OACI

# Doc 9303

# Documents de voyage lisibles à la machine

Huitième édition (Révision), 2021

## Partie 1 : Introduction

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 (Révision), 2021

## Partie 1 : Introduction

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 www.icao.int/security/mrtd permet de télécharger les documents et d'obtenir des renseignements supplémentaires.

*Huitième édition (Révision), 2021*

**Doc 9303, *Documents de voyage lisibles à la machine***
**Partie 1 — *Introduction***

Commande nº : 9303P1
ISBN 978-92-9265-526-6

## 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 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| RECTIFICATIFS | | |
|---|---|---|
| N° | Date | Inscrit par |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# TABLE DES MATIÈRES

# 1. AVANT-PROPOS

Les travaux de l'OACI sur les documents de voyage lisibles à la machine ont commencé en 1968 avec l'institution, par le Comité du transport aérien du Conseil, d'un Groupe d'experts sur la carte-passeport. Ce groupe était chargé d'élaborer des recommandations relatives à un passeport normalisé, sous forme de livret ou de carte, qui soit lisible par machine, l'objectif étant d'accélérer le congé des passagers aux postes de contrôle. Ses travaux ont abouti à une série de recommandations, notamment l'adoption de la reconnaissance optique de caractères (ROC) comme technique de lecture automatique privilégiée, cette technique étant parvenue à maturité, économique et fiable. En 1980, les spécifications et les éléments indicatifs élaborés par le groupe d'experts ont été publiés dans la première édition du Doc 9303, intitulé *Passeport lisible à la machine*, sur la base duquel l'Australie, le Canada et les États-Unis ont délivré les premiers passeports lisibles par machine.

En 1984, l'OACI a institué le maintenant dénommé Groupe consultatif technique sur les documents de voyage lisibles à la machine (TAG/MRTD). Constitué de fonctionnaires d'administrations nationales spécialisés dans l'émission et l'inspection aux frontières de passeports et d'autres documents de voyage, il a pour mandat d'actualiser et de développer les spécifications élaborées par le groupe d'experts. Le mandat de ce groupe a été élargi par la suite, en premier lieu pour y inclure l'élaboration de spécifications relatives à un visa lisible par machine et ultérieurement celle de spécifications pour des cartes lisibles par machine utilisables comme documents de voyage officiels.

En 1998, le Groupe de travail des nouvelles technologies du TAG/MRTD a commencé les travaux pour établir le système d'identification biométrique le plus efficace et les méthodes connexes de stockage de données à utiliser dans les applications de documents de voyage lisibles à la machine (DVLM), en s'attachant en particulier aux considérations relatives à l'émission des documents et à l'immigration. Le gros des travaux était accompli lorsque les événements du 11 septembre 2001 ont poussé les États à attacher une plus grande importance à la sécurisation des documents de voyage et à l'identification de leur titulaire. Les travaux ont été rapidement achevés et entérinés par le Groupe TAG/MRTD et le Comité du transport aérien.

Les rapports techniques qui ont suivi, portant sur l'utilisation de la technologie biométrique et des puces sans contact, la structure de données logique (SDL) et l'infrastructure à clés publiques (ICP), ont été incorporés dans le Volume 2 de la sixième édition du Doc 9303, Partie 1, *Passeports lisibles à la machine*, en 2006, et dans le Volume 2 de la troisième édition du Doc 9303, Partie 3, *Documents de voyage officiels lisibles à la machine*, en 2008.

# 2. PORTÉE

Le Doc 9303 se divise en plusieurs parties qui contiennent les spécifications générales, applicables à tous les DVLM, et les spécifications qui s'appliquent exclusivement à chaque format de DVLM. Voir le § 5.1, Structure du Doc 9303, pour un aperçu des différentes parties du document.

Ces spécifications ne visent pas à constituer une norme pour les documents d'identité nationaux. Toutefois, un État dont les documents d'identité sont reconnus par d'autres États comme documents de voyage valables devra concevoir ses documents d'identité de manière qu'ils soient conformes aux spécifications des Doc 9303-3 et Doc 9303-4, Doc 9303-5 ou Doc 9303-6.

Même si les spécifications du Doc 9303-4 visent particulièrement les passeports, elles s'appliquent également à d'autres documents d'identité de format TD3, par exemple le laissez-passer, la pièce d'identité des gens de mer et les documents de voyage de réfugiés.

Le présent document, la Partie 1 du Doc 9303, est une introduction à ces spécifications. Il décrit les treize parties du Doc 9303, donne des renseignements généraux sur l'OACI et définit la terminologie et les abréviations utilisées dans toutes les parties du Doc 9303.

# 3. CONSIDÉRATIONS GÉNÉRALES

## 3.1 Rôle directeur de l'OACI

En prenant l'initiative d'élaborer des spécifications normalisées pour les passeports et d'autres documents de voyage, l'OACI a suivi la tradition établie par les Conférences sur les passeports des années 1920 organisées par la Société des Nations (SDN) et par les travaux de l'Organisation des Nations Unies, qui a succédé à la SDN. Le mandat de l'OACI de continuer à assumer le rôle de chef de file dans ce domaine s'ancre dans la Convention relative à l'aviation civile internationale (« Convention de Chicago »), qui couvre l'éventail complet des conditions requises pour que les activités d'aviation civile soient efficaces et ordonnées, y compris certaines dispositions relatives au congé des personnes aux frontières, à savoir :

a) l'obligation incombant aux personnes qui voyagent par voie aérienne et aux équipages des aéronefs de se conformer aux règlements relatifs à l'immigration, à la douane et aux passeports (article 13) ;

b) l'obligation incombant aux États de faciliter les formalités de congé aux frontières et d'éviter de retarder le congé sans nécessité (article 22) ;

c) l'obligation incombant aux États de collaborer en la matière (article 23) ;

d) l'obligation incombant aux États d'élaborer et d'adopter des procédures normalisées internationalement pour les formalités de douane et d'immigration [article 37, alinéa j)].

Au titre de ce mandat, l'OACI élabore et tient à jour des normes internationales dans l'Annexe 9 — *Facilitation* à la Convention de Chicago, que les États membres sont appelés à mettre en œuvre. Un principe fondamental dans l'élaboration de ces normes est que les autorités publiques, pour faciliter les formalités d'inspection pour la vaste majorité des voyageurs aériens, doivent avoir un niveau de confiance satisfaisant dans la fiabilité des documents de voyage et l'efficacité des procédures d'inspection. La production de spécifications normalisées pour les documents de voyage et les données qu'ils contiennent visent à établir cette confiance.

En 2004, l'Assemblée de l'OACI a déclaré que les travaux de coopération portant sur les spécifications destinées à renforcer la sécurité et l'intégrité des documents de voyage devraient être entrepris par l'Organisation en toute priorité. Outre l'Organisation internationale de normalisation (ISO), le Groupe TAG/MRTD consulte notamment l'Association du transport aérien international (IATA), le Conseil international des aéroports (ACI) et l'Organisation internationale de police criminelle (INTERPOL).

En 2005, les États membres de l'OACI, alors au nombre de 188, ont approuvé une nouvelle norme spécifiant que tous les États devaient commencer, au plus tard en 2010, à émettre des passeports lisibles à la machine conformément aux dispositions du Doc 9303. Tous les documents non lisibles à la machine devaient avoir expiré en 2015 au plus tard. Cette norme a été publiée dans la 13e édition (2011) de l'Annexe 9 — *Facilitation*.

## 3.2 Coûts et avantages relatifs des DVLM

Il ressort de l'expérience acquise dans l'émission de passeports lisibles par machine, en conformité avec les spécifications établies dans le Doc 9303, que le coût de production des DVLM n'est pas nécessairement plus élevé que celui des

documents conventionnels, quoique ce coût augmentera lorsque les méthodes d'identification biométrique et les documents de voyage électroniques seront appliqués. Avec l'augmentation des volumes de trafic et du nombre d'États qui s'attachent à rationaliser leurs formalités de congé en utilisant des bases de données informatisées et en recourant aux échanges de données électroniques, les DVLM sont appelés à jouer un rôle central dans les systèmes de conformité modernes améliorés. Les équipements de lecture des documents et l'accès aux bases de données représentent sans doute un investissement substantiel, mais la meilleure sécurisation, l'accélération du congé et la plus grande précision des vérifications qu'assurent ces systèmes devraient permettre de récupérer cet investissement. L'emploi de DVLM dans des systèmes de congé automatisés pourrait aussi permettre aux États d'éliminer les documents papier tels que les manifestes de passagers et les cartes d'embarquement/débarquement, ainsi que les frais d'administration associés aux procédures manuelles.

### 3.3 Mode opératoire

Le DVLM de base, avec la ROC, est conçu pour permettre à la fois une lecture mécanique et une lecture visuelle.

Les États membres de l'OACI ont reconnu que la normalisation est une nécessité et que les bénéfices de l'adoption des modèles normalisés que prévoit le Doc 9303 pour les passeports et autres documents de voyage vont au-delà des avantages évidents qu'elle présente pour les États qui disposent des lecteurs automatiques et des bases de données utilisés dans les systèmes de congé automatisés. En fait, les caractéristiques physiques et les éléments de sécurité des données de ces documents offrent eux-mêmes de fortes sauvegardes contre l'altération, la falsification et la contrefaçon. De plus, l'adoption d'une présentation normalisée pour la zone visuelle d'un DVLM facilite l'inspection par les préposés des compagnies aériennes et des administrations, de sorte que le congé du trafic à faible risque est accéléré, que les cas qui posent problème sont plus facilement décelés et que l'application de la loi est améliorée. L'introduction facultative d'éléments d'identification biométriques avec stockage de données dans un circuit intégré sans contact offrira une sécurité accrue et une meilleure protection contre la fraude, tout en facilitant pour le détenteur légitime du document l'obtention de visas pour voyager et le congé par les systèmes d'inspection aux frontières.

*Note.— Il y aura certainement des cas de problème d'interface entre un DVLM électronique (DVLM-e) et un appareil de lecture à un point frontalier. Il y a plusieurs raisons pour lesquelles cela pourrait se produire, une défaillance du DVLM-e n'étant que l'une d'entre elles. L'OACI souligne qu'un DVLM-e présentant un problème de lecture est néanmoins un document valide. Le fait qu'un DVLM-e ne peut pas être lu pourrait cependant être le résultat d'une attaque frauduleuse et l'État récepteur devrait établir ses propres procédures pour traiter cette possibilité ; ces procédures devraient comporter une inspection plus rigoureuse du document et de son détenteur, mais aussi tenir compte de la possibilité que la défaillance n'implique aucune intention frauduleuse.*

### 3.4 Entérinement par l'ISO

Les sections de spécifications techniques du Doc 9303 ont été entérinées par l'Organisation internationale de normalisation (ISO) en tant que norme ISO 7501. Cet entérinement est possible grâce au mécanisme de liaison dans le cadre duquel les fabricants de documents de voyage, d'appareils de lecture et d'autres technologies fournissent des avis sur les questions techniques et d'ingénierie au Groupe TAG/TRIP sous les auspices de l'ISO. Cette relation de travail a permis aux spécifications de l'OACI d'obtenir, et lui permettra sans doute de continuer à obtenir, le statut de normes mondiales au moyen d'une procédure simplifiée au sein de l'ISO.

Le mécanisme de liaison avec l'ISO a été appliqué avec succès non seulement à l'entérinement de nouvelles spécifications relatives aux documents de voyage comme normes de l'ISO, mais aussi à l'approbation des amendements apportés aux spécifications. Les futures révisions du Doc 9303 seront donc traitées de la même manière que précédemment en ce qui concerne l'entérinement par l'ISO.

# 4. DÉFINITIONS ET RÉFÉRENCES

## 4.1 Sigles et acronymes

| Sigle ou acronyme français | Sigle ou acronyme anglais | Signification |
|---|---|---|
| | *3DES* | triple DES |
| | *AA* | authentification active *(Active Authentication)* |
| AA | *AO* | agent d'autorisation *(Authorizing Officer)* |
| AC | *CA* | autorité de certification *(Certification Authority)* |
| ACSN | *CSCA* | autorité de certification signataire nationale *(Country Signing Certification Authority)* |
| | *AES* | norme de chiffrement avancé *(Advanced Encryption Standard)* |
| | *AID* | identifiant d'application *(Application Identifier)* |
| | *APDU* | unité de données de protocole d'application *(Application Protocol Data Unit)* |
| AVV | *VVA* | autorité de validation des visas *(Visa Validation Authority)* |
| | *BAC* | contrôle d'accès de base *(Basic Access Control)* |
| | *BER* | règles de codage de base *(Basic Encoding Rules)* |
| | *BLOB* | grand objet binaire *(Binary Large Object)* |
| | *BSC* | certificat du signataire de code à barres *(Bar Code Signer Certificate)* |
| | *CA* | authentification de puce *(Chip Authentication)* |
| | *CAM* | mappage d'authentification de puce *(Chip Authentication Mapping)* |
| | *CAN* | code d'accès à la carte *(Card Access Number)* |
| | *CAR* | référence de l'autorité de certification *(Certification Authority Reference)* |
| | *CBC* | chiffrement par chaîne de blocs *(Cipher Block Chaining)* |
| | *CBEFF* | cadre de formats d'échange biométriques communs *(Common Biometric Exchange Format Framework)* |
| | *CCD* | dispositif à couplage de charge *(Charge-Coupled Device)* |
| CCI | *ICC* | carte à circuit intégré *(Integrated Circuit Card)* |
| | $C_{DS}$ | certificat de signataire de document *(Document Signer Certificate)* |
| | *CIC* | circuit intégré sans contact *(Contactless Integrated Circuit)* |
| CFA | *ABC* | contrôle frontalier automatisé *(Automated Border Control)* |
| CI | *IC* | circuit intégré *(Integrated Circuit)* |
| | *CID* | identifiant de carte *(Card Identifier)* |
| | *CMAC* | code chiffré d'authentification de message *(Cipher-Based Message Authentication Code)* |

| Sigle ou acronyme français | Sigle ou acronyme anglais | Signification |
|---|---|---|
| | *CMOS* | semi-conducteur complémentaire à l'oxyde de métal *(Complementary Metal–Oxide–Semiconductor)* |
| | *CRL* | liste de certificats révoqués *(Certificate Revocation List)* |
| | *CSD* | distance appareil-sujet : distance entre les yeux d'une personne et le centre optique de l'objectif de l'appareil photo *(Camera To Subject Distance)* |
| | *CVCA* | autorité de certification de vérification nationale *(Country Verifying Certification Authority)* |
| | *DER* | règles de codage distinctives *(Distinguished Encoding Rules)* |
| | *DES* | norme de chiffrement de données *(Data Encryption Standard)* |
| | *DF* | fichier dédié *(Dedicated File)* |
| | *DG* | groupe de données *(Data Group)* |
| | *DH* | Diffie-Hellmann |
| | *DN* | nom distinctif *(Distinguished Name)* |
| | *DO* | objet de données *(Data Object)* |
| | *DOVID* | image diffractive optiquement variable *(Diffractive Optically Variable Image Device) dispositif diffractif présentant des effets optiquement variables (par exemple : effets holographiques)* |
| | *DSA* | algorithme de signature numérique *(Digital Signature Algorithm)* |
| | *DTA* | autorisation de voyage numérique *(Digital Travel Authorization)* |
| | *DTBS* | données à signer *(Data To Be Signed)* |
| | *DSC* | certificat de signataire de document *(Document Signer Certificate)* |
| | *DV* | vérificateur de documents *(Document Verifier)* |
| DVLM | *MRTD* | document de voyage lisible à la machine *(Machine Readable Travel Document)* |
| DVLM-e | *eMRTD* | DVLM électronique *(Electronic MRTD)* |
| DVOLM | *MROTD* | document de voyage officiel lisible à la machine sous forme de carte *(Machine Readable Official Travel Document in the form of a card)* |
| DVOLM-e | *eMROTD* | DVOLM électronique *(Electronic MROTD)* |
| | *EAL* | niveau d'assurance d'évaluation *(Evaluation Assurance Level)* |
| | *ECDH* | Diffie-Hellmann à courbe elliptique *(Elliptic Curve Diffie Hellmann)* |
| | *ECDSA* | algorithme de signature numérique à courbe elliptique *(Elliptic Curve Digital Signature Algorithm)* |
| | *ECKA* | concordance de clés à courbe elliptique *(Elliptic Curve Key Agreement)* |
| | *EEPROM* | mémoire morte programmable effaçable électriquement *(Electrically Erasable Programmable Read Only Memory)* |
| | *EF* | fichier élémentaire *(Elementary File)* |

| Sigle ou acronyme français | Sigle ou acronyme anglais | Signification |
|---|---|---|
| | *EM* | écart entre les yeux et la bouche *(Eye to Mouth distance)* |
| | *eRP* | titre de séjour électronique *(Electronic Residence Permit)* |
| | *ETS* | système électronique de voyage *(Electronic Travel System)* |
| | *EVZ* | zone de visibilité de l'œil *(Eye Visibility Zone)*<br>zone rectangulaire à une distance V de toute partie visible du globe oculaire, qui équivaut au moins à 5 % de l'IED |
| | *FAR* | taux de fausses acceptations *(False Acceptance Rate)* |
| | *FIPS* | norme fédérale de traitement de l'information *(Federal Information Processing Standard)* |
| | *FRR* | taux de faux rejets *(False Rejection Rate)* |
| FTM | *MTF* | fonction de transfert de modulation *(Modulation Transfer Function)* |
| FTM20 | *MTF20* | fréquence spatiale la plus élevée (FTM supérieure ou égale à 20 %) |
| | *GM* | mappage générique *(Generic Mapping)* |
| | *HD* | angle d'écart horizontal *(Horizontal Deviation Angle)*<br>écart maximum horizontal autorisé par rapport à la ligne imaginaire entre le nez d'une personne et l'objectif de l'appareil photo |
| ICP | *PKI* | infrastructure à clés publiques *(Public Key Infrastructure)* |
| | *IED* | écart pupillaire *(Inter Eye Distance)* |
| | *IFD* | dispositif d'interface *(Interface Device)* |
| | *IM* | mappage intégré *(Integrated Mapping)* |
| | *IR* | lumière infrarouge *(Infrared Light)* |
| | *IS* | système d'inspection *(Inspection System)* |
| | *IV* | vecteur initial *(Initial Vector)* |
| | *LDAP* | protocole rapide d'accès à l'annuaire *(Lightweight Directory Access Protocol)* |
| | *MAC* | code d'authentification de message *(Message Authentication Code)* |
| | *MF* | fichier principal *(Master File)* |
| | *NAD* | adresse nodale *(Node Address)* |
| | *NIST* | National Institute of Standards and Technology |
| | *NTWG* | Groupe de travail des technologies nouvelles *(New Technologies Working Group)* |
| OACI | *ICAO* | Organisation de l'aviation civile internationale |
| | *OID* | identificateur d'objet *(Object Identifier)* |
| | *OVD* | dispositif optiquement variable *(Optically Variable Device)* |
| | *OVF* | élément optiquement variable *(Optically Variable Feature)* |
| | *OVI* | encre à effet optique variable *(Optically Variable Ink)* |

| Sigle ou acronyme français | Sigle ou acronyme anglais | Signification |
|---|---|---|
| | *PACE* | établissement de connexion avec authentification par mot de passe *(Password Authenticated Connection Establishment)* |
| | *PCD* | dispositif de couplage de proximité *(Proximity Coupling Device)* |
| | *PICC* | carte à circuit intégré de proximité *(Proximity Integrated Circuit Card)* |
| | *PIX* | extension d'identifiant propriétaire *(Proprietary Identifier Extension)* |
| PLM | *MRP* | passeport lisible à la machine *(Machine Readable Passport)* |
| PLM-e | *eMRP* | PLM électronique *(Electronic MRP)* |
| | *RA* | autorité d'enregistrement *(Registration Authority)* |
| RCP | *PKD* | répertoire de clés publiques *(Public Key Directory)* |
| | *RFID* | identification par radiofréquence *(Radio Frequency Identification)* |
| | *RID* | identificateur enregistré *(Registered Identifier)* |
| ROC | *OCR* | reconnaissance optique de caractères *(Optical Character Recognition)* |
| ROC-B | *OCR-B* | caractères pour la reconnaissance optique définis dans la norme ISO 1073-2 *[Optical Character Recognition font (OCR-B) defined in ISO 1073-2]* |
| | *ROI* | région d'intérêt *(Region Of Interest)* |
| | *ROM* | mémoire morte *(Read Only Memory)* |
| | *RSA* | Rivest, Shamir et Adleman |
| RVB | *RGB* | rouge, vert, bleu *(Red-Green-Blue)* |
| SD | *DS* | signataire de document *(Document Signer)* |
| SDL | *LDS* | structure de données logique *(Logical Data Structure)* |
| | *SFR* | réponse en fréquence spatiale *(Spatial Frequency Response)* |
| | *SHA* | algorithme de hachage sécurisé *(Secure Hash Algorithm)* |
| SLF | *AFS* | spécialiste de la lutte contre la fraude *(Anti-Fraud Specialist)* |
| | *SM* | messagerie sécurisée *(Secure Messaging)* |
| | *SNR* | radio signal/bruit *(Signal to Noise Radio)* |
| | *SPOC* | point unique de contact *(Single Point Of Contact)* |
| | $SO_D$ | objet de sécurité du document *(Document Security Object)* |
| sRVB | *sRGB* | espace colorimétrique standard RVB pour une utilisation sur écrans, imprimantes et Internet basé sur la recommandation UIT-R BT.709 |
| | *SSC* | compteur de séquence d'envoi *(Send Sequence Counter)* |
| | *TA* | authentification du terminal *(Terminal Authentification)* |
| | *TAG/MRTD* | Groupe consultatif technique sur les documents de voyage lisibles à la machine *(Technical Advisory Group on Machine Readable Travel Documents)* |

| Sigle ou acronyme français | Sigle ou acronyme anglais | Signification |
|---|---|---|
| | *TAG/TRIP* | Groupe consultatif technique sur le Programme d'identification des voyageurs *(Technical Advisory Group on the Traveller Identification Programme)* |
| | *TD1* | document de voyage officiel lisible à la machine de format 1 *(Size 1 Machine Readable Official Travel Document)* |
| | *TD2* | document de voyage officiel lisible à la machine de format 2 *(Size 2 Machine Readable Official Travel Document)* |
| | *TD3* | document de voyage lisible à la machine de format 3 *(Size 3 Machine Readable Travel Document)* |
| | *TLV* | étiquette, longueur, valeur *(Tag, Length, Value)* |
| | *TR* | rapport technique *(Technical Report)* |
| | *UID* | identificateur unique *(Unique Identifier)* |
| | *UV* | lumière ultraviolette *(UltraViolet light)* |
| | *VDS* | cachet numérique visible *(Visible Digital Seal)* |
| | *VIS* | système d'information sur les visas (Union européenne) *(Visa Information System of the European Union)* |
| VLM-A | *MRV-A* | visa lisible à la machine de grand format (type A) *[Full size (Format A) Machine Readable Visa]* |
| VLM-B | *MRV-B* | visa lisible à la machine de petit format (type B) *[Small size (Format B) Machine Readable Visa]* |
| | *VS* | signataire de visa *(Visa Signer)* |
| | *WSQ* | technique de compression Wavelet Scalar Quantization *(Wavelet Scalar Quantization)* |
| ZIV | *VIZ* | zone d'inspection visuelle *(Visual Inspection Zone)* |
| ZLA | *MRZ* | zone de lecture automatique *(Machine Readable Zone)* |
| ZLE | *ERZ* | zone de lecture effective *(Effective Reading Zone)* |

### 4.2 Termes et définitions

| Terme | Définition |
|---|---|
| Accès aléatoire | Mode de stockage des données permettant l'extraction de certains éléments d'information sans nécessité d'effectuer une recherche séquentielle dans toutes les données stockées. |
| Adobe RVB | Espace colorimétrique RVB pensé pour englober la plupart des couleurs reproductibles par les imprimantes CMJN à partir des couleurs primaires RVB sur un appareil (par exemple : écran d'ordinateur). |
| Algorithme | Processus mathématique spécifié pour le calcul ; ensemble de règles qui, si elles sont suivies, donneront un résultat prescrit. |

| Terme | Définition |
|---|---|
| Algorithme asymétrique | Ce type d'opération cryptographique utilise une clé pour le chiffrement du texte en clair et une autre clé pour le déchiffrement du texte chiffré correspondant. Ces deux clés, liées l'une à l'autre, constituent une paire de clés. |
| Algorithme de chiffrement par blocs | Voir « chiffrement par blocs ». |
| Algorithme de contrôle | Composants logiciels qui permettent la mise en œuvre spécifique d'opérations de vérification courantes (par exemple : recherche de motifs). |
| Algorithme de hachage sécurisé (SHA) | Fonction de hachage mise au point par le NIST et publiée en 1993 comme norme fédérale de traitement de l'information FIPS-180. |
| Algorithme de signature numérique (DSA) | Algorithme asymétrique publié par le NIST dans la norme FIPS 186. Cet algorithme offre seulement une fonction de signature numérique. |
| Algorithme symétrique | Type d'opération cryptographique utilisant la même clé ou le même ensemble de clés pour le chiffrement de texte en clair et le déchiffrement du texte chiffré correspondant. |
| Altération frauduleuse | Procédé visant la modification d'un document authentique pour en permettre l'utilisation pour des voyages par une personne non autorisée ou vers une destination non autorisée. Les données personnelles du titulaire légitime, en particulier le portrait, constituent la cible principale d'une telle altération. |
| Amorçage *(bootstrapping)* | Méthode employée pour tester la fiabilité d'un ensemble de données. |
| Ancre de confiance | Dans les systèmes cryptographiques à structure hiérarchique, entité faisant autorité dont la fiabilité est admise et non calculée. |
| Appariement | Processus de comparaison d'un échantillon biométrique avec un gabarit stocké précédemment et d'attribution d'un score au niveau de similarité. Une décision d'acceptation ou de rejet est alors basée sur le score dépassant ou non le seuil donné. |
| Appariement biométrique | Processus d'utilisation d'un algorithme qui compare des gabarits tirés de la référence biométrique et de l'entrée biométrique capturée en direct, le résultat étant une détermination de correspondance ou de non-correspondance. |
| Asymétrique | Se dit lorsque des clés différentes sont nécessaires à chaque extrémité d'une liaison de communication. |
| Attaque en force | Tentative de décryptage en utilisant toutes les clés possibles et en vérifiant si le texte en clair obtenu a du sens. |
| Attaque par usurpation | Présentation au sous-système de capture de données biométriques d'un objet artificiel ou d'une caractéristique d'une personne dans une tentative d'entraver la politique de vérification du système biométrique. |
| Authenticité | Propriété assurant que la structure de données logique et ses éléments ont été créés par l'État émetteur ou l'organisation émettrice. |
| Authentification | Processus de validation de l'identité revendiquée d'un participant à une transaction électronique. |
| Autorisation | Processus de sécurité pour décider si un service peut être fourni ou non. |

| Terme | Définition |
|---|---|
| Autorisation de voyage | Document papier ou numérique délivré par l'État récepteur autorisant une personne à voyager. |
| Autorisation de voyage numérique | Visa électronique délivré et géré par l'État émetteur. |
| Autorité de certification (AC) | Organisme de confiance qui émet des certificats numériques pour l'ICP. |
| Autorité de délivrance | Entité habilitée à délivrer un DVLM à son titulaire légitime. |
| Autorité d'enregistrement | Personne ou organisme en charge de l'identification et de l'authentification d'un demandeur de certificat numérique. Cette autorité n'émet pas et ne signe pas de certificats. |
| Autorité de validation des visas (AVV) | Autorité qui valide un cachet numérique visible sur un visa selon une politique de validation. |
| Base de données d'authentification | Base de données où les algorithmes d'authentification pour les opérations courantes de vérification sont stockés pour chaque modèle de document. |
| Biométrie multiple | Emploi de plus d'une technologie biométrique. |
| Bit | Chiffre binaire. La plus petite unité d'information possible dans un code numérique. |
| Bloc | Chaîne ou groupe de bits sur lequel opère un algorithme de chiffrement par blocs. |
| Bloc de données émetteur | Série de groupes de données inscrits dans la technologie optionnelle d'expansion de capacité par l'État émetteur ou l'organisation émettrice. |
| Bloc de données récepteur | Série de groupes de données inscrits dans la technologie optionnelle d'expansion de capacité par un État récepteur ou une organisation réceptrice autorisée. |
| Borne photographique | Système semi-automatisé permettant de prendre des photos d'identité numériquement à un comptoir. Il s'agit généralement d'un espace ouvert, équipé d'un appareil photo et d'un système d'éclairage. Un panneau amovible est placé derrière la personne au moment de la photographie. |
| Cabine photographique | Système automatisé permettant de prendre des photos d'identité numériquement dans un espace public ou professionnel. La personne s'installe dans un environnement lumineux hautement contrôlé équipé d'un appareil photo, d'un système d'éclairage et de matériel périphérique (une imprimante par exemple). L'entrée dans la cabine se fait par un ou deux côtés, protégés de la lumière ambiante par des rideaux réfléchissants. |
| Cachet numérique | Au long, cachet numérique visible. |
| Cachet numérique visible (VDS) | Structure de données contenant les caractéristiques d'un document, signée selon un procédé cryptographique, codée sous la forme d'un code à barres bidimensionnel et imprimée sur le document. |
| Cadre de formats d'échange biométriques communs (CBEFF) | Format commun de fichier qui facilite l'échange et l'interopérabilité des données biométriques. |
| Capture | Méthode de prélèvement d'un échantillon biométrique sur l'utilisateur. |

| Terme | Définition |
|---|---|
| Capture en direct | Processus de capture d'un échantillon biométrique par interaction entre le détenteur d'un DVLM et un système biométrique. |
| Caractéristique | Élément d'un document qui permet de prouver l'authenticité de celui-ci (par exemple une photographie absorbant les rayons infrarouges). |
| Caractéristique (numérique) d'un document | Propriété d'un document, sous format numérique ou non, qui peut servir à vérifier le contenu de celui-ci, comme des informations textuelles (le nom du détenteur par exemple), la date de délivrance ou une image imprimée du détenteur du document. |
| Carte | Support conforme aux spécifications des normes ISO/CEI 7810, ISO/CEI 7811, ISO 7812, utilisé pour véhiculer l'information. |
| Carte à circuit intégré (carte CI, CCI) | Carte dans laquelle sont insérés un ou plusieurs CI. |
| Carte d'identité (carte ID) | Carte utilisée comme document d'identité. |
| Centre de l'œil | Point situé au milieu de l'axe reliant le coin intérieur au coin extérieur de l'œil.<br><br>*Note 1.— Le centre des deux yeux correspond aux points caractéristiques 12.1 et 12.2 dans la norme ISO/IEC 14496-2.*<br><br>*Note 2.— Les coins intérieur et extérieur de l'œil sont définis dans la norme ISO/IEC 14496-2. Ils correspondent aux points caractéristiques 3.12 et 3.8 pour l'œil droit, et 3.11 et 3.7 pour l'œil gauche.* |
| Centre du visage | Point situé au milieu de l'axe reliant le centre des deux yeux. |
| Certificat | Fichier électronique, délivré par une autorité de certification, attestant qu'une paire de clés cryptographiques appartient à la personne ou au composant matériel ou logiciel indiqué. En signant le certificat, l'autorité de certification confirme le lien entre l'identité d'une personne ou d'un composant et la paire de clés cryptographiques. Le certificat peut être révoqué s'il n'atteste plus la validité de ce lien et il a une période de validité limitée. |
| Certificat de clé publique | Information sur la clé publique d'une entité, signée par l'autorité de certification et rendue ainsi inoubliable. |
| Certificat de signataire de code à barres (BSC) | Certificat qui contient la clé publique du signataire de code à barres. Il est utilisé pour vérifier la validité des données signées à l'aide de la clé privée du signataire de code à barres. |
| Certificat de signataire de visa | Certificat qui contient les informations d'identification de l'entité qui a signé un cachet numérique visible sur un visa, ainsi que la clé publique correspondant à la clé privée à l'aide de laquelle la signature a été créée. |
| Certificat X.509 v3 | Document électronique reconnu à l'échelle internationale, utilisé pour prouver l'identité et la propriété d'une clé publique sur un réseau de communication. Contient le nom de l'émetteur, des informations identifiant l'utilisateur et la signature numérique de l'émetteur. |
| Champ | Espace spécifié pour un certain élément de données, à l'intérieur d'une zone. |
| Chiffrement | Codage de l'information par l'usage d'une clé afin qu'elle ne puisse pas être utilisée par une personne non autorisée. |

| Terme | Définition |
|---|---|
| Chiffrement | Écriture secrète basée sur une clé, ou ensemble de règles ou de symboles prédéterminés. |
| Chiffrement par blocs | Transformation de blocs de données en clair en blocs (chaînes ou groupes) de bits, au moyen d'algorithmes. |
| Circuit intégré (CI) | Composant électronique destiné à exécuter des fonctions de traitement et/ou de mémoire. |
| Circuit intégré sans contact | Dispositif semi-conducteur qui stocke les données des DVLM et qui communique avec un lecteur en utilisant l'énergie des radiofréquences selon la norme ISO/CEI 14443. |
| Clé maîtresse | Racine de la chaîne de calcul de clés. |
| Clé privée | Élément privé d'une paire de clés asymétriques intégrée (connue seulement de l'utilisateur), employée dans la cryptographie à clé publique pour déchiffrer ou signer des informations. |
| Clé publique | Composante publique d'une paire de clés asymétriques intégrées, utilisée pour chiffrer ou vérifier des informations. |
| Clés asymétriques | Paire de clés d'utilisateur distinctes mais intégrées, comprenant une clé publique et une clé privée. Chaque clé est à sens unique, ce qui signifie qu'une clé utilisée pour chiffrer des informations ne peut pas l'être pour déchiffrer ces mêmes informations. |
| Code à barres | Représentation graphique unidimensionnelle ou bidimensionnelle, lisible à la machine, des données relatives à l'objet correspondant. |
| Code d'authentification de message (MAC) | Un MAC est un condensé de message joint au message lui-même. Le MAC ne peut être calculé ou vérifié que si un secret est connu. Il est joint par l'expéditeur et vérifié par le destinataire qui est capable de détecter une falsification de message. |
| Code de pays | Code à deux ou à trois lettres défini dans ISO 3166-1, utilisé pour désigner une autorité de délivrance de documents ou la nationalité du titulaire du document. |
| Comparaison | Processus de comparaison d'un échantillon biométrique avec un ou plusieurs gabarits de référence stockés. Voir aussi « comparaison un-à-beaucoup » et « comparaison individuelle ». |
| Comparaison individuelle (1:1) | Processus biométrique (algorithme) consistant à comparer un échantillon photographique avec un échantillon enregistré correspondant à l'identité déclarée. Synonyme de « vérification ». |
| Comparaison un-à-beaucoup (1:N) | Processus biométrique (algorithme) consistant à rechercher un échantillon photographique a priori inconnu parmi un nombre N d'échantillons enregistrés dans une base de données. Synonyme d'« identification ». |
| Comparaison un-à-quelques-uns | Hybride de l'identification (1:N) et de la vérification (1:1). En général, il s'agit dans ce processus de comparer un échantillon biométrique soumis avec un petit nombre de gabarits biométriques de référence qui sont en mémoire. Généralement effectuée par rapport à une « liste de surveillance » de personnes pour qui des investigations d'identité détaillées sont justifiées ou qui sont connues comme délinquants, terroristes, etc. |
| Contrefaçon | Copie ou reproduction non autorisée d'un document de sécurité authentique, réalisée par un moyen quelconque. |
| Cryptographie | Méthode de transformation d'informations en forme chiffrée, inintelligible, à l'aide d'un algorithme et d'une clé. |

| Terme | Définition |
|---|---|
| Cryptographie à clé publique | Forme de chiffrement asymétrique où toutes les parties possèdent une paire de clés (clé privée et clé publique) à utiliser pour le chiffrement et la signature numérique de données. |
| Déchiffrement | Rétablissement d'un fichier chiffré dans son état d'origine au moyen d'une clé. |
| Désignation de champ | Mot ou groupe de mots imprimé, identifiant un champ. Dans des circonstances exceptionnelles, lorsque les mots en différentes langues officielles n'entrent pas dans le champ de données, ils peuvent être remplacés par des numéros. Ces numéros doivent être accompagnés d'un texte explicatif ailleurs dans le PLM. |
| Dessin en bichromie | Dessin constitué d'un motif enchevêtré de petites formes irrégulières, imprimé en deux ou plusieurs couleurs et nécessitant un repérage précis de l'impression pour préserver l'intégrité de l'image. |
| Dessin en lignes noires/ lignes blanches | Dessin fait de traits fins, souvent en forme de guillochis, parfois utilisé comme bordure d'un document de sécurité. Le motif migre d'une image négative à une image positive en progressant à travers la page. |
| Dessin en relief (tridimensionnel) (médaillon) | Dessin d'un fond de sécurité dans lequel est incorporée une image générée de façon à créer l'illusion qu'elle est imprimée en relief ou en creux sur la surface du support. |
| Détection d'une attaque par usurpation | Repérage automatisé d'une attaque par usurpation. |
| Détenteur | Personne en possession d'un DVLM-e, qui soumet un échantillon biométrique pour vérification ou identification en revendiquant une identité légitime ou fausse. Personne qui interagit avec un système biométrique pour s'enrôler ou faire vérifier sa propre identité. |
| Dispositif d'interface | Terminal, appareil ou dispositif de communication auquel la CCI est reliée pendant le fonctionnement. |
| Dispositif optiquement variable (OVD) | Élément de sécurité présentant une apparence différente des couleurs ou de l'image selon l'angle de vue ou les conditions de vérification. |
| Distance de lecture | Distance pratique maximale entre le CI sans contact avec son antenne et l'appareil de lecture. |
| Distorsion (grossissement) | Déformation d'une image lorsque le niveau de grossissement varie selon la distance avec l'appareil et la profondeur du visage. |
| Distorsion radiale | Déformation d'une image lorsque le niveau de grossissement varie selon la distance avec l'axe optique. |
| Document de voyage lisible à la machine (DVLM) | Document officiel conforme aux spécifications énoncées dans le Doc 9303, délivré par un État ou une organisation, que le titulaire utilise pour des voyages internationaux (par exemple, PLM, VLM, DVOLM) et qui contient des données visuelles (se prêtant à la lecture oculaire) obligatoires et, séparément, dans une forme lisible par machine, un condensé des données obligatoires. |
| Document de voyage officiel électronique lisible à la machine (DVOLM-e) | DVOLM de format TD1 ou TD2 conforme aux spécifications du Doc 9303-5 ou du Doc 9303-6, respectivement, qui contient en outre un circuit intégré sans contact et qui permet l'identification biométrique de son titulaire. |

| Terme | Définition |
|---|---|
| Document de voyage officiel lisible à la machine (DVOLM) | Document, généralement sous forme d'une carte de format TD1 ou TD2, qui est conforme aux spécifications du Doc 9303-5 et du Doc 9303-6, et qui peut être utilisé pour franchir des frontières internationales par voie d'accord entre les États concernés. |
| Document de voyage officiel lisible à la machine de format 1 (TD1) | Carte de dimensions nominales guidées par celles qui sont spécifiées pour la carte de type ID-1 (ISO/IEC 7810) (hormis l'épaisseur). |
| Document de voyage officiel lisible à la machine de format 2 (TD2) | Carte ou vignette conforme aux dimensions définies pour la carte de type ID-2 (ISO/IEC 7810) (hormis l'épaisseur). |
| Document d'identité | Document utilisé pour identifier son titulaire et son émetteur, qui peut porter des données requises comme entrées pour l'utilisation prévue de ce document. |
| Document source | Document utilisé comme preuve d'identité lors d'une demande de document de voyage. |
| Document vierge | Document de voyage qui ne contient pas de données personnelles. D'une manière générale, les documents vierges constituent la réserve de documents qui seront utilisés pour créer les documents de voyage personnalisés. |
| Données à signer (DTBS) | Message envoyé comme entrée à l'algorithme de génération de signatures d'un schéma de signature. |
| Données biométriques | Information extraite de l'élément biométrique et utilisée soit pour construire un modèle de référence (données de gabarit), soit pour effectuer une comparaison avec un gabarit de référence créé précédemment (données de comparaison). |
| Données personnelles | Renseignements biographiques sur le titulaire du document, apparaissant comme texte dans la zone d'inspection visuelle et la zone de lecture automatique du DVLM ou sur la puce, s'il y en a une. |
| Données sensibles | Ces données sont considérées comme étant plus sensibles en confidentialité que les autres données. L'accès aux données sensibles DEVRAIT être plus restreint. Dans le Doc 9303-11, l'authentification par terminal est définie comme un mécanisme interopérable permettant l'accès aux données sensibles. Si la fonction d'interopérabilité n'est pas nécessaire, d'autres mécanismes peuvent être utilisés. |
| DVLM électronique (DVLM-e) | DVLM (passeport, visa ou carte) qui contient un circuit intégré sans contact et qui permet l'identification biométrique de son titulaire conformément aux normes énoncées dans les parties pertinentes du Doc 9303 — *Documents de voyage lisibles à la machine*. |
| Écart entre les yeux et la bouche | Distance entre le centre du visage (M) et le point central de la bouche (point caractéristique 2.3 dans la norme ISO/IEC 14496-2). |
| Écart pupillaire | Distance entre le centre de l'œil gauche et le centre de l'œil droit. |
| Échange de clés | Processus par lequel des clés de session sont mises entre les mains de ceux qui conversent. |

| Terme | Définition |
|---|---|
| Échantillon biométrique | Données brutes capturées comme une valeur discrète, sans ambiguïté, unique et linguistiquement neutre, représentant une caractéristique biométrique d'une personne enrôlée, telle qu'elle a été saisie par un système biométrique (les échantillons biométriques peuvent comprendre, par exemple, l'image d'une empreinte digitale et le gabarit qui en est dérivé, aux fins de vérification d'identité). |
| Échec à l'acquisition | Se produit lorsqu'un système biométrique ne réussit pas à obtenir l'élément biométrique nécessaire à l'enrôlement d'une personne. |
| Échec à l'enrôlement | Se produit lorsqu'un système biométrique ne réussit pas à enrôler une personne. |
| Écoute électronique | Interception non autorisée d'une communication de données. |
| Écrémage | Lecture électronique des données stockées dans le CI sans contact sans que la lecture du document soit autorisée. |
| Élément biométrique à interopérabilité mondiale | Se rapporte à l'image du visage spécifiée dans le Doc 9303-9. |
| Élément biométrique vérifiable par machine | Élément physique d'identification personnelle unique (par exemple, image faciale, empreinte digitale ou iris), stocké électroniquement dans la puce d'un DVLM-e. |
| Élément de données | Incorporation d'informations codées dans la structure des données ou de l'image d'un document, généralement dans les données de personnalisation, en particulier le portrait. |
| Élément de structure | Élément de sécurité faisant intervenir l'incorporation dans ou sur le DVLM d'une structure mesurable, dont la présence peut être détectée et mesurée par l'appareil de détection. |
| Élément de substance | Élément de sécurité faisant intervenir l'incorporation dans le DVLM d'un matériau qui ne serait pas présent normalement et dont la présence n'apparaît pas de façon évidente à l'inspection visuelle. La présence de ce matériau peut être décelée par la présence et l'importance d'une propriété appropriée de la substance ajoutée. |
| Élément (d'identification) biométrique | Caractéristique physique unique mesurable ou trait comportemental personnel utilisé pour reconnaître l'identité, ou vérifier l'identité déclarée, d'une personne enrôlée. |
| Élément fenêtré ou transparent | Élément de sécurité créé par la construction du support, dont une partie est enlevée ou remplacée par un matériau transparent qui peut contenir des éléments de sécurité supplémentaires tels que des lentilles ou des éléments tactiles. |
| Élément lenticulaire | Élément de sécurité dans lequel une structure lenticulaire est intégrée dans la surface du document ou utilisée comme dispositif de vérification. |
| Élément optiquement variable (OVF) | Image ou élément dont l'apparence (couleur et/ou dessin) varie selon l'angle de vue ou d'éclairage. Exemples : éléments incluant des structures diffractives à haute résolution (DOVID — image diffractive optiquement variable), hologrammes, encres à couleur changeante (par exemple, encres à propriétés optiquement variables) ou autres matériaux diffractifs ou réfléchissants. |
| Élément tactile | Élément superficiel donnant au document un « toucher » particulier. |
| Émetteur | Organisme qui délivre des DVLM. |
| Empreinte(s) digitale(s) | Représentation(s) visuelle(s) de la structure superficielle du bout d'un ou de plusieurs doigts du titulaire du document. |

| Terme | Définition |
|---|---|
| Encre de couleur changeante | Encre dont la caractéristique visuelle varie selon l'angle de vue et/ou la qualité d'une source stimulante/lumineuse. |
| Encre de numérotation pénétrante | Encre contenant un composant qui pénètre profondément dans un support. |
| Encre fluorescente | Encre contenant un matériau qui émet une lueur lors de l'exposition à la lumière à une certaine longueur d'onde, généralement à la lumière ultraviolette (UV). |
| Encre infrarouge | Encre visible dans la région infrarouge du spectre lumineux. |
| Encre invisible dans l'infrarouge | Encre formant une image visible lors de l'exposition à la lumière dans la partie visible du spectre et qui ne peut être décelée si elle est illuminée dans la région infrarouge. |
| Encre marquée | Encres contenant des composés qui ne sont pas des substances s'y trouvant naturellement et qui peuvent être décelés au moyen d'un équipement spécial. |
| Encre métallique | Encre présentant un aspect métallisé. |
| Encre phosphorescente | Encre contenant un pigment qui émet une lueur lorsqu'il est exposé à la lumière d'une certaine longueur d'onde, cette lueur réactive restant visible pour disparaître progressivement lorsque cesse l'exposition à la source lumineuse. |
| Encre photochromique | Encre qui subit un changement de couleur réversible lorsqu'elle est exposée à la lumière d'une longueur d'onde spécifique. |
| Encres métamères | Deux encres formulées pour être apparemment de la même couleur lorsqu'elles sont observées dans des conditions spécifiées, normalement à la lumière du jour, mais qui sont contrastées sous d'autres longueurs d'onde. |
| Encres réactives | Encres contenant des réactifs de sécurité comme protection contre les tentatives de falsification par effacement chimique, une réaction détectable se produisant lorsqu'un agent de blanchiment ou un solvant entre en contact avec le document. |
| Encre thermochrome | Encre qui subit un changement de couleur réversible lorsque l'image imprimée est exposée à un certain changement de température. |
| Enregistrement | Processus qui consiste à faire connaître l'identité d'une personne à un système biométrique, en associant à cette identité un identifiant unique, et à recueillir et à enregistrer dans le système les attributs pertinents de la personne. |
| Enrôlement | Processus de collecte d'échantillons biométriques d'une personne, après quoi des gabarits de référence biométriques représentant l'identité de cette personne sont créés et stockés. |
| Ensemble de données d'authentification | Ensemble d'opérations de vérification courantes spécifiques à un modèle de document dans la base de données d'authentification. |
| Ensemble de données de référence | Les images (image visible et images sensibles aux rayons infrarouges et ultraviolets) d'un document de référence définissent les opérations de vérification courantes pour un modèle de document correspondant. |
| Ensemble de documents de référence | Ensemble des documents dont les ensembles de données de référence sont utilisés pour définir les opérations de vérification courantes. |
| État émetteur | Pays qui émet le DVLM. |

| Terme | Définition |
|---|---|
| État récepteur | Pays qui inspecte le DVLM du détenteur. |
| Étiquette (caractéristique) | Octet qui identifie de manière unique une caractéristique d'un document. Le mappage entre les étiquettes et les caractéristiques correspondantes doit être défini dans un profil. |
| Extraction | Processus de conversion d'un échantillon biométrique capturé en données biométriques, afin de permettre la comparaison avec un gabarit de référence. |
| Facteur de recadrage | Rapport entre la longueur de la diagonale du format plein cadre (43,3 mm) et celle du capteur d'image sélectionné de l'appareil. Il permet de choisir un objectif à la focale appropriée pour un champ de vision équivalent au format plein cadre. |
| Falsification | Altération frauduleuse de toute partie d'un document authentique. |
| Fausse acceptation | Se produit lorsqu'un système biométrique identifie incorrectement une personne ou vérifie incorrectement un imposteur par rapport à une identité déclarée. |
| Faux rejet | Se produit lorsqu'un système biométrique ne réussit pas à identifier une personne enrôlée ou à vérifier l'identité déclarée, légitime, d'une personne enrôlée. |
| Feuillet | Élément de support d'un passeport comprenant plus d'une page de passeport. |
| Fibres | Petites particules filiformes incorporées dans un support lors de la fabrication. |
| Fil de sécurité | Fine bandelette de plastique ou d'un autre matériau, incorporée ou partiellement incorporée dans la masse du support papier lors de sa fabrication, et qui peut être métallisée ou partiellement démétallisée. |
| Filigrane | Dessin présentant généralement une gradation de tons, formé dans la masse du papier ou d'un autre support lors de sa fabrication, par déplacement de matériaux dans ce support, et habituellement visible par transparence. |
| Filigrane numérique | Voir « stéganographie ». |
| Film de sécurité | Matériau transparent, pouvant comprendre des éléments de sécurité, destiné à être solidement scellé pour protéger la page de données personnelles ou toute autre page d'un document. |
| Film de sécurité ou revêtement à image diffractive optiquement variable (DOVID) | Film de sécurité ou revêtement contenant une DOVID couvrant une surface entière ou situé de façon à protéger les données essentielles sur le document. |
| Film de sécurité thermoscellé | Film destiné à être scellé sur la page de données personnelles d'un passeport en livret, par application de chaleur et de pression. |
| Gabarit biométrique | Données extraites et comprimées tirées d'un échantillon biométrique. |
| Gabarit de référence biométrique | Ensemble de données définissant une mesure biométrique d'une personne, qui sert de base à la comparaison avec un ou des échantillons biométriques soumis ultérieurement. |
| Gabarit/gabarit de référence | Données représentant une mesure biométrique d'une personne enrôlée, qu'un système biométrique utilise à des fins de comparaison avec des échantillons biométriques soumis ultérieurement. |

| Terme | Définition |
|---|---|
| Galerie | Base de données de gabarits biométriques de personnes précédemment enrôlées, dans laquelle une sonde peut être recherchée. |
| Gestion de clés | Processus par lequel des clés cryptographiques sont fournies pour être utilisées entre parties autorisées qui communiquent. |
| Gravure laser | Procédé utilisant le laser pour graver des données personnalisées sur le support. Les données peuvent être du texte, des portraits et d'autres éléments de sécurité. |
| Groupe de données | Série d'éléments de données apparentés, regroupés au sein d'une structure de données logique. |
| Guillochis | Motif en traits fins continus, généralement généré par ordinateur et formant une image unique qu'il n'est possible de reproduire exactement qu'en accédant au matériel, au logiciel et aux paramètres utilisés pour créer le dessin d'origine. |
| Hachage | Formule mathématique utilisée pour convertir un message de longueur quelconque en une chaîne unique de longueur fixe de caractères numériques dite « condensé de message » qui représente le message d'origine. Le hachage est une fonction à sens unique, ce qui signifie qu'il est impossible d'inverser le processus pour déterminer le message d'origine. Par ailleurs, une fonction de hachage ne produira pas le même condensé de message à partir de deux entrées différentes. |
| Hors bande | Désigne les communications utilisant un moyen ou un canal de communication autre que celui qui a été préalablement établi. |
| Identifiant | Chaîne de données unique, utilisée comme clé dans le système biométrique pour désigner l'identité d'une personne et les attributs qui lui sont associés. Un exemple d'identifiant serait un numéro de DVLM. |
| Identifiant d'application (AID) | Élément de données qui identifie une application. Les applications DVLM-e utilisent un AID normalisé, qui constitue une des quatre catégories d'AID. Il est formé d'un identificateur enregistré de fournisseur d'application (RID) et d'une extension d'identifiant d'application propriétaire (PIX). |
| Identification biométrique | Moyen d'identifier le titulaire d'un DVLM ou de confirmer son identité par la mesure d'une ou plusieurs propriétés de sa personne. |
| Identification/identifier | Le processus de comparaison entre un échantillon biométrique soumis et tous les gabarits biométriques de référence contenus dans une base de données, pour déterminer s'il correspond à l'un d'eux et, dans l'affirmative, déterminer l'identité du détenteur du DVLM-e. Le système biométrique qui utilise ce processus de comparaison cherche à trouver une identité au sein d'une base de données, et non à vérifier une identité déclarée. S'oppose à « vérification ». |
| Identité | L'ensemble collectif de caractéristiques personnelles et physiques distinctes, de données et de qualités permettant l'identification définitive d'une personne par rapport à d'autres. Dans un système biométrique, l'identité est généralement établie lorsque la personne est enregistrée dans le système sur la base de l'utilisation de « documents sources » tels qu'un certificat de naissance et un certificat de citoyenneté. |

| Terme | Définition |
|---|---|
| Illuminant CIE normalisé D65 | Illuminant couramment utilisé, normalisé par la Commission internationale de l'éclairage (CIE). Il fait partie des illuminants de la série D (lumière du jour) qui tentent de représenter les conditions d'éclairage naturel habituelles dans différentes régions du monde. |
| Image | Représentation d'un élément biométrique généralement captée par caméra vidéo, appareil photo ou scanneur. Aux fins des applications biométriques, elle est stockée sous forme numérisée. |
| Image diffractive optiquement variable | Élément de sécurité contenant dans sa construction une image holographique ou une image équivalente, dont l'apparence se modifie selon l'angle de vue ou d'éclairage. |
| Image enfouie | Image ou information codée ou cachée au sein d'une image visuelle primaire. Voir aussi « stéganographie ». |
| Image fantôme | Représentation secondaire du portrait du titulaire sur le document, de contraste et/ou saturation et/ou format réduit. |
| Image frontale complète (du visage) | Portrait du titulaire du DVLM produit en accord avec les spécifications établies dans le Doc 9303. |
| Image jeton | Portrait du titulaire du DVLM, généralement une image frontale complète dont la taille a été ajustée pour assurer une distance déterminée entre les yeux. Une légère rotation peut aussi être effectuée pour qu'une ligne horizontale imaginaire entre les centres des deux yeux soit parallèle au bord supérieur du rectangle du portrait, si cela n'a pas été réalisé lors de la prise de vue ou de la capture du portrait original. |
| Image laser variable | Élément généré par gravure laser ou perforation laser, présentant des informations ou des images qui changent selon l'angle de vue. |
| Image latente | Image cachée formée au sein d'une image en relief, qui est composée de structures linéaires de direction et de profil variables, faisant apparaître l'image cachée sous des angles d'observation préalablement déterminés ; cette image est réalisée en taille douce. |
| Image secondaire | Image reproduisant le portrait du titulaire présentée ailleurs dans le document par un procédé quelconque. |
| Imposteur | Personne qui demande et obtient un document en utilisant une fausse identité ou qui modifie sa propre apparence physique pour se faire passer pour une autre personne afin d'utiliser un document lui appartenant. |
| Impression irisée (séparation de l'encrier) | Technique par laquelle deux ou plusieurs couleurs d'encre sont imprimées simultanément sur une presse de manière à créer une fusion continue des couleurs semblable à l'effet vu dans un arc-en-ciel. |
| Indice de lumination (IL) | Chiffre qui caractérise le couplage d'une vitesse d'obturation et d'un nombre d'ouverture (f/ ou f:) d'un appareil photo. Ainsi, toutes les combinaisons qui produisent la même exposition ont le même indice de lumination. |
| Infrastructure à clés publiques (ICP) | Ensemble de politiques, de processus et de technologies utilisé pour vérifier, enrôler et certifier des utilisateurs d'une application de sécurité. Une ICP emploie des pratiques de cryptographie à clé publique et de certification de clés pour sécuriser les communications. |

| Terme | Définition |
|---|---|
| Initialisation (d'une carte intelligente) | Processus qui consiste à peupler une mémoire persistante (EEPROM, etc.) avec des données qui sont communes à un grand nombre de cartes, en incluant aussi un minimum d'éléments propres à la carte (par exemple, numéro de série de CCI et clés de personnalisation). |
| Inspection | Examen par un État ou une organisation d'un DVLM qui lui est présenté par un voyageur (le détenteur du DVLM) pour en vérifier l'authenticité. |
| Inspection de niveau 1 | Examen superficiel pour une inspection rapide au point d'utilisation (éléments visuels ou tactiles facilement identifiables). |
| Inspection de niveau 2 | Examen au moyen d'un équipement simple par des inspecteurs qualifiés. |
| Inspection de niveau 3 | Inspection par des spécialistes de la police scientifique. |
| Intégration de systèmes | Processus par lequel des systèmes utilisés en interaction avec le détenteur de la carte, les systèmes internes ou les partenaires sont intégrés entre eux. |
| Intégrité | Propriété assurant que la structure de données logique et ses éléments n'ont pas été altérés par rapport à ceux que l'État émetteur ou l'organisation émettrice a créés. |
| Interface | Définition technique normalisée de la connexion entre deux composants. |
| Interopérabilité | Capacité qu'ont plusieurs systèmes indépendants ou éléments de sous-systèmes de travailler ensemble. |
| Interopérabilité mondiale | Capacité qu'ont les systèmes d'inspection (manuels ou automatisés), dans les différents pays du monde, d'obtenir et d'échanger des données, de traiter les données reçues de systèmes d'autres États, et d'utiliser ces données pour les opérations d'inspection dans leurs pays respectifs. L'interopérabilité mondiale est un objectif majeur des spécifications normalisées relatives à l'insertion des données lisibles visuellement et lisibles par machine dans tous les DVLM-e. |
| JPEG et JPEG2000 | Norme pour la compression de données d'images, utilisée en particulier dans le stockage d'images faciales. |
| Laissez-passer | Document, généralement semblable à un passeport, émis sous les auspices d'une entité supranationale (par exemple, les Nations Unies). |
| Liste d'écarts | Liste signée émise par un État émetteur spécifiant les non-conformités des documents de voyage et/ou des clés et des certificats. |
| Liste de certificats révoqués (CRL) | Liste des certificats qui ont été révoqués, aussi appelée « liste de révocation de certificats ». Les documents liés à un certificat figurant sur une de ces listes, ou signés dans le cadre d'un tel certificat, ne sont donc plus dignes de confiance. |
| Liste de contrôle | Liste signée numériquement des certificats d'ACSN bénéficiant de la confiance de l'État récepteur qui a émis la liste de contrôle (voir Doc 9303-12) |
| Marque habituelle | Symbole qui remplace la signature écrite du titulaire lorsque celui-ci est incapable de signer. |
| Marques de collationnement | Voir « repères de collationnement ». |

| Terme | Définition |
|---|---|
| Marqueur | Substance qui n'est pas contenue naturellement dans les composants physiques d'un DVLM et qui peut y être ajoutée, constituant habituellement un élément de niveau 3, et dont la détection exige l'emploi d'un équipement spécial. |
| Mémoire morte (ROM) | Mémoire non volatile écrite une seule fois, généralement pendant la production du CI, utilisée pour stocker les systèmes d'exploitation et algorithmes utilisés par le semi-conducteur dans une carte à circuit intégré pendant des transactions. |
| Mémoire morte programmable effaçable électriquement (EEPROM) | Technologie de mémoire non volatile permettant d'effacer et de réécrire des données électriquement. |
| Mémoire non volatile | Mémoire à semi-conducteurs qui conserve son contenu si le courant est coupé (c.-à-d. ROM, EEPROM). |
| Mémoire vive (RAM) | Mémoire volatile à accès aléatoire utilisée dans le CI qui exige une alimentation électrique pour maintenir les données. |
| Menton | Partie avant-centre de la mâchoire inférieure. |
| Message | Plus petite collection d'informations dotée de sens, transmise d'un expéditeur à un destinataire. Ces informations peuvent être constituées d'une ou plusieurs transactions par carte ou d'informations en rapport avec des transactions par carte. |
| Message sécurisé | Message protégé contre l'altération ou l'émission illicites. |
| Microimpression | Texte ou symboles imprimés plus petits que 0,25 mm/0,7 point pica. |
| Modèle de document | Regroupe les séries de documents d'un État qui ont la même apparence visuelle, comme les documents (D, P, 1, 2005), (D, P, 2, 2007) et (D, P, 3, 2010). Il est possible que plusieurs modèles de document valides d'un même État soient en circulation à un moment donné [par exemple : (GBR, P, 1, 2008) et (GBR, P, 2, 2010)]. |
| Moirage (effet de) | Apparence ondulée d'une scène ou d'un objet photographié causée par la présence de détails répétitifs (par exemple : traits, points, etc.) qui dépassent la résolution du capteur de l'appareil. |
| Morphose | Technique de modification d'image où deux visages ou plus sont transformés ou fusionnés pour ne former qu'un seul visage sur une photographie. |
| Motif anti-scan | Image généralement formée de traits fins à déplacement angulaire variable, incorporée dans le dessin du fond de sécurité. Vue normalement, cette image enfouie ne se distingue pas du reste de l'impression de sécurité du fond, mais elle devient visible lorsque l'original est scanné ou photocopié. |
| Motif en repérage recto-verso (par transparence) | Motif imprimé en parfait repérage sur les deux faces d'une page intérieure du document, qui, lorsque la page est observée par transparence, forme une image enchevêtrée. |
| MP | Modèle de mesure (longueur de côté) : zones de mesure d'intensité carrées mesurant 30 % de l'écart pupillaire. Elles sont utilisées pour mesurer l'intensité de la lumière sur les joues, le front et le menton. |

| Terme | Définition |
|---|---|
| Mystification | Action de contrefaire l'adresse émettrice d'une transmission de façon à pénétrer illégalement dans un système sécurisé.<br><br>*Note.— Usurpation d'identité, déguisement, substitution d'identité* (piggybacking) *et imitation sont des formes de mystification.* |
| Norme de chiffrement de données (DES) | Méthode de chiffrement de données spécifiée dans la norme FIPS 46-3. |
| Numéro de contrôle | Numéro attribué à un document au moment de sa fabrication à des fins de comptabilisation et de sécurisation. |
| Numéro de document | Numéro qui identifie un document de façon unique. Il est recommandé que le numéro de document et le numéro de contrôle soient identiques. |
| Numéro d'identification personnel (NIP) | Code de sécurité numérique utilisé comme mécanisme de vérification 1:1 locale avec l'objectif de déterminer si le détenteur de la carte est effectivement la personne naturelle autorisée à accéder à un certain service ou à l'utiliser, tel que le droit de déverrouiller certaines informations sur la carte. |
| Octet | Ensemble de huit bits, généralement traité comme une unité. |
| Opérations de vérification courantes | Procédure de vérification de propriétés spécifiques d'un élément (par exemple : vérification de la présence d'une photographie à l'aide d'une lampe infrarouge). |
| Organisation émettrice | Organisation habilitée à émettre un DVLM officiel (par exemple, l'Organisation des Nations Unies, qui émet le laissez-passer). |
| Organisme récepteur autorisé | Organisme autorisé à traiter un document de voyage officiel (exploitant d'aéronefs, par exemple) et, comme tel, susceptible d'être autorisé dans l'avenir à enregistrer des détails dans la technologie optionnelle d'expansion de capacité. |
| Page de renseignements | Page d'un passeport en livret, de préférence la deuxième ou l'avant-dernière page, qui contient les données personnelles du titulaire du document. Voir « données personnelles ». |
| Page de renseignements du PLM | Page à dimensions fixes dans le PLM, contenant une présentation normalisée des données lisibles visuellement et à la machine. |
| Paire de clés | Paire de clés numériques — une clé publique et une clé privée — utilisée pour chiffrer et signer des informations numériques. |
| Parallaxe | Différence ou déplacement apparent de la position d'un objet selon deux lignes de visée différentes, correspondant à l'angle ou au demi-angle d'inclinaison entre ces deux lignes. |
| Participant au RCP | État membre de l'OACI ou autre entité qui émet ou a l'intention d'émettre des DVLM-e et qui se conforme aux dispositions régissant la participation au RCP de l'OACI. |
| Passeport électronique (PLM-e) | DVLM de format TD3 conforme aux spécifications du Doc 9303-4, qui contient en outre un circuit intégré sans contact et qui permet l'identification biométrique de son titulaire. |

| Terme | Définition |
|---|---|
| Passeport lisible à la machine (PLM) | Passeport conforme aux spécifications énoncées dans le Doc 9303-4. Le PLM est normalement réalisé sous la forme d'un livret au format TD3 contenant des pages réservées aux renseignements sur le titulaire et sur l'État émetteur ou l'organisation émettrice, et des pages réservées aux visas et autres endossements. Les renseignements lisibles par machine sont présentés en deux lignes de texte ROC-B, de 44 caractères chacune. |
| Perforation laser | Procédé de perforation du support à l'aide du laser pour créer des numéros, des lettres ou des images. |
| Personnalisation | Processus par lequel le portrait, la signature et les données personnelles sont appliqués au document. |
| Personne enrôlée | Être humain, c'est-à-dire personne physique, à qui un DVLM est délivré par un État émetteur ou une organisation émettrice. |
| Politique de sécurité du système | Ensemble de lois, de règles et de pratiques qui régulent la façon dont des informations sensibles et d'autres ressources sont gérées, protégées et distribuées au sein d'un certain système. |
| Portrait | Représentation visuelle de l'image faciale du titulaire du DVLM, imprimée ou stockée sous format numérique. |
| Poste de CFA | Poste de contrôle frontalier automatisé des documents de voyage électroniques lisibles à la machine. |
| Réactifs chimiques | Réactifs de sécurité utilisés pour protéger contre les falsifications par effacement chimique, des couleurs irréversibles se développant lorsqu'un agent de blanchiment ou des solvants entrent en contact avec le document. |
| Remplissage | Ajout de bits supplémentaires d'un côté ou de l'autre d'une chaîne de données jusqu'à une longueur prédéfinie. |
| Repères de collationnement | Repères consécutifs imprimés sur le bord extérieur de chaque page en commençant au haut de la première page. Le repère suivant est situé un peu plus bas sur la page suivante et ainsi de suite jusqu'au dernier repère, situé au bas de la dernière page. Cette méthode d'impression fait apparaître une ligne continue sur la tranche du passeport. Toute page retirée du passeport crée une discontinuité dans la ligne. Si elle est imprimée en couleur UV, la ligne devient visible lorsqu'elle est exposée à la lumière UV. |
| Répertoire OACI de clés publiques | Base de données centrale servant, d'une part, de répertoire de certificats de signataires de documents, de listes de contrôle de l'ACSN, de certificats de liaison de l'ACSN et de listes de certificats révoqués émis par les participants, et, d'autre part, de système de diffusion mondiale, tenue par l'OACI au nom des participants dans le but de faciliter la validation des données figurant dans les DVLM-e. |
| Répertoire/répertoire de clés publiques (RCP) | Répertoire où sont stockées des informations. En général, le répertoire d'une infrastructure ICP donnée est un répertoire des certificats de chiffrement à clés publiques émis par l'autorité de certification de cette ICP, ainsi que d'autres informations client. Le répertoire contient aussi des certificats croisés, des listes de certificats révoqués et des listes de révocation d'autorités. |
| Réponse | Message retourné par l'esclave au maître après le traitement d'une commande reçue par l'esclave. |

| Terme | Définition |
|---|---|
| Résistance à la falsification | Capacité de composants d'un document de résister à l'altération. |
| Revêtement | Film ou enduit de protection ultra-mince qui peut être appliqué à la surface d'un document, au lieu d'un film de sécurité. |
| Rivest, Shamir et Adleman (RSA) | Algorithme asymétrique développé par Ron Rivest, Adi Shamir et Len Adleman et utilisé dans la cryptographie à clé publique. Il est basé sur le fait qu'il est facile de multiplier deux grands nombres premiers mais qu'il est difficile de les factoriser à partir du produit. |
| Schéma de signature (cryptographique) numérique | Tuple de trois algorithmes. L'algorithme de génération de clés reçoit un paramètre de sécurité en entrée et délivre une paire de clés (clé privée et clé publique) en sortie. L'algorithme de signature reçoit une clé privée et un message en entrée, et délivre une signature cryptographique en sortie. L'algorithme de vérification reçoit une clé publique, un message et une signature en entrée, puis délivre le message « valide » si la signature a bien été générée par l'entrée de la clé privée de la paire de clés et du message dans l'algorithme de génération de signatures, ou le message « invalide » si ce n'est pas le cas. |
| Score | Nombre, sur une échelle allant de bas à haut, mesurant le succès avec lequel l'enregistrement d'une sonde biométrique (la personne faisant l'objet d'une recherche) est apparié à un certain enregistrement d'une galerie (personne enrôlée précédemment). |
| Sécurité physique | Ensemble de mesures de sécurité appliquées durant la production et la personnalisation pour empêcher le vol et l'accès non autorisé au processus. |
| Seuil | Score « repère ». La comparaison entre la valeur obtenue après les opérations de vérification courantes et le seuil correspondant détermine la décision d'acceptation ou de refus. |
| Signataire de code à barres | Entité qui signe numériquement les données (en-tête et message) codées sous la forme du code à barres, lequel contient aussi la signature. |
| Signataire de document | Organisme qui émet un document biométrique et certifie que les données stockées sur le document sont authentiques, d'une façon qui permettra la détection d'altérations frauduleuses. |
| Signataire de liste d'écarts | Entité qui signe numériquement la liste d'écarts. Le signataire de liste d'écarts est autorisé par son AC signataire nationale à exécuter cette fonction par l'émission d'un certificat de signataire de liste d'écarts. |
| Signataire de liste de contrôle | Entité qui signe numériquement une liste de contrôle de certificats d'ACSN. Le signataire de la liste de contrôle est autorisé par son ACSN nationale à exécuter cette fonction par l'émission d'un certificat de signataire de liste de contrôle. |
| Signataire de visa (VS) | Autorité qui reçoit des données de la part d'un système de personnalisation des visas et qui utilise un certificat de signataire de visa ainsi que la clé privée correspondante pour coder et signer un cachet numérique visible. |
| Signature affichée | Signature manuscrite originale ou reproduction de la signature originale imprimée par un procédé numérique. |
| Signature (cryptographique) numérique | Résultat d'une opération cryptographique permettant de valider l'information par des moyens électroniques. Il NE s'agit PAS de la signature numérisée du titulaire de DVLM. |

| Terme | Définition |
|---|---|
| Sommet du crâne | Extrémité supérieure de la tête, à la racine des cheveux. |
| Sonde | Échantillon biométrique de la personne enrôlée dont on cherche à établir l'identité. |
| Stéganographie | Image ou information codée ou cachée au sein d'une image visuelle primaire. |
| Structure de données logique (SDL) | Structure qui décrit comment les données doivent être stockées et formatées dans le CI sans contact d'un DVLM-e. |
| Substitution de photographie | Type de falsification dans lequel le portrait figurant dans un document est remplacé par un portrait différent après la délivrance de ce document. |
| Sujet | Personne qui apparaît sur le portrait affiché et qui devrait être titulaire du DVLM. |
| Support sans fluorescence sous UV | Support ne présentant pas de fluorescence visuellement décelable lorsqu'il est exposé à la lumière ultraviolette. |
| Symbologie du code à barres | Mappage des messages et des codes à barres. Ce mappage est défini dans la spécification du code à barres et comprend le codage de chiffres ou de caractères, la dimension de la « zone de silence » (marge autour du code à barres), ainsi que le calcul des sommes de contrôle pour la correction d'erreurs. |
| Synthétique | Matériau non basé sur le papier, utilisé pour la page de données personnelles ou les cartes. Le terme « synthétique » est employé comme synonyme de « plastique », qui comprend des matériaux tels que le polycarbonate, le PET et des matériaux ou des combinaisons de matériaux semblables. |
| Système | Installation informatique particulière, avec un objet particulier et un environnement d'exploitation particulier. |
| Système à clé publique | Méthode cryptographique utilisant une paire de clés, l'une d'entre elles étant une clé privée et l'autre une clé publique. Si le chiffrement utilise la clé publique, le déchiffrement exige l'application de la clé privée correspondante, et vice versa. |
| Système biométrique | Système informatisé qui peut :<br>1. capturer pour un PLM un échantillon biométrique provenant d'un utilisateur ;<br>2. extraire de cet échantillon des données biométriques ;<br>3. comparer la valeur (les valeurs) de ces données biométriques spécifiques aux valeurs contenues dans un ou plusieurs gabarits de référence ;<br>4. décider du degré de concordance des données, autrement dit exécuter un processus de comparaison, basé sur des règles, spécifique aux besoins de l'identification sans ambiguïté et de la validation de l'identité de la personne enrôlée en ce qui concerne la transaction en cause ;<br>5. indiquer si une identification ou une vérification d'identité a été réalisée ou non. |
| Système d'exploitation | Programme qui gère les divers programmes d'application utilisés par un ordinateur. |
| Système d'inspection | Système utilisé pour l'inspection de DVLM par toute entité publique ou privée qui a besoin de valider le DVLM et d'utiliser ce document pour une vérification d'identité, par exemple, autorités de contrôle frontalier, compagnies aériennes et autres opérateurs de transports, institutions financières. |

| Terme | Définition |
|---|---|
| Taille douce | Technique d'impression employée pour la production de documents de sécurité, utilisant une haute pression pour l'impression et des encres spéciales pour créer une image en relief perceptible tactilement à la surface du document. |
| Taille du gabarit | Quantité de mémoire d'ordinateur qu'occupent les données biométriques. |
| Taux de fausses acceptations (FAR) | Probabilité qu'un système biométrique identifie incorrectement une personne ou ne réussisse pas à rejeter un imposteur. Ce taux suppose normalement des tentatives d'imposteurs passifs. Le taux de fausses acceptations peut être estimé par la formule : FAR = NFA/NIIA ou FAR = NFA/NIVA, FAR étant le taux de fausses acceptations, NFA le nombre de fausses acceptations, NIIA le nombre de tentatives d'identification d'imposteurs et NIVA le nombre de tentatives de vérification d'imposteurs. |
| Taux de fausses correspondances | Variante du « taux de fausses acceptations » ; employée pour éviter la confusion dans des applications qui rejettent les prétendants alors que leurs données biométriques correspondent à celles d'une personne enrôlée. Dans de telles applications, les concepts d'acceptation et de rejet sont inversés, ce qui inverse le sens des termes « fausse acceptation » et « faux rejet ». |
| Taux de fausses non-correspondances | Variante du « taux de faux rejets » ; employée pour éviter la confusion dans des applications qui rejettent les prétendants alors que leurs données biométriques correspondent à celles d'une personne enrôlée. Dans de telles applications, les concepts d'acceptation et de rejet sont inversés, ce qui inverse le sens des termes « fausse acceptation » et « faux rejet ». |
| Taux de faux rejets (FRR) | Probabilité qu'un système biométrique échoue à identifier une personne enrôlée ou à vérifier l'identité déclarée, légitime, d'une personne enrôlée. Le taux de faux rejets peut être estimé par la formule : FRR = NFR/NEIA ou FRR = NFR/NEVA, FRR étant le taux de faux rejets, NFR le nombre de faux rejets, NEIA le nombre de tentatives d'identification de personnes enrôlées et NEVA le nombre de tentatives de vérification de personnes enrôlées. Cette estimation suppose que les tentatives d'identification/de vérification sont représentatives des tentatives pour l'ensemble de la population de personnes enrôlées. Le taux de faux rejets exclut normalement les erreurs par « échec à l'acquisition ». |
| Utilisateur | Personne qui interagit avec un système biométrique pour s'enrôler ou faire vérifier sa propre identité. |
| Validation | Processus qui consiste à démontrer que le système considéré répond à tous égards aux spécifications qui s'y rapportent. |
| Vérification biométrique | Moyen d'identifier le titulaire d'un DVLM ou de confirmer son identité par la mesure et la validation d'une ou plusieurs propriétés uniques de sa personne. |
| Vérification de document assistée par ordinateur | Processus utilisant un dispositif pour aider à la vérification de l'authenticité du document en ce qui concerne les données et/ou la sécurisation. |
| Vérification/vérifier | Biométrie : Processus de comparaison entre un échantillon biométrique soumis et un gabarit de référence biométrique d'une personne enrôlée dont l'identité est revendiquée, afin de déterminer si l'échantillon correspond au gabarit de la personne enrôlée. S'oppose à « identification ».<br><br>Authentification par machine : Exécution des opérations de vérification courantes sur un ensemble de données réelles d'un modèle de document. Le résultat de la vérification prend souvent la forme d'une valeur numérique. |

| Terme | Définition |
|---|---|
| Verrouillage (puce) | Après personnalisation, la puce DOIT être verrouillée. Alors, les commandes de personnalisation ne peuvent plus être exécutées et aucune donnée de personnalisation ne peut plus être inscrite sur la puce sans exécution réussie du mécanisme d'authentification. Une puce verrouillée ne peut pas être « déverrouillée ». |
| Vignette | Autocollant utilisé comme page de renseignements dans un passeport. Cette pratique n'est généralement pas recommandée, particulièrement pour les documents ayant une longue durée de validité. |
| Visa lisible à la machine (VLM) | Visa conforme aux spécifications énoncées dans le Doc 9303-7. Le VLM est normalement apposé sur une des pages réservées aux visas dans un passeport. |
| Visa lisible à la machine de grand format (type A) (VLM-A) | VLM conforme aux spécifications dimensionnelles énoncées dans le Doc 9303-7, celles-ci étant telles qu'il occupe entièrement une des pages du passeport réservées aux visas. |
| Visa lisible à la machine de petit format (type B) (VLM-B) | VLM conforme aux dimensions spécifiées dans le Doc 9303-7, prévues pour laisser une zone vierge sur la page de visa du passeport. |
| Visa papier | Document de voyage en papier apposé à l'intérieur du passeport du voyageur. |
| Wavelet Scalar Quantization (WSQ) | Procédé de compression des données, utilisé en particulier pour le stockage des images d'empreintes digitales. |
| Zone | Espace défini, contenant un groupement logique d'éléments de données sur le DVLM. Sept (7) zones sont définies pour les DVLM. |
| Zone de lecture automatique (ZLA) | Espace de dimensions fixes situé sur le DVLM, contenant des renseignements obligatoires et des renseignements facultatifs dans une forme se prêtant à la lecture automatique utilisant les méthodes ROC. |
| Zone de lecture effective (ZLE) | Espace de dimensions fixées, commun à tous les DVLM, à l'intérieur duquel les données lisibles par machine figurant dans la ZLA peuvent être lues par des appareils de lecture de documents. |
| Zone d'inspection visuelle (ZIV) | Parties du DVLM (de la page de renseignements dans le cas du PLM) destinées à l'inspection visuelle, recto et verso (le cas échéant), non définies comme constituant la ZLA. |

### 4.3 Mots clés

Les mots clés suivants sont employés pour signifier les obligations.

Les mots clés « DOIT/DOIVENT », « NE DOIT/DOIVENT PAS », « EXIGE/EXIGENT », « IL FAUT », « IL NE FAUT PAS », « DEVRAIT/DEVRAIENT » ou « IL FAUDRAIT », « NE DEVRAIT/DEVRAIENT PAS », « RECOMMANDÉ », « PEUT/PEUVENT » et « OPTIONNEL », écrits en lettres capitales dans le Doc 9303, doivent être interprétés de la façon décrite dans le document RFC 2119 (pour les termes anglais correspondants « MUST », « MUST NOT », « REQUIRED », « SHALL », « SHALL NOT », « SHOULD », « SHOULD NOT », « RECOMMENDED », « MAY » et « OPTIONAL »).

| | |
|---|---|
| DOIT/DOIVENT | Ces mots ou les termes « EXIGE » et « IL FAUT » signifient que la définition est une exigence absolue de la spécification. |

| | |
|---|---|
| NE DOIT/DOIVENT PAS<br>IL NE FAUT PAS | Ces mots signifient que la définition est une interdiction absolue de la spécification. |
| DEVRAIT/DEVRAIENT<br>IL FAUDRAIT | Ces mots ou le terme « RECOMMANDÉ » signifient qu'il peut exister des raisons valables, dans des circonstances particulières, pour ne pas tenir compte d'un point particulier, mais les implications complètes devront être comprises et pesées avec soin avant de choisir une voie différente. |
| NE DEVRAIT/<br>DEVRAIENT PAS | Ces mots ou l'expression « PAS RECOMMANDÉ » signifient qu'il peut exister des raisons valables, dans des circonstances particulières, où le comportement particulier est acceptable, voire utile, mais les implications complètes devront être comprises et pesées avec soin avant de mettre en œuvre toute façon de procéder ainsi décrite. |
| PEUT/PEUVENT | Ces mots, ou l'adjectif « OPTIONNEL », signifient qu'un élément est vraiment optionnel. Un usager peut choisir de l'inclure parce qu'une application particulière l'exige ou parce qu'il estime que cela renforcerait l'application, tandis qu'un autre usager pourra omettre le même élément. Une implémentation qui n'inclut pas une option particulière DOIT pouvoir interagir avec une autre implémentation qui inclut l'option, quoique peut-être avec une fonctionnalité réduite. Dans la même veine, une implémentation qui inclut une option particulière DOIT pouvoir interagir avec une autre implémentation n'incluant pas l'option (exception faite, bien sûr, de ce que l'option prévoit). |
| CONDITIONNEL | L'emploi d'un élément dépend de l'emploi d'autres éléments. Les conditions dans lesquelles l'élément est « EXIGÉ/REQUIS » ou « RECOMMANDÉ » sont précisées. Ce mot clé est utilisé dans le Doc 9303 mais ne figure pas dans le document RFC 2119. |

*Orientations pour l'utilisation.* Les impératifs du type défini dans le présent document doivent être appliqués avec soin et modération. En particulier, ils ne DOIVENT être utilisés que lorsqu'ils sont réellement requis pour l'interopération ou pour limiter un comportement qui pourrait être préjudiciable (par exemple, en limitant les retransmissions). Ils ne doivent pas, par exemple, être utilisés pour tenter d'imposer une méthode particulière aux responsables de la mise en œuvre alors que cette méthode n'est pas requise pour l'interopérabilité.

*Considérations de sécurité*. Ces termes sont fréquemment employés pour spécifier un comportement ayant des incidences sur la sécurité. Les effets sur la sécurité de la non-application d'un DOIT ou d'un DEVRAIT, ou de l'application d'un élément dont il est spécifié qu'il NE DOIT PAS ou NE DEVRAIT PAS être appliqué, peuvent être très subtils. Les auteurs de documents devraient prendre le temps de préciser les incidences sur la sécurité de la non-application des recommandations ou des spécifications, car la plupart des responsables de la mise en œuvre n'auront pas les connaissances découlant de l'expérience et des analyses qui ont produit la spécification.

Les éléments OPTIONNELS mis en œuvre DOIVENT l'être de la façon décrite dans le Doc 9303.

Les appendices du Doc 9303 sont de nature informative. En cas de déclaration de conformité à un appendice (informatif), les mots clés utilisés dans l'appendice en question DOIVENT respecter les spécifications.

### 4.4 Identificateurs d'objets

Les identificateurs d'objets OACI sont spécifiés dans les Doc 9303-10, 9303-11 et 9303-12. Le présent paragraphe donne la liste de ces identificateurs :

```
-- cadre de sécurité OACI
id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136)}

id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}

id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}


-- objet de sécurité SDL
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 1}


-- liste de contrôle de l'ACSN
id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 2}

id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 3}


-- protocole d'authentification active
id-icao-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 5}


-- changement de nom d'ACSN
id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}

id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icao-
mrtd-security-extensions 1}


-- liste de type de documents, voir TR « Maintenance SDL et ICP »
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {id-
icao-mrtd-security-extensions 2}


-- identificateurs d'objets de base de liste d'écarts
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}

id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 8}

id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}

id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 1}

id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 2}
```

```
id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 3}

id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 4}

id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}

id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}

id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 3}

id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}

id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}

id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}


-- identificateurs d'objets LDS2
id-icao-mrtd-security-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 8}

id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}

id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}

id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 3}

id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}

id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-
travelRecords 1}

id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= { id-icao-lds2-
travelRecords 3}

id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}

id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-
visaRecords 1}

id-icao-lds2-visaRecords-access OBJECT IDENTIFIER ::= { id-icao-lds2-visaRecords 3}

id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}

id-icao-lds2- additionalBiometrics-application OBJECT IDENTIFIER ::= { id-icao-
lds2- additionalBiometrics 1}
```

```
id-icao-lds2- additionalBiometrics-access OBJECT IDENTIFIER ::= { id-icao-lds2-
additionalBiometrics 3}


-- identificateurs d'objets SPOC
id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}

id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-spoc 1}

id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-spoc 2}


-- Identificateurs d'objets VDS
id-icao-vds OBJECT IDENTIFIER ::= { id-icao-mrtd-security 11}


-- Identificateurs d'objets DTC
id-icao-dtc OBJECT IDENTIFIER ::= { id-icao-mrtd-security 12}

id-icao-dtcSigner OBJECT IDENTIFIER ::= {id-icao-dtc 1}

id-icao-dtcAttributes OBJECT IDENTIFIER ::= {id-icao-dtc 2}

id-icao-dtcCapabilitiesInfo OBJECT IDENTIFIER ::= {id-icao-dtcAttributes 1}


-- Identificateurs d'objets EF.DIR
id-EFDIR OBJECT IDENTIFIER ::= { id-icao-mrtd-security 13}
```

### 4.5 Utilisation de notes

Même si les notes des normes ISO/IEC sont de nature informative, celles du Doc 9303 font partie du texte normatif et sont employées pour souligner les exigences ou pour donner des renseignements supplémentaires.

## 5. APERÇU DU DOC 9303

### 5.1 Structure du Doc 9303

Le Doc 9303 est constitué de 13 parties. Chaque partie décrit un élément particulier des DVLM. Les parties du Doc 9303 sont conçues de manière à permettre à une entité émettrice de DVLM de composer un ensemble complet de spécifications applicables à un type (format) particulier de DVLM. La relation entre le format des DVLM et les parties du Doc 9303 est décrite au § 5.2 de la présente partie.

Les parties suivantes constituent les spécifications complètes du Doc 9303 sur les DVLM :

**Partie 1 — Introduction**
La présente partie du Doc 9303.

**Partie 2 — Spécifications pour la sécurité de la conception, de la fabrication et de la délivrance des DVLM**
La Partie 2 contient des spécifications obligatoires et des spécifications optionnelles sur les précautions que doivent prendre les autorités de délivrance de documents de voyage pour sécuriser, contre tout acte frauduleux, les DVLM et les moyens utilisés pour les personnaliser et les délivrer à leurs titulaires légitimes. Elle présente aussi des spécifications obligatoires et des spécifications optionnelles sur la sécurité physique des locaux où les DVLM sont produits, personnalisés et délivrés, ainsi que sur le contrôle de sécurité des personnels chargés de ces opérations.

**Partie 3 — Spécifications communes à tous les DVLM**
La Partie 3 définit des spécifications communes aux DVLM de format TD1, TD2 et TD3, notamment celles qui sont nécessaires pour assurer l'interopérabilité mondiale, qu'il s'agisse d'inspection visuelle ou de lecture par machine (reconnaissance optique des caractères). Les spécifications détaillées applicables à chacun des formats figurent dans les Parties 4 à 7 du Doc 9303.

**Partie 4 — Spécifications pour les passeports lisibles à la machine (PLM) et autres DVLM de format TD3**
La Partie 4 définit des spécifications pour les passeports lisibles à la machine (PLM) et autres DVLM de format TD3. Par souci de concision, le terme PLM est employé dans cette partie mais, sauf indication contraire, les spécifications de ce document s'appliquent également à tous les autres DVLM de format TD3.

**Partie 5 — Spécifications pour les documents de voyage officiels lisibles à la machine (DVOLM) de format TD1**
La Partie 5 définit les spécifications applicables aux DVOLM de format TD1.

**Partie 6 — Spécifications pour les documents de voyage officiels lisibles à la machine (DVOLM) de format TD2**
La Partie 6 définit les spécifications applicables aux DVOLM de format TD2.

**Partie 7 — Visas lisibles à la machine**
La Partie 7 définit les spécifications relatives aux visas lisibles à la machine (VLM). Ces spécifications assurent la compatibilité et les échanges à l'échelle mondiale par des moyens de lecture visuelle (oculaire) et de lecture par machine. Elles établissent des normes pour des visas qui peuvent, s'ils sont émis par un État et acceptés par un État récepteur, être utilisés pour voyager. Le VLM doit contenir, au minimum, les données spécifiées dans la Partie 7, sous une forme lisible à l'œil nu ainsi que par les méthodes de reconnaissance optique des caractères décrites dans cette partie.

La Partie 7 contient des spécifications applicables aux visas de type A et de type B. Elle est basée sur la troisième édition du Doc 9303, Partie 2, *Visas lisibles à la machine* (2005).

**Partie 8 — Documents de voyage d'urgence**
La Partie 8 contient des orientations et des spécifications sur les documents de voyage d'urgence. Ces éléments indicatifs ont pour but de promouvoir un système cohérent de délivrance des documents de voyage d'urgence afin de renforcer la sécurité des documents, protéger les personnes, améliorer la confiance du personnel frontalier lorsqu'il examine les documents de voyage d'urgence aux points d'entrée et aux points de départ, et remédier aux vulnérabilités induites par des pratiques et des éléments de sécurité non systématiques. La Partie 8 contient également des spécifications sur l'utilisation de cachets numériques visibles sur les documents de voyage d'urgence.

**Partie 9 — Déploiement de l'identification biométrique et stockage électronique des données dans les DVLM-e**
Les spécifications définies dans la Partie 9 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 qui souhaitent émettre un DVLM électronique (DVLM-e) utilisable par tout État récepteur convenablement équipé pour lire, à partir de ce document, une quantité beaucoup plus grande de données concernant le DVLM-e lui-même et 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.

**Partie 10 — Structure de données logique (SDL) pour le stockage des données biométriques et d'autres données dans le circuit intégré (CI) sans contact**
La Partie 10 du Doc 9303 définit la structure de données logique (SDL) des DVLM-e requise pour l'interopérabilité mondiale. La technologie d'expansion de la capacité du CI sans contact utilisée dans un DVLM-e choisie par un État émetteur ou une organisation émettrice doit permettre l'accès aux données par les États récepteurs. La Partie 10 contient les spécifications relatives à l'organisation normalisée de ces données, ce qui exige l'identification de tous les éléments de données obligatoires et optionnels ainsi qu'un ordonnancement et/ou un groupement prescriptif des éléments de données, qui DOIT être suivi pour réaliser l'interopérabilité universelle permettant de lire les renseignements (éléments de données) enregistrés à l'aide de la technologie d'expansion de capacité qui peut être utilisée à titre facultatif sur un DVLM (DVLM-e).

**Partie 11 — Mécanismes de sécurité pour les DVLM**
La Partie 11 présente des spécifications destinées à permettre aux États et aux fournisseurs de mettre en œuvre des éléments de sécurité cryptographiques pour les DVLM électroniques (DVLM-e) avec accès en lecture seulement à un circuit intégré (CI) sans contact.

Les protocoles cryptographiques spécifiés visent à :

- empêcher l'écrémage des données contenues dans le CI sans contact ;
- empêcher l'interception illicite des communications entre le CI sans contact et le lecteur ;
- assurer l'authentification des données stockées dans le CI sans contact sur la base de l'infrastructure à clés publiques (ICP) décrite à la Partie 12 et assurer l'authentification du CI lui-même.

**Partie 12 — Infrastructure à clés publiques pour les DVLM**
La Partie 12 définit l'infrastructure à clés publiques (ICP) pour l'application DVLM-e. Elle spécifie les exigences/prescriptions pour les États émetteurs et les organisations émettrices, notamment la mise en place d'une autorité de certification (AC), qui émet les certificats et les CRL. Elle spécifie également les prescriptions applicables aux États récepteurs et à leurs systèmes d'inspection qui valident ces certificats et ces CRL.

**Partie 13 — Cachets numériques visibles pour les documents non électroniques**
La Partie 13 fournit les spécifications applicables au cachet numérique, qui permet de garantir l'authenticité et l'intégrité de documents non électroniques de façon relativement peu coûteuse mais hautement sécurisée à l'aide de la cryptographie asymétrique. Les renseignements figurant sur le document non électronique sont signés selon un procédé cryptographique, puis la signature est codée sous la forme d'un code à barres bidimensionnel et imprimée sur le document lui-même.

### 5.2 Relation entre le format des DVLM et les parties pertinentes du Doc 9303

Le Tableau 1-1 décrit les parties du Doc 9303 qui s'appliquent aux types (formats) particuliers de DVLM.

**Tableau 1-1. Format des DVLM et parties du Doc 9303**

| | Partie du Doc 9303 | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| DVLM de format TD3 (PLM) | √ | √ | √ | √ | | | | | | | | | |
| DVLM-e de format TD3 (PLM-e) | √ | √ | √ | √ | | | | | √ | √ | √ | √ | |
| DVOLM de format TD1 | √ | √ | √ | | √ | | | | | | | | |
| DVOLM-e de format TD1 | √ | √ | √ | | √ | | | | √ | √ | √ | √ | |
| DVOLM de format TD2 | √ | √ | √ | | | √ | | | | | | | |
| DVOLM-e de format TD2 | √ | √ | √ | | | √ | | | √ | √ | √ | √ | |
| VLM | √ | √ | √ | | | | √ | | | | | | √ |
| Document de voyage d'urgence | √ | √ | √ | | | | | √ | | | | | √ |

## 6. RÉFÉRENCES (NORMATIVES)

Certaines dispositions des normes internationales constituent, par référence, des dispositions du Doc 9303. En cas de différences entre les spécifications du Doc 9303 et les normes citées en référence, pour tenir compte des besoins spécifiques de la réalisation de documents de voyage lisibles par machine, y compris les visas lisibles par machine, les spécifications énoncées dans le présent document prévalent.

Annexe 9 Annexe 9 — *Facilitation* à la Convention relative à l'aviation civile internationale (Convention de Chicago).

RFC 2119 RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC2119, mars 1997.

**— FIN —**

ISBN 978-92-9265-526-6