite être comparée à une autre image échantillon capturée au moment où une confirmation d'identité sera nécessaire et où un score comparatif sera déterminé. Un élément intrinsèque de cet algorithme est un contrôle qualité à l'aide d'un mécanisme d'évaluation de la qualité de l'échantillon. Les normes de qualité doivent être aussi élevées que possible, car toutes les vérifications futures sont tributaires de la qualité de l'image capturée à l'origine. Si la qualité n'est pas acceptable, le processus de *capture* devrait être répété.

- Le processus d'*identification* prend le gabarit tiré du nouvel échantillon et le compare à des gabarits mis en mémoire d'utilisateurs enrôlés pour déterminer si l'utilisateur s'est déjà enrôlé dans le système et, dans l'affirmative, si c'est sous la même identité.

- Le processus de *vérification* prend le nouvel échantillon d'un détenteur de DVLM-e et le compare à un gabarit tiré de l'image stockée de ce détenteur pour déterminer si celui-ci se présente sous la même identité.

3.4 Applications d'une solution biométrique

L'application essentielle des techniques biométriques est la vérification d'identité, qui établit la relation entre le détenteur d'un DVLM-e et le DVLM-e dont ledit détenteur est porteur.

Plusieurs applications typiques de la biométrie interviennent au cours du processus d'enrôlement qu'implique la demande d'un DVLM-e.

Les données biométriques de l'utilisateur générées par le processus d'enrôlement peuvent être utilisées pour une recherche dans une ou plusieurs bases de données biométriques (identification), afin de déterminer si l'utilisateur est connu de l'un des systèmes correspondants (par exemple, comme étant titulaire d'un DVLM-e sous une identité différente, ayant un casier judiciaire ou étant détenteur d'un DVLM-e d'un autre État ou d'une autre organisation).

Lorsque les utilisateurs entrent en possession du DVLM-e (ou se présentent pour une des étapes du processus de délivrance, après le dépôt de la demande initiale et la capture des données biométriques), ses données biométriques peuvent être recueillies de nouveau et vérifiées par rapport aux données biométriques capturées initialement.

L'identité des agents qui procèdent à l'enrôlement peut être vérifiée pour confirmer que ces agents sont habilités à effectuer les tâches qui leur sont confiées. Ce processus peut comprendre une authentification biométrique pour initier une signature numérique de journaux d'audit de différentes étapes du processus d'émission, permettant ainsi à la biométrie de relier les agents aux opérations dont ils ont la responsabilité.

Il y a aussi plusieurs applications typiques de la biométrie aux frontières.

Chaque fois qu'un voyageur (c'est-à-dire un détenteur de DVLM-e) entre dans un État ou sort d'un État, son identité peut être vérifiée par rapport à l'image créée lors de la délivrance de son document de voyage. Cela permet de s'assurer que le détenteur d'un document est bien le titulaire légitime à qui ce document a été délivré et renforce l'efficacité de tout système de renseignements préalables concernant les voyageurs (RPCV). Un État émetteur ou une organisation émettrice jugera peut-être utile de stocker le ou les gabarits biométriques sur le document de voyage avec l'image, de sorte que l'identité d'un voyageur pourra être vérifiée aux endroits à l'intérieur du pays où le système biométrique est sous le contrôle de l'émetteur.

Vérification sur deux facteurs — Il est possible de comparer les données d'images biométriques actuelles capturées sur le voyageur et les données biométriques provenant de son document de voyage (ou d'une base de données centrale) (s'il y a lieu en construisant des gabarits biométriques de chacune) pour confirmer que le document de voyage n'a pas été altéré.

Vérification sur trois facteurs — Il est possible de comparer les données d'images biométriques actuelles capturées sur le voyageur, les données biométriques figurant dans son document de voyage et les données biométriques stockées dans une base de données centrale (s'il y a lieu, en construisant des gabarits biométriques de chacune) pour confirmer que le document de voyage n'a pas été altéré. Cette technique établit la correspondance entre la personne, son DVLM-e et la base de données où sont enregistrées les données qui ont été inscrites dans ce DVLM-e lors de sa délivrance.

Vérification sur quatre facteurs — Une quatrième vérification confirmatoire, qui n'est pas électronique, est la comparaison visuelle des résultats de la vérification sur trois facteurs avec la photographie numérisée qui figure sur le DVLM-e du voyageur.

Outre les applications de la biométrie pour l'enrôlement et les contrôles frontaliers, utilisées dans les comparaisons 1:1 et 1:N, les États ou organisations devraient aussi considérer les aspects suivants et fixer leurs propres critères à leur propos :

- Précision des fonctions de comparaison biométrique du système. Les États émetteurs ou les organisations émettrices doivent coder l'image faciale sur le DVLM-e et, à titre facultatif, un ou plusieurs éléments biométriques sur l'empreinte digitale ou l'iris, conformément aux spécifications relatives à la SDL. (Les éléments biométriques peuvent aussi être stockés dans une base de données à laquelle a accès l'État récepteur ou l'organisation réceptrice.) L'image biométrique est normalisée par l'OACI, mais il appartient aux États récepteurs ou aux organisations réceptrices de choisir leur propre logiciel de vérification biométrique et de déterminer leurs propres seuils pour les scores d'acceptation de la vérification d'identité et le rejet des imposteurs.

- Le débit (par exemple, nombre de voyageurs par minute) du système biométrique ou du système de contrôle frontalier dans son ensemble.

- L'adéquation d'une technologie biométrique donnée (visage ou empreinte digitale ou caractéristiques oculaires) aux contrôles frontaliers.

3.5 Contraintes liées aux technologies biométriques

Il est reconnu que la mise en œuvre de la plupart des technologies biométriques est fonction de leur développement. Vu la rapidité de l'évolution des technologies, toutes les spécifications (y compris celles qui sont énoncées dans le présent document) doivent tenir compte de cette évolution et des changements qui résulteront des améliorations technologiques.

Les informations biométriques stockées sur les documents de voyage doivent être conformes aux lois nationales de l'État émetteur ou de l'organisation émettrice en matière de protection des données et de protection de la vie privée.

4. SÉLECTION DES ÉLÉMENTS BIOMÉTRIQUES APPLICABLES AUX DVLM-e

On sait depuis longtemps que le nom et la réputation ne sont pas des traits suffisants pour garantir que le détenteur à qui un document de voyage (DVLM-e) a été délivré par l'État émetteur ou l'organisation émettrice est la personne qui, dans un État récepteur ou une organisation réceptrice, affirme être le même détenteur.

La seule méthode qui permette de relier la personne à son document de voyage de façon incontestable consiste à associer d'une manière infalsifiable une caractéristique physique, c'est-à-dire un élément biométrique, de cette personne à son document de voyage.

4.1 Élément biométrique principal : image faciale

Codage d'images de visages de référence

Le portrait imprimé sur le DVLM conforme aux normes de l'OACI est un élément essentiel de ce document et l'un des plus importants supports d'information liant le document à son détenteur. Un portrait normalisé de haute qualité aide les organismes de délivrance à contrôler l'identité et les organismes frontaliers à inspecter le document de voyage manuellement ou par traitement automatisé. L'Annexe D.1 de la norme ISO/IEC 39794-5 spécifie les exigences relatives à la capture et au codage des images du visage.

4.2 Éléments biométriques supplémentaires optionnels

Les États émetteurs ou les organisations émettrices peuvent, de façon optionnelle, ajouter des données supplémentaires à leurs processus de vérification d'identité (et à ceux d'autres États) en incluant plusieurs éléments biométriques dans leurs documents de voyage, c'est-à-dire une combinaison de visage et/ou d'empreintes digitales et/ou d'iris. Ces éléments supplémentaires sont particulièrement pertinents lorsque des États ou des organisations possèdent déjà des bases de données d'empreintes digitales ou oculaires, par rapport auxquelles il leur est possible de vérifier les éléments biométriques qui leur sont présentés, par exemple dans le cadre d'un système de cartes ID.

Stockage d'un élément biométrique optionnel — empreinte digitale

Il existe trois classes de technologies biométriques basées sur les empreintes digitales : systèmes basés sur des images de doigts, systèmes basés sur les minuties du doigt et systèmes basés sur la forme du doigt. Des normes ont été établies pour rendre la plupart des systèmes interopérables au sein de leur classe, mais ils ne sont pas interopérables entre classes. C'est ainsi que l'on voit émerger trois normes pour l'interopérabilité des empreintes digitales : stockage des données d'images, stockage des données de minuties et stockage des données de forme. Lorsqu'un État émetteur ou une organisation émettrice choisit d'insérer des données d'empreintes digitales dans son DVLM-e, le stockage de l'image de l'empreinte digitale est obligatoire pour permettre une interopérabilité mondiale entre classes. Le stockage d'un gabarit qui lui est associé est optionnel, à la discrétion de l'État émetteur ou de l'organisation émettrice.

Lorsqu'un État émetteur ou une organisation émettrice choisit de stocker sur le CI sans contact une ou des images d'empreintes digitales, la taille optimale de l'image DEVRAIT être adéquate pour une vérification 1:1.

La norme ISO/IEC 39794-4 spécifie les exigences relatives à la capture et au codage des images de doigts.

Stockage d'un élément biométrique optionnel — iris

Lorsqu'un État émetteur ou une organisation émettrice choisit de fournir des données sur l'iris dans son DVLM-e, le stockage de l'image de l'iris est obligatoire pour permettre l'interopérabilité mondiale. Le stockage d'un gabarit qui lui est associé est optionnel, à la discrétion de l'État émetteur ou de l'organisation émettrice.

Lorsqu'un État émetteur ou une organisation émettrice choisit de stocker sur le CI sans contact une ou des images d'iris, la taille optimale de l'image DEVRAIT être adéquate pour une vérification 1:1.

La norme ISO/IEC 39794-6 spécifie les exigences relatives à la capture et au codage des images d'iris.

5. STOCKAGE DE DONNÉES BIOMÉTRIQUES ET AUTRES EN FORMAT LOGIQUE DANS UN CI SANS CONTACT

Il est EXIGÉ que des images numériques soient utilisées et qu'elles soient stockées électroniquement dans le document de voyage.

5.1 Caractéristiques du CI sans contact

Le support de stockage électronique spécifié par l'OACI comme technologie d'expansion de capacité à utiliser dans les DVLM-e pour le déploiement de la biométrie EST un CI sans contact de grande capacité.

CI sans contact et codage

Les CI sans contact utilisés dans les DVLM-e DOIVENT être conformes aux normes ISO/IEC 14443, type A ou type B, et ISO/IEC 7816-4. La SDL DOIT être codée selon la méthode de l'accès direct. La distance de lecture (obtenue par une combinaison du DVLM-e et du dispositif de lecture) va généralement jusqu'à 10 cm, comme il est indiqué dans la norme ISO/IEC 14443. Un profil d'application conforme à la norme ISO/IEC 14443 pour les DVLM figure dans le Doc 9303, Partie 10.

Capacité de stockage de données du CI sans contact

La capacité de stockage de données du CI sans contact est à la discrétion de l'État émetteur ou de l'organisation émettrice, mais DOIT être suffisante pour stocker l'image faciale obligatoire, la reproduction des renseignements figurant dans la ZLA et les éléments nécessaires pour sécuriser les données. Le stockage d'images supplémentaires du visage, d'empreintes digitales et/ou de l'iris peut exiger une augmentation significative de la capacité de stockage. Il n'est pas spécifié de capacité de données maximale pour le CI.

Stockage d'autres données

Un État émetteur ou une organisation émettrice PEUT utiliser la capacité de stockage du CI sans contact dans un DVLM-e pour accroître la capacité de données lisibles par machine du DVLM-e au-delà de celle qui est définie pour les échanges mondiaux. Il peut s'agir, par exemple, de donner accès, avec lecture par machine, à des renseignements issus de documents sources (par exemple, détails du certificat de naissance), aux détails de confirmation d'identité personnelle stockée (biométrie) et/ou de vérification de l'authenticité du document.

5.2 Structure de données logique

Pour assurer l'interopérabilité universelle aux fins de la lecture par machine des détails stockés, il FAUT utiliser une structure de données logique (SDL) qui définit le format d'enregistrement des détails dans le CI sans contact.

Structure des données stockées

La SDL est spécifiée dans le Doc 9303-10, qui décrit en détail les informations, obligatoires et optionnelles, à inclure dans des blocs de données biométriques spécifiques de la SDL.

Éléments de données minimaux à stocker dans la SDL

Les éléments de données obligatoires minimaux à stocker dans la SDL sur le CI sans contact DOIVENT être une reproduction des données de la ZLA dans le groupe de données 1 et de l'image faciale du titulaire dans le groupe de données 2. De plus, dans un DVLM-e conforme, le CI DOIT contenir l'objet de sécurité (EF.SOD) nécessaire pour valider l'intégrité des données créées par l'émetteur — stocké dans le fichier dédié n° 1 comme le spécifie la SDL (voir le Doc 9303-10). L'objet de sécurité (EF.SOD) est constitué des hachages des groupes de données utilisés.

5.3 Sécurité des données stockées et protection de l'information personnelle

Tant les États émetteurs ou les organisations émettrices que les États récepteurs doivent avoir l'assurance que les données stockées sur le CI sans contact n'ont pas été altérées depuis qu'elles ont été enregistrées au moment de la délivrance du document. De plus, les lois des États émetteurs ou des organisations émettrices ou leurs pratiques en matière de protection des renseignements personnels peuvent exiger que l'accès aux données ne soit possible que pour une personne ou un organisme autorisé. C'est pourquoi l'OACI a élaboré les spécifications énoncées dans le Doc 9303-11 et le Doc 9303-12, concernant l'application et l'utilisation de techniques modernes de cryptographie, en

particulier les dispositifs d'infrastructure à clés publiques (ICP), qui DOIVENT être utilisés par les États émetteurs ou les organisations émettrices dans leurs DVLM établis conformément aux spécifications du Doc 9303. Il s'agit essentiellement de renforcer la sécurité par des moyens informatisés d'authentification des DVLM-e et de leurs détenteurs légitimes internationalement. De plus, des méthodes sont recommandées pour mettre en œuvre une authentification internationale des DVLM-e et ouvrir la voie à leur utilisation pour faciliter les applications biométriques ou de commerce électronique. Les spécifications du Doc 9303-11 permettent à l'État émetteur ou à l'organisation émettrice de protéger les données stockées contre l'accès non autorisé au moyen d'un contrôle d'accès.

La présente édition du Doc 9303 est basée sur l'hypothèse que les données DSL1 ne seront pas écrites sur le CI sans contact après sa personnalisation. L'étape finale du processus de personnalisation DOIT donc être de verrouiller le CI sans contact. Une fois le CI sans contact verrouillé (après la personnalisation et avant la délivrance) d'autres données ne peuvent être écrites sur le CI sans contact qu'après l'exécution réussie d'un mécanisme d'authentification (TA), comme spécifié dans le document 9303-10 et Doc 9303-11. Après la délivrance du DVLM-e, un CI sans contact verrouillé ne peut plus être déverrouillé.

Infrastructure à clés publiques (ICP)

Le but du mécanisme ICP décrit est principalement de permettre aux autorités d'inspection des DVLM-e (États récepteurs ou organisations réceptrices) de vérifier l'authenticité et l'intégrité des données stockées dans le DVLM-e. Les spécifications n'ont pas pour but de prescrire une mise en œuvre intégrale d'une structure ICP complexe, mais visent plutôt à indiquer un mode d'implémentation permettant aux États ou aux organisations de faire des choix dans plusieurs domaines (tels que l'authentification active, l'anti-écrémage, le contrôle d'accès, le contrôle frontalier automatisé, etc.), ce qui leur donne la possibilité de mettre en œuvre progressivement des fonctions supplémentaires sans qu'il y ait non-conformité avec le cadre d'ensemble.

Des certificats sont employés pour la sécurisation, avec une méthodologie pour la diffusion de (certificats de) clés publiques aux États membres ou organisations, et l'ICP est adaptée pour répondre aux objectifs de l'OACI.

Les spécifications relatives à l'ICP sont énoncées en détail dans le Doc 9303-12.

6. MÉTHODES D'ESSAI POUR LES DVLM-e

L'OACI, en coopération avec l'ISO, a mis au point des méthodes d'essai pour établir la conformité des DVLM-e avec les spécifications énoncées dans les parties 9, 10, 11 et 12 du Doc 9303. Ces méthodes d'essai sont spécifiées dans les rapports techniques de l'OACI et sont tenues à jour sous la coordination de l'ISO/CEI JTC 1/SC 17/WG 3.

Il est RECOMMANDÉ aux États émetteurs et aux organisations émettrices de qualifier leurs DVLM-e, leurs systèmes d'inspection et leurs solutions ICP en fonction des spécifications d'essai indiquées ci-après :

ISO/IEC 18745-2	Essais spécifiques de l'interface sans contact des DVLM-e
OACI — TR RF & PROTOCOL P3	Essai de la SDL et des protocoles
OACI — TR RF & PROTOCOL P4	Essais pour les systèmes d'inspection
OACI — TR RF & PROTOCOL P5	Tests pour les objets ICP

7. RÉFÉRENCES (NORMATIVES)

OACI — TR RF & PROTOCOL P3	RF Protocol and Application Test Standard for eMRTD — Part 3: Tests for Application Protocol and Logical Data Structure.
OACI — TR RF & PROTOCOL P4	RF Protocol and Application Test Standard for eMRTD — Part 4: Conformity Test for Inspection Systems.
OACI — TR RF & PROTOCOL P5	RF Protocol and Application Test Standard for eMRTD — Part 5: Tests pour les objets ICP.
ISO/IEC 2382-37	Technologies de l'information – Vocabulaire – Partie 37 : Biométrie
ISO/IEC 7816-4	ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange* (Cartes d'identification — Cartes à circuit intégré — Partie 4 : Organisation, sécurité et commandes pour les échanges).
ISO/IEC 10373-6	ISO/IEC 10373-6:2016, *Identification cards — Test methods — Part 6: Proximity cards* (Cartes d'identification — Méthodes d'essai — Partie 6 : Cartes de proximité).
ISO/IEC 18745-2	ISO/IEC 18745-2:2016, *Information technology — Test methods for machine readable travel documents (MRTD) and associated devices — Part 2: Test methods for the contactless interface* [Technologies de l'information — Méthodes d'essais pour documents de voyage lisibles par machine et dispositifs associés — Partie 2 : Méthodes d'essais de l'interface sans contact].
ISO/IEC 14443-1	ISO/IEC 14443-1:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics* [Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité — Partie 1 : Caractéristiques physiques].
ISO/IEC 14443-2	ISO/IEC 14443-2:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface* [Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité — Partie 2 : Interface radiofréquence et des signaux de communication]. *Note.— Les dernières modifications de la norme ISO/IEC 14443-2 spécifient des limites REQUISES de perturbation électromagnétique (EMD). Cependant, les DVLM-e déjà délivrés et en cours d'émission ne sont pas nécessairement conformes à ce nouveau paramètre. Pour conserver la compatibilité amont en matière de conformité, les limites EMD spécifiées dans la norme ISO/IEC 14443-2 devraient demeurer OPTIONNELLES pour les DVLM-e dans le cadre du Doc 9303.*
ISO/IEC 14443-3	ISO/IEC 14443-3:2016 (version corrigée du 01/09/2016), *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision* [Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité — Partie 3 : Initialisation et anticollision].

ISO/IEC 14443-4	ISO/IEC 14443-4:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol* [Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité — Partie 4 : Protocole de transmission].
ISO/IEC 19794-4	ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data* (Technologies de l'information — Formats d'échange de données biométriques — Partie 4 : Données d'image du doigt).
ISO/IEC 19794-5	ISO/IEC 19794-5:2005, *Information technology — Biometric data interchange formats — Part 5: Face image data* (Technologies de l'information — Formats d'échange de données biométriques — Partie 5 : Données d'image du visage).
ISO/IEC 19794-6	ISO/IEC 19794-6:2005, *Information technology — Biometric data interchange formats — Part 6: Iris image data* (Technologies de l'information — Formats d'échange de données biométriques — Partie 6 : Données d'image de l'iris).
ISO/IEC 39794-4	ISO/IEC 39794-4, *Information technology — Extensible biometric data interchange formats — Part 4: Finger image data* (Technologies de l'information — Formats d'échange de données biométriques extensibles — Partie 4 : Données d'image du doigt).
ISO/IEC 39794-5	ISO/IEC 39794-5, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data* (Technologies de l'information — Formats d'échange de données biométriques extensibles — Partie 5 : Données d'image du visage).
ISO/IEC 39794-6	ISO/IEC 39794-6, *Information technology — Extensible biometric data interchange formats — Part 6: Iris image data* (Technologies de l'information — Formats d'échange de données biométriques extensibles — Partie 6 : Données d'image de l'iris).

— — — — — — — —

Appendice A à la Partie 9 (INFORMATIF)

PROCESSUS DE LECTURE DES DVLM-e

A.1 PRÉCAUTIONS À PRENDRE DANS LA CONFECTION DES DVLM-e

Les États émetteurs ou les organisations émettrices doivent veiller à ce que le CI et son antenne ne soient pas endommagés par inadvertance au cours des processus de confection et de personnalisation. Par exemple, une chaleur excessive lors du laminage ou une perforation de l'image dans la zone du CI ou de son antenne risquerait d'endommager l'ensemble CI. De même, lorsque le CI est inséré dans la couverture avant, l'estampage métallique sur l'extérieur de la couverture, après l'assemblage, risque aussi d'endommager le CI ou les connexions à son antenne.

A.2 LECTURE DES DONNÉES ROC ET DES DONNÉES DU CI

Il est fortement recommandé qu'un État récepteur ou une organisation réceptrice lise tant les données ROC que les données stockées sur le CI. Lorsqu'un État émetteur ou une organisation émettrice verrouille le CI contre l'interception illicite, la lecture des données ROC est nécessaire pour accéder aux données du CI. Il est souhaitable qu'un lecteur unique soit utilisé pour les deux opérations, le lecteur étant équipé pour les deux types de lecture. Si le PLM est ouvert à la page de renseignements et posé sur un lecteur de page entière, certains PLM auront le CI situé derrière le recto de la page de renseignements, tandis que d'autres auront le CI dans la partie du livret qui ne se trouve pas dans le lecteur de page entière.

A.3 CONSTRUCTION DU LECTEUR

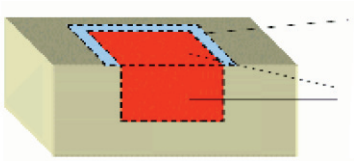
Les États ou organisations doivent donc installer un équipement de lecture capable de traiter les PLM des deux géométries et de préférence capable de lire les caractères ROC et le CI. La Figure A-1 montre des configurations possibles du lecteur, chacune d'elles permettant de lire les caractères ROC et le CI. Le livret est à demi ouvert et deux antennes assurent la lecture du CI, qu'il soit ou non en face de la ZLA. La figure montre aussi une configuration moins satisfaisante dans laquelle le DVLM-e est placé sur un lecteur de caractères ROC ou glissé dans ce lecteur pour la lecture de la ZLA, puis placé sur un lecteur pour la lecture des données du CI. Cet arrangement est moins commode pour les préposés au contrôle frontalier.

Géométries de lecture

Les fabricants de lecteurs doivent donc envisager la conception de solutions de lecture par machine qui tiennent compte des diverses possibilités d'orientation et qui soient (idéalement) capables de lire simultanément la ZLA et le CI sans contact.

Processus de lecture simultané

Lecteur de page entière avec 2 antennes orientées perpendiculairement, ou une seule grande antenne couvrant la superficie d'un livret ouvert



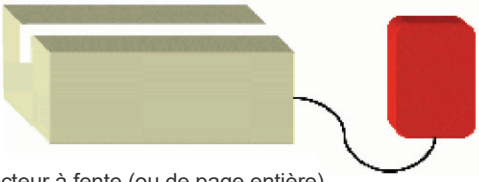
Lecture ROC

Zone de lecture du CI (2 antennes ou 1 grande antenne)

ou

Processus de lecture en 2 étapes

Lecteur à fente ou lecteur de page entière pour caractères ROC, relié à un lecteur RF séparé



Lecteur à fente (ou de page entière) pour lecture des caractères ROC

Lecture du CI

Étape 1 : Glisser le DVLM dans le lecteur ROC ou le poser sur le lecteur.
Étape 2 : Si le DVLM contient une puce, le poser sur le lecteur de CI.

Figure A-1. Processus de lecture

A.4 PROCESSUS DE LECTURE

La Figure A-2 montre les processus qui interviennent dans la lecture d'un DVLM-e avant et en incluant la vérification biométrique du détenteur.

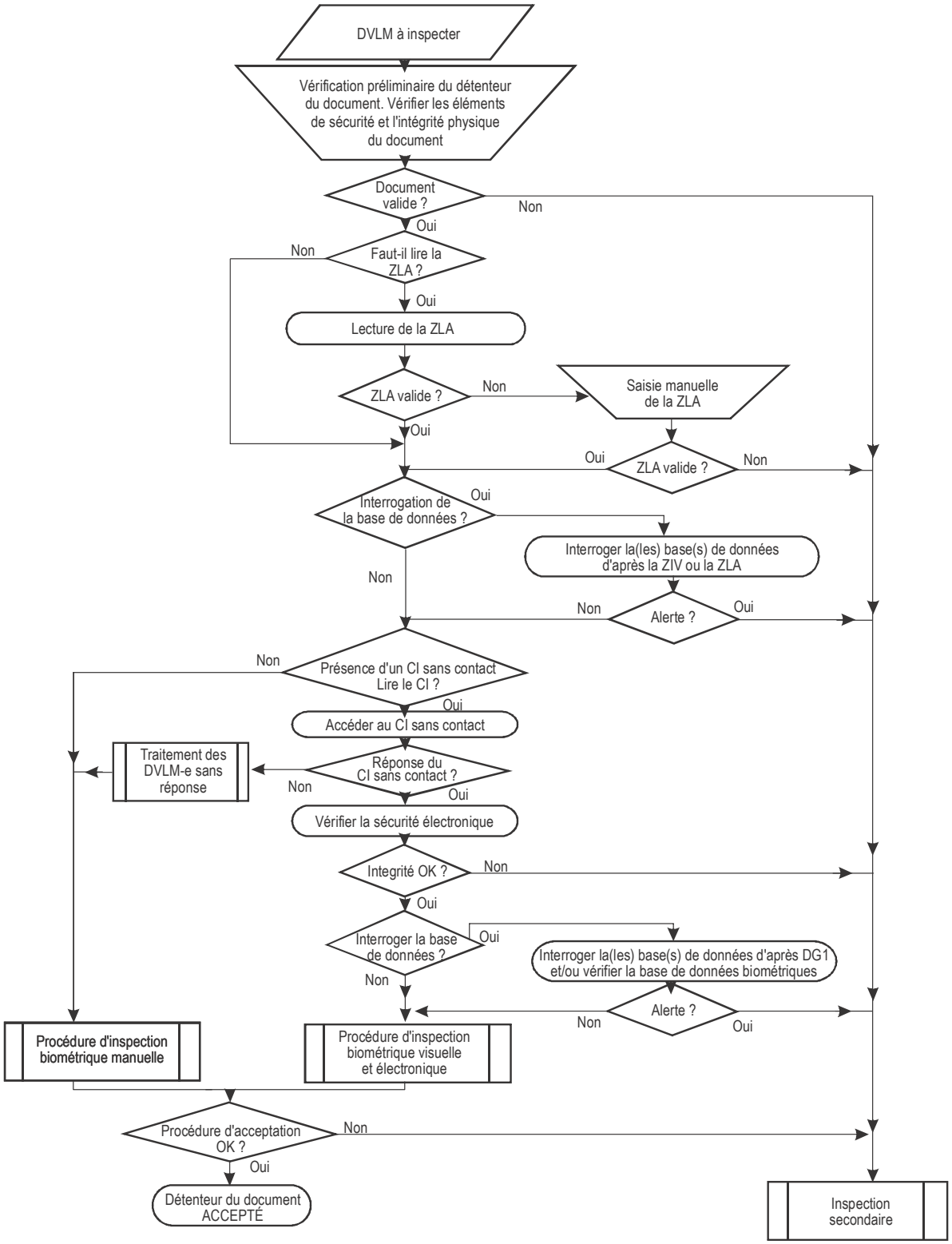


Figure A-2. Processus de lecture du DVLM-e

— FIN —

ISBN 978-92-9275-354-2