OACI

Doc 9303

Documents de voyage lisibles à la machine

Huitième édition, 2021

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

Huitième édition, 2021

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

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

Commande nº : 9303P10
ISBN 978-92-9265-564-8 (version imprimée)
ISBN 978-92-9275-557-7 (version électronique)

AMENDEMENTS

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

RELEVÉ DES AMENDEMENTS ET DES RECTIFICATIFS

AMENDEMENTS		
N°	Date	Inscrit par
1	14/6/24	OACI

RECTIFICATIFS		
N°	Date	Inscrit par

TABLE DES MATIÈRES

Page

Page

1. PORTÉE

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 circuit intégré (CI) sans contact. Ceci exige l'identification de tous les éléments de données, obligatoires ou optionnels, et un ordonnancement et/ou un groupement prescriptifs des éléments de données qui DOIVENT être suivis afin de réaliser l'interopérabilité universelle de la lecture électronique des passeports électroniques.

Le Doc 9303-10 énonce les spécifications qui permettront aux États et aux intégrateurs d'utiliser les CI sans contact dans un document de voyage électronique. 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 huitième édition du Doc 9303 intègre les spécifications des applications facultatives dossiers de voyage, dossiers de visa et éléments biométriques supplémentaires (appelées applications SDL2) comme extension de l'application obligatoire DVLM-e (appelée SDL1).

La Partie 10 doit 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 9 — *Déploiement de l'identification biométrique et stockage électronique des données dans les DVLM* ;
- Partie 11 — *Mécanismes de sécurité pour les DVLM* ;
- Partie 12 — *Infrastructure à clés publiques pour les DVLM*.

2. STRUCTURE DU DOC 9303-10

La Partie 10 du Doc 9303 est organisée en sections qui incluent :

Les spécifications communes aux applications SDL1 et SDL2 :

- attributs communs ;

- toutes les commandes pour les SDL1 et SDL2 ;
- fichiers élémentaires (EF) communs pour les SDL1 et SDL2 ;

Spécifications pour l'application de DVLM-e SDL1 ;

Spécifications pour les applications de la SDL2 :

- dossiers de voyage ;
- dossiers de visa ;
- éléments biométriques supplémentaires ;
- spécifications pour les conditions d'accès aux fichiers SDL2.

Le DVLM-e peut prendre en charge un, plusieurs ou tous ces éléments :

- application DVLM-e SDL1 (OBLIGATOIRE) ;
- application de dossiers de voyage SDL2 (OPTIONNELLE) ;
- application de dossiers de visa SDL2 (OPTIONNELLE) ;
- application d'éléments biométriques supplémentaires SDL2 (OPTIONNELLE).

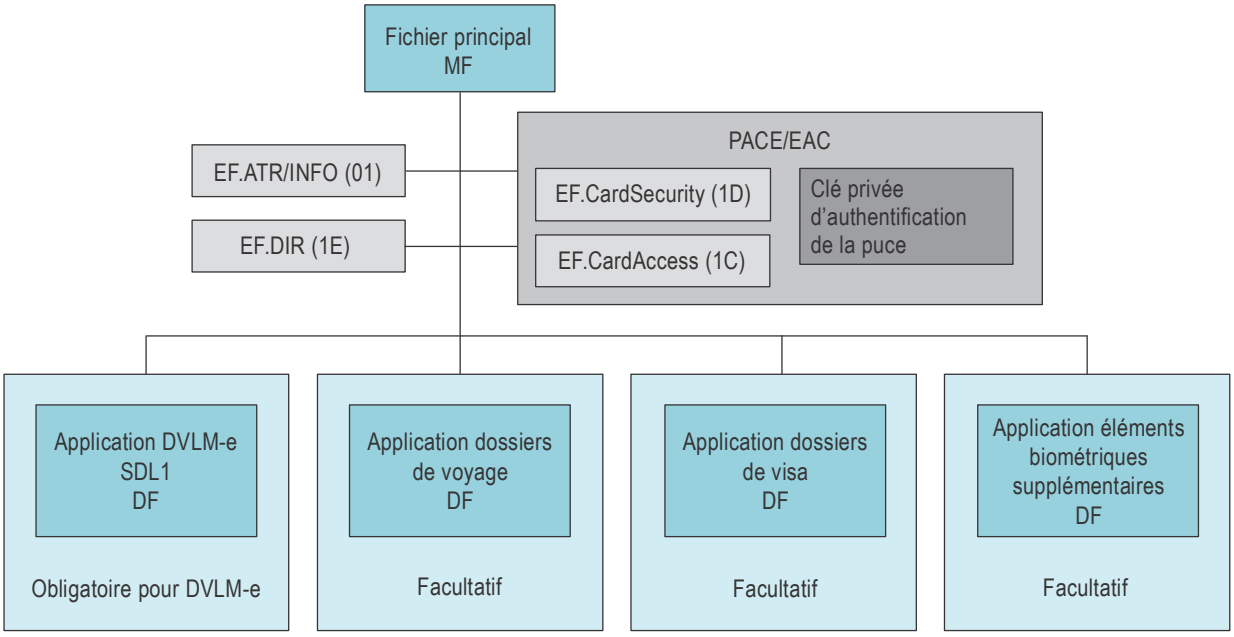


Figure 1. Applications pour SDL1 et SDL2

3. SPÉCIFICATIONS COMMUNES AUX SDL1 ET SDL2

3.1 Exigences minimales d'interopérabilité

Les exigences minimales d'interopérabilité des passeports électroniques 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 ;

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 Protocole de transmission

Le DVLM-e DOIT prendre en charge le protocole de transmission semi-duplex défini dans la norme ISO/IEC 14443-4. Le DVLM-e DOIT prendre en charge les protocoles de transmission de type A ou de type B, ainsi que les protocoles d'initialisation, d'anticollision et de transmission conformément à la norme ISO/IEC 14443.

3.4.1 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.

3.4.2 Identificateur aléatoire ou identificateur fixe pour le CI sans contact

Le DVLM-e peut servir de « radiobalise » dans laquelle le CI sans contact émet un identifiant unique (UID) pour le type A et un PUPI pour le type B lorsqu'il est initialement activé. Cela pourrait permettre l'identification de l'autorité émettrice. 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 identifiants 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.

3.5 Jeu de commandes

Les commandes, les formats et leurs octets d'état sont tous définis dans les normes ISO/IEC 7816 4 et ISO/IEC 7816-8, à l'exception de la commande FILE AND MEMORY MANAGEMENT. Le jeu de commandes minimum que DOIT prendre en charge le DVLM-e SDL1 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)/MUTUAL AUTHENTICATE (authentification mutuelle) ;
INTERNAL AUTHENTICATE (authentification interne) ;
MANAGE SECURITY ENVIRONMENT (gestion de l'environnement de sécurité) ;
GENERAL AUTHENTICATE (authentification générale).

Si des applications SDL2 optionnelles sont présentes, le DVLM-e DOIT aussi prendre en charge les commandes suivantes :

Pour l'application des dossiers de voyage :
READ RECORD (lecture de dossier) ;
APPEND RECORD (ajout de dossier) ;
SEARCH RECORD (recherche de dossier) ;
FILE AND MEMORY MANAGEMENT (gestion des fichiers et de la mémoire) ;
PERFORM SECURITY OPERATION (PSO) (effectuer une opération de sécurité).

Pour l'application des dossiers de visa :
READ RECORD (lecture de dossier) ;
APPEND RECORD (ajout de dossier) ;
SEARCH RECORD (recherche de dossier) ;
FILE AND MEMORY MANAGEMENT (gestion des fichiers et de la mémoire) ;
PERFORM SECURITY OPERATION (PSO) (effectuer une opération de sécurité).

Pour l'application d'éléments biométriques supplémentaires :

UPDATE BINARY (mise à jour binaire) ;
READ RECORD (lecture de dossier) ;
APPEND RECORD (ajout de dossier) ;
SEARCH RECORD (recherche de dossier) ;
ACTIVATE (activer) ;
FILE AND MEMORY MANAGEMENT (gestion des fichiers et de la mémoire) ;
PERFORM SECURITY OPERATION (PSO) (effectuer une opération de sécurité).

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

3.5.1 SELECT (sélectionner)

Le DVLM-e SDL1 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 EF court sont OBLIGATOIRE pour le système d'exploitation du CI sans contact, mais OPTIONNELS pour le lecteur.

3.5.2 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.

3.6 Formats de commande et options de paramétrage (SDL1 et SDL2)

3.6.1 Sélection de l'application DF à l'aide de la commande SELECT

Les applications doivent être sélectionnées par leur nom de DF indiquant l'identifiant d'application (AID). Après la sélection d'une application, il est possible d'accéder au fichier dans cette application.

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

3.6.1.1 Sélection du fichier principal

Tableau 1. Commande SELECT pour la sélection du fichier principal (MF)

CLA	« 00 »
INS	« A4 »
P1	« 00 »
P2	« 0C »
Champ Lc	Absent
Champ de données	Absent
Champ Le	Absent

Réponse de commande SELECT

Champ de données	Absent
SW1-SW2	« 9000 » Traitement normal Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

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

3.6.1.2 Sélection de l'application DF

Une application DF DOIT être sélectionnée en utilisant la commande SELECT avec un nom de DF indiquant l'identifiant d'application (AID). Les paramètres de la commande unité de données de protocole d'application (APDU) sont présentés ci- après :

Tableau 2. Commande SELECT avec AID pour la sélection de l'application DF

CLA	« 00 »
INS	« A4 »
P1	« 04 »
P2	« 0C »
Champ Lc	Longueur du champ de données de la commande
Champ de données	Nom du DF (AID)
Champ Le	Absent

Réponse de commande SELECT

Champ de données	Absent
SW1-SW2	« 9000 » Traitement normal Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

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

EF est sélectionné par la commande SELECT avec l'identificateur EF. Lorsque l'EF est sélectionné, il faut s'assurer que l'application DF stockant l'EF a été préalablement sélectionnée.

Tableau 3. Commande SELECT avec l'identificateur de fichier pour la sélection EF

CLA	« 00 » / « 0C »
INS	« A4 »
P1	« 02 »
P2	« 0C »
Champ Lc	« 02 »
Champ de données	Identificateur de fichier
Champ Le	Absent

Réponse de commande SELECT

Champ de données	Absent
SW1-SW2	« 9000 » Traitement normal Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

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 code INS pair et un identificateur EF court, comme il est spécifié au Tableau 5.

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

Il y a deux méthodes pour lire les données d'un DVLM-e : la sélection de l'EF suivie de la lecture des données de l'EF sélectionné, ou la lecture directe des données en utilisant l'identificateur EF court. La prise en charge de l'identificateur EF court est OBLIGATOIRE pour le DVLM-e. Il est donc RECOMMANDÉ que le système d'inspection utilise un identificateur EF court.

3.6.3.1 Lecture des données d'un EF sélectionné (fichier transparent)

Tableau 4. Commande READ BINARY pour l'EF sélectionné

CLA	« 00 » / « 0C »
INS	« B0 »
P1	Décalage
P2	
Champ Lc	Absent
Champ de données	Absent
Champ Le	Présent pour le codage Ne > 0

Réponse de commande READ BINARY

Champ de données	Lecture des données
SW1-SW2	« 9000 » Traitement normal Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

3.6.3.2 Lecture de données en utilisant l'identificateur EF (fichier transparent)

Tableau 5. Commande READ BINARY avec l'identificateur EF court

CLA	« 00 » / « 0C »
INS	« B0 »
P1	Identificateur EF court
P2	Décalage
Champ Lc	Absent
Champ de données	Absent
Champ Le	Présent pour le codage Ne > 0. Nombre maximum d'octets escomptés dans le champ de données de la réponse

Réponse de commande READ BINARY

Champ de données	Lecture des données
SW1-SW2	« 9000 » Traitement normal Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

3.6.4 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-e. Pour plus de renseignements sur les champs de longueur étendue, voir la norme ISO/IEC 7816-4.

3.6.4.1 Puces de DVLM-e et longueur étendue

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

3.6.4.2 Terminaux

Pour les terminaux, la prise en charge de champs de longueur étendue est OBLIGATOIRE. Un terminal DEVRAIT vérifier si l'ATR/ATS ou l'EF.ATR/INFO de la puce du DVLM-e indique ou non la prise en charge de champs de longueur

étendue avant d'utiliser cette option. Le terminal NE DOIT PAS utiliser les champs de 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-e ne soient explicitement indiquées dans l'ATS ou dans l'EF.ATR/INFO.

- MSE:Set KAT ;
- GENERAL AUTHENTICATE (authentification générale).

3.6.5 Chaînage des commandes

Le chaînage des commandes DOIT être utilisé pour la commande GENERAL AUTHENTICATE (authentification générale) 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.

3.6.6 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 de commande READ BINARY lorsque le décalage est supérieur à 32 767 octets

CLA	« 00 » / « 0C »
INS	« B1 »
P1	Voir le Tableau 7
P2	
Champ Lc	Longueur du champ de données de la commande
Champ de données	Décalage DO « 54 »
Champ Le	Présent pour le codage Ne > 0. Nombre maximum d'octets escomptés dans le champ de données de la réponse

Réponse de commande READ BINARY

Champ de données	Discrétionnaire DO « 53 »
SW1-SW2	« 9000 » Traitement normal Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

Tableau 7. Codage P1-P2 de la commande READ BINARY avec INS = B1

P1								P2								Signification
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	EF sélectionné
0	0	0	0	0	0	0	0	0	0	0	Pas tous égaux					Identificateur EF court
Pas tous zéro											X	X	X	X	X	Identificateur EF

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 ISO/IEC 7816-4 : « BER-TLV length fields »).

Pour des raisons de performance, la durée des communications entre le DVLM-e et le terminal DEVRAIT être aussi courte que possible. Le champ de longueur et le champ de valeur de l'objet de données BER-TLV DEVRAIENT donc 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 : « 0001 » est codé comme suit : Tag = « 54 » Longueur = « 01 » Valeur = « 01 » ;
- Décalage : « FFFF » est codé comme suit : Tag = « 54 » Longueur = « 02 » Valeur = « FFFF ».

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.

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.

Note 1.— Dans certains cas, il existe des DVLM-e où 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.

Note 2.— 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.

3.7 Traitement des dossiers et commandes (SDL2)

Les dossiers de voyage, les dossiers de visa et les certificats DOIVENT être stockés dans un EF sous les applications respectives et avoir une structure linéaire avec des dossiers de taille variable. Voir les figures 4 et 5.

Les dossiers de chaque EF DOIVENT être référencés par un numéro de dossier. Chaque numéro de dossier DOIT être unique et séquentiel (la référence zéro du dossier sélectionné est hors du champ d'application du présent document).

Dans chaque EF prenant en charge une structure linéaire, les numéros de dossier DOIVENT être attribués de manière séquentielle lors de l'ajout, par exemple dans l'ordre de création ; le premier dossier (numéro un) est le premier dossier créé.

Les commandes ISO/IEC 7816-4 suivantes DOIVENT être utilisées pour l'accès aux dossiers :

- APPEND RECORD — ajout de dossiers de voyage, de dossiers de visas, de certificats ;
- READ RECORD(S) — lecture d'un ou de plusieurs dossiers de voyage, dossiers de visas, certificats ;
- SEARCH RECORD — recherche d'un ou de plusieurs dossiers de voyage, dossiers de visas, certificats.

Note.— Les sigles utilisés dans cette sous-section sont définis dans ISO/IEC 7816-4.

3.7.1 Commande APPEND RECORD (ajout de dossier)

Cette commande amorce l'ajout d'un nouveau dossier à la fin d'une structure linéaire.

Tableau 8. Commande APPEND RECORD (ajout de dossier)

CLA	« 0C »
INS	« E2 »
P1	« 00 » (toute autre valeur est invalide)
P2	Voir le Tableau 10
Champ Lc	Longueur du champ de données de la commande
Champ de données	Dossier à ajouter
Champ Le	Absent

Tableau 9. Réponse à APPEND RECORD

Champ de données	Absent
SW1-SW2	« 9000 » Traitement normal ; « 6A84 » Pas assez d'espace mémoire dans le fichier ; « 6700 » Longueur incorrecte (le dossier à ajouter est plus long que la longueur maximale spécifiée) ; Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

Tableau 10. Codage de P2 dans la commande APPEND RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Signification
x	x	x	x	x	-	-	-	Identificateur EF court
-	-	-	-	-	0	0	0	Toute autre valeur est RFU

3.7.2 Commande READ RECORD (lecture de dossier)

Cette commande renvoie le contenu complet ou partiel d'un ou de plusieurs dossiers adressés au EF sélectionné. En fonction de la taille du dossier et du contenu du champ Le, le champ de données de réponse contient l'un des éléments suivants :

- la première partie du dossier traité ;
- un (ou plusieurs) dossier(s) complet(s) traité(s) ;
- un (ou plusieurs) dossier(s) complet(s) traité(s), suivi(s) de la première partie du dossier suivant.

Voir ISO/IEC 7816-4 pour plus de détails et l'appendice H pour un exemple de lecture d'un dossier de voyage.

La Figure 2 illustre le champ de données de réponse. La comparaison de Nr avec la structure TLV indique si le dossier unique (lecture d'un dossier) ou le dernier dossier (lecture de tous les dossiers) est incomplet, complet ou rempli.

Tableau 11. Commande READ RECORD (lecture de dossier)

CLA	« 0C »	
INS	« B2 »	
P1	Numéro de dossier (« 00 » fait référence au dossier actuel)	
P2	Voir le Tableau 13	
Champ Lc	Absent	
Champ de données	INS = « B2 »	Absent
Champ Le	Nombre maximum d'octets à lire encodés comme champ de longueur étendue ; Le = « 00 00 00 » (toute autre valeur est hors du champ de la spécification)	

Tableau 12. Réponse de READ RECORD

Champ de données	Lecture des données
SW1-SW2	« 9000 » Traitement normal ; « 6A83 » (dossier non trouvé) ; Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

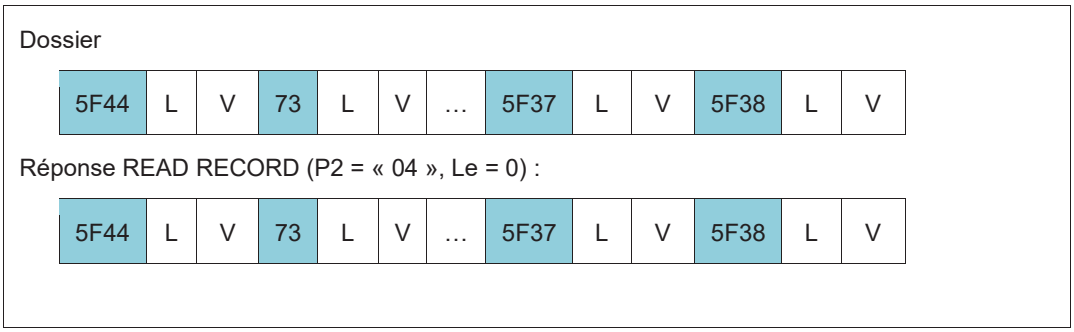
Tableau 13. Codage de P2 dans la commande READ RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Signification
x	x	x	x	x	-	-	-	Identificateur EF court
-	-	-	-	-	1	x	x	**Numéro de dossier dans P1**
-	-	-	-	-	1	0	0	— Lecture de dossier P1
-	-	-	-	-	1	0	1	— Lire tous les dossiers de P1 jusqu'au dernier

Note 1.— Les autres combinaisons de bits sont hors du champ d'application de cette spécification. Si le champ Le ne contient que des octets définis sur « 00 », la commande doit lire complètement soit le dossier unique demandé, soit la séquence de dossiers demandée, en fonction des bits 3, 2 et 1 de P2 et dans la limite de la longueur maximale prise en charge pour le champ Le étendu.

Note 2.— La commande READ RECORD avec des champs de longueur courte est hors du champ d'application de cette spécification.

Cas a — Lecture complète d'un dossier (le champ Le ne contient que des octets définis sur « 00 »)



Cas b — Lecture de plusieurs dossiers jusqu'à la fin du fichier (le champ Le ne contient que des octets définis sur « 00 »)

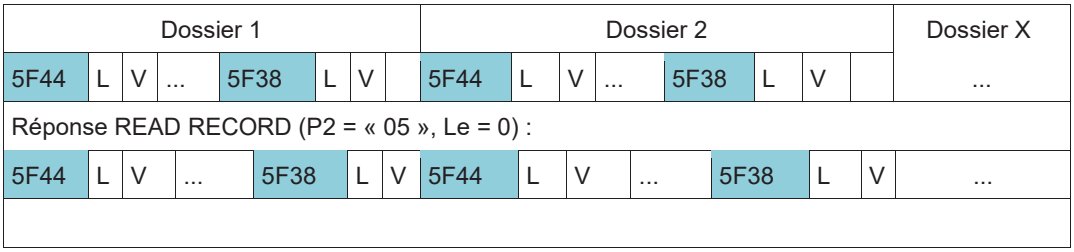


Figure 2. Champs de données de réponse

3.7.3 Commande SEARCH RECORD (rechercher dans le dossier)

Cette commande lance une recherche sur les dossiers stockés dans l'EF concerné. Le champ de données de la commande contient le traitement de dossier DO « 7F76 » définissant la référence du fichier, la configuration de la recherche et la chaîne de recherche (voir le Tableau 17). Le champ de données de réponse renvoie le traitement de

dossier DO « 7F76 » contenant un ou plusieurs DO « 02 » et contenant le numéro de dossier correspondant aux critères de recherche dans l'EF adressé.

Dans un EF prenant en charge des dossiers de taille variable avec une structure linéaire, la recherche PEUT NE PAS prendre en compte les dossiers dont la fenêtre de recherche est plus courte que la chaîne de recherche.

Tableau 14. Commande SEARCH RECORD (rechercher dans le dossier)

CLA	« 0C »
INS	« A2 »
P1	« 00 »
P2	Voir le Tableau 16
Champ Lc	Longueur du champ de données de la commande
Champ de données	Traitement des dossiers DO « 7F76 » (voir Tableau 17)
Champ Le	« 00 » (longueur courte) ou « 00 00 » (longueur étendue)

Tableau 15. Réponse SEARCH RECORD

Champ de données	Gabarit de traitement de dossier DO « 7F76 » contenant une référence de fichier DO « 51 » avec un ou plusieurs entiers DO « 02 » et contenant un numéro de dossier correspondant aux critères de recherche
SW1-SW2	« 9000 » Traitement normal ; « 6282 » Avertissement : Recherche infructueuse Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

Note.— Le champ de données de réponse peut être absent si aucune correspondance n'est trouvée.

Tableau 16. Codage de P2 dans la commande SEARCH RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Signification
1	1	1	1	1	0	0	0	Recherche d'un dossier par le biais de plusieurs EF
Toute autre valeur est RFU.								

Tableau 17. Gabarit de traitement de dossier pour la recherche améliorée de dossiers multiples

Étiquette	Valeur				Notes
« 7F76 »					Traitement de dossier DO
	Étiquette	**Valeur**			
	« 51 »	Identificateur de fichier ou identificateur EF court			Référence du fichier DO
	« A1 »				Gabarit de configuration de recherche
		Étiquette	**Valeur**		
		« 80 »	« 00 » / « 30 »		Paramètre de configuration de la recherche : - recherche dans l'ordre ascendant de numéro de dossier - largeur de pas pour la recherche : octet par octet - fin de la recherche : « 00 » - rechercher tous les dossiers adressés « 30 » - arrêter la recherche après la première correspondance
		« B0 »			Gabarit de fenêtre de recherche
			Étiquette	**Valeur**	
			« 02 »	Décalage	
			« 02 »	Nombre d'octets	
	Étiquette	**Valeur**			
	« A3 »				Gabarit de chaîne de recherche
		Étiquette	**Valeur**		
		« B1 »			
			Étiquette	**Valeur**	
			« 81 »	Chaîne de recherche	

Note 1.— Un DO de décalage vide dans le gabarit de fenêtre de recherche n'est pas pris en charge.

Note 2.— Si le gabarit de fenêtre de recherche utilise la valeur « 00 » pour le nombre d'octets, la puce du DVLM-e SLD2 DOIT rechercher tous les octets à partir du décalage dans les dossiers.

Note 3.— La commande SEARCH RECORD ne prend en charge que les DO spécifiés dans le Tableau 17. Cela implique que la commande SEARCH RECORD prend en charge exactement un DO de référence de fichier dans le DO de traitement de dossier et exactement une chaîne de recherche dans le gabarit de chaîne de recherche. La commande PEUT ignorer les DO supplémentaires ou répondre avec un code d'erreur si des DO supplémentaires sont utilisés.

3.8 Traitement des fichiers transparents et autres (SDL2)

Les EF transparents biométriques supplémentaires sont créées par l'émetteur du DVLM-e SDL2 dans l'état opérationnel désactivé (le mécanisme de création est hors du champ de cette spécification). À l'état désactivé, l'EF peut être sélectionné, écrit, mis à jour et lu avec les autorisations appropriées.

Les commandes ISO/IEC 7816-4 suivantes DOIVENT être utilisées pour l'écriture et la lecture des EF transparents biométriques supplémentaires :

- UPDATE BINARY (mise à jour binaire) écrire des données biométriques supplémentaires ;
- READ BINARY (lire binaire) lire des éléments biométriques supplémentaires.

La commande ISO/IEC 7816-9 suivante DOIT être utilisée pour activer l'EF transparent après que les conditions d'accès en lecture et en écriture du SDL2 ont été satisfaites :

- ACTIVATE (activer) activation des éléments biométriques supplémentaires EF.

Note.— Les sigles utilisés dans cette sous-section sont définis dans ISO/IEC 7816-4.

À l'état activé, l'EF peut être sélectionné et lu avec les autorisations appropriées (liées à l'état activé), et aucune autorisation d'aucune sorte ne permet d'écrire ou d'ajouter l'EF transparent.

La commande FILE AND MEMORY MANAGEMENT (FMM) DOIT être utilisée avant l'écriture pour déterminer si l'espace mémoire disponible dans l'EF est suffisant.

L'IS DOIT utiliser la séquence d'écriture suivante pour l'EF.Biometrics :

- La première commande UPDATE BINARY (INS impair) DOIT contenir les DO suivants dans le champ de données :
  - DO « 54 » contenant le décalage « 00 » ;
  - DO « 53 » qui PEUT contenir le premier bloc des données à stocker. Ce DO PEUT être vide (« 53 00 ») ;
  - Propriétaire DO « C0 » indiquant la taille totale EF (taille de la mémoire à allouer) est facultative.

  Note 1.— Le DVLM-e SDL2 PEUT utiliser les informations relatives à la taille de l'EF dans DO « C0 » pour l'attribution de la mémoire interne (p. ex. pour une attribution dynamique explicite de la mémoire). Si le DVLM-e SDL2 ne prend pas en charge l'information sur la taille des EF DO (p. ex. la mémoire a été allouée statiquement par l'émetteur, ou le DVLM-e SDL2 prend en charge la réallocation dynamique implicite de la mémoire EF), alors le DVLM-e SDL2 PEUT ignorer le DO « C0 », procéder à l'écriture du premier bloc de l'EF et renvoyer « 9000 », ou il PEUT renvoyer l'erreur « 6A80 » pour paramètre incorrect dans le champ de données de commande.

  Note 2.— Si le DVLM-e SDL2 renvoie une erreur en réponse à UPDATE BINARY avec le DO propriétaire « C0 », l'IS DOIT envoyer la commande norme ISO/IEC 7816-4 UPDATE BINARY (INS impair) avec décalage zéro DO « 54 » et DO « 53 », sans le DO « C0 ».

- Les commandes UPDATE BINARY suivantes (INS impair, sans DO « C0 ») DEVRAIENT utiliser le décalage n+1, où n désigne le nombre d'octets écrits jusqu'à présent dans l'EF biométrique,

c'est-à-dire que le terminal DEVRAIT écrire séquentiellement les données EF sans qu'il y ait d'écart ou de chevauchement entre les deux commandes UPDATE BINARY consécutives.

- La commande READ BINARY PEUT être utilisée après toute commande UPDATE BINARY pour vérifier les données écrites dans l'EF.

- La commande ACTIVATE DOIT finaliser la personnalisation de l'EF biométrique en désactivant définitivement l'écriture dans l'EF.

3.8.1 Commande UPDATE BINARY (mise à jour binaire)

Un CI sans contact qui prend en charge l'application d'éléments biométriques supplémentaires DOIT prendre en charge la commande UPDATE BINARY avec l'octet INS impair « D7 » conformément au Tableau 18.

La valeur de l'objet de données décalés BER-TLV dans le champ de données de la commande spécifie le décalage ; la valeur de l'objet de données discrétionnaire BER-TLV dans le champ de données de la commande spécifie les données à écrire ; la valeur de l'objet de données taille des fichiers BER-TLV facultatif dans le champ de données de la commande spécifie la taille totale de l'EF. Les champs de longueur de ces objets de données BER-TLV doivent être codés aussi brièvement que possible.

Lorsque le champ de données de commande de la commande UPDATE BINARY est propriétaire de DO « C0 », le bit 8 de l'octet CLA de la commande APDU DOIT être réglé sur 1 (CLA = « 8C »).

Tableau 18. Commande UPDATE BINARY avec INS impair

CLA	« 0C / 8C »
INS	« D7 »
P1	Identificateur de fichier « 00 00 » identifie l'EF actuel
P2	
Lc	Longueur du champ de données de la commande
Champ de données	Objet de données décalé (étiquette « 54 ») || Objet de données discrétionnaire (étiquette « 53 ») || Objet de données sur la taille du fichier (étiquette « C0 ») (optionnel)
Le	Absent

Tableau 19. Réponse UPDATE BINARY (mise à jour binaire)

Champ de données	Absent
SW1-SW2	« 9000 » Traitement normal ; « 6A84 » (pas assez d'espace mémoire dans le fichier) « 6A80 » Paramètres incorrects dans le champ de données de commande (p. ex. DO « C0 » non pris en charge) « 6982 » Statut de sécurité non satisfait : L'EF.Biometrics est en état d'activation EF Autres valeurs pour indiquer les erreurs de vérification ou d'exécution

Si l'IS ne suit pas la séquence UPDATE BINARY telle que spécifiée à la section 3.8 (c'est-à-dire que la première mise à jour binaire ne commence pas au décalage 0), la puce du DVLM-e du SDL2 PEUT terminer la commande UPDATE BINARY avec une erreur.

3.8.2 Commande ACTIVATE (activer)

La commande ACTIVATE permet de faire passer des éléments biométriques supplémentaires de l'EF sélectionné de l'état désactivé à l'état activé.

Tableau 20. Commande ACTIVATE (activer)

CLA	« 0C »
INS	« 44 »
P1	« 00 »
P2	« 00 »
Lc	Absent
Champ de données	Absent
Le	Absent

Tableau 21. Réponse ACTIVATE

Champ de données	Absent
SW1-SW2	« 9000 » Traitement normal ; Autres valeurs pour indiquer les erreurs de vérification ou d'exécution *Note 1.— SW1-SW2 = « 61XX » (traitement normal) et SW1-SW2 = « 62XX » ou « 63XX » (traitement d'avertissement) sont hors du champ d'application de ce document.*

Après l'exécution réussie de cette commande, l'EF.Biometrics actuellement sélectionné DOIT passer à l'état Activé. Si une erreur se produit (SW différent de « 9000 »), l'EF.Biometrics actuellement sélectionné DOIT rester à l'état désactivé.

Immédiatement après l'exécution réussie de cette commande (SW1-SW2 = « 9000 »), l'autorisation effective requise pour effectuer une action sur l'EF.Biometrics DOIT être celle qui correspond à l'état Activated (conformément au Tableau 98). L'autorisation effective correspondant à l'état désactivé NE DOIT PAS lever de droits d'accès pour l'EF.Biometrics.

3.8.3 Commande FILE AND MEMORY MANAGEMENT (gestion des fichiers et de la mémoire)

La commande FILE AND MEMORY MANAGEMENT (FMM) adresse une requête sur la taille de la mémoire utilisée ou libre pour le EF adressé. Cette commande est adressée au DVLM-e du SDL2 en tant que propriétaire. Cette commande peut être utilisée pour vérifier l'espace libre disponible pour l'EF adressé avant d'écrire ou d'ajouter. Cette commande peut également être utilisée afin d'obtenir le dernier numéro de dossier ajouté pour la

lecture. P1 indique la méthode d'adressage EF, l'EF actuel ou la référence de fichier DO « 51 » peuvent être utilisés. P2 indique le contenu SDL2 de la requête. Le nombre total d'octets dans l'EF adressé avec structure transparente ou de dossier et le nombre de dossiers existants ou restants pour l'EF du dossier adressé sont fournis. Le nombre total d'octets comprend les octets disponibles dans l'EF sans aucune information structurelle. Ce nombre exclut toute information structurelle qui pourrait être requise par la puce du DVLM-e SDL2. L'hypothèse pour le nombre de dossiers restants est que la taille de tous les dossiers restants est maximale. Après une commande FMM réussie, l'EF référencé devient l'EF actuel.

Tableau 22. Commande FILE AND MEMORY MANAGEMENT (FMM) (Gestion des fichiers et de la mémoire)

CLA	« 8C »	
INS	« 5F »	
P1	Voir le Tableau 23	
P2	Voir le Tableau 24	
Lc	Absent pour le codage Nc = 0, présent pour le codage Nc > 0	
Champ de données	P1 = « 00 »	Absent
	P1 = « 01 »	Référence du fichier DO « 51 » (Voir ISO/IEC 7816-4)
Le	« 00 »	

P1 spécifie la méthode de sélection EF. P2 contient une carte binaire spécifiant quelles informations DOIVENT être incluses dans la réponse.

Tableau 23. Codage de P1 dans la commande FFM

b8	b7	b6	b5	b4	b3	b2	b1	Signification
0	0	0	0	0	0	0	0	EF actuel
0	0	0	0	0	0	0	1	Référence du fichier DO « 51 » dans le champ de données de la commande
Toute autre valeur est RFU.								

Tableau 24. Codage de P2 dans la commande FFM

b8	b7	b6	b5	b4	b3	b2	b1	Signification
-	-	-	-	-	-	-	1	Nombre total d'octets dans l'EF adressé
-	-	-	-	-	-	1	-	Nombre de dossiers restants dans le dossier EF adressé
-	-	-	-	-	1	-	-	Nombre de dossiers existants dans le dossier EF adressé
x	x	x	x	x	-	-	-	00000 (toute autre valeur est RFU)
Toute autre valeur est RFU.								

Tableau 25. Codage du DO « 51 » dans le champ de données de la commande FMM

Étiquette	Longueur	Valeur
« 51 »	1	Identificateur EF court (les bits b8 à b4 codent un nombre de 1 à 30 ; les bits b3 à b1 sont mis à 000)
	2	Identificateur de fichier

La réponse à la commande FMM contient un ensemble de DO représentant les informations demandées sur le fichier et la taille de la mémoire.

Tableau 26. Réponse de commande FMM

Champ de données	Information absente ou de contrôle selon P2. Voir le Tableau 27.
SW1-SW2	« 9000 », erreurs de contrôle ou d'exécution conformément à l'ISO/IEC 7816-4

Tableau 27. FILE AND MEMORY MANAGEMENT (gestion des fichiers et de la mémoire)

Étiquette	Longueur	Valeur		
« 7F78 »	Var	Gestion des fichiers et de la mémoire des DO		
		Étiquette	**Len**	**Valeur**
		« 81 »	Var	Nombre total d'octets dans l'EF adressé
		« 82 »	Var	Nombre de dossiers restants dans le dossier EF adressé
		« 83 »	Var	Nombre de dossiers existants dans le dossier EF adressé

Note 1.— La puce du DVLM-e du SDL2 DOIT renvoyer uniquement les objets de données dans le DO FMM qui sont demandés par le biais de P2.

Note 2.— Les données de réponse du FMM sont valables uniquement pour l'EF spécifié. Les données de réponse FMM provenant de différents EF peuvent ne pas être indépendantes, par exemple si différents EF partagent la mémoire disponible. L'IS devrait en tenir compte s'il combine les données de réponse du FMM de différents EF.

Note 3.— Lorsque la messagerie sécurisée est appliquée à la commande FMM, la messagerie sécurisée DO « 85 » DOIT être utilisée pour l'encapsulation des données de commande cryptées.

3.9 Spécifications relatives à la structure des fichiers

Les informations contenues dans un DVLM-e du SDL2 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.

Note.— La nécessité d'avoir un fichier principal dépend du choix des systèmes d'exploitation, applications SDL1 ou SDL2, et des conditions optionnelles d'accès.

3.9.1 Codage des données

Les types de codage suivants sont autorisés pour les éléments de données :

A = caractère alphabétique [a-z, A-Z] ;
N = caractère numérique [0-9] ;
S = caractère spécial [« < »] ;
B = données binaires ;
U = caractères UNICODE codés en UTF-8.

Codage UTF-8 des caractères UNICODE :

- pour tout caractère inférieur ou égal à 127 (hex « 7F »), le codage UTF-8 utilise un octet qui est identique à la valeur ASCII ;

- pour les caractères inférieurs ou égaux à 2 047 (hex « 07FF »), le codage UTF-8 utilise deux octets ;

  - le premier octet a deux bits de poids fort activés et le troisième bit désactivé (c'est-à-dire hex « C2 » à « DF ») ;

  - le deuxième octet a le bit de poids fort activé et le second bit désactivé (c'est-à-dire « 80 » à « BF ») ;

- pour tous les caractères supérieurs ou égaux à 2 048 et inférieurs à 65 535 (hex « FFFF »), le codage UTF-8 utilise trois octets.

3.10 Sélection d'application — DF

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

- L'application DVLM-e du SDL1 est OBLIGATOIRE ;

  - l'application DVLM-e du SDL1 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.SOD) ;

  - l'objet de sécurité du document (EF.SOD) dans l'application DVLM-e du SDL1 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 du SDL1.

- l'application DVLM-e du SDL1 PEUT éventuellement prendre en charge les applications SLD2 supplémentaires décrites dans le Doc 9303 comme :

  - demande de dossiers de voyage ;

- demande de dossiers de visa ;

- application d'éléments biométriques supplémentaires.

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.

Les applications SDL1 et SDL2 DOIVENT être sélectionnées en utilisant l'identifiant d'application (AID) comme nom de DF réservé. L'AID DOIT être constituée de l'identifiant d'application enregistré attribué par l'ISO selon la norme ISO/IEC 7816-5 et d'une extension d'identifiant d'application propriétaire (PIX) spécifiée dans le présent document :

Le contexte de l'application DVLM-e SDL1 utilise deux schémas différents d'attribution d'étiquettes pour l'étiquette de classe d'application, tels que définis dans le Doc 9303-10 (étiquette SDL) et l'ISO/IEC 7816-6 (étiquette intersectorielle) :

- EF.ATR/INFO et EF.DIR utilisent le schéma d'attribution d'étiquette intersectorielle ;

- les DF et leurs EF utilisent le schéma d'attribution d'étiquette SDL.

Les étiquettes intersectorielles spécifiées dans ce document sont utilisées dans le contexte de la SDL, de sorte qu'un schéma d'attribution d'étiquettes coexistantes n'est pas nécessaire.

3.11 Fichiers élémentaires communs (EF)

Les EF communs suivants pour les applications SDL1 et SDL2 PEUVENT exister dans le MF (fichier principal) :

- EF.ATR/INFO ;

- EF.DIR ;

- EF.CardAccess ;

- EF.CardSecurity.

3.11.1 EF.ATR/INFO (CONDITIONNEL)

EF.ATR/INFO est un EF transparent contenu dans le fichier principal et il est REQUIS à titre conditionnel si l'application optionnelle SDL2 est présente. Cet EF est optionnel si seule l'application SDL1 est présente. L'identificateur EF court au niveau du MF est « 01 ».

Tableau 28. EF.ATR/INFO

Nom de fichier	EF.ATR/INFO
ID de fichier	« 2F01 »
Identificateur EF court	« 01 »
Sélectionner l'accès	TOUJOURS
Accès en lecture	TOUJOURS
Accès en écriture/en mise à jour/en effacement	JAMAIS
Structure du fichier	Transparent
Taille	Variable

Le contenu du fichier EF.ATR/INFO peut être récupéré en utilisant la commande SELECT suivie de la commande READ BINARY. Le champ de données de la réponse à la commande READ BINARY contient le contenu du fichier EF.ATR/INFO.

Tableau 29. Éléments de données du fichier EF.ATR/INFO pour SDL2

Étiquette	Longueur	Valeur	Notes
« 47 »	« 03 »	**Capacités des cartes**	
		octet 1 - première fonction du logiciel	b8 = 1 : sélection de DF par nom complet de DF b7 à b4 et b1 sont en dehors du champ d'application du Doc 9303 b3 = 1 : EF court pris en charge b2 = 1 : numéro de dossier pris en charge
		octet 2 - deuxième fonction du logiciel	b8, b7, b6 et b5 sont hors du champ d'application du doc 9303 b4 to b1 = 0001 : taille de l'unité de données d'un octet
		octet 3 - troisième fonction du logiciel	b8 = 1 : prise en charge du chaînage des commandes b7 = 1 : les champs Lc et Le étendus prennent en charge b6 = 1 : informations sur la longueur étendue dans le fichier EF.ATR/INFO b5 à b1 sont hors du champ d'application du Doc 9303

« 7F66 »	Var	**Informations sur la longueur étendue**			
		Étiquette	**Longueur**	**Valeur**	**Notes**
		« 02 »	Var	entier positif — le nombre maximum d'octets dans une commande APDU	DOIT être au moins 1 000 (décimal) pour SDL2
		« 02 »	Var	entier positif — le nombre maximum d'octets attendus dans l'APDU de réponse	DOIT être au moins 1 000 (décimal) pour SDL2

Note 1.— D'autres objets de données PEUVENT être présents dans le fichier EF.ATR/INFO.

Note 2.— EF.ATR/INFO utilise le schéma d'attribution d'étiquettes intersectorielles tel que défini dans l'ISO/IEC 7816-4.

3.11.2 EF.DIR (CONDITIONNEL)

EF.DIR est un EF transparent contenu dans le fichier principal défini par l'ISO/IEC 7816-4. EF.DIR est conditionnellement REQUIS si des applications optionnelles SDL2 sont présentes. Si des applications SDL2 optionnelles sont présentes, le fichier EF.DIR DOIT être inclus dans les SecurityInfos présent dans le fichier EF.CardSecurity. Une description complète de SecurityInfo pour le fichier EF.DIR se trouve dans le Doc 9303-11. L'identificateur EF court au niveau du MF est « 1E ».

Tableau 30. EF.DIR

Nom de fichier	EF.DIR
ID de fichier	« 2F00 »
Identificateur EF court	« 1E »
Sélectionner l'accès	TOUJOURS
Accès en lecture	TOUJOURS
Accès en écriture/en mise à jour/en effacement	JAMAIS
Structure du fichier	Transparent
Taille	Variable

Il est RECOMMANDÉ que le fichier EF.DIR soit présent dans le MF. Le fichier EF.DIR DOIT être présent si plus que l'application SDL1 obligatoire est présente et indiquer une liste d'applications supportées par le DVLM-e. Il DOIT contenir un ensemble de gabarits d'application contenant des identifiants d'application DO dans n'importe quel ordre.

Tableau 31. Format du fichier EF.DIR

<table>
<tr><th>Étiquette</th><th>L</th><th colspan="3">Valeur</th><th>Description</th></tr>
<tr><td>« 61 »</td><td>« 09 »</td><td colspan="3"></td><td>Gabarit d'application DVLM-e du SDL1</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Étiquette</td><td>L</td><td>Valeur</td><td rowspan="2">Application DVLM-e du SDL1 Internationale
AID : « A0 00 00 02 47 10 01 »</td></tr>
<tr><td>« 4F »</td><td>« 07 »</td><td>« A0 00 00 02 47 10 01 »</td></tr>
<tr><td>« 61 »</td><td>« 09 »</td><td colspan="3"></td><td>Gabarit d'application de dossiers de voyage</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Étiquette</td><td>L</td><td>Valeur</td><td rowspan="2">Dossiers de voyage International AID :
« A0 00 00 02 47 20 01 »</td></tr>
<tr><td>« 4F »</td><td>« 07 »</td><td>« A0 00 00 02 47 20 01 »</td></tr>
<tr><td>« 61 »</td><td>« 09 »</td><td colspan="3"></td><td>Gabarit d'application de dossiers de visa</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Étiquette</td><td>L</td><td>Valeur</td><td rowspan="2">Dossiers de visa International AID :
« A0 00 00 02 47 20 02 »</td></tr>
<tr><td>« 4F »</td><td>« 07 »</td><td>« A0 00 00 02 47 20 02 »</td></tr>
<tr><td>« 61 »</td><td>« 09 »</td><td colspan="3"></td><td>Gabarit d'application d'éléments biométriques supplémentaires</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Étiquette</td><td>L</td><td>Valeur</td><td rowspan="2">Éléments biométriques supplémentaires internationaux AID :
« A0 00 00 02 47 20 03 »</td></tr>
<tr><td>« 4F »</td><td>« 07 »</td><td>« A0 00 00 02 47 20 03 »</td></tr>
</table>

Note.— Le fichier EF.DIR utilise le schéma standard d'attribution d'étiquette tel que défini dans l'ISO/IEC 7816-4.

3.11.3 EF.CardAccess (CONDITIONNEL)

Le fichier EF.CardAccess est un EF 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. Une description complète de SecurityInfos pour PACE peut être trouvée dans le Doc 9303-11.

L'identificateur EF court au niveau du MF est « 1C ».

Tableau 32. EF.CardAccess

Nom de fichier	EF.CardAccess
ID de fichier	« 011C »
Identificateur EF court	« 1C »
Sélectionner l'accès	TOUJOURS
Accès en lecture	TOUJOURS
Accès en écriture/en mise à jour/en effacement	JAMAIS
Structure du fichier	Transparent
Taille	Variable

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

- `PACEInfo` ;
- `PACEDomainParameterInfo`.

Tableau 33. Stockage du fichier EF.CardAccess dans le CI

Nom de fichier	EF.CardAccess
ID de fichier	« 011C »
ID EF court	« 1C »
Accès en lecture	TOUJOURS
Accès en écriture	JAMAIS
Taille	Variable
Contenu	DER encoded SecurityInfos. Voir le Doc 9303-11.

3.11.4 Fichier EF.CardSecurity (CONDITIONNEL)

Le fichier EF.CardSecurity est un EF 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.

L'identificateur EF court au niveau du MF est « 1D ».

Le fichier EF.CardSecurity contenu dans le MF est REQUIS si :

- PACE avec mappage d'authentification de puce est pris en charge par le CI ;
- l'authentification du terminal dans le MF est prise en charge par le CI ; ou
- l'authentification de la puce dans le MF est prise en charge par le CI.

et DOIT contenir :

- les informations ChipAuthenticationInfo requises pour l'authentification de la puce ;
- les informations ChipAuthenticationPublicKeyInfo requises pour l'authentification PACE-CAM/Chip ;
- les informations TerminalAuthenticationInfo requises pour l'authentification du terminal ;
- les informations de sécurité SecurityInfos contenues dans le fichier EF.CardAccess.

Le fichier EF.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-e 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 34. Stockage du fichier EF.CardSecurity sur le CI

Nom de fichier	EF.CardSecurity
ID de fichier	« 011D »
ID EF court	« 1D »
Accès en lecture	PACE
Accès en écriture	JAMAIS
Taille	Variable

Le fichier CardSecurity DOIT être mis en œuvre sous forme de données signées (SignedData) conformément à RFC 3369 avec le type de contenu id-SecurityObject dans le champ encapContentInfo. Les objets de sécurité DOIVENT être signés par le signataire du document. Le certificat de signataire du document DOIT être inclus dans les données signées (SignedData). L'identificateur d'objet suivant DOIT être utilisé pour identifier le type de contenu :

```
bsi-de OBJECT IDENTIFIER ::= {
    itu-t(0) identified-organization(4) etsi(0)
    reserved(127) etsi-identified-organization(0) 7
}
id-SecurityObject OBJECT IDENTIFIER ::= {
    bsi-de applications(3) eID(2) 1
}
```

La structure des données SignedData est définie comme suit :

```
SignedData ::= SEQUENCE{
    version CMSVersion,
    digestAlgorithmes DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONNEL,
    crls [1] IMPLICIT RevocationInfoChoices OPTIONNEL,
    signerInfos
}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

EncapsulatedContentInfo ::= SEQUENCE {
    eContentType ContentType,
    eContent [0] EXPLICIT OCTET STRING OPTIONNEL
}
```

```
ContentType ::=  OBJECT IDENTIFIER

SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
    version CMSVersion,
    sid SignerIdentifier,
    digestAlgorithm DigestAlgorithmIdentifiers,
    signedAttrs [0] IMPLICIT SignedAttributes OPTIONNEL,
    signatureAlgoritm SignatureAlgorithmIdentifier,
    signature SignatureValue,
    unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONNEL
}

SignerIdentifier ::= CHOICE {
    issuerAndSerialNumber IssuerAndSerialNumber,
    subjectKeyIdentifier [0] SubjectKeyIdentifier
}

SignatureValue ::= OCTET STRING
```

4. APPLICATION DVLM-e SDL1 (OBLIGATOIRE)

La structure DVLM-e du SDL1 fournit un espace pour stocker et signer numériquement les éléments de données obligatoires et facultatifs qui peuvent être utilisés pour relier le titulaire au document. Les informations stockées dans la partie DVLM-e du SDL1 du DVLM-e deviennent statiques au moment de la délivrance, et ne peuvent être modifiées d'aucune manière. Cette fonction est nécessaire pour garantir la protection des informations personnelles et pour faciliter la détection de la falsification des documents. Bien que la version DVLM-e du SLD1 comprenne des champs de données facultatifs qui pourraient être utilisés pour étendre l'utilisation du DVLM-e (c.-à-d. des éléments biométriques supplémentaires, le passage automatisé à la frontière, etc.), l'exigence de protéger en écriture l'application à puce du DVLM-e SDL1 au moment de la délivrance est OBLIGATOIRE.

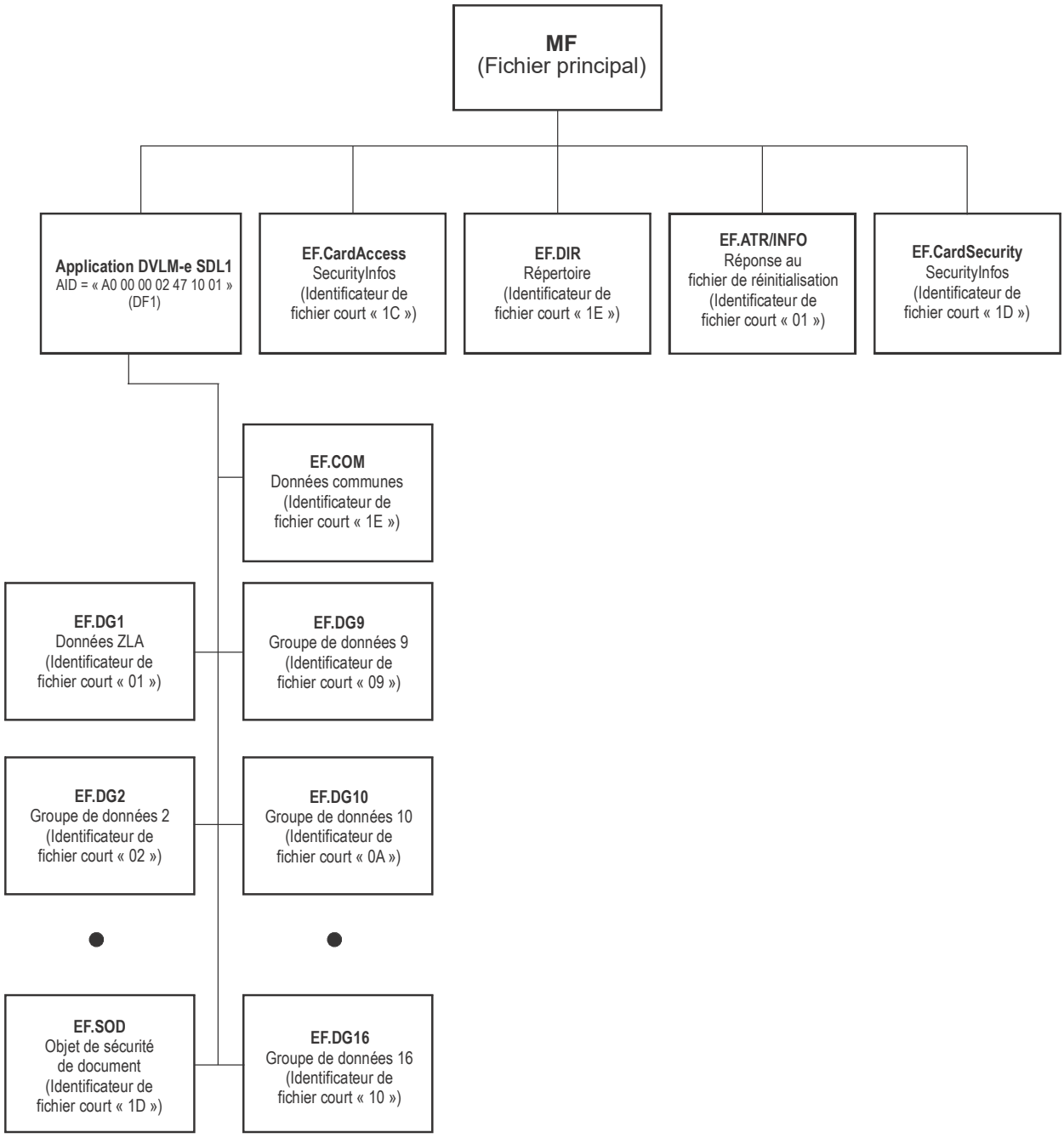


Figure 3. Résumé de la structure du fichier DVLM-e du SDL1

4.1 Sélection d'application — DF

L'application DVLM-e du SDL1 DOIT être sélectionnée en utilisant l'identification d'application (AID) comme nom de DF réservé. L'AID DOIT être constituée de l'identifiant d'application enregistré attribué par l'ISO selon la norme ISO/IEC 7816-5 et d'une extension d'identifiant d'application propriétaire (PIX) spécifiée dans le présent document :

- l'identifiant d'application enregistré est : « A000000247 » ;
- l'application de données stockée de l'émetteur DOIT utiliser PIX = « 1001 » ;
- l'AID complète de l'application DVLM-e du SLD1 est : « A0 00 00 02 47 10 01 ».

Le CI DOIT rejeter la sélection d'une application si l'extension pour cette application est absente.

4.2 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.

4.3 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 :

Afin de 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 SDL1 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.

4.4 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.

4.5 Exigences de la SDL

La technologie d'expansion de la capacité du CI sans contact utilisée dans un DVLM-e SDL1 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 structure de données logique (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.

4.5.1 Sécurité

Seul l'État émetteur ou l'organisation émettrice DOIT avoir 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. Une fois la puce verrouillée (après la personnalisation et avant la délivrance), il n'est plus possible d'y inscrire, de modifier ou de supprimer des données de l'application SLD1. Après délivrance, une puce verrouillée ne peut plus être déverrouillée.

4.5.2 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 EF distinct (EF.SOD). 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.

4.5.3 Ordonnancement de la SDL

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

4.5.4 Capacité de stockage de données du CI sans contact

La capacité de stockage de données du CI sans contact est à la discrétion de l'État émetteur, mais DOIT être au minimum de 32 ko. Cette capacité minimale est nécessaire pour stocker l'image faciale obligatoire, 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.

Lorsque l'infrastructure ICP d'un État n'est pas disponible pour signer les données du DVLM-e SDL1 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 SDL1 soit laissé vierge et soit verrouillé. Le DVLM-e SDL1 DEVRAIT contenir une annotation appropriée à cet effet. Cette circonstance devrait être exceptionnelle.

4.5.5 Stockage d'autres données

Un État PEUT utiliser la capacité de stockage du CI sans contact dans un DVLM-e pour étendre la capacité de données lisibles par machine du DVLM-e SDL1 au-delà de celle définie pour l'interopérabilité mondiale. Il peut s'agir, par exemple, de fournir un accès lisible par une machine aux informations des documents de l'éleveur (p. ex. les détails du certificat de naissance), aux détails de confirmation de l'identité personnelle stockée (biométrie) et/ou de vérification de l'authenticité des documents.

4.5.6 Norme internationale pour le codage des données biométriques

La norme ISO/IEC 39794 a succédé à l'ISO/IEC 19794:2005 comme norme internationale pour le codage des données biométriques. La table de temps de transition suivante a été définie :

- les systèmes d'inspection DOIVENT être en mesure de traiter les données ISO/IEC 39794 d'ici le 1-1-2026, après une période de préparation de six ans débutant le 1-1-2020 ;
- entre 2026 et 2030, les États émetteurs et les organisations émettrices peuvent utiliser les formats de données spécifiés dans la norme ISO/IEC 19794-X:2005 ou dans la norme ISO/IEC 39794-X pendant une période de transition de quatre ans. Pendant cette période de transition, les tests d'interopérabilité et de conformité seront essentiels ;
- à partir du 1-1-2030, les émetteurs de passeports DOIVENT utiliser la norme ISO/IEC 39794-X pour le codage des données biométriques.

Le rapport technique de l'OACI, ISO/IEC 39794-5, Profil d'application des DVLM-e[1], fournit des orientations sur la transition de l'ISO/IEC 19794:2005 à l'ISO/IEC 39794.

La structure de données logique des DVLM-e comprend le DG2, visage (obligatoire), le DG3, empreinte(s) digitale(s) (optionnel), et le DG4, iris (optionnel). Chaque groupe de données comporte des données biométriques qui sont codées conformément aux normes internationales afin de maintenir l'interopérabilité au niveau international.

Tous les DG mentionnés ci-dessus (DG2, DG3 et DG4) DOIVENT utiliser le gabarit du groupe de gabarits d'informations biométriques (BIT), avec BIT imbriqués (voir le Doc 9303-10). La structure des BIT imbriqués comprend des données biométriques qui peuvent être codées selon l'un des deux types de normes suivants : la série ISO/IEC 19794, première édition, et la série ISO/IEC 39794.

Les données biométriques codées selon la série ISO/IEC 19794, première édition, sont enregistrées dans l'objet de données étiqueté « 5F2E », alors que les données biométriques codées selon la série ISO/IEC 39794 sont enregistrées dans l'objet de données étiqueté « 7F2E ».

Tableau 1 : Étiquettes de données biométriques

Étiquette	Nº de norme
5F2E	Série ISO/IEC 19794, première édition
7F2E	Série ISO/IEC 39794

Les données biométriques enregistrées dans l'objet de données étiqueté « 7F2E » DOIVENT utiliser la structure de données figurant dans le tableau ci-après.

1. Pour renseignements, consulter la page www.icao.int/security/fal/trip.

Tableau 2 : Structure de données du DO « 7F2E »

Étiquette	L	Valeur				
7F2E	Var	Gabarit de données biométriques défini par la norme ISO/IEC 7816-11.				
		Étiquette	**L**	**Valeur**		
		A1	Var	Données biométriques en format normalisé (construit)		
				Étiquette	**L**	**Valeur**
				64, 65 ou 66	Var	DO défini par la série ISO/IEC 39794, tableau 3.

Tableau 3 : Étiquettes pour les DO définis par la norme ISO/IEC 39794

Nº de norme	Étiquette
ISO/IEC 39794-4	64
ISO/IEC 39794-5	65
ISO/IEC 39794-6	66

4.6 fichiers élémentaires (EF) DVLM-e SDL1

4.6.1 *Information sur l'en-tête et la présence de groupes de données EF.COM (OBLIGATOIRE)*

L'EF.COM est situé dans l'application DVLM-e SDL1 (identificateur de fichier court = « 1E ») 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 SLD1 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 35. 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.

(PAGE LAISSÉE EN BLANC INTENTIONNELLEMENT)

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.

Il est RECOMMANDÉ que les systèmes d'inspection qui dépendent de l'EF.COM soient modifiés pour utiliser dès que possible le SO_D décrit dans la version 1.8.

4.6.1.1 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 4.6 du présent document. Le format normalisé pour le numéro de version de SDL est « aabb », où :

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

4.6.1.2 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 dans la section 4.7.1 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.

4.6.2 Objet de sécurité du document EF.SOD (OBLIGATOIRE)

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

Tableau 36. Étiquettes EF.SOD

Étiquette	L	Valeur
« 77 »	Var	Objet de sécurité du document

Il existe actuellement deux versions disponibles de l'objet de sécurité du document EF.SOD. Il existe l'EF.SOD V0 traditionnel qui se trouve à l'appendice D et le RECOMMANDÉ EF.SOD V1 dans cette section. Un seul EF.SOD est REQUIS et autorisé.

4.6.2.1 Objet de sécurité du document EF.SOD V1 pour la SDL v1.8

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 LDSVersionInfo OPTIONAL
   -- Si elle est présente, la version DOIT être V1
}
LDSVersionInfo ::= SEQUENCE {
   ldsVersion PrintableString,
   unicodeVersion PrintableString }
```

4.6.2.2 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 dans le format des 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 37. Type de données signées pour SO_D V1

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.

Valeur		Observations
Certificates	m	Il est REQUIS des États qu'ils incluent 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 qu'une seule 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	
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.

4.6.2.3 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

-- 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
```

```
-- Identifiants 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 PrintableString
   unicodeVersion PRINTABLE STRING }
END
```

Note 1.— Le champ valeur du groupe de données `(dataGroupHashValue)` *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. Le système d'inspection DOIT accepter le champ* `DigestAlgorithmIdentifiers` *avec les deux conditions, c'est-à-dire des paramètres absents et des paramètres* `NULL`.

4.7 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 EF court, comme le montre le Tableau 38. 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 38. Éléments de données obligatoires et facultatifs qui se combinent pour former la structure des groupes de données 1 (DG1) à 16 (DG16)

Groupe de données	Nom du fichier EF	Identificateur EF court	Identificateur EF	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 »
DG10	EF.DG10	« 0A »	« 01 0A »	« 6A »
DG11	EF.DG11	« 0B »	« 01 0B »	« 6B »
DG12	EF.DG12	« 0C »	« 01 »	« 6C »
DG13	EF.DG13	« 0D »	« 01 0D »	« 6D »

Groupe de données	Nom du fichier EF	Identificateur EF court	Identificateur EF	Étiquette
DG14	EF.DG14	« 0E »	« 01E »	« 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	« 01 »	« 2F 01 »	
Commun	EF.CardSecurity	« 1D »	« 01 1D »	

4.7.1 GROUPE DE DONNÉES 1 — Informations de la zone de lecture automatique (OBLIGATOIRE)

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 SDL1 (format TD1, TD2 ou TD3).

Cet élément de données contient les renseignements de la ZLA REQUIS pour le document dans le gabarit « 61 ». Le gabarit contient un objet de données, la ZLA dans l'objet de données « 5F1F ». 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 39. Étiquettes du groupe de données 1

Étiquette	L	Valeur		
« 61 »	Var			
		Étiquette	**L**	**Valeur**
		« 5F1F »	Var	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.)

4.7.1.1 GROUPE DE DONNÉES 1 — Éléments de données du EF.DG1 pour un DVLM-e SDL1 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, parties 3 et 5. Les éléments de données et leur format dans chaque zone du groupe de données pour le format TD1 DOIVENT figurer dans le tableau suivant :

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

Tableau 40. Éléments de données pour le format TD1

Élément de données	Optionnel ou OBLIGATOIRE	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

4.7.1.2 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, parties 3 et 6. Les éléments de données et leur format dans chaque zone du groupe de données pour le format TD2 DOIVENT figurer dans le tableau suivant :

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

Tableau 41. Éléments de données pour le format TD2

Élément de données	Optionnel ou OBLIGATOIRE	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

4.7.1.3 GROUPE DE DONNÉES 1 — Éléments de données du EF.DG1 pour un DVLM-e SDL1de 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, parties 3 et 4. Les éléments de données et leur format dans chaque zone du groupe de données pour le format TD3 DOIVENT figurer dans le tableau suivant :

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

Tableau 42. Éléments de données pour le format TD3

Élément de données	Optionnel ou OBLIGATOIRE	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

4.7.2 GROUPE DE DONNÉES 2 — Éléments d'identification codés — Visage (OBLIGATOIRE)

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 43. Étiquettes du groupe de données 2

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

4.7.2.1 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 44. Groupe de données 2 — Étiquettes de codage biométrique

Étiquette	L	Valeur				
7F61	Var	Gabarit de groupe de gabarits 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)
				« 85 »	« 08 »	Période de validité (de – à –) (optionnel)
				« 86 »	« 04 »	Créateur des données de référence biométriques (PID) (optionnel)
				« 87 »	« 02 »	Propriétaire de format (REQUIS)

Étiquette	L	Valeur				
				« 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). Voir section 4.5.6.	

L'OID par défaut de CBEFF est utilisé. L'objet de données OID (étiquette « 06 ») juste au-dessous du gabarit d'informations biométriques (BIT, étiquette « 7F60 ») 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.

Note.— L'ISO/IEC 39794 succédera à l'ISO/IEC 19794:2005 en tant que norme internationale pour le codage des données biométriques. Voir section 4.5.6.

4.7.2.2 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 45. Éléments de données du DG2

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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 l'élément de données 01.
03	M	Codage(s) de données biométriques du visage		Var	B	L'élément de données peut se reproduire, comme défini par l'élément de données 01.

4.7.3 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 46. Étiquettes du groupe de données 3

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

4.7.3.1 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 47. Étiquettes imbriquées du groupe de données 3

Étiquette	L	Valeur				
« 7F61 »	Var	Gabarit de groupe de gabarits 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)

Étiquette	L	Valeur				
				« 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). Voir section 4.5.6.	
		Étiquette	**L**			
		« 7F60 »	Var	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
				« 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). Voir section 4.5.6.	

L'OID par défaut de CBEFF est utilisé. L'objet de données OID (étiquette « 06 ») juste au-dessous du gabarit d'informations biométriques (BIT, étiquette « 7F60 ») 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 19794-4.

Note.— L'ISO/IEC 39794 succédera à l'ISO/IEC 19794:2005 en tant que norme internationale pour le codage des données biométriques. Voir section 4.5.6.

4.7.3.2 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 48. Éléments de données du DG3

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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 l'élément de données 01.
03	M [si les éléments codés de doigt(s) sont enregistrés]	Codage(s) de données biométriques de doigt(s)		Var	B	L'élément de données peut se reproduire, comme défini par l'élément de données 01.

4.7.3.2.1 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 49. 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

b8	b7	b6	b5	b4	b3	b2	b1	Sous-type d'élément biométrique
			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

4.7.3.2.2 Codage de zéro instance

Les États qui émettent des DVLM-e SDL1 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 SDL1 dont les éléments biométriques ne sont pas présents ou remplis au moment de l'émission du DVLM-e SDL1 mais dont le DG3 est déclaré. Pour des fins d'interopérabilité, les États qui utilisent les empreintes digitales dans leurs DVLM-e SDL1 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 SDL1. Dans ce cas, le compteur de gabarit indique une valeur de « 00 ».

Il est RECOMMANDÉ d'ajouter une étiquette « 53 » avec contenu défini par l'émetteur (p. ex., un nombre aléatoire).

Tableau 50. Codage de zéro instance

<table>
<tr><th>Étiquette</th><th>L</th><th colspan="5">Valeur</th></tr>
<tr><td>« 63 »</td><td>Var</td><td colspan="5">Élément SDL</td></tr>
<tr><td></td><td></td><th>Étiquette</th><th>L</th><th colspan="3">Valeur</th></tr>
<tr><td></td><td></td><td>« 7F 61F »</td><td>« 03 »</td><td colspan="3">Gabarit de groupe d'informations biométriques</td></tr>
<tr><td></td><td></td><td></td><td>« 02 »</td><td>« 01</td><td>« 00 »</td><td>Indique qu'aucun gabarit d'informations biométriques n'est enregistré dans ce groupe de données.</td></tr>
<tr><td></td><td></td><td>« 53 »</td><td>Var</td><td colspan="3">Contenu défini par l'émetteur (p. ex., un nombre aléatoire).</td></tr>
</table>

4.7.3.2.3 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 51. Codage d'une instance

<table>
<tr><th>Étiquette</th><th>L</th><th colspan="7">Valeur</th></tr>
<tr><td>63</td><td>Var</td><td colspan="7">Élément SDL, aa étant la longueur totale de tout le contenu des données SDL.</td></tr>
<tr><td></td><td></td><td>Étiquette</td><td>L</td><td colspan="5">Valeur</td></tr>
<tr><td></td><td></td><td>« 7F 61F »</td><td>Var</td><td colspan="5">Gabarit de groupe d'informations biométriques</td></tr>
<tr><td></td><td></td><td></td><td>« 02 »</td><td>« 01 »</td><td>« 01 »</td><td colspan="3">Indique le nombre total d'empreintes digitales enregistrées dans les gabarits d'informations biométriques qui suivent.</td></tr>
<tr><td></td><td></td><td></td><td>« 7F 60 »</td><td>Var</td><td colspan="5">1er gabarit d'informations biométriques, cc étant la longueur totale de tout le BIT.</td></tr>
<tr><td></td><td></td><td></td><td></td><td>« A1 »</td><td>Var</td><td colspan="3">Gabarit d'en-tête biométrique</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>« 81 »</td><td>« 01 »</td><td>« 08 »</td><td>Type d'élément biométrique :
« empreinte digitale »</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>« 82 »</td><td>« 01 »</td><td>« 0A »</td><td>Sous-type d'élément biométrique :
« index gauche »</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>« 87 »</td><td>« 02 »</td><td>« 01 01 »</td><td>Propriétaire de format :
JTC 1 SC 37</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>« 88 »</td><td>« 02 »</td><td>« 00 07 »</td><td>Type de format :
ISO/IEC 19794-4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td colspan="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.</td></tr>
<tr><td></td><td></td><td></td><td></td><td>« 5F 2E »</td><td>Var</td><td colspan="3">Données biométriques. Le bloc de données biométriques DOIT contenir exactement une image d'empreinte digitale.</td></tr>
</table>

Note.— L'ISO/IEC 39794 succédera à l'ISO/IEC 19794:2005 en tant que norme internationale pour le codage des données biométriques. Voir section 4.5.6.

4.7.3.2.4 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 52. Codage de plus d'une instance

Étiquette	**L**	**Valeur**						
« 63 »	Var	Élément SDL, *aa* étant la longueur totale de tout le contenu de données SDL.						
		Étiquette	**L**	**Valeur**				
		« 7F 61F »	Var	Gabarit de groupe de gabarits d'informations biométriques.				
			« 02 »	« 01 »	« 02 »	Indique le nombre total d'empreintes digitales enregistrées dans les gabarits d'informations biométriques qui suivent.		
			« 7F 60 »	Var	1er gabarit d'informations biométriques.			
				« A1 »	Var	Gabarit d'en-tête biométrique.		
					« 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 »	Var	Bloc de données biométriques. Le bloc de données biométriques DOIT contenir exactement une image d'empreinte digitale.		
			« 7F 60 »	Var	Deuxième gabarit d'informations biométriques.			
				« A1 »	Var	Gabarit d'en-tête biométrique.		
					« 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

Étiquette	L	Valeur						
					« 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 »	Var	Bloc de données biométriques. Le bloc de données biométriques DOIT contenir exactement une image d'empreinte digitale.		

Note.— L'ISO/IEC 39794 succédera à l'ISO/IEC 19794:2005 en tant que norme internationale pour le codage des données biométriques. Voir section 4.5.6.

4.7.4 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 53. Étiquettes du groupe de données 4

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

4.7.4.1 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 54. Étiquettes imbriquées du groupe de données 4

Étiquette	L	Valeur		
« 7F61 »	Var	Gabarit de groupe de gabarits 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

Étiquette	L	Valeur				
			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)
				« 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). Voir section 4.5.6.	
		Étiq.	**L**	**Valeur**		
		« 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)
				« 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). Voir section 4.5.6.	

L'OID par défaut de CBEFF est utilisé. L'objet de données OID (étiquette « 06 ») juste au-dessous du gabarit d'informations biométriques (BIT, étiquette « 7F60 ») 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 19794-6.

Note.— L'ISO/IEC 39794 succédera à l'ISO/IEC 19794:2005 en tant que norme internationale pour le codage des données biométriques. Voir section 4.5.6.

4.7.4.2 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 55. Éléments de données du DG4

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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 l'élément de données 01.
03	M [si l'élément codé de l'œil (des yeux) est inclus]	Codage(s) de données biométriques de l'œil (des yeux)		Var	B	L'élément de données peut se reproduire, comme défini par l'élément de données 01.

4.7.4.2.1 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 56. 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

4.7.4.2.2 Codage de zéro instance

Les États qui émettent des DVLM-e SDL1 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 SDL1 dont les éléments biométriques ne sont pas présents ou remplis au moment de l'émission du DVLM-e SDL1 mais dont le DG4 est déclaré. Pour des fins d'interopérabilité, les États qui utilisent les iris dans leurs DVLM-e SDL1 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 SDL1. Dans ce cas, le compteur de gabarit indique une valeur de « 00 ».

Il est RECOMMANDÉ d'ajouter une étiquette « 53 » avec contenu défini par l'émetteur (p. ex., un nombre aléatoire).

Tableau 57. Codage de zéro instance

Étiquette	L	Valeur				
« 76 »	Var	Élément SDL				
		Étiq.	**L**	**Valeur**		
		« 7F 61F »	« 03 »	Gabarit de groupe de gabarits 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).		

4.7.4.2.3 Codage d'une instance

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

4.7.4.2.4 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.

4.7.5 GROUPE DE DONNÉES 5 — Portrait affiché (OPTIONNEL)

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

Tableau 58. 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 59. Formats DG5

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

4.7.5.1 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 60. Éléments de données du DG5

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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 par l'élément de données 01.
03	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.
04	M (si le portrait affiché est enregistré)	Représentation du portrait affiché		Var	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.

4.7.6 GROUPE DE DONNÉES 6 — Réservé pour usage futur

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

Tableau 61. Étiquettes du groupe de données 6

Étiquette	L	Valeur
« 66 »	Var	

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

Les éléments de données attribués au DG6 sont réservés pour usage futur.

4.7.7 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 62. 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 (EXGIÉ 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 63. Formats DG7

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

4.7.7.1 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 au sein de chaque DG7 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 64. Éléments de données du DG7

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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	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.

4.7.8 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 (DG8) DOIVENT être les suivants :

Tableau 65. 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.

4.7.8.1 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 66. Éléments de données du DG8

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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 les éléments de données 02 à 03).
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, U,B	Format défini à la discrétion de l'État émetteur ou de l'organisation émettrice.

4.7.9 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 (DG9) DOIVENT être les suivants :

Tableau 67. 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.

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

Les éléments de données du 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 68. Éléments de données du DG9

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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 les éléments de données 02 à 03).
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	B	

4.7.10 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 (DG10) DOIVENT être les suivants :

Tableau 69. Étiquettes du groupe de données 10

<table>
<tr><th>Étiquette</th><th>L</th><th colspan="3">Valeur</th></tr>
<tr><td>« 6A »</td><td>Var</td><td colspan="3"></td></tr>
<tr><td></td><td></td><th>Étiquette</th><th>L</th><th>Valeur</th></tr>
<tr><td></td><td></td><td>« 02 »</td><td>« 01 »</td><td>Entier — Nombre d'instances de ce type de gabarit (REQUIS dans le premier gabarit. Non utilisé dans les gabarits suivants.)</td></tr>
<tr><td></td><td></td><td></td><td>Var</td><td>À définir.</td></tr>
</table>

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

La présente section décrit les éléments de données qui peuvent être présents dans le 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 70. Éléments de données du DG10

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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 les éléments de données 02 et 03).
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, U,B	Format défini à la discrétion de l'État émetteur ou de l'organisation émettrice.

4.7.11 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 71. 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.
		« 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			Information sur la garde du document

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

La présente section décrit les éléments de données qui peuvent être présents dans le 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.— Le DG11 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 72. Éléments de données du DG11

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre 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	U	Texte libre.
04	O	Date de naissance complète	8	F	N	AAAAMMJJ
05	O	Lieu de naissance	99 Max	Var	U	Texte libre.
06	O	Adresse	99 Max	Var	U	Texte libre.
07	O	Téléphone	99 Max	Var	N,S	Texte libre. Codage recommandé UIT-T E.164
08	O	Profession	99 Max	Var	U	Texte libre.
09	M si l'élément de données 08 est inclus	Titre	99 Max	Var	U	Texte libre.
10	M si l'élément de données 09 est inclus	Résumé personnel	99 Max	Var	U	Texte libre.
11	M si l'élément de données 10 est inclus	Preuve de citoyenneté		Var	B	Image du document de citoyenneté formatée selon l'ISO/IEC 10918-1.
12	O	Autre(s) document(s) de voyage valide(s)	99 Max	Var	U	Texte libre, séparé par <.

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage	Exigences de codage
		Numéro du document de voyage				
13	O	Information sur la garde du document	999 Max	Var	U	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.

4.7.12 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 73. 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 »).
		« 5F1B »	Var			Mentions, observations
		« 5F1C »	Var			Exigences fiscales/de sortie
		« 5F1D »	Var			Image du recto du document. Image selon l'ISO/IEC 10918.

Étiquette	L	Valeur				
		« 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.

4.7.12.1 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, 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 74. Éléments de données du DG12

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	O	Autorité de délivrance	99 Max	Var	U	Texte libre.
02	O	Date d'émission	8	F	N	Date d'émission du document : c-à-d. AAAAMMJJ
03	O	Détails sur autre(s) personne(s)	99 Max	Var	U	Texte libre.
04	O	Mention(s)/ observation(s)	99 Max	Var	U	Texte libre.
05	O	Exigences fiscales/ de sortie	99 Max	Var	U	Texte libre.
06	O	Image du recto du DVLM-e		Var	B	Formaté conformément à l'ISO/IEC 10918-1
07	O	Image du verso du DVLM-e		Var	B	Formaté conformément à l'ISO/IEC 10918-1

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage	Exigences de codage
08	O	Date et heure de personnalisation	14	F	N	ssaammjjhhmmss
09	O	Numéro de série du système de personnalisation	99 Max	Var	U	Texte libre.

4.7.13 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 75. Étiquettes du groupe de données 13

Étiquette	L	Valeur
« 6D »	Var	

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

Le groupe de données 14 (DG14) 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 DVLM-e est REQUIS si la puce du DVLM-e prend en charge l'authentification de puce ou le PACE-GM/-IM.

Tableau 76. Étiquettes du groupe de données 14

Étiquette	L	Valeur
« 6E »	Var	Voir Doc 9303-10 DG14 SecurityInfos

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

La présente section décrit les éléments de données qui peuvent être présents dans le 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 77. Éléments de données du DG14

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage	Exigences de codage
	O	SecurityInfos		Var	B	Voir SecurityInfos du DG14, Doc 9303-10, § 4.7.14.2.

4.7.14.2 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.

4.7.15 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 78. Étiquettes du groupe de données 15

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

4.7.15.1 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 79. Éléments de données du DG15

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage	Exigences de codage
	O	ActiveAuthenticationPublicKeyInfo		Var	B	Voir le Doc 9303-11.

4.7.16 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 groupe de données 16 (DG16), comme tous les autres groupes de données, NE DEVRAIT PAS être mis à jour après sa publication ; le DG16 est représenté par une valeur de hachage dans le SO_D et le SO_D n'est signé qu'une seule fois à l'émission.

Tableau 80. 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 »	« 08 »			Date d'enregistrement des données
« 5F51 »	Var			Nom de la personne
« 5F52 »	Var			Téléphone
« 5F53 »	Var			Adresse

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

La présente section décrit les éléments de données qui peuvent être présents dans le 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, F = champ de longueur fixe, Var = champ de longueur variable.

Tableau 81. Éléments de données du DG16

Élément de données	Optionnel ou OBLIGATOIRE	Nom de l'élément de données	Nombre d'octets	Fixe ou variable	Type de codage	Exigences de codage
01	M si DG16 est inclus	Nombre de personnes identifiées	1	F	N	Identifie le nombre de personnes incluses dans le groupe de données.
02	M si DG16 est inclus	Détails de date enregistrés	8	F	N	Date enregistrée pour la notification ; format = AAAAMMJJ
03	M si DG16 est inclus	Nom de la personne à aviser Identifiants principal et secondaire		Var	A,N,S	Caractères de remplissage (<) insérés selon la ZLA. Troncation non autorisée.
04	M si l'élément de données 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). Codage recommandé UIT-T E.164.
05	M	Adresse de la personne à aviser		Var	U	Texte libre.

5. APPLICATIONS SDL2 (OPTIONNEL)

La structure de données logiques 2 (SDL2) est une extension facultative et rétrocompatible de la puce SDL1 du DVLM-e qui permettrait le stockage numérique et sécurisé des informations relatives aux voyages, après la délivrance du document. La SDL2 étend l'utilisation du DVLM-e par l'ajout d'applications qui pourraient permettre le stockage numérique de données de voyage (visas et tampons de voyage), et d'autres informations susceptibles de faciliter le voyage du titulaire (des éléments biométriques supplémentaires), pendant sa période de validité. Le fait de mieux exploiter tout le potentiel du DVLM-e en « numérisant » le reste des données contenues dans les documents offre une série d'avantages en matière de facilitation, tout en protégeant davantage le document contre des vulnérabilités telles que la contrefaçon, la copie et la lecture ou l'écriture non autorisées.

Les applications supplémentaires et optionnelles décrites comme SDL2 sont :

- dossiers de voyage (tampons) ;
- dossiers électroniques ;
- éléments biométriques supplémentaires.

Il est OBLIGATOIRE que l'application DVLM-e SDL1 soit présente avant que toute application OPTIONNELLE SDL2 puisse être déclarée.

5.1 Application pour les dossiers de voyage (CONDITIONNEL)

L'application de dossiers de voyage PEUT être mise en œuvre par un État émetteur ou une organisation émettrice. Les éléments suivants sont E REQUIS à titre conditionnel si l'application optionnelle dossiers de voyage a été invoquée.

Les dossiers de voyage d'entrée et de sortie sont stockés dans deux fichiers élémentaires distincts, EF.EntryRecords et EF.ExitRecords, sous l'application DF dossiers de voyage, tous deux ayant une structure linéaire avec des enregistrements de taille variable conformément à la norme ISO/IEC 7816-4. Les certificats de signataire de dossiers de voyage sont stockés dans un fichier élémentaire EF.Certificates séparé, ayant une structure linéaire avec des dossiers de taille variable.

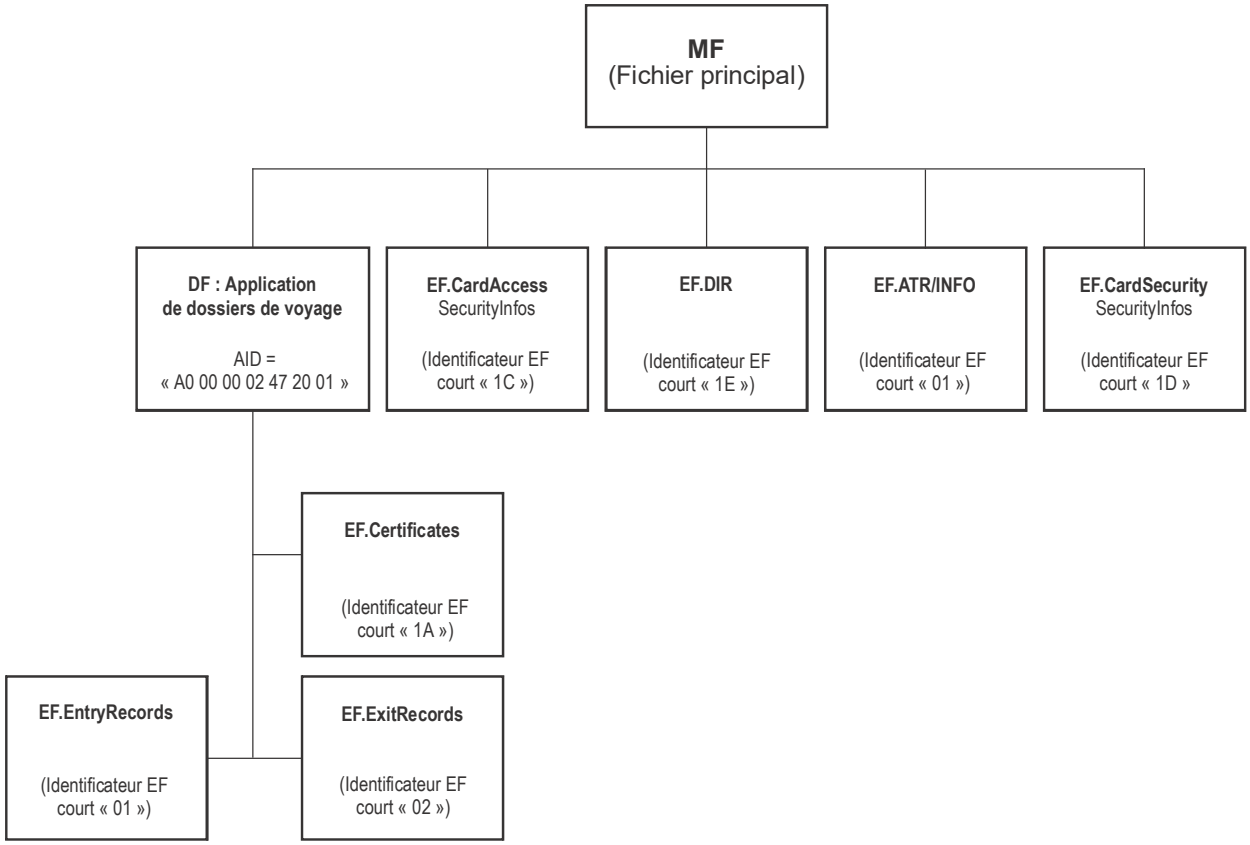


Figure 4. Structure des dossiers de voyage

5.1.1 Sélection d'application — DF

L'application de dossiers de voyage DOIT être sélectionnée en utilisant l'identifiant d'application (AID) comme nom de DF réservé. L'AID DOIT être constituée de l'identifiant d'application enregistré attribué par l'ISO selon la norme ISO/IEC 7816-5 et d'une extension d'identifiant d'application propriétaire (PIX) de l'application de dossiers de voyage :

- l'identifiant de l'application enregistrée est « A0 00 00 02 47 » ;
- l'application dossiers de voyage DOIT utiliser PIX = « 20 01 » ;
- l'AID complète de l'application Dossiers de voyage DOIT être « A0 00 00 02 47 20 01 ».

Si l'autorisation effective n'accorde de droits d'accès à aucune donnée dans une application SDL2, la sélection de cette application DOIT être rejetée par le CI.

5.1.2 EF.Certificates (OBLIGATOIRE)

Les certificats de signataire de dossiers de voyage sont stockés dans un EF dans l'application DF et ont une structure linéaire avec des dossiers de taille variable. Ces certificats sont destinés à être utilisés par le IS pour poursuivre la validation hors ligne des signatures numériques pour chaque dossier dans les fichiers EF.ExitRecords et EF.EntryRecords.

Tableau 82. EF.Certificates

Nom de fichier	EF.Certificates
ID de fichier	« 011A »
Identificateur EF court	« 1A »
Accès sélectionner / FMM	PACE+TA (autorisation de dossier de voyage bit b3 selon le Tableau 96)
Accès à lecture de dossier / recherche de dossier	PACE+TA (autorisation de dossier de voyage bit b3 selon le Tableau 96)
Accès à ajout de dossier	PACE+TA (autorisation de dossier de voyage bit b4 selon le Tableau 96)
Accès à écriture de dossier / mise à jour de dossier	JAMAIS
Accès à effacement de dossier	JAMAIS
Structure du fichier	Structure linéaire avec des dossiers de taille variable
Taille	Variable

Le dossier de certificat contient un seul certificat d'objet de données SDL2-TS de signataire X.509. Un dossier de certificat PEUT être référencé par un ou plusieurs dossiers de voyage entrée ou sortie.

Tableau 83. Format de dossier du fichier EF.Certificates

Étiquette	Contenu	Obligatoire /Optionnel	Format	Exemple
« 5F3A »	Numéro de série du certificat	M	V(22)B	« 5F3A » « Len » (Code pays || Numéro de série)
« 72 »	Certificat X.509	M	V (900) B	« 72 » « Len » (Certificat X.509)

Note.— Les étiquettes intersectorielles spécifiées dans ce tableau sont utilisées dans le contexte du SDL, de sorte qu'un schéma d'attribution d'étiquettes coexistantes n'est pas nécessaire.

DO « 5F3A » DOIT contenir un code de pays à deux lettres conformément au Doc 9303, Partie 3 (même codage et même valeur que le nom du pays émetteur du certificat X.509 figurant sur le certificat du sujet) suivi du numéro de série du certificat.

Chaque certificat X.509 contient un ensemble d'éléments de données codés ASN.1 illustrés dans le Tableau 84. Se référer aux exigences détaillées pour le certificat X.509 dans la spécification du profil de certificat du Doc 9303-12.

Tableau 84. Exemple de structure de certificat X.509

Champ			Description	Exemple de valeur
Certificat				
	version		Doit être version 3	2
	numéro de série		Entier positif unique	20 octets maximum
	signature		Algorithme de signature	ecdsa-with-SHA256
	émetteur			
		nom du pays	Nom du pays émetteur	« États-Unis »
		nom courant	Nom de l'émetteur (9 caractères maximum.)	« DHSCA0001 »
	validité			
		pas avant	Date d'entrée en vigueur du certificat	« 131225000000Z »
		pas après	Date d'expiration du certificat	« 230824235959Z »
	sujet			
		nom du pays	Nom du pays IS	« États-Unis »
		nom courant	Nom de l'IS (9 caractères maximum.)	« SFO000001 »
	subjectPublicKeyInfo			
		Algorithme à clé publique	ecPublicKey	
		Clé publique su sujet	Clé publique de l'IS	Clé publique ECC256

	extensions			
		AuthorityKeyIdentifier		
		ExtKeyUsage		
Algorithme de signature			ecdsa-with-SHA256	
Signature			Signature de l'émetteur	Signature ECDSA256

Note.— Ce tableau est un exemple à titre d'illustration uniquement. Les dossiers de certificats sont écrits dans le fichier EF.Certificates situé sous l'application DF dossier de voyage à l'aide de la commande APPEND RECORD. Les dossiers de certificats peuvent être lus depuis le fichier EF.Certificates en utilisant la commande READ RECORD. Les dossiers de certificats NE DOIVENT PAS être mis à jour ou effacés. Le nombre maximum de dossiers dans un fichier EF.Certificates contenu dans l'application dossier de voyage DF DOIT être de 254.

5.1.3 Fichier EF.ExitRecords (OBLIGATOIRE)

Les dossiers de sortie DOIVENT être ajoutés par un IS autorisé lors de l'embarquement.

Tableau 85. Fichier EF.ExitRecords

Nom de fichier	Fichier EF.ExitRecords
ID de fichier	« 0102 »
Identificateur EF court	« 02 »
Accès sélectionner / FMM	PACE+TA (autorisation de dossier de voyage bit b1 selon le Tableau 96)
Accès à lecture de dossier / recherche de dossier	PACE+TA (autorisation de dossier de voyage bit b1 selon le Tableau 96)
Accès à ajout de dossier	PACE+TA (autorisation de dossier de voyage bit b2 selon le Tableau 96)
Accès à écriture de dossier / mise à jour de dossier	JAMAIS
Accès à effacement de dossier	JAMAIS
Structure du fichier	Structure linéaire avec des dossiers de taille variable
Taille	Variable

Le contenu d'un dossier sortie est présenté dans le tableau 86.

Note.— Les étiquettes intersectorielles spécifiées dans le tableau ci-après sont utilisées dans le contexte du SDL, de sorte qu'un schéma d'attribution d'étiquettes coexistantes n'est pas nécessaire.

Tableau 86. Format de dossier entrée/sortie

Étiquette	Étiquette	Contenu	Obligatoire/ OPTIONNEL	Format	Exemple
« 5F44 »		État d'embarquement/débarquement (copie pour le DOSSIER DE RECHERCHE)	M	F (3) A	États-Unis
« 73 »	Dossier de voyage entrée/sortie (information signée)				
	« 5F44 »	État d'embarquement/débarquement	M	F (3) A	États-Unis
	« 5F4C »	Approbations, refus et révocations de visas	O	V (50) A,N,S,U	Texte libre
	« 5F45 »	Date du voyage (Date d'entrée/de sortie)	M	F (8) N	20120814 (aaaammjj)
	« 5F4B »	Autorité compétente d'inspection	M	V (10) A,N,S	CBP
	« 5F46 »	Lieu d'inspection (port d'entrée/de sortie)	M	V (10) A,N,S	SFO
	« 5F4A »	Référence de l'inspecteur	M	V (20) A,N,S	SFO00001234
	« 5F4D »	Résultat de l'inspection	O	V (50) A,N,S,U	Texte libre
	« 5F49 »	Mode de transport	O	F (1) A	A (air), S (mer), L (terre)
	« 5F48 »	Durée du séjour (jours)	O	V (2) B	« 00FF » (255 jours)
	« 5F4E »	Conditions que le titulaire est tenu de respecter pendant son séjour dans l'État émetteur	O	V(50) A,N,S,U	Texte libre
« 5F37 »	Jeton d'authenticité (Signature)		M	V (140) B	« 5F » « 37 » Len (Signature)
« 5F38 »	Référence (numéro de dossier) au certificat de signataire SDL2-TS dans le stock de certificats		M	F (1) B	« 01 » …« FE »

Note 1.— A = caractère alphabétique [a-z, A-Z], N = caractère numérique [0-9], S = caractère spécial [« < »], B = données binaires, F = champ de longueur fixe, V = champ de longueur variable.

Note 2.— Puisque les certificats de signataires SDL2-TS sont susceptibles d'être les mêmes dans plusieurs dossiers de voyage (p. ex. lors de l'entrée et de la sortie d'un pays par le même aéroport n'ayant qu'un seul signataire SDL2-TS), avant l'écriture/l'ajout d'un nouveau certificat dans le fichier EF.Certificates, l'IS doit rechercher dans le fichier EF.Certificates une copie du même certificat et référencer le certificat existant. Cela réduira la taille de l'EF.Certificates et permettra des recherches plus rapides.

Note 3.— Le DVLM-e SDL2 n'impose pas qu'un IS écrive des dossiers d'entrée uniquement dans l'EF.EntryRecords, mais pas dans l'EF.ExitRecords, et vice versa.

Note 4.— Code à trois lettres de l'État d'embarquement/débarquement selon le Doc 9303-3.

L'ordre des objets de données dans un dossier est fixe. L'IS DOIT constituer le contenu du dossier en utilisant les objets de données dans l'ordre spécifié dans le tableau.

Chaque dossier DOIT contenir une signature numérique (jeton d'authenticité) calculée dans le cadre du DO « 73 », y compris l'étiquette 73 et la longueur. La signature est générée par le signataire du SDL2-TS.

Les certificats de signataire du SDL2-TS nécessaires pour vérifier la signature du dossier de voyage DOIVENT être stockés dans le fichier EF.Certificates sous l'application DF dossiers de voyage s'ils ne sont pas déjà disponibles dans le même fichier.

Les dossiers de voyage sont écrits (ajoutés) au fichier EF en utilisant APPEND RECORD. Les dossiers de voyage NE DOIVENT PAS être modifiés (mis à jour) ou supprimés. Le nombre maximum de dossiers autorisés dans chaque fichier EF DOIT être de 254.

5.1.4 Fichier EF.EntryRecords (OBLIGATOIRE)

Les dossiers d'entrée DOIVENT être ajoutés par un IS autorisé lors du débarquement.

Tableau 87. Fichier EF.EntryRecords

Nom de fichier	Fichier EF.EntryRecords
ID de fichier	« 0101 »
Identificateur EF court	« 01 »
Accès sélectionner / FMM	PACE+TA (autorisation de dossier de voyage bit b1 selon le Tableau 96)
Accès à lecture de dossier / recherche de dossier	PACE+TA (autorisation de dossier de voyage bit b1 selon le Tableau 96)
Accès à ajout de dossier	PACE+TA (autorisation de dossier de voyage bit b2 selon le Tableau 96)
Accès à écriture de dossier / mise à jour de dossier	JAMAIS
Accès à effacement de dossier	JAMAIS
Structure du fichier	Structure linéaire avec des dossiers de taille variable
Taille	Variable

La structure du dossier d'entrée est identique à celle du dossier de sortie spécifiée dans le tableau 86.

5.2 Application pour les dossiers de visa (CONDITIONNEL)

L'application des dossiers de visa PEUT être mise en œuvre par un État émetteur ou une organisation émettrice. Les éléments suivants sont REQUIS à titre conditionnel si l'application optionnelle dossiers de visa a été invoquée.

Les dossiers de visa sont stockés dans le fichier élémentaire EF.VisaRecords sous l'application DF dossier de visa. Le fichier EF DOIT avoir une structure linéaire avec des dossiers de taille variable conformément à la norme ISO/IEC 7816-4. Les certificats de signataire de dossiers de visa sont stockés dans un fichier élémentaire EF.Certificates séparé, ayant une structure linéaire avec des dossiers de taille variable.

5.2.1 Sélection d'application — DF

L'application de dossiers de visa DOIT être sélectionnée en utilisant l'identifiant d'application (AID) comme nom de DF réservé. L'AID DOIT être constituée de l'identifiant d'application enregistré attribué par l'ISO selon la norme ISO/IEC 7816-5 et d'une extension d'identifiant d'application propriétaire (PIX) de l'application de dossiers de visa :

- l'identifiant de l'application enregistrée est « A0 00 00 02 47 » ;
- l'application dossiers de visa DOIT utiliser PIX = « 20 02 » ; et
- l'AID complète de l'application Dossiers de visa est : « A0 00 00 02 47 20 02 ».

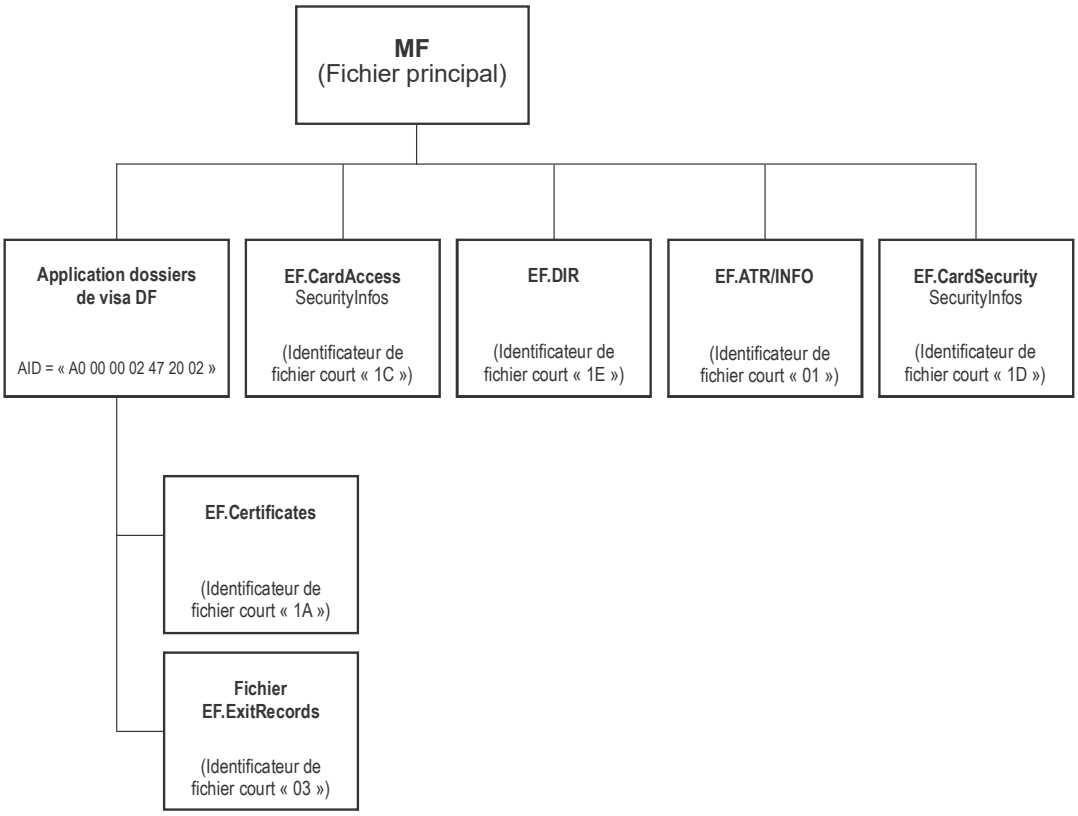


Figure 5. Structure des dossiers de visa

Si l'autorisation effective n'accorde de droits d'accès à aucune donnée dans une application SDL2, la sélection de cette application DOIT être rejetée par le CI.

5.2.2 EF.Certificates (OBLIGATOIRE)

Les certificats de signataire de dossiers de visa sont stockés dans un EF dans l'application DF et ont une structure linéaire avec des dossiers de taille variable. Ces certificats sont destinés à être utilisés par l'IS pour poursuivre la validation hors ligne des signatures numériques pour chaque dossier dans le fichier EF.VisaRecords.

Tableau 88. EF.Certificates

Nom de fichier	EF.Certificates
ID de fichier	« 011A »
Identificateur EF court	« 1A »
Accès sélectionner / FMM	PACE+TA (autorisation de dossier de visa bit b3 selon le Tableau 97)
Accès à lecture de dossier / recherche de dossier	PACE+TA (autorisation de dossier de visa bit b3 selon le Tableau 97)
Accès à ajout de dossier	PACE+TA (autorisation de dossier de visa bit b4 selon le Tableau 97)
Accès à écriture de dossier / mise à jour de dossier	JAMAIS
Accès à effacement de dossier	JAMAIS
Structure du fichier	Structure linéaire avec des dossiers de taille variable
Taille	Variable

Le dossier de certificat contient un seul certificat d'objet de données SDL2-V de signataire X.509. Un dossier de certificat PEUT être référencé par un ou plusieurs dossiers de visa.

La structure du dossier de certificat dans l'application de visa est identique à celle du dossier de certificat dans l'application de dossier de voyage spécifiée dans le Tableau 83.

Les dossiers de certificats sont écrits dans le fichier EF.Certificates situé sous l'application DF dossier de visa à l'aide de la commande APPEND RECORD. Les dossiers de certificats peuvent être lus depuis le fichier EF.Certificates en utilisant la commande READ RECORD. Les dossiers de certificats NE DOIVENT PAS être mis à jour ou effacés. Le nombre maximum de dossiers dans un fichier EF.Certificates contenu dans l'application DF dossier de visa DOIT être de 254.

5.2.3 EF.VisaRecords (OBLIGATOIRE)

Les dossiers de visa DOIVENT être stockés dans le fichier EF.VisaRecords ayant une structure linéaire avec des dossiers de taille variable.

Tableau 89. EF.VisaRecords

Nom de fichier	EF.VisaRecords
ID de fichier	« 0103 »
Identificateur EF court	« 03 »
Accès sélectionner / FMM	PACE+TA (autorisation de dossier de visa bit b1 selon le Tableau 97)
Accès à lecture de dossier / recherche de dossier	PACE+TA (autorisation de dossier de visa bit b1 selon le Tableau 97)
Accès à ajout de dossier	PACE+TA (autorisation de dossier de visa bit b2 selon le Tableau 97)
Accès à écriture de dossier / mise à jour de dossier	JAMAIS
Accès à effacement de dossier	JAMAIS
Structure du fichier	Structure linéaire avec des dossiers de taille variable
Taille	Variable

Chaque dossier de visa DOIT contenir une séquence d'objets de données BER-TLV (DO « 5F28 » et DO « 71 »), suivie du jeton d'authenticité (Signature) DO et du DO a, contenant la référence au certificat de signataire SDL2-V dans EF.Certificates. DO « 71 » contient un ensemble de DO (champs) énumérés dans le tableau ci-après.

Note.— Les étiquettes intersectorielles spécifiées dans le tableau ci-après sont utilisées dans le contexte du SDL, de sorte qu'un schéma d'attribution d'étiquettes coexistantes n'est pas nécessaire.

Tableau 90. Format EF.VisaRecords

Étiquette	Étiquette	Contenu	OBLIGATOIRE/ OPTIONNEL/ CONDITIONNEL	Format	Exemple
« 5F28 »		État émetteur ou organisation émettrice (copie pour SEARCH RECORD)	M	F (3) A	NLD
« 71 »	Dossier de visa (information signée)				
	« 5F28 »	État émetteur ou organisation émettrice	M	F (3) A	NLD
	« 43 »	Type de document	M	F (2) A,N,S	VS
	« 5F71 »	Visa de type A lisible à la machine	O	F (48) A,N,S	
	« 5F72 »	Visa de type B lisible à la machine	O	F (44) A,N,S	VCD<<DENT<<ARTHUR< PHILIP<<<<<<<<<<<

Étiquette	Étiquette	Contenu	OBLIGATOIRE/ OPTIONNEL/ CONDITIONNEL	Format	Exemple
	« 5F73 »	Nombre d'entrées	O	V (1) B	« 01 » – « FF »
	« 5F74 »	Durée du séjour (jours, mois, années)	O	F (3) B	« 010000 » – « FFFFFF »
	« 5F75 »	Numéro du passeport	O	F (9) A,N,S	XI85935F8
	« 5F76 »	Type/classe/catégorie de visa	O	V (4) B	
	« 5F77 »	Information sur le territoire	O	V (8) B	
	« 49 »	Lieu d'émission (autorité de délivrance)	M	V (50) A, Sp	NEW YORK
	« 5F25 »	Date d'entrée en vigueur (date d'émission)	M	F (8) N	20120826 (aaaammjj)
	« 5F24 »	Date d'expiration	M	F (8) N	20130826 (aaaammjj)
	« 5A »	Numéro de document	M	F (9) A,N,S	XI85935F8
	« 5F32 »	Informations complémentaires (annotations : durée, limitations et droits payés)	O	V (50) A,N,S,U	Texte libre
	« 5B »	Nom du titulaire (nom complet)	M	V (50) A, Sp	VAN DER STEEN MARIANNE LOUISE
	« 5F33 »	Identifiant primaire (nom de famille)	M	V (50) A, Sp	VAN DER STEEN
	« 5F34 »	Identifiant secondaire (prénom)	M	V (50) A, Sp	MARIANNE LOUISE
	« 5F35 »	Sexe	M	F (1) A,S	F, M, ou <
	« 5F2B »	Date de naissance	M	F (8) N,S	19870814 (aaaammjj)
	« 5F2C »	Nationalité	M	F (3) A	NLD
	« 5F1F »	MRZ	M	V (50) A,N,S	VAN<DER<STEEN<< MARIANNE<LOUISE
	« 5F40 »	Référence à des éléments biométriques supplémentaires EF	O	F (2) B	« 0201 »
« 5F37 »	Jeton d'authenticité (Signature)		M	V (140), B	« 5F » « 37 » Len {Signature}
« 5F38 »	Référence (numéro de dossier) au certificat de signataire SDL2-V dans le stock de certificats		M	F (1) B	« 01 » …« FE »

Note 1.— A = caractère alphabétique [a-z, A-Z], N = caractère numérique [0-9], S = caractère spécial [« < »], B = données binaires, F = champ à longueur fixe, V = champ à longueur variable, Sp = espace.

Note 2.— Code à trois lettres de l'État émetteur, conformément au Doc 9303-3.

Note 3.— Le DO « 5F40 » optionnel, s'il est présent, DOIT contenir l'identificateur de deux octets de l'EF au sein de l'application éléments biométriques supplémentaires contenant les données biométriques. Ce DO ne peut être utilisé que si l'application éléments biométriques supplémentaires est présente sur le DVLM-e.

L'ordre des objets de données dans un dossier est fixe. L'IS DOIT constituer le contenu du dossier en utilisant les objets de données dans l'ordre spécifié dans le tableau.

Chaque dossier de visa DOIT contenir une signature numérique (jeton d'authenticité) calculée dans le cadre du DO « 71 », y compris l'étiquette 71 et la longueur. La signature est générée par le signataire de la SDL2-V.

Les certificats de signataire SDL2-V nécessaires pour vérifier la signature du dossier de visa sont stockés dans un fichier EF.Certificates distinct, situé sous l'application DF dossier de visa.

Chaque dossier de visa DOIT être ajouté au fichier EF.VisaRecords à l'aide de APPEND RECORD. Les dossiers de visa NE DOIVENT PAS être modifiés (mis à jour) ou supprimés. Le nombre maximum de dossiers autorisés dans chaque fichier EF.VisaRecords DOIT être de 254.

5.3 Application éléments biométriques supplémentaires (CONDITIONNEL)

L'application éléments biométriques supplémentaires PEUT être mise en œuvre par un État émetteur ou une organisation émettrice Les éléments suivants sont REQUIS à titre conditionnel si l'application optionnelle éléments biométriques supplémentaires a été invoquée ou un dossier de visa l'a référencé.

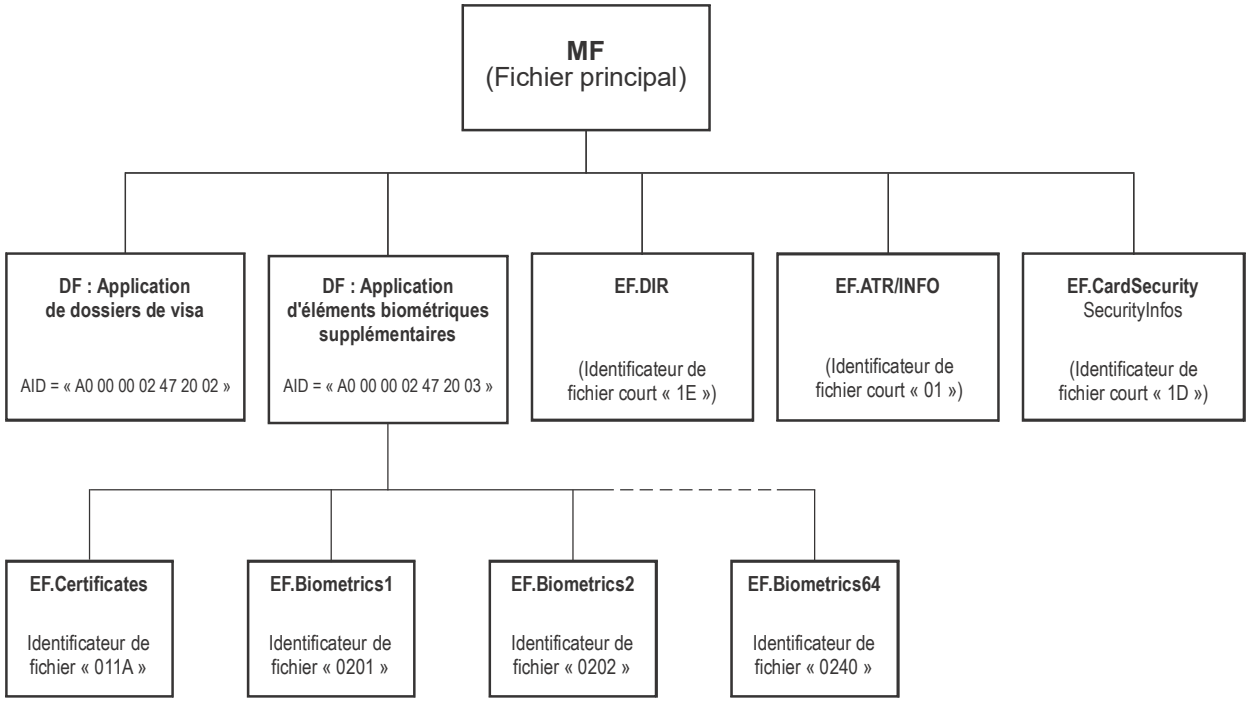


Figure 6. Structure de l'application éléments biométriques supplémentaires

5.3.1 Sélection d'application — DF

L'application éléments biométriques supplémentaires DOIT être sélectionnée en utilisant l'identifiant d'application (AID) comme nom DF réservé. L'AID DOIT être constitué de l'identifiant d'application enregistré attribué par l'ISO selon la norme ISO/IEC 7816-5 et d'une extension d'identifiant d'application propriétaire (PIX) de l'application éléments biométriques supplémentaires :

- l'identifiant de l'application enregistrée est « A0 00 00 02 47 » ;
- l'application éléments biométriques supplémentaires DOIT utiliser PIX = « 20 03 » ;
- l'AID complète de l'application éléments biométriques supplémentaires est : « A0 00 00 02 47 20 03 ».

Si l'autorisation effective n'accorde de droits d'accès à aucune donnée dans une application SDL2, la sélection de cette application DOIT être rejetée par le CI.

5.3.2 EF.Certificates (OBLIGATOIRE)

Les certificats de signataires des éléments biométriques supplémentaires sont stockés dans un fichier EF.Certificates dans l'application DF et ont une structure linéaire avec des dossiers de taille variable. Ces certificats sont destinés à être utilisés par l'IS pour poursuivre la validation hors ligne de la signature numérique dans l'EF.Biometrics.

Tableau 91. EF.Certificates

Nom de fichier	EF.Certificates
ID de fichier	« 011A »
Identificateur EF court	« 1A »
Accès sélectionner / FMM	PACE+TA (autorisation des éléments biométriques supplémentaires octet 1 bit b1 (voir Tableau 98)
Accès à lecture de dossier / recherche de dossier	PACE+TA (autorisation des éléments biométriques supplémentaires octet 1 bit b1 (voir Tableau 98)
Accès à ajout de dossier	PACE+TA (autorisation des éléments biométriques supplémentaires octet 1 bit b2 (voir Tableau 98)
Accès à écriture de dossier / mise à jour de dossier	JAMAIS
Accès à effacement de dossier	JAMAIS
Structure du fichier	Structure linéaire avec des dossiers de taille variable
Taille	Variable

Le dossier de certificat contient un seul certificat d'objet de données de signataire d'éléments biométriques supplémentaires X.509. Un dossier de certificat PEUT être référencé par un ou plusieurs EF éléments biométriques supplémentaires.

La structure du dossier de certificat dans l'application éléments biométriques supplémentaires est identique à celle du dossier de certificat dans l'application de dossier de voyage spécifiée dans le tableau 83.

Les dossiers de certificat sont écrits dans le fichier EF.Certificates situé sous l'application DF éléments biométriques supplémentaires à l'aide de la commande APPEND RECORD. Les dossiers de certificats peuvent être lus depuis le fichier EF.Certificates en utilisant la commande READ RECORD. Les dossiers de certificats NE DOIVENT PAS être mis à jour ou effacés. Le nombre maximum de dossiers dans un fichier EF.Certificates contenu dans l'application DF éléments biométriques supplémentaires DOIT être de 64.

5.3.3 Fichier EF.Biometrics

Les éléments biométriques supplémentaires DOIVENT être stockées dans les EF sous l'application éléments biométriques supplémentaires et avoir une structure transparente conformément à la norme ISO/IEC 7816-4.

Chaque EF éléments biométriques supplémentaires PEUT être lié à un ou plusieurs dossiers dans le fichier EF.VisaRecords de l'application dossier de visa (ou d'autres fichier EF et applications) à l'aide de l'identificateur EF éléments biométriques supplémentaires.

Tableau 92. Fichier EF.Biometrics1 à fichier EF.Biometrics64

Nom de fichier	Fichier EF.Biometrics1 à fichier EF.Biometrics64
ID de fichier	« 0201 » à « 0240 »
Identificateur EF court	S.O.
Accès en Sélection / FMM / lecture à l'état désactivé	PACE+TA (autorisation éléments biométriques supplémentaires selon le Tableau 98, bits b2, b4, b6, b8 de l'octet 2-17)
Accès en écriture à l'état désactivé	PACE+TA (autorisation éléments biométriques supplémentaires selon le Tableau 98, bits b2, b4, b6, b8 de l'octet 2-17)
Accès à activer à l'état désactivé	PACE+TA (autorisation éléments biométriques supplémentaires selon le Tableau 98, bits b2, b4, b6, b8 de l'octet 2-17)
Accès en Sélection / FMM / lecture à l'état activé	PACE+TA (autorisation éléments biométriques supplémentaires selon le Tableau 98, bits b1, b3, b5, b7 de l'octet 2-17)
Accès en écriture à l'état activé	JAMAIS
Accès à activer à l'état activé	JAMAIS
Accès en effacement	JAMAIS
Structure du fichier	Structure transparente
Taille	Variable

Chaque EF éléments biométriques supplémentaires DOIT contenir un objet de données BER-TLV DO « 7F2E » encapsulant trois objets de données : les données biométriques DO « 5F2E » suivies du jeton d'authenticité (signature) DO « 5F37 » et DO « 5F38 » contenant la référence à un certificat de signataire d'éléments biométriques supplémentaires dans le fichier EF.Certificates comme indiqué dans le tableau ci-après.

Le contenu de DO « 5F2E » est laissé à la discrétion de l'émetteur d'éléments biométriques supplémentaires et n'entre pas dans le cadre de la présente spécification.

Le mécanisme de création d'EF éléments biométriques supplémentaires est hors du champ d'application de cette spécification. L'émetteur DEVRAIT pré-créer un certain nombre d'EF éléments biométriques supplémentaires.

Note.— Les étiquettes intersectorielles spécifiées dans le tableau ci-après sont utilisées dans le contexte du SDL, de sorte qu'un schéma d'attribution d'étiquettes coexistantes n'est pas nécessaire.

Tableau 93. Format de fichier EF.Biometrics

Étiquette	Étiquette	Contenu	OBLIGATOIRE/ OPTIONNEL/ CONDITIONNEL	Format	Exemple
« 7F2E »		Gabarit de données biométriques	M		« 7F » « 2E » Len (DO « 5F2E » || DO « 5F37 » || DO « 5F38 »)
	« 5F2E »	Données d'éléments biométriques supplémentaires	M	V, B	« 5F 2E » Len {Biometric data}
	« 5F37 »	Jeton d'authenticité (Signature)	M	V (140), B	« 5F » « 37 » Len (Signature)
	« 5F38 »	Référence (numéro de dossier) au certificat de signataire d'éléments biométriques supplémentaires dans le magasin de certificats	M	F (1) B	« 01 » …« 40 »

Note.— B = données binaires, F = champ de longueur fixe, V = champ de longueur variable.

L'ordre des objets de données dans le fichier EF est fixe.

Chaque EF éléments biométriques supplémentaires DOIT contenir une signature numérique (jeton d'authenticité) calculée dans le cadre du DO « 5F2E », y compris l'étiquette et la longueur. La signature est générée par le signataire des éléments biométriques supplémentaires.

Le certificat de signataire des éléments biométriques supplémentaires requis pour vérifier la signature des éléments biométriques supplémentaires est stocké dans un magasin de fichiers EF.Certificates séparé situé sous l'application DF des éléments biométriques supplémentaires.

Chaque EF d'éléments biométriques supplémentaires DOIT être écrit à l'aide de la commande UPDATE BINARY.

Les EF éléments biométriques supplémentaires NE DOIVENT PAS être modifiés (mis à jour) ou effacés. Le nombre maximal d'EF éléments biométriques supplémentaires est de 64.

Tous les noms, identificateurs et identificateurs courts possibles des EF éléments biométriques supplémentaires sont répertoriés dans le Tableau 94.

Tableau 94. Identificateurs de fichier EF.Biometrics

Nom du fichier EF	Identificateur EF	Identificateur EF court
EF.Biometrics1	« 0201 »	S.O.
EF.Biometrics2	« 0202 »	S.O.
EF.Biometrics3	« 0203 »	S.O.
EF.Biometrics4	« 0204 »	S.O.
EF.Biometrics5	« 0205 »	S.O.
EF.Biometrics6	« 0206 »	S.O.
EF.Biometrics7	« 0207 »	S.O.
EF.Biometrics8	« 0208 »	S.O.
EF.Biometrics9	« 0209 »	S.O.
EF.Biometrics10	« 020A »	S.O.
EF.Biometrics11	« 020B »	S.O.
EF.Biometrics12	« 020 »	S.O.
EF.Biometrics13	« 020D »	S.O.
EF.Biometrics14	« 020E »	S.O.
EF.Biometrics15	« 020F »	S.O.
EF.Biometrics16	« 0210 »	S.O.
EF.Biometrics17	« 0211 »	S.O.
EF.Biometrics18	« 0212 »	S.O.
EF.Biometrics19	« 0213 »	S.O.
EF.Biometrics20	« 0214 »	S.O.
EF.Biometrics21	« 0215 »	S.O.
EF.Biometrics22	« 0216 »	S.O.
EF.Biometrics23	« 0217 »	S.O.
EF.Biométrie24	« 0218 »	S.O.
EF.Biometrics25	« 0219 »	S.O.
EF.Biometrics26	« 021A »	S.O.
EF.Biometrics27	« 021B »	S.O.
EF.Biometrics28	« 021 »	S.O.
EF.Biometrics29	« 021D »	S.O.
EF.Biometrics30	« 021E »	S.O.
EF.Biometrics31	« 021F »	S.O.
EF.Biometrics32	« 0220 »	S.O.

Nom du fichier EF	Identificateur EF	Identificateur EF court
EF.Biometrics33	« 0221 »	S.O.
EF.Biometrics34	« 0222 »	S.O.
EF.Biometrics35	« 0223 »	S.O.
EF.Biometrics36	« 0224 »	S.O.
EF.Biometrics37	« 0225 »	S.O.
EF.Biometrics38	« 0226 »	S.O.
EF.Biometrics39	« 0227 »	S.O.
EF.Biometrics40	« 0228 »	S.O.
EF.Biometrics41	« 0229 »	S.O.
EF.Biometrics42	« 022A »	S.O.
EF.Biometrics43	« 022B »	S.O.
EF.Biometrics44	« 022 »	S.O.
EF.Biometrics45	« 022D »	S.O.
EF.Biometrics46	« 022E »	S.O.
EF.Biometrics47	« 022F »	S.O.
EF.Biometrics48	« 0230 »	S.O.
EF.Biometrics49	« 0231 »	S.O.
EF.Biometrics50	« 0232 »	S.O.
EF.Biometrics51	« 0233 »	S.O.
EF.Biometrics52	« 0234 »	S.O.
EF.Biometrics53	« 0235 »	S.O.
EF.Biometrics54	« 0236 »	S.O.
EF.Biometrics55	« 0237 »	S.O.
EF.Biometrics56	« 0238 »	S.O.
EF.Biometrics57	« 0239 »	S.O.
EF.Biometrics58	« 023A »	S.O.
EF.Biometrics59	« 023B »	S.O.
EF.Biometrics60	« 023 »	S.O.
EF.Biometrics61	« 023D »	S.O.
EF.Biometrics62	« 023E »	S.O.
EF.Biometrics63	« 023F »	S.O.
EF.Biometrics64	« 0240 »	S.O.

5.4 Conditions d'accès au dossier d'application SDL2 (CONDITIONNEL)

5.4.1 Rôles et niveaux d'autorisation par défaut (OBLIGATOIRE)

Chaque certificat CV contient un modèle d'autorisation du détenteur de certificat (CHAT) qui identifie le rôle du détenteur de certificat (IS, DV, CVCA) et contient des droits d'accès à DG3/DG4 de l'application DVLM-e SDL2 REQUISE (pour des raisons d'ancienneté ou d'autres utilisations nationales).

Le CHAT contient une séquence de deux objets :

a) Un identificateur d'objet spécifiant le type de terminal et le format du modèle TR- 03110 :

```
id-roles OBJECT IDENTIFIER ::= {bsi-de applications(3) mrtd(1) 2}
id-IS       OBJECT IDENTIFIER ::= {id-roles 1}
```

b) Un objet de données discrétionnaire A (étiquette « 53 ») contenant le rôle codé en bits et les droits d'accès en lecture seule du titulaire du certificat, conformément au tableau suivant :

Tableau 95. Autorisation par défaut du CHAT

	Description	Octet 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Rôle	CVCA	1	1						
	DV (domestique)	1	0						
	DV (étranger)	0	1						
	IS	0	0						
Accès en lecture	RFU								
	RFU								
	RFU								
	RFU								
	DG4 (iris)							1	
	DG3 (doigt)								1

Note.— Le DVLM-e SDL2 DOIT ignorer la valeur des bits RFU dans l'autorisation du titulaire du certificat.

5.4.2 Niveaux d'autorisation des applications (OBLIGATOIRE)

Les autorisations des détenteurs de certificats pour chaque application SDL2 sont codées dans des extensions de certificats CV (une extension par application). L'extension de certificat est un gabarit discrétionnaire (étiquette « 73 ») comprenant deux objets de données : un identificateur d'objet d'autorisation (étiquette « 06 ») pour une application spécifique et un objet de données discrétionnaire (étiquette « 53 ») contenant des droits d'accès codés en bits du détenteur du certificat à une application spécifiée.

Pour déterminer l'autorisation effective d'un détenteur de certificat, la puce DVLM-e SDL2 calcule un "et" booléen binaire des droits d'accès contenus dans les extensions de certificat du certificat IS et des certificats DV et CVCA référencés.

Pour l'application dossier de voyage, les identificateurs d'objet d'autorisation et les codages de droits d'accès sont :

```
id-icao-lds2-travelRecords        OBJECT IDENTIFIER  ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER::= {id-icao-lds2-
travelRecords 3}
```

Tableau 96. Autorisations pour l'application de dossiers de voyage

	Description	Octet 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Droits d'accès	RFU								
	RFU								
	RFU								
	RFU								
	Ajout d'EF.Certificates					1			
	Lecture/Recherche/Sélection/FMM d'EF.Certificates						1		
	Ajout d'EF.EntryRecords/ExitRecords							1	
	Lecture/Recherche/Sélection/FMM d'EF.EntryRecords/ExitRecords								1

Pour l'application dossier de visa, les identificateurs d'objets d'autorisation et les codages de droits d'accès sont :

```
id-icao-lds2-travelRecords       OBJECT IDENTIFIER ::= {id-icao-lds2 2}
id-icao-lds2-visaRecords-access OBJECT IDENTIFIER  ::= {id-icao-lds2-
visaRecords 3}
```

Tableau 97. Autorisations pour l'application de dossiers de visa

	Description	Octet 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Droits d'accès	RFU								
	RFU								
	RFU								
	RFU								
	Ajout d'EF.Certificates					1			
	Lecture/Recherche/Sélection/FMM d'EF.Certificates						1		
	Ajout d'EF.VisaRecords							1	
	Lecture/Recherche/Sélection/FMM d'EF.VisaRecords								1

Pour l'application éléments biométriques supplémentaires, les identificateurs d'objet d'autorisation et les codages de droits d'accès sont :

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

Tableau 98. Autorisations pour l'application éléments biométriques supplémentaires

	Description	Identificateur EF	Autorisations							
			b8	b7	b6	b5	b4	b3	b2	b1
Octet 1	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	Ajout d'EF.Certificates	« 011A »							1	
	Sélection/FMM/Lecture/Recherche d'EF.Certificates	« 011A »								1
Octet 2	Sélection/FMM/Écriture/Activation/Lecture d'EF.Biometrics1 à l'état désactivé	« 0201 »	1							
	Sélection/FMM/Lecture d'EF.Biometrics1 à l'état activé	« 0201 »		1						
	Sélection/FMM/écriture/Activation/Lecture d'EF.Biometrics2 à l'état désactivé	« 0202 »			1					
	Sélection/FMM/Lecture d'EF.Biometrics2 à l'état activé	« 0202 »				1				
	Sélection/FMM/Écriture/Activation/Lecture d'EF.Biometrics3 à l'état désactivé	« 0203 »					1			
	Sélection/FMM/Lecture d'EF.Biometrics3 à l'état activé	« 0203 »						1		
	Sélection/FMM/Écriture/Activation/Lecture d'EF.Biometrics4 à l'état désactivé	« 0204 »							1	
	Sélection/FMM/Lecture d'EF.Biometrics4 à l'état activé	« 0204 »								1

…

Octet 17	Sélection/FMM/Écriture/Activation/Lecture d'EF.Biometrics61 à l'état désactivé	« 023D »	1							
	Sélection/FMM/Lecture d'EF.Biometrics61 à l'état activé	« 023D »		1						
	Sélection/FMM/Écriture/Activation/Lecture d'EF.Biometrics62 à l'état désactivé	« 023E »			1					
	Sélection/FMM/Lecture d'EF.Biometrics62 à l'état activé	« 023E »				1				
	Sélection/FMM/Écriture/Activation/Lecture d'EF.Biometrics63 à l'état désactivé	« 023F »					1			
	Sélection/FMM/Lecture d'EF.Biometrics63 à l'état activé	« 023F »						1		
	Sélection/FMM/Écriture/Activation/Lecture d'EF.Biometrics64 à l'état désactivé	« 0240 »							1	
	Sélection/FMM/Lecture d'EF.Biometrics64 à l'état activé	« 0240 »								1

Note 1.— Le DVLM-e SDL2 DOIT ignorer la valeur des bits RFU dans l'autorisation du titulaire du certificat.

Note 2.— Les États émetteurs ou les organisations émettrices NE DOIVENT PAS émettre de certificats de terminal avec des autorisations d'écriture/activation pour l'IS s'ils ne disposent que d'autorisations de lecture pour les éléments biométriques supplémentaires.

6. IDENTIFICATEURS D'OBJET

6.1 Résumé d'application SDL1 et SDL2 d'identificateurs d'objets

Tableau 99. OID des applications SDL1.7, SDL1.8 et SDL2

Identificateur d'objet	Valeur	Observations
id-icao	joint-iso-itu-t(2) international-organizations(23) icao(136)	OID DE L'OACI
id-icao-mrtd	id-icao 1	OID du DVLM-e
id-icao-mrtd-security	id-icao-mrtd 1	
id-icao-ldsSecurityObject	id-icao-mrtd-security 1	objet de sécurité SDL
id-icao-mrtd-security-cscaMasterList	id-icao-mrtd-security 2	liste de contrôle de l'ACSN
id-icao-mrtd-security-cscaMasterListSigningKey	id-icao-mrtd-security 3	
id-icao-mrtd-security-documentTypeList	id-icao-mrtd-security 4	liste de type de document
id-icao-mrtd-security-aaProtocolObject	id-icao-mrtd-security 5	protocole d'authentification active
id-icao-mrtd-security-extensions	id-icao-mrtd-security 6	changement de nom d'ACSN
id-icao-mrtd-security-extensions-nameChange	id-icao-mrtd-security-extensions 1	

Identificateur d'objet	Valeur	Observations
id-icao-mrtd-security-extensions-documentTypeList	id-icao-mrtd-security-extensions 2	Type de document DS
id-icao-mrtd-security-DeviationList	id-icao-mrtd-security 7	Liste des défauts des OID de base
id-icao-mrtd-security-DeviationListSigningKey	id-icao-mrtd-security 8	
id-icao-lds2	id-icao-mrtd-security 9	identificateurs d'objets SDL2
id-icao-lds2-travelRecords	id-icao-lds2 1	OID de base de l'application dossier de voyage
id-icao-lds2-travelRecords-application	id-icao-lds2-travelRecords 1	Dossiers de voyage AID
id-icao-lds2-travelRecords-access	id-icao-lds2-travelRecords 3	Extension du certificat d'autorisation
id-icao-lds2-visaRecords	id-icao-lds2 2	OID de base de l'application dossier de visa
id-icao-lds2-visaRecords-application	id-icao-lds2-visaRecords 1	Dossiers de visa AID
id-icao-lds2-visaRecords-access	id-icao-lds2-visaRecords 3	Extension du certificat d'autorisation
id-icao-lds2-additionalBiometrics	id-icao-lds2 3	OID de base des éléments biométriques supplémentaires
id-icao-lds2-additionalBiometrics-application	id-icao-lds2-additionalBiometrics 1	Éléments biométriques supplémentaires AID
id-icao-lds2-additionalBiometrics-access	id-icao-lds2-additionalBiometrics 3	Extension du certificat d'autorisation
id-icao-lds2Signer	id-icao-lds2 8	Identificateurs d'objets des signataires du SDL2
id-icao-tsSigner	id-icao-lds2Signer 1	Certificat de signataire du tampon de voyage SDL2
id-icao-vSigner	id-icao-lds2Signer 2	Certificat de signataire de visa SDL2
id-icao-bSigner	id-icao-lds2Signer 3	Certificat de signataire des éléments biométriques SDL2
id-icao-spoc	id-icao-mrtd-security 10	Identificateurs d'objet SPOC
id-icao-spocClient	id-icao-spoc 1	Client
id-icao-spocServer	id-icao-spoc 2	Serveur

7. SPÉCIFICATIONS ASN.1

```
id-icao OBJECT IDENTIFIER ::= {joint-iso-itu-t(2) international-organizations(23)
icao(136) }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}
```

```
id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 2}
id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 3}
id-icao-mrtd-security-documentTypeList OBJECT IDENTIFIER ::= {id-icao-mrtd-security
4}
id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security
5}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icao-mrtd-
security-extensions 1}
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {id-icao-
mrtd-security-extensions 2}
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 8}

id-icao-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}
```

Application SDL2 dossiers de voyage identificateurs d'objets

```
id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-
travelRecords 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords
3}
```

Application SDL2 dossiers de visa identificateurs d'objets

```
id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}
id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords
1}
id-icao-lds2-visaRecords-access OBJECT IDENTIFIER:= {id-icao-lds2-visaRecords 3}
```

Application SDL2 éléments biométriques supplémentaires identificateurs d'objets

```
id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}
id-icao-lds2-additionalBiometrics-application OBJECT IDENTIFIER ::= {id-icao-lds2-
additionalBiometrics 1}
id-icao-lds2-additionalBiometrics-access OBJECT IDENTIFIER ::= {id-icao-lds2-
additionalBiometrics 3}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-lds2 8}
id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}
id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}
id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 3}

id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}
id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-spoc 1}
id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-spoc 2}
```

8. 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: 2017, *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 19794-6 — ISO/IEC 19794-6:2011, *Information technology — Biometric data interchange formats — Part 6: IRIS image data* [Technologies de l'information — Formats d'échange de données biométriques — Partie 6 : Données d'image de l'iris].

ISO/IEC 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].

ISO/IEC 19795-6 — ISO/IEC 19795-6:2012, *Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation* [Technologies de l'information — Tests et rapports sur les performances biométriques — Partie 6 : Méthodologies d'essai pour l'évaluation opérationnelle].

ISO/IEC 39794-4 — ISO/IEC 39794-4:2019, *Information technology — Extensible 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 39794-5 — ISO/IEC 39794-5:2019, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data* [Technologies de l'information — Formats d'échange de données biométriques — Partie 5 : Données d'image du visage].

ISO/IEC 39794-6 — ISO/IEC 39794-6:2021, *Information technology — Extensible biometric data interchange formats — Part 6: Iris image data* [Technologies de l'information — Formats d'échange de données biométriques extensibles — Partie 6 : Données d'image de l'iris].

— — — — — — — —

Appendice A à la Partie 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 SDL1 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 SDL1 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 cadre de formats d'échange biométriques communs (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 »* « 0101 »
    - **« 88 »** *« 02 »* « 0008 »
  - **« 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 AVISER — 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)

LE 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 SDL1 et le DVLM-e SDL2 DOIVENT répondre à tous les tests spécifiés dans l'ISO/IEC 18745-2 qui appliquent les spécifications de la classe 1.

Il est RECOMMANDÉ que les DVLM-e respectent également les spécifications de la classe 1. 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 ;
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 être sous la forme d'une carte plastique au format TD3, cousue dans le livret lors de sa fabrication ; ou
Couverture arrière — Les placer dans la structure de la couverture arrière.

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 doit pouvoir répondre à toute REQ/WUP appropriée à son type après un champ magnétique alternatif non modulé de 10 ms. Il est RECOMMANDÉ de pouvoir répondre à tout REQ/WUP approprié à son type après un champ magnétique alternatif non modulé 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.

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.

B.5 PERTURBATIONS ÉLECTROMAGNÉTIQUES (EMD)

La prise en charge des perturbations électromagnétiques 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.

B.6 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.7 MISE SOUS ÉCRAN

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

B.8 IDENTIFIANT UNIQUE (UID) ET IDENTIFIANT PICC PSEUDO-UNIQUE (PUPI) (RECOMMANDÉ)

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

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

B.9 PLAGE DE FRÉQUENCES DE RÉSONANCE (RECOMMANDÉ)

Il n'existe aucune exigence quant à la fréquence de résonance, les demandeurs de DVLM-e PEUVENT limiter leur fréquence de résonance par défaut à une certaine plage afin d'accroître l'interopérabilité.

B.10 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.11 TEMPS D'ATTENTE DE TRAME (FWI) ET REQUÊTE DE PROLONGATION DE DURÉE D'ATTENTE BLOC S [S(WTX)] (RECOMMANDÉ)

Il est RECOMMANDÉ de fixer pour le DVLM-e une valeur FWI inférieure ou égale à 11 afin d'améliorer les performances. Il est 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'ISO/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 deux A/m à toutes les positions est 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 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 devrait 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 : 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 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.6 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 classe 1 dans le volume fonctionnel.

Les classes 2 et 3 sont obligatoires dans l'ISO/IEC 14443, mais optionnelles dans le système d'inspection du DVLM-e.

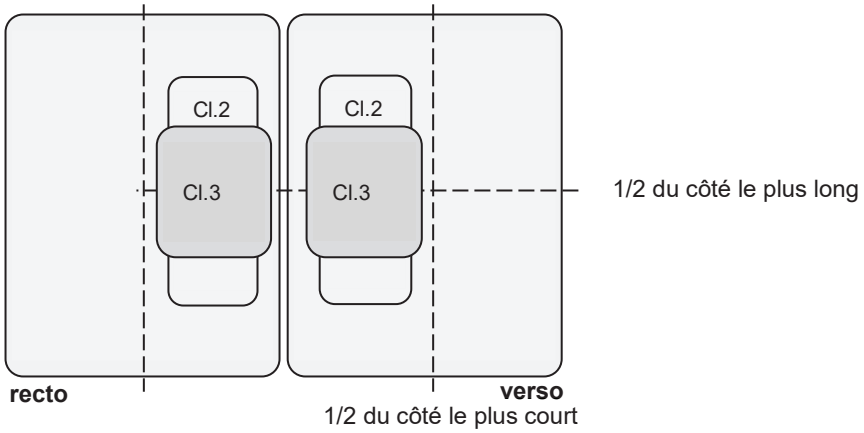


Figure C-1. Positions obligatoires sur chaque surface ID-3 dans laquelle une antenne de classe 2 et de classe 3 doit être lue par un système d'inspection associé au DVLM-e de type 1 et 2

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.

C.7 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.8 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.9 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.10 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'identifiant de carte (CID) et l'adresse nodale (NAD).

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

C.11 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.12 RÉTABLISSEMENT EN CAS D'ERREUR (RECOMMANDÉ)

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

C.13 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.

— — — — — — — —

Appendice D à la Partie 10
(INFORMATIF)

OBJET DE SÉCURITÉ DU DOCUMENT EF.SOD VERSION V0 LDS V1.7 (ANCIENNE)

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}
```

D.1 TYPE DE DONNÉES SIGNÉES POUR SO_D 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 = OBLIGATOIRE — 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 D-1. 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	
issuerandSerialNumber	c	Il est recommandé que les États prennent en charge ce champ plutôt que subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	L'identificateur d'algorithme 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 ; cependant, les États émetteurs n'ont pas à traiter ces attributs sauf pour vérifier la valeur de la signature.
signatureAlgorithm	m	L'identificateur d'algorithme 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 la 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.

D.2 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

-- 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        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 (`dataGroupHashValue`) 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. Le système d'inspection DOIT accepter le champ `DigestAlgorithmIdentifiers` avec les deux conditions, c'est-à-dire des paramètres absents et des paramètres `NULL`.

— — — — — — — —

Appendice E à la Partie 10
(INFORMATIF)

SCHÉMA DES STRUCTURES DE FICHIERS

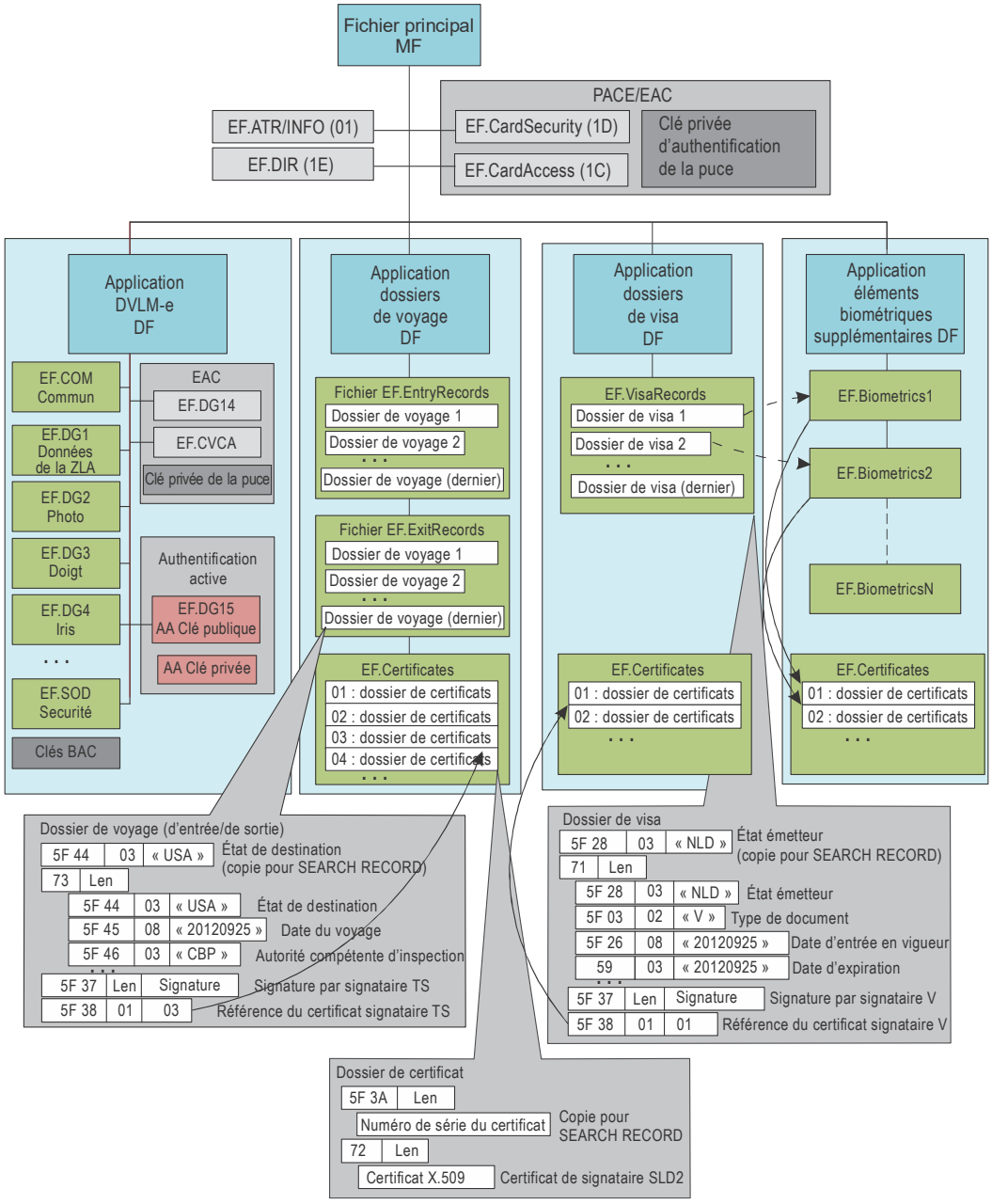


Figure E-1. Schéma des structures de fichiers

Appendice F à la Partie 10
(INFORMATIF)

SCHÉMA DE L'AUTORISATION SDL

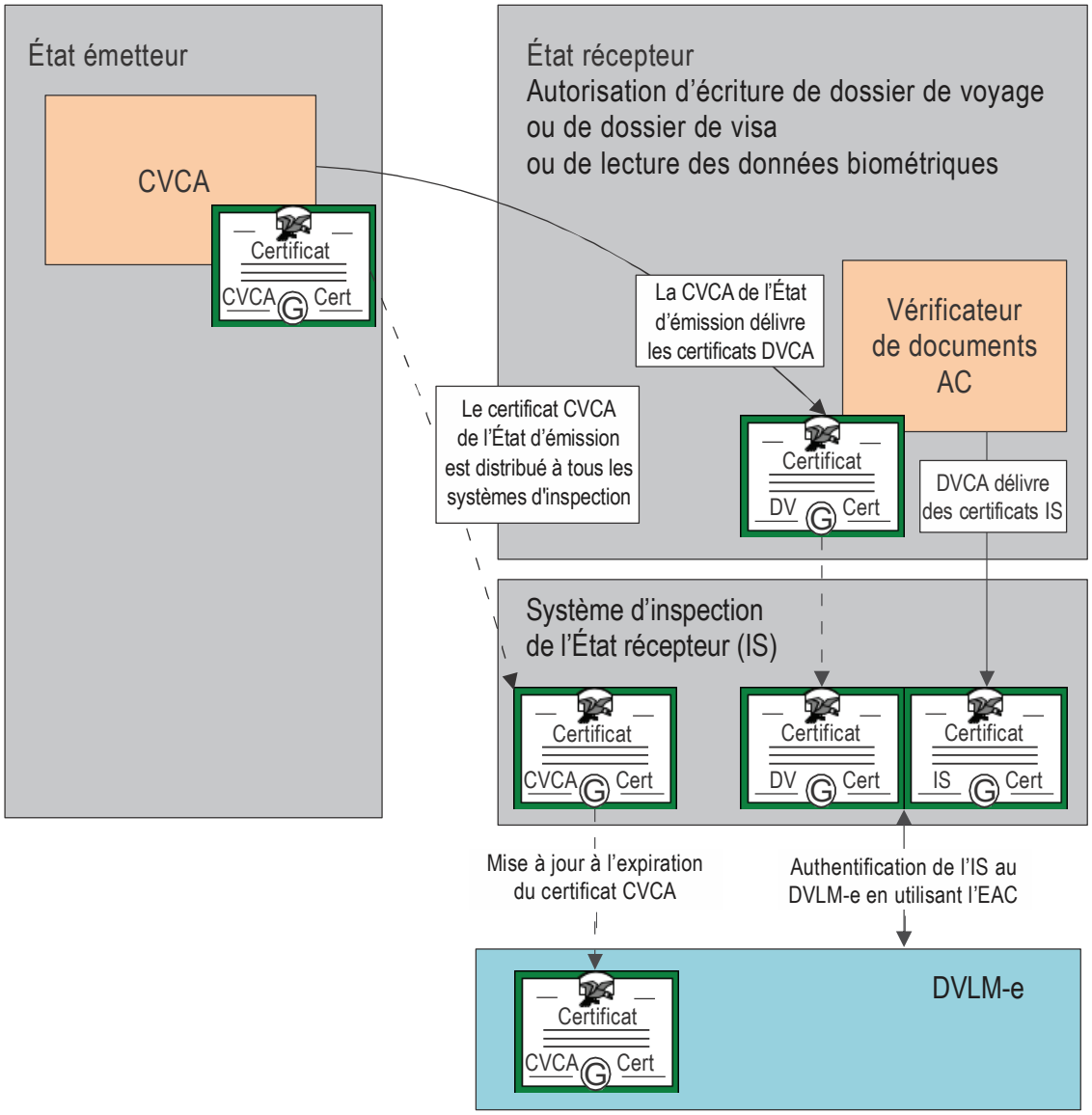


Figure F-1. Schéma de l'autorisation SDL

Appendice G à la Partie 10
(INFORMATIF)

SCHÉMA DES SIGNATURES NUMÉRIQUES SDL

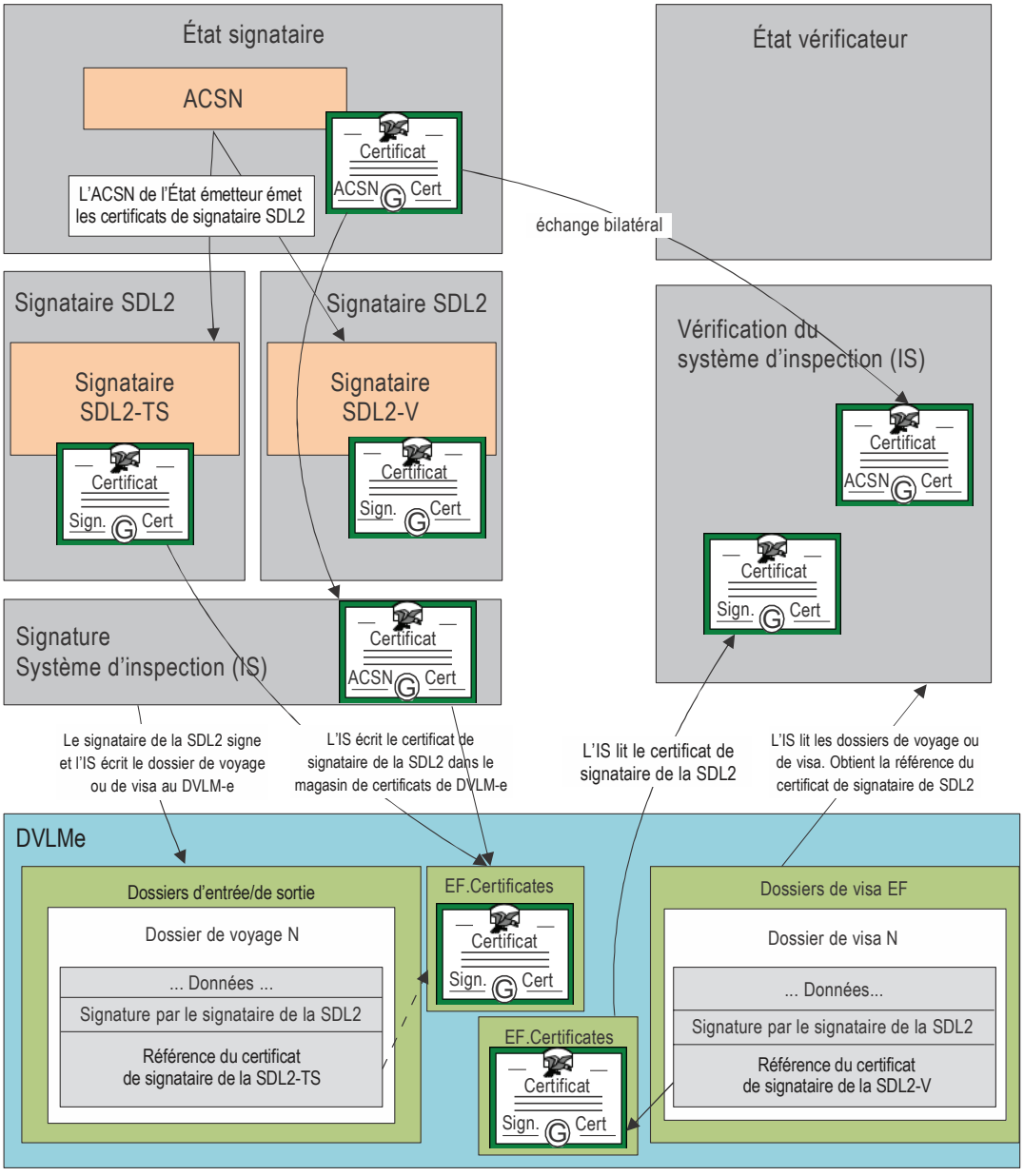


Figure G-1. Signature numérique SDL

— — — — — — — —

Appendice H à la Partie 10
(INFORMATIF)

EXEMPLE DE LECTURE DE DOSSIERS DE VOYAGE

H.1 COMMANDE FMM RÉCUPÉRANT LE NOMBRE DE DOSSIERS D'ENTRÉE

CLA	INS	P1	P2	Lc	Données	Le
« 80 »	« 5E »	« 01 »	« 04 »	« 04 »	« 51 02 01 01 »	« 00 »

CLA : classe propriétaire / pas de messagerie sécurisée
INS : FMM
P1 : « 01 » — Identificateur EF dans le champ de données de commande
P2 : « 04 » — Renvoie le nombre de dossiers existants dans un dossier EF
Lc : « 04 »
Données : DO « 51 » contenant des dossiers d'entrée identificateur EF « 0101 »
Le : « 00 » (Le court)

Réponse : FILE AND MEMORY MANAGEMENT DO (gestion des fichiers et de la mémoire DO) représentant le nombre de dossiers dans l'EF.

Données	SW1-SW2
« 7F78 03 » « 83 01 FD »	« 90 00 »

Le DO des données de réponse contient le dernier numéro de dossier qui peut être utilisé dans la prochaine commande READ RECORD (P1).

Par exemple, le dernier numéro de dossier « 00 » signifie qu'il n'y a aucun dossier dans ce fichier, et la réponse « FD » signifie que le nombre de dossiers est de 253 (le nombre maximum de dossiers est de 254).

H.2 COMMANDE READ RECORD PERMETTANT DE RÉCUPÉRER LE DERNIER DOSSIER DE VOYAGE DE LA LISTE RÉCUPÉRÉE

La commande suivante peut être utilisée pour récupérer un seul dossier en utilisant le numéro de dossier renvoyé par la commande FMM :

CLA	INS	P1	P2	Le
« 00 »	« B2 »	« FD »	« 04 »	« 00 00 00 »

CLA : classe intersectorielle / pas de messagerie sécurisée
INS : READ RECORD(S) [LECTURE DE DOSSIER(S)]
P1 : numéro de dossier provenant de la réponse de la commande précédente
P2 : numéro de dossier dans P1 / lecture de dossier P1
Le : « 00 00 00 » (Le étendu), lecture entière de dossier

Réponse : Le numéro de dossier est 253 (« FD »).

Données	SW1-SW2
« 5F44 » « Len » <Data> || « 73 » « Len » <Data> || « 5F37 » « Len » <Data> || « 5F38 » « Len » <Data>	« 90 00 »

H.3 COMMANDE READ RECORD PERMETTANT DE RÉCUPÉRER DEUX DOSSIERS DE VOYAGE À PARTIR DE LA LISTE RÉCUPÉRÉE

La commande suivante peut être utilisée pour récupérer deux dossiers (ou plus) de la liste renvoyée par la commande FMM. La lecture de plusieurs dossiers dans un seul échange d'APDU améliore les performances. Le nombre de dossiers qui peuvent être récupérés par une seule commande peut être déterminé à partir des informations sur la longueur étendue dans l'EF.ATR/INFO et la taille maximale de dossier de voyage.

CLA	INS	P1	P2	Le
« 00 »	« B2 »	« FC »	« 05 »	« 00 00 00 »

CLA : classe intersectorielle / pas de messagerie sécurisée
INS : READ RECORD(S) [LECTURE DE DOSSIER(S)]
P1 : numéro de dossier diminué de la réponse du FMM (253 - 1 = 252 = « FC »)
P2 : numéro de dossier dans P1 / lecture de tous les dossiers de P1 jusqu'au dernier dossier
Le : « 00 00 00 » (Le étendu), lecture entière de dossier

Réponse : les deux derniers dossiers 252 (« FC ») et 253 (« FD ») sont renvoyés.

Données	SW1-SW2
« 5F44 » « Len » <Data> || « 73 » « Len » <Data> || « 5F37 » « Len » <Data> || « 5F38 » « Len » <Data> || « 5F44 » « Len » <Data> || « 73 » « Len » <Data> || « 5F37 » « Len » <Data> || « 5F38 » « Len » <Data>	« 90 00 »

— — — — — — — —

Appendice I à la Partie 10
(INFORMATIF)

EXEMPLE DE RECHERCHE DE DOSSIERS PAR ÉTAT

I.1 COMMANDE SEARCH RECORD — RECHERCHE DE DOSSIER(S) DE VOYAGE PAR ÉTAT DE DESTINATION

CLA	INS	P1	P2	Lc	Données	Le
« 00 »	« A2 »	« 00 »	« F8 »	Var	« 7F » « 76 » « Len » « 51 01 01 » « A1 » « 0B » « 80 01 00 » « B0 06 » « 02 01 03 » « 02 01 03 » « A3 07 » « B1 05 » « 81 03 » xx xx xx	« 00 »

CLA : classe intersectorielle / pas de messagerie sécurisée
INS : SEARCH RECORD(S) [RECHERCHE DE DOSSIER(S)]
P1 : numéro de dossier = « 00 »
P2 : recherche dans plusieurs EF
Lc : longueur du champ de données de la commande
Données : DO « 7F76 » - DO de traitement de dossier
DO « 51 » - DO de référence du fichier (identificateur court EF.EntryRecords « 01 »)
DO « A1 » - Modèle de configuration de recherche
DO « 80 » - Paramètre de configuration de recherche : « 00 » - (recherche de tous les dossiers)
DO « B0 » - Modèle de fenêtre de recherche
DO « 02 » - Décalage : « 03 »
DO « 02 » - Nombre d'octets : « 03 »
DO « A3 » - Modèle de chaîne de recherche
DO « B1 » - DO de Chaîne de recherche
DO « 81 » - Chaîne de recherche (code pays) : xx xx xx
Le : « 00 » (Le court)

Réponse : DO « 7F76 » - DO de traitement de dossier
DO « 51 » - identificateur court EF.EntryRecords « 01 »
Un ou plusieurs DO « 02 » contenant des numéros de dossier correspondants

Données	SW1-SW2
« 7F » « 76 » « Len » « 51 01 01 » « 02 01 03 » « 02 01 04 »	« 90 00 »

— — — — — — — —

APPENDICE J À LA PARTIE 10
(INFORMATIF)

EXEMPLE D'ÉCRITURE DE DOSSIER DE VOYAGE ET DE CERTIFICAT

J.1 COMMANDE SEARCH RECORD — RECHERCHE D'EF.CERTIFICATES PAR UN NUMÉRO DE SÉRIE DE CERTIFICAT

L'IS vérifie si le certificat de signataire SDL2-TS avec les numéros de série requis existe dans EF.Certificates. La commande suivante peut être utilisée pour rechercher des certificats :

CLA	INS	P1	P2	Lc	Données	Le
« 00 »	« A2 »	« 00 »	« F8 »	Var	« 7F » « 76 » « Len » « 51 01 1A » « A1 » « 0B » « 80 01 30 » « B0 06 » « 02 01 03 » « 02 01 » {Search string size} « A3 » « Len » « B1 » « Len » « 81 » « Len » xx xx ... xx xx	« 00 »

CLA : classe intersectorielle / pas de messagerie sécurisée
INS : SEARCH RECORD(S) [RECHERCHE DE DOSSIER(S)]
P1 : numéro de dossier = « 00 »
P2 : recherche dans plusieurs EF
Lc : longueur du champ de données de la commande
Données : DO « 7F76 » - DO de traitement de dossier
DO « 51 » - DO de référence du fichier (identificateur court EF.EntryRecords « 1A »)
DO « A1 » - Modèle de configuration de recherche
DO « 80 » - Paramètre de configuration de recherche : « 30 » (arrêt si le dossier a été trouvé)
DO « B0 » - Modèle de fenêtre de recherche
DO « 02 » - Décalage : « 03 »
DO « 02 » - Nombre d'octets : taille de la chaîne de recherche
DO « A3 » - Modèle de chaîne de recherche
DO « B1 » - DO de Chaîne de recherche

DO « 81 » - Recherche de la concaténation du code pays et du numéro de série du certificat : xx xx ... xx xx

Le : « 00 » (Le court)

Réponse : DO « 7F76 » - DO de traitement de dossier
DO « 51 » - Identificateur court EF.Certificates « 1A »
DO « 02 » - contient le numéro de dossier correspondant

Données	SW1-SW2
« 7F 76 06 » « 51 01 1A » « 02 01 01 »	« 90 00 »

ou le code d'avertissement « 62 82 » si aucun dossier ne correspond aux critères de recherche :

SW1-SW2
« 62 82 »

Si un dossier EF.Certificate correspond aux critères de recherche, l'IS peut éventuellement utiliser le numéro de dossier renvoyé (« 01 ») dans une commande READ RECORD pour vérifier si le certificat est le bon. Si aucun dossier EF.Certificate ne correspond aux critères de recherche, l'IS écrit le certificat dans EF.Certificates à l'aide de la commande APPEND RECORD de la section J.2 et écrit finalement le dossier d'entrée à l'aide de la commande APPEND RECORD de la section J.3.

J.2 COMMANDE APPEND RECORD — ÉCRITURE DU CERTIFICAT

L'IS écrit le certificat de signataire SDL2-TS dans EF.Certificates. La commande suivante peut être utilisée pour l'écriture des certificats :

CLA	INS	P1	P2	Lc	Données	Le
« 00 »	« E2 »	« 00 »	« D0 »	« 00 » XX XX	« 5F3A » « Len » {certificate serial number} || « 72 » « Len » {X.509 certificate}"	Absent

CLA : classe intersectorielle / pas de messagerie sécurisée
INS : APPEND RECORD (AJOUT DE DOSSIER)
P1 : « 00 » (toute autre valeur est invalide)
P2 : identifiant EF court (= « 1A »)
Lc : Longueur de dossier (Lc étendu)
Données : Données de dossier

Réponse : code de succès ou d'erreur

SW1-SW2
« 90 00 »

J.3 COMMANDE APPEND RECORD — ÉCRITURE DU DOSSIER DE VOYAGE

L'IS génère un dossier de voyage en faisant référence au certificat de signataire SDL2-TS et l'écrit dans EF.EntryRecords en utilisant la commande suivante :

CLA	INS	P1	P2	Lc	Données	Le
« 00 »	« E2 »	« 00 »	« 08 »	« 00 » XX XX	« 5F44 » « Len » {destination state} || « 73 » « Len » {Entry travel record} || « 5F37 » « Len » {Signature} || « 5F38 » « Len » {Cert Ref}	Absent

CLA : classe intersectorielle / pas de messagerie sécurisée
INS : APPEND RECORD (AJOUT DE DOSSIER)
P1 : « 00 » (toute autre valeur est invalide)
P2 : identificateur EF court (= « 01 »)
Lc : Longueur de dossier (Lc étendu)
Données : Données de dossier

Réponse : code de succès ou d'erreur

SW1-SW2
« 90 00 »

— FIN —

ISBN 978-92-9275-557-7