OACI

Doc 9303

Documents de voyage lisibles à la machine

Septième édition, 2015

Partie 10 : Structure de données logique (SDL) pour le stockage des données biométriques et d'autres données dans le circuit intégré (CI) sans contact

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

Septième édition, 2015

Partie 10 : Structure de données logique (SDL) pour le stockage des données biométriques et d'autres données dans le circuit intégré (CI) sans contact

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.

Doc 9303, *Documents de voyage lisibles à la machine*
Partie 10 — *Structure de données logique (SDL) pour le stockage des données biométriques et d'autres données dans le circuit intégré (CI) sans contact*

ISBN 978-92-9258-023-0

RELEVÉ DES MODIFICATIONS

Doc 9303, Partie 10

DATE	Nº	SECTIONS OU PAGES CONCERNÉES	
31/8/16	1	Page 4	2. Exigences de la SDL — Correction du titre de la Figure 1.
		Pages 5, 20 à 28, 34, 42, 59 et 60, et Tableaux 23, 26 et 33	Changements multiples tirés de : Resolved Wellington, avril 2016. Commentaire sur le Doc 9303-10, 7e édition et diverses corrections éditoriales mineures.
		Page 24	5.2.5 Type de données signées pour SO_D V1 — Tableau 14 : remplacement de « Les États peuvent choisir d'inclure le certificat de signataire de document (C_{DS}) qui peut être utilisé pour vérifier la signature dans le champ signerInfos. » par « Les États DOIVENT inclure le certificat de signataire de document (C_{DS}) qui peut être utilisé pour vérifier la signature dans le champ signerInfos. »
		Appendice A	Suppression du paragraphe « A.6 Détails supplémentaires sur le document — EF.DG12 »
5/9/16	1	Appendice B	Inclusion des sections relatives au DVLM-e du profil d'application dans le nouvel Appendice B [Mise en place du CI sans contact dans un PLM-e (INFORMATIF)]
		Appendice C	Inclusion des sections relatives aux systèmes d'inspection du DVLM-e du profil d'application dans le nouvel Appendice C [Systèmes d'inspection (INFORMATIF)]

TABLE DES MATIÈRES

Page

1. PORTÉE

La septième édition du Doc 9303 est une restructuration des spécifications de l'OACI relatives aux documents de voyage lisibles à la machine (DVLM). Sans apporter de modifications substantielles aux spécifications elles-mêmes, cette nouvelle édition réorganise le contenu du Doc 9303 pour regrouper, dans des parties distinctes, les spécifications applicables aux documents de voyage officiels lisibles à la machine (DVOLM) de format 1 (TD1), aux DVOLM de format 2 (TD2), aux DVLM de format 3 (TD3) et aux visas. Ces différentes parties du document contiennent les spécifications générales, applicables à tous les DVLM, et les spécifications qui s'appliquent exclusivement à chaque format de DVLM.

La Partie 10 du Doc 9303 définit la structure de données logique (SDL) des DVLM-e requise pour l'interopérabilité mondiale ainsi que les spécifications de l'organisation des données sur le CI sans contact. Ceci exige l'identification de tous les éléments de données, obligatoires ou optionnels, et un ordonnancement et/ou un groupement prescriptif des éléments de données, qui DOIVENT être suivis afin de réaliser l'interopérabilité universelle de la lecture électronique des DVLM-e.

Le Doc 9303-10 énonce les spécifications qui permettront aux États d'utiliser les CI sans contact dans les DVLM-e. Cette partie définit tous les éléments de données obligatoires et optionnels, les structures de fichiers et les profils d'application des CI sans contact.

La Partie 10 devrait être lue en parallèle avec les parties suivantes du Doc 9303 :

- Partie 1 — *Introduction* ;
- Partie 3 — *Spécifications communes à tous les DVLM* ;
- Partie 4 — *Spécifications pour les passeports lisibles à la machine (PLM) et autres DVLM de format TD3* ;
- Partie 5 — *Spécifications pour les documents de voyage officiels lisibles à la machine (DVOLM) de format TD1* ;
- Partie 6 — *Spécifications pour les documents de voyage officiels lisibles à la machine (DVOLM) de format TD2* ;

et les parties applicables au CI sans contact :

- Partie 11 — *Mécanismes de sécurité pour les DVLM* ;
- Partie 12 — *Infrastructure à clés publiques pour les DVLM*.

2. EXIGENCES DE LA SDL

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.

L'OACI a établi que la SDL prédéfinie et normalisée doit remplir un certain nombre de conditions obligatoires :

- assurer une facilitation efficiente et optimale pour le détenteur légitime ;
- assurer la protection des éléments enregistrés dans la technologie optionnelle d'expansion de la capacité ;
- permettre l'interopérabilité mondiale des données des technologies d'expansion de la capacité sur la base de l'utilisation d'une SDL unique, commune à tous les DVLM-e ;
- répondre aux besoins divers des États émetteurs et des organisations émettrices en matière d'expansion optionnelle de la capacité ;
- offrir une capacité d'expansion au fur et à mesure de l'évolution des besoins des utilisateurs et des technologies disponibles ;
- permettre une diversité d'options en matière de protection des données ;
- utiliser dans toute la mesure possible les spécifications internationales existantes, en particulier les spécifications internationales émergentes pour une biométrie interopérable à l'échelle mondiale.

2.1 Sécurité

L'intégrité et l'authenticité des données sont nécessaires pour une interopérabilité mondiale de confiance.

Les groupes de données 1-16 inclus DOIVENT être protégés en écriture. Un hachage pour chaque groupe de données utilisé DOIT être stocké dans l'objet de sécurité du document ($EF.SO_D$).

Seul l'État émetteur ou l'organisation émettrice aura accès en écriture à ces groupes de données. Il n'y a donc aucune exigence en matière d'échanges et les méthodes employées pour réaliser la protection en écriture n'entrent pas dans le cadre des présentes spécifications.

2.2 Authenticité et intégrité des données

Un objet d'authenticité/intégrité est inclus pour permettre de confirmer l'authenticité et l'intégrité des éléments enregistrés. Chaque groupe de données DOIT être représenté dans cet objet d'authenticité/intégrité, qui est enregistré dans un fichier élémentaire distinct ($EF.SO_D$). Les éléments de confirmation de l'identité (p. ex., les gabarits biométriques) PEUVENT aussi être protégés individuellement, à la discrétion de l'État émetteur ou de l'organisation émettrice, en utilisant le cadre de formats d'échange biométriques communs (CBEFF), employé pour les groupes de données 2-4 des éléments d'identification codés et les éléments optionnels de sécurité des éléments biométriques supplémentaires définis dans le Doc 9303-12.

2.3 Ordonnancement de la SDL

Seul le schéma d'ordonnancement aléatoire DOIT être utilisé pour l'interopérabilité internationale.

2.3.1 Schéma d'ordonnancement aléatoire

Le schéma d'ordonnancement aléatoire permet l'enregistrement des groupes de données et des éléments de données en suivant un ordre aléatoire, compatible avec la fonctionnalité de la technologie optionnelle d'expansion de capacité qui permet l'extraction directe d'éléments de données spécifiques même s'ils sont enregistrés en désordre. Des éléments de données de longueur variable sont codés comme objets de données TLV spécifiés dans la notation ASN.1.

2.3.2 Représentation du fichier à accès aléatoire

La représentation du fichier à accès aléatoire a été définie sur la base des considérations et des présupposés suivants :

- Prendre en charge une large variété de mises en œuvre. La SDL comprend une grande variété d'éléments de données optionnels. Ces éléments de données sont inclus afin de faciliter l'authentification du DVLM-e et celle du détenteur légitime, et d'accélérer le traitement aux points de contrôle des documents et des personnes.
- La structure de données doit prendre en charge :
  - un ensemble limité ou étendu d'éléments de données ;
  - des occurrences multiples de certains éléments de données ;
  - une évolution continue des mises en œuvre spécifiques.
- Prendre en charge au moins un ensemble de données d'application.
- Permettre d'autres applications spécifiques nationales.
- Prendre en charge l'authentification active optionnelle du document en utilisant une paire de clés asymétriques mémorisée.
- Prendre en charge un accès rapide à certains éléments de données pour faciliter un traitement rapide du document
  - accès immédiat aux éléments de données nécessaires ;
  - accès direct aux gabarits et aux données biométriques.

2.3.3 Groupement des éléments de données

Des groupements d'éléments de données ajoutés par des États émetteurs ou des organisations réceptrices agréées peuvent être présents, ou non, dans la SDL. Plusieurs enregistrements d'éléments de données groupés, ajoutés par des États récepteurs ou des organisations réceptrices agréées, peuvent être présents dans la SDL.

La possibilité pour un État récepteur ou une organisation réceptrice agréée d'ajouter des données à la SDL n'est pas prise en charge dans la présente édition du Doc 9303.

La SDL est considérée comme une entité cohérente unique contenant le nombre de groupements d'éléments de données enregistrés dans la technologie optionnelle d'expansion de capacité au moment de la lecture par machine.

La SDL a été conçue avec une flexibilité suffisante pour pouvoir être appliquée à tous les types de DVLM-e. Dans les figures et les tableaux qui suivent, certains éléments de données sont applicables uniquement aux visas lisibles à la machine (VLM) ou aux passeports lisibles à la machine (PLM), ou exigent une présentation différente pour ces documents.

Des groupements logiques d'éléments de données apparentés ont été établis à l'intérieur de la SDL. Ces groupements logiques s'appellent groupes de données.

À chaque groupe de données est attribué un numéro de référence. La Figure 1 indique le numéro de référence attribué à chaque groupe de données, par exemple « DG2 » pour identifier le groupe de données 2, élément(s) d'identification codé(s) pour le visage du titulaire légitime du DVLM-e (c'est-à-dire éléments biométriques du visage).

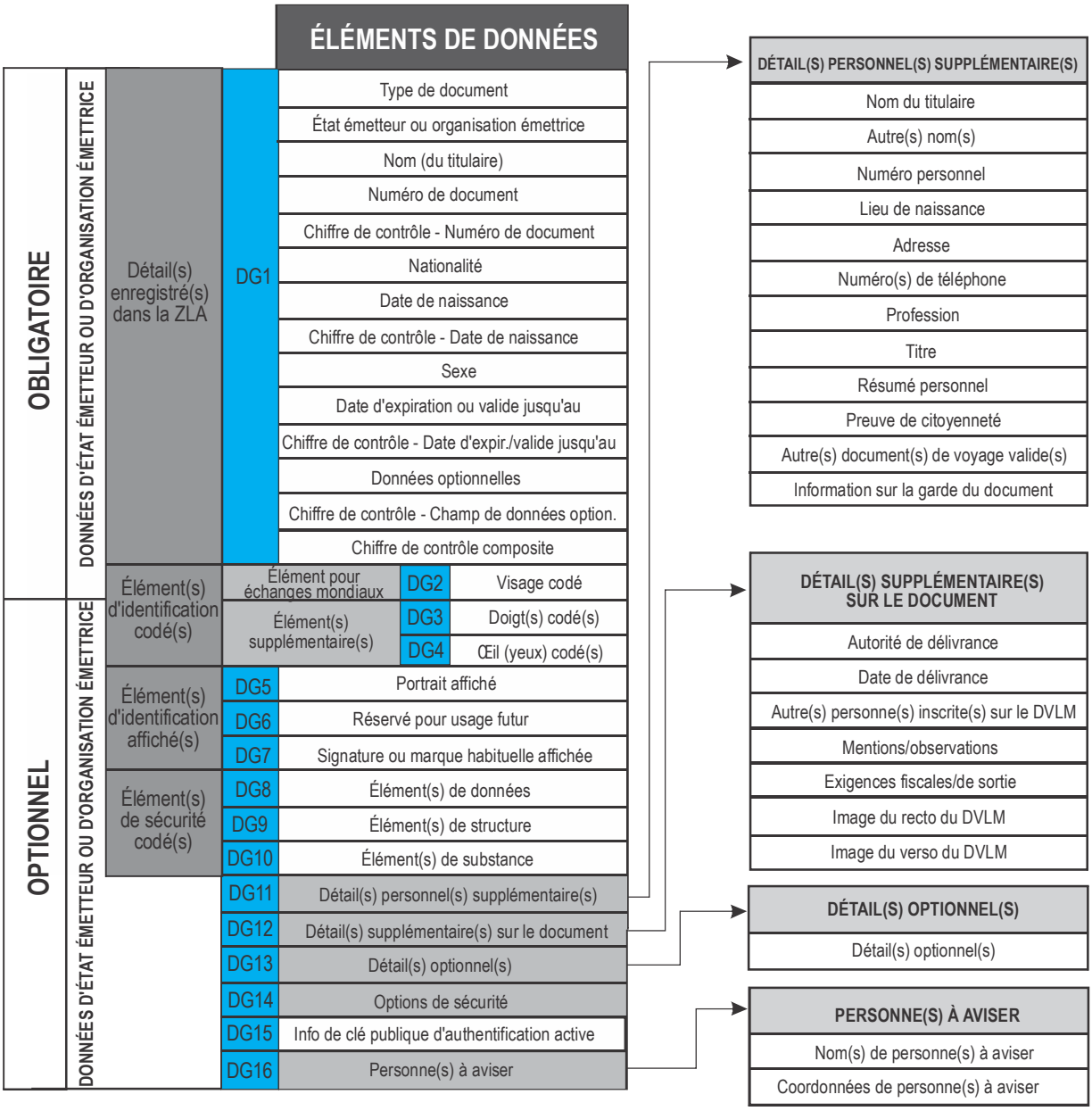

Figure 1. Numéros de référence de groupes de données assignés à la SDL

3. PROFIL D'APPLICATION DES CI SANS CONTACT

3.1 Exigences minimales d'interopérabilité

Les exigences minimales d'interopérabilité des DVLM-e de proximité à CI sans contact DOIVENT être les suivantes :

- ISO/IEC 14443-1, ISO/IEC 14443-2, ISO/IEC 14443-3 et ISO/IEC 14443-4, y compris tous les amendements et rectificatifs correspondants ;
- conformité avec les spécifications d'essai de l'ISO/IEC 10373-6, y compris tous les amendements et rectificatifs correspondants ;
- interface signal de type A ou type B ;
- prise en charge de la structure de fichier définie par la norme ISO/IEC 7816-4 pour des fichiers transparents de longueur variable ;
- prise en charge d'une ou de plusieurs applications et des commandes ISO/IEC 7816-4 appropriées spécifiées dans le Doc 9303 ;
- l'identifiant de famille d'application (AFI) est 0xE1 (DVLM-e). Le CRC_B de l'identifiant d'application (AID : 0xA0000002471001) DOIT être 0xF35E.

3.2 Caractéristiques électriques

La puissance radioélectrique et l'interface signal DOIVENT être celles qui sont définies dans la norme ISO/IEC 14443-2. Une vitesse de transmission minimale de 424 kilobits par seconde est conseillée. L'emploi de fonctions EMD spécifiées dans la norme ISO/IEC 14443-2 est OPTIONNEL.

3.3 Caractéristiques physiques

Il est recommandé que les dimensions de la zone de couplage d'antenne soient conformes à l'ISO/IEC 14443-1, Classe 1 (antenne pour format ID-1) seulement.

3.4 Capacité de stockage de données du CI sans contact

La capacité de stockage de données du CI est à la discrétion de l'État émetteur, mais DOIT être au minimum de 32 Ko. Cette capacité minimale est nécessaire pour stocker l'image faciale obligatoire (en général de 15 à 20 Ko), les renseignements figurant dans la ZLA et les éléments nécessaires pour sécuriser les données. Le stockage d'images supplémentaires du visage, d'empreintes digitales et/ou de l'iris peut exiger une augmentation significative de la capacité de stockage. Il n'est pas spécifié de capacité de données maximale pour le CI sans contact.

Lorsque l'infrastructure ICP d'un État n'est pas disponible pour signer les données du DVLM-e dans le cadre de la personnalisation et que l'émission des documents ne peut pas être retardée, il est RECOMMANDÉ que le CI sans contact du DVLM-e soit laissé vierge et soit verrouillé. Le DVLM-e DEVRAIT contenir une annotation appropriée à cet effet. Cette circonstance devrait être exceptionnelle.

3.5 Stockage d'autres données

Un État PEUT utiliser la capacité de stockage du CI sans contact dans un DVLM-e pour accroître la capacité de données lisibles par machine du DVLM-e au-delà de celle qui est définie pour l'interopérabilité mondiale afin, par exemple, de donner accès par lecture automatique à des renseignements issus de documents d'identité (p. ex., détails de l'acte de naissance), à des éléments de confirmation d'identité personnels stockés (éléments biométriques) et/ou à des détails permettant de vérifier l'authenticité du document.

3.6 Éléments de données minimaux à stocker dans la SDL

Les éléments de données obligatoires minimaux à stocker dans la SDL sur le CI sans contact DOIVENT être une reproduction des données de la ZLA dans le groupe de données 1 et l'image faciale du titulaire dans le groupe de données 2. De plus, dans un DVLM-e conforme, le CI DOIT contenir l'objet de sécurité du document ($EF.SO_D$) requis pour valider l'intégrité des données créées par l'émetteur. Ces éléments de données sont stockés dans le fichier dédié (DF), appelé application DVLM-e, et spécifié dans la SDL. L'objet de sécurité du document ($EF.SO_D$) est constitué des hachages des groupes de données utilisés.

3.7 Protocole d'initialisation, d'anticollision et de transmission conforme à l'ISO/IEC 14443

3.7.1 Protocole de transmission

Le DVLM-e DOIT prendre en charge le protocole de transmission semi-duplex défini dans la norme ISO/IEC 14443-4. Il DOIT prendre en charge le protocole de transmission de type A ou le protocole de transmission de type B.

3.7.2 Commande de demande et réponse à la demande

Le CI sans contact DOIT répondre à une commande de demande de type A (REQA) ou à une commande de demande de type B (REQB) par une réponse à la demande de type A (ATQA) ou une réponse à la demande de type B (ATQB), selon le cas.

3.7.3 Identificateur aléatoire ou identificateur fixe pour le CI sans contact

Le DVLM-e peut servir de « radiobalise » dans lequel le CI sans contact émet un identificateur unique (UID) pour le type A et un PUPI pour le type B lorsqu'il est initialement activé, ce qui pourrait permettre l'identification de l'autorité de délivrance. L'ISO/IEC 14443 permet le choix entre la présentation par le DVLM-e d'un identificateur fixe, attribué uniquement pour ce DVLM-e, ou d'un numéro aléatoire, qui est différent à chaque début du dialogue de communication. Certains États émetteurs préfèrent utiliser un numéro unique pour des raisons de sécurité ou pour toute autre raison. D'autres sont plus préoccupés par la confidentialité des données et la possibilité que les personnes soient suivies grâce aux identificateurs uniques de CI.

Le choix de l'une ou l'autre option ne réduit en rien l'interopérabilité vu que tout lecteur conforme à l'ISO/IEC 14443 comprendra les deux méthodes. L'emploi d'identificateurs aléatoires de CI est RECOMMANDÉ, mais les États PEUVENT choisir d'appliquer des UID uniques pour le type A ou des PUPI uniques pour le type B.

3.8 Jeu de commandes

Les commandes, formats et codes de retour sont tous définis dans l'ISO/IEC 7816-4. Le jeu de commandes minimum que DOIT prendre en charge le DVLM-e est le suivant :

SELECT (sélectionner) ;
READ BINARY (lire binaire).

Il est estimé que des commandes supplémentaires seront requises pour établir l'environnement de sécurité approprié et appliquer les dispositions de sécurité optionnelles identifiées dans le Doc 9303-11. La mise en œuvre des mécanismes spécifiés dans le Doc 9303-11 exige la prise en charge des commandes supplémentaires suivantes :

GET CHALLENGE (acquérir question) ;
EXTERNAL AUTHENTICATE (authentification externe) ;
INTERNAL AUTHENTICATE (authentification interne) ;
MANAGE SECURITY ENVIRONMENT (gestion de l'environnement de sécurité) ;
GENERAL AUTHENTICATE (authentification générale).

Le Doc 9303-11 donne des renseignements supplémentaires sur les protocoles de commande.

3.8.1 SELECT (sélectionner)

Le DVLM-e admet deux méthodes de sélection de structure : l'identificateur de fichier et l'identificateur EF court. Les lecteurs prennent en charge au moins une des deux méthodes. L'identificateur de fichier et l'identificateur de fichier court sont REQUIS pour le système d'exploitation du CI sans contact, mais OPTIONNELS pour le lecteur.

3.8.2 READ BINARY (lire binaire)

La prise en charge par un DVLM-e de la commande READ BINARY avec un octet INS impair est CONDITIONNELLE. Le DVLM-e DOIT prendre en charge cette variante de la commande s'il admet des groupes de données de 32 768 octets ou plus.

3.9 Formats de commande et options de paramétrage

3.9.1 Sélection d'application

Les applications doivent être sélectionnées soit par leur identificateur de fichier, soit par leur nom d'application. Après la sélection d'une application, il est possible d'accéder au fichier dans cette application.

Note.— Les noms d'application doivent être uniques. Il est donc possible de sélectionner une application en utilisant le nom d'application lorsque c'est nécessaire.

3.9.1.1 Sélection du fichier principal

Tableau 1. Sélection du fichier principal (MF)

CLA	INS	P1	P2	Lc	Données	Le
00	A4	00	0C	Vide	Vide	Vide

Note.— Il est RECOMMANDÉ de ne pas utiliser la commande de sélection du fichier principal (SELECT MF).

3.9.1.2 Sélection d'application par l'identificateur d'application

Une application DOIT être sélectionnée en employant le nom de DF. Les paramètres de la commande APDU sont indiqués ci-après :

Tableau 2. Commande de sélection d'application (SELECT Application)

CLA	INS	P1	P2	Lc	Données	Le
00	A4	04	0C	Var	AID	–

La première instruction de l'ISO/IEC 7816-4 est la sélection d'application (select application), avec le code 0x00A4040C07A0000002471001. Toutes les applications DVLM-e prennent en charge la commande de sélection d'application.

3.9.2 Sélection d'EF à l'aide de la commande SELECT (sélectionner)

Les fichiers doivent être sélectionnés par leur identificateur de fichier. Lorsque des fichiers sont sélectionnés par l'identificateur de fichier, il faut s'assurer que l'application dans laquelle sont stockés les fichiers a été préalablement sélectionnée.

Tableau 3. Commande de sélection de fichier (SELECT File)

CLA	INS	P1	P2	Lc	Données	Le
00	A4	02	0C	02	ID de fichier	–

Le DVLM-e DOIT prendre en charge la commande SELECT avec l'identificateur de fichier spécifié au Tableau 3. Le système d'inspection DOIT prendre en charge au moins une des deux méthodes suivantes :

- la commande SELECT avec l'identificateur de fichier spécifié au Tableau 3 ;
- la commande READ BINARY avec un octet INS pair et un identificateur de fichier court (SFI), comme il est spécifié au Tableau 5.

3.9.3 Lecture des données d'un EF (READ BINARY)

Il y a deux méthodes pour lire les données d'un DVLM-e : la sélection du fichier suivie de la lecture des données, ou la lecture directe des données en utilisant l'identificateur de fichier court. Vu que la prise en charge de l'identificateur de fichier court est REQUISE pour les DVLM-e, il est RECOMMANDÉ que les systèmes d'inspection utilisent l'identificateur de fichier court.

3.9.3.1 Lecture des données d'un fichier sélectionné (fichier transparent)

Tableau 4. Commande READ BINARY

CLA	INS	P1	P2	Lc	Données	Le
00	B0	Décalage MSB	Décalage LSB	–	–	MaxRet

3.9.3.2 Lecture de données en utilisant l'identificateur de fichier court (fichier transparent)

Tableau 5. Commande READ BINARY avec l'identificateur de fichier court

CLA	INS	P1	P2	Lc	Données	Le
00	B0	SFI	Décalage LSB	–	–	MaxRet

3.9.4 Prise en charge du Lc/Le étendu

Selon la taille des objets cryptographiques (p. ex., clés publiques, signatures), les APDU à champs de longueur étendue DOIVENT être employées pour envoyer ces données à la puce du DVLM. Voir l'ISO/IEC 7816-4.

3.9.4.1 Puces de DVLM

Pour les puces des DVLM, la prise en charge de la longueur étendue est CONDITIONNELLE. Si les algorithmes cryptographiques et les tailles de clés choisies par l'État émetteur exigent l'utilisation de la longueur étendue, les puces des DVLM DOIVENT prendre en charge la longueur étendue. La prise en charge de la longueur étendue par la puce du DVLM DOIT être indiquée dans l'ATR/ATS ou dans l'EF.ATR/INFO, comme il est spécifié dans l'ISO/IEC 7816-4.

3.9.4.2 Terminaux

Les terminaux DOIVENT prendre en charge la longueur étendue. Un terminal DEVRAIT vérifier si l'ATR/ATS ou l'EF.ATR/INFO de la puce du DVLM indique ou non la prise en charge de la longueur étendue avant d'utiliser cette option. Le terminal NE DOIT PAS utiliser la longueur étendue pour des APDU autres que les commandes indiquées ci-après, à moins que les tailles exactes des tampons entrée et sortie de la puce du DVLM ne soient explicitement indiquées dans l'ATR/ATS ou dans l'EF.ATR/INFO :

- MSE:Set KAT ;
- General Authenticate (authentification générale).

3.9.5 Chaînage des commandes

Le chaînage des commandes DOIT être utilisé pour la commande d'authentification générale (General Authenticate) afin de lier la séquence des commandes à l'exécution du protocole. Le chaînage des commandes NE DOIT PAS être employé à d'autres fins à moins que la puce ne l'indique clairement. Pour plus de renseignements sur le chaînage des commandes, voir l'ISO/IEC 7816-4.

3.9.6 EF de plus de 32 767 octets

La taille maximale d'un EF est normalement de 32 767 octets, mais certains CI sans contact admettent des fichiers plus grands. Une option de paramétrage et un format de commande READ BINARY (lire binaire) différents sont nécessaires pour accéder à la zone de données lorsque le décalage est supérieur à 32 767. Ce format de commande devrait être utilisé après détermination de la longueur du gabarit et de la nécessité d'accéder aux données dans la zone de données étendue. Par exemple, si la zone de données contient plusieurs objets de données biométriques, il n'est peut-être pas nécessaire de lire la zone de données en entier. Ce format de commande doit être utilisé lorsque le décalage pour la zone de données est supérieur à 32 767. Le décalage est placé dans le champ commande plutôt que dans les paramètres P1 et P2.

Tableau 6. Format des commandes pour les EF de plus de 32 767 octets

CLA	INS	P1	P2	Lc	Données	Le	Observations
00	B1	00	00	Var	Décalage de TLV codé	00	Lecture de fichiers de plus de 32 767 octets

Le champ longueur et le champ valeur de l'objet de données BER-TLV sont de longueur variable et peuvent être codés de différentes manières (voir l'ISO/IEC 7816-4 : « BER-TLV length fields »).

Pour des raisons de performance, la durée des communications entre le DVLM-e et le terminal doit être aussi courte que possible. Le champ de longueur et le champ de valeur de l'objet de données BER-TLV DEVRAIENT être aussi courts que possible. Cela s'applique non seulement aux objets de données décalés dans les commandes READ BINARY avec INS impair, mais aussi à tous les autres objets de données BER-TLV échangés entre le DVLM-e et le terminal.

Exemple pour décalage codé dans le champ de données :

- Décalage : 0x0001 est codé comme suit : Étiquette *(Tag)*=0x54 Longueur *(Length)*=0x01 Valeur *(Value)*=0x01 ;
- Décalage : 0xFFFF est codé comme suit : Étiquette =0x54 Longueur =0x02 Valeur =0xffff.

Les commandes READ BINARY suivantes doivent spécifier le décalage dans le champ données ; la commande finale READ BINARY devrait demander la zone de données restante.

L'octet Le contient soit 0x00, soit le nombre d'octets contenant des TL et V étendues.

Dans certains cas, les commandes READ BINARY B1 et B0 (traditionnelle) ne peuvent pas se chevaucher. Autrement dit, B0 ne devrait être utilisée que pour lire les 32 767 premiers octets et B1 pour lire les octets dépassant 32 K. Dans les autres cas, il pourrait y avoir un faible chevauchement de 256 octets autour du seuil de 32 767 octets pour permettre une transition plus fluide entre B0 et B1. Pour ce dernier groupe, la commande B1 pourrait être employée dès le début du fichier, c'est-à-dire avec un décalage commençant à 0 afin que la même commande puisse être utilisée pour lire la totalité du contenu. En ce qui concerne l'ISO/IEC 7816-4, aucune contrainte n'est spécifiée pour la valeur de décalage lorsque le bit 1 de l'INS est mis à 1 pour permettre une utilisation plus large.

L'octet INS impair ne doit pas être employé par le système d'inspection si la taille d'un EF est de 32 767 octets ou moins.

4. SPÉCIFICATIONS RELATIVES À LA STRUCTURE DE FICHIERS

Les informations contenues dans un DVLM-e sont stockées dans un système de fichiers défini dans l'ISO/IEC 7816-4. Le système de fichiers est organisé de façon hiérarchisée en fichiers dédiés (DF) et en fichiers élémentaires (EF). Les fichiers DF contiennent des fichiers EF ou d'autres fichiers DF. Un fichier principal (MF) optionnel peut être la racine du système de fichiers. Voir la Figure 2 pour une représentation graphique de la structure des fichiers.

Note.— La nécessité d'avoir un fichier principal dépend du choix des systèmes d'exploitation et des conditions optionnelles d'accès.

4.1 Sélection d'application — DF

Les DVLM-e DOIVENT prendre en charge au moins une application, comme suit :

- une application DOIT être constituée des données enregistrées par l'État émetteur ou l'organisation émettrice, des groupes de données 1 à 16 ainsi que de l'objet de sécurité du document ($EF.SO_D$) ;
- l'objet de sécurité du document ($EF.SO_D$) est constitué des valeurs de hachage définies dans le Doc 9303-11 et le Doc 9303-12 pour les groupes de données utilisés et il est nécessaire pour valider l'intégrité des données créées par l'émetteur et stockées dans l'application DVLM-e.

Les États émetteurs et les organisations émettrices peuvent aussi ajouter d'autres applications. La structure de fichiers DOIT prendre en charge des applications supplémentaires, mais les spécificités de ces applications n'entrent pas dans le cadre du Doc 9303.

L'application DVLM-e DOIT être sélectionnée en utilisant l'identification d'application (AID) comme nom de DF réservé. L'AID DOIT être constituée de l'identificateur d'application enregistré attribué par l'ISO selon la norme ISO/IEC 7816-5 et d'une extension d'identificateur d'application propriétaire (PIX) spécifiée dans le présent document :

- l'identificateur d'application enregistré est : 0xA000000247 ;
- l'application de données stockée de l'émetteur DOIT utiliser PIX = 0x1001 ;
- l'AID complète de l'application DVLM-e est : 'A0 00 00 02 47 10 01'.

4.2 Groupes de données

Chaque application peut comprendre plusieurs groupes de données, parfois appelés fichiers élémentaires (EF). L'application État émetteur ou organisation émettrice peut avoir jusqu'à 16 groupes de données. Le groupe de données 1 (DG1), la zone de lecture automatique (ZLA), et le groupe de données 2 (DG2), le visage codé, sont REQUIS. Tous les autres groupes de données sont OPTIONNELS. Tous les groupes de données sont sous forme de gabarits de données et ont des étiquettes ASN.1 individuelles.

Chaque groupe de données est constitué d'une série d'objets de données dans un gabarit. Chaque groupe de données DOIT être stocké dans un fichier élémentaire (EF) distinct. Chacun des objets de données du groupe de données peut être extrait directement après que la position relative au sein du fichier transparent aura été déterminée.

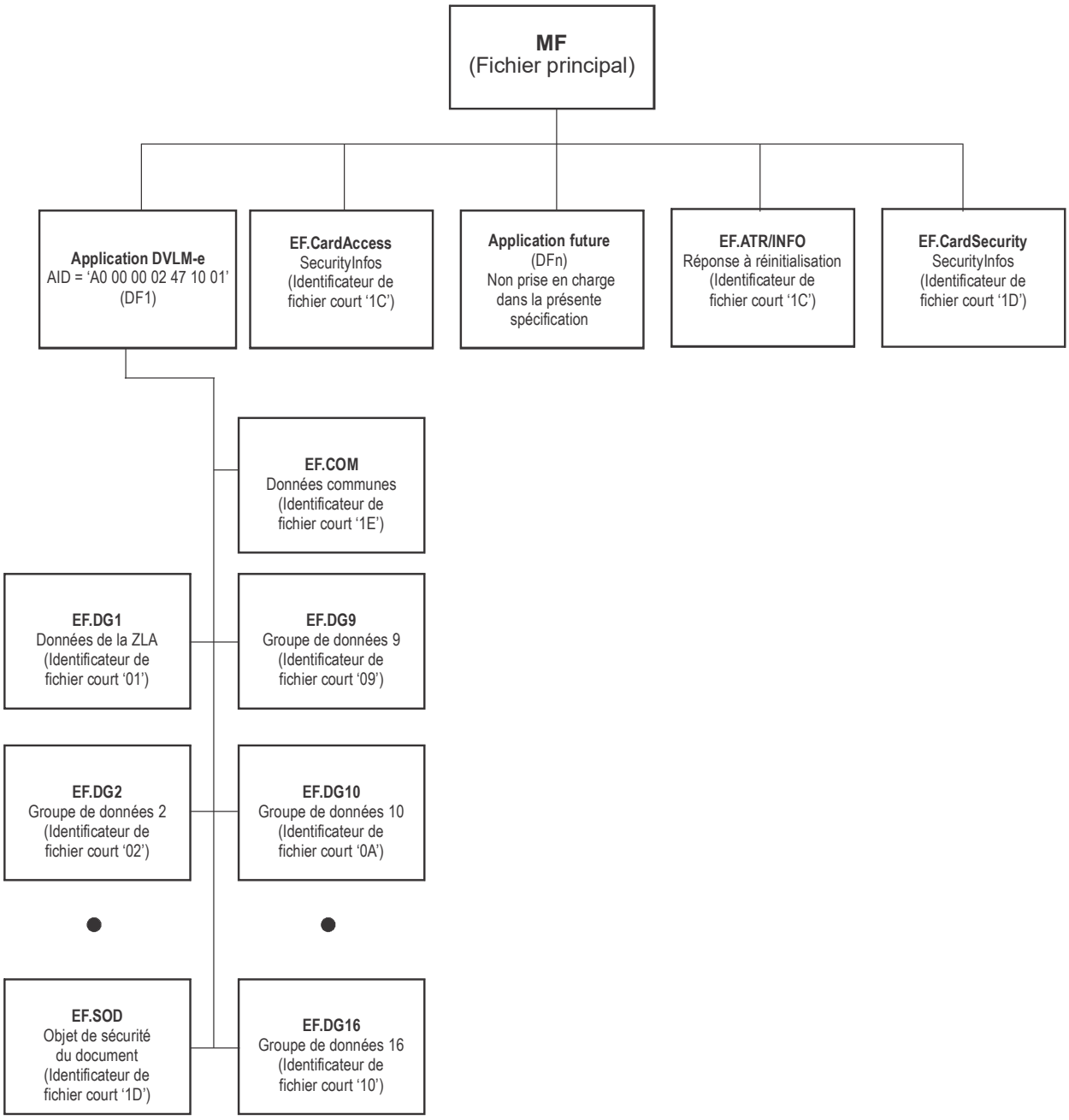

Figure 2. Schéma de la structure des fichiers

4.3 Règles de codage des éléments de données

Les fichiers contiennent les éléments de données sous forme d'objets de données dans un gabarit. La structure et le codage des objets de données sont définis dans les normes ISO/IEC 7816-4 et ISO/IEC 7816-6. Chaque objet de données a une étiquette d'identification, qui est spécifiée en codage hexadécimal (p. ex., 0x5A). Les étiquettes définies dans la présente section utilisent l'option de codage coexistante. Chaque objet de données a une étiquette unique, une longueur et une valeur. Les objets de données qui peuvent être présents dans un fichier sont identifiés comme

obligatoires (M, pour mandatory) ou optionnels (O). Des étiquettes communes à différents secteurs sont employées lorsque c'est possible. À noter que la définition et le format spécifiques de certaines étiquettes ont été modifiés pour les adapter à l'application DVLM-e. Exemples :

- L'étiquette 0x5A est définie comme numéro de document au lieu de numéro de compte primaire, et a le format F9N au lieu de V19N.
- L'étiquette 0x5F20, nom du titulaire de la carte, a été redéfinie comme « nom du titulaire », avec une longueur pouvant atteindre 39 caractères, codés selon le format spécifié dans le Doc 9303.
- L'étiquette 0x65 est définie comme portrait affiché au lieu de données relatives au titulaire de la carte.
- Au besoin, des étiquettes supplémentaires ont été définies dans la plage 0x5F01 à 0x5F7F.

4.3.1 Note normative sur le codage des éléments de données

Il y a un manque de correspondance entre les spécifications de la SDL (versions 1.7 et 1.8) et l'ISO/IEC 8825-1 (règles de codage BER/DER) ; la norme ISO/IEC 8825-1 spécifie que pour les étiquettes ayant un numéro entre 0 et 30 (inclusivement), le champ d'identification doit comprendre un seul octet codé comme suit :

- les bits 8 et 7 représentent la classe de l'étiquette ;
- le bit 6 prend la valeur 0 ou 1 ;
- les bits 5 à 1 représentent la valeur binaire du numéro de l'étiquette, le bit 5 étant le bit le plus significatif ;

ce qui signifie, par exemple, que l'étiquette du numéro de version de la spécification SDL devrait être 0x41 = 0x01000001b, où :

- 01 désigne la classe application (bits 8 et 7) ;
- 0 signifie qu'il s'agit d'une primitive (bit 6) ;
- 00001 est le code représentant le numéro d'étiquette 1 (bits 5 à 1).

Dans le Doc 9303, l'étiquette du numéro de version de la spécification SDL est 0x5F0 = 0x0101111100000001b, où :

- 01 désigne la classe application ;
- 0 signifie qu'il s'agit d'une primitive (non construite) ;
- 11111 signifie que le numéro d'étiquette est codé dans les octets qui suivent ;
- 0 signifie qu'il s'agit du dernier octet représentant le numéro d'étiquette ;
- 0000001 est le code représentant le numéro d'étiquette 1.

Ceci s'applique à toutes les étiquettes de 0 à 30 (inclusivement) :

- 0x5F01, 0x5F08, 0x5F09, 0x5F0A, 0x5F0B, 0x5F0C, 0x5F0E, 0x5F0F, 0x5F10, 0x5F11, 0x5F12, 0x5F13, 0x5F14, 0x5F15, 0x5F16, 0x5F17, 0x5F18, 0x5F19, 0x5F1A, 0x5F1B, 0x5F1C, 0x5F1D, 0x5F1E.

Les responsables de la mise en œuvre doivent être conscients de cette différence et suivre les spécifications données dans le Doc 9303. Il convient cependant de noter que :

- les mises en œuvre de DVLM-e ne peuvent pas être créées en utilisant un générateur fondé sur l'ASN.1 ;
- les analyseurs ASN.1/BER peuvent indiquer une erreur au lieu d'analyser correctement EF.COM ;
- le hachage sur EF.COM ne peut pas être recréé en décodant la structure de EF.COM et en la recodant ensuite.

4.3.2 Carte de présence d'éléments de données (DEPM)

Un concept de cartes de présence est employé avec un certain nombre de groupes de données qui contiennent une série d'éléments de données subordonnés, pouvant être inclus à la discrétion de l'État ou de l'organisation qui effectue l'enregistrement. Ces cartes de présence, dites cartes de présence d'éléments de données (DEPM) sont situées au début des groupes de données spécifiques qui permettent l'expansion optionnelle.

Une DEPM contient des informations qui permettront à un État récepteur ou une organisation réceptrice agréée de déterminer quels éléments de données sont présents dans le groupe de données.

La DEPM est constituée d'une liste d'étiquettes compatibles avec la convention pour l'identification des éléments de données enregistrés dans le(s) CI sans contact, où chaque étiquette indique si un certain élément de données est enregistré dans le groupe de données. Cette forme de DEPM est codée comme une liste d'étiquettes au sein du groupe de données pertinent.

4.3.3 Règles de codage de la longueur d'un objet de données TLV BER ASN.1

La forme de longueur ASN.1 définie dans l'ISO/IEC 8825-1 DOIT être utilisée.

Tableau 7. Règles de codage de longueur

Plage	Nombre d'octets	1er octet	2e octet	3e octet
0 à 127	1	valeur binaire	néant	néant
128 à 255	2	81	valeur binaire	néant
256 à 65 535	3	82	valeur binaire MSB LSB	

4.4 Étiquettes normatives utilisées dans le contexte de la SDL

Tableau 8. Étiquettes normatives

Étiquette	Définition	Lieu d'utilisation
02	Entier	Gabarits biométriques et d'affichages
5C	Liste d'étiquettes	EF.COM et de nombreux autres fichiers
5F01	Numéro de version de la SDL	EF.COM
5F08	Date de naissance (tronquée)	ZLA
5F09	Image compressée (ANSI/NIST-ITL 1-2000)	Doigt affiché
5F0A	Éléments de sécurité — Données codées	Éléments de sécurité (détails à définir)
5F0B	Éléments de sécurité — Structure	Éléments de sécurité (détails à définir)
5F0C	Éléments de sécurité	Éléments de sécurité (détails à définir)
5F0E	Nom complet, en caractères nationaux	Détails personnels supplémentaires
5F0F	Autres noms	Détails personnels supplémentaires
5F10	Numéro personnel	Détails personnels supplémentaires
5F11	Lieu de naissance	Détails personnels supplémentaires
5F12	Téléphone	Détails personnels supplémentaires
5F13	Profession	Détails personnels supplémentaires
5F14	Titre	Détails personnels supplémentaires
5F15	Résumé personnel	Détails personnels supplémentaires
5F16	Preuve de citoyenneté (image 10918)	Détails personnels supplémentaires
5F17	Numéros d'autres documents de voyage valides	Détails personnels supplémentaires
5F18	Information sur la garde du document	Détails personnels supplémentaires
5F19	Autorité de délivrance	Détails supplémentaires sur le document
5F1A	Autres personnes sur le document	Détails supplémentaires sur le document
5F1B	Mentions/observations	Détails supplémentaires sur le document
5F1C	Exigences fiscales/de sortie	Détails supplémentaires sur le document
5F1D	Image du recto du document	Détails supplémentaires sur le document

Étiquette	Définition	Lieu d'utilisation
5F1E	Image du verso du document	Détails supplémentaires sur le document
5F1F	Éléments de données de la ZLA	Objets de données de la ZLA
5F26	Date d'émission	Détails supplémentaires sur le document
5F2B	Date de naissance (8 chiffres)	Détails personnels supplémentaires
5F2E	Bloc de données biométriques	Données biométriques
5F36	Niveau de version Unicode	EF.COM
5F40	Gabarit d'image compressée	Portrait affiché
5F42	Adresse	Détails personnels supplémentaires
5F43	Gabarit d'image compressée	Signature ou marque affichée
5F50	Date d'enregistrement des données	Personne à aviser
5F51	Nom de la personne	Nom de la personne à aviser
5F52	Téléphone	N° de téléphone de la personne à aviser
5F53	Adresse	Adresse de la personne à aviser
5F55	Date et heure de personnalisation du document	Détails supplémentaires sur le document
5F56	Numéro de série du système de personnalisation	Détails supplémentaires sur le document
60	Éléments de données communs	EF.COM
61	Gabarit pour groupe de données de la ZLA	
63	Gabarit pour groupe de données d'éléments biométriques du doigt	
65	Gabarit pour image faciale numérisée	
67	Gabarit pour signature ou marque habituelle numérisée	
68	Gabarit pour sécurité assistée par machine — Données codées	
69	Gabarit pour sécurité assistée par machine — Structure	
6A	Gabarit pour sécurité assistée par machine — Substance	
6B	Gabarit pour détails personnels supplémentaires	
6C	Gabarit pour détails supplémentaires sur le document	

Étiquette	Définition	Lieu d'utilisation
6D	Détails optionnels	
6E	Réservé pour usage futur	
70	Personne à aviser	
75	Gabarit pour groupe de données d'éléments biométriques du visage	
76	Gabarit pour groupe de données d'éléments biométriques de l'iris (œil)	
77	EF.SO_D (EF pour objet de sécurité du document)	
7F2E	Bloc de données biométriques (chiffré)	
7F60	Gabarit d'informations biométriques	
7F61	Gabarit de groupe d'informations biométriques	
8x	Étiquettes spécifiques au contexte	CBEFF
90	Code de hachage chiffré	Code d'authenticité/intégrité
A0	Objets de données construits de façon spécifique au contexte	Détails personnels supplémentaires
Ax ou Bx	Gabarit se répétant, où x définit l'occurrence	En-tête biométrique

4.4.1 Étiquettes utiles pour traitement intermédiaire (informatif)

Tableau 9. Étiquettes intermédiaires

Étiquette	Définition	Lieu d'utilisation
53	Données optionnelles	Partie de la ZLA
59	Date d'expiration	Partie de la ZLA
5A	Numéro de document	Partie de la ZLA
5F02	Chiffre de contrôle — Données optionnelles (TD3 seulement)	Partie de la ZLA
5F03	Type de document	Partie de la ZLA
5F04	Chiffre de contrôle — Numéro de document	Partie de la ZLA
5F05	Chiffre de contrôle — Date de naissance	Partie de la ZLA

Étiquette	Définition	Lieu d'utilisation
5F06	Chiffre de contrôle — Date d'expiration	Partie de la ZLA
5F07	Chiffre de contrôle — Composite	Partie de la ZLA
5B	Nom de titulaire du document	Partie de la ZLA
5F28	État émetteur ou organisation émettrice	Partie de la ZLA
5F2B	Date de naissance	Partie de la ZLA
5F2C	Nationalité	Partie de la ZLA
5F35	Sexe	Partie de la ZLA
5F57	Date de naissance (6 chiffres)	Partie de la ZLA

4.4.1.1 Étiquettes réservées pour usage futur (normatif)

Tableau 10. Étiquettes réservées pour usage futur

Étiquette	Définition	Lieu d'utilisation
5F44	Pays d'entrée/de sortie	Dossiers de voyage
5F45	Date d'entrée/de sortie	Dossiers de voyage
5F46	Port d'entrée/de sortie	Dossiers de voyage
5F47	Indicateur d'entrée/de sortie	Dossiers de voyage
5F48	Longueur du séjour	Dossiers de voyage
5F49	Catégorie (classification)	Dossiers de voyage
5F4A	Référence de l'inspecteur	Dossiers de voyage
5F4B	Indicateur d'entrée/de sortie	Dossiers de voyage
71	Gabarit pour visas électroniques	
72	Gabarit pour dispositifs de passage de frontière	
73	Gabarit pour groupe de données de dossier de voyage	

4.5 Numéro de version de la SDL

Des mises à niveau futures de l'organisation de la SDL des DVLM-e ont été anticipées et seront publiées dans le cadre d'amendements des spécifications de l'OACI. Un numéro de version sera attribué à chaque mise à niveau, pour que les États récepteurs et les organisations réceptrices agréées puissent bien décoder toutes les versions de la SDL.

4.5.1 SDL version 1.7

La version 1.7 de la SDL DOIT mettre en œuvre l'objet de sécurité du document EF.SOD version V0 indiqué à la section 5 du présent document.

4.5.2 SDL version 1.8

La version 1.8 de la SDL DOIT mettre en œuvre l'objet de sécurité du document EF.SO_D version V1 indiqué à la section 5 du présent document.

5. FICHIERS ÉLÉMENTAIRES

5.1 Information sur l'en-tête et la présence de groupes de données EF.COM (REQUIS)

L'EF.COM est situé dans l'application DVLM-e (identificateur de fichier court = 0x1E) et contient les informations sur la version de la SDL, les informations sur la version Unicode et une liste des groupes de données présents pour l'application. L'application DVLM-e ne doit avoir qu'un seul fichier EF.COM qui contient les informations communes pour l'application.

Les éléments de données qui peuvent figurer dans ce gabarit sont :

Tableau 11. Étiquettes normatives EF.COM

Étiquette	**L**	**Valeur**		
60	Var	Information au niveau application		
		Étiquette	**L**	**Valeur**
		5F01	04	Numéro de version de la SDL en format aabb, où aa définit la version de SDL et bb définit le niveau d'actualisation.
		5F36	06	Numéro de version Unicode en format aabbcc, où aa définit la version principale, bb définit la version mineure et cc définit le niveau de diffusion.
		5C	Var	Liste d'étiquettes. Liste de tous les groupes de données présents.

Un en-tête et une carte de présence de groupes de données DOIVENT être inclus. L'en-tête DOIT contenir les informations suivantes, qui permettent à un État ou à une organisation réceptrice agréée de localiser et de décoder les divers groupes de données et éléments de données que contient le bloc de données enregistré par l'État émetteur ou l'organisation émettrice.

Dans la version 1.7 de la SDL, le fichier EF.COM n'est pas signé, ce qui entraîne une possibilité de manipulation non détectée de ses contenus. Il est par conséquent souhaitable que le numéro de version de la SDL fasse partie de l'information signée et soit ainsi protégé par authentification passive. Il est RECOMMANDÉ que les systèmes d'inspection qui dépendent de l'EF.COM soient modifiés pour utiliser dès que possible le SOD décrit dans la version 1.8.

5.1.1 Numéro de version de la SDL

Le numéro de version de la SDL définit la version du format de la SDL. Le format exact à utiliser pour stocker cette valeur est défini à la section 6 du présent document. Le format normalisé pour le numéro de version de SDL est « aabb », où :

- « aa » = nombre (01-99) identifant la version principale de la SDL (p. ex., additions significatives à la SDL) ;
- « bb » = nombre (01-99) identifiant la version mineure de la SDL.

5.1.2 Numéro de version Unicode

Le numéro de version Unicode identifie la méthode de codage employée lors de l'enregistrement de caractères alphabétiques, numériques ou spéciaux, y compris les caractères nationaux. Le format exact à utiliser pour stocker cette valeur est défini à la section 6 du présent document. Le format normalisé pour le numéro de version Unicode est « aabbcc », où :

- « aa » = nombre identifiant la version principale de la spécification Unicode (c'est-à-dire additions significatives à la spécification, publiées sous forme de livre) ;
- « bb » = nombre identifiant la version mineure de la spécification Unicode (c'est-à-dire additions de caractères ou modifications normatives plus significatives, publiées sous forme de rapport technique) ;
- « cc » = nombre identifiant la version actualisation de la spécification Unicode (c'est-à-dire tous les autres changements apportés à des parties normatives ou à des parties informatives importantes de la norme, qui pourraient modifier le comportement du programme. Ces changements figurent dans de nouveaux fichiers de base de données de caractères Unicode et dans une page de mise à jour.) Pour des raisons historiques, la numérotation au sein de chacun des champs (c'est-à-dire a, b, et c) n'est pas nécessairement consécutive.

Le jeu de caractères universels (UCS) DOIT être conforme à l'ISO/IEC 10646.

5.2 Objet de sécurité du document $EF.SO_D$ (REQUIS)

En plus des groupes de données de la SDL, le CI sans contact contient un objet de sécurité du document stocké dans $EF.SO_D$. Cet objet est signé numériquement par l'État émetteur et contient des valeurs de hachage du contenu de la SDL.

Tableau 12. Étiquettes $EF.SO_D$

Étiquette	L	Valeur
77	Var	Objet de sécurité du document

Il existe actuellement deux versions disponibles de l'objet de sécurité du document $EF.SO_D$. La version $EF.SO_D$ V0 ou la version $EF.SO_D$ V1 DOIT être mise en œuvre. Un seul $EF.SO_D$ est autorisé.

5.2.1 Objet de sécurité du document EF.SOD version V0 pour la SDL v1.7 (REQUIS)

L'objet de sécurité du document V0 pour la SDL v1.7 ne contient pas l'information sur la version de la SDL et la version Unicode :

```
LDSSecurityObject ::= SEQUENCE {
      version LDSSecurityObjectVersion,
      hashAlgorithm DigestAlgorithmIdentifier,
      dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
      DataGroupHash}
```

5.2.2 Type de données signées pour SOD V0

L'objet de sécurité du document est mis en œuvre sous forme de type de données signées (SignedData), comme il est spécifié dans RFC 3369. Tous les objets de sécurité DOIVENT être produits en format conforme aux règles de codage distinctives (DER) pour préserver l'intégrité des signatures qu'ils contiennent.

Note 1.— m REQUIS — le champ DOIT être présent.
Note 2.— x ne pas utiliser — le champ NE DEVRAIT PAS être rempli.
Note 3.— o optionnel — le champ PEUT être présent.
Note 4.— c choix — le contenu du champ est un choix entre différentes options.

Tableau 13. Type de données signées pour SO_D V0

Valeur		Observations
SignedData		
Version	m	Valeur = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	Objet de sécurité SDL id-icao-mrtd-security-ldsSecurityObject.
eContent	m	Le contenu codé d'un ldsSecurityObject.
Certificates	o	Les États peuvent choisir d'inclure le certificat de signataire de document (C_{DS}) qui peut être utilisé pour vérifier la signature dans le champ signerInfos.
Crls	x	Il est recommandé que les États n'utilisent pas ce champ.
signerInfos	m	Il est recommandé que les États ne fournissent que 1 signerInfo dans ce champ.
SignerInfo	m	
Version	m	La valeur de ce champ est dictée par le champ sid. Voir les règles concernant ce champ dans RFC 3369 (Doc 9303-12).
Sid	m	

Valeur		Observations
issuerandSerialNumber	c	Il est recommandé que les États prennent en charge ce champ plutôt que subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	Identificateur de l'algorithme utilisé pour produire la valeur de hachage sur encapsulatedContent et signedAttrs.
signedAttrs	m	Les États producteurs voudront peut-être inclure des attributs supplémentaires à insérer dans la signature, mais ces attributs n'ont pas à être traités par les États récepteurs, sauf pour vérifier la valeur de la signature.
signatureAlgorithm	m	L'identificateur de l'algorithme utilisé pour produire la valeur de la signature et les paramètres qui pourraient y être associés.
Signature	m	Résultat du processus de génération de signature.
unsignedAttrs	o	Les États producteurs voudront peut-être utiliser ce champ, mais son utilisation n'est pas recommandée et les États récepteurs peuvent ne pas en tenir compte.

5.2.3 Objet de sécurité du document de la SDL pour SO_D V0 — Profil ASN.1

```
LDSSecurityObjectV0 {joint-iso-itu-t (2) international(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Imports de RFC 3280 [PROFILE],
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) }

-- Constantes

ub-DataGroups INTEGER ::= 16

-- Identificateurs d'objet
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}
id-icao-mrtd-security-ldsSecurityObject   OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 1}

-- Objet de sécurité SDL

LDSSecurityObjectVersion ::= INTEGER {V0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier
```

```
LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash }

DataGroupHash ::= SEQUENCE {
   dataGroupNumber            ,
   dataGroupHashValue   OCTET STRING }

DataGroupNumber ::= INTEGER {
   dataGroup1            (1),
   dataGroup2            (2),
   dataGroup3            (3),
   dataGroup4            (4),
   dataGroup5            (5),
   dataGroup6            (6),
   dataGroup7            (7),
   dataGroup8            (8),
   dataGroup9            (9),
   dataGroup10          (10),
   dataGroup11          (11),
   dataGroup12          (12),
   dataGroup13          (13),
   dataGroup14          (14),
   dataGroup15          (15),
   dataGroup16          (16)}
END
```

Note 1.— Le champ valeur du groupe de données (`dataGroupValue`) contient le hachage calculé sur le contenu complet du fichier élémentaire (EF) de groupe de données, spécifié par le numéro du groupe de données (`dataGroupNumber`).

Note 2.— Les identificateurs d'algorithme de condensé (`DigestAlgorithmIdentifiers`) DOIVENT omettre les paramètres « `NULL` », tandis que l'identificateur d'algorithme de signature (`SignatureAlgorithmIdentifier`) (défini dans RFC 3447) DOIT inclure `NULL` comme paramètre si aucun paramètre n'est présent, même lorsque les algorithmes SHA2 sont utilisés conformément à RFC 5754. Les mises en œuvre DOIVENT accepter `DigestAlgorithmIdentifiers` avec les deux conditions, c'est-à-dire paramètres absents ou paramètres `NULL`.

5.2.4 Objet de sécurité du document EF.SO$_D$ V1 pour la SDL v1.8 (REQUIS)

L'objet de sécurité du document V1 pour la SDL v1.8 a été étendu au moyen d'un attribut signé, contenant l'information sur la version de la SDL et la version Unicode :

```
LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash,
   ldsVersionInfo OPTIONAL
   -- Si elle est présente, la version DOIT être V1 }
```

```
LDSVersionInfo ::= SEQUENCE {
ldsVersion PrintableString,
   unicodeVersion PrintableString }
```

Note .— Les identificateurs d'algorithme de condensé (`DigestAlgorithmIdentifiers`) DOIVENT omettre les paramètres « `NULL` », tandis que l'identificateur d'algorithme de signature (`SignatureAlgorithmIdentifier`) (défini dans RFC 3447) DOIT inclure `NULL` comme paramètre si aucun paramètre n'est présent, même lorsque les algorithmes SHA2 sont utilisés conformément à RFC 5754. Les mises en œuvre DOIVENT accepter `DigestAlgorithmIdentifiers` avec les deux conditions, c'est-à-dire paramètres absents ou paramètres `NULL`.

5.2.5 Type de données signées pour SO_D V1

L'objet de sécurité du document est mis en œuvre sous forme de type de données signées (SignedData), comme il est spécifié dans RFC 3369, *Cryptographic Message Syntax (CMS),* août 2002. Tous les objets de sécurité DOIVENT être produits en format conforme aux règles de codage distinctives (DER) pour préserver l'intégrité des signatures qu'ils contiennent.

Note 1.— m REQUIS — le champ DOIT être présent.
Note 2.— x ne pas utiliser — le champ NE DEVRAIT PAS être rempli.
Note 3.— o optionnel — le champ PEUT être présent.
Note 4.— c choix — le contenu du champ est un choix entre différentes options.

Tableau 14. Type de données signées pour SO_D V1

Valeur		Commentaires
SignedData		
Version	m	Valeur = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	Objet de sécurité SDL id-icao-mrtd-security-ldsSecurityObject.
eContent	m	Le contenu codé d'un ldsSecurityObject.
Certificates	m	Les États DOIVENT inclure le certificat de signataire de document (C_{DS}) qui peut être utilisé pour vérifier la signature dans le champ signerInfos.
Crls	x	Il est recommandé que les États n'utilisent pas ce champ.
signerInfos	m	Il est recommandé que les États ne fournissent que 1 signerInfo dans ce champ.
SignerInfo	m	
Version	m	La valeur de ce champ est dictée par le champ sid. Voir les règles concernant ce champ dans RFC 3369 (Doc 9303-12).

Valeur		Commentaires
Sid	m	
issuerandSerialNumber	c	Il est recommandé que les États prennent en charge ce champ plutôt que subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	Identificateur de l'algorithme utilisé pour produire la valeur de hachage sur encapsulatedContent et signedAttrs.
signedAttrs	m	Les États producteurs voudront peut-être inclure des attributs supplémentaires à insérer dans la signature, mais ces attributs n'ont pas à être traités par les États récepteurs, sauf pour vérifier la valeur de la signature.
signatureAlgorithm	m	L'identificateur de l'algorithme utilisé pour produire la valeur de la signature et les paramètres qui pourraient y être associés.
Signature	m	Résultat du processus de génération de signature.
unsignedAttrs	o	Les États producteurs voudront peut-être utiliser ce champ, mais son utilisation n'est pas recommandée et les États récepteurs peuvent ne pas en tenir compte.

5.2.6 Objet de sécurité du document de la SDL pour SO_D V1 — Profil ASN.1

```
LDSSecurityObjectV1 { joint-iso-itu-t(2) international(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Imports de RFC 3280 [PROFILE]
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) }

-- Constantes

ub-DataGroups INTEGER ::= 16

-- Identificateurs d'objet

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

```
-- Objet de sécurité SDL

LDSSecurityObjectVersion ::= INTEGER {V0(0), V1(1)
-- Si LDSSecurityObjectVersion est V1, ldsVersionInfo DOIT être présent }

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash,
   ldsVersionInfo OPTIONAL
   -- Si elle est présente, la version DOIT être V1 }

DataGroupHash ::= SEQUENCE {
   dataGroupNumber,
   dataGroupHashValue   OCTET STRING }

DataGroupNumber ::= INTEGER {
   dataGroup1            (1),
   dataGroup2            (2),
   dataGroup3            (3),
   dataGroup4            (4),
   dataGroup5            (5),
   dataGroup6            (6),
   dataGroup7            (7),
   dataGroup8            (8),
   dataGroup9            (9),
   dataGroup10          (10),
   dataGroup11          (11),
   dataGroup12          (12),
   dataGroup13          (13),
   dataGroup14          (14),
   dataGroup15          (15),
   dataGroup16          (16)}

LDSVersionInfo ::= SEQUENCE {
   ldsVersion PRINTABLE STRING
   unicodeVersion PRINTABLE STRING }
END
```

Note 1.— Le champ valeur du groupe de données (`dataGroupValue`) contient le hachage calculé sur le contenu complet du fichier élémentaire (EF) de groupe de données, spécifié par le numéro du groupe de données (`dataGroupNumber`).

Note 2.— Les identificateurs d'algorithme de condensé (`DigestAlgorithmIdentifiers`) DOIVENT omettre les paramètres « `NULL` », tandis que l'identificateur d'algorithme de signature (`SignatureAlgorithmIdentifier`) (défini dans RFC 3447) DOIT inclure `NULL` comme paramètre si aucun paramètre n'est présent, même lorsque les algorithmes SHA2 sont utilisés conformément à RFC 5754. Les mises en œuvre DOIVENT accepter `DigestAlgorithmIdentifier`s avec les deux conditions, c'est-à-dire paramètres absents ou paramètres `NULL`.

5.3 Fichier EF.CardAccess (CONDITIONNEL)

Le fichier EF.CardAccess est un fichier élémentaire transparent contenu dans le fichier principal et il est requis à titre conditionnel si la commande de contrôle d'accès PACE optionnelle définie dans le Doc 9303-11 est invoquée. Le Doc 9303-11 donne une description complète des `protocoles SecurityInfos` pour PACE.

5.3.1 Stockage dans le CI sans contact

Le fichier CardAccess contenu dans le fichier principal est REQUIS si PACE est pris en charge par la puce du DVLM et DOIT contenir les informations de sécurité (SecurityInfos) suivantes requises pour PACE :

- `PACEInfo`;
- `PACEDomainParameterInfo`.

Tableau 15. Stockage du fichier EF.CardAccess dans le CI

Nom de fichier	**EF.CardAccess**
ID de fichier	0x011C
ID de fichier court	0x1C
Accès en lecture	TOUJOURS
Accès en écriture	JAMAIS
Taille	Variable
Contenu	DER encoded `SecurityInfos`. Pour les protocoles spécifiques, voir le Doc 9303-11.

5.4 Fichier EF.CardSecurity (CONDITIONNEL)

Le fichier EF.CardSecurity est un fichier élémentaire transparent contenu dans le fichier principal et il est REQUIS à titre conditionnel si le protocole PACE optionnel avec mappage d'authentification de puce défini dans le Doc 9303-11 est invoqué. Le Doc 9303-11 donne une description complète de SecurityInfos pour PACE avec mappage d'authentification de puce.

5.4.1 Stockage dans le CI sans contact

Le fichier CardSecurity contenu dans le fichier principal est REQUIS si PACE avec mappage d'authentification de puce est pris en charge par la puce du DVLM et DOIT contenir les informations de sécurité (`SecurityInfos`) suivantes :

- les informations ChipAuthenticationPublicKeyInfo requises pour PACE-CAM ;
- les informations de sécurité `SecurityInfos` contenues dans CardAccess.

Tableau 16. Stockage du fichier EF.CardSecurity sur le CI

Nom de fichier	**EF.CardSecurity**
ID de fichier	0x011D
ID de fichier court	0x1D
Accès en lecture	PACE
Accès en écriture	JAMAIS
Taille	Variable
Contenu	`SignedData` codées DER résumées. Voir le Doc 9303-11. Données signées ID.

6. ÉLÉMENTS DE DONNÉES FORMANT LES GROUPES DE DONNÉES 1 À 16

Les groupes de données 1 (DG1) à 16 (DG16) sont constitués chacun d'un certain nombre d'éléments de données, obligatoires, optionnels ou conditionnels. L'ordre spécifié des éléments de données dans le groupe de données DOIT être suivi. Chaque groupe de données DOIT être stocké dans un EF transparent. L'adressage des EF DOIT être fait au moyen de l'identificateur de fichier court, comme le montre le Tableau 16. Les EF DOIVENT avoir pour ces fichiers des noms de fichier qui DOIVENT être conformes au nombre n, EF.DGn, où n est le numéro du groupe de données.

Tableau 17. Éléments de données, obligatoires ou optionnels, qui se combinent pour former la structure des groupes de données 1 (DG1) à 16 (DG16)

Groupe de données	**Nom du fichier EF**	**Identificateur de fichier court**	**FID**	**Étiquette**
Commun	EF.COM	1E	01 1E	60
DG1	EF.DG1	01	01 01	61
DG2	EF.DG2	02	01 02	75
DG3	EF.DG3	03	01 03	63
DG4	EF.DG4	04	01 04	76
DG5	EF.DG5	05	01 05	65
DG6	EF.DG6	06	01 06	66
DG7	EF.DG7	07	01 07	67
DG8	EF.DG8	08	01 08	68
DG9	EF.DG9	09	01 09	69

Groupe de données	Nom du fichier EF	Identificateur de fichier court	FID	Étiquette
DG10	EF.DG10	0A	01 0A	6A
DG11	EF.DG11	0B	01 0B	6B
DG12	EF.DG12	0C	01 0C	6C
DG13	EF.DG13	0D	01 0D	6D
DG14	EF.DG14	0E	01 0E	6E
DG15	EF.DG15	0F	01 0F	6F
DG16	EF.DG16	10	01 10	70
Objet de sécurité du document	$EF.SO_D$	1D	01 1D	77
Commun	EF.CARDACCESS	1C	01 1C	
Commun	EF.ATR/INFO			
Commun	EF.CardSecurity	1D	01 1D	

6.1 GROUPE DE DONNÉES 1 — Informations de la zone de lecture automatique (REQUIS)

Les éléments de données du groupe de données 1 (DG1) sont destinés à représenter le contenu entier de la zone de lecture automatique (ZLA), qu'il s'agisse de données réelles ou de caractères de remplissage. Les détails sur la mise en œuvre de la ZLA dépendent du type de DVLM-e (format TD1,TD2 ou TD3).

Cet élément de données contient les renseignements de la ZLA REQUIS pour le document dans le gabarit 0x61. Le gabarit contient un objet de données, la ZLA dans l'objet de données 0x5F1F. L'objet de données ZLA est un élément de données composite, identique aux informations de la ZLA imprimées en ROC-B sur le document.

Tableau 18. Étiquettes du groupe de données 1

Étiquette	L	Valeur		
61	Var			
		Étiquette	**L**	**Valeur**
		5F1F	F	L'objet de données ZLA est un élément de données composite. (REQUIS) (L'élément de données contient tous les champs obligatoires depuis le type de document jusqu'au chiffre de contrôle composite.)

6.1.1 GROUPE DE DONNÉES 1 — Éléments de données du EF.DG1 pour un DVLM-e de format TD1

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 1 (DG1). Les exigences de stockage, d'ordonnancement et de codage du DG1 devraient être exactement les mêmes que celles de la ZLA imprimée, décrites dans le Doc 9303-3 et le Doc 9303-5. Les éléments de données et leur format dans chaque zone du groupe de données pour le format TD1 figurent dans le tableau suivant :

Note.— A = caractère alphabétique [A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], F = champ de longueur fixe.

Tableau 19. Éléments de données pour le format TD1

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage
01	M	Code de document	2	F	A,S
02	M	État émetteur ou organisation émettrice	3	F	A,S
03	M	Numéro de document (neuf caractères les plus significatifs)	9	F	A,N,S
04	M	Chiffre de contrôle — Numéro du document ou caractère de remplissage (<) indiquant que le numéro du document dépasse neuf caractères	1	F	N,S
05	M	Données optionnelles et/ou, dans le cas d'un numéro de document dépassant neuf caractères, caractères les moins significatifs du numéro de document plus le chiffre de contrôle du numéro de document et plus le caractère de remplissage	15	F	A,N,S
06	M	Date de naissance	6	F	N,S
07	M	Chiffre de contrôle — Date de naissance	1	F	N
08	M	Sexe	1	F	A,S
09	M	Date d'expiration	6	F	N
10	M	Chiffre de contrôle — Date d'expiration	1	F	N
11	M	Nationalité	3	F	A,S
12	M	Données optionnelles	11	F	A,N,S
13	M	Chiffre de contrôle composite	1	F	N
14	M	Nom du titulaire	30	F	A,N,S

6.1.2 GROUPE DE DONNÉES 1 — Éléments de données du EF.DG1 pour un DVLM-e de format TD2

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 1 (DG1). Les exigences de stockage, d'ordonnancement et de codage du DG1 devraient être exactement les mêmes que celles de la ZLA imprimée, décrites dans le Doc 9303-3 et le Doc 9303-6. Les éléments de données et leur format dans chaque zone du groupe de données pour le format TD2 figurent dans le tableau suivant :

Note.— A = caractère alphabétique [A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], F = champ de longueur fixe.

Tableau 20. Éléments de données pour le format TD2

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage
01	M	Code de document	2	F	A,S
02	M	État émetteur ou organisation émettrice	3	F	A,S
03	M	Nom du titulaire	31	F	A,N,S
04	M	Numéro de document (neuf caractères principaux)	9	F	A,N,S
05	M	Chiffre de contrôle	1	F	N,S
06	M	Nationalité	3	F	A,S
07	M	Date de naissance	6	F	N,S
08	M	Chiffre de contrôle	1	F	N
09	M	Sexe	1	F	A,S
10	M	Date d'expiration	6	F	N
11	M	Chiffre de contrôle	1	F	N
12	M	Données optionnelles plus caractère de remplissage	7	F	A,N,S
13	M	Chiffre de contrôle composite — ligne 2 de la ZLA	1	F	N

6.1.3 GROUPE DE DONNÉES 1 — Éléments de données du EF.DG1 pour un DVLM-e de format TD3

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 1 (DG1). Les exigences de stockage, d'ordonnancement et de codage du DG1 devraient être exactement les mêmes que celles de la ZLA imprimée, décrites dans le Doc 9303-3 et le Doc 9303-4. Les éléments de données et leur format dans chaque zone du groupe de données pour le format TD3 figurent dans le tableau suivant :

Note.— A = caractère alphabétique [A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], F = champ de longueur fixe.

Tableau 21. Éléments de données pour le format TD3

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage
01	M	Code de document	2	F	A,S
02	M	État émetteur ou organisation émettrice	3	F	A,S
03	M	Nom du titulaire	39	F	A,S
04	M	Numéro de document	9	F	A,N,S
05	M	Chiffre de contrôle — Numéro de document	1	F	N,S
06	M	Nationalité	3	F	A,S
07	M	Date de naissance	6	F	N,S
08	M	Chiffre de contrôle — Date de naissance	1	F	N
09	M	Sexe	1	F	A,S
10	M	Date d'expiration	6	F	N
11	M	Chiffre de contrôle — Date d'expiration ou valide jusqu'au	1	F	N
12	M	Données optionnelles	14	F	A,N,S
13	M	Chiffre de contrôle	1	F	N
14	M	Chiffre de contrôle composite	1	F	N

6.2 GROUPE DE DONNÉES 2 — Éléments d'identification codés — Visage (REQUIS)

Le groupe de données 2 (DG2) représente l'élément biométrique interopérable mondialement pour la confirmation d'identité assistée par ordinateur avec les DVLM, qui DOIT être une image du visage du titulaire, comme entrée dans un système de reconnaissance faciale. S'il existe plus d'un enregistrement, le plus récent codage interopérable internationalement doit être la première entrée.

Tableau 22. Étiquettes du groupe de données 2

Étiquette	L	Valeur
75	Var	Voir codage biométrique du EF.DG2

6.2.1 Codage biométrique du EF.DG2

Le DG2 DOIT utiliser le gabarit de groupe de gabarits d'informations biométriques (BIT), avec BIT imbriqués, spécifié dans la norme ISO/IEC 7816-11, qui prévoit la possibilité de stocker plusieurs gabarits biométriques et qui est en harmonie avec le CBEFF. Le sous-en-tête biométrique définit le type d'élément biométrique qui est présent et l'élément biométrique spécifique. L'option imbriquée de l'ISO/IEC 7816-11 doit toujours être utilisée, même pour les codages d'un seul gabarit biométrique. Ce dernier cas est indiqué par une numérotation n = 1.

Chaque gabarit biométrique imbriqué a la structure suivante :

Tableau 23. Groupe de données 2 — Étiquettes de codage biométrique

Étiquette	L	Valeur				
7F61	Var	Gabarit de groupe d'informations biométriques				
		Étiquette	**L**	**Valeur**		
		02	01	Entier — Nombre d'instances de ce type d'élément biométrique		
		7F60	Var	1er gabarit d'informations biométriques		
			Étiquette	**L**		
			A1	Var	Gabarit d'en-tête biométrique (BHT)	
				Étiq.	**L**	**Valeur**
				80	02	Version d'en-tête OACI 0101 (optionnel) — Version du format d'en-tête d'usager CBEFF
				81	01-03	Type d'élément biométrique (optionnel)
				82	01	Sous-type d'élément biométrique optionnel pour DG2
				83	07	Date et heure de création (optionnel)

Étiquette	L	Valeur				
				85	08	Période de validité (de – à –) (optionnel)
				86	02	Créateur des données de référence biométriques (PID) (optionnel)
				87	02	Propriétaire de format (REQUIS)
				88	02	Type de format (REQUIS)
			5F2E ou 7F2E	Var	Données biométriques (codées selon le propriétaire de format), aussi appelé bloc de données biométriques (BDB).	

L'OID par défaut de CBEFF est utilisé. L'objet de données OID (étiquette 0x06) juste au-dessous du gabarit d'informations biométriques (BIT, étiquette 0x7F60) spécifié dans l'ISO/IEC 7816-11 n'est pas inclus dans cette structure. De même, l'autorité d'attribution des étiquettes n'est pas spécifiée dans la structure.

Pour faciliter l'interopérabilité, le premier élément biométrique enregistré dans chaque groupe de données DOIT être codé conformément à l'ISO /IEC 19794-5.

6.2.2 GROUPE DE DONNÉES 2 — Éléments de données du EF.DG2

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 2 (DG2). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 24. Éléments de données du DG2

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^{bre} d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M	Nombre de codages biométriques du visage enregistrés	1	F	N	1 à 9 identifiant le nombre de codages uniques de données sur le visage.
02	M	En-tête		Var	A,N	L'élément de données peut se reproduire, comme défini par DE 01.
03	M	Codage(s) de données biométriques du visage		Var	A,N,S,B	L'élément de données peut se reproduire, comme défini par DE 01.

6.3 GROUPE DE DONNÉES 3 — Élément d'identification supplémentaire — Doigt(s) (OPTIONNEL)

L'OACI reconnaît que les États membres peuvent choisir d'utiliser la reconnaissance d'une empreinte digitale comme technologie biométrique supplémentaire pour la confirmation d'identité assistée par ordinateur ; cet élément DOIT être codé comme groupe de données 3 (DG3).

Tableau 25. Étiquettes du groupe de données 3

Étiquette	L	Valeur
63	Var	Voir codage biométrique du EF.DG3

6.3.1 Codage biométrique du EF.DG3

Le DG3 DOIT utiliser le gabarit de groupe de gabarits d'informations biométriques (BIT), avec BIT imbriqués, spécifié dans la norme ISO/IEC 7816-11, qui prévoit la possibilité de stocker plusieurs gabarits biométriques et qui est en harmonie avec le CBEFF. Le sous-en-tête biométrique définit le type d'élément biométrique qui est présent et l'élément biométrique spécifique. L'option imbriquée de l'ISO/IEC 7816-11 DOIT être utilisée, même pour les codages d'un seul gabarit biométrique. Ce dernier cas est indiqué par une numérotation n = 1. Le nombre d'instances dans DG3 peut être « 0...n ».

Chaque gabarit biométrique imbriqué a la structure suivante :

Tableau 26. Étiquettes imbriquées du groupe de données 3

Étiquette	L	Valeur				
7F61	Var	Gabarit de groupe d'informations biométriques				
		Étiquette	**L**	**Valeur**		
		02	01	Entier — Nombre d'instances de ce type d'élément biométrique		
		7F60	Var	1er gabarit d'informations biométriques		
			Étiquette	**L**		
			A1	Var	Gabarit d'en-tête biométrique (BHT)	
				Étiq.	**L**	**Valeur**
				80	02	Version d'en-tête OACI 0101 (optionnel) — Version du format d'en-tête d'usager CBEFF
				81	01-03	Type d'élément biométrique (optionnel)
				82	01	Sous-type d'élément biométrique REQUIS pour DG3
				83	07	Date et heure de création (optionnel)
				85	08	Période de validité (de – à –) (optionnel)
				86	04	Créateur des données de référence biométriques (PID) (optionnel)
				87	02	Propriétaire de format (REQUIS)
				88	02	Type de format (REQUIS)
			5F2E ou 7F2E	Var	Données biométriques (codées selon le propriétaire de format), aussi appelé bloc de données biométriques (BDB).	
		Étiquette	**L**			
		7F60	X	2e gabarit d'informations biométriques		
			Étiquette	**L**		
			A1	Var	Gabarit d'en-tête biométrique (BHT)	
				Étiq.	**L**	**Valeur**
				80	02	Version d'en-tête OACI 0101 (optionnel) — Version du format d'en-tête d'usager CBEFF
				81	01-03	Type d'élément biométrique (optionnel)
				82	01	Sous-type d'élément biométrique REQUIS pour DG3

Étiquette	L	Valeur				
				83	07	Date et heure de création (optionnel)
				85	08	Période de validité (de – à –) (optionnel)
				86	04	Créateur des données de référence biométriques (PID) (optionnel)
				87	02	Propriétaire de format (REQUIS)
				88	02	Type de format (REQUIS)
			5F2E ou 7F2E	Var	Données biométriques (codées selon le propriétaire de format), aussi appelé bloc de données biométriques (BDB).	

L'OID par défaut de CBEFF est utilisé. L'objet de données OID (étiquette 0x06) juste au-dessous du gabarit d'informations biométriques (BIT, étiquette 0x7F60) spécifié dans la norme ISO/IEC 7816-11 n'est pas inclus dans cette structure. De même, l'autorité d'attribution des étiquettes n'est pas spécifiée dans la structure.

Pour faciliter l'interopérabilité, le premier élément biométrique enregistré dans chaque groupe de données DOIT être codé conformément à l'ISO /IEC 19794-5.

6.3.2 GROUPE DE DONNÉES 3 — Éléments de données du EF.DG3

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 3 (DG3). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 27. Éléments de données du DG3

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^{bre} d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M [si les éléments codés de doigt(s) sont enregistrés]	Nombre de codages biométriques de doigt(s) enregistrés	1	F	N	0 à n identifiant le nombre de codages uniques de données sur le(s) doigt(s).
02	M [si les éléments codés de doigt(s) sont enregistrés]	En-tête		Var	B	L'élément de données peut se reproduire, comme défini par DE 01.
03	M [si les éléments codés de doigt(s) sont enregistrés]	Codage(s) de données biométriques de doigt(s)		Var	A,N,S,B	L'élément de données peut se reproduire, comme défini par DE 01.

6.3.2.1 Codage du sous-type d'élément biométrique

Les étiquettes de gabarit d'en-tête biométrique et les valeurs qui leur ont été assignées sont le minimum que DOIT prendre en charge chaque mise en œuvre, comme l'indique le tableau ci-après. Chacun des gabarits d'informations biométriques a la structure suivante :

Tableau 28. Schéma de codage de sous-éléments biométriques pour le codage de sous-éléments : CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Sous-type d'élément biométrique
0	0	0	0	0	0	0	0	Aucune information donnée
						0	1	Droit
						1	0	Gauche
			0	0	0			Aucune signification
			0	0	1			Pouce
			0	1	0			Index
			0	1	1			Majeur
			1	0	0			Annulaire
			1	0	1			Auriculaire
X	X	X						Réservé pour usage futur

6.3.2.2 Codage de zéro instance

Les États qui émettent des DVLM-e sans empreintes digitales NE DEVRAIENT PAS remplir le DG3. Le groupe de données DG3 de cette structure a l'inconvénient de produire un hachage DG3 statique dans le SO_D pour tous les DVLM-e dont les éléments biométriques ne sont pas présents ou remplis au moment de l'émission du DVLM-e mais dont le DG3 est déclaré. Pour des fins d'interopérabilité, les États qui utilisent les empreintes digitales dans leurs DVLM-e DOIVENT stocker un gabarit de groupe d'informations biométriques vide lorsque les empreintes digitales ne sont pas disponibles au moment de l'émission du DVLM-e. Dans ce cas, le compteur de gabarit indique une valeur de 0x00.

Il est RECOMMANDÉ d'ajouter une étiquette 0x53 avec contenu défini par l'émetteur (p. ex., un nombre aléatoire).

Tableau 29. Codage de zéro instance

Étiquette	L	Valeur				
63	Var	Élément SDL				
		Étiquette	**L**	**Valeur**		
		7F 61	03	Gabarit de groupe d'informations biométriques		
			02	01	00	Indique qu'aucun gabarit d'informations biométriques n'est enregistré dans ce groupe de données.
		53	Var	Contenu défini par l'émetteur (p. ex., un nombre aléatoire).		

6.3.2.3 Codage d'une instance

Lorsqu'une seule empreinte digitale est disponible, l'instance unique DOIT être codée de la manière suivante (exemple pour DG3 : empreinte digitale) :

Tableau 30. Codage d'une instance

Étiquette	L	Valeur						
63	aa	Élément SDL, *aa* étant la longueur totale de tout le contenu des données SDL.						
		Étiq.	**L**	**Valeur**				
		7F 61	bb	Gabarit de groupe d'informations biométriques, *bb* étant la longueur totale de tout le contenu du gabarit de groupe.				
			02	01	01	Indique le nombre total d'empreintes digitales enregistrées dans les gabarits d'informations biométriques qui suivent.		
			7F 60	cc	1er gabarit d'informations biométriques, *cc* étant la longueur totale de tout le BIT.			
				A1	dd	Gabarit d'en-tête biométrique, *dd* étant la longueur totale de BHT.		
					81	01	08	Type d'élément biométrique : « empreinte digitale »
					82	01	0A	Sous-type d'élément biométrique : « index gauche »
					87	02	01 01	JTC 1 SC 37
					88	02	00 07	Type de format : ISO/IEC 19794-4
					À noter que le BHT peut contenir des éléments optionnels additionnels. L'empreinte digitale peut bien sûr être celle d'un doigt gauche ou droit, selon l'image disponible.			
				5F 2E	ee	Bloc de données biométriques, *ee* étant la longueur totale de la structure ISO/IEC 19794-4 codée. Le bloc de données biométriques DOIT contenir exactement une image d'empreinte digitale.		

6.3.2.4 Codage de plus d'une instance

Pour assurer l'interopérabilité, chaque élément DOIT être enregistré dans un gabarit d'informations biométriques particulier. La position de l'élément DOIT être spécifiée dans le sous-type d'élément biométrique CBEFF, si cette information est disponible. Le tableau suivant contient un exemple détaillé du codage CBEFF d'un élément DG3 interopérable avec deux images d'empreintes digitales :

Tableau 31. Codage de plus d'une instance

Étiquette	**L**	**Valeur**						
63	aa	Élément SDL, *aa* étant la longueur totale de tout le contenu de données SDL.						
		Étiq.	**L**	**Valeur**				
		7F 61	bb	Gabarit de groupe d'informations biométriques, *bb* étant la longueur totale de tout le contenu du gabarit de groupe.				
			02	01	02	Indique le nombre total d'empreintes digitales enregistrées dans les gabarits d'informations biométriques qui suivent.		
			7F 60	cc	1er gabarit d'informations biométriques, *cc* étant la longueur totale de tout le BIT.			
				A1	Dd	Gabarit d'en-tête biométrique, *dd* étant la longueur totale de BHT.		
					81	01	08	Type d'élément biométrique : « empreinte digitale »
					82	01	0A	Sous-type d'élément biométrique : « index gauche »
					87	02	01 01	Propriétaire de format : JTC 1 SC 37
					88	02	00 07	Type de format : ISO/IEC 19794-4
					À noter que le BHT peut contenir des éléments optionnels additionnels. Il est possible aussi que l'ordre des empreintes digitales (gauche/droit) soit différent.			
				5F 2E	ee	Bloc de données biométriques, *ee* étant la longueur totale de la structure ISO/IEC 19794-4 codée. Le bloc de données biométriques DOIT contenir exactement une image d'empreinte digitale.		
			7F 60	ff	2e gabarit d'informations biométriques, *ff* étant la longueur totale de tout le BIT.			

Étiquette	L	Valeur						
				A1	Gg	Gabarit d'en-tête biométrique, *gg* étant la longueur totale de BHT.		
					81	01	08	Type d'élément biométrique : « empreinte digitale »
					82	01	09	Sous-type d'élément biométrique : « index droit »
					87	02	01 01	Propriétaire de format : JTC 1 SC 37
					88	02	00 07	Type de format : ISO/IEC 19794-4
					À noter que le BHT peut contenir des éléments optionnels additionnels. Il est possible aussi que l'ordre des empreintes digitales (gauche/droit) soit différent.			
				5F 2E	Hh	Bloc de données biométriques, *hh* étant la longueur totale de la structure ISO/IEC 19794-4 codée. Le bloc de données biométriques DOIT contenir exactement une image d'empreinte digitale.		

6.4 GROUPE DE DONNÉES 4 — Élément d'identification supplémentaire — Iris (OPTIONNEL)

L'OACI reconnaît que les États membres peuvent choisir d'utiliser la reconnaissance de l'iris comme technologie biométrique supplémentaire pour la confirmation d'identité assistée par ordinateur ; cet élément DOIT être codé comme groupe de données 4 (DG4).

Tableau 32. Étiquettes du groupe de données 4

Étiquette	L	Valeur
76	Var	Voir codage biométrique du EF.DG4

6.4.1 Codage biométrique du EF.DG4

Le DG4 DOIT utiliser le gabarit de groupe de gabarits d'informations biométriques (BIT), avec BIT imbriqués, spécifié dans la norme ISO/IEC 7816-11, qui prévoit la possibilité de stocker plusieurs gabarits biométriques et qui est en harmonie avec le CBEFF. Le sous-en-tête biométrique définit le type d'élément biométrique qui est présent et l'élément biométrique spécifique. L'option imbriquée de l'ISO/IEC 7816-11 DOIT être utilisée, même pour les codages d'un seul gabarit biométrique. Ce dernier cas est indiqué par une numérotation n = 1. Le nombre d'instances dans DG4 peut être « 0...n ».

Chaque gabarit biométrique imbriqué a la structure suivante :

Tableau 33. Étiquettes imbriquées du groupe de données 4

Étiquette	L	Valeur				
7F61	Var	Gabarit de groupe d'informations biométriques				
		Étiq.	**L**	**Valeur**		
		02	1	Entier — Nombre d'instances de ce type d'élément biométrique		
		7F60	Var	1er gabarit d'informations biométriques		
			Étiq.	**L**		
			A	Var	Gabarit d'en-tête biométrique (BHT)	
				Étiq.	**L**	**Valeur**
				80	02	Version d'en-tête OACI 0101 (optionnel) — Version du format d'en-tête d'usager CBEFF
				81	01-03	Type d'élément biométrique (optionnel)
				82	01	Sous-type d'élément biométrique REQUIS pour DG4
				83	07	Date et heure de création (optionnel)
				85	08	Période de validité (de – à –) (optionnel)
				86	04	Créateur des données de référence biométriques (PID) (optionnel)
				87	02	Propriétaire de format (REQUIS)
				88	02	Type de format (REQUIS)
			5F2E ou 7F2E	Var	Données biométriques (codées selon le propriétaire de format), aussi appelé bloc de données biométriques (BDB).	
		Étiq.	**L**			
		7F60	Var	2e gabarit d'informations biométriques		
			Étiq.	**L**		
			A1	Var	Gabarit d'en-tête biométrique (BHT)	
				Étiq.	**L**	**Valeur**
				80	02	Version d'en-tête OACI 0101 (optionnel) — Version du format d'en-tête d'usager CBEFF
				81	01-03	Type d'élément biométrique (optionnel)

Étiquette	L	Valeur				
				82	01	Sous-type d'élément biométrique REQUIS pour DG4
				83	07	Date et heure de création (optionnel)
				85	08	Période de validité (de – à –) (optionnel)
				86	04	Créateur des données de référence biométriques (PID) (optionnel)
				87	02	Propriétaire de format (REQUIS)
				88	02	Type de format (REQUIS)
			5F2E ou 7F2E	Var	Données biométriques (codées selon le propriétaire de format), aussi appelé bloc de données biométriques (BDB).	

L'OID par défaut de CBEFF est utilisé. L'objet de données OID (étiquette 0x06) juste au-dessous du gabarit d'informations biométriques (BIT, étiquette 0x7F60) spécifié dans la norme ISO/IEC 7816-11 n'est pas inclus dans cette structure. De même, l'autorité d'attribution des étiquettes n'est pas spécifiée dans la structure.

Pour faciliter l'interopérabilité, le premier élément biométrique enregistré dans chaque groupe de données DOIT être codé conformément à l'ISO /IEC 19794-5.

6.4.2 GROUPE DE DONNÉES 4 — Éléments de données du EF.DG4

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 4 (DG4). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 34. Éléments de données du DG4

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^{bre} d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M [si l'élément codé de l'œil (des yeux) est inclus]	Nombre de codages biométriques de l'œil enregistrés	1	F	N	1 à 9 identifiant le nombre de codages uniques de données sur l'œil (les yeux).
02	M [si l'élément codé de l'œil (des yeux) est inclus]	En-tête		Var	B	L'élément de données peut se reproduire, comme défini par DE 01.

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^{bre} d'octets	Fixe ou variable	Type de codage	Exigences de codage
03	M [si l'élément codé de l'œil (des yeux) est inclus]	Codage(s) de données biométriques de l'œil (des yeux)		Var	A,N,S,B	L'élément de données peut se reproduire, comme défini par DE 01.

6.4.2.1 Codage du sous-type d'élément biométrique

Les étiquettes de gabarit d'en-tête biométrique et les valeurs qui leur ont été assignées sont le minimum que DOIT prendre en charge chaque mise en œuvre, comme l'indique le tableau ci-après. Chacun des gabarits d'informations biométriques a la structure suivante :

Tableau 35. Schéma de codage de sous-éléments biométriques pour le codage de sous-éléments : CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Sous-type d'élément biométrique
0	0	0	0	0	0	0	0	Aucune information donnée
						0	1	Droit
						1	0	Gauche
			0	0	0			Réservé pour usage futur
			0	0	1			Réservé pour usage futur
			0	1	0			Réservé pour usage futur
			0	1	1			Réservé pour usage futur
			1	0	0			Réservé pour usage futur
			1	0	1			Réservé pour usage futur
X	X	X						Réservé pour usage futur

6.4.2.2 Codage de zéro instance

Les États qui émettent des DVLM-e sans iris NE DEVRAIENT PAS remplir le DG4. Le groupe de données DG4 de cette structure a l'inconvénient de produire un hachage DG4 statique dans le SO_D pour tous les DVLM-e dont les éléments biométriques ne sont pas présents ou remplis au moment de l'émission du DVLM-e mais dont le DG4 est déclaré. Pour des fins d'interopérabilité, les États qui utilisent les iris dans leurs DVLM-e DOIVENT stocker un gabarit de groupe d'informations biométriques vide lorsque les iris ne sont pas disponibles au moment de l'émission du DVLM-e. Dans ce cas, le compteur de gabarit indique une valeur de 0x00.

Il est RECOMMANDÉ d'ajouter une étiquette 0x53 avec contenu défini par l'émetteur (p. ex., un nombre aléatoire).

Tableau 36. Codage de zéro instance

Étiquette	L	Valeur				
76	Var	Élément SDL				
		Étiq.	**L**	**Valeur**		
		7F 61	03	Gabarit de groupe d'informations biométriques		
			02	01	00	Indique qu'aucun gabarit d'informations biométriques n'est enregistré dans ce groupe de données.
		53	Var	Contenu défini par l'émetteur (p. ex., un nombre aléatoire).		

6.4.2.3 Codage d'une instance

Lorsqu'un seul iris est disponible, l'instance unique DOIT être codée.

6.4.2.4 Codage de plus d'une instance

Pour assurer l'interopérabilité, chaque élément DOIT être enregistré dans un gabarit d'informations biométriques particulier. La position de l'élément DOIT être spécifiée dans le sous-type d'élément biométrique CBEFF, si cette information est disponible.

6.5 GROUPE DE DONNÉES 5 — Portrait affiché (OPTIONNEL)

Les éléments de données attribués au groupe de données 5 (DG5) DOIVENT être les suivants :

Tableau 37. Étiquettes du groupe de données 5

Étiquette	L	Valeur		
65	Var			
		Étiquette	**L**	**Valeur**
		02	Var	Nombre d'instances de ce type d'image affichée (REQUIS dans le premier gabarit. Non utilisé dans les gabarits suivants.)
		5F40	Var	Portrait affiché

Les propriétaires de format suivants sont reconnus pour le type spécifié d'image affichée :

Tableau 38. Formats DG5

Image affichée	Propriétaire du format
Image faciale affichée	ISO/IEC 10918, option JFIF

6.5.1 GROUPE DE DONNÉES 5 — Éléments de données du EF.DG5 (optionnel)

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 5 (DG5). Les éléments de données et leur format au sein du DG5 DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 39. Éléments de données du DG5

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^{bre} d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M (si le portrait affiché est enregistré)	Nombre de portraits affichés enregistrés	1	F	N	1 à 9 identifiant le nombre d'enregistrements uniques du portrait affiché.
02	M (si le portrait affiché est enregistré)	Représentation(s) du portrait affiché		Var	A,N	L'élément de données peut se reproduire, comme défini par DE 01.
	M (si le portrait affiché est enregistré)	Nombre d'octets dans la représentation du portrait	5	F	N	00001 à X9, indiquant le nombre d'octets dans la représentation du portrait affiché suivant immédiatement.
	M (si le portrait affiché est enregistré)	Représentation du portrait affiché		Var	A,N,S,B	Formaté selon l'ISO/IEC 10918-1 ou l'ISO/IEC 15444.

Note.— L'élément de données 02 DOIT être codé comme il est défini dans l'ISO/IEC 10918, en utilisant l'option JFIF, ou l'ISO/IEC 15444 en employant le système de codage d'images JPEG 2000.

6.6 GROUPE DE DONNÉES 6 — Réservé pour usage futur

Les éléments de données attribués au groupe de données 6 (DG6) DOIVENT être les suivants :

Tableau 40. Étiquettes du groupe de données 6

Étiquette	L	Valeur
66	Var	

6.6.1 GROUPE DE DONNÉES 6 — Éléments de données du EF.DG6

Les éléments de données attribués au groupe de données 6 (DG6) sont réservés pour usage futur.

6.7 GROUPE DE DONNÉES 7 — Signature ou marque habituelle affichée (OPTIONNEL)

Les éléments de données attribués au groupe de données 7 (DG7) DOIVENT être les suivants :

Tableau 41. Étiquettes du groupe de données 7

Étiquette	L	Valeur		
67	Var			
		Étiquette	**L**	**Valeur**
		02	Var	Nombre d'instances de ce type d'image affichée (REQUIS dans le premier gabarit. Non utilisé dans les gabarits suivants.)
		5F43	Var	Signature affichée

Les propriétaires de format suivants sont reconnus pour le type spécifié d'image affichée :

Tableau 42. Formats DG7

Image affichée	Propriétaire du format
Signature ou marque habituelle affichée	ISO/IEC 10918, option JFIF

6.7.1 GROUPE DE DONNÉES 7 — Éléments de données du EF.DG7 (optionnel)

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 7 (DG7). Les éléments de données et leur format dans chaque groupe de données 7 DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 43. Éléments de données du DG7

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^{bre} d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M (si la signature ou la marque habituelle affichée est enregistrée)	Nombre de signatures ou de marques habituelles affichées	1	F	N	1 à 9 identifiant le nombre d'enregistrements uniques de la signature ou de la marque habituelle affichée.
02	M (si la signature ou la marque habituelle affichée est enregistrée)	Représentation de la signature ou de la marque habituelle affichée		Var	A,N,S,B	L'élément de données peut se reproduire, comme défini par DE 01. Formaté selon l'ISO/IEC 10918-1 ou l'ISO/IEC 15444.

Note.— L'élément de données 02 DOIT être codé comme il est défini dans l'ISO/IEC 10918, en utilisant l'option JFIF, ou dans l'ISO/IEC 15444 en employant le système de codage d'images JPEG 2000.

6.8 GROUPE DE DONNÉES 8 — Élément(s) de données (OPTIONNEL)

Ce groupe de données reste à définir. D'ici là, il est disponible pour usage propriétaire temporaire. Ces éléments de données pourraient utiliser une structure similaire à celle qui est employée pour les gabarits biométriques, la vérification d'éléments de sécurité assistée par machine et le(s) détail(s) codé(s). Les éléments de données se combinant pour former le groupe de données 8 (GD8) DOIVENT être les suivants :

Tableau 44. Étiquettes du groupe de données 8

Étiquette	L	Valeur		
68	Var	À définir		
		Étiquette	**L**	**Valeur**
		02	1	Entier — Nombre d'instances de ce type de gabarit (REQUIS dans le premier gabarit. Non utilisé dans les gabarits suivants.)
			Var	Gabarit d'en-tête. Détails à définir.

6.8.1 GROUPE DE DONNÉES 8 — Éléments de données du EF.DG8

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 8 (DG8). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 45. Éléments de données du DG8

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^bre^ d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M (si cet élément codé est utilisé)	Nombre d'éléments de données	1	F	N	1 à 9 identifiant le nombre de codages uniques de l'élément ou des éléments de données (englobe DE 02 à DE 04).
02	M (si cet élément codé est utilisé)	En-tête (à définir)	1			Détails de l'en-tête à définir.
03	M (si cet élément codé est utilisé)	Information sur les éléments de données	999 Max	Var	A,N,S,B	Format défini à la discrétion de l'État émetteur ou de l'organisation émettrice.

6.9 GROUPE DE DONNÉES 9 — Élément(s) de structure (OPTIONNEL)

Ce groupe de données reste à définir. D'ici là, il est disponible pour usage propriétaire temporaire. Ces éléments de données pourraient utiliser une structure similaire à celle qui est employée pour les gabarits biométriques. Les éléments de données se combinant pour former le groupe de données 9 (GD9) DOIVENT être les suivants :

Tableau 46. Étiquettes du groupe de données 9

Étiquette	L	Valeur		
69	Var	À définir		
		Étiquette	**L**	**Valeur**
		02	01	Entier — Nombre d'instances de ce type de gabarit (REQUIS dans le premier gabarit. Non utilisé dans les gabarits suivants.)
			X	Gabarit d'en-tête. Détails à définir.

6.9.1 GROUPE DE DONNÉES 9 — Éléments de données du EF.DG9

Les éléments de données du groupe de données 9 (DG9) et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant *:*

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 47. Éléments de données du DG9

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^bre d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M (si cet élément codé est utilisé)	Nombre d'éléments de structure	1	F	N	1 à 9 identifiant le nombre de codages uniques de l'élément ou des éléments de structure (englobe DE 02 à DE 04).
02	M (si cet élément codé est utilisé)	En-tête (à définir)			N	Détails de l'en-tête à définir.
03	M (si cet élément codé est utilisé)	Information sur les éléments de structure		Var		

6.10 GROUPE DE DONNÉES 10 — Élément(s) de substance (OPTIONNEL)

Ce groupe de données reste à définir. D'ici là, il est disponible pour usage propriétaire temporaire. Ces éléments de données pourraient utiliser une structure similaire à celle qui est employée pour les gabarits biométriques. Les éléments de données se combinant pour former le groupe de données 10 (GD10) DOIVENT être les suivants :

Tableau 48. Étiquettes du groupe de données 10

Étiquette	L	Valeur		
6A	Var			
		Étiquette	**L**	**Valeur**
		02	01	Entier — Nombre d'instances de ce type de gabarit (REQUIS dans le premier gabarit. Non utilisé dans les gabarits suivants.)
			Var	À définir.

6.10.1 GROUPE DE DONNÉES 10 — Éléments de données du EF.DG10

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 10 (DG10). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 49. Éléments de données du DG10

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^bre^ d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M (si cet élément codé est utilisé)	Nombre d'éléments de substance enregistrés	1	F	N	1 à 9 identifiant le nombre de codages uniques de l'élément ou des éléments de substance (englobe DE 02 à DE 04).
02	M (si cet élément codé est utilisé)	En-tête (à définir)	à déterm.	à déterm.	N	Détails à définir.
03	M (si cet élément codé est utilisé)	Information sur les éléments de substance	999 Max	Var	A,N,S,B	Format défini à la discrétion de l'État émetteur ou de l'organisation émettrice.

6.11 GROUPE DE DONNÉES 11 — Détail(s) personnel(s) supplémentaire(s) (OPTIONNEL)

Ce groupe de données est utilisé pour des détails supplémentaires concernant le détenteur du document. Tous les éléments de données de ce groupe étant optionnels, une liste d'étiquettes est employée pour définir ceux qui sont présents. Les éléments de données se combinant pour former le groupe de données 11 (DG11) DOIVENT être les suivants :

Note.— Ce gabarit peut contenir des caractères non latins.

Tableau 50. Étiquettes du groupe de données 11

Étiquette	L	Valeur				
6B	Var					
		Étiq.	**L**	**Valeur**		
		5C	Var			Liste d'étiquettes avec liste des éléments de données dans le gabarit.

Étiquette	L	Valeur				
		5F0E	Var			Nom complet du titulaire du document en caractères nationaux. Codé selon les règles du Doc 9303.
		A0	Var			Classe propre au contenu
				Étiq.	**L**	**Valeur**
				02	01	Nombre d'autres noms
				5F0F	Var	Autre nom formaté selon le Doc 9303. L'objet de données se répète autant de fois qu'il est indiqué dans le nombre d'autres noms (objet de données avec l'étiquette « 02 »).
		Étiq.	**L**	**Valeur**		
		5F10	Var			Numéro personnel
		5F2B	08			Date de naissance complète aaaammjj
		5F11	Var			Lieu de naissance. Champs séparés par « < ».
		5F42	Var			Adresse permanente. Champs séparés par « < ».
		5F12	Var			Téléphone
		5F13	Var			Profession
		5F14	Var			Titre
		5F15	Var			Résumé personnel
		5F16	Var			Preuve de citoyenneté. Image compressée selon l'ISO/IEC 10918.
		5F17	Var			Numéros d'autres documents de voyage valides. Séparés par « < ».
		5F18	Var			Informations sur la garde du document

6.11.1 GROUPE DE DONNÉES 11 — Éléments de données du EF.DG11

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 11 (DG11). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note 1.— L'élément de données 11 DOIT être codé comme il est défini dans l'ISO/IEC 10918, en utilisant l'option JFIF, ou dans l'ISO/IEC 15444 en employant le système de codage d'images JPEG 2000.

Note 2.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 51. Éléments de données du DG11

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^bre d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	O	Nom du titulaire (au complet)	99 Max	Var	B	Caractères de remplissage (<) insérés selon la ZLA. Pas de caractères de remplissage insérés en fin de ligne. Troncation non autorisée.
02	O	Autre(s) nom(s)	99 Max	Var	B	Caractères de remplissage (<) insérés selon la ZLA. Pas de caractères de remplissage insérés en fin de ligne. Troncation non autorisée.
03	O	Numéro personnel	99 Max	Var	A,N,S	Texte libre.
04	O	Date de naissance complète	8	F	B	SSAAMMJJ
05	O	Lieu de naissance	99 Max	Var	B	Texte libre.
06	O	Adresse	99 Max	Var	A,N,S,B	Texte libre.
07	O	Téléphone	99 Max	Var	N,S	Texte libre.
08	O	Profession	99 Max	Var	B	Texte libre.
09	M (si DE 08 est inclus)	Titre	99 Max	Var	B	Texte libre.
10	M (si DE 09 est inclus)	Résumé personnel	99 Max	Var	B	Texte libre.
11	M (si DE 10 est inclus)	Preuve de citoyenneté		Var	A,N,S,B	Image du document de citoyenneté formatée selon l'ISO/IEC 10918-1.
12	O	Autre(s) document(s) de voyage valide(s) Numéro du document de voyage	99 Max	Var	A,N,S,B	Texte libre, séparé par « < ».
13	O	Information sur la garde du document	999 Max	Var	B	Texte libre.

Note.— Si le mois (MM) ou le jour (JJ) sont inconnus, la manière interopérable de l'indiquer dans le DG11 est de mettre les caractères respectifs à « 00 ». Si le siècle et l'année (SSAA) sont inconnus, la manière interopérable de l'indiquer dans le DG11 est de mettre les caractères respectifs à « 0000 ». Les dates attribuées par l'émetteur doivent toujours être utilisées de manière cohérente.

6.12 GROUPE DE DONNÉES 12 — Détail(s) supplémentaire(s) sur le document (OPTIONNEL)

Ce groupe de données est utilisé pour des renseignements supplémentaires sur le document. Tous les éléments de données dans ce groupe sont optionnels.

Tableau 52. Étiquettes du groupe de données 12

Étiquette	L	Valeur				
6C	Var					
		Étiq.	**L**	**Valeur**		
		5C	Var			Liste d'étiquettes avec liste des éléments de données dans le gabarit.
		5F19	Var			Autorité de délivrance
		5F26	08			Date d'émission aaaammjj
		A0	Var			Classe propre au contenu
				Étiq.	**L**	**Valeur**
				02	01	Nombre d'autres personnes
				5F1A	Var	Nom de l'autre personne formaté selon les règles du Doc 9303. L'objet de données se répète autant de fois que l'indique le nombre d'autres noms DE02 (objet de données avec l'étiquette « 02 »).
		Étiq.	**L**	**Valeur**		
		5F1B	Var			Mentions, observations
		5F1C	Var			Exigences fiscales/de sortie
		5F1D	Var			Image du recto du document. Image selon l'ISO/IEC 10918.
		5F1E	Var			Image du verso du document. Image selon l'ISO/IEC 10918.
		5F55	0E			Date et heure de personnalisation du document aaaammjjhhmmss
		5F56	Var			Numéro de série du système de personnalisation

Il est RECOMMANDÉ que les systèmes d'inspection prennent en charge le codage 8 octets de l'heure/la date tant en ASCII et en BCD.

6.12.1 GROUPE DE DONNÉES 12 — Éléments de données du EF.DG12

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 12 (DG12). Les éléments de données et leur format dans chaque groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note 1.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Note 2.— Les éléments de données 07 et 08 DOIVENT être codés comme il est défini dans l'ISO/IEC 10918, en utilisant l'option JFIF, ou dans l'ISO/IEC 15444 en employant le système de codage d'images JPEG 2000.

Tableau 53. Éléments de données du DG12

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^bre^ d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	O	Autorité de délivrance	99 Max	Var	B	Texte libre.
02	O	Date d'émission	8	F	N	Date d'émission du document : AAAAMMJJ
03	O	Détails sur autre(s) personne(s)	99 Max	Var	B	Texte libre.
04	O	Mention(s)/observation(s)	99 Max	Var	B	Texte libre.
05	O	Exigences fiscales/ de sortie	99 Max	Var	B	Texte libre.
06	O	Image du recto du DVLM		Var	A,N,S,B	Formaté selon l'ISO/IEC 10918-1.
07	O	Image du verso du DVLM		Var	A,N,S,B	Formaté selon l'ISO/IEC 10918-1.
08	O	Date et heure de personnalisation	14	F	N	ssaammjjhhmmss
09	O	Numéro de série du système de personnalisation	99 Max	Var	A,N,S	Texte libre.

6.13 GROUPE DE DONNÉES 13 — Détail(s) optionnel(s) (OPTIONNEL)

Les éléments de données se combinant pour former le groupe de données 13 (DG13) sont à la discrétion de l'État émetteur ou de l'organisation émettrice et DOIVENT être comme suit :

Tableau 54. Étiquettes du groupe de données 13

Étiquette	L	Valeur
'6D'	Var	

6.14 GROUPE DE DONNÉES 14 — Options de sécurité (CONDITIONNEL)

Le groupe de données 14 contient des options de sécurité pour les mécanismes de sécurité supplémentaires. Pour plus de renseignements, voir le Doc 9303-11. Le fichier DG14 contenu dans l'application PLM-e est REQUIS si la puce du DVLM-e prend en charge le mappage d'authentification de puce ou le PACE-GM/-IM.

Tableau 55. Étiquettes du groupe de données 14

Étiquette	L	Valeur
6^E	Var	Voir SecurityInfos du groupe de données 14 (Doc 9303-10)

6.14.1 GROUPE DE DONNÉES 14 — Éléments de données du EF.DG14

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 14 (DG14). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 56. Éléments de données du DG14

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^bre d'octets	Fixe ou variable	Type de codage	Exigences de codage
	O	SecurityInfos		Var	B	Voir SecurityInfos du DG14, Doc 9303-10, § 6.14.2.

6.14.2 GROUPE DE DONNÉES 14 — SecurityInfos (informations de sécurité)

La structure de données générique ASN.1 SecurityInfos suivante permet diverses mises en œuvre d'options de sécurité pour des éléments biométriques secondaires. Pour des raisons d'interopérabilité, il est RECOMMANDÉ que cette structure de données soit fournie par la puce du DVLM-e dans le DG14 pour indiquer les protocoles de sécurité pris en charge. La structure de données est spécifiée ci-après :

```
      SecurityInfos     ::=   SET of SecurityInfo

      SecurityInfo      ::=   SEQUENCE {
            protocol    OBJECT IDENTIFIER,
            requiredData      ANY DEFINED BY protocol,
            optionalData      ANY DEFINED BY protocol OPTIONAL
}
```

Les éléments contenus dans la structure de données SecurityInfos ont la signification suivante :

- le protocole d'identificateur d'objet identifie le protocole pris en charge ;
- l'élément requiredData de type ouvert contient les données obligatoires propres au protocole ;
- l'élément optionalData de type ouvert contient les données optionnelles propres au protocole.

6.15 GROUPE DE DONNEES 15 — Information de clé publique d'authentification active (CONDITIONNEL)

Ce groupe de données OPTIONNEL contient la clé publique d'authentification active et il est REQUIS lorsque l'authentification active optionnelle de la puce est mise en œuvre comme il est décrit dans le Doc 9303-11.

Tableau 57. Étiquettes du groupe de données 15

Étiquette	L	Valeur
6F	Var	Voir le Doc 9303-11

6.15.1 GROUPE DE DONNÉES 15 — Éléments de données du EF.DG15

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 15 (DG15). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 58. Éléments de données du DG15

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^{bre} d'octets	Fixe ou variable	Type de codage	Exigences de codage
	O	ActiveAuthenticationPublicKeyInfo		Var	B	Voir le Doc 9303-11.

6.16 GROUPE DE DONNÉES 16 — Personne(s) à aviser (OPTIONNEL)

Ce groupe de données contient des informations sur les notifications en cas d'urgence. Il est codé comme une série de gabarits, en utilisant la désignation d'étiquette « Ax ». Le DG16 (comme tous les autres groupes de données) ne devrait pas être actualisé après l'émission ; il est représenté par une valeur de hachage dans le SO_D et le SO_D n'est signé qu'une fois à l'émission.

Tableau 59. Étiquettes du groupe de données 16

Étiquette	L	Valeur		
70	Var			
		Étiquette	**L**	**Valeur**
		02	01	Nombre de gabarits (seulement dans le premier gabarit)
		Ax	Var	Début des gabarits, avec incréments x (x = 1, 2, 3…) pour chaque occurrence
5F50	04			Date d'enregistrement des données
5F51	Var			Nom de la personne
5F52	Var			Téléphone
5F53	Var			Adresse

6.16.1 GROUPE DE DONNÉES 16 — Éléments de données du EF.DG16

La présente section décrit les éléments de données qui peuvent être présents dans le groupe de données 16 (DG16). Les éléments de données et leur format dans chaque zone du groupe de données DOIVENT être conformes aux indications du tableau suivant :

Note.— A = caractère alphabétique [a..z, A..Z], N = caractère numérique [0..9], S = caractère spécial [« < »], B = données binaires 8 bits (autres que A, N ou S), F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 60. Éléments de données du DG16

Élément de données	Optionnel ou REQUIS	Nom de l'élément de données	N^{bre} d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M (si DG 16 est inclus)	Nombre de personnes identifiées	2	F	N	Identifie le nombre de personnes incluses dans le groupe de données.
02	M (si DG 16 est inclus)	Détails de date enregistrés	8	F	N	Date enregistrée pour la notification ; format = SSAAMMJJ
03	M (si DG 16 est inclus)	Nom de la personne à aviser Identifiants principal et secondaire		Var	B	Caractères de remplissage (<) insérés selon la ZLA. Troncation non autorisée.
04	M (si DE 03 est inclus)	Numéro de téléphone de la personne à aviser		Var	N,S	Numéro de téléphone en format international (code pays et numéro local).
05	M	Adresse de la personne à aviser		Var	B	Texte libre.

7. RÉFÉRENCES (NORMATIVES)

ISO/IEC 14443-1 — ISO/IEC 14443-1:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics* [Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité — Partie 1 : Caractéristiques physiques].

ISO/IEC 14443-2 — ISO/IEC 14443-2:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface [Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité — Partie 2 : Interface radiofréquence et des signaux de communication].

ISO/IEC 14443-3 — ISO/IEC 14443-3:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3:Initialization and Anticollision* [Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité — Partie 3 : Initialisation et anticollision].

ISO/IEC 14443-4 — ISO/IEC 14443-4:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol* [Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact — Cartes de proximité — Partie 4 : Protocole de transmission].

ISO/IEC 10373-6 — ISO/IEC 10373-6:2016, *Identification cards — Test methods — Part 6: Proximity cards* [Cartes d'identification — Méthodes d'essai — Partie 6 : Cartes de proximité].

ISO/IEC 18745-2 — ISO/IEC 18745-2:2016 *Information technology — Test methods for machine readable travel documents (MRTD) and associated devices — Part 2: Test methods for the contactless interface* [Technologies de l'information — Méthodes d'essai pour les documents de voyage lisibles par machine (MRTD) et dispositifs associés — Partie 2: Méthodes d'essai de l'interface sans contact].

ISO/IEC 7816-2 — ISO/IEC 7816-2: 2007, *Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts* [Cartes d'identification — Cartes à circuit intégré — Partie 2 : Cartes à contacts — Dimensions et emplacements des contacts].

ISO/IEC 7816-4 — ISO/IEC 7816-4: 2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange* [Cartes d'identification — Cartes à circuit intégré — Partie 4 : Organisation, sécurité et commandes pour les échanges].

ISO/IEC 7816-5 — ISO/IEC 7816-5: 2004, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers* [Cartes d'identification — Cartes à circuit intégré — Partie 5 : Enregistrement des fournisseurs d'application].

ISO/IEC 7816-6 — ISO/IEC 7816-6: 2016, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange (Defect report included*) [Cartes d'identification — Cartes à circuit intégré — Partie 6 : Éléments de données intersectoriels pour les échanges (y compris rapport de défaillance)].

ISO/IEC 7816-11 — ISO/IEC 7816-11: 2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods* [Cartes d'identification — Cartes à circuit intégré — Partie 11 : Vérification personnelle par méthodes biométriques].

ISO/IEC 8825-1	ISO/IEC 8825-1:2008, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)* [Technologies de l'information — Règles de codage ASN.1 : Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)].
ISO/IEC 19794-4	ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data* [Technologies de l'information — Formats d'échange de données biométriques — Partie 4 : Données d'image du doigt].
ISO/IEC 19794-5	ISO/IEC 19794-5:2005, *Information technology — Biometric data interchange formats — Part 5: Face image data* [Technologies de l'information — Formats d'échange de données biométriques — Partie 5 : Données d'image de la face].
ISO/IEC 10646	ISO/IEC 10646:2012, *Information technology — Universal Coded Character Set (UCS)* [Technologies de l'information — Jeu universel de caractères codés (JUC)].
RFC 3369	*Cryptographic Message Syntax 2002.*
ISO/CEI 10918-1	ISO/CEI 10918-1:1994, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines* [Technologies de l'information — Compression numérique et codage des images fixes de nature photographique : Prescriptions et lignes directrices].
ISO/CEI 15444	ISO/CEI 15444-n, *JPEG 2000 image coding system* [Système de codage d'images JPEG 2000].
ISO/IEC 19785	ISO/IEC 19785-n, *Information technology — Common Biometric Exchange Formats Framework* [Technologies de l'information — Cadre de formats d'échange biométriques communs].

— — — — — — — —

Appendice A à la Partie 10
(INFORMATIF)

EXEMPLES DE MAPPAGE DE LA STRUCTURE DE DONNÉES LOGIQUE

Le texte suivant donne, à titre informatif, des exemples de mappage de la structure de données logique (SDL, version 1.7) en utilisant une représentation d'accès aléatoire à un CI sans contact sur un DVLM-e.

A.1 ÉLÉMENTS DE DONNÉES COMMUNS — EF.COM

L'exemple qui suit indique une implémentation de la version 1.7 de la SDL en utilisant Unicode version 4.0.0, avec présence des groupes de données 1 (étiquette '61'), 2 (étiquette '75'), 4 (étiquette '76') et 12 (étiquette '6C').

Pour cet exemple et tous les autres, les étiquettes sont imprimées en **gras**, les longueurs sont imprimées en *italique*, et les valeurs sont imprimées en caractères romains. Les étiquettes hexadécimales, longueurs et valeurs sont entre guillemets ('xx').

'60' *'16'*
'5F01' *'04'* '0107'
'5F36' *'06'* '040000'
'5C' *'04'* '6175766C'

En représentation hexadécimale complète, cet exemple se lirait :

'60' *'16'*
'5F01' *'04'* '30313037'
'5F36' *'06'* '303430303030'
'5C' *'04'* '6175766C'

Une version SDL 15.99 hypothétique serait codée comme suit :

'60' *'16'*
'5F01' *'04'* '1599'
'5F36' *'06'* '040000'
'5C' *'04'* '6175766C'

ou en hexadécimal :

'60' *'16'*
'5F01' *'04'* '31353939'
'5F36' *'06'* '303430303030'
'5C' *'04'* '6175766C'

A.2 INFORMATION DE LA ZLA — EF.DG1

A.2.1 DVLM-e de format TD1

Ci-dessous un exemple du DG1 utilisant ces informations dans un DVLM-e de format TD1. La longueur de l'élément de données ZLA est de 90 octets ('5A').

'61' *'5D'* **'5F1F'** *'5A'*

```
I<NLDXI85935F86999999990<<<<<<7208148F1108268NLD<<<<<<<<<<<4VAN<DER<STEEN<<MARI
ANNE<LOUISE
```

A.2.2 DVLM-e de format TD2

Ci-dessous un exemple du DG1 utilisant ces informations dans un DVLM-e de format TD2. La longueur de l'élément de données ZLA est de 72 octets ('48').

'61' *'4B'* **'5F1F'** *'48'*

```
I<ATASMITH<<JOHN<T<<<<<<<<<<<<<<<<<<<<<<<<<<123456789<HMD7406222M10123130121<<<54
```

A.3 GABARITS BIOMÉTRIQUES — EF.DG2 À EF.DG4

Les DG2 à DG4 utilisent l'option imbriquée hors carte de la norme ISO/IEC 7816-11 pour avoir la possibilité de stocker des gabarits biométriques multiples d'une certaine sorte, en harmonie avec le CBEFF, NISTR 6529a. Le sous-en-tête biométrique définit le type d'élément biométrique qui est présent et l'élément biométrique spécifique.

Exemple : Un élément biométrique facial, signé, avec longueur de bloc de données biométriques de 12 642 octets ('3162' octets), codé en utilisant un dispositif avec PID de '00 01 00 01' ET le type de format '00 04' appartenant au fournisseur de gabarit '00 0A', capturé le 15 mars 2002 (sans décalage UTC) et valide du 1er avril 2002 au 31 mars 2007. La version 1.0 du gabarit d'usager OACI est utilisée.

La longueur totale du gabarit est de 12 704 octets. Le gabarit est stocké en commençant au début de EF.DG2 (SFID 02).

'75' *'82319EC'*
- **'7F61'** *'823199'*
  - **'02'** *'01'* '01'
  - **'7F60'** *'823191'*
  - **'A1'** *'26'*
    - **'80'** *'02'* '0101'
    - **'81'** *'01'* '02'
    - **'83'** *'07'* '20020315133000'
    - **'85'** *'08'* '2002040120070331'
    - **'86'** *'04'* '00010001'
    - **'87'** *'02'* '000A'
    - **'88'** *'02'* '0004'
  - **'5F2E'** *'823162'* '… 12 642 octets de données biométriques …'

A.4 GABARITS D'IMAGE AFFICHÉE — EF.DG5 À EF.DG7

Note.— Un EF pour chaque DG.

Exemple : Gabarit de l'image avec longueur de données de l'image affichée de 2 000 octets. La longueur du gabarit est de 2 008 octets ('07D8').

'65' *'8207D8'*

'02' *'01'* 1
'5F40' *'8207D0'* '….2 000 octets de données d'image …'

A.5 DÉTAILS PERSONNELS SUPPLÉMENTAIRES — EF.DG11

L'exemple qui suit montre les détails personnels suivants : nom complet (John J. Smith), lieu de naissance (Anytown, MN), adresse permanente (123 Maple Rd, Anytown, MN), numéro de téléphone (1-612-555-1212) et profession (agent de voyages). La longueur du gabarit est de 99 octets ('63').

'6B' *'63'*

'5C' *'0A'* **'5F0E' '5F11' '5F42' '5F12' '5F13'**
'5F0E' *'0D'* SMITH<<JOHN<J
'5F11' *'0A'* ANYTOWN<MN
'5F42' *'17'* 123 MAPLE RD<ANYTOWN<MN
'5F12' *'0E'* 16125551212
'5F13' *'0C'* TRAVEL<AGENT

A.6 PERSONNE(S) À INFORMER — EF.DG16

Exemple avec deux entrées : Charles R. Smith d'Anytown, MN et Mary J. Brown d'Ocean Breeze, CA. La longueur du gabarit est de 162 octets ('A2').

'70' *'81A2'*

'02' *'01'* 2
'A1' '4C'
'5F50' *'08'* 20020101
'5F51' *'10'* SMITH<<CHARLES<R
'5F52' *'0B'* 19525551212
'5F53' *'1D'* 123 MAPLE RD<ANYTOWN<MN<55100
'A2' '4F'
'5F50' *'08'* 20020315
'5F51' *'0D'* BROWN<<MARY<J
'5F52' *'0B'* 14155551212
'5F53' *'23'* 49 REDWOOD LN<OCEAN BREEZE<CA<94000

— — — — — — — —

Appendice B à la Partie 10
(INFORMATIF)

MISE EN PLACE DU CI SANS CONTACT DANS UN PLM-e

B.1 FORMAT ET CLASSE DE L'ANTENNE D'UN DVLM-e

Le format de l'antenne est à la discrétion de l'État émetteur. À l'exception du format de l'antenne, le DVLM-e DOIT répondre à tous les tests spécifiés dans l'ISO/IEC 18745-2 qui appliquent les spécifications de la classe 1.

Note.— L'ISO/IEC 14443-2 a élaboré les exigences pour la classe 1 en vue d'une interopérabilité maximale. Dans l'ISO/IEC 14443-2 et l'ISO/IEC 10373-6, un objet sans contact n'indiquant aucune classe est toujours testé par rapport à la classe 1.

Il est RECOMMANDÉ que les DVLM-e respectent également les spécifications de la classe 1, y compris sa spécification de format d'antenne (voir B.8 ci-dessous), car les DVLM-e non conformes aux spécifications de la classe 1 peuvent entraîner des problèmes d'interopérabilité.

Pour les DVLM-e de format **TD3** (**ID-3**), le DVLM-e DOIT contenir une antenne ainsi qu'un circuit intégré (CI) qui sont ensemble conformes à la classe 1 comme défini dans l'ISO/IEC 14443-1 et l'ISO/IEC 14443-2 à l'exception du format d'antenne. Il n'y a pas de position obligatoire pour le CI, qui PEUT être placé dans une position arbitraire. L'emplacement de l'antenne sans contact est à la discrétion de l'État émetteur dès lors qu'elle est située dans l'un des emplacements suivants :

Page de renseignements — Placer le CI et l'antenne dans la structure d'une page de renseignements constituant une page intérieure du livret ;

Centre du livret — Placer le CI et son antenne entre les pages centrales du livret ;

Couverture — Les placer dans la structure de la couverture ;

Page séparée cousue — Incorporer le CI et son antenne dans une page séparée, qui PEUT avoir la forme d'une carte plastique au format TD3, cousue dans le livret lors de sa confection ;

Couverture arrière — Les placer dans la structure de la couverture arrière.

Note.— Aucune position obligatoire de l'antenne n'était prévue dans les éditions antérieures du Doc 9303.

B.2 INITIALISATION ET INVITATION À ÉMETTRE

Un DVLM-e porté à un champ magnétique alternatif de 1.5 A/m comme mesuré dans l'ISO/IEC 18745-2 est vivement RECOMMANDÉ pour pouvoir répondre à toute REQ/WUP appropriée à son type après un champ magnétique alternatif non modulé de 5 ms.

Note.— Pour le système d'inspection associé au DVLM-e, une trame de 10 ms de porteuse non modulée doit être fournie pour des raisons d'ancienneté. Il peut toutefois être souhaitable que les DVLM-e communiquent également avec d'autres systèmes d'inspection sans contact et des dispositifs mobiles (les téléphones intelligents NFC, par exemple, utilisent une trame de 5 ms).

B.3 ANTICOLLISION ET TYPE

Le DVLM-e PEUT être conforme au type A ou au type B comme défini dans l'ISO/IEC 14443-2. Il ne DOIT pas modifier son type à moins qu'il n'ait été réinitialisé par le système d'inspection associé au DVLM-e.

B.4 DÉBITS BINAIRES OBLIGATOIRES

Le DVLM-e DOIT obligatoirement fournir au moins les débits binaires suivants, comme défini dans l'ISO/IEC 14443-2 : 106 kbit/s et 424 kbit/s dans les deux sens entre le DVLM-e et le système d'inspection associé au DVLM-e.

B.5 PERTURBATIONS ÉLECTROMAGNÉTIQUES

La prise en charge des perturbations électromagnétiques n'est pas obligatoire.

Note.— L'élément de prise en charge des perturbations électromagnétiques améliore la fiabilité de la communication sans contact entre le DVLM-e et le système d'inspection associé au DVLM-e face aux perturbations électromagnétiques générées par le DVLM-e. La consommation de courant dynamique du DVLM-e lors de l'exécution d'une commande peut entraîner un effet de modulation de charge arbitraire (qui peut ne pas être purement résistif) sur le champ magnétique. Dans certains cas, le système d'inspection associé au DVLM-e peut interpréter incorrectement les perturbations électromagnétiques comme des données transmises par le DVLM-e, ce qui peut nuire à la réception correcte de la réponse du DVLM-e.

B.6 DÉBITS BINAIRES (OPTIONNEL)

Le débit binaire de 212 kbit/s et tous les débits binaires allant de 848 kbit/s jusqu'à 6,78 Mbit/s dans les deux sens et de 10,17 Mbit/s à 27,12 Mbit/s depuis le système d'inspection associé au DVLM-e, comme défini dans l'ISO/IEC 14443-2, sont facultatifs. Le demandeur de ce profil d'application DOIT déclarer ses débits binaires supportés dans le tableau de déclaration du demandeur en vue de vérifications appropriées.

Note 1.— La prise en charge de l'échange de paramètres additionnels est obligatoire pour les débits binaires supérieurs à 848 kbit/s.

Note 2.— La compatibilité rétroactive est pleinement assurée car le système d'inspection associé au DVLM-e sélectionne uniquement le débit binaire qu'il prend en charge.

B.7 PRISE EN CHARGE DE L'ÉCHANGE DE PARAMÈTRES ADDITIONNELS (OPTIONNEL)

Le DVLM-e PEUT prendre en charge l'échange de paramètres additionnels tels que définis dans l'ISO/IEC 14443-4 afin de négocier des débits binaires supérieurs à 106 kbit/s. Il PEUT également utiliser les mêmes paramètres additionnels pour négocier des trames avec une correction d'erreur comme spécifié dans l'ISO/IEC 14443-4.

B.8 FORMAT ET CLASSE DE L'ANTENNE

Il est RECOMMANDÉ de suivre les règles relatives à la position de l'antenne comme défini dans l'ISO/IEC 14443-1 et l'ISO/IEC 14443-2 pour la classe 1.

B.9 MISE SOUS ÉCRAN

Il est RECOMMANDÉ de ne mettre sous écran aucune page du DVLM-e.

B.10 IDENTIFICATEUR UNIQUE (UID) ET IDENTIFICATEUR PICC PSEUDO-UNIQUE (PUPI) (RECOMMANDÉ)

Le DVLM-e PEUT fournir un UID/PUPI aléatoire ou fixe comme défini dans l'SO/IEC 14443-3.

Il est RECOMMANDÉ d'utiliser un UID/PUPI aléatoire pour renforcer la confidentialité du titulaire et réduire les possibilités de suivi.

Note.— Toutes les éditions du Doc 9303 ont RECOMMANDÉ un UID/PUPI aléatoire.

B.11 ADRESSE DE NŒUD (RECOMMANDÉ)

Il est RECOMMANDÉ de prendre en charge l'adresse de nœud.

Note.— L'adresse de nœud peut être utilisée pour des cartes sans contact et DVLM-e multiples dans un champ ou des hôtes multiples au sein d'un système d'inspection.

B.12 IDENTIFICATEUR DE CARTE (RECOMMANDÉ)

Le DVLM-e DEVRAIT prendre en charge l'identificateur de carte.

B.13 PLAGE DE FRÉQUENCES DE RÉSONANCE (RECOMMANDÉ)

Bien qu'il n'existe aucune exigence quant à la fréquence de résonance, certains demandeurs de ce profil d'application PEUVENT limiter leur fréquence de résonance par défaut à une certaine plage afin d'accroître l'interopérabilité. Dans ce cas, cette plage DEVRAIT être fournie au laboratoire d'essai avec tous les autres éléments repris dans le tableau de déclaration du demandeur qui figure dans l'ISO/IEC 18745-2.

B.14 TAILLES DE TRAME (RECOMMANDÉ)

Le DVLM-e PEUT prendre en charge des tailles de trame de 4 Ko maximum conformément à l'ISO/IEC 14443. Cependant, il est RECOMMANDÉ de prendre en charge des tailles de trame d'au moins 1 Ko. En cas de prise en charge de tailles de trame supérieures à 1 Ko, l'utilisation de trames avec une correction d'erreur comme définie dans l'ISO/IEC 14443-4 est RECOMMANDÉE.

Note.— Une taille de trame supérieure réduit considérablement le temps de traitement total d'une application DVLM-e.

B.15 TEMPS D'ATTENTE DE TRAME (FWI) ET REQUÊTE DE PROLONGATION DE DURÉE D'ATTENTE BLOC S [S(WTX)] (RECOMMANDÉ)

Il est vivement RECOMMANDÉ de fixer pour le DVLM-e une valeur FWI inférieure ou égale à 11 afin d'améliorer les performances. Il est vivement RECOMMANDÉ d'utiliser des commandes S(WTX) pour prolonger le temps d'attente de trame pour chaque commande particulière qui requiert plus de temps en utilisant les commandes S(WTX) d'un WTXM d'une valeur maximale de 10.

Si des requêtes S(WTX) multiples sont transmises par le DVLM-e, il est RECOMMANDÉ que le temps de traitement total pour le bloc I ne dépasse pas 5 s.

Note.— Les valeurs FWI inférieures RECOMMANDÉES dans le présent document réduisent considérablement la perte de temps dans les erreurs de transmission, tandis que les S(WTX) constituent le moyen idéal pour octroyer davantage de temps si nécessaire.

— — — — — — — —

Appendice C à la Partie 10
(INFORMATIF)

SYSTÈMES D'INSPECTION

C.1 VOLUME FONCTIONNEL ET POSITIONS D'ESSAI

Un système d'inspection associé à un DVLM-e DOIT avoir un volume fonctionnel conforme à l'un des types de systèmes d'inspection définis dans l'ISO/IEC 18745-2. Le volume fonctionnel est le volume dans lequel toutes les exigences de ce rapport technique sont remplies.

Note.— Les positions d'essai de chaque type de système d'inspection sont précisées dans l'SO/IEC 18745-2 pour ce qui concerne la surface de 0 mm (dispositif) du système d'inspection associé au DVLM-e.

C.2 FORME D'ONDE PARTICULIÈRE ET EXIGENCES RF

Les formes d'onde du champ magnétique alternatif utilisées pour communiquer DOIVENT être conformes à l'ISO/IEC 14443-2. En général, il n'y a pas d'exceptions ou d'écarts par rapport à la norme de base, à l'exception de l'intensité de champ.

Pour les systèmes d'inspection associés à un DVLM-e de type 1, 2 et 3, une intensité de champ d'au moins 2 A/m à toutes les positions est vivement RECOMMANDÉE pour la classe 1. Pour les systèmes d'inspection associés à un DVLM-e de type M, l'intensité de champ DOIT être d'au moins 1,5 A/m à toutes les positions pour la classe 1.

Note.— Il peut être souhaitable que les DVLM-e communiquent également avec d'autres systèmes d'inspection sans contact et des dispositifs mobiles (les téléphones intelligents NFC, par exemple, utilisent une intensité de champ de 1,5 A/m).

C.3 SÉQUENCES D'INVITATION À ÉMETTRE ET TEMPS DE DÉTECTION DU DVLM-e

La séquence d'invitation à émettre du système d'inspection associé au DVLM-e DOIT fournir une trame de 10 ms de porteuse non modulée avant toute REQA/WUPA ou REQB/WUPB.

Pour une détection et un traitement rapides, le système d'inspection du DVLM-e :

- DOIT inviter à émettre pour le type A et le type B avec une occurrence des requêtes égale pour les deux types ;
- pour les systèmes d'inspection de Type 1, 2 et 3, une réinitialisation RF doit intervenir entre toute REQ/WUP du même type ;
- DOIT garantir au moins une commande d'invitation à émettre pour le type A et le type B dans la trame de 150 ms pour un DVLM-e présent dans le volume fonctionnel minimal obligatoire selon l'ISO/IEC 18745-2 à toute position.

Le système d'inspection du DVLM-e PEUT inviter à émettre pour des produits sans contact de tout autre type de modulation sur la porteuse 13,56 MHz dès lors que toutes les exigences ci-dessus sont remplies.

Note.— La trame de 10 ms de porteuse non modulée est requise pour détecter tous les DVLM-e dans le champ et s'appuie sur les spécifications précédentes.

C.4 DÉBITS BINAIRES OBLIGATOIRES

Le système d'inspection associé au DVLM-e DOIT obligatoirement fournir les débits binaires suivants, comme défini dans l'ISO/IEC 14443-2 : 106 kbit/s et 424 kbit/s dans les deux sens du DVLM-e au système d'inspection associé au DVLM-e et vice versa.

C.5 TAILLES DE TRAME

Le système d'inspection associé au DVLM-e :

- de type 1, 2 et 3 est vivement RECOMMANDÉ pour prendre en charge toutes les tailles de trame définies jusqu'à 256 octets.
- de Type M ne comporte aucune exigence quant à la taille des trames.

Note.— Toutes les tailles comprises entre le minimum et le maximum ne sont pas expressément testées dans l'ISO/IEC 18745-2:2016.

C.6 INTERFACE SANS CONTACT DES SYSTÈMES D'INSPECTION MOBILES DE TYPE M

Si un dispositif mobile est utilisé pour lire un DVLM-e de toute taille, ce dispositif est de type M. Dans ce cas, la position centrale du système d'inspection est définie comme la position à la surface du système d'inspection avec la plus forte intensité de champ mesurée pour la classe 1. Les systèmes d'inspection associés au DVLM-e de type M DOIVENT fournir des orientations suffisantes pour que l'utilisateur place correctement le DVLM-e sur le dispositif.

C.7 PERTURBATIONS ÉLECTROMAGNÉTIQUES (EMD)

Le soutien de l'EMD n'est pas obligatoire.

Note.— L'élément EMD améliore la fiabilité de la communication sans contact entre le DVLM-e et le système d'inspection associé au DVLM-e face aux perturbations électromagnétiques générées par le DVLM-e. La consommation de courant dynamique du DVLM-e lors de l'exécution d'une commande peut entraîner un effet de modulation de charge arbitraire (qui peut ne pas être purement résistif) sur le champ magnétique. Dans certains cas, le système d'inspection associé au DVLM-e peut interpréter incorrectement les perturbations électromagnétiques comme des données transmises par le DVLM-e, ce qui peut nuire à la réception correcte de la réponse du DVLM-e.

C.8 CLASSES D'ANTENNES PRISES EN CHARGE

Le système d'inspection associé au DVLM-e de type 1 et de type 2 DOIT au moins prendre en charge les DVLM-e dans le volume fonctionnel.

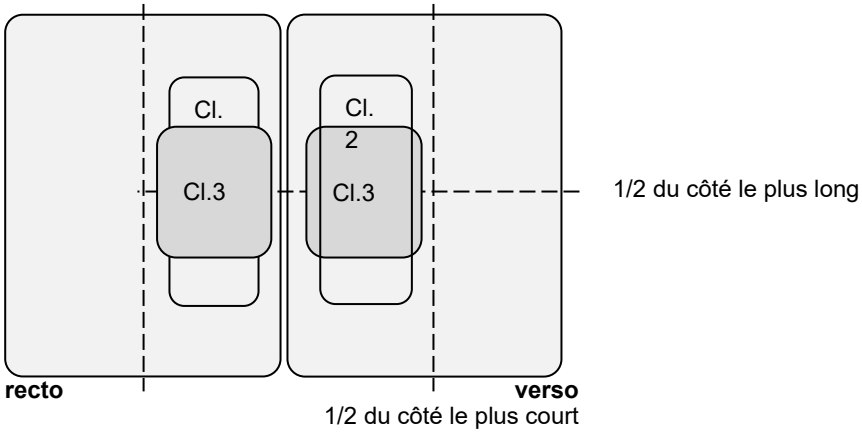

Figure C-1. Positions obligatoires sur chaque surface ID-3 dans laquelle une antenne de classe 2 et de classe 3 DOIT être lue par un système d'inspection associé au DVLM-e de type 1 et 2

Afin de disposer d'une période de migration, les classes 2 et 3 ne sont pas obligatoires sur toutes les positions comme prescrit par la norme de base. Étant donné que des projets autres que DVLM-e peuvent utiliser les classes 2 et 3, le système d'inspection du DVLM-e de type 1 et de type 2 DOIT au moins prendre en charge également les classes 2 et 3 dans la seule position particulière définie à la Figure C-1.

Le système d'inspection associé au DVLM-e de type 3 DOIT prendre en charge les classes 1, 2 et 3 sur sa seule position centrale.

Le système d'inspection associé au DVLM-e de type M DOIT prendre en charge les antennes de classe 1, 2 et 3 sur sa position centrale.

C.9 TAILLES DE TRAME ET CORRECTION D'ERREUR (OPTIONNEL)

Le système d'inspection associé au DVLM-e PEUT éventuellement prendre en charge toutes les tailles de trame de 4 Ko maximum comme défini dans l'ISO/IEC 14443-3. Il est RECOMMANDÉ d'utiliser des trames avec une correction d'erreur comme définie dans l'ISO/IEC 14443-3 pour toutes les tailles de trame prises en charge supérieures à 1 Ko.

Note.— Pour les systèmes d'inspection associés au DVLM-e de type M, les tailles de trame supérieures à 256 octets ne sont actuellement pas envisagées.

C.10 PRISE EN CHARGE DE CLASSES ADDITIONNELLES (OPTIONNEL)

Les systèmes d'inspection associés au DVLM-e de tous les types PEUVENT en outre prendre en charge les classes 4, 5 et 6 pour être interopérables, par exemple avec des dispositifs mobiles offrant moins de couplage à la bobine d'antenne du système d'inspection associé au DVLM-e.

C.11 DÉBITS BINAIRES (OPTIONNEL)

Le débit binaire de 212 kbit/s et tous les débits binaires allant de 848 kbit/s jusqu'à 6,78 Mbit/s dans les deux sens et de 10,17 Mbit/s à 27,12 Mbit/s depuis le système d'inspection associé au DVLM-e, comme défini dans l'ISO/IEC 14443-2, sont optionnels.

Note 1.— La prise en charge de l'échange de paramètres additionnels est obligatoire pour utiliser des débits binaires supérieurs à 848 kbit/s.

Note 2.— La compatibilité rétroactive est pleinement assurée dans l'élément des paramètres additionnels.

C.12 TEMPÉRATURE DE FONCTIONNEMENT (RECOMMANDÉ)

Il est RECOMMANDÉ que le système d'inspection associé au DVLM-e fonctionne à des températures comprises entre -10 °C et 50 °C.

C.13 PRISE EN CHARGE DE DVLM-e MULTIPLES ET AUTRES CARTES OU OBJETS OU CARTES OU HÔTES MULTIPLES (RECOMMANDÉ)

Il est vivement RECOMMANDÉ de concevoir le système d'inspection associé au DVLM-e de façon à prendre en charge plus d'un DVLM-e ou un DVLM-e et tout autre carte ou objet conforme à l'ISO/IEC 14443.

Une des règles suivantes ou une combinaison de celles-ci PEUT notamment être appliquée :

- appliquer les algorithmes anticollision complets définis dans l'ISO/IEC 14443-3 ;
- rechercher la prise en charge de l'ISO/IEC 14443-4 et exclure les cartes qui n'assurent pas la prise en charge ;
- rechercher une application DVLM-e ;
- utiliser l'identificateur de carte et l'adresse de nœud.

Note.— L'adresse de nœud peut également être utilisée pour des dispositifs mobiles avec des hôtes multiples.

C.14 TAILLES DE TRAME (RECOMMANDÉ)

Le système d'inspection associé au DVLM-e PEUT prendre en charge des tailles de trame de 4 Ko maximum conformément à l'ISO/IEC 1444-3. Cependant, il est RECOMMANDÉ de prendre en charge des tailles de trame d'au moins 1 Ko. En cas de prise en charge de tailles de trame égales ou supérieures à 1 Ko, l'utilisation de trames avec une correction d'erreur comme définie dans l'ISO/IEC 14443-4 est RECOMMANDÉE.

Il est RECOMMANDÉ de diviser la charge utile de la couche d'application en un nombre minimal de trames avec une longueur effective de la taille de trame maximale prise en charge à l'exception de la dernière trame.

C.15 RÉTABLISSEMENT EN CAS D'ERREUR (RECOMMANDÉ)

À la suite d'une erreur de transmission ou d'un DVLM-e sans réponse, il est vivement RECOMMANDÉ que le système d'inspection associé au DVLM-e transmette un deuxième R(NAK) conformément à la règle 4 de l'ISO/IEC 14443-4 relative au système d'inspection.

C.16 DÉTECTION D'ERREUR ET MÉCANISME DE RÉTABLISSEMENT (RECOMMANDÉ)

Lors de l'utilisation de débits binaires facultatifs ainsi que de tailles de trame facultatives supérieures à 256 octets, si le nombre d'erreurs de transmission est plus élevé que d'habitude, il est RECOMMANDÉ de réduire le débit binaire et la taille de trame effective.

— FIN —