

ایکاو



Doc 9303

وثائق السفر المقرؤة آلياً

الطبعة الثامنة - ٢٠٢١

الجزء ١٠: بنية البيانات المنطقية لخزن بيانات الاستدلال
البيولوجي وغيرها في دائرة متكاملة لا تلامسية



اعتمدتها الأمينة العامة ونشرت بموجب سلطتها

منظمة الطيران المدني الدولي

ايكاو



Doc 9303

وثائق السفر المقرؤة آلياً

الطبعة الثامنة - ٢٠٢١

الجزء ١٠ : بنية البيانات المنطقية لخزن بيانات الاستدلال
البيولوجي وغيرها في دائرة متكاملة لا تلمسية

اعتمدتها الأمينة العامة ونشرت بموجب سلطتها

منظمة الطيران المدني الدولي

تُنشر هذه الوثيقة في طبعات منفصلة باللغات العربية والاسبانية والإنجليزية
والروسية والصينية والفرنسية
منظمة الطيران المدني الدولي
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

تتوفر التفاصيل والمعلومات الإضافية على الرابط www.icao.int/Security/FAL/TRIP

الوثيقة Doc 9303، وثائق السفر المقررة آلياً
الجزء العاشر — بنية البيانات المنطقية لخزن بيانات الاستدلال البيولوجي وغيرها في دائرة متكاملة لاتلasmisية
Order No.: 9303P10
ISBN 978-92-9265-552-5 (print version)
ISBN 978-92-9275-591-2 (electronic version)

© ICAO 2021

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذا المنشور أو تخزينه في نظام لاسترجاع
الوثائق أو تداوله في أي شكل أو بأي وسيلة، دون الحصول على إذن كتابي مسبق من منظمة
الطيران المدني الدولي.

التعديلات

تعلن التعديلات في ملحق كatalog المنتجات والخدمات. ويمكن الاطلاع على الكatalog وملحقه في موقع الإيكاو على الإنترنت www.icao.int. والجدول أدناه مخصص لتسجيل مثل هذه التعديلات.

سجل التعديلات والتصويبات

التصويبات	التاريخ	الرقم
أدخل بواسطة		

ليس في التسميات المستخدمة في هذا المطبوع ولا في طريقة عرض مادته ما يتضمن التعبير عن أي رأي كان للإيكاو بشأن الوضع القانوني لأي بلد أو إقليم أو مدينة أو منطقة، أو لسلطات أي منها، أو بشأن تعين تحومها أو حدودها.

جدول المحتويات

١	١ - المجال
١	٢ - بنية الجزء العاشر من الوثيقة ٩٣٠٣
٢	٣ - المواصفات المشتركة بين بنية البيانات المنطقية ١ وبنية البيانات المنطقية ٢
٢	٤ - الحد الأدنى من المتطلبات للتشغيل المتبادل
٣	٥ - الخصائص الكهربائية
٣	٦ - الخصائص المادية
٣	٧ - بروتوكول الإرسال
٤	٨ - مجموعة الأوامر
٥	٩ - أشكال الأوامر وخواص البارامتريات (LDS1 و LDS2)
١٠	١٠ - التعامل مع السجلات والأوامر (LDS2)
١٥	١١ - التعامل مع الملفات الشفافة وغيرها (LDS2)
١٩	١٢ - مواصفات بنية الملفات
٢٠	١٣ - اختيار التطبيق — الملف المخصص
٢١	١٤ - الملفات الأولية المشتركة
٢٧	٤ - تطبيق وثائق السفر الإلكترونية المقررة آلياً ذات البنية LDS1 (إلزامي)
٢٩	١٥ - اختيار التطبيق — الملف المخصص
٢٩	١٦ - خطط الترتيب العشوائي
٢٩	١٧ - تمثيل ملف الاطلاع العشوائي
٣٠	١٨ - تجميع عناصر البيانات
٣٠	١٩ - متطلبات بنية البيانات المنطقية
٣٣	٢٠ - الملفات الأولية لوثائق السفر الإلكترونية المقررة آلياً ذات البنية LDS1
٣٧	٢١ - عناصر البيانات التي تشكل مجموعات البيانات من ١ إلى ١٦
٦٦	٥ - تطبيقات بنية البيانات المنطقية LDS2 (اختيارية)
٦٦	٢٢ - تطبيق سجلات السفر (مشروع)
٧٢	٢٣ - تطبيق سجلات التأشيرة (مشروع)
٧٦	٢٤ - تطبيق بيانات الاستدلال البيولوجي الإضافية (مشروع)
٨٢	٢٥ - شروط الاطلاع على ملفات تطبيقات 2 LDS2 (مشروع)
٨٥	٦ - معرفات المواد
٨٥	٧ - ١٦ - موجز معرفات المواد الخاصة بتطبيقات LDS1 و LDS2
٨٦	٨ - مواصفات الترميز 1 ANS.1
٨٧	٩ - المراجع (معيارية)

App A-1 المرفق (أ) بالجزء ١٠ — أمثلة لتحديد مجالات بنية البيانات المنطقية (إعلامية)
App A-1 ١- الملف الأولي المشترك — عناصر البيانات المشتركة
App A-2 ٢- ملف أولي. مجموعة البيانات ١ — معلومات الجزء المقررة آلياً
App A-2 ٣- ملف أولي. مجموعة البيانات ٢ إلى ملف أولي. مجموعة البيانات ٤ — نماذج الاستدلال البيولوجي
App A-2 ٤- ملف أولي. مجموعة البيانات ٥ إلى ملف أولي. مجموعة البيانات ٧ — نماذج الصور المعروضة
App A-3 ٥- ملف أولي. مجموعة البيانات ١١ — التفاصيل الشخصية الإضافية
App A-3 ٦- ملف أولي. مجموعة البيانات ١٦ — الشخص الذي يتعين إخطاره (الأشخاص الذين يتعين إخطارهم)
App B-1 المرفق (ب) بالجزء ١٠ — الدائرة المتكاملة اللاتلامسية في جواز سفر إلكتروني مقرورة آلياً (إعلامية)
App B-1 ب-١ حجم الهوائي وفئة جواز السفر الإلكتروني المقررة آلياً
App B-1 ب-٢ التمهيد والاقتراع
App B-1 ب-٣ مضاد الاصطدام والطراز
App B-1 ب-٤ معدلات البتات الإلزامية
App B-2 ب-٥ الاضطراب الكهرومغناطيسي (EMD)
App B-2 ب-٦ الدعم (الاختياري) لتبادل بaramترات إضافية
App B-2 ب-٧ الحماية
App B-2 ب-٨ المعرف الفريد (UID) (الموصى به) ومعرف بطاقة الدائرة المتكاملة القريبة (PUPI)
App B-2 ب-٩ نطاق تردد الرنين (الموصى به)
App B-2 ب-١٠ أحجام الأطر (الموصى بها)
App B-3 ب-١١ العدد الصحيح لوقت الانتظار الإلزامي (الموصى به) (FWI) وطلب كتلة S لتمديد وقت الانتظار [S(WTX)]
App C-1 المرفق (ج) بالجزء ١٠ — نظم التفتيش (إعلامية)
App C-1 ج-١ حجم التشغيل وموقع الاختبار
App C-1 ج-٢ شكل الموجة المعنون ومتطلبات التردودات اللاسلكية
App C-1 ج-٣ تسلسلات الاقتراع وقت الكشف عن وثائق السفر الإلكترونية المقررة آلياً
App C-2 ج-٤ معدلات البت الإلزامية
App C-2 ج-٥ الاضطراب الكهرومغناطيسي (EMD)
App C-2 ج-٦ فئات الهوائي المدعومة
App C-3 ج-٧ (اختياري) أحجام الأطر وتصويب الخطأ
App C-3 ج-٨ الدعم (اختياري) لفئات الإضافية
App C-3 ج-٩ معدلات البتات (اختيارية)
 ج-١٠ الدعم (الموصى به) لوثائق السفر الإلكترونية المقررة آلياً المتعددة وبالبطاقات أو الأشياء الأخرى أو المضيقين المتعددين
App C-3 ج-١١ أحجام الأطر (الموصى بها)
App C-4 ج-١٢ استرداد الخطأ (الموصى به)
App C-4 ج-١٣ الكشف عن الخطأ (الموصى بها) وآلية الاسترداد
App D-1 المرفق (د) بالجزء ١٠ — المادة الأمنية للوثيقة (EF.SOD) الإصدار V0 البنية LDS V1.7 (قيمة) (إعلامية)
App D-1 د-١ البيانات الموقعة من أجل الوثيقة SOd V0

App D-2	وصف الترميز ١ ASN.1 لبنية البيانات المنطقية للمادة الأمنية للوثيقة SO _D V0	٢- د
App E-1	المرفق (ه) بالجزء ١٠ — موجز بنى الملفات (إعلامية)	
App F-1	المرفق (و) بالجزء ١٠ — موجز أدونات بنية البيانات المنطقية (إعلامية)	
App G-1	المرفق (ز) بالجزء ١٠ — موجز التواقيع الرقمية لبنيّة البيانات المنطقية (إعلامية)	
App H-1	المرفق (ح) بالجزء ١٠ — مثال لقراءة سجل السفر (إعلامية)	
App H-1	ح-١ الأمر FMM لاستعادة عدد سجلات الدخول	
App H-1	ح-٢ الأمر READ RECORD لاستعادة سجل السفر الأخير من القائمة المستعادة	
App H-2	ح-٣ الأمر READ RECORD لاستعادة سجلي للسفر الآخرين من القائمة المستعادة	
App I-1	المرفق (ط) بالجزء ١٠ — مثال لتفتيش السجلات بحسب الدولة (إعلامية)	
App I-1	ط-١ الأمر SERCH RECORD للبحث عن سجل (سجلات) السفر بحسب دولة المقصد	
App J-1	المرفق (ي) بالجزء ١٠ — مثال لكتابية سجل وشهادة السفر (إعلامية)	
App J-1	ي-١ الأمر SERCH RECORD للبحث عن شهادات الملفات الأولية بحسب رقم الشهادة التسلسلي	
App J-2	ي-٢ الأمر APPEND RECORD لكتابية الشهادة	
App J-3	ي-٣ الأمر APPEND RECORD لكتابية سجل السفر	

١ - المجال

يحدد الجزء العاشر من الوثيقة Doc 9303 بنية البيانات المنطقية (LDS) لوثائق السفر الإلكترونية المقرورة آلياً المطلوبة للتشغيل المتبادل عالمياً ويحدد مواصفات لتنظيم البيانات على الدائرة المتكاملة اللاتلامسية. ويطلب هذا تحديد جميع عناصر البيانات الالزامية والاختيارية وترتيباً و/أو تجميعاً إلزامياً لعناصر البيانات التي يجب متابعتها لتحقيق التشغيل المتبادل عالمياً لقراءة الإلكترونية للجواز الإلكتروني.

تتوفر الوثيقة 10-9303 Doc مواصفات لتمكين الدول وشركات تجميع الخدمات من تنفيذ دائرة متكاملة لاتلامسية لإدخالها في وثيقة سفر الكترونية. ويحدد هذا الجزء جميع عناصر البيانات الالزامية والاختيارية وبنى الملفات ومعالم التطبيق من أجل الدائرة المتكاملة اللاتلامسية.

تضمن الطبعة الثامنة للوثيقة Doc 9303 المواصفات الفنية لسجلات السفر الاختيارية وسجلات التأشيرات والتطبيقات الإضافية للاستدلال البيولوجي (تعرف باسم تطبيقات LDS2) باعتبارها امتداداً للتطبيق الإلزامي لوثيقة السفر الإلكترونية المقرورة آلياً.

ويجب أن يقرأ الجزء العاشر بالاقتران مع ما يلي:

- الجزء ١ — المقدمة؛
- الجزء ٣ — المواصفات الفنية المشتركة بين كل وثائق السفر الرسمية المقرورة آلياً؛
- الجزء ٤ — المواصفات الفنية للجوازات المقرورة آلياً ووثائق السفر المقرورة آلياً الأخرى من الحجم TD3؛
- الجزء ٥ — المواصفات الفنية لوثائق السفر الرسمية المقرورة آلياً من الحجم ١؛
- الجزء ٦ — المواصفات الفنية لوثائق السفر الرسمية المقرورة آلياً من الحجم ٢.

والجزئين المتصلين بالدائرة المتكاملة اللاتلامسية:

- الجزء ٩ — نشر تحديد الهوية بالاستدلال البيومترى والتخزين الإلكتروني للبيانات في وثائق السفر المقرورة آلياً؛
- الجزء ١١ — آليات أمن وثائق السفر المقرورة آلياً؛
- الجزء ١٢ — البنية الأساسية للمفاتيح العامة لوثائق السفر المقرورة آلياً.

٢ - بنية الجزء العاشر من الوثيقة Doc 9303

يقسم الجزء العاشر من الوثيقة Doc 9303 إلى أقسام تشمل ما يلي:

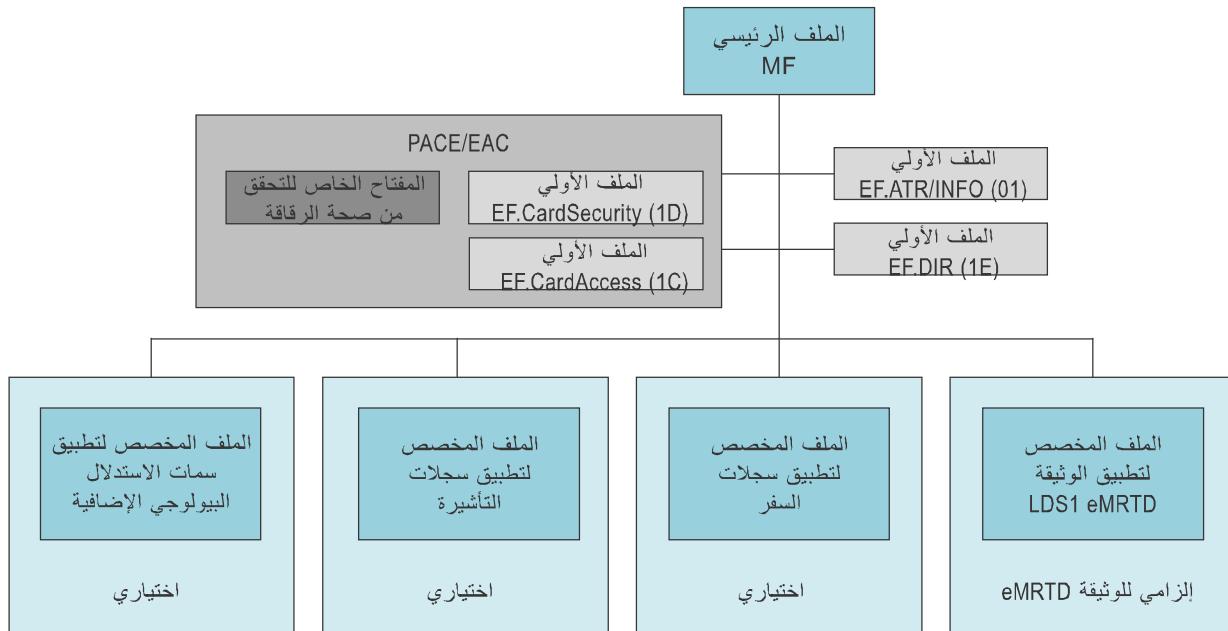
المواصفات الفنية المشتركة لكل من تطبيقات بنية البيانات المنطقية LDS1 وبنية البيانات المنطقية LDS2:

- النوع المشتركة؛
- وجميع الأوامر الخاصة ببنية البيانات المنطقية LDS1 وبنية البيانات المنطقية LDS2؛
- والملفات الأولية المشتركة لكل من بنية البيانات المنطقية LDS1 وبنية البيانات المنطقية LDS2؛

المواصفات الفنية لتطبيق وثائق السفر الإلكترونية المقرورة آلياً ذات البنية LDS1؛

المواصفات الفنية لتطبيقات البنية LDS2:

- سجلات السفر؛
- وسجلات التأشيرة؛
- وبيانات الاستدلال البيولوجي الإضافية؛
- والمواصفات الفنية لشروط الاطلاع على ملفات البنية LDS2.



الشكل ١ — تطبيقات بنية البيانات المنطقية LDS1 و LDS2

يمكن لوثيقة السفر الإلكترونية المقرورة آلياً أن تدعم أحد هذه التطبيقات أو عدداً منها أو جميعها:

- تطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 إلزامياً؛
- تطبيق سجلات السفر ذات البنية LDS2 اختيارياً؛
- تطبيق سجلات التأشيرة ذات البنية LDS2 اختيارياً؛
- تطبيق بيانات الاستدلال البيولوجي الإضافية ذات البنية LDS2 اختيارياً؛

٣ - المواصفات الفنية المشتركة بين بنية البيانات المنطقية LDS1 وبنية البيانات المنطقية LDS2

١-٣ الحد الأدنى من المتطلبات للتشغيل المتبادل

يجب أن يكون ما يلي هو الحد الأدنى من المتطلبات للتشغيل المتبادل للجواز الإلكتروني المستند إلى دائرة متکاملة لاتلامسية قريبة:

- [ISO/IEC 14443-4] ويشمل ذلك جميع التعديلات والتصويبات المرتبطة بها؛
- [ISO/IEC 10373-6] الممثلة لمواصفات الاختبار بما في ذلك جميع التعديلات والتصويبات المرتبطة بها؛
- تكامل الإشارة من النوع A أو النوع B؛
- دعم بنية ملف على النحو المعروف بواسطة [ISO/IEC 7816-4] بالنسبة للملفات الشفافة متغيرة الطول؛
- الدعم لواحد أو أكثر من التطبيقات والأوامر [ISO/IEC 7816-4] الملائمة على النحو المحدد في الوثيقة Doc 9303؛

٢-٣ الخصائص الكهربائية

يجب أن تكون قوة التردد اللاسلكي وتكامل الإشارة على النحو المعروف في [ISO/IEC 14443-2]. ويوصى بحد أدنى قدره ٤٢٤ كيلوبت في الثانية لسرعة الارسال. واستخدام سمات EMD المحددة في [ISO/IEC 14443-2] اختياري.

٣-٣ الخصائص المادية

يوصى بأن يكون حجم مساحة هوائي الاقتران وفقاً لـ [ISO/IEC 14443-1] Class 1 (ID-1 antenna size) فقط.

٤-٣ بروتوكول الارسال

يجب أن تتحمّل وثيقة السفر الالكترونية المقرورة آلياً بروتوكول الارسال نصف المزدوج المعروف في [ISO/IEC 14443-4]. ويجب أن تحتمّل وثيقة السفر الالكترونية المقرورة آلياً إما النوع (أ) أو النوع (ب) من بروتوكول الارسال، وببروتوكولات الاستهلاك ومنع الاصطدام والإرسال وفقاً لـ [ISO/IEC 14443].

١-٤-٣ الطلب الأمر والإجابة عن الطلب

يجب أن تستجيب دائرة متكاملة لاتلامسية للطلب الأمر من النوع (أ) (REQA) أو الطلب الأمر من النوع (ب) (REQB) مع الإجابة عن الطلب من النوع (أ) (ATQA) أو الإجابة عن الطلب من النوع (ب) (ATQB)، حسب ما يكون ملائماً.

٢-٤-٣ المعرف العشوائي مقابل المعرف الثابت للدائرة متكاملة لاتلامسية

قد تُستخدم وثيقة السفر الالكترونية المقرورة آلياً كـ "منارة" ترسل الدائرة متكاملة لاتلامسية فيها معرفاً فريداً (UID) للنوع (أ)، وPUPI للنوع (ب) عند تشغيله في البداية. وقد يسمح هذا بالتعرف على سلطة الإصدار. ويسمح [ISO/IEC 14443] باختيار الخيار ما إذا كانت وثيقة السفر الالكترونية المقرورة آلياً تقدم معرفاً ثابتاً، مخصصاً بشكل فريد لوثيقة السفر الالكترونية المقرورة آلياً تلك، أو رقمًا عشوائياً، مختلفاً في كل بداية لحوار الاتصال. ويفضل بعض دول الإصدار تنفيذ رقم فريد لأسباب أمنية أو أي سبب آخر. وتعطي جهات إصدار أخرى أفضليّة أكبر للشواغل بشأن خصوصية البيانات وإمكانية تتبع الأشخاص بسبب معرفات دوائر متكاملة ثابتة.

اختيار أحد الخيارات أو خيار آخر لا يقل القابلية للتشغيل المتبدّل نظراً لأن أي جهاز قراءة طرفي عندما يكون ممثلاً للمعيار ISO/IEC 14443 سيفهم كلا الأسلوبين. ويوصى باستخدام معرفات عشوائية للدائرة متكاملة، لكن، يجوز للدول أن تختار تطبيق معرفات فريدة للنوع (أ) أو أجهزة PUPI للنوع (ب).

٥-٣ مجموعة الأوامر

جميع الأوامر والنماذج وبيانات الحالة عليها معزفة في [ISO/IEC 7816-4] و[ISO/IEC 7816-8] باستثناء الأمر FILE AND MEMORY MANAGEMENT. ويجب أن يكون الحد الأدنى من مجموعة الأوامر التي تحملها وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 كما يلي:

SELECT;

.READ BINARY

من المعروف أنه سيكون من المطلوب إصدار أوامر إضافية لتهيئة البيئة الأمنية الصحيحة وتنفيذ الأحكام الأمنية الاختيارية المعروفة في الوثيقة Doc 9303-11 دعماً بالأوامر الإضافية التالية:

GET CHALLENGE;
EXTERNAL AUTHENTICATE/MUTUAL AUTHENTICATE;
INTERNAL AUTHENTICATE;
MANAGE SECURITY ENVIRONMENT;
GENERAL AUTHENTICATE.

إذا كانت تطبيقات البنية LDS2 موجودة، يجب أن تدعم وثيقة السفر الإلكترونية المقرورة آلياً إضافة إلى ذلك الأوامر التالية:

بالنسبة لتطبيق سجلات السفر:

READ RECORD;
APPEND RECORD;
SEARCH RECORD;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

وبالنسبة لتطبيق سجلات التأشيرة:

READ RECORD;
APPEND RECORD;
SEARCH RECORD;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

وبالنسبة لتطبيق بيانات الاستدلال البيولوجي الإضافية:

UPDATE BINARY;
READ RECORD;
APPEND RECORD;
SEARCH RECORD;
ACTIVATE;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

يمكن الحصول على مزيد من التفاصيل بشأن بروتوكولات الأوامر في الوثيقة Doc 9303-11.

١-٥-٣ قم بالاختيار

تدعم وثيقة السفر الالكترونية المقرورة آلياً ذات البنية LDS1 أساليب اختيار ذات بندين هما معرف الملف ومعرف الملف الأولي القصير. وتدعم أجهزة القراءة واحداً من الأسلوبين على الأقل. ومعرف الملف ومعرف الملف الأولي القصير إلزامي لنظام تشغيل الدائرة المتكاملة الالامسية، لكنه اختياري بالنسبة لجهاز القراءة.

٢-٥-٣ اقرأ ثانياً

دعم الأمر اقرأ ثانياً ببأيت INS منفرد عن طريق وثيقة سفر الكترونية مقرورة آلياً مشروط. ويجب أن تدعم وثيقة السفر الالكترونية المقرورة آلياً هذا النوع من الأوامر إذا كانت تحتمل مجموعات بيانات بواقع ٣٢ ٧٦٨ بآيات أو أكثر.

٦-٣ أشكال الأوامر وخيارات البارامتراط (البنية LDS1 والبنية LDS2)

١-٦-٣ اختيار الملف المخصص للتطبيق باستخدام أمر الاختيار SELECT

يتعين اختيار التطبيقات بحسب اسم ملفها المخصص الذي يدل على معرف التطبيق (AID). وبعد اختيار تطبيق، يمكن الاطلاع على الملف داخل هذا التطبيق.

ملاحظة — يتعين أن تكون أسماء الملفات المخصصة فريدة. ولذلك فإن اختيار تطبيق باستخدام اسم الملف المخصص يمكن القيام به من أي مكان يطلب فيه.

١-٦-١-١ اختيار الملف الرئيسي

الجدول ١ — الأمر SELECT لاختيار الملف الرئيسي

CLA	'00'
INS	'A4'
P1	'00'
P2	'0C'
Lc field	Absent
Data field	Absent
Le field	Absent

الاستجابة للأمر SELECT

Data field	Absent
SW1-SW2	'9000' Normal processing Other values to indicate checking or execution errors

ملاحظة — يوصى بعدم استخدام الأمر .SELECT MF

٢-٦-٣ اختيار الملف المخصص للتطبيق

يجب اختيار أي ملف مخصص للتطبيق باستخدام الأمر SELECT مع اسم الملف المخصص الذي يشير إلى معرف التطبيق (AID). وترتدد أدناه بaramترات أمر وحدة بيانات بروتوكول التطبيق (APDU):

الجدول ٢ — الأمر SELECT مع معرف التطبيق لاختيار الملف المخصص للتطبيق

CLA	'00'
INS	'A4'
P1	'04'
P2	'0C'
Lc field	Length of the command data field
Data field	DF name (AID)
Le field	Absent

الاستجابة للأمر SELECT

Data field	Absent
SW1-SW2	'9000' Normal processing Other values to indicate checking or execution errors

٢-٦-٤ اختيار ملف أولي باستخدام الأمر SELECT

يتم اختيار الملف الأولي بواسطة الأمر SELECT مع معرف الملف الأولي. وعند اختيار الملف الأولي يتعمين التأكيد من أن الملف المخصص للتطبيق المخزن في داخله الملف الأولي قد سبق اختياره.

الجدول ٣ — الأمر SELECT مع معرف الملف لاختيار الملف الأولي

CLA	'00' / '0C'
INS	'A4'
P1	'02'
P2	'0C'
Lc field	'02'
Data field	File Identifier
Le field	Absent

الاستجابة للأمر SELECT

Data field	Absent
SW1-SW2	'9000' Normal processing Other values to indicate checking or execution errors

يجب أن تدعم وثيقة السفر الالكترونية المفروعة آلياً الأمر SELECT مع معرف الملف حسبما هو محدد في الجدول ٣ . ويجب أن يدعم نظام التفتيش واحداً من الأسلوبين التاليين على الأقل:

- الأمر SELECT مع معرف الملف حسبما هو محدد في الجدول ٣؛
- الأمر READ BINARY مع رمز INS متعادل ومعروف ملف أولي قصير SFI حسبما هو محدد في الجدول ٥ .

٣-٦-٣ قراءة البيانات من ملف أولي (READ BINARY)

يوجد أسلوبان لقراءة البيانات من وثيقة السفر الالكترونية المفروعة آلياً: عن طريق اختيار الملف الأولي ثم قراءة بيانات الملف الأولي المختار ، أو عن طريق قراءة البيانات مباشرة باستخدام معرف الملف الأولي القصير . ويكون دعم معرف الملف الأولي القصير إلزامياً من أجل وثيقة السفر الالكترونية المفروعة آلياً . ولذلك يوصى بأن يستخدم نظام التفتيش معرف الملف الأولي القصير .

١-٣-٦-٣ قراءة بيانات ملف أولي مختار (ملف شفاف)

الجدول ٤ – الأمر READ BINARY لاختيار ملف أولي

CLA	'00' / '0C'
INS	'B0'
P1	
P2	Offset
Lc field	Absent
Data field	Absent
Le field	Present for encoding Ne > 0

الاستجابة للأمر READ BINARY

Data field	Data read
SW1-SW2	'9000' Normal processing Other values to indicate checking or execution errors

٢-٣-٦-٣ قراءة بيانات باستخدام معرف الملف القصير (الملف الشفاف)

الجدول ٥ — الأمر READ BINARY مع معرف ملف أولي قصير

CLA	'00' / '0C'
INS	'B0'
P1	Short EF Identifier
P2	Offset
Lc field	Absent
Data field	Absent
Le field	Present for encoding $Ne > 0$. Maximum number of bytes expected in the response data field

الاستجابة للأمر READ BINARY

Data field	Data read
SW1-SW2	'9000' Normal processing Other values to indicate checking or execution errors

٤-٦-٣ دعم الممتدة Lc/Le

استناداً إلى حجم مواد علم الشيفرة (مثلاً المفاتيح العامة، التوقيعات)، يجب استخدام وحدات بيانات بروتوكول التطبيق ذات الخانات الممتدة لإرسال هذه البيانات إلى رقاقة وثيقة السفر الإلكترونية المقرورة آلياً. وللحصول على تفاصيل بشأن خانة الطول الممتدة، انظر ISO/IEC 7816-4.]

٣-٦-٤-١ الطول الممتدة ورقمات وثيقة السفر الإلكترونية المقرورة آلياً

بالنسبة لرقمات وثيقة السفر الإلكترونية المقرورة آلياً، فإن دعم خانة الطول الممتدة ملزماً. وإذا كانت خوارزميات علم الشيفرة وأحجام المفاتيح التي تختارها دولة الاصدار تتطلب استخدام خانة طول ممتدة، يجب أن تتحمل رقمات وثيقة السفر الإلكترونية المقرورة آلياً خانة طول ممتدة. وإذا كانت رقاقة وثيقة السفر الإلكترونية المقرورة آلياً تتحمل خانة طول ممتدة فيجب بيان هذا في EF.ATR/INFO أو في ATS على النحو المحدد في [ISO/IEC 7816-4].

٣-٦-٤-٢ الوحدات الطرفية

بالنسبة للوحدات الطرفية، من المطلوب دعم الطول الممتدة. وينبغي أن تفحص أي وحدة طرفية ما إذا كان أو لم يكن الدعم لخانة الطول الممتدة مبيتاً في ATR/ATS أو في EF.ATR/INFO لرقاقة وثيقة السفر المقرورة آلياً قبل استخدام هذا الخيار. ويجب أن لا تستخدم الوحدة الطرفية خانة الطول الممتدة من أجل وحدات بيانات بروتوكول التطبيق غير الأوامر التالية ما لم تكون أحجام المدخل الدقيق ومخرج الحماية لرقاقة وثيقة السفر الإلكترونية المقرورة آلياً مبيتاً صراحة في على النحو المحدد في EF.ATR/INFO أو في ATS.

- MSE:Set KAT
- GENERAL AUTHENTICATE

٥-٦-٣ تسلسل الأوامر

يجب استخدام تسلسل الأوامر بالنسبة لأمر التحقق العام (GENERAL AUTHENTICATE) لربط سلسلة الأوامر بتنفيذ البروتوكول. ويجب عدم استخدام تسلسل الأوامر لأغراض أخرى ما لم تبين الرقاقة ذلك بوضوح. وللمزيد من التفاصيل بشأن تسلسل الأوامر، انظر -[4] ISO/IEC 7816-

٦-٦-٣ الملفات الأولية الأكبر من ٣٢ ٧٦٧ بايت

الحجم الأقصى لأي ملف أولي هو عادة ٣٢ ٧٦٧ بايت، لكن بعض الدوائر المتكاملة اللاتلامسية تحمل ملفات أكبر. ومن المطلوب خيار بارامتر (READ BINARY) مختلف وشكل أمر للاطلاع على منطقة البيانات عندما يكون التعويض أكبر من ٣٢ ٧٦٧. وهذا الشكل للأمر ينبغي استخدامه بعد تحديد طول النموذج وتحديد الحاجة للاطلاع على البيانات في منطقة بيانات موسعة. وعلى سبيل المثال، إذا كانت منطقة البيانات تحتوي على مواد بيانات متعددة للاستدلال البيولوجي، فقد لا يكون من الضروري قراءة منطقة البيانات كلها. وبمجرد أن يكون التعويض لمنطقة البيانات أكبر من ٣٢ ٧٦٧، ينبغي استخدام هذا الشكل للأمر. ويوضع التعويض في خانة الأمر بدلاً عن وضعه في البارامترين P1 و P2.

الجدول ٦ — شكل الأمر READ BINARY عندما يكون التعويض أكبر من ٣٢ ٧٦٧ بايت

CLA	'00' / '0C'
INS	'B1'
P1	See Table 7
P2	
Lc field	Length of the command data field
Data field	Offset DO'54'
Le field	Present for encoding Ne > 0. Maximum number of bytes expected in the response data field

الاستجابة للأمر READ BINARY

Data field	Discretionary DO'53'
SW1-SW2	'9000' Normal processing Other values to indicate checking or execution errors

الجدول ٧ — الترميز P1-P2 للأمر INS=B1 مع READ BINARY

P1								P2								Meaning
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	Selected EF
0	0	0	0	0	0	0	0	0	0	0	Not all equal					Short EF identifier
Not all zero								X	X	X	X	X	EF identifier			

كل من خانتي الطول والقيمة لمادة البيانات BER-TLV يتفاوت طولهما ويمكن تمييزهما بطرق مختلفة (انظر [ISO/IEC 7816-4]: “BER-TLV”).

لأسباب تتعلق بالأداء، ينبغي إبقاء الاتصال بين وثيقة السفر الإلكترونية المقرورة آلياً والوحدة الطرفية أقصر ما يمكن. ولذلك فإن خانتي الطول والقيمة في مادة البيانات BER-TLV ينبغي أن تكون أقصر ما يمكن. ولا ينطبق هذا على مواد بيانات التعويض في أوامر INS READ INS READ BINARY المفرودة فحسب بل أيضاً على جميع مواد البيانات BER-TLV الأخرى المتداخلة بين وثيقة السفر الإلكترونية المقرورة آلياً والوحدة الطرفية.

فيما يلي أمثلة للتعويض المرمز في خانة البيانات:

- '0001' is encoded as Tag = '54' Length = '01' Value = '01'
- Offset: 'FFFF' is encoded as Tag = '54' Length = '02' Value = 'FFFF'

يجب أن تحدد أوامر READ BINARY التالية التعويض في خانة البيانات. وينبغي أن يطلب الأمر READ BINARY النهائي مساحة البيانات المتبقية.

وفيما يتعلق ب[ISO/IEC 7816-4]، لا توجد قيود محددة على التعويض إذا كانت البة 1 في INS مضبوطة على 1 للسماح باستخدام أوسع الملاحظة 1 — في بعض الحالات، يوجد وثائق سفر إلكترونية مقرورة آلياً لا يمكن فيها التداخل بين B1 وبين الأوامر الثانية التقليدية B0 READ Binary. وبعبارة أخرى، ينبغي استخدام B0 فقط لقراءة أول ٣٢ بايت و B1 من K ٣٢ بايت. ولأغراض أخرى يمكن أن يوجد تداخل صغير لـ ٢٥٦ بايت حول عتبة ٣٢ ٧٦٧ للسماح بانتقال أسلس بين B0 و B1. وهذه المجموعة الأخيرة، يمكن استخدام B1 منذ بداية الملف، أي مع تعويض بيدأ من ٠ للسماح باستخدام نفس الأمر لقراءة المضمون الكامل.

الملاحظة 2 — لا يوجد استخدام البايت المنفرد INS بواسطة نظام التفتيش إذا كان حجم ملف أولي ٣٢ ٧٦٧ بايت أو أقل.

٧-٣ التعامل مع السجلات والأوامر (LDS2)

يجب تخزين سجلات السفر وسجلات التأشيرة والشهادات في ملف أولي تحت التطبيقات الخاصة بها وأن يكون لها بنية خطية مع سجلات متغيرة الحجم. انظر الشكلين ٤ و ٥.

ويجب أن يشار إلى السجلات داخل كل ملف أولي برقم السجل. ويجب أن يكون رقم كل سجل فريداً ومتسلسلاً (الإشارة بصفر للسجل الذي تم اختياره لا تدرج ضمن نطاق هذه الوثيقة).

وداخل كل ملف أولي يدعم بنية خطية، يجب أن تSEND أرقام السجلات بشكل متسلسل عند إلهاقها، مثلًا حسب ترتيب إنشائهما: فالسجل الأول (رقم واحد) هو السجل الذي أنشئ أولاً.

ويجب استخدام الأوامر [ISO/IEC 7816-4] التالية للاطلاع على السجلات:

- | | | |
|--|----------------|---|
| إلحاق سجلات السفر والتأشيرات والشهادات، | APPEND RECORD | • |
| قراءة سجل واحد أو أكثر من سجلات السفر والتأشيرات والشهادات؛ | READ RECORD(S) | • |
| البحث عن سجل واحد أو أكثر من سجلات السفر والتأشيرات والشهادات. | SEARCH RECORD | • |

ملاحظة — تعرف المختصرات المستخدمة في هذا القسم الفرعى في [ISO/IEC 7816-4].

١-٧-٣ الأمر APPEND RECORD

يستهل هذا الأمر إلحاق سجل جديد بنهاية البنية الخطية.

الجدول ٨ — الأمر APPEND RECORD

CLA	'0C'
INS	'E2'
P1	'00' (any other value is invalid)
P2	See Table 10
Lc field	Length of the command data field
Data field	Record to be appended
Le field	Absent

الجدول ٩ — الاستجابة للأمر APPEND RECORD

Data field	Absent
SW1-SW2	'9000' Normal processing; '6A84' Not enough memory space in the file; '6700' Wrong length (the record to be appended is longer than the specified maximum length); Other values to indicate checking or execution errors

الجدول ١٠ — ترميز P2 في الأمر APPEND RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	-	-	-	Short EF identifier
-	-	-	-	-	0	0	0	Any other value is RFU

٢-٧-٣ الأمر READ RECORD

يستعيد هذا الأمر المحتوى الكلي أو الجزئي لسجل واحد أو أكثر من سجلات الملف الأولى المختار المعالج. وتبعاً لحجم السجل ومحتوى خانة Le، تتضمن خانة بيانات الاستجابة أيًّا مما يلي:

- الجزء الأول من السجل المعالج؛
- سجل (أو أكثر) من السجلات المعالجة؛
- سجل (أو أكثر) من السجلات المعالجة بالكامل والتي يليها الجزء الأول من السجل التالي.

انظر [ISO/IEC 7816-4] للحصول على التفاصيل والمرفق (ح) للاطلاع على مثال عن قراءة أحد سجلات السفر.

ويوضح الشكل ٢ خانة بيانات الاستجابة. وتبيَن المقارنة بين Nr وبنية TLV ما إذا السجل الوحيد (قراءة سجل واحد) أو السجل الأخير (قراءة جميع السجلات) غير كامل أو كاملاً أو محشوًأ.

الجدول ١١ — الأمر READ RECORD

CLA	'0C'	
INS	'B2'	
P1	Record number ('00' references the current record)	
P2	See Table 13	
Lc field	Absent	
Data field	INS = 'B2'	Absent
Le field	Maximum number of bytes to be read encoded as extended length field; Le = '00 00 00' (any other value is out of scope of the specification)	

الجدول ١٢ — الاستجابة للأمر READ RECORD

Data field	Data read
SW1-SW2	'9000' Normal processing; '6A83' (Record not found); Other values to indicate checking or execution errors

الجدول ١٣ — ترميز P2 في الأمر READ RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	-	-	-	Short EF identifier
-	-	-	-	-	1	x	x	Record number in P1
-	-	-	-	-	1	0	0	— Read record P1
-	-	-	-	-	1	0	1	— Read all records from P1 up to the last

الملاحظة ١ — لا تدرج مجموعات الباتات الأخرى ضمن نطاق هذه المعاصفة. وإذا لم تكن خانة Le تتضمن إلا مجموعة البات ٠٠، ينبغي عندئذ أن يقرأ الأمر بالكامل إما السجل المطلوب وحده أو التسلسل المطلوب من السجلات، وذلك تبعاً للباتات ٣ و ٢ و ١ من P2 و ضمن حد الطول الأقصى المدعوم لخانة Le الممتدة.

الملاحظة ٢ — لا يدرج الأمر READ RECORD ذو خانات الطول القصيرة ضمن نطاق هذه المعاصفة.

الحالة أ — قراءة كاملة لسجل واحد (تحتوي الخانة Le فقط على مجموعة البات ٠٠)

Record	5F44 L V 73 L V ... 5F37 L V 5F38 L V
	READ RECORD response (P2 = '04', Le = 0):
	5F44 L V 73 L V ... 5F37 L V 5F38 L V

الحالة ب — قراءة عدة سجلات حتى نهاية الملف (تحتوي الخانة Le فقط على مجموعة البايت '00،)

السجل ١	السجل ٢	السجل ×
5F44 L V ... 5F38 L V	5F44 L V ... 5F38 L V	...
(P2 = '05', Le = 0):		
5F44 L V ... 5F38 L V 5F44 L V ... 5F38 L V ...		

الشكل ٢ — خانات بيانات الاستجابة

٣-٧-٣ الأمر SEARCH RECORD

يستهل هذا الأمر البحث في السجلات المخزنة في الملف الأولي الخاص بها. وتحتوي خانة بيانات الأمر على مناولة السجل 'DO'7F76 التي تعرف مرجع الملف وتشكلية البحث وسلسلة البحث (انظر الجدول ١٧). تعيّد خانة بيانات الاستجابة مرجع الملف 'DO'7F76 الذي يتضمن واحداً أو أكثر من المراجع 'DO'02' ويتضمن رقم السجل الذي يتطابق مع معايير البحث داخل الملف الأولي المعالج. وفي الملف الأولي الذي يدعم سجلات متغيرة الحجم ذات بنية خطية، قد لا يأخذ البحث في الاعتبار السجلات التي تكون نافذة البحث فيها أقصر من سلسلة البحث.

الجدول ١٤ — الأمر SEARCH RECORD

CLA	'0C'
INS	'A2'
P1	'00'
P2	See Table 16
Lc field	Length of command data field
Data field	Record handling DO'7F76' (See Table 17)
Le field	'00' (short length) or '00 00' (extended length)

الجدول ١٥ — الاستجابة للأمر SEARCH RECORD

Data field	Record handling template DO'7F76' containing one file reference DO'51' with one or more integer DO'02' and containing a record number matching the search criteria
SW1-SW2	'9000' Normal processing; '6282' Warning: Unsuccessful search Other values to indicate checking or execution errors

ملاحظة — قد يكون حقل بيانات الاستجابة غائباً إذا لم يتم العثور على تطابق.

الجدول ١٦ — ترميز P2 في الأمر SEARCH RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	1	1	1	0	0	0	Search record through multiple EFs
Any other value is RFU.								

الجدول ١٧ — نموذج مناولة الملفات في البحث المعزز عن سجلات متعددة

Tag	Value			Notes
'7F76'				Record handling DO
	Tag	Value		
	'51'	File identifier or short EF identifier		File reference DO
	'A1'			Search configuration template
	Tag	Value		
	'80'	'00' / '30'		Search configuration parameter: - search in record number ascending order - step-width for the search: byte-wise - search termination: '00' - Search all addressed records '30' - Terminate search after the first match
	'B0'			Search window template
		Tag	Value	
		'02'	Offset	
		'02'	Number of bytes	
	Tag	Value		
	'A3'			Search string template
	Tag	Value		
	'B1'			
		Tag	Value	
		'81'	Search string	

الملاحظة ١ — لا يتم دعم تعويض خالٍ DO في نموذج نافذة البحث.

الملاحظة ٢ — إذا كان نموذج نافذة البحث يستعمل القيمة '00' لعدد البایتات، يجب على رقاقة وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS2 أن تبحث عن جميع البایتات من التعويض الموجود في السجلات.

الملحوظة ٣ — لا يدعم الأمر SEARCH RECORD إلا المراجع DOS المحددة في الجدول ١٧ . وهذا يعني ضمناً أن الأمر SEARCH RECORD يدعم بالضبط مرجع ملف واحد DO في مناولة الملف DO وسلسلة بحث واحدة بالضبط في نموذج سلسلة البحث . وقد يتجاهل الأمر مراجع DOS إضافية أو يجب برمز خطأ في حال استعمال مراجع DOS إضافية .

٨-٣ التعامل مع الملفات الشفافة وغيرها (LDS2)

تتولى جهة إصدار وثيقة السفر الإلكترونية المفروعة آلياً ذات البنية LDS2 في حالة إبطال التشغيل إنشاء الملفات الأولية الإضافية للاستدلال البيولوجي (تقع آلية الإنشاء خارج نطاق هذه الموصفة) . وفي حالة الإبطال، يمكن أن يتم اختيار الملف الأولي بشكل مكتوب أو تحديه أو قراءته بمجرد الحصول على أذونات مناسبة .

ويجب استخدام الأوامر [ISO/IEC 7816-4] من أجل كتابة وقراءة الملفات الأولية الإضافية للاستدلال البيولوجي :

- | | |
|---|-----------------|
| كتابة معلومات الاستدلال البيولوجي الإضافية؛ | UPDATE BINARY • |
| قراءة معلومات الاستدلال البيولوجي الإضافية. | READ BINARY • |

ويجب استخدام الأمر [ISO/IEC 7816-9] لتفعيل الملف الأولي الشفاف بعد تلبية شروط الاطلاع على كتابة وقراءة البنية LDS2 :

- تفعيل الملف الأولي للاستدلال البيولوجي الإضافي. ACTIVATE •

ملحوظة — ترد المختصرات المستخدمة في هذا القسم الفرعية في [ISO/IEC 7816-4] .

وفي حالة التفعيل، يمكن اختيار وقراءة الملف الأولي بمجرد الحصول على أذونات مناسبة (متعلقة بحالة التفعيل) ولا يوجد توقيض من أي نوع يسمح بكتابة الملف الأولي الشفاف أو الإضافة إليه .

يجب أن يستخدم الأمر "إدارة الملف والذاكرة" (FMM) قبل الكتابة لتحديد ما إذا كان هناك حيز كاف متاح من الذاكرة في الملف الأولي . يتضمن الرد على الأمر FMM مجموعة من مواد البيانات تمثل المعلومات المطلوبة عن الملف وحجم الذاكرة .

- يجب أن يحتوي أول أمر UPDATE BINARY (INS مفرد) على المراجع DOS التالية في خانة البيانات:

- DO'54' ويتضمن التعويض '00'؛
- DO'53' الذي قد يتضمن الكتلة الأولى من البيانات المزمع تخزينها . وقد يكون هذا المرجع DO حالياً ('53 00');
- ويكون المرجع 'DO'C0' المسجل الملكية الذي يبين الحجم الإجمالي للملف الأولي (حجم الذاكرة التي يجب تخصيصها) اختيارياً.

الملحوظة ١ — يجوز لوثيقة السفر الإلكترونية المفروعة آلياً ذات البنية LDS2 أن تستخدم المعلومات عن حجم الملف الأولي في المرجع 'DO'C0' من أجل تخصيص الذاكرة الداخلية (مثلاً من أجل التخصيص الدينامي الصريح للذاكرة) . وإذا لم تدعم وثيقة السفر الإلكترونية المفروعة آلياً ذات البنية LDS2 المرجع DO للمعلومات عن حجم الملف الأولي (مثلاً عندما تخصص جهة الإصدار الذاكرة بطريقة إحصائية، أو عندما تدعم وثيقة السفر الإلكترونية المفروعة آلياً ذات البنية LDS2 إعادة تخصيص دينامي وصريح للذاكرة)، يمكن عندئذ لوثيقة السفر الإلكترونية المفروعة آلياً ذات البنية LDS2 أن تتجاهل المرجع 'DO'C0'، وأن تستمر بكتابة الكتلة الأولى من الملف الأولي وتعيد '9000'، أو يمكن أن تعيد الخطأ '6A80' في حال وجود بارامتر غير صحيح في خانة بيانات الأمر .

الملحوظة ٢ — إذا أعادت وثيقة السفر الإلكترونية المقررة آلياً ذات البنية *LDS2* أي خطأ في استجابة للأمر *UPDATE* مع المرجع *DO'C0*' المسجل الملكية، يجب على نظام التقىش أن يرسل عندئذ الأمر *UPDATE BINARY* [ISO/IEC 7816-4] مع تعويض *INS* مفرد) مع تعويض *DO'54* و *'53* بقيمة صفر، من دون *'C0*'.

- ينبغي أن تستخدم الأوامر *INS* *UPDATE BINARY* (مفرد، من دون *'C0*) اللاحقة التعويض *n+1* حيث تشير *n* إلى عدد البيانات المكتوبة حتى الآن في معلومات الاستدلال البيولوجي، أي ينبغي أن تكتب الوحدة الطرفية بيانات الملف الأولى بشكل متسلسل من دون وجود فراغ أو تداخل بين أمرين متاليين من أوامر *UPDATE BINARY*.
- يمكن استخدام الأمر *READ BINARY* بعد أي أمر *UPDATE BINARY* للتحقق من البيانات المكتوبة في الملف الأولى.
- يجب أن ينهي الأمر *ACTIVATE* إضفاء الطابع الشخصي لمعلومات الاستدلال البيولوجي من خلال تعطيل الكتابة في الملف الأولى بصورة دائمة.

١٨-٣ الأمر *UPDATE BINARY*

يجب على الدائرة المنكاملة اللاتلasmية التي تدعم تطبيق الاستدلال البيولوجي الإضافي أن تدعم الأمر *UPDATE BINARY* مع بait *INS* مفرد '*D7*' وفقاً للجدول ١٨.

يتحدد التعويض من قيمة مادة بيانات التعويض *BER-TLV* في خانة بيانات الأمر؛ وتحدد البيانات المزمع كتابتها من قيمة مادة البيانات التقديرية *BER-TLV* في خانة بيانات الأمر؛ ويتحدد الحجم الإجمالي للملف الأولى من قيمة المادة الاختيارية لبيانات حجم الملف *BER-TLV* في خانة بيانات الأمر. وينبغي تمييز مواد بيانات *BER-TLV* في أقرب وقت ممكن.

وعندما يكون لخانة بيانات الأمر *UPDATE BINARY* المرجع '*DO'C0*' المسجل الملكية، يجب أن تضبط البة ٨ في البايت *CLA* للأمر *APDU MUST* على ١ (*CLA = '8C'*).

الجدول ١٨ — الأمر *UPDATE BINARY* مع *INS* مفرد

<i>CLA</i>	'0C' / '8C'
<i>INS</i>	'D7'
<i>P1</i>	File identifier
<i>P2</i>	'00 00' identifies the current EF
<i>Lc</i>	Length of the command data field
<i>Data field</i>	Offset Data Object (tag '54') Discretionary Data Object (tag '53') File Size Data Object (tag 'C0') (optional)
<i>Le</i>	Absent

الجدول ١٩ — الاستجابة للأمر *UPDATE BINARY*

<i>Data field</i>	Absent
<i>SW1-SW2</i>	'9000' Normal processing; '6A84' (Not enough memory space in the file) '6A80' Incorrect parameters in the command data field (e.g., <i>DO'C0</i> not

supported) '6982' Security status not satisfied: The EF.Biometrics is in EF Activated state Other values to indicate checking or execution errors

وإذا لم يتبغ نظام التفتيش التسلسلي UPDATE BINARY كما هو محدد في القسم ٨-٣ (أي لا يبدأ أول UPDATE BINARY عند التعويض)، يمكن لوثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS2 أن تنهي الأمر UPDATE BINARY بخطأ.

٢-١-٣ الأمر ACTIVATE

يستهل الأمر ACTIVATE انتقال الملف الأولي للاستدلال البيولوجي الإضافي الذي تم اختياره حالياً من حالة إبطال التفعيل إلى حالة التفعيل.

ACTIVATE — الأمر ٢٠

CLA	'0C'
INS	'44'
P1	'00'
P2	'00'
Lc	Absent
Data field	Absent
Le	Absent

ACTIVATE — الاستجابة للأمر ٢١

Data field	Absent
SW1-SW2	'9000' Normal processing; Other values to indicate checking or execution errors <i>Note 1.— SW1-SW2 = '61XX' (normal processing) and SW1-SW2 = '62XX' or '63XX' (warning processing) are out of scope of this document.</i>

وبعد تنفيذ هذا الأمر بنجاح، يجب تحويل الملف الأولي للاستدلال البيولوجي الإضافي الذي تم اختياره حالياً إلى حالة التفعيل. وفي حال حدوث أخطاء (SW مختلفة عن '9000')، يجب أن يبقى الملف الأولي للاستدلال البيولوجي الإضافي الذي تم اختياره حالياً في حالة إبطال التفعيل.

وبعد تنفيذ هذا الأمر مباشرة ('9000'=SW1-SW2)، يجب أن يكون الإذن الفعلي المطلوب لاتخاذ إجراء بشأن الملف الأولي للاستدلال البيولوجي هو الإذن المطابق لحالة التفعيل (وفقاً للجدول ٩٨). ويجب أن لا يرتب الإذن الفعلي المطابق لحالة إبطال التفعيل أي حقوق للاطلاع على الملف الأولي للاستدلال البيولوجي.

٣-١-٣ الأمر FILE AND MEMORY MANAGEMENT (ادارة الملف والذاكرة)

يبدأ الأمر FILE AND MEMORY MANAGEMENT (FMM) باستفسار عن حجم الذاكرة المستخدمة أو الحرة للملف الأولي المعالج. ويقدم هذا الأمر لوثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS2 بوصفها مسجلة الملكية. ويمكن استخدام هذا الأمر للتحقق من الحيز الحر المتوفّر للملف الأولي المعالج قبل الكتابة أو الإضافة. كما يمكن استخدام هذا الأمر للحصول على رقم آخر سجل الحق من أجل القراءة. ويبين P1 طريقة مخاطبة الملف الأولي، حيث يمكن استخدام الملف الأولي الحالي أو مرجع الملف 'DO'51'. ويبين P2 محتوى الاستفسار. ويتوفر العدد الإجمالي للبيانات في الملف الأولي المعالج مع بنية شفافة أو بنية السجل وعدد السجلات القائمة أو

المتبقي للملف الأولي المعالج. ويشمل العدد الإجمالي للبيانات المتوفرة في الملف الأولي من دون أي معلومات بنوية. ويستثنى هذا العدد أي معلومات بنوية يمكن أن تطلبها رقاقة وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS2. والافتراض بشأن عدد السجلات المتبقية هو أن حجم السجلات المتبقية هو بحد الأقصى. وبعد نجاح الأمر FMM، يصبح الملف الأولي المشار إليه الملف الأولي الحالي.

الجدول ٢٢ — الأمر (FMM) وادارة الملفات و الذاكرة

CLA	'8C'	
INS	'5F'	
P1	See Table 23	
P2	See Table 24	
Lc	Absent for encoding Nc = 0, present for encoding Nc > 0	
Data field	P1 = '00'	Absent
	P1 = '01'	File reference DO'51' (See [ISO/IEC 7816-4])
Le	'00'	

يحدد P1 طريقة اختيار الملف الأولى، ويتضمن P2 خريطة بات تحدد المعلومات التي يجب إدراجها في الاستجابة.

الحدول ٢٣ — ترميز P1 في الأمر FILE AND MEMORY MANAGEMENT (FMM)

b8	b7	b6	b5	b4	b3	b2	b1		Meaning
0	0	0	0	0	0	0	0		Current EF
0	0	0	0	0	0	0	1		File reference DO'51' in the command data field

Any other value is RFU.

الجدول ٤ - ترميز P2 في الأمر FMM

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	1	Total number of bytes in the addressed EF
-	-	-	-	-	-	1	-	Number of remaining records in the addressed record EF
-	-	-	-	-	1	-	-	Number of existing records in the addressed record EF
x	x	x	x	x	-	-	-	00000 (any other value is RFU)

Any other value is RFU.

الجدول ٢٥ — ترميز 'DO'51' في خانة بيانات الأمر (FMM)

Tag	Length	Value
'51'	1	Short EF identifier (bits b8 to b4 encode a number from 1 to 30; bits b3 to b1 are set to 000)
	2	File identifier

تحتوي استجابة أمر بيانات FMM على مجموعة من الرسائل الآمنة DOs تمثل الملف المطلوب ومعلومات حجم الذاكرة.

الجدول ٢٦ — الاستجابة للأمر (FMM)

Data field	Absent or control information according to P2. See Table 27.
SW1-SW2	'9000', checking or execution errors as per [ISO/IEC 7816-4]

الجدول ٢٧ — إدارة الملفات والذاكرة

Tag	Length	Value		
'7F78'	Var	File and memory management DOs		
		Tag	Len	Value
		'81'	Var	Total number of bytes in the addressed EF
		'82'	Var	Number of remaining records in the addressed record EF
		'83'	Var	Number of existing records in the addressed record EF

الملاحظة ١ — يجب أن تعيد وثيقة السفر الإلكترونية المقروءة آلياً ذات البنية LDS2 فقط مواد البيانات في DO FMM التي تطلب بواسطة P2.

الملاحظة ٢ — لا تكون بيانات الاستجابة للأمر FMM صالحة إلا للملف الأولي المحدد. وقد لا تكون بيانات الاستجابة للأمر FMM الواردة من ملفات أولية مختلفة مستقلة عن بعضها البعض، مثلاً إذا كانت الملفات الأولية المختلفة تشارك في الذاكرة المتاحة. وينبغي أن يأخذ نظام التعقب ذلك في الاعتبار إذا جمعت بيانات استجابة ملفات أولية مختلفة للأمر FMM.

الملاحظة ٣ — عند تطبيق الرسائل الآمنة على الأمر FMM، يجب استخدام الرسائل الآمنة 'DO'85' لتغليف بيانات الأمر المشفرة.

٩-٣ مواصفات بنية الملف

تكون المعلومات في أي وثيقة سفر الكترونية مقروءة آلياً ذات البنية LDS2 مخزنة في نظام ملفات معروف في [ISO/IEC 7816-4]. ونظام الملفات منظم هرمياً في ملفات مخصصة (DFs) وملفات أولية (EFs). وتحتوي الملفات المخصصة (DFs) على ملفات أولية أو ملفات مخصصة أخرى. ويحوز أن يكون أحد الملفات الرئيسي الاختيارية (MF) الجذر لنظام الملفات.

ملاحظة — تتحدد الحاجة إلى ملف رئيسي باختيار نظم التشغيل وتطبيقات LDS1 أو LDS2 وظروف الإطلاق الاختياري.

١-٩-٣ ترميز البيانات

يسمح بأنواع الترميز التالية لعناصر البيانات:

A = سمة أبجدية [a-z, A-Z]؛

N = سمة رقمية [0-9]؛

S = سمة خاصة [<,>]؛

B = سمة ثنائية؛

UTF-8 = سمات مرمرة بحسب الترميز الموحد .UNICODE

الترميز UTF-8 لرموز UNICODE :

- بالنسبة لأي سمة تساوي أو تقل عن ١٢٧ (‘7F’ hex)، يستخدم الترميز UTF-8 بait واحد يكُون مشابهاً تماماً للقيمة ASCII.
- بالنسبة للرموز التي تساوي ٤٧ (‘07FF’ hex)، يستخدم الترميز UTF-8 اثنين من البايتات:
 - في البايت الأول تكون البتتان الأكثر دلالة محددين والبتة الثالثة خالية (أي من ‘C2’ hex إلى ‘DF’ hex)؛
 - في البايت الثاني تكون البتة الأكثر دلالة محددة والبتة الثانية خالية (أي من ‘80’ إلى ‘BF’ hex)؛
- بالنسبة لجميع الرموز التي تساوي أو تزيد على ٥٣٥ (‘FFFF’ hex)، يستخدم الترميز UTF-8 ثلاثة بايتات.

١٠-٣ اختيار التطبيق - الملف المخصص

يجب أن تتحمّل وثائق السفر الإلكترونية المقرورة آلياً تطبيقاً واحداً على الأقل كما يلي:

- تطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 إلزامي:
 - يجب أن يتّألف تطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 من بيانات سجّاتها دولة أو منظمة الاصدار، ومن مجموعات البيانات من ١ إلى ٦ إلى جانب المادة الأمنية للوثيقة (EF.SOD)؛
 - تتّألف المادة الأمنية للوثيقة (EF.SOD) داخل تطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 من قيم البصمات الرقمية كما هي معرفة في الوثيقة 9303-11 Doc 9303-12 والوثيقة 9303-12 Doc 9303-12 لمجموعات البيانات المستخدمة، وهي مطلوبة للتحقق من صحة البيانات التي أنشأتها جهة الاصدار والمخزنة في تطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1.
 - يمكن لتطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 أن يدعم اختيارياً تطبيقات البنية LDS2 الإضافية الواردة في الوثيقة Doc 9303 باعتباره:
 - تطبيق سجلات السفر؛
 - وتطبيق سجلات التأشيرة؛
 - وتطبيق بيانات الاستدلال البيولوجي الإضافية.

بالإضافة إلى ذلك، قد ترغب دول أو منظمات الاصدار في إضافة تطبيقات أخرى. ويجب أن تلائم بنية الملف مثل هذه التطبيقات الإضافية، لكن تفاصيل هذه التطبيقات تقع خارج نطاق الوثيقة Doc 9303.

يجب اختيار تطبيقات البنية LDS1 و LDS2 باستخدام تعريف التطبيق كإسم ملف مخصص محجوز. ويجب أن يتتألف تعريف التطبيق من معرف التطبيق المسجل الذي عينته المنظمة الدولية لتوحيد المقاييس وفقاً لـ [ISO/IEC 7816-5] وامتداد لمعرف تطبيق الملكية (PIX) على النحو المحدد في هذه الوثيقة:

ويستخدم سياق وثيقة السفر الإلكترونية المقررة آلياً ذات البنية LDS1 خطتين مختلفتين لتخصيص وسم فئة التطبيق، على النحو المحدد في الوثيقة 10-6 [ISO/IEC 7816-6] (وسم ما بين الصناعات):

- يستخدم كل من EF.INFO و EF.ATR/INFO خطة تخصيص وسم ما بين الصناعات؛
- تستخدم الملفات المخصصة وملفاتها الأولية خطة تخصيص الوسم.

وتحتاج وسوم ما بين الصناعات المحددة في هذه الوثيقة في سياق بنية المعلومات المنطقية، وبالتالي فإن خطة تخصيص الوسوم المتعاشة ليست ضرورية.

١١-٣ الملفات الأولية المشتركة

يمكن أن توجد الملفات الأولية لتطبيقات LDS1 و LDS2 في إطار الملف الرئيسي:

- الملف الأولي EF.ATR/INFO؛
- والملف الأولي EF.DIR؛
- والملف الأولي EF.CardAccess؛
- والملف الأولي EF.CardSecurity.

١-١١-٣ الملف الأولي EF.ATR/INFO (مشروع)

الملف الأولي EF.ATR/INFO هو ملف أولي شفاف يرد في الملف الرئيسي ويكون طلبه مشروطاً بوجود تطبيق LDS2 الاختياري. ويكون الملف الأولي اختيارياً فقط إذا كان تطبيق LDS1 موجوداً. ويتمثل معرف الملف الأولي القصير على مستوى الملف الرئيسي بالقيمة '01'.

الجدول — ٢٨ EF.ATR/INFO

File Name	EF.ATR/INFO
File ID	'2F01'
Short EF Identifier	'01'
Select Access	ALWAYS
Read Access	ALWAYS
Write/Update/Erase Access	NEVER
File structure	Transparent
Size	Variable

يمكن استرجاع محتويات الملف الأولي EF.ATR/INFO باستخدام الأمر SELECT يليه الأمر READ BINARY. وتحتوي خانة بيانات الاستجابة للأمر READ BINARY على محتوى الملف الأولي EF.ATR/INFO.

الجدول ٢٩ — عناصر بيانات الملف الأولي EF.ATR/INFO للبنية LDS2

Tag	Length	Value	Notes										
'47'	'03'	Card capabilities											
		byte 1 - first software function	b8 = 1: DF selection by full DF name b7 to b4 and b1 are out of scope of Doc 9303 b3 = 1: short EF identifier supported b2 = 1: record number supported										
		byte 2 - second software function	b8, b7, b6 and b5 are out of scope of Doc 9303 b4 to b1 = 0001: one byte data unit size										
'7F66'	Var	Extended length information											
		<table border="1"> <thead> <tr> <th>Tag</th><th>Length</th><th>Value</th><th>Notes</th></tr> </thead> <tbody> <tr> <td>'02'</td><td>Var</td><td>Positive integer - the maximum number of bytes in a command APDU</td><td>MUST be at least 1 000 (decimal) for LDS2</td></tr> <tr> <td>'02'</td><td>Var</td><td>Positive integer - the maximum number of bytes expected in the response APDU</td><td>MUST be at least 1 000 (decimal) for LDS2</td></tr> </tbody> </table>	Tag	Length	Value	Notes	'02'	Var	Positive integer - the maximum number of bytes in a command APDU	MUST be at least 1 000 (decimal) for LDS2	'02'	Var	Positive integer - the maximum number of bytes expected in the response APDU
Tag	Length	Value	Notes										
'02'	Var	Positive integer - the maximum number of bytes in a command APDU	MUST be at least 1 000 (decimal) for LDS2										
'02'	Var	Positive integer - the maximum number of bytes expected in the response APDU	MUST be at least 1 000 (decimal) for LDS2										

الملاحظة ١ — قد يوجد المزيد من مواد البيانات في الملف الأولي EF.ATR/INFO.

الملاحظة ٢ — يستخدم الملف الأولي EF.ATR/INFO خطة تخصيص وسم ما بين الصناعات على النحو المعروف في

[ISO/IEC 7816-4]

٢-١١-٣ الملف الأولي EF.DIR (مشروط)

الملف الأولي EF.DIR هو ملف أولي شفاف يحتوي عليه الملف الرئيسي المعرف في [ISO/IEC 7816-4]. وهو مطلوب شرطياً إذا كانت تطبيقات LDS2 الاختيارية موجودة. وإذا كان أي من تطبيقات LDS2 الاختيارية موجوداً يجب أن يدرج الملف الأولي EF:DIR في Security/Infos في الملف الأولي EF.DIR. ويمكن الاطلاع على وصف كامل له EF.CardSecurity في الوثيقة Doc 9303-11. ويتمثل معرف الملف الأولي القصير على مستوى الملف الرئيسي بالقيمة '1E'.

الجدول — ٣٠ EF.DIR

File Name	EF.DIR
File ID	'2F00'
Short EF Identifier	'1E'
Select Access	ALWAYS
Read Access	ALWAYS
Write/Update/Erase Access	NEVER
File structure	Transparent
Size	Variable

ويوصى بأن يكون الملف الأولي EF.DIR يحتوي عليه الملف الرئيسي. ويجب أن يكون الملف الأولي EF.DIR موجوداً إذا كان أكثر من التطبيق LDS1 الإلزامي موجوداً ويشير إلى قائمة التطبيقات التي تدعمها وثيقة السفر الإلكترونية المقرورة آلياً. ويجب أن يتضمن مجموعة من نماذج التطبيقات التي تحتوي على معرف التطبيق DO بأي ترتيب.

الجدول — ٣١ شكل الملف الأولي EF.DIR

Tag	L	Value			Description
'61'	'09'				LDS1 eMRTD Application Template
		Tag	L	Value	LDS1 eMRTD Application International AID: 'A0 00 00 02 47 10 01'
		'4F'	'07'	'A0 00 00 02 47 10 01'	
'61'	'09'				Travel Records Application Template
		Tag	L	Value	Travel Records International AID: 'A0 00 00 02 47 20 01'
		'4F'	'07'	'A0 00 00 02 47 20 01'	
'61'	'09'				Visa Records Application Template
		Tag	L	Value	Visa Records International AID: 'A0 00 00 02 47 20 02'
		'4F'	'07'	'A0 00 00 02 47 20 02'	

'61'	'09'				Additional Biometrics Application Template
Tag	L	Value		Additional Biometrics International AID:	
		'4F'	'07'	'A0 00 00 02 47 20 03'	

ملاحظة — يستخدم الملف الأولي EF.DIR خطة معيارية لتخفيض الوسم على النحو المعروف في [ISO/IEC 7816-4].

٣-١١-٣ الملف الأولي للاطلاع على البطاقة EF.CardAccess (مشروع)

الملف الأولي EF.CardAccess هو ملف أولي شفاف يحتوي عليه الملف الرئيسي وهو مطلوب شرطياً إذا تم الاحتياج بفتح الاتصال الاختياري بكلمة سر مصدق عليها لمراقبة الدخول على النحو المعروف في الوثيقة 11 Doc. 9303-11 SecurityInfos. ويمكن الاطلاع على وصف كامل لـ Doc 9303-11 لفتح الاتصال بكلمة سر مصدق عليها في الوثيقة 11 Doc.

ويتمثل معرف الملف الأولي القصير على مستوى الملف الرئيسي بالقيمة '1C'.

الجدول ٣٢ — الملف الأولي EF.CardAccess

File Name	EF.CardAccess
File ID	'011C'
Short EF Identifier	'1C'
Select Access	ALWAYS
Read Access	ALWAYS
Write/Update/Erase Access	NEVER
File structure	Transparent
Size	Variable

ويكون الملف الرئيسي CardAccess الذي يحتوي عليه الملف الرئيسي مطلوباً إذا كان فتح الاتصال بكلمة سر مصدق عليها مدعوماً برقاقة وثيقة سفر مقرورة آلياً ويجب أن يحتوي على المعلومات الأمنية SecurityInfos التالية المطلوبة لفتح الاتصال بكلمة سر مصدق عليها:

- PACEInfo
- ACEDomainParameterInfo

الجدول ٣٣ — تخزين الملف الأولي EF.CardAccess علىدائرة المتكاملة

File Name	EF.CardAccess
File ID	'011C'
Short EF ID	'1C'
Read Access	ALWAYS
Write Access	NEVER

Size	Variable
Content	DER encoded SecurityInfos. See Doc 9303-11.

٤-١١-٣ الملف الأولي لأمن البطاقة EF.CardSecurity (مشروط)

الملف الأولي لأمن البطاقة *EF.CardSecurity* هو ملف أولي شفاف يحتوي عليه الملف الرئيسي وهو مطلوب شرطياً إذا جرى الاحتجاج بفتح الاتصال اختياري بكلمة سر مصدق عليها مع رسم خريطة التحقق من صحة الرقاقة على النحو المعرف في الوثيقة Doc 9303-11. ويمكن الحصول على وصف كامل لـ *SecurityInfos* من أجل فتح الاتصال بكلمة سر مصدق عليها مع رسم خريطة التتحقق من صحة الرقاقة في الوثيقة Doc 9303-11.

ويتمثل معرف الملف الأولي القصير على مستوى الملف الرئيسي بالقيمة '1D'.

ويمكن الملف الأولي EF.CardSecurity الذي يحتوي عليه الملف الرئيسي مطلوباً إذا كان:

- فتح الاتصال اختياري بكلمة سر مصدق عليها مع رسم خريطة التتحقق من صحة الرقاقة مدعوماً من الدائرة المتكاملة؛
- أو التتحقق من صحة الوحدة الطرفية في الملف الرئيسي مدعوماً من الدائرة المتكاملة؛
- أو التتحقق من صحة الرقاقة في الملف الرئيسي مدعوماً من الدائرة المتكاملة.

ويجب أن يحتوي على ما يلي:

- معلومات التتحقق من صحة الرقاقة ChipAuthenticationInfo حسبما يطلب التتحقق من صحة الرقاقة؛
- معلومات المفتاح العمومي للتحقق من صحة الرقاقة ChipAuthenticationInfo حسبما يطلب Authentication،
- معلومات التتحقق من صحة الوحدة الطرفية terminalAuthenticationInfo حسبما يطلب التتحقق من صحة الرقاقة؛
- المعلومات الامنية SecurityInfos الواردة في الملف الأولي CardAccess.

ويمكن الملف الأولي EF.CardSecurity الذي يحتوي عليه الملف الرئيسي مطلوباً إذا كان فتح الاتصال بكلمة سر مصدق عليها مع رسم خريطة التتحقق من صحة الرقاقة مدعوماً من رقاقة الوثيقة الإلكترونية المقرؤة آلياً ويجب أن يحتوي على المعلومات الامنية التالية:

- ChipAuthenticationPublicKeyInfo as required for PACE-CAM
- The SecurityInfos contained in CardAccess

الجدول ٤ - تخزين الملف الأولي EF.CardSecurity على الدائرة المتكاملة

File Name	EF.CardSecurity
File ID	'011D'
Short EF ID	'1D'
Read Access	PACE
Write Access	NEVER
Size	Variable

يُنفَّذ ملف أمن البطاقة CardSecurity كنوع من البيانات الموقعة SignedData، على النحو المحدد في [RFC 3369] مع نوع المحتوى id-SecurityObject داخل الخانة encapsContentInfo. ويجب أن تكون المواد الأمنية موقعة من قبل موقع الوثيقة. ويجب أن تكون شهادة موقع الوثيقة مدرجة في البيانات الموقعة. ويجب أن يستخدم معرف المواد لتعريف نوع المحتوى:

```
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
}
```

وتعزَّز بنية البيانات الموقعة SignedData كما يلي:

```
SignedData ::= SEQUENCE{
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapsContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
    signerInfos SignerInfos
}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

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

ContentType ::= OBJECT IDENTIFIER

SignerInfos ::= SET OF SignerInfo

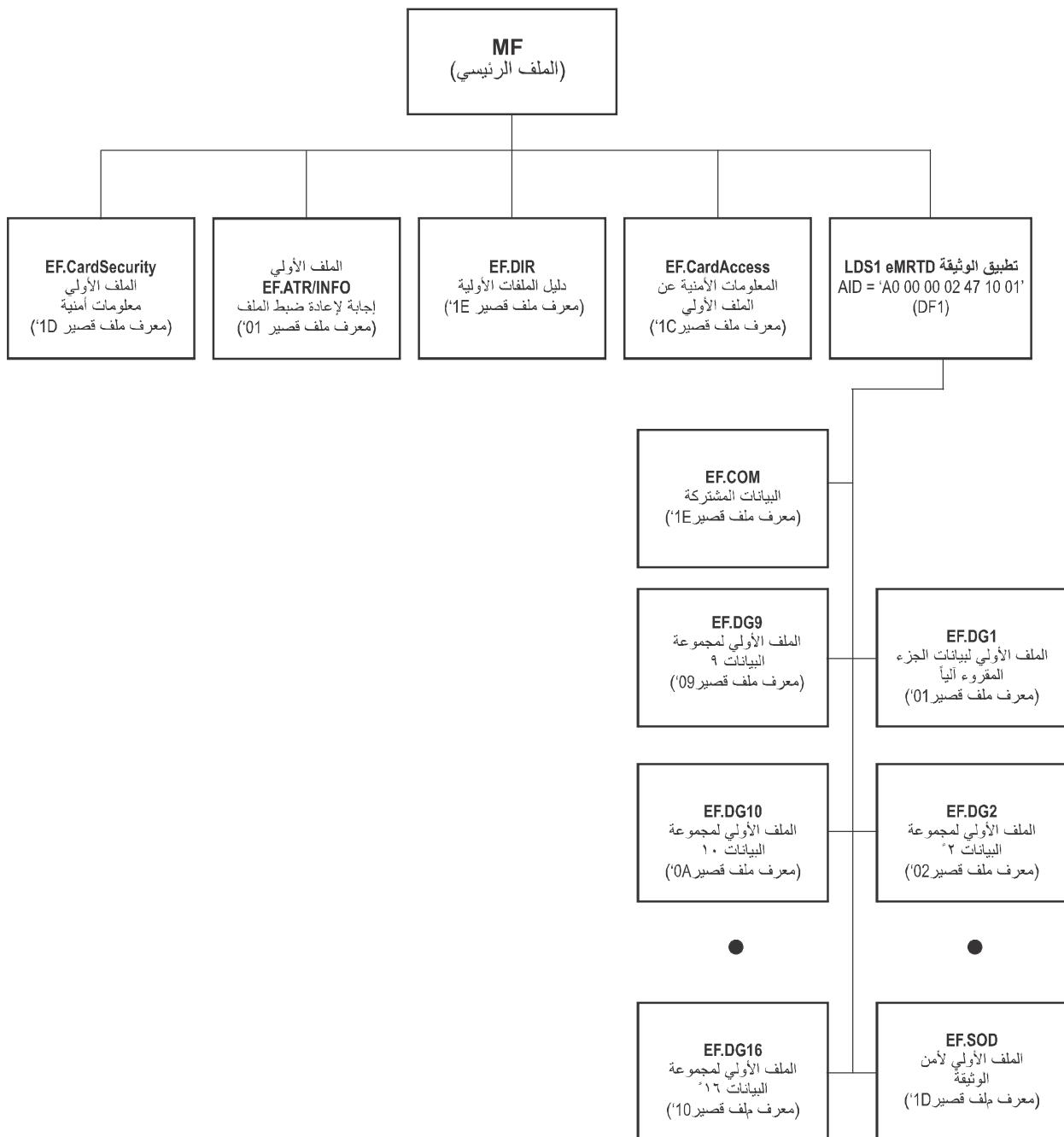
SignerInfo ::= SEQUENCE {
    version CMSVersion,
    sid SignerIdentifier,
    digestAlgorithm DigestAlgorithmIdentifier,
    signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
    signatureAlgorithm SignatureAlgorithmIdentifier,
    signature SignatureValue,
    unsignedAttrs [1] IMPLICIT UnsignedAttributes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

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

SignatureValue ::= OCTET STRING

٤ - تطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1

توفر وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 حيزاً لتخزين عناصر البيانات الإلزامية والاختيارية التي يمكن استخدامها لربط صاحب الوثيقة بالوثيقة وتسيقها رقمياً. وتصبح المعلومات المخزنة في الجزء ذي البنية LDS1 من وثيقة السفر الإلكترونية المقرورة آلياً ثابتة وقت إصدار الوثيقة، ولا يمكن تعديلها بأي طريقة ممكنة. وهذه السمة ضرورية لضمان حماية المعلومات الشخصية وإمكانية كشف التلاعب بالوثيقة بصورة أسهل. ومع أن الصيغة LDS1 لوثيقة السفر الإلكترونية المقرورة آلياً تشمل خانات بيانات اختيارية يمكن استخدامها لتوسيع استخدام وثيقة السفر الإلكترونية المقرورة آلياً (أي معلومات إضافية للاستدلال البيولوجي، والتخلص الجمركي على الحدود وما إلى ذلك)، فإن شرط الحماية من الكتابة على تطبيق رقاقة وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 يعتبر إلزامياً.



الشكل ٣ — موجز بنية ملف وثيقة السفر الإلكترونية المقرؤة آلياً ذات البنية LDS1

٤-١ اختيار التطبيق — الملف المخصص

يجب اختيار تطبيق وثيقة السفر الإلكترونية المفروضة آلياً ذات البنية LDS1 باستخدام تعريف التطبيق كاسم ملف مخصص محجوز. ويجب أن يتألف تعريف التطبيق من معرف التطبيق المسجل الذي عينته المنظمة الدولية لتوحيد المقاييس وفقاً لـ [ISO/IEC 7816-5] وامتداد لمعرف تطبيق الملكية (PIX) على النحو المحدد في هذه الوثيقة:

- معرف التطبيق المسجل هو 'A000000247'؛
- يجب أن يستخدم تطبيق البيانات المخزنة لجهة الإصدار الامتداد '1001' = PIX؛
- معرف التطبيق الكامل لوثيقة السفر الإلكترونية المفروضة آلياً ذات البنية LDS1 هو 'A0 00 00 02 47 10 01'.

ويجب أن ترفض الدائرة المتكاملة اختيار أحد التطبيقات إذا كان الامتداد الخاص بهذا التطبيق غير موجود.

٤-٢ خطة الترتيب العشوائي

تسمح خطة الترتيب العشوائي بتسجيل مجموعات البيانات وعناصر البيانات باتباع ترتيب عشوائي يكون متسقاً مع إمكانية تكنولوجيا التوسيع الاختياري للسعة بما يمكن من الاستعادة المباشرة لعناصر بيانات محددة حتى ولو كانت مسجلة بدون ترتيب. وتتمز عناصر البيانات المتغيرة الطول كمواد بيانات TLV محددة في الترميز ASN.1.

٤-٣ تمثيل ملف الاطلاع العشوائي

لدعم مجموعة واسعة من عمليات التنفيذ، تشمل بنية البيانات المنطقية مجموعة كبيرة من عناصر البيانات الاختيارية. ودرج عناصر البيانات هذه لتسهيل التحقق من صحة وثيقة السفر الإلكترونية المفروضة آلياً ذات البنية LDS1، ولتسريع معالجة الوثيقة (نقاط الشخص).

يجب أن تدعم بنية البيانات ما يلي:

- مجموعة محددة أو واسعة من عناصر البيانات؛
- وأحداث متعددة لعناصر بيانات محددة؛
- والتطور المستمر لعمليات تنفيذ محددة؛
- ودعم مجموعة واحدة على الأقل من بيانات التطبيق؛
- والسماح لتطبيقات وطنية محددة أخرى؛
- ودعم التتحقق الشامل الاختياري من حصة الوثيقة باستخدام زوج مفاتيح لا تناولري مخزن؛
- ودعم الاطلاع السريع على عناصر بيانات مختارة لتسهيل المعالجة السريعة للوثيقة؛
- والاطلاع الفوري على عناصر البيانات الضرورية؛
- والاطلاع المباشر على نماذج البيانات وبيانات الاستدلال البيولوجي.

٤-٤ تجميع عناصر البيانات

قد يكون تجميع عناصر البيانات الذي تضيفه دول الإصدار أو المنظمات المستقبلة المعتمدة أو لا يكون موجوداً في بنية البيانات المنطقية. وقد تتضمن بنية البيانات المنطقية أكثر من تسجيل واحد لعناصر البيانات المجمعة التي تضيفها الدول المستقبلة والمنظمات المستقبلة المعتمدة. ولا تدعم هذه الطبعة من الوثيقة Doc 9303 قدرة الدول المستقبلة والمنظمات المستقبلة المعتمدة على إضافة بيانات إلى بنية البيانات المنطقية. وتعتبر بنية البيانات المنطقية كياناً متلاحمًا واحداً يحتوي على عدد من تجمعيات عناصر البيانات التي سجلت في تكنولوجيا التوسيع الاختياري للسعة وقت القراءة الآلية.

وقد صممت بنية البيانات المنطقية بمرونة كافية بحيث يمكن تطبيقها على جميع أنواع وثائق السفر الإلكترونية المقرورة آلياً. وفي الأشكال والجداول التالية، لا تطبق بعض بنود البيانات إلا على التأشيرات المقرورة آلياً والجوازات المقرورة آلياً أو تحتاج إلى تمثيل مختلف فيما يتعلق بهذه الوثائق.

وقد حددت ضمن بنية البيانات المنطقية تجمعيات منطقية لعناصر البيانات ذات الصلة. ويشار إلى تجمعيات البيانات هذه باسم مجموعات البيانات.

٤-٥ متطلبات بنية البيانات المنطقية

يجب على تكنولوجيا توسيع سعة الدائرة المتكاملة اللاسلكية الواردة في وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 التي اختارتها دولة الإصدار أو المنظمة المستقبلة المعتمدة أن تسمح للدول المستقبلة بالاطلاع على البيانات.

وقد قررت الإيكاو أن بنية البيانات المنطقية الوحيدة المعروفة مسبقاً يجب أن تلبى عدداً من المتطلبات الإلزامية:

- ضمان التسهيل الفعال والأمثل لصاحب الوثيقة القانوني؛
- ضمان حماية التفاصيل المسجلة في تكنولوجيا التوسيع الاختياري للسعة؛
- السماح بالتشغيل المتبادل عالمياً لبيانات السعة الزائدة استناداً إلى بنية بيانات منطقية واحدة مشتركة بين جميع وثائق السفر الإلكترونية المقرورة آلياً؛
- تلبية الاحتياجات المنوعة للدول والمنظمات المستقبلة بشأن التوسيع الاختياري للسعة؛
- توفير سعة توسيع حسب احتياجات المستعمل وتطور التكنولوجيا المتوفرة؛
- دعم مجموعة متنوعة من خيارات حماية البيانات؛
- استعمال الموصفات الدولية القائمة إلى أقصى حد ممكن، ولا سيما الموصفات الدولية الناشئة بشأن بيانات الاستدلال البيولوجي القابلة للتشغيل المتبادل عالمياً.

٤-٥-١ الأمن

يجب على دولة أو منظمة الإصدار وحدها أن يكون لديها تصريح بالكتابة في مجموعات البيانات هذه. لذلك لا يوجد متطلبات للتبدل ولا تعتبر طرق تحقيق حماية من الكتابة جزءاً من المعايير. وبمجرد إغلاق الرقاقة (بعد إضفاء الطابع الشخصي وقبل الإصدار) لا يمكن كتابة أي بيانات في رقاقة تطبيق LDS1 أو تعديلها أو حذف منها. ولا يمكن فتح رقاقة مغلقة بعد الإصدار.

٤-٥-٤ صحة البيانات وسلامتها

تدرج مادة للصحة/السلامة للسماح بتأكيد صحة وسلامة التفاصيل المسجلة. ويجب أن تتمثل كل مجموعة بيانات في مادة الصحة/السلامة هذه، التي تسجل داخل ملف أولي (EF.SOD). وباستخدام بنية إطار شكل الملف المشترك لتبادل الاستدلالات البيولوجية (CBEFF) المستخدم في مجموعات البيانات ٤-٢ المرمزة لسمة التعرف والسمات الاختيارية "الأمن معلومات الاستدلال البيولوجي الإضافية" المحددة في الوثيقة Doc 9303-12، يمكن أيضاً حماية تفاصيل تأكيد الهوية (مثل نماذج الاستدلال البيولوجي) بصورة فردية بحسب تقدير دولة أو منظمة الإصدار.

٤-٥-٣ ترتيب بنية المعلومات المنطقية

يجب أن لا تستخدم خطة الترتيب العشوائي إلا للتشغيل المتداول دولياً.

٤-٥-٤ سعة تخزين البيانات لدائرة المتكاملة الالاتلامسية

سعة تخزين البيانات لدائرة المتكاملة الالاتلامسية تكون وفقاً لتقدير دولة الاصدار ولكن يجب أن تكون كحد أدنى ٣٢ كيلوبايت. وهذا الحد الأدنى من السعة ضروري لتخزين صورة الوجه المخزنة إلزامياً وبيانات الجزء المفروء آلياً والعناصر الازمة لتأمين البيانات. وقد يتطلب تخزين صور إضافية للوجه وأو بصمات الأصابع وأو القرحية زيادة كبيرة في سعة تخزين البيانات. ولا يوجد حد أقصى محدد لسعة البيانات لدائرة المتكاملة الالاتلامسية.

وفي حالة عدم توافر بنية أساسية للمفاتيح العامة للدولة للتوقيع على بيانات وثيقة السفر الالكترونية المفروءة آلياً ذات البنية LDS1 كجزء من إضافة البيانات الشخصية، وعدم إمكان تأجيل إصدار الوثيقة (الوثائق)، يوصى بترك الدائرة المتكاملة الالاتلامسية لوثيقة السفر الالكترونية المفروءة آلياً ذات البنية LDS1 خالية ومغلقة. وينبغي أن تحتوي وثيقة السفر الالكترونية المفروءة آلياً ذات البنية LDS1 على تظهير ملائم بهذا الشأن. ومن المتوقع أن يكون هذا ظرفاً استثنائياً.

٤-٥-٥ تخزين البيانات أخرى

يجوز أن تستخدم أي دولة سعة تخزين الدائرة المتكاملة الالاتلامسية في وثيقة سفر الكترونية مفروءة آلياً لزيادة سعة وثيقة السفر الالكترونية المفروءة آلياً ذات البنية LDS1 من البيانات المفروءة آلياً لتجاوز تلك المحددة للتشغيل المتداول عالمياً. ويمكن أن يكون هذا لأغراض مثل إتاحة الاضطلاع بالقراءة الآلية للتعرف على معلومات الوثيقة (مثل تفاصيل شهادة الميلاد) وأو تأكيد الهوية الشخصية المخزنة (سمات الاستدلال البيولوجي) وأو تفاصيل التحقق من صحة الوثيقة.

٤-٥-٦ المعيار الدولي لترميز بيانات الاستدلال البيولوجي

جاء المعيار ISO/IEC 39794:2005 ليخلف المعيار [ISO/IEC 19794:2005] كمعيار دولي لترميز بيانات الاستدلال البيولوجي. وقد تم تحديد الجدول الزمني التالي للانتقال:

- يجب أن تكون نظم التفتيش قادرة على معالجة بيانات ISO/IEC 39794 بحلول ٢٠٢٦/١١ بعد فترة تحضيرية مدتها ٦ سنوات تبدأ في ٢٠٢٠/١١؛
- وبين عامي ٢٠٢٦ و٢٠٣٠، يمكن لدول وجهات إصدار الجوازات أن تستخدم أشكال البيانات المحددة في ISO/IEC 19794-X:2005 أو في ISO/IEC 39794-X:2005 خلال الفترة الانتقالية البالغة ٤ سنوات؛
- واعتباراً من ٢٠٣٠/١١، يجب على جهات إصدار الجوازات أن تستخدم ISO/IEC 39794-X لترميز بيانات الاستدلال البيولوجي.

ويورد تقرير الإيكاو الفني ISO/IEC 39794-5 "معلمات تطبيق وثائق السفر الإلكترونية المقررة آلياً"^١ إرشادات بشأن الانتقال من ISO/IEC 39794 إلى ISO/IEC 19794:2005.

وتشمل بنية البيانات المنطقية في وثائق السفر الإلكترونية المقررة آلياً مجموعة البيانات ٢ للوجه (الزمامية) ومجموعة البيانات ٣ ل بصمات الأصابع (اختيارية) ومجموعة البيانات ٤ لحديقة العين (اختيارية). وتشتمل كل مجموعة من مجموعات البيانات على بيانات الاستدلال البيولوجي التي جرى ترميزها وفقاً للمعايير الدولية حفاظاً على إمكانية التشغيل البيني على الصعيد الدولي.

ويجب أن تستخدم جميع مجموعات البيانات المذكورة أعلاه (المجموعات ٢ و ٣ و ٤) نموذج المجموعة لنموذج معلومات الاستدلال البيولوجي (BIT) مع تحديد البيانات المتداخلة (انظر الوثيقة Doc 9303-10). وتحتوي بنية نموذج معلومات الاستدلال البيولوجي على معلومات استدلال بيولوجي يمكن ترميزها باستخدام أحد معيارين إما الإصدار الأول من سلسلة ISO/IEC 19794 وإما سلسلة ISO/IEC 39794.

ومعلومات الاستدلال البيولوجي المُرْمَزة وفقاً للإصدار الأول من سلسلة ISO/IEC 19794 يجري تخزينها في مادة البيانات المعرفة بالوسم '7F2E'.

الجدول ١ : وسوم معلومات الاستدلال البيولوجي

Tag	Standard No.
5F2E	ISO/IEC 19794 series first edition
7F2E	ISO/IEC 39794 series

ومعلومات الاستدلال البيولوجي المُرْمَزة في مادة البيانات والمعرفة بالوسم '7F2E'، يجب أن تستخدم بنية البيانات الواردة في الجدول التالي.

الجدول ٢ : هيكل البيانات وفقاً DO'7F2E'

Tag	L	Value				
		Tag	L	Value		
7F2E	Var.	Biometric data template defined in ISO/IEC 7816-11.				
		A1	Var.	Biometric data in standardized format (Constructed)		
				Tag	L	
				64, 65 or 66	Var	Value
						DO defined in the ISO/IEC 39794 series Table 3.

الجدول ٣ : وسوم مواد البيانات المعرفة وفقاً للسلسلة ISO/IEC 39794.

Standard No.	Tag
ISO/IEC 39794-4	64
ISO/IEC 39794-5	65
ISO/IEC 39794-6	66

^١ يمكن الاطلاع على المرجع على www.icao.int/security/fal/trip

٦-٤ الملفات الأولية لوثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1

٤-٦-١ المعلومات عن وجود العنوان ومجموعة البيانات EF.COM (إنرامية)

يوجد ملف EF.COM في تطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 (معرف الملف القصير = 'E') ويتضمن معلومات عن إصدار بنية البيانات المنطقية ومعلومات إصدار الرموز الموحدة وقائمة بمجموعات البيانات الموجودة للتطبيق. وتطبيق وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 يجب أن يحتوي على ملف EF.COM واحد فقط يتضمن المعلومات المشتركة للتطبيق.

فيما يلي عناصر البيانات التي قد ترد في هذا النموذج:

الجدول ٣٥ — الوسوم المعيارية للملف الأولي المشترك (EF.COM)

Tag	L	Value		
'60'	Var	Application level information		
		Tag	L	Value
		'5F01'	'04'	LDS Version number with format aabb, where aa defines the version of the LDS and bb defines the update level.
		'5F36'	'06'	Unicode Version number with format aabbcc, where aa defines the major version, bb defines the minor version and cc defines the release level.
		'5C'	Var	Tag list. List of all Data Groups present.

يجب إدراج عنوان وخريطة لوجود مجموعة البيانات. ويجب أن يتضمن العنوان المعلومات التالية التي تمكّن أي دولة مستلمة أو منظمة مستلمة من تحديد موضع وحل شيفرة مختلف مجموعات البيانات وعناصر البيانات المضمنة داخل حزمة البيانات المسجلة بواسطة دولة أو منظمة الإصدار.

ويوصى بتعديل نظم التقىش التي تعتمد على EF.COM من أجل استخدام المادة الامنية لوثيقة المحددة في الإصدار ١.٨ لبنية البيانات المنطقية في أقرب وقت ممكن.

٤-٦-١-١ رقم إصدار بنية البيانات المنطقية

يحدد رقم اصدار بنية البيانات المنطقية اصدار شكل بنية البيانات المنطقية. وسيحدد في القسم ٤-٦ من هذه الوثيقة الشكل الدقيق الذي يستخدم لتخزين هذه القيمة. والشكل الموحد لرقم اصدار بنية بيانات منطقية هو "aabb" ، حيث:

- "aa" = الرقم (01-99) الذي يحدد الاصدار الأكبر لبنية البيانات المنطقية (أي الاضافات الهاامة لبنية البيانات المنطقية)؛
- "bb" = الرقم (01-99) الذي يحدد الاصدار الأصغر لبنية البيانات المنطقية.

٤-٦-١-٢ رقم إصدار الرموز الموحدة

يحدد عدد اصدارات الرموز الموحدة أسلوب الترميز المستخدم عند تسجيل رموز ألبائية ورقمية وخاصة، بما في ذلك الرموز الوطنية. وسيحدد في القسم ٤-٧-٤ من هذه الوثيقة الشكل الدقيق الذي يتعين استخدامه لتخزين هذه القيمة. والشكل الموحد لرقم اصدار الرموز الموحدة هو "aabbcc" ، حيث،:

- "aa" = رقم يحدد الاصدار الأكبر لمواصفة الرموز الموحدة (أي الاضافات الهاامة إلى المواصفة، المنشورة ككتاب)؛

- "bb" = رقم يحدد الاصدار الأصغر لمواصفة الرموز الموحدة (أي إضافات الرموز أو التغييرات المعيارية الأكثر أهمية، المنشورة كتقرير فني)؛
 - "cc" = رقم يحدد الاصدار الحديث لمواصفة الرموز الموحدة (أي تغييرات أخرى للأجزاء الاعلامية المعيارية أو الهامة للمواصفة التي يمكن أن تغير مسلك البرنامج. وتتجلى هذه التغييرات في ملفات جديدة لقاعدة بيانات الرموز الموحدة وصفحة حديثة). ولأسباب تاريخية، فإن الترقيم داخل كل من الخانات (أي a, b, c) ليس متالياً بالضرورة.
- يجب أن تمثل مجموعة الحروف العالمية (UCS) للمعيار [ISO/IEC 10646].

٤-٢-٦ المادة الأمنية للوثيقة EF.SOD (اللزامية)

بالإضافة إلى مجموعات بنية البيانات المنطقية، تحتوي الدائرة المتكاملة اللاتلامية أيضاً على مادة أمنية للوثيقة مخزنة في EF.SOD وهذه المادة موقعة رقمياً بواسطة دولة الإصدار وتحتوي على قيم بصمات رقمية لمحتويات بنية البيانات المنطقية.

الجدول ٣٦ — وسوم EF.SOD

القيمة	L	الوسم
المادة الأمنية للوثيقة	Var	'77'

يوجد حالياً إصداران من المادة الأمنية للوثيقة EF.SOD تم نشرهما. وهناك الملف القديم V0 EF.SOD ويمكن الاطلاع عليه في المرفق (د) والممل الموصى به EF.SOD V1 الوارد في هذا القسم. وهناك ملف واحد EF.SOD فقط مطلوب ويسمح به.

٤-٢-٧-١ المادة الأمنية للوثيقة EF.SOD VI LDS v1.8

تم توسيع المادة الأمنية للوثيقة V1 بالنسبة إلى LDS v1.8 بفتح موقع يتضمن بنية البيانات المنطقية ومعلومات إصدار الرموز الموحدة:

```

LDSSecurityObject ::= SEQUENCE {
    version LDSSecurityObjectVersion,
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
        DataGroupHash,
    ldsVersionInfo LDSVersionInfo OPTIONAL
        -- If present, version MUST be V1
}
LDSVersionInfo ::= SEQUENCE {
    ldsVersion PrintableString,
    unicodeVersion PrintableString }

```

٤-٢-٧-٢ نوع البيانات الموقعة من أجل المادة الأمنية للوثيقة SOD VI

تُثْدَّ المادة الأمنية للوثيقة كنوع من البيانات الموقعة، على النحو المحدد في [RFC 3369]. ويجب إنتاج جميع المواد الأمنية في شكل قاعدة الترميز المميز (DER) للحفاظ على سلامة التوقيعاتداخلها.

الملاحظة ١ — $m =$ مطلوبة — يجب أن تكون الخانة موجودة.
الملاحظة ٢ — $x =$ لا تستخدم — لا ينبغي ملء الخانة.

الملاحظة ٣ — o = اختيارية — يجوز أن تكون الخانة موجودة.
الملاحظة ٤ — c = اختيار — مضمنون الخانة هو خيار من بدائل.

الجدول ٣٧ — نوع البيانات الموقعة من أجل المادة الأمنية للوثيقة SO_D V1

Value		Comments
SignedData		
Version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
Certificates	o	States are REQUIRED to include the Document Signer Certificate (CDS) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States provide only 1 signerInfo within this field.
SignerInfo	m	
Version	m	The value of this field is dictated by the sid field. See RFC3369 Doc 9303-12 for rules regarding this field.
Sid	m	
issuerandSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving States may choose to ignore them.

ASN.1 Profile LDS Document Security Object for SOD VO ٣-٢-٧-٤

```

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

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

-- Imports from 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) };

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers

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}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {v0(0), v1(1)
-- If LDSSecurityObjectVersion is V1, ldsVersionInfo MUST be present
}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
version LDSSecurityObjectVersion,
hashAlgorithm DigestAlgorithmIdentifier,
dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
DataGroupHash,
ldsVersionInfo LDSVersionInfo OPTIONAL
-- If present, version MUST be V1
}
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) }

```

```
LDSVersionInfo ::= SEQUENCE {
    ldsVersion PrintableString
    unicodeVersion Printable String
}

END
```

Note 1.— The field dataGroupHashValue contains the calculated hash over the complete contents of the Data Group EF, specified by dataGroupNumber.

Note 2.— DigestAlgorithmIdentifiers MUST omit “NULL” parameters, while the SignatureAlgorithmIdentifier (as defined in RFC 3447) MUST include NULL as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Inspection system MUST accept the field DigestAlgorithmIdentifiers with both conditions, i.e. absent parameters and NULL parameters.

٤-٧ عناصر البيانات التي تشكل مجموعات البيانات من ١ إلى ١٦

مجموعات البيانات من ١ (DG1) حتى ١٦ (DG16) تتألف فردياً من عدد من عناصر البيانات الالزامية والاختيارية والمشروطة. ويجب اتباع الترتيب المحدد لعناصر البيانات داخل مجموعة البيانات. ويجب تخزين كل مجموعة بيانات في ملف أولي شفاف واحد. ويجب معالجة الملفات الأولية بمعرف للملفات الأولية القصيرة على النحو المبين في الجدول ٣٨. ويجب أن تكون للملفات الأولية أسماء ملفات يجب أن تكون وفقاً للرقم n، EF.DGn حيث n هي رقم مجموعة البيانات.

الجدول ٣٨ — عناصر البيانات الالزامية والاختيارية التي تجتمع لتكوين بنية مجموعات البيانات من ١ (DG1) إلى ١٦ (DG16)

Data Group	EF Name	Short File Identifier	FID	Tag
Common	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 0C’	‘6C’
DG13	EF.DG13	‘0D’	‘01 0D’	‘6D’
DG14	EF.DG14	‘0E’	‘01 0E’	‘6E’
DG15	EF.DG15	‘0F’	‘01 0F’	‘6F’

Data Group	EF Name	Short File Identifier	FID	Tag
DG16	EF.DG16	'10'	'01 10'	'70'
Document Security Object	EF.SO_D	'1D'	'01 1D'	'77'
Common	EF.CARDACCESS	'1C'	'01 1C'	
Common	EF.ATR/INFO	'01'	'2F 01'	
Common	EF.CardSecurity	'1D'	'01 1D'	

٤-٧-١ مجموعة البيانات ١ — معلومات الجزء المقرورة آلياً (الزامية)

المقصود بعناصر البيانات لمجموعة البيانات ١ (DG1) هو التعبير عن محتويات الجزء المقرورة آلياً بأكملها سواء كان يحتوي على بيانات فعلية أو رموز لسد الفراغ، والتفاصيل بشأن تنفيذ الجزء المقرورة آلياً تعتمد على نوع وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 (الأشكال TD1 أو TD2 أو TD3).

ويحتوي هذا العنصر من البيانات على معلومات الجزء المقرورة آلياً (MRZ) المطلوبة من أجل الوثيقة في النموذج '61'. ويحتوي النموذج على مادة بيانات واحدة، هي الجزء المقرورة آلياً في مادة البيانات '5F1F'. ومادة بيانات الجزء المقرورة آلياً هي مادة مركبة، مطابقة لمعلومات OCR- MRZ B المطبوعة على الوثيقة.

الجدول ٣٩ — وسوم مجموعة البيانات ١

Tag	L	Value		
'61'	Var			
		Tag	L	Value
		'5F1F'	F	The MRZ data object as a composite Data Element. (REQUIRED) (The Data Element contains all mandatory fields from Document Type through to Composite check digit.)

٤-٧-١-١ مجموعة البيانات ١ — عناصر بيانات الملف الأولى. مجموعة البيانات ١ من أجل وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 من الحجم TD1

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات ١ (DG1). ومتطلبات تخزين وترتيب وترميز مجموعة البيانات ١ (DG1) ينبغي أن تكون مماثلة بالضبط لما يوجد في الجزء المقرورة آلياً المطبوع ونوصف في الوثيقة Doc 9303-3 والوثيقة 9303-5 Doc 9303-5.

عناصر البيانات وشكلها داخل كل خانة لمجموعة بيانات من أجل وثيقة السفر ١ يجب أن تكون كما في الجدول التالي:

A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length — ملاحظة

.field

الجدول ٤٠ — عناصر البيانات لشكل وثيقة السفر TD1

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Document number (Nine most significant characters)	9	F	A,N,S
04	M	Check digit — Document number or filler character (<) indicating document number exceeds nine characters	1	F	N,S
05	M	Optional data and/or in the case of a Document Number exceeding nine characters, least significant characters of document number plus document number check digit plus filler character	15	F	A,N,S
06	M	Date of birth	6	F	N,S
07	M	Check digit — Date of birth	1	F	N
08	M	Sex	1	F	A,S
09	M	Date of Expiry	6	F	N
10	M	Check digit — Date of expiry	1	F	N
11	M	Nationality	3	F	A,S
12	M	Optional data	11	F	A,N,S
13	M	Composite check digit	1	F	N
14	M	Name of holder	30	F	A,N,S

٤-١-٧-٢ مجموعه البيانات ١ - الملف الأولي. مجموعه البيانات ١ عناصر البيانات لوثيقة السفر الالكترونية المفروعة آلياً من الحجم TD2 يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعه البيانات ١ (DG1). ومتطلبات تخزين وترتيب وترميز مجموعه البيانات ١ (DG1) مقصود بها أن تكون مماثلة بالضبط لما يوجد في الجزء المفروع آلياً المطبوع وتوصف في الوثيقة Doc 9303-3 والوثيقة Doc 9303-6. وعناصر البيانات وشكلها داخل كل خانة لمجموعة بيانات من أجل وثيقة السفر ٢ يجب أن تكون كما في الجدول التالي:

A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length — ملاحظة —

.field

الجدول ٤ — عناصر بيانات لشكل وثيقة السفر TD2

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Name of holder	31	F	A,N,S
04	M	Document number (Nine principal characters)	9	F	A,N,S
05	M	Check digit	1	F	N,S
06	M	Nationality	3	F	A,S
07	M	Date of birth	6	F	N,S
08	M	Check digit	1	F	N
09	M	Sex	1	F	A,S
10	M	Date of expiry	6	F	N
11	M	Check digit	1	F	N
12	M	Optional data plus filler character	7	F	A,N,S
13	M	Composite Check Digit - MRZ line 2	1	F	N

٤-١-٣-٤ مجموعة البيانات ١ — الملف الأولي مجموعة البيانات ١ عناصر البيانات لوثيقة السفر الالكترونية المقرورة آلياً ذات البنية من الحجم *LDS1*

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات ١ (DG1). ومتطلبات تخزين وترتيب وترميز مجموعة البيانات ١ (DG1) مقصود بها أن تكون مماثلة بالضبط لما يوجد في الجزء المقرر آلياً المطبوع وتوصف في الوثيقة ٣ Doc 9303-3 والوثيقة ٤ Doc 9303-4. وعناصر البيانات وشكلها داخل كل خانة لمجموعة بيانات من أجل وثيقة السفر ٣ يجب أن تكون كما في الجدول التالي:

A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length — ملاحظة

.field

الجدول ٤ - عناصر البيانات لشكل وثيقة السفر TD3

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Name of holder	39	F	A,S
04	M	Document number	9	F	A,N,S
05	M	Check digit — Document number	1	F	N,S
06	M	Nationality	3	F	A,S
07	M	Date of birth	6	F	N,S
08	M	Check digit — Date of birth	1	F	N
09	M	Sex	1	F	A,S
10	M	Date of expiry	6	F	N
11	M	Check digit — Date of expiry or valid until date	1	F	N
12	M	Optional data	14	F	A,N,S
13	M	Check digit	1	F	N
14	M	Composite check digit	1	F	N

٤-٧-٢- مجموعة البيانات ٢ - السمات المرفزة للتعرف على الهوية - الوجه (الزمي)

تمثل مجموعة البيانات ٢ (DG2) سمة الاستدلال البيولوجي القابلة للتشغيل المتبادل عالمياً للتحقق من الهوية بالاستعانة بالآلات مع وثائق السفر المقرورة آلياً، التي يجب أن تكون صورة لوجه حامل الوثيقة كمدخل لنظام للتعرف على الوجه. وإذا كان يوجد أكثر من تسجيل واحد، فيجب أن يكون أحدث ترميز قابل للتشغيل المتبادل عالمياً هو أول ما يتم تسجيله.

الجدول ٤٣ — وسوم مجموعة البيانات ٢

Tag	L	Value
‘75’	Var	See Biometric encoding of EF.DG2

٤-٢-٧-١ الترميز بالاستدلال البيولوجي للملف الأولى. مجموعة البيانات ٢

يجب أن تستخدم مجموعة البيانات ٢ نموذج المجموعة لنمذج معلومات الاستدلال البيولوجي (BIT) مع تحديد البتات المتداخلة في [ISO/IEC 7816-11]، مما يسمح بإمكانية تخزين عدة نماذج استدلال بيولوجي وهو منسجم مع شكل الملف المشترك لتبادل الاستدلالات البيولوجية (CBEFF). ويحدد العنوان الفرعي للاستدلال البيولوجي نوع الاستدلال البيولوجي الموجود وسمة الاستدلال البيولوجي المحددة. والخيارات المتداخلة لـ [ISO/IEC 7816-11] يتبعن دائماً استخدامه، حتى للتزميات لنمذج استدلال بيولوجي منفرد. والحالة الأخيرة مبنية عن طريق الترقيم بواسطة $n=1$.

لدى كل نموذج متداخل البنية التالية:

الجدول ٤٤ — مجموعة البيانات ٢ – وسوم الترميز للاستدلال البيولوجي

Tag	L	Value	
‘7F61’	Var	Biometric Information Group Template	
	Tag	L	Value
	‘02’	‘01’	Integer — Number of instances of this type of biometric
	‘7F60’	Var	1st Biometric Information Template
	Tag	L	
	‘A1’	Var	Biometric Header Template (BHT)
	Tag	L	Value
	‘80’	‘02’	ICAO header version 0101 (Optional) — Version of the CBEFF patron header format
	‘81’	‘01-03’	Biometric type (Optional)
	‘82’	‘01’	Biometric subtype Optional for DG2
	‘83’	‘07’	Creation date and time (Optional)
	‘85’	‘08’	Validity period (from through) (Optional)
	‘86’	‘04’	Creator of the biometric reference data (PID) (Optional)
	‘87’	‘02’	Format owner (REQUIRED)
	‘88’	‘02’	Format type (REQUIRED)
	‘5F2E’ or ‘7F2E’	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).

يُستخدم معرف البند الأصلي لشكل ملف مشترك لتبادل الاستدلالات البيولوجية. موضوع البيانات لمعرف البند (‘06’ Tag) الوارد تحت نموذج معلومات الاستدلال البيولوجي (BIT, Tag ‘7F60’) مباشرة المحدد في [ISO/IEC 7816-11] لا تحتوي عليه هذه البنية. وبالتالي فإن سلطة تخصيص الاسم غير محددة في البنية.

لتسهيل التشغيل المتبادل، يجب ترميز أول سمة استدلال بيولوجي مسجلة في كل مجموعة بيانات حسب [ISO/IEC19794-5].
ملاحظة — المعيار ISO/IEC 39794 سوف يلي المعيار ISO/IEC 19794:2005 كمعيار دولي لترميز بيانات الاستدلال البيولوجي. انظر القسم ٤-٥-٦.

٤-٢-٧-٢ — مجموعة البيانات ٢ — الملف الأولي. عناصر البيانات لمجموعة البيانات ٢

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات ٢ (DG2): يجب أن تكون عناصر البيانات وشكلها في خانة كل مجموعة بيانات على النحو الوارد في الجداول التالية:

*A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], —
B = Binary data, F = fixed-length field, Var = variable-length field.*

الجدول ٤ — عناصر البيانات لمجموعة البيانات ٢

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M	Number of face biometric encodings recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the face.
02	M	Header		Var	A,N	Data Element may recur as defined by Data element 01.
03	M	Face biometric data encoding(s)		Var	A,N,S,B	Data Element may recur as defined by Data element 01.

٤-٣-٧-٣ — السمة الإضافية للتعرف على الهوية — الإصبع (الأصابع) (اختيارية)

تعرف الإيكاو بأنه يجوز للدول الأعضاء أن تختار التعرف على بصمة الإصبع كتقنيات استدلال بيولوجي إضافية دعماً لتأكيد الهوية بمساعدة آية، التي يجب ترميزها بوصفها مجموعة البيانات ٣ (DG3).

الجدول ٦ — وسوم مجموعة البيانات ٣

Tag	L	Value
‘63’	Var	See Biometric encoding of EF.DG3

٤-٣-٧-١ — الترميز بالاستدلال البيولوجي للملف الأولي. مجموعة البيانات ٣

يجب أن تستخدم مجموعة البيانات ٣ نموذج المجموعة لنماذج معلومات الاستدلال البيولوجي (BIT) مع نماذج معلومات استدلال بيولوجي متداخلة محددة في [ISO/IEC 7816-11]، تتيح إمكانية تخزين نماذج استدلال بيولوجي متعددة وهي منسجمة مع شكل الملف المشترك لتبادل الاستدلالات البيولوجية (CBEFF). ويحدد العنوان الفرعي للاستدلال البيولوجي نوع الاستدلال البيولوجي الموجود وسمة الاستدلال البيولوجي

المحددة. ويجب استخدام الخيار المتداخل لـ [7816-11] ISO/IEC، حتى لعمليات ترميز نموذج استدلال بيولوجي منفرد. ويشار إلى الحالة الأخيرة عن طريق الترقيم بـ $n=1$. وعدد الأمثلة في مجموعة البيانات ٣ يمكن أن يكون $n=0...n$.

كل نموذج متداخل يتضمن البنية التالية:

الجدول ٤ — الوسوم المتداخلة لمجموعة البيانات ٣

Tag	L	Value		
‘7F61’	Var	Biometric Information Group Template		
		Tag	L	Value
		‘02’	‘01’	Integer — Number of instances of this type of biometric
		‘7F60’	Var	1st Biometric Information Template
		Tag	L	
		‘A1’	Var	Biometric Header Template (BHT)
		Tag	L	Value
		‘80’	‘02’	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
		‘81’	‘01-03’	Biometric type (Optional)
		‘82’	‘01’	Biometric subtype REQUIRED for DG3
		‘83’	‘07’	Creation date and time (Optional)
		‘85’	‘08’	Validity period (from through) (Optional)
		‘86’	‘04’	Creator of the biometric reference data (PID) (Optional)
		‘87’	‘02’	Format owner (REQUIRED)
		‘88’	‘02’	Format type (REQUIRED)
		‘5F2E’ or ‘7F2E’	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB). See 4.5.6.
		Tag	L	
		‘7F60’	Var	2nd Biometric Information Template
		Tag	L	
		‘A1’	Var	Biometric Header Template (BHT)
		Tag	L	Value
		‘80’	‘02’	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
		‘81’	‘01-03’	Biometric type (Optional)
		‘82’	‘01’	Biometric subtype REQUIRED for DG3
		‘83’	‘07’	Creation date and time (Optional)

Tag	L	Value				
		‘85’	‘08’	Validity period (from through) (Optional)		
		‘86’	‘04’	Creator of the biometric reference data (PID) (Optional)		
		‘87’	‘02’	Format owner (REQUIRED)		
		‘88’	‘02’	Format type (REQUIRED)		
		‘5F2E’ or ‘7F2E’	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB). See 4.5.6.		

يُستخدم معرف البند الأصلي لشكل الملف المشترك لتبادل الاستدلالات البيولوجية. وموضع البيانات لمعرف البند (‘06’ Tag) الوارد تحت نموذج معلومات الاستدلال البيولوجي (BIT, Tag ‘7F60’) [ISO/IEC 7816-11] لا تحتوي عليه هذه البنية. وبالمثل فإن سلطة تخصيص الوسم غير محددة في البنية.

لتسهيل التشغيل المتبادل، فإن سمة الاستدلال البيولوجي الأولى المسجلة في كل مجموعة بيانات يجب ترميزها حسب [ISO/IEC19794-4].
ملاحظة — المعيار ISO/IEC 39794 سوف يلي المعيار ISO/IEC 19794:2005 كمعيار دولي لترميز بيانات الاستدلال البيولوجي. انظر القسم ٤-٥-٤.

٤-٣-٧-٣ مجموعات البيانات ٣ — الملف الأولي. مجموعات البيانات ٣ عناصر البيانات

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات ٣ (DG3). ويجب أن تكون عناصر البيانات وشكلها داخل كل خانة مجموعة بيانات كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character [‘<’], — .
.B = Binary data, F = fixed-length field, Var = variable-length field>

الجدول ٤٩ — عناصر البيانات لمجموعة البيانات ٣

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If encoded finger(s) feature recorded)	Number of finger(s) biometric encodings recorded	1	F	N	0 to n identifying number of unique encodings of data on the finger(s).
02	M (If encoded finger(s) feature recorded)	Header		Var	B	Data Element may recur as defined by Data element 01.
03	M (If encoded finger(s) feature recorded)	Finger biometric data encoding(s)		Var	B	Data Element may recur as defined by Data element 01.

٤-٢-٣-١ ترميز الأنواع الفرعية من الاستدلال البيولوجي

وسم نماذج عناوين الاستدلال البيولوجي والقيم المخصصة لها هي الحد الأدنى الذي يجب أن يتحمّله كل تنفيذ حسب ما هو مبين في الجدول التالي. وكل نموذج معلومات استدلال بيولوجي منفرد له البنية التالية:

الجدول ٤ - ترميز خطة السمات الفرعية لترميز السمات الفرعية: شكل ملف مشترك لتبادل الاستدلالات البيولوجية

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Sub-type
0	0	0	0	0	0	0	0	No information given
						0	1	Right
						1	0	Left
			0	0	0			No meaning
			0	0	1			Thumb
			0	1	0			Pointer
			0	1	1			Middle
			1	0	0			Ring
			1	0	1			Little
X	X	X						Reserved for future use

٤-٣-٢-٢-٢ ترميز المثال صفر

الدول التي لا تصدر وثائق سفر الكترونية مقررة آلياً ذات البنية LDS1 مع بصمات أصابع لا ينبغي أن تملأ مجموعة البيانات ٣ (DG3). وما يعيّب مجموعة البيانات ٣ لهذه البنية أنها ستنتج بصفة رقمية ثابتة لمجموعة البيانات ٣ في المادة الأمنية للوثيقة بالنسبة لجميع وثائق السفر الإلكترونية المقررة آلياً ذات البنية LDS1 حيث لا تكون سمات الاستدلال البيولوجي موجودة ومملوقة في وقت إصدار وثيقة السفر الإلكترونية المقررة آلياً، لكن يتم الإعلان عن مجموعة البيانات ٣. ولأغراض التشغيل المتبادل فإن الدول المؤيدة لبصمات الأصابع في وثائقها الإلكترونية المقررة آلياً ذات البنية LDS1 يجب أن تخزن نموذجاً خالياً لمجموعة معلومات الاستدلال البيولوجي في الحالات التي لا تتوفر فيها بصمات أصابع في وقت إصدار وثيقة السفر الإلكترونية المقررة آلياً ذات البنية LDS1. ويسجل عدد النموذج قيمة قدرها '٠٠' في هذه الحالة.

يوصى بـ الوسم '53' والمحتوى الذي حدنته جهة الاصدار (رقم عشوائي متala).

الجدول ٥٠ — ترميز الأمثلة الصفر

Tag	L	Value				
63	Var	LDS element				
		Tag	L	Value		
		'7F 61'	'03'	Biometric Information Group Template		
			'02'	'01'	'00'	Defines that there are no Biometric Information Templates stored in this Data Group.
		'53'	Var	Issuer defined content (e.g. a random number).		

٤-٣-٧-٣ ترميز المثال واحد

في الحالات التي تتواجد فيها بصمة إصبع واحدة فقط، يجب ترميز المثال المنفرد بالطريقة التالية (مثلاً لمجموعة البيانات ٣ — بصمة الأصبع):

الجدول ٥١ — ترميز المثال واحد

Tag	L	Value				
'63'	Var	LDS element where aa is the total length of the entire LDS data content				
		Tag	L	Value		
		'7F 61'	Var	Biometric Information Group Template, where bb is the total length of the entire Group Template content.		
			'02'	'01'	'01'	Defines the total number of fingerprints stored as Biometric Information Templates that follow.
			'7F 60'	Var	First biometric information template where cc is the total length of the entire BIT	
				'A1'	Var	Biometric Header Template, where dd is the total length of the BHT
					'81'	'01' '08' Biometric type "Fingerprint"
					'82'	'01' '0A' Biometric subtype "left pointer finger"
					'87'	'02' '01 01' Format Owner JTC 1 SC 37
					'88'	'02' '00 07' Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. Of course, this fingerprint can either be a left or right finger depending on the available image.	
			'5F 2E'	Var	Biometric Data Block where ee is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.	

ملاحظة — المعيار ISO/IEC 39794 سوف يلي المعيار ISO/IEC 19794:2005 كمعيار دولي لترميز بيانات الاستدلال البيولوجي. انظر القسم ٤-٥-٦.

٤-٣-٢-٤ ترميز أكثر من المثال واحد

لتحقيق التشغيل المتبادل يجب تخزين كل سمة في نموذج معلومات استدلال بيولوجي منفرد. ويجب تحديد موضع السمة داخل نوع الاستدلال البيولوجي الفرعي لشكل ملف مشترك لتبادل الاستدلالات البيولوجية إذا توافرت هذه المعلومات. ويحتوي الجدول التالي على أمثلة محلولة لترميز شكل ملف مشترك لتبادل الاستدلالات البيولوجية لعنصر مجموعة البيانات ٣ (DG3) قابل للتشغيل المتبادل مع صورتين ل بصمات الأصابع.

الجدول ٥٢ — ترميز أكثر من المثال واحد

Tag	L	Value					
63	aa	LDS element where aa is the total length of the entire LDS data content					
		Tag	L	Value			
		‘7F 61’	Var	Biometric Information Group Template, where bb is the total length of the entire Group Template content.			
			‘02’	‘01’	‘02’	Defines the total number of fingerprints stored as Biometric Information Templates that follow.	
			‘7F 60’	Var	First biometric information template where cc is the total length of the entire BIT		
				‘A1’	Var	Biometric Header Template, where dd is the total length of the BHT	
					‘81’	‘01’	‘08’
					‘82’	‘01’	‘0A’
					‘87’	‘02’	‘01 01’
					‘88’	‘02’	‘00 07’
					Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.		
				5F 2E	Var	Biometric Data Block where ee is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.	
			‘7F 60’	ff	Second biometric information template where ff is the total length of the entire BIT		
				‘A1’	Var	Biometric Header Template, where gg is the total length of the BHT	
					‘81’	‘01’	‘08’
					‘82’	‘01’	‘09’
					‘87’	‘02’	‘01 01’
					‘88’	‘02’	‘00 07’
					Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.		
				‘5F 2E’	Var	Biometric Data Block where hh is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.	

ملاحظة — المعيار ISO/IEC 39794 سوف يلي المعيار ISO/IEC 19794:2005 كمعيار دولي لترميز بيانات الاستدلال البيولوجي. انظر القسم ٤-٥-٧.

٤-٧-٤ مجموعه البيانات ٤ — سمة إضافية لتعريف الهوية — الحقة (الحققان) (اختيارية)

تعترف الايكاو بأنه يجوز للدول الأعضاء اختيار استخدام التعرف على الحقة كتقنيات استدلال بيولوجي إضافية دعماً لتأكيد الهوية بمساعدة الآلة، التي يجب ترميزها بوصفها مجموعه البيانات ٤ (DG4).

الجدول ٥٣ — وسوم مجموعه البيانات ٤

Tag	L	Value
‘76’	Var	See Biometric encoding of EF.DG4

٤-٧-٤-١ الترميز بالاستدلال البيولوجي للملف الأولي. مجموعه البيانات ٤

يجب أن تستخدم مجموعه البيانات ٤ نموذج المجموعة لنمودج معلومات الاستدلال البيولوجي (BIT) مع البيانات المتداخلة المحددة في [ISO/IEC 7816-11]، التي تسمح بإمكان تخزين نماذج استدلال بيولوجي متعددة وهي متقدمة مع شكل الملف المشترك لتبادل الاستدلالات البيولوجية (CBEFF). ويعرف العنوان الفرعي للاستدلال البيولوجي نوع الاستدلال البيولوجي الموجود وسمة الاستدلال البيولوجي المحددة. ويجب استخدام الخيار المتداخل لـ [ISO/IEC 7816-11] حتى لعمليات ترميز نموذج استدلال بيولوجي منفرد. والحاله الأخيرة مبنية عن طريق الترقيم باستخدام n. عدد الأمثلة في مجموعه البيانات ٤ يمكن أن يكون ’n...0’.

لكل نموذج متداخل البنية التالية:

الجدول ٤ — الوسوم المتداخلة لمجموعه البيانات ٤

Tag	L	Value		
‘7F61’	Var	Biometric Information Template Group Template		
		Tag	L	Value
		‘02’	‘1’	Integer — Number of instances of this type of biometric
		‘7F60’	Var	1st Biometric Information Template
		Tag	L	Value
		‘A1’	Var	Biometric Header Template (BHT)
		Tag	L	Value
		‘80’	‘02’	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
		‘81’	‘01-03’	Biometric type (Optional)
		‘82’	‘01’	Biometric sub-type, REQUIRED for DG4
		‘83’	‘07’	Creation date and time (Optional)
		‘85’	‘08’	Validity period (from through) (Optional)
		‘86’	‘04’	Creator of the biometric reference data (PID) (Optional)
		‘87’	‘02’	Format owner (REQUIRED)
		‘88’	‘02’	Format type (REQUIRED)
		‘5F2E’ or ‘7F2E’	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).
	‘7F60’	Var		2nd Biometric Information Template

Tag	L	Value			
		Tag	L	Value	
		‘A1’	Var	Biometric Header Template (BHT)	
			Tag	L	Value
			‘80’	‘02’	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
			‘81’	‘01-03’	Biometric type (Optional)
			‘82’	‘01’	Biometric sub-type REQUIRED for DG4
			‘83’	‘07’	Creation date and time (Optional)
			‘85’	‘08’	Validity period (from through) (Optional)
			‘86’	‘04’	Creator of the biometric reference data (PID) (Optional)
			‘87’	‘02’	Format owner (REQUIRED)
			‘88’	‘02’	Format type (REQUIRED)
		‘5F2E’ or ‘7F2E’	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB). See 4.5.6.	

يُستخدم معرف البند الأصلي لشكل الملف المشترك لتبادل الاستدلالات البيولوجية. ومادة بيانات معرف البند (‘06’ Tag) تحت نموذج معلومات الاستدلال البيولوجي فقط (‘06’, 7F60, Tag, BIT) المحدد في [ISO/IEC 7816-11] غير مدرج في هذه البنية. وبالمثل فإن سلطة تخصيص الوسوم غير محددة في البنية.

لتسهيل القابلية للتشغيل المتبادل، فإن أول استدلال بيولوجي مسجل في كل مجموعة بيانات يجب ترميزه حسب [ISO/IEC19794-6].

ملاحظة —المعيار ISO/IEC 39794 سوف يلي المعيار ISO/IEC 19794:2005 كمعيار دولي لترميز بيانات الاستدلال البيولوجي. انظر القسم ٤-٥-٦.

٤-٤-٣-٤ مجموعات البيانات ٤ — الملف الأولي. عناصر بيانات مجموعات البيانات ٤

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات (DG4). ويجب أن تكون عناصر البيانات وشكلاها في كل خانة مجموعة بيانات كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], — ملاحظة —
.B = Binary data, F = fixed-length field, Var = variable-length field.

الجدول ٥٥ — عناصر البيانات لمجموعة البيانات ٤

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M, if encoded eye(s) feature included	Number of eye biometric encodings recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the eye(s).
02	M, if encoded eye(s) feature included	Header		Var	B	Data Element may recur as defined by Data element 01.
03	M, if encoded eye(s) feature included	Eye biometric data encoding(s)		Var	B	Data Element may recur as defined by Data element 01.

٤-٧-٢-١ ترميز النوع الفرعي من الاستدلال البيولوجي

وسم نموذج عنوان الاستدلال البيولوجي والقيم المخصصة لها هي الحد الأدنى الذي يجب أن يدعمه كل تنفيذ على النحو المبين في الجدول التالي. وكل نموذج معلومات استدلال بيولوجي منفرد البنية التالية:

الجدول ٥٦ — ترميز خطة السمات الفرعية لترميز السمات الفرعية:

شكل ملف مشترك لتبادل الاستدلالات البيولوجية

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Sub-type
0	0	0	0	0	0	0	0	No information given
					0	1		Right
					1	0		Left
			0	0	0			Reserved for future use
			0	0	1			Reserved for future use
			0	1	0			Reserved for future use
			0	1	1			Reserved for future use
			1	0	0			Reserved for future use
			1	0	1			Reserved for future use
X	X	X						Reserved for future use

٤-٢-٤-٢-٤ ترميز المثال صفر

الدول التي لا تصدر وثائق سفر الكترونية مقررة آلياً ذات البنية LDS1 تتضمن حدقات ينبغي ألا تملأ مجموعة البيانات ٤ (DG4). ومجموعة البيانات ٤ لهذه البنية تتسم بالعيوب المتمثل في أنها ستتخرج عنها بصمة رقمية ثابتة لمجموعة البيانات ٤ في المادة الأمنية للوثيقة بالمثل لجميع وثائق السفر الالكترونية المقررة آلياً ذات البنية LDS1 التي تكون سمات الاستدلال البيولوجي غير موجودة فيها وملئت في وقت إصدار وثيقة السفر الالكترونية المقررة آلياً ذات البنية LDS1 لكن مجموعة البيانات ٤ معلم عنها. ولأغراض التشغيل المتبادل فإن الدول الداعمة للحدقات في وثائق سفرها الالكترونية المقررة آلياً ذات البنية LDS1 يجب أن تخزن نموذجاً غير مملوء لمجموعة معلومات الاستدلال البيولوجي في الحالات التي لا توجد فيها حدقات في وقت إصدار وثيقة السفر الالكترونية المقررة آلياً ذات البنية LDS1. ويدل عدد النموذج على قيمة '00' في هذه الحالة.

يوصى بإضافة الوسم '53' إلى المضمون المحدد من قبل جهة الإصدار (رقم عشوائي مثلاً).

الجدول ٥٧ — ترميز الأمثلة صفر

Tag	L	Value			
'76'	Var	LDS element			
		Tag	L	Value	
		'7F 61'	'03'	Biometric Information Template Group Template	
			'02'	'01'	'00'
				Defines that there are no Biometric Information Templates stored in this Data Group.	
		'53'	Var	Issuer defined content (e.g. a random number).	

٤-٢-٤-٣-٤ ترميز المثال واحد

في الحالات التي توجد فيها حدقه واحدة فقط، يجب ترميز مثال منفرد.

٤-٢-٤-٤-٤ ترميز أكثر من مثال واحد

لتحقيق القابلية للتشغيل المتبادل يجب تخزين كل سمة في نموذج معلومات استدلال بيولوجي منفرد. ويجب تحديد موضع السمة داخل النوع الفرعي من الاستدلال البيولوجي لشكل الملف المشترك لتبادل الاستدلالات البيولوجية إذا توافرت هذه المعلومات.

٤-٧-٥ مجموعة البيانات ٥ — صورة الوجه المعروضة (اختيارية)

يجب أن تكون عناصر البيانات المخصصة لمجموعة البيانات ٥ (DG5) كما يلي:

الجدول ٥٨ — وسوم مجموعة البيانات ٥

Tag	L	Value		
	Var			
	Tag	L	Value	
	'02'	Var	Number of instances of this type of displayed image (REQUIRED in first template. Not used in succeeding templates.)	
	'5F40'	Var	Displayed portrait	

أصحاب الشكل التالي معترف بهم بالنسبة للنوع المحدد من الصورة المعروضة.

الجدول ٥٩ — أشكال مجموعة البيانات ٥

Displayed Image	Format Owner
Displayed Facial Image	[ISO/IEC 10918], JFIF option

٤-٥-٧-١ مجموعه البيانات ٥ — ملف أولي . عناصر بيانات مجموعة البيانات ٥ (اختيارية)

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات ٥ (DG5). وعناصر البيانات وشكلها داخل مجموعة البيانات ٥ (DG5) يجب أن تكون كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], — ملاحظة
.B = Binary data, F = fixed-length field, Var = variable-length field.

الجدول ٦٠ — عناصر البيانات لمجموعة البيانات ٥

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If displayed portrait recorded)	Number of displayed portraits recorded	1	F	N	1 to 9 identifying number of unique recordings of displayed portrait.
02	M (If displayed portrait recorded)	Displayed portrait representation(s)		Var	A,N	Data Element may recur as defined by Data element 01.
	M (If displayed portrait recorded)	Number of bytes in representation of displayed portrait	5	F	N	00001 to X9, identifying number of bytes in representation of displayed portrait immediately following.
04	M (If displayed portrait recorded)	Representation of displayed portrait		Var	B	Formatted as per [ISO/IEC 10918-1] or [ISO/IEC 15444].

ملاحظة — يجب ترميز عنصر البيانات 02 على النحو المعرف في [ISO/IEC 10918] باستخدام خيار JFIF أو [ISO/IEC 15444] باستخدام نظام ترميز الصور JPEG 2000 .

٤-٦-٦ مجموعه البيانات ٦ — محجوزة للاستخدام في المستقبل

عناصر البيانات المخصصة لمجموعة البيانات ٦ (DG6) يجب أن تكون كما يلي:

الجدول ٦١ — وسوم مجموعة البيانات ٦

Tag	L	Value
‘66’	Var	

٤-٦-٧-١ مجموعه البيانات ٧ — ملف أولي. عناصر بيانات مجموعه البيانات ٧

عناصر البيانات لمجموعة البيانات ٧ (DG6) محجوزة للاستخدام في المستقبل.

٤-٦-٧-٢ مجموعه البيانات ٧ — التوقيع المعروض أو العلامة المعتادة (اختياري أو اختيارية)

عناصر البيانات المخصصة لمجموعة البيانات ٧ (DG7) يجب أن تكون كما يلي:

الجدول ٦٢ — وسوم مجموعة البيانات ٧

Tag	L	Value		
		Tag	L	Value
‘67’	Var			
		‘02’	Var	Number of instances of this type of displayed image (REQUIRED in first template. Not used in succeeding templates.)
		‘5F43’	Var	Displayed Signature

أصحاب الأشكال التالية معترف بهم بالنسبة لنوع المحدد من الصورة المعروضة:

الجدول ٦٣ — أشكال مجموعه البيانات ٧

Displayed Image	Format Owner
Displayed Signature/usual mark	[ISO/IEC 10918], JFIF option

٤-٦-٧-٢-١ مجموعه البيانات ٧ — ملف أولي. عناصر بيانات مجموعه البيانات ٧ (اختيارية)

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات ٧ (DG7). وعناصر البيانات وشكلها داخل كل مجموعة بيانات ٧ (DG7) يجب أن تكون كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], — ملاحظة
B = Binary data, F = fixed-length field, Var = variable-length field.

الجدول ٦٤ — عناصر البيانات لمجموعة البيانات ٧

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If displayed signature or usual mark recorded)	Number of displayed signature or usual marks	1	F	N	1 to 9 identifying number of unique recordings of displayed signature or usual mark.
02	M (If displayed signature or usual mark recorded)	Displayed signature or usual mark representation		Var	B	Data Element may recur as defined by DE 01. Formatted as per [ISO/IEC 10918-1] or [ISO/IEC 15444].

ملاحظة — يجب ترميز عنصر البيانات 02 على النحو المعروف في [ISO/IEC 10918] على النحو المعروف في [ISO/IEC 10918]، باستخدام خيار JFIF، أو [ISO/IEC 15444] باستخدام نظام ترميز الصور JPEG 2000.

٤-٧-١ مجموعه البيانات ٨ — سمة (سمات) البيانات (اختيارية)

لا يزال يتبع تعريف هذه المجموعة من البيانات. وحتى ذلك الحين، فهي متوفّرة للاستخدام المؤقت بناء على الملكية. ويمكن أن يستخدم هذا العنصر من البيانات بنية مماثلة لبنيّة نماذج الاستدلال البيولوجي والتحقق من السمات الأمنية بالاستعانة بالآلات والتقصيل (التقاصيل) المرمزة. وعناصر البيانات المجمعة لتكون مجموعه البيانات ٨ (DG8) يجب أن تكون كما يلي:

الجدول ٦٥ — وسوم مجموعة البيانات ٨

Tag	L	Value		
‘68’	Var	To Be Defined		
		Tag	L	Value
		‘02’	‘1’	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			Var	Header Template. Details to be defined.

٤-٨-١ مجموعه البيانات ٨ — ملف أولي. عناصر بيانات مجموعه البيانات ٨

يصف هذا القسم عناصر البيانات التي قد توجد في مجموعه البيانات ٨ (DG8). وعناصر البيانات وأشكالها داخل كل خانة مجموعه بيانات يجب أن تكون كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], — ملاحظة —
.B = Binary data, F = fixed-length field, Var = variable-length field.d

الجدول ٦٦ — عناصر البيانات لمجموعة البيانات ٨

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of data feature(s)	1	F	N	1 to 9, identifying number of unique encodings of data feature(s) (embraces Data elements 02 and 03).
02	M (If this encoded feature is used)	Header (to be defined)	1			Header details to be defined.
03	M (If this encoded feature is used)	Data feature(s) data	999 Max	Var	A,N,S,U, B	Format defined at the discretion of issuing State or organization.

٤-٧-٩ مجموعة البيانات ٩ — السمة (السمات) البنوية (اختيارية)

لا يزال يتعين تحديد هذه المجموعة من البيانات. وإلى أن يتم ذلك، فهي متاحة من أجل الاستخدام المؤقت بناء على الملكية. ويمكن أن تستخدم هذه العناصر للبيانات بنية مماثلة لبنية نماذج الاستدلال البيولوجي. وعناصر البيانات التي تجمع لتشكل مجموعة البيانات ٩ (DG9) يجب أن تكون كما يلي:

الجدول ٦٧ — وسوم مجموعة البيانات ٩

Tag	L	Value		
‘69’	Var	To Be Defined		
		Tag	L	Value
		‘02’	‘01’	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			X	Header Template. Details to be defined.

٤-٧-١٠ مجموعة البيانات ٩ — ملف أولي. عناصر بيانات مجموعة البيانات ٩

عناصر البيانات لمجموعة البيانات ٩ (DG9) وشكلها داخل كل خانة مجموعة بيانات يجب أن تكون كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], — ملاحظة — .B = Binary data, F = fixed-length field, Var = variable-length field.

الجدول ٦٨ — عناصر بيانات مجموعة البيانات ٩

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of structure feature(s)	1	F	N	1 to 9, identifying number of unique encodings of structure feature(s) (embraces Data elements 02 and 03).
02	M (If this encoded feature is used)	Header (to be defined)			N	Header details to be defined
03	M (If this encoded feature is used)	Structure feature(s) data		Var		

٤-١٠-٧-٤ مجموعة البيانات ١٠ — السمة (السمات) البنائية (اختيارية)

لا يزال يتعين تحديد هذه المجموعة من البيانات. وإلى أن يتم ذلك، فهي متاحة من أجل الاستخدام المؤقت بناء على الملكية. ويمكن أن تستخدم هذه العناصر للبيانات بمثابة لبنية نماذج الاستدلال البيولوجي. وعناصر البيانات التي تتجمع لتشكل مجموعة البيانات ١٠ (DG10) يجب أن تكون كما يلي:

الجدول ٦٩ — وسوم مجموعة البيانات ١٠

Tag	L	Value		
'6A'	Var			
		Tag	L	Value
		'02'	'01'	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			Var	To Be Defined.

٤-١٠-٧-٥ مجموعة البيانات ١٠ — ملف أولي. عناصر بيانات مجموعة البيانات ١٠

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات ١٠ (DG10). وعناصر البيانات وشكلها داخل كل خانة مجموعة بيانات يجب أن تكون كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], —
B = Binary data, F = fixed-length field, Var = variable-length field.

الجدول ٧٠ — عناصر البيانات لمجموعة البيانات ١٠

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of substance feature(s) recorded	1	F	N	1 to 9, identifying number of unique encodings of substance feature(s) (embraces Data elements 02 and 03).
02	M (If this encoded feature is used)	Header (to be defined)	TBD	TBD	N	Details to be defined.
03	M (If this encoded feature is used)	Substance feature(s) data	999 Max	Var	A,N,S,B	Format defined at the discretion of issuing State or organization.

٤-١١-٧-٤ مجموعة البيانات ١١ — التفصيل الشخصي الإضافي (التفاصيل الشخصية الإضافية) (اختيارية)

تُستخدم هذه المجموعة من البيانات للتفاصيل الإضافية عن حامل الوثيقة. ونظراً لأن جميع عناصر البيانات داخل هذه المجموعة اختيارية، تُستخدم قائمة باللوسوم لتحديد تلك الموجودة منها. وعناصر البيانات التي تتجمع لتشكل مجموعة البيانات ١١ (DG11) يجب أن تكون كما يلي:

ملاحظة — قد يحتوي هذا النموذج على حروف غير لاتينية.

الجدول ٧١ — وسوم مجموعة البيانات ١١

Tag	L	Value			
‘6B’	Var				
		Tag	L	Value	
		‘5C’	Var		Tag list with list of Data Elements in the template.
		‘5F0E’	Var		Full name of document holder in national characters. Encoded per Doc 9303 rules.
		‘A0’	Var		Content-specific class
			Tag	L	Value
			‘02’	‘01’	Number of other names
			‘5F0F’	Var	Other name formatted per Doc 9303. The data object repeats as many times as indicated in number of other names (data object with Tag ‘02’)
		Tag	L	Value	
		‘5F10’	Var		Personal number
		‘5F2B’	‘08’		Full date of birth yyyyymmdd
		‘5F11’	Var		Place of birth. Fields separated by ‘<’
		‘5F42’	Var		Permanent address. Fields separated by ‘<’
		‘5F12’	Var		Telephone
		‘5F13’	Var		Profession
		‘5F14’	Var		Title
		‘5F15’	Var		Personal summary
		‘5F16’	Var		Proof of citizenship. Compressed image per [ISO/IEC 10918]
		‘5F17’	Var		Other valid TD numbers. Separated by ‘<’
		‘5F18’	Var		Custody information

٤-١١-٧-١ مجموعه البيانات ١١ — ملف أولي. عناصر بيانات مجموعه البيانات ١١

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعه البيانات ١١ (DG11). وعناصر البيانات وشكلها داخل خانة كل مجموعه بيانات يجب أن تكون كما في الجدول التالي:

ملاحظة ١ — يجب ترميز مجموعه البيانات ١١ على النحو المحدد في [ISO/IEC 10918], باستخدام الخيار JFIF أو [ISO/IEC 15444] باستخدام نظام ترميز الصور JPEG 2000 .

ملاحظة ٢ — *A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.*

الجدول ٧٢ — عناصر البيانات لمجموعة البيانات ١١

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	O	Name of holder (in full)	99 Max	Var	B	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
02	O	Other name(s)	99 Max	Var	B	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
03	O	Personal number	99 Max	Var	U	Free-form text.
04	O	Full date of birth	8	F	N	YYYYMMDD
05	O	Place of birth	99 Max	Var	U	Free-form text.
06	O	Address	99 Max	Var	U	Free-form text.
07	O	Telephone	99 Max	Var	N,S	Free-form text. Encoding per ITU-T E.164 recommended
08	O	Profession	99 Max	Var	U	Free-form text.
09	M, if Data element 08 included	Title	99 Max	Var	U	Free-form text.
10	M, if Data element 09 included	Personal summary	99 Max	Var	U	Free-form text.
11	M, if Data element 10 included	Proof of citizenship		Var	B	Image of citizenship document formatted as per [ISO/IEC 10918-1]
12	O	Other valid travel document(s) Travel document number	99 Max	Var	U	Free-form text, separated by <.
13	O	Custody information	999 Max	Var	U	Free-form text.

ملاحظة — في حالة عدم معرفة الشهر (MM) أو اليوم (DD)، فإن الطريقة القابلة للتشغيل المتداول لبيان هذا في مجموعة البيانات ١١ هي ضبط الحروف المعنية على '00'. وفي حالة عدم معرفة القرن والسنة (CCYY)، فإن الطريقة القابلة للتشغيل المتداول لبيان هذا في مجموعة البيانات ١١ هي ضبط الحروف المعنية على '0000'. ويجب دائماً أن تستخدم باستمرار التواريخ التي خصصتها جهة الاصدار.

٤-٧-٢-١٢ مجموعة البيانات ١٢ — تفصيل الوثيقة الاضافي (تفاصيل الوثائق الاضافية) (اختيارية)

تُستخدم هذه المجموعة للبيانات للمعلومات الاضافية عن الوثيقة. وجميع عناصر البيانات داخل هذه المجموعة اختيارية.

الجدول ٧٣ — وسوم مجموعة البيانات ١٢

Tag	L	Value		
‘6C’	Var			
	Tag	L	Value	
	‘5C’	Var	Tag list with list of Data Elements in the template	
	‘5F19’	Var	Issuing Authority	
	‘5F26’	‘08’	Date of issue. yyymmdd	
	‘A0’	Var	Content-specific class	
		Tag	L	Value
		‘02’	‘01’	Number of other persons
		‘5F1A’	Var	Name of other person formatted per Doc 9303 rules. The data object repeats as many times as indicated in number of other names Data element 02 (data object with Tag ‘02’).
	‘5F1B’	Var		Endorsements, observations
	‘5F1C’	Var		Tax/Exit requirements
	‘5F1D’	Var		Image of front of document. Image per ISO/IEC 10918.
	‘5F1E’	Var		Image of rear of document. Image per ISO/IEC 10918.
	‘5F55’	‘0E’		Date and time of document personalization yyymmddhhmmss
	‘5F56’	Var		Serial number of personalization system

يُوصى بأن تدعم نظم التفتيش ترميز كل من ASCII 8 bytes و BCD.

٤-١٢-٧-١٢ مجموعة البيانات ١٢ — ملف أولي. عناصر بيانات مجموعة البيانات ١٢

يصف هذا القسم عناصر البيانات التي قد تتضمنها مجموعة البيانات ١٢ (DG12). وعناصر البيانات وشكلها داخل كل مجموعة بيانات يجب أن تكون كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], — B = Binary data, F = fixed-length field, Var = variable-length field.

ملاحظة ٢ — يجب ترميز عنصري البيانات 07 و 08 على النحو المحدد في [ISO/IEC 10918]، باستخدام الخيار JFIF أو [ISO/IEC 15444] باستخدام نظام ترميز الصور 2000 JPEG .

الجدول ٧٤ — عناصر البيانات لمجموعة البيانات ١٢

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	O	Issuing Authority	99 Max	Var	U	Free-form text.
02	O	Date of issue	8	F	N	Date of issue of document; i.e. YYYYMMDD.
03	O	Other person(s) details	99 Max	Var	U	Free-form text
04	O	Endorsement(s)/Observation(s)	99 Max	Var	U	Free-form text.
05	O	Tax/Exit requirements	99 Max	Var	U	Free-form text.
06	O	Image of front of eMRTD		Var	B	Formatted as per [ISO/IEC 10918-1]
07	O	Image of rear of MRTD		Var	B	Formatted as per [ISO/IEC 10918-1]
08	O	Personalization time	14	F	N	yyyymmddhhmmss
09	O	Personalization device serial number	99 max	Var	U	Free format.

٤-٧-١٣ مجموعة البيانات ١٣ — التفاصيل الاختيارية (اختيارية)

عناصر البيانات المجموعة لتكون مجموعة البيانات ١٣ (DG13) متروكة لاختيار دولة أو منظمة الاصدار ويجب أن تكون كما يلي:

الجدول ٧٥ — وسوم مجموعة البيانات ١٣

Tag	L	Value
‘6D’	Var	

٤-٧-٤ مجموعة البيانات ٤ - الخيارات الأمنية (مشروطة)

تحتوي مجموعة البيانات ٤ (DG14) على خيارات أمنية من أجل الآليات الأمنية الإضافية. وللابلاغ على التفاصيل انظر الوثيقة Doc 9303-11. والملف DG14 الذي تحتوي عليه طلب وثيقة السفر الالكترونية المقرورة آلياً مطلوب إذا كان تحديد التحقق من صحة الرقاقة أو GM-/IM- مدعوماً برقاقة وثيقة السفر الالكترونية المقرورة آلياً.

الجدول ٧٦ - وسوم مجموعة البيانات ٤

Tag	L	Value
'6E'	Var	Refer to Doc 9303-10 DG14 SecurityInfos

٤-٧-١ مجموعة البيانات ٤ - ملف أولي. عناصر بيانات مجموعة البيانات ٤

يصف هذا القسم عناصر البيانات التي قد تكون موجودة في مجموعة البيانات ٤ (DG14). ويجب أن تكون عناصر البيانات وشكلها داخل كل خانة مجموعة بيانات كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], — ملاحظة
 .B = Binary data, F = fixed-length field, Var = variable-length field.

الجدول ٧٧ - عناصر البيانات لمجموعة البيانات ٤

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
	O	SecurityInfos		Var	B	Refer to Doc 9303-10. DG14 SecurityInfos as defined in 4.7.14.2

٤-١-٤ مجموعة البيانات ٤ SecurityInfos (المعلومات الأمنية)

المعلومات الأمنية التالية عن بنية البيانات العامة لمجموعة الرموز الأولى لتركيب الخلاصات تتيح مختلف أشكال تنفيذ الخيارات الأمنية لسمات الاستدلال البيولوجي الثانية. ولأسباب متعلقة بالتشغيل المتبدال، يوصى بأن توفر هذه البنية للبيانات رقاقة وثيقة السفر الالكترونية المقرورة آلياً في مجموعة البيانات ٤ لبيان البروتوكولات الأمنية المدعومة. وبنية البيانات محددة على النحو التالي:

```

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

العناصر التي تحتوي عليها بنية بيانات المعلومات الأمنية لها المعنى التالي:

- البروتوكول المعرف للمادة يعرف البروتوكول الداعم؛
- البيانات المطلوبة من النوع المفتوح تحتوي على بيانات إلزامية خاصة بالبروتوكول؛
- البيانات اختيارية من النوع المفتوح تحتوي على بيانات اختيارية خاصة بالبروتوكول.

٤-١٥-٧-١٥ مجموعه البيانات ١٥ — معلومات المفتاح العام للتحقق الإيجابي من الصحة الفعال (مشروطة)

هذه المجموعة من البيانات اختيارية تحتوي على المفتاح العام للتحقق الإيجابي من الصحة الفعال وهو مطلوب عند تنفيذ التحقق الإيجابي من الصحة الفعال اختياري للتحقق من صحة الرقاقة على النحو الموصوف في الوثيقة Doc 9303-11.

الجدول ٧٨ — وسوم مجموعه البيانات ١٥

Tag	L	Value
'6F'	Var	Refer to Doc 9303-11

٤-١٥-٧-١٥-١ مجموعه البيانات ١٥ — ملف أولي. عناصر بيانات مجموعه البيانات ١٥

يصف هذا القسم عناصر البيانات التي يجوز أن تكون موجودة في مجموعه البيانات ١٥ (DG15). وعناصر البيانات وشكلها داخل كل خانة مجموعه بيانات يجب أن تكون كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], —
B = Binary data, F = fixed-length field, Var = variable-length field.

الجدول ٧٩ — عناصر البيانات لمجموعه البيانات ١٥

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
O	ActiveAuthenticationPublicKeyInfo			Var	B	See Doc 9303-11

٤-١٦-٧-١٦ مجموعه البيانات ١٦ — الشخص الذي يتعين إبلاغه (الأشخاص الذين يتعين إبلاغهم) (اختيارية)

تتضمن هذه المجموعة للبيانات قوائم بمعلومات الإبلاغ عند الطوارئ. وهي مرمرة كسلسلة من النماذج باستخدام الدالة بالوسم 'Ax'. ومجموعه البيانات ١٦ (DG16) (شأنها شأن جميع مجموعات البيانات الأخرى) لا ينبغي تحريرها بعد الاصدار، ويتم تمثيل مجموعه البيانات ١٦ بقيمة بحصة رقمية في المادة الأمنية للوثيقة والمادة الأمنية للوثيقة يتم التوقيع عليها مرة واحدة فقط عند الاصدار.

الجدول ٨٠ — وسوم مجموعة البيانات ١٦

Tag	L	Value		
‘70’	Var			
		Tag	L	Value
		‘02’	‘01’	Number of templates (occurs only in first template)
		‘Ax’	Var	Start of template, where x (x = 1,2,3...) increments for each occurrence
‘5F50’	‘08’			Date data recorded
‘5F51’	Var			Name of person
‘5F52’	Var			Telephone
‘5F53’	Var			Address

٤-١٦-٧-١ مجموعه البيانات ١٦ — ملف أولى. عناصر بيانات مجموعه البيانات ١٦

يصف هذا القسم عناصر البيانات التي يجوز تقديمها في مجموعة البيانات ١٦ (DG16). وعناصر البيانات وشكلها داخل كل خانة مجموعة بيانات يجب أن تكون كما في الجدول التالي:

A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character [;<=], — ملاحظة

.B = Binary data, F = fixed-length field, Var = variable-length field.

الدول ٨١ — عناصر البيانات لمجموعة البيانات ١٦

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M, if DG16 included	Number of persons identified	1	F	N	Identifies number of persons included in the Data Group.
02	M, if DG16 included	Date details recorded	8	F	N	Date notification date recorded; Format = YYYYMMDD.
03	M, if DG16 included	Name of person to notify Primary and secondary identifiers		Var	A,N,S	Filler characters (<) inserted as per MRZ. Truncation not permitted.
04	M, if Data element 03 included	Telephone number of person to notify		Var	N,S	Telephone number in international form (country code and local number). Encoding per ITU-T E.164 recommended.
05	M	Address of person to notify		Var	U	Free-form text.

٥ - تطبيقات البنية LDS2 (اختيارية)

بنية البيانات المنطقية ٢ (LDS2) هي امتداد اختياري لوثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 ومتافق معها عكسياً يسمح بالتخزين الرقمي والأمن للمعلومات المتعلقة بالسفر، وذلك بعد أن يتم إصدار الوثيقة. تقوم البنية LDS2 بتوسيع استخدام وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 عبر إضافة تطبيقات قد تسمح بالتخزين الرقمي لبيانات السفر (التأشيرات وأختام السفر) وللمعلومات الأخرى التي تسهل سفر صاحب الوثيقة (بيانات الاستدلال البيولوجي) خلال فترة صلاحيتها. ويساهم تحسين الاستفادة من كامل إمكانات وثيقة السفر الإلكترونية المقرورة آلياً من خلال "رقمنة" باقي البيانات التي تحتويها الوثيقة في توفير مجموعة من فوائد التسهيل، ويوفر في الوقت نفسه حماية أكبر لوثائقه من مواطن الضعف من قبيل التزوير والنسخ والقراءة أو الكتابة غير المصرح بها.

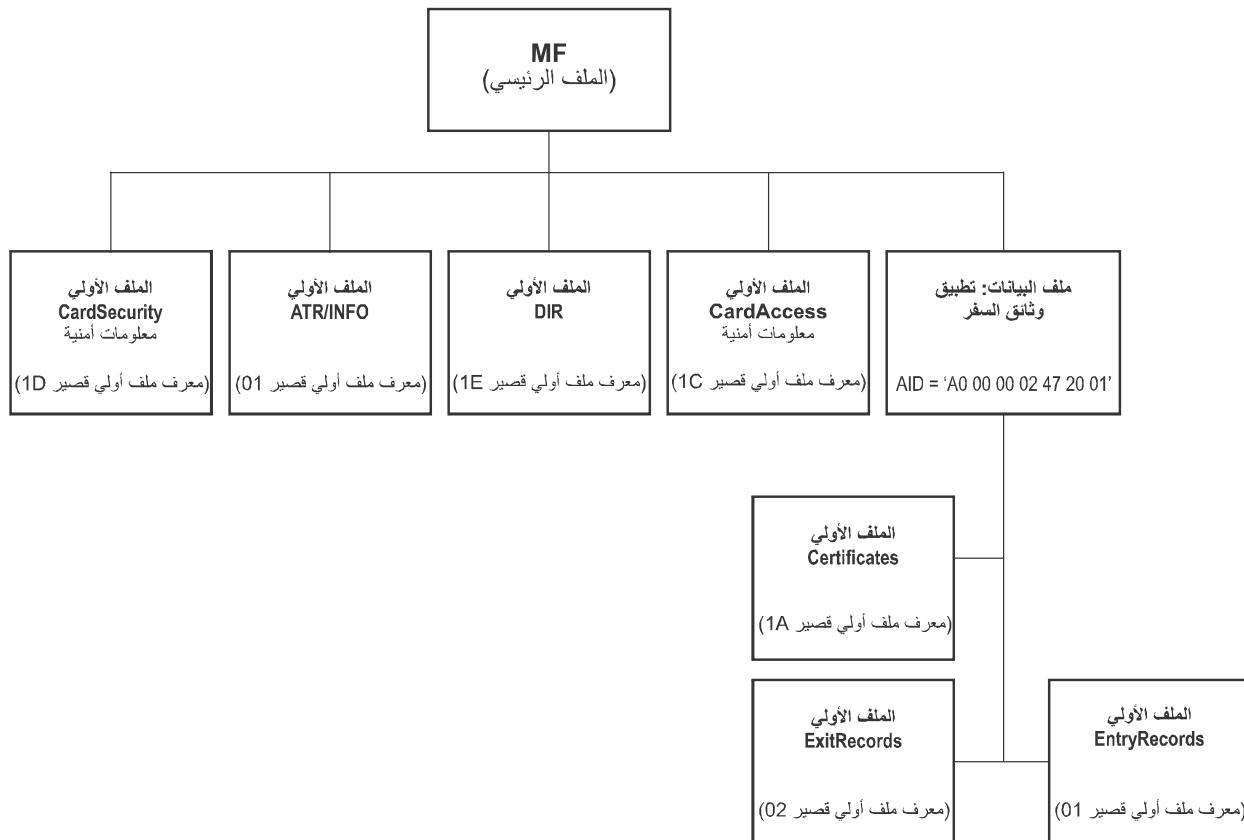
وفيما يلي التطبيقات الإضافية والاختيارية الواردة على شكل البنية LDS2:

- سجلات السفر (الأختام)؛
- والتأشيرات الإلكترونية؛
- وبيانات الاستدلال البيولوجي الإضافية.

ويشترط بأن تكون وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS1 موجودة قبل الإعلان عن أي تطبيقات LDS2 اختيارية.

١-٥ تطبيق سجلات السفر (مشروع)

يجوز لدولة أو منظمة الإصدار أن تتفّق تطبيق سجلات السفر. وإذا تم الاستناد إلى التطبيق اختياري لسجلات السفر، ينبغي القيام بما يلي بصورة مشروطة.



الشكل ٤ — بنية سجلات السفر

تخزن سجلات السفر الخاصة بالدخول والخروج في ملفين أوليين هما الملف الأولي لسجلات الدخول EF.EntryRecords والملف الأولي لسجلات الخروج EF.ExitRecords تحت الملف المخصص لتطبيق سجلات السفر بحيث يكون لهما بنية خطية ذات سجلات متغيرة الحجم وفقاً لـ [ISO/IEC 7816-4]. وتخزن شهادات موقع سجلات السفر في ملف أولي منفصل هو EF.Certificates يكون له بنية خطية ذات سجلات متغيرة الحجم.

١-١-٥ ملف التطبيق — الملف المخصص

يجب أن يتم اختيار تطبيق سجلات السفر باستخدام معرف التطبيق كاسم ملف مخصص محجوز. ويتألف معرف التطبيق من معرف التطبيق المسجل الذي تخصصه المنظمة الدولية لتوحيد المقاييس وفقاً لـ [ISO/IEC 7816-5] يليه امتداد لمعرف تطبيق الملكية (PIX) الخاص بتطبيق سجلات السفر .

- يكون معرف التطبيق المسجل 'A0 00 00 02 47' ؟
- ويجب أن يستخدم تطبيق سجلات السفر 'PIX = 20 01' ؛
- ويجب أن يكون معرف التطبيق الكامل لتطبيق سجلات السفر 'A0 00 00 02 47 20 01' .

إذا لم يمنح الإذن الفعال حقوق الوصول إلى أي بيانات في تطبيق البنية LDS2، يجب أن ترفض الدارة المتكاملة اختيار التطبيق.

٥-١-٢ الملف الأولي EF.Certificates (النرمي)

تخزن شهادات موقع سجلات السفر في ملف أولي داخل الملف المخصص للتطبيق وتكون بنيتها خطية ذات سجلات متغيرة الحجم. ويتوخى أن يستخدم نظام التفتيش هذه الشهادات لمواصلة التحقق من صحة التواقيع الرقمية خارج شبكة الإنترنت لكل سجل في كلا الملفين الأوليين . EF.EntryRecord و EF.ExitRecords

الجدول ٨٢ — الملف الأولي EF.Certificates

File Name	EF.Certificates
File ID	'011A'
Short EF Identifier	'1A'
Select / FMM Access	PACE+TA (Travel record authorization bit b3 according to Table 96)
Read record / Search Record Access	PACE+TA (Travel record authorization bit b3 according to Table 96)
Append Record Access	PACE+TA (Travel record authorization bit b4 according to Table 96)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

يحتوي سجل الشهادات على مادة بيانات الشهادة X.509 لموقع واحد LDS2-TS. ويمكن الإشارة إلى سجل شهادات بسجل سفر واحد أو أكثر للدخول أو الخروج.

الجدول ٨٣ — الملف الأولي EF.Certificates

Tag	Content	Mandatory /Optional	Format	Example
'5F3A'	Certificate serial number	M	V(22)B	'5F3A' 'Len' {Country code SerialNumber }
'72'	X.509 certificate	M	V (900) B	'72' 'Len' { X.509 Certificate }

ملاحظة — تستخدم وسوم ما بين الصناعات المحددة في هذا الجدول في سياق بنية البيانات المنطقية، وبالتالي لا يلزم خطة التخصيص وسوم مترابطة.

يجب أن تحتوي مادة البيانات '5F3A' على رمز البلد المؤلف من حرفين وفقاً للوثيقة Doc 9303، الجزء الثالث (نفس الترميز والقيمة كما في الشهادة X.509 الذي يصدر اسم البلد countryName على شهادة المواطن) يليه الرقم التسليلي للشهادة.

تحتوي كل شهادة X.509 على مجموعة من البيانات المرمزة وفقاً للترميز ASN.1 والمبينة في الجدول ٨٤. ويمكن الاطلاع على المتطلبات التفصيلية للشهادة X.509 في مواصفة الوصف الموجز للشهادة الواردة في الوثيقة Doc 9303-12.

الجدول ٨٤ — مثال لبنية الشهادة X.509

Field	Description	Example value
Certificate		
version	Must be version 3	2
serialNumber	Unique positive integer	20 bytes max
signature	Signature algorithm	ecdsa-with-SHA256
issuer		
countryName	Issuing country name	'US'
commonName	Issuer name (9 characters max.)	'DHSCA0001'
validity		
notBefore	Cert. effective date	'131225000000Z'
notAfter	Cert. expiration date	'230824235959Z'
subject		
countryName	IS country name	'US'
commonName	IS name (9 characters max.)	'SFO000001'
subjectPublicKeyInfo		
Public Key Algorithm	ecPublicKey	
Subject Public Key	IS public key	ECC256 Public Key
extensions		
AuthorityKeyIdentifier		
ExtKeyUsage		
Signature Algorithm	ecdsa-with-SHA256	
Signature	Issuer's Signature	ECDSA256 signature

ملاحظة — هذا الجدول هو مثال لغرض التوضيح فقط. تكتب سجلات الشهادات في الملف الأولي EF.Certificates تحت الملف المخصص لتطبيق سجلات السفر باستخدام الأمر APPEND RECORD. ويمكن قراءة سجلات الشهادات من الملف EF.Certificates باستخدام الأمر READ RECORD. ويجب عدم تحديث سجلات الشهادات أو محوها. ويجب أن يكون العدد الأقصى للسجلات في الملف EF.Certificates تحت الملف المخصص لتطبيق سجلات السفر ٢٥٤.

٣-١-٥ الملف الأولي EF.ExitRecords (الإرادي)

يجب أن يقوم نظام تقيش مصريح له بإلحق سجلات الخروج بعد ركوب الطائرة.

الجدول ٨٥ — الملف الأولي EF.ExitRecords

File Name	EF.ExitRecords
File ID	'0102'
Short EF Identifier	'02'
Select / FMM Access	PACE+TA (Travel record authorization bit b1 according to Table 96)
Read Record / Search Record Access	PACE+TA (Travel record authorization bit b1 according to Table 96)
Append Record Access	PACE+TA (Travel record authorization bit b2 according to Table 96)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

ويبيّن الجدول ٨٦ محتوى سجل الخروج.

ملاحظة — تستخدم وسوم ما بين الصناعات المحددة في الجدول أدناه في سياق بنية البيانات المنطقية، وبالتالي لا يلزم خطة التخصيص وسوم مترافق.

الجدول ٨٦ — شكل سجل الدخول/الخروج

Tag	Tag	Content	Mandatory /OPTIONAL	Format	Example
'5F44'		Embarkation/Debarkation State (copy for SEARCH RECORD)	M	F (3) A	USA
'73'		Entry / Exit Travel Record (signed info)			
	'5F44'	Embarkation/Debarkation State	M	F (3) A	USA
	'5F4C'	Visa approvals, refusals, and revocations	O	V (50) A,N,S,U	Free-form text
	'5F45'	Travel date (Date of entry/exit)	M	F (8) N	20120814 (yyyymmdd)
	'5F4B'	Inspection authority	M	V (10) A,N,S	CBP
	'5F46'	Inspection location (Port of Entry/Exit)	M	V (10) A,N,S	SFO
	'5F4A'	Inspector reference	M	V (20) A,N,S	SFO00001234
	'5F4D'	Result of inspection	O	V (50) A,N,S,U	Free-form text
	'5F49'	Mode of travel	O	F (1) A	A (Air), S (Sea), L (Land)
	'5F48'	Duration of stay (days)	O	V (2) B	'00FF' (255 days)
	'5F4E'	Conditions holder is required to observe while in the issuing State	O	V(50) A,N,S,U	Free-form text
'5F37'		Authenticity token (Signature)	M	V (140) B	'5F' '37' Len {Signature}

Tag	Tag	Content	Mandatory /OPTIONAL	Format	Example
'5F38'		Reference (record number) to LDS2-TS Signer certificate in Certificates Store	M	F (1) B	'01' ... 'FE'

الملحوظة ١ — *A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<'], .B = Binary data, F = fixed-length field, V = variable-length field.*

الملحوظة ٢ — حيث يرجح أن تكون شهادات موقع LDS2-TS هي نفسها في سجلات سفر متعددة (مثلاً عند الدخول إلى بلد والخروج منه من نفس المطار الذي يكون لديه موقع واحد LDS2-TS)، قبل كتابة أو إلحاقي شهادة جديدة في الملف EF.Certificates، ينبغي أن يبحث نظام التفتيش في الملف EF.Certificates عن نسخة عن الشهادة نفسها، وأن يضع إحالة للشهادة القائمة. يسهم ذلك في تقليل حجم الملف EF.Certificates ويسمح بإجراء بحث أسرع.

الملحوظة ٣ — لا تفرض وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS2 على نظام التفتيش أن يكتب سجلات الدخول في الملف الأولي EF.EntryRecords، ولكن ليس في الملف الأولي EF.ExitRecords، والعكس بالعكس.

الملحوظة ٤ — رمز دولة الصعود/النزول المؤلف من ثلاثة أحرف وفقاً للوثيقة Doc 9303-3.

يكون ترتيب مواد البيانات في السجل ثابتاً. ويجب على نظام التفتيش أن يبني محتوى السجل باستخدام مواد البيانات بالترتيب المحدد في الجدول.

ويجب أن يحتوي كل سجل على توقيع رقمي (إشارة التحقق من الصحة) يتم حسابه خلال 'DO'73، بما في ذلك Tag 73 والطول. ويتولد التوقيع بواسطة موقع LDS2-TS.

ويجب أن تخزن شهادات موقع LDS2-TS الالزمة للتحقق من توقيع سجل السفر في الملف الأولي EF.Certificates تحت الملف المخصص لتطبيق سجلات السفر إذا لم يكن متوفراً أصلاً في الملف ذاته.

تكتب سجلات السفر في الملف الأولي باستخدام الأمر APPEND RECORD. ويجب عدم تغيير (تحديث) سجلات السفر أو محوها. ويجب أن يكون العدد الأقصى للسجلات في كل ملف أولي ٢٥٤.

٤-١-٤ الملف الأولي EF.EntryRecords (إنرامي)

يجب أن يقوم نظام تفتيش مصرح له بإلحاقي سجلات الدخول بعد النزول من الطائرة.

الجدول ٨٧ — الملف الأولي EF.EntryRecords

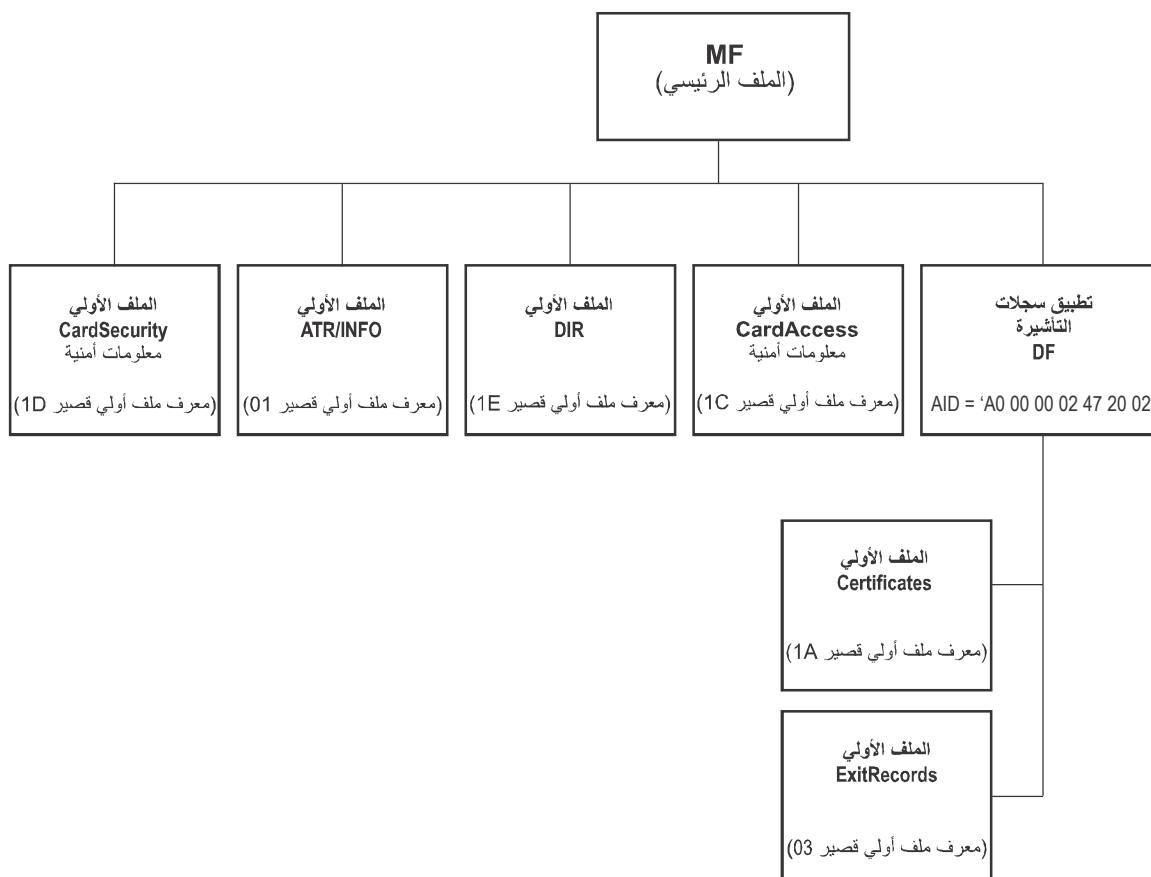
File Name	EF.EntryRecords
File ID	'0101'
Short EF Identifier	'01'
Select / FMM Access	PACE+TA (Travel record authorization bit b1 according to Table 96)
Read Record / Search Record Access	PACE+TA (Travel record authorization bit b1 according to Table 96)
Append Record Access	PACE+TA (Travel record authorization bit b2 according to Table 96)
Write / Update Record Access	NEVER
Erase Record Access	NEVER

File structure	Linear structure with records of variable size
Size	Variable

تكون بنية سجل الدخول مطابقة لبنية سجل الخروج المحددة في الجدول .٨٨

٢-٥ تطبيق سجلات التأشيرات (مشروع)

يجوز لدولة أو منظمة الإصدار أن تتفّق تطبيق سجلات التأشيرات. وإذا تم الاستناد إلى التطبيق الاختياري لسجلات التأشيرات، ينبغي القيام بما يلي .



الشكل ٥ – بنية سجلات التأشيرات

تخزن سجلات التأشيرات في الملف الأولي EF.VisaRecords تحت الملف المخصص لتطبيق سجلات التأشيرات. ويجب أن يكون الملف الأولي بنية خطية ذات سجلات متغيرة الحجم وفقاً لـ [ISO/IEC 7816-4]. وتخزن شهادات موقع سجلات التأشيرات في ملف أولي منفصل هو EF.Certificates يكون له بنية خطية ذات سجلات متغيرة الحجم.

١-٢-٥ ملف التطبيق — الملف المخصص

يجب أن يتم اختيار تطبيق سجلات التأشيرات باستخدام معرف التطبيق كاسم ملف مخصص محجوز. ويتألف معرف التطبيق من معرف التطبيق المسجل الذي تخصصه المنظمة الدولية لتوحيد المقاييس وفقاً لـ [ISO/IEC 7816-5] يليه امتداد لمعرف تطبيق الملكية (PIX) الخاص بتطبيق سجلات التأشيرات:

- يكون معرف التطبيق المسجل 'A0 00 00 02 47'؛
- ويجب أن يستخدم تطبيق سجلات التأشيرات '02' = PIX؛
- ويجب أن يكون معرف التطبيق الكامل لتطبيق سجلات التأشيرات 'A0 00 00 02 47 20 02'.

وإذا لم يمنح الإذن الفعال حقوق الوصول إلى أي بيانات في تطبيق البنية LDS2، يجب أن ترفض الدارة المتكاملة اختيار التطبيق.

٢-٢-٥ الملف الأولي EF.Certificates (الإنزامي)

تخزن شهادات موقع سجلات التأشيرات في ملف أولي EF.Certificates داخل للتطبيق الملف المخصص وتكون بنيتها خطية ذات سجلات متغيرة الحجم. ويتوخى أن يستخدم نظام التفتيش هذه الشهادات لمواصلة التحقق من صحة التوقيع الرقمية خارج شبكة الإنترنت لكل سجل في الملف الأولي EF.VisaRecords.

الجدول ٨٨ — الملف الأولي EF.Certificates

File Name	EF.Certificates
File ID	'011A'
Short EF Identifier	'1A'
Select / FMM Access	PACE+TA (Visa record authorization bit b3 according to Table 97)
Read Record / Search Record Access	PACE+TA (Visa record authorization bit b3 according to Table 97)
Append Record Access	PACE+TA (Visa record authorization bit b4 according to Table 97)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

يحتوي سجل الشهادات على مادة بيانات الشهادة X.509 لموقع واحد LDS2-TS. ويمكن الإشارة إلى سجل الشهادات بوحدة أو أكثر من سجلات التأشيرات VisaRecords.

تكون بنية سجل الشهادات في تطبيق التأشيرات مطابقة لبنية سجل الشهادات في تطبيق سجلات السفر المحدد في الجدول ٨٣.

تكتب سجلات الشهادات في الملف الأولي EF.Certificates الواقع تحت الملف المخصص لتطبيق سجلات التأشيرات باستخدام الأمر APPEND RECORD. ويمكن قراءة سجلات الشهادات باستخدام الأمر READ RECORD. ويجب عدم تحديث أو حذف سجلات الشهادات. ويجب أن يكون العدد الأقصى للسجلات في الملف EF.Certificates تحت الملف المخصص لتطبيق سجلات التأشيرات ٢٥٤.

٣-٢-٥ الملف الأولي EF.VisaRecords (النرمي)

يجب أن تخزن سجلات التأشيرات في الملف الأولي EF.VisaRecords الذي تكون بنيته خطية ذات سجلات متغيرة الحجم

الجدول ٨٩ — الملف الأولي EF.VisaRecords

File Name	EF.VisaRecords
File ID	'0103'
Short EF Identifier	'03'
Select / FMM Access	PACE+TA (Visa record authorization bit b1 according to Table 97)
Read Record / Search Record Access	PACE+TA (Visa record authorization bit b1 according to Table 97)
Append Record Access	PACE+TA (Visa record authorization bit b2 according to Table 97)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

ويجب أن يحتوي كل سجل من سجلات التأشيرات على تسلسل من مواد البيانات BER-TLV (DO '5F28' و '71' DO)، يليه مادة بيانات إشارة التحقق من الصحة (التوقيع) ومادة بيانات تحتوي على مرجع لشهادة موقع LDS2-V في الملف EF.Certificates. وتحتوي مادة البيانات DO '71، على مجموعة من مواد البيانات (الخانات) المدرجة في الجدول أدناه.

ملاحظة — تستخدم وسوم ما بين الصناعات المحددة في الجدول أدناه في سياق بنية البيانات المنطقية، وبالتالي لا يلزم خطة التخصيص وسوم متعاقبة.

الجدول ٩٠ — شكل الملف الأولي EF.VisaRecords

Tag	Tag	Content	MANDATORY/ OPTIONAL/ CONDITIONAL	Format	Example
'5F28'		Issuing State or organization (Copy for SEARCH RECORD)	M	F (3) A	NLD
'71'		Visa Record (signed info)			
'5F28'		Issuing State or organization	M	F (3) A	NLD
'43'		Document Type	M	F (2) A,N,S	VS
'5F71'		Machine Readable Visa of Type A	O	F (48) A,N,S	
'5F72'		Machine Readable Visa of Type B	O	F (44) A,N,S	VCD<<DENT<<ARTHUR<PHILIP<<<<<<<<
'5F73'		Number of entries	O	V (1) B	'01' – 'FF'
'5F74'		Duration of stay (days, months, years)	O	F (3) B	'010000' – 'FFFFFF'
'5F75'		Passport number	O	F (9) A,N,S	XI85935F8
'5F76'		Visa Type/class/category	O	V (4) B	
'5F77'		Territory Information	O	V (8) B	
'49'		Place of issuance (Issuing authority)	M	V (50) A, Sp	NEW YORK
'5F25'		Effective Date (Date of issuance)	M	F (8) N	20120826 (yyyymmdd)
'5F24'		Expiration Date	M	F (8) N	20130826 (yyyymmdd)
'5A'		Document number	M	F (9) A,N,S	XI85935F8
'5F32'		Additional information (endorsements: duration, limitations and fees paid)	O	V (50) A,N,S,U	Free-form text
'5B'		Name of holder (full name)	M	V (50) A, Sp	VAN DER STEEN MARIANNE LOUISE
'5F33'		Primary Identifier (surname)	M	V (50) A, Sp	VAN DER STEEN
'5F34'		Secondary Identifier (given name)	M	V (50) A, Sp	MARIANNE LOUISE
'5F35'		Sex	M	F (1) A,S	F, M, or <
'5F2B'		Date of birth	M	F (8) N,S	19870814 (yyyymmdd)
'5F2C'		Nationality	M	F (3) A	NLD
'5F1F'		MRZ	M	V (50) A,N,S	VAN<DER<STEEN<< MARIANNE<LOUISE
'5F40'		Reference to Additional Biometrics EF	O	F (2) B	'0201'
'5F37'		Authenticity token (Signature)	M	V (140), B	'5F' '37' Len {Signature}
'5F38'		Reference (record number) to LDS2-V Signer certificate in Certificates Store	M	F (1) B	'01' ... 'FE'

الملاحظة ١ — *A = Alpha character [a-z, A-Z], N = Numeric character [0-9], S = Special character ['<']*

.B = Binary data, F = fixed-length field, V = variable-length field, Sp = Space.

الملاحظة ٢ — رمز دولة الإصدار المؤلف من ثلاثة أحرف وفقاً للوثيقة ٣ Doc 9303-3.

الملاحظة ٣ — يجب أن تحتوي مادة البيانات 'DO'5F40'، في حال وجودها، على نوعين من الملفات الأولية ضمن تطبيق بيانات الاستدلال البيولوجي الإضافية الذي يحتوي على بيانات الاستدلال البيولوجي. ولا يجوز استخدام مادة البيانات هذه إلا إذا كان تطبيق بيانات الاستدلال البيولوجي الإضافية موجوداً على وثيقة السفر الإلكترونية المقررة آلياً.

يكون ترتيب مواد البيانات في السجل ثابتاً. ويجب على نظام التفتيش أن يبني محتوى السجل باستخدام مواد البيانات بالترتيب المحدد في الجدول.

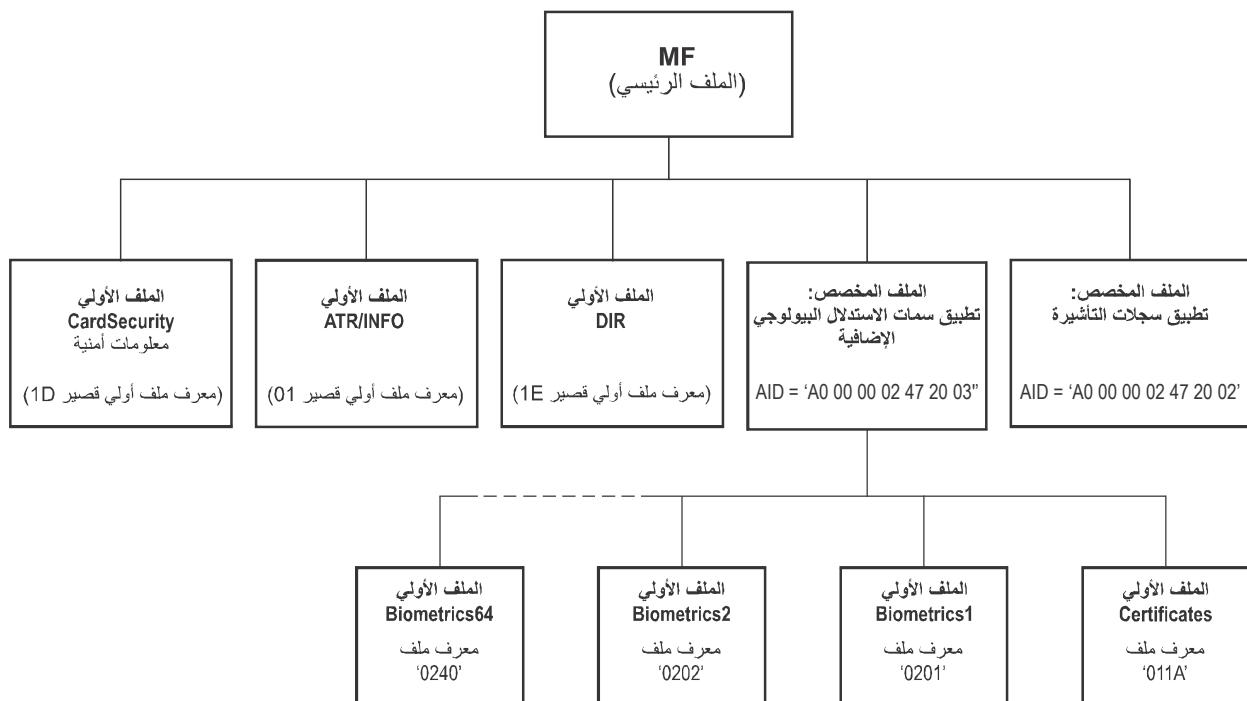
ويجب أن يحتوي كل سجل تأشيرات على توقيع رقمي (إشارة التحقق من الصحة) يتم حسابه في 'DO'71'، بما في ذلك Tag 71 والطول. وييتولد التوقيع بواسطة موقع LDS2-TS.

ويجب أن تخزن شهادات موقع LDS2-TS الالزامية للتحقق من توقيع سجل التأشيرات في مخزن الملف الأولي EF.Certificates الواقع تحت الملف المخصص لتطبيق سجلات التأشيرات.

ويجب أن يلحق كل سجل تأشيرات بالملف الأولي APPEND RECORD EF.VisaRecords باستخدام الأمر RECORD APPEND. ويجب عدم تغيير (تحديث) سجلات التأشيرات أو محوها. ويجب أن يكون العدد الأقصى للسجلات في الملف EF.VisaRecords الأولي ٢٥٤.

٣-٥ تطبيق بيانات الاستدلال البيولوجي الإضافية (مشروع)

يجوز لدولة أو منظمة الإصدار أن تنفذ تطبيق بيانات الاستدلال البيولوجي الإضافية، وإذا تم الاستناد إلى التطبيق الاختياري بيانات الاستدلال البيولوجي الإضافية أو نسبه إلى أي سجل تأشيرات، ينبغي القيام بما يلي.



الشكل ٦ – بنية تطبيق بيانات الاستدلال البيولوجي الإضافية

١-٣-٥ ملف التطبيق – الملف المخصص

يجب أن يتم اختيار تطبيق بيانات الاستدلال البيولوجي الإضافية باستخدام معرف التطبيق كاسم ملف مخصص محجوز . ويتألف معرف التطبيق من معرف التطبيق المسجل الذي تخصصه المنظمة الدولية لتوحيد المقاييس وفقاً لـ [ISO/IEC 7816-5] بليه امتداد لمعرف تطبيق الملكية (PIX) الخاص بتطبيق بيانات الاستدلال البيولوجي الإضافية :

- يكون معرف التطبيق المسجل 'A0 00 00 02 47 20 03' ؟
 - ويجب أن يستخدم تطبيق بيانات الاستدلال البيولوجي الإضافية '20 03'؛ PIX =
 - ويجب أن يكون معرف التطبيق الكامل لتطبيق بيانات الاستدلال البيولوجي الإضافية 03 20 47 00 00 00 02 .A0
- وإذا لم يمنح الإنفعال حقوق الوصول إلى أي بيانات في تطبيق البنية LDS2، يجب أن ترفض الدارة المتكاملة اختيار التطبيق.

٢-٣-٥ الملف الأولي EF.Certificates (الإلزامي)

تخزن شهادات موقع بيانات الاستدلال البيولوجي الإضافية في ملف أولي EF.Certificates داخل الملف المخصص للتطبيق وتكون بنيتها خطية ذات سجلات متغيرة الحجم. ويتوخى أن يستخدم نظام التفتيش هذه الشهادات لمواصلة التحقق من صحة التوقيع الرقمية خارج شبكة الإنترنت لكل سجل في الملف الأولي EF.Biometrics.

الجدول ٩١ — الملف الأولي EF.Certificates

File Name	EF.Certificates
File ID	'011A'
Short EF Identifier	'1A'
Select / FMM Access	PACE+TA (Additional Biometrics authorization byte 1 bit b1 (see Table 98)
Read Record/Search Record access	PACE+TA (Additional Biometrics authorization byte 1 bit b1 (see Table 98)
Append Record Access	PACE+TA (Additional Biometrics authorization byte 1 bit b2 (see Table 98)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

يحتوي سجل الشهادات على مادة بيانات الشهادة 509.X لموقع واحد لبيانات الاستدلال البيولوجي الإضافية. ويمكن الإشارة إلى سجل الشهادات بوحدة أو أكثر من الملف الأولي لبيانات الاستدلال البيولوجي الإضافية.

تكون بنية سجل الشهادات في تطبيق بيانات الاستدلال البيولوجي الإضافية مطابقة لبنية سجل الشهادات في تطبيق سجلات السفر المحدد في الجدول ٨٣.

تكتب سجلات الشهادات في الملف الأولي EF.Certificates الواقع تحت الملف المخصص لتطبيق بيانات الاستدلال البيولوجي الإضافية باستخدام الأمر APPEND RECORD. ويمكن قراءة سجلات الشهادات من الملف الأولي EF.Certificates باستخدام الأمر READ RECORD. ويجب عدم تحديث أو حذف سجلات الشهادات. ويجب أن يكون العدد الأقصى للسجلات في الملف EF.Certificates تحت الملف المخصص لتطبيق بيانات الاستدلال البيولوجي الإضافية ٢٥٤.

٥-٣-٣ الملف الأولي EF.Biometrics

يجب أن تخزن بيانات الاستدلال البيولوجي الإضافية تحت تطبيق بيانات الاستدلال البيولوجي الإضافية في ملفات أولية وأن تكون لها بنية شفافة وفقاً لـ [ISO/IEC 7816-4].

الجدول ٩٢ — الملف الأولي EF.Biometrics إلى EF.Biometrics64

File Name	EF.Biometrics1 through EF.Biometrics64
File ID	'0201' through '0240'
Short EF Identifier	N/A
Select / FMM / Read Access in Deactivated state	PACE+TA (Additional Biometrics authorization according to Table 98, bits b2, b4, b6, b8 of byte 2-17)
Write Access in Deactivated state	PACE+TA (Additional Biometrics authorization according to Table 98, bits b2, b4, b6, b8 of byte 2-17)
Activate Access in Deactivated state	PACE+TA (Additional Biometrics authorization according to Table 98, bits b2, b4, b6, b8 of byte 2-17)
Select / FMM / Read Access in Activated state	PACE+TA (Additional Biometrics authorization according to Table 98, bits b1, b3, b5, b7 of byte 2-17)
Write Access in Activated state	NEVER
Activate Access in Activated state	NEVER
Erase Access	NEVER
File structure	Transparent structure
Size	Variable

ويجب أن يحتوي كل ملف أولي لبيانات الاستدلال البيولوجي الإضافية على مادة البيانات 'DO'7F2E' في BER-TLV التي تحتوي على ثلاثة من مواد البيانات: مادة بيانات الاستدلال البيولوجي DO'5F2E' يليها مادة بيانات إشارة التحقق من الصحة (التوقيع) DO'5F37' ومادة البيانات DO'5F38' التي تحتوي على مرجع لشهادة موقع بيانات الاستدلال البيولوجي الإضافية الواردة في الملف EF.Certificates كما هو مبين في الجدول أدناه.

ويعود محتوى المادة 'DO'5F2E' إلى جهة إصدار بيانات الاستدلال البيولوجي الإضافية ويقع خارج نطاق هذه المعاصفة. ولا تدرج آلية إنشاء الملف الأولي لبيانات الاستدلال البيولوجي الإضافية ضمن نطاق هذه المعاصفة. وينبغي أن تتشكل جهة الإصدار مسبقاً عدداً من الملفات الأولية لبيانات الاستدلال البيولوجي الإضافية.

ملاحظة — تستخدم وسوم ما بين الصناعات المحددة في الجدول أدناه في سياق بنية البيانات المنطقية، وبالتالي لا يلزم خطة تخصيص وسوم متعارضة.

الجدول ٩٣ — شكل الملف الأولي EF.Biometrics

Tag	Tag	Content	MANDATORY/ OPTIONAL/ CONDITIONAL	Format	Example
'7F2E'		Biometric Data Template	M		'7F' '2E' Len {DO'5F2E' DO'5F37' DO'5F38'}
	'5F2E'	Additional Biometric data	M	V, B	'5F' '2E' Len {Biometric data}
	'5F37'	Authenticity token (Signature)	M	V (140), B	'5F' '37' Len {Signature}
	'5F38'	Reference (record number) to Additional Biometrics Signer certificate in Certificates Store	M	F (1) B	'01' ... '40'

B = Binary data, F = fixed-length field, V = variable-length field.

يكون ترتيب مواد البيانات في السجل ثابتاً.

ويجب أن يحتوي كل ملف أولي لبيانات الاستدلال البيولوجي الإضافية على توقيع رقمي (إشارة التحقق من الصحة) يتم حسابه في المادة 'DO'5F2E'، بما في ذلك الوسم والطول. ويتوارد التوقيع بواسطة موقع بيانات الاستدلال البيولوجي الإضافية.

وتخزن شهادة موقع لبيانات الاستدلال البيولوجي الإضافية الازمة للتحقق من توقيع بيانات الاستدلال البيولوجي الإضافية في مخزن منفصل للملف الأولي EF.Certificates الواقع تحت الملف المخصص لتطبيق بيانات الاستدلال البيولوجي الإضافية.

ويجب أن يكتب كل ملف أولي لبيانات الاستدلال البيولوجي الإضافية باستخدام الأمر UPDATE BINARU.

ويجب عدم تغيير (تحديث) بيانات الاستدلال البيولوجي الإضافية أو محوها. ويجب أن يكون العدد الأقصى للملفات الأولية لبيانات الاستدلال البيولوجي الإضافية ٦٤.

ونترد في الجدول ٩٤ جميع الأسماء والمعرفات والمعرفات القصيرة الممكنة للملف الأولي لبيانات الاستدلال البيولوجي الإضافية.

الجدول ٩٤ — معرفات الملف الأولى EF.Biometrics

EF name	EF identifier	Short EF identifier	EF name	EF identifier	Short EF identifier
EF.Biometrics1	'0201'	N/A	EF.Biometrics33	'0221'	N/A
EF.Biometrics2	'0202'	N/A	EF.Biometrics34	'0222'	N/A
EF.Biometrics3	'0203'	N/A	EF.Biometrics35	'0223'	N/A
EF.Biometrics4	'0204'	N/A	EF.Biometrics36	'0224'	N/A
EF.Biometrics5	'0205'	N/A	EF.Biometrics37	'0225'	N/A
EF.Biometrics6	'0206'	N/A	EF.Biometrics38	'0226'	N/A
EF.Biometrics7	'0207'	N/A	EF.Biometrics39	'0227'	N/A
EF.Biometrics8	'0208'	N/A	EF.Biometrics40	'0228'	N/A
EF.Biometrics9	'0209'	N/A	EF.Biometrics41	'0229'	N/A
EF.Biometrics10	'020A'	N/A	EF.Biometrics42	'022A'	N/A
EF.Biometrics11	'020B'	N/A	EF.Biometrics43	'022B'	N/A
EF.Biometrics12	'020C'	N/A	EF.Biometrics44	'022C'	N/A
EF.Biometrics13	'020D'	N/A	EF.Biometrics45	'022D'	N/A
EF.Biometrics14	'020E'	N/A	EF.Biometrics46	'022E'	N/A
EF.Biometrics15	'020F'	N/A	EF.Biometrics47	'022F'	N/A
EF.Biometrics16	'0210'	N/A	EF.Biometrics48	'0230'	N/A
EF.Biometrics17	'0211'	N/A	EF.Biometrics49	'0231'	N/A
EF.Biometrics18	'0212'	N/A	EF.Biometrics50	'0232'	N/A
EF.Biometrics19	'0213'	N/A	EF.Biometrics51	'0233'	N/A
EF.Biometrics20	'0214'	N/A	EF.Biometrics52	'0234'	N/A
EF.Biometrics21	'0215'	N/A	EF.Biometrics53	'0235'	N/A
EF.Biometrics22	'0216'	N/A	EF.Biometrics54	'0236'	N/A
EF.Biometrics23	'0217'	N/A	EF.Biometrics55	'0237'	N/A
EF.Biometrics24	'0218'	N/A	EF.Biometrics56	'0238'	N/A
EF.Biometrics25	'0219'	N/A	EF.Biometrics57	'0239'	N/A
EF.Biometrics26	'021A'	N/A	EF.Biometrics58	'023A'	N/A
EF.Biometrics27	'021B'	N/A	EF.Biometrics59	'023B'	N/A
EF.Biometrics28	'021C'	N/A	EF.Biometrics60	'023C'	N/A
EF.Biometrics29	'021D'	N/A	EF.Biometrics61	'023D'	N/A
EF.Biometrics30	'021E'	N/A	EF.Biometrics62	'023E'	N/A
EF.Biometrics31	'021F'	N/A	EF.Biometrics63	'023F'	N/A
EF.Biometrics32	'0220'	N/A	EF.Biometrics64	'0240'	N/A

٤-٤ شروط الاطلاع على ملفات تطبيقات LDS2 (مشروع)

٤-٤-١ أدوار ومستويات الترخيص الأصلية لتطبيقات LDS2

تحتوي شهادة السيرة الذاتية على نموذج الترخيص لصاحب الشهادة الذي يحدد دور صاحب الشهادة (نظام التفتيش، جهة التحقق من الوثيقة، سلطات التتحقق من الشهادات في البلد) ويحتوي على حقوق الاطلاع على مجموعة البيانات ٣ (DG3) أو مجموعة البيانات ٤ (DG\$) من التطبيق المطلوب لوثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS2 المطلوبة (لأسباب قديمة أو استخدامات وطنية أخرى).

ويشمل نموذج الترخيص لصاحب الشهادة سلسلة من مادتين:

أ) أحد معرفات المواد الذي يحدد نوع الوحدة الطرفية وشكل النموذج :[TR- 03110]

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

ب) مادة بيانات استنسابية ('53' tag) تحتوي على دور مرمز بالبنات وحقوق الاطلاع للقراءة فقط على صاحب الشهادة وفقاً للجدول التالي:

الجدول ٩٥ — نموذج الترخيص لصاحب الشهادة

	Description	Byte 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Role	CVCA	1	1						
	DV (domestic)	1	0						
	DV (foreign)	0	1						
	IS	0	0						
Read Access	RFU								
	RFU								
	RFU								
	RFU								
	DG4 (Iris)								1
	DG3 (Finger)								1

ملاحظة — يجب أن تتجاهل وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS2 قيمة البنات المحجوزة لاستعمالها في المستقبل (RFU) في الترخيص لصاحب الشهادة.

٤-٤-٢ مستويات ترخيص التطبيق (الإنزامي)

ترمز ترخيص صاحب الشهادة بالنسبة لكل تطبيق من تطبيقات LDS2 في امتدادات شهادة السيرة الذاتية (امتداد واحد لكل تطبيق). وامتداد الشهادة هو نموذج استنسابي ('73' tag) يشمل مادتي بيانات: معرف مادة الترخيص ('06' tag) لكل تطبيق محدد ومادة بيانات استنسابية ('53' tag) تحتوي على حقوق اطلاع مرمرة ثانية لصاحب الشهادة على تطبيق محدد.

ولتحديد الترخيص الفعال لصاحب الشهادة، تقوم رقاقة وثيقة السفر الإلكترونية المقرورة آلياً ذات البنية LDS2 بحساب العامل 'and' المنطقى الثنائي لحقوق الاطلاع الواردة في امتدادات الشهادة الخاصة بشهادة نظام التفتيش، وشهادة جهة التتحقق من الوثيقة وشهادة سلطات التتحقق من الشهادات في البلد.

وبالنسبة لتطبيق سجلات السفر ، تكون معرفات مادة الترخيص وعمليات تميز حقوق الاطلاع كما يلي:

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

الجدول ٩٦ — التراخيص الخاصة بتطبيق سجلات السفر

	Description	Byte 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Access rights	RFU								
	RFU								
	RFU								
	RFU								
	Append EF.Certificates							1	
	Read/Search>Select/FMM EF.Certificates							1	
	Append EF.EntryRecords/ExitRecords							1	
	Read/Search>Select/FMM EF.EntryRecords/ExitRecords								1

وبالنسبة لتطبيق سجلات التأشيرات، تكون معرفات مادة الترخيص وعمليات تميز حقوق الاطلاع كما يلي:

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

الجدول ٩٧ — التراخيص الخاصة بتطبيق سجلات التأشيرات

	Description	Byte 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Access rights	RFU								
	RFU								
	RFU								
	RFU								
	Append EF.Certificates							1	
	Read/Search>Select/FMM EF.Certificates							1	
	Append EF.VisaRecords							1	
	Read/Search>Select/FMM EF.VisaRecords								1

وبالنسبة لتطبيق بيانات الاستدلال البيولوجي الإضافية، تكون معرفات مادة الترخيص وعمليات تميز حقوق الاطلاع كما يلي:

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

الجدول ٩٨ — التراخيص الخاصة بتطبيق بيانات الاستدلال البيولوجي الإضافية

	Description	EF Identifier	Authorizations							
			b8	b7	b6	b5	b4	b3	b2	b1
Byte 1	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	Append EF.Certificates	'011A'								1
	Select/FMM/Read/Search EF.Certificates	'011A'								1
Byte 2	Select/FMM/Write/Activate/Read EF.Biometrics1 in Deactivated state	'0201'	1							
	Select/FMM/Read EF.Biometrics1 in Activated state	'0201'		1						
	Select/FMM/Write/Activate/Read EF.Biometrics2 in Deactivated state	'0202'			1					
	Select/FMM/Read EF.Biometrics2 in Activated state	'0202'				1				
	Select/FMM/Write/Activate/Read EF.Biometrics3 in Deactivated state	'0203'					1			
	Select/FMM/Read EF.Biometrics3 in Activated state	'0203'						1		
	Select/FMM/Write/Activate/Read EF.Biometrics4 in Deactivated state	'0204'							1	
	Select/FMM/Read EF.Biometrics4 in Activated state	'0204'								1
...										

Byte 17	Select/FMM/Write/Activate/Read EF.Biometrics61 in Deactivated state	'023D'	1							
	Select/FMM/Read EF.Biometrics61 in Activated state	'023D'		1						
	Select/FMM/Write/Activate/Read EF.Biometrics62 in Deactivated state	'023E'			1					
	Select/FMM/Read EF.Biometrics62 in Activated state	'023E'				1				
	Select/FMM/Write/Activate/Read EF.Biometrics63 in Deactivated state	'023F'					1			
	Select/FMM/Read EF.Biometrics63 in Activated state	'023F'						1		
	Select/FMM/Write/Activate/Read EF.Biometrics64 in Deactivated state	'0240'							1	
	Select/FMM/Read EF.Biometrics64 in Activated state	'0240'								1

الملاحظة ١ — يجب أن تتجاهل وثيقة السفر الإلكترونية المقررة آلياً ذات البنية LDS2 قيمة البتات الممحوza لاستعمالها في المستقبل (RFU) في التراخيص لصاحب الشهادة.

الملاحظة ٢ — يجب ألا تصدر دول أو منظمات الإصدار شهادات الوحدات الطرفية مع تراخيص لنظام التقىش بالكتابة/التفعيل إذا كان لديها فقط تراخيص لقراءة بيانات الاستدلال البيولوجي الإضافية.

٦ - معرفات المواد

١-٦ موجز معرفات المواد الخاصة بتطبيقات LDS1 و LDS2

الجدول ٩٩ — معرفات تطبيقات LDS1.7 و LDS1.8 و LDS2

Object Identifier	Value	Comments
id-icao	joint-iso-itu-t(2) international-organizations(23) icao(136)	ICAO OID
id-icao-mrtd	id-icao 1	eMRTD OID
id-icao-mrtd-security	id-icao-mrtd 1	
id-icao-ldsSecurityObject	id-icao-mrtd-security 1	LDS security object
id-icao-mrtd-security-cscaMasterList	id-icao-mrtd-security 2	CSCA master list
id-icao-mrtd-security-cscaMasterListSigningKey	id-icao-mrtd-security 3	
id-icao-mrtd-security-documentTypeList	id-icao-mrtd-security 4	document type list
id-icao-mrtd-security-aaProtocolObject	id-icao-mrtd-security 5	Active Authentication protocol
id-icao-mrtd-security-extensions	id-icao-mrtd-security 6	CSCA name change
id-icao-mrtd-security-extensions-nameChange	id-icao-mrtd-security-extensions 1	
id-icao-mrtd-security-extensions-documentTypeList	id-icao-mrtd-security-extensions 2	DS document type
id-icao-mrtd-security-DeviationList	id-icao-mrtd-security 7	Defect List Base OIDs
id-icao-mrtd-security-DeviationListSigningKey	id-icao-mrtd-security 8	
id-icao-lds2	id-icao-mrtd-security 9	LDS2 Object Identifiers
id-icao-lds2-travelRecords	id-icao-lds2 1	Travel Records application base OID
id-icao-lds2-travelRecords-application	id-icao-lds2-travelRecords 1	Travel Records AID
id-icao-lds2-travelRecords-access	id-icao-lds2-travelRecords 3	Authorization certificate extension
id-icao-lds2-visaRecords	id-icao-lds2 2	Visa Records application base OID
id-icao-lds2-visaRecords-application	id-icao-lds2-visaRecords 1	Visa Records AID
id-icao-lds2-visaRecords-access	id-icao-lds2-visaRecords 3	Authorization certificate extension
id-icao-lds2-additionalBiometrics	id-icao-lds2 3	Additional Biometrics base OID
id-icao-lds2-additionalBiometrics-application	id-icao-lds2-additionalBiometrics 1	Additional Biometrics AID
id-icao-lds2-additionalBiometrics-access	id-icao-lds2-additionalBiometrics 3	Authorization certificate extension
id-icao-lds2Signer	id-icao-lds2 8	LDS2 Signers Object Identifiers
id-icao-tsSigner	id-icao-lds2Signer 1	LDS2 Travel Stamp Signer certificate
id-icao-vSigner	id-icao-lds2Signer 2	LDS2 Visa Signer certificate
id-icao-bSigner	id-icao-lds2Signer 3	LDS2 Biometrics Signer certificate
id-icao-spoc	id-icao-mrtd-security 10	SPOC Object Identifiers
id-icao-spocClient	id-icao-spoc 1	Client
id-icao-spocServer	id-icao-spoc 2	Server

ASN.1 مواصفات الترميز - ٧

```

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}

```

LDS2 Travel Records application Object Identifiers

```

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}

```

LDS2 Visa Records application Object Identifiers

```

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}

```

LDS2 Additional Biometrics application Object Identifiers

```

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}

```

٨ — المراجع (معيارية)

- ISO/IEC 14443-1 ISO/IEC 14443-1:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics*
- 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*
- ISO/IEC 14443-3 ISO/IEC 14443-3:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and Anticollision*
- ISO/IEC 14443-4 ISO/IEC 14443-4:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*
- ISO/IEC 10373-6 ISO/IEC 10373-6:2016, *Identification cards — Test methods — Part 6: Proximity cards*
- 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*
- 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*
- ISO/IEC 7816-4 ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*
- ISO/IEC 7816-5 ISO/IEC 7816-5:2004, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*
- ISO/IEC 7816-6 ISO/IEC 7816-6:2016, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange (Defect report included)*
- ISO/IEC 7816-11 ISO/IEC 7816-11:2017, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*
- 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)*
- ISO/IEC 19794-4 ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data*
- ISO/IEC 19794-5 ISO/IEC 19794-5:2005, *Information technology — Biometric data interchange formats — Part 5: Face image data*
- ISO/IEC 19794-6 ISO/IEC 19794-6:2011, *Information technology — Biometric data interchange formats — Part 6: IRIS image data*
- ISO/IEC 10646 ISO/IEC 10646:2012, *Information technology — Universal Coded Character Set (UCS)*
- RFC 3369 Cryptographic Message Syntax 2002
- ISO/IEC 10918-1 ISO/IEC 10918-1:1994, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines*

ISO/IEC 15444	ISO/IEC 15444-n, <i>JPEG 2000 image coding system</i>
ISO/IEC 19785	ISO/IEC 19785-n, <i>Information technology — Common Biometric Exchange Formats Framework</i>
ISO/IEC 19795-6	ISO/IEC 19795-6:2012, <i>Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation</i>
ISO/IEC 39794-4	ISO/IEC 39794-4:2019, <i>Information technology — Extensible biometric data interchange formats — Part 4: Finger image data</i>
ISO/IEC 39794-5	ISO/IEC 39794-5:2019, <i>Information technology — Extensible biometric data interchange formats — Part 5: Face image data</i>
ISO/IEC 39794-6	ISO/IEC 39794-6:2021, <i>Information technology — Extensible biometric data interchange formats — Part 6: Iris image data</i>

المرفق (أ) بالجزء ١٠

أمثلة لتحديد مجالات بنية البيانات المنطقية (إعلامية)

يصف النص الإعلامي التالي أمثلة لتحديد مجالات بنية البيانات المنطقية (LDS v1.7) باستخدام تمثيل للاطلاع العشوائي على دائرة متكاملة لاتلامسية بوثيقة سفر الكترونية مقرئه آلياً.

أ- ١ الملف الأولي المشترك عناصر البيانات المشتركة

يبين المثال التالي تنفيذاً لنسخة بنية البيانات المنطقية 1.7 باستخدام نسخة الرموز الموحدة الموجودة 4.0.0 مع وجود مجموعات البيانات (tag 1 (tag '75'), 2 (tag '76'), and 12 (tag '6C') . '61').

لهذا المثال وجميع الأمثلة الأخرى، تطبع الوسوم بالبند **bold**، وتطبع الأطوال بالبند *italics* وتطبع القيم بالبند roman. أما الوسوم الستعشرية والأطوال والقيم فهي بين علامتي اقتباس ("xx").

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

سيُقرأ المثال في تمثيل ستعشرى كامل بوصفه:

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

سوف يتم ترميز نسخة افتراضية من بنية بيانات منطقية 15.99 بوصفها:

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

أو ستعشرية:

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

٢-١ ملف أولى. مجموعة البيانات ١ معلومات الجزء المقرؤء آلياً

١-٢-١ وثيقة السفر الإلكترونية المقرؤة آلياً من الحجم وثيقة سفر TD1

يبين أدناه مثال لمجموعة البيانات 1 باستخدام هذه المعلومات في وثيقة سفر الكترونية مقرئه آلياً ذات البنية LDS1 من الحجم TD1. وطول عنصر بيانات الجزء المقرئه آلياً هو ٩٠ بait (٥A').

‘61’ ‘5D’ ‘5F1F’ ‘5A’

I<NL>XI85935F8699999990<<<<<7208148F1108268NLD<<<<<<<<<4VAN<DER<STEEN<<MARI
ANNE<LOUISE

٢-٢-١ وثيقة السفر الإلكترونية المقرؤة آلياً من الحجم وثيقة سفر TD2

يبين أدناه مثال لمجموعة البيانات ١ باستخدام هذه المعلومات في وثيقة سفر الكترونية مقرورة آلياً ذات البنية LDS1 من الحجم TD2. وطول عنصر بيانات الجزء المقرورة آلياً هو ٧٢ بait (٤٨).

‘61’ ‘4B’ ‘5F1F’ ‘48’

٣-١ نماذج الاستدلال البيولوجي ؛ مجموعة البيانات ٤ إلى ملف أولى. مجموعة البيانات ٢ إلى ملف أولى.

تستخدم مجموعة البيانات ٢ إلى مجموعة البيانات ٤ الخيار المتداخل خارج البطاقة [ISO/IEC 7816-11] للحصول على إمكانية تخزين عدة نماذج استدلال بيولوجي من نوع منسجم مع إطار أشكال الملف المشترك لتبادل الاستدلالات البيولوجية (CBEFF)، [NISTR 6529a]. يحدد العنوان الفرعي للاستدلال البيولوجي نوع الاستدلال البيولوجي الموجود وسمة الاستدلال البيولوجي المحددة.

مثال: سمة استدلال بيولوجي وجهية موقعة واحدة ذات حزمة بيانات استدلال بيولوجي طولها ٦٤٢ بايت (٣١٦٢ بايت)، تم ترميزها باستخدام جهاز مزود بـ PID بواحدة ٠١ ٠٠ ٠١، باستخدام نوع الشكل '٠٤٠٠' المملوك لمقدم النموذج '٠٠٠A' تم القاطعه بتاريخ ٢٠٠٢/٣/١٥ (بدون التعويض عن التوقيت العالمي المنسق) وهو صالح من ٢٠٠٧/٣/٣١ لغاية ٢٠٠٢/٤/١. وٌستخدم النسخة ١.٠ من نموذج قالب الايكاو.

‘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’ ‘0001’
‘88’ ‘02’ ‘0008’
‘5F2E’ ‘823162’ ‘... 12 642 bytes of biometric data ...’

نماذج الصور المعروضة ٧ نماذج مجموعة البيانات ٥ إلى ملف أولى. مجموعة البيانات ٤-٤ ملف أولى.

ملاحظة — ملف أولي، واحد لكل مجموعة بيانات.

مثال: نموذج صورة مع بيانات صورة معروضة طولها ٢٠٠٠ بait. وطول النموذج هو ٢٠٠٨ بait (٠٧D8').

‘65’ ‘8207D8’

‘02’ ‘01’ 1
‘5F40’ ‘8207D0’ ‘....2 000 bytes of image data ...’

أ-٥ ملف أولي. مجموعة البيانات ١١ التفاصيل الشخصية الإضافية

يبين المثال التالي التفاصيل الشخصية التالية: الاسم الكامل (John J. Smith)، مكان الميلاد (Anytown, MN)، العنوان الدائم (123 Maple Rd, Anytown, MN 555-1212)، رقم الهاتف (612-555-1212)، والمهنة (وكيل سفر). وطول النموذج هو ٩٩ بايت (‘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

أ-٦ ملف أولي. مجموعة البيانات ١٦ الشخص الذي يتعين اخباره (الأشخاص الذين يتعين اخبارهم)

مثال من تدوينين: Charles R. Smith of Anytown, MN and Mary J. Brown of Ocean Breeze, CA. وطول النموذج ١٦٢ بايت (‘A2’).

‘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

المرفق (ب) بالجزء ١٠

الدائرة المتكاملة اللاتلامسية في جواز سفر إلكتروني مقروء آلياً (علامية)

ب-١ حجم الهوائي وفئة جواز السفر الإلكتروني المقروء آلياً

حجم الهوائي هو حسب تقدير دولة الإصدار. وباستثناء حجم الهوائي، يجب أن يفي كل من وثيقة السفر الإلكترونية المقروءة آلياً ذات البنية LDS1 وLDS2 بجميع الاختبارات المحددة في [2-2] ISO/IEC 18745 مع تطبيق مواصفات الدرجة الأولى.

وهو موصى به من أجل وثائق السفر الإلكترونية المقروءة آلياً ليكون أيضاً ممثلاً لمواصفات الدرجة الأولى. ولا يوجد وضع إلزامي للدائرة المتكاملة، التي يجوز وضعها في موقع جزافي. ويترك موقع الهوائي اللا تلامسي وفقاً لتقدير دولة الإصدار طالما هي في أحد المواقع التالية:

- صفحة البيانات — دائرة متكاملة وهوائي داخل بنية صفحة بيانات يشكلان صفحة داخلية؛
- وسط كتيب — وضع الدائرة المتكاملة وهوائيها بين الصفحات الوسطى لكتاب؛
- غلاف — الوضع داخل بنية أو بناء الغلاف؛
- صفحة منفصلة مخيطة — إدماج الدائرة المتكاملة وهوائيها داخل صفحة منفصلة، التي يجوز أن تكون في شكل بطاقة بلاستيكية بحجم ID3، مخيطة داخل الكتاب خلال صنعه؛ أو وضعه داخل بنية أو بناء الغلاف الخلفية.
- الغلاف الخلفي —

ب-٢ التمهيد والاقتراع

وثيقة السفر الإلكترونية المقروءة آلياً التي يؤتى بها إلى مجال مغناطيسي قدره 1.5 A/m حسبما يقاس في [2-2] ISO/IEC 18745 يجب أن تستجيب لأي REQ/WUP ملائم لنوعها بعد مجال مغناطيسي غير مضمون بقيمة 10 Am . ويوصى بها بقوة لتكون قادرة على الاستجابة لأي ملائم لنوعه بعد مجال مغناطيسي غير مضمون سعة الموجة البالغة 5 Am .

ب-٣ مضاد الاصطدام والطراز

يجوز لوثيقة السفر الإلكترونية المقروءة آلياً إما أن تعلن الامتثال للطراز A أو للطراز B حسبما تم تعريفهما في [2-2] ISO/IEC 14443. ويجب ألا تغير طرازها ما لم يعاد تشكيل طرازها بواسطة نظام التقتيش المرتبط بوثيقة السفر الإلكترونية المقروءة آلياً.

ب-٤ معدلات البتات الإلزامية

يجب أن توفر وثيقة السفر الإلكترونية المقروءة آلياً على الأقل معدلات البتات التالية، حسبما هي معرفة في [2-2] ISO/IEC 14443، إلزامياً:
١٦ كيلوبت/ثانية و٤٤ كيلوبت/ثانية في كلا الاتجاهين بين وثيقة السفر الإلكترونية المقروءة آلياً ووثيقة السفر مثيلتها المرتبطة بنظام التقتيش.

معدل البت 212 kbit/s، وكل معدلات البتات من 848 kbit/s إلى 6.78 Mbit/s لكلا الاتجاهين، ومن s 10.17 Mbit/s إلى 27.12 Mbit/s من نظام التقنيش المرتبط بوثيقة السفر الإلكترونية المقرورة آلياً إلى وثيقة السفر المذكورة، حسبما هي معرفة في [ISO/IEC 14443-2]، هي اختيارية.

بـ ٥ الاضطراب الكهرومغناطيسي (EMD)

دعم الاضطراب الكهرومغناطيسي ليس إلزامياً.

ملاحظة — خاصية EMD تعزز متانة الاتصال اللا تلامسي بين وثيقة السفر الإلكترونية المقرورة آلياً ونظام التقنيش المرتبط بها ضد الاضطراب الكهرومغناطيسي الذي تولده وثيقة السفر الإلكترونية المقرورة آلياً. وقد يسبب استهلاك وثيقة السفر الإلكترونية المقرورة آلياً الديناميكي للتيار خلال تنفيذ أحد الأوامر تأثير تعديل شحنة جزافية (قد لا تكون مقاومة بشكل بحث) على المجال المغناطيسي. وفي بعض الحالات، قد يخطئ نظام التقنيش المرتبط بوثيقة السفر الإلكترونية المقرورة آلياً في تفسير اضطراب كهرومغناطيسي بوصفه بيانات أرسلتها وثيقة السفر المذكورة، وقد يؤثر هذا سلبياً على الاستقبال الصحيح لاستجابة وثيقة السفر المذكورة.

بـ ٦ الدعم (الاختياري) لتبادل بارامترات إضافية

يجوز لوثيقة السفر الإلكترونية المقرورة آلياً أن تدعم تبادل بارامترات إضافية كما هي معرفة في [ISO/IEC 14443-4] بغية التفاوض بشأن معدلات بتات أعلى من 106 kbit/s. ويجوز أيضاً استخدام البارامترات الإضافية نفسها للتفاوض بشأن أطر ذات تصويب لخطأ على النحو المحدد في [ISO/IEC 14443-4].

بـ ٧ الحماية

يوصى بعدم حماية أي صفحة من صفحات وثيقة السفر الإلكترونية المقرورة آلياً.

بـ ٨ المعرف الفريد (UID) (الموصى به) ومعرف بطاقة الدائرة المتكاملة القريبة (PUPU)

يجوز أن توفر وثيقة السفر الإلكترونية المقرورة آلياً UID/PUPU بالصدفة أو ثابت على النحو المعرف في [ISO/IEC 14443-3].
ويوصى باستخدام UID/PUPU بالصدفة لتحسين خصوصية حامل وثيقة السفر الإلكترونية المقرورة آلياً وتقليل إمكان التتبع.

بـ ٩ نطاق تردد الرنين (الموصى به)

لا يوجد شرط على تردد رنين طالبي وثيقة السفر الإلكترونية المقرورة آلياً. ويجوز لطالبي الوثيقة الحدّ من تردد الرنين بالخلاف إلى نطاق معين لزيادة التشغيل المتبادل.

بـ ١٠ أحجام الأطر (الموصى به)

يجوز أن تدعم وثيقة السفر الإلكترونية المقرورة آلياً أحجام أطر حتى إلى ٤ كيلوبايت وفقاً لـ [ISO/IEC 14443]. غير أنه، من الموصى به دعم أحجام الأطر التي لا تقل عن ١ كيلوبايت. وإذا دعمت الأطر لأحجام أعلى من ١ كيلوبايت، يوصى باستخدام أطر ذات تصحيح للخطأ على النحو المعرف في [ISO/IEC 14443-4].

ملاحظة — استخدام حجم إطار أعلى سيُخفض بقدر كبير الوقت الإجمالي لمعالجة تطبيق وثيقة سفر إلكترونية مقرورة آلياً.

بـ- ١١ العدد الصحيح لوقت الانتظار الإطاري (الموصى به) (FWI) وطلب كتلة S لتمديد وقت الانتظار [S(WTX)]

يوصى لوثيقة السفر الإلكترونية المقرورة آلياً أن تقوم بضبط قيمة العدد الصحيح لوقت الانتظار الإطاري تقل عن أو تساوي ١١ من أجل تحسين الأداء. ويوصى باستخدام أوامر (WTX) لتمديد وقت الانتظار بما لا يزيد على ١٠.

في حالة تعدد طلبات (WTX) أرسلتها وثيقة السفر الإلكترونية المقرورة آلياً، فإن وقت المعالجة الإجمالي لكتلة الحالية I يوصى بأن لا يتجاوز ٥ ثوان.

ملاحظة — القيم الأدنى كما يوصى بها هنا لوقت الانتظار الإطاري تخفض ضياع الوقت في أحطان الإرسال جوهرياً، في حين أن (WTX) هي الوسيلة المثالية لتوفير مزيد من الوقت عند الاحتياج إليه.

المرفق (ج) بالجزء ١٠

نظم التفتيش (إعلامية)

ج-١ حجم التشغيل وموقع الاختبار

أي نظام تفتيش مرتبط بوثيقة سفر إلكترونية مقرورة آلياً يجب أن يكون له حجم تشغيل وفقاً لواحد من أنواع نظام التفتيش المحددة في [ISO/IEC 18745-2]. وحجم التشغيل هو الحجم الذي تكون فيه جميع متطلبات هذا التقرير مستوفاة.

ملاحظة — موقع الاختبار لكل نوع من نظم التفتيش تلقى مزيداً من التحديد في [ISO/IEC 18745-2] فيما يتعلق (بالأداة) صفر مليمتر من وثيقة السفر الإلكترونية المقرورة آلياً المرتبطة بنظام التفتيش.

ج-٢ شكل الموجة المعين ومتطلبات الترددات اللاسلكية

أشكال الموجات للمجال المغناطيسي البديل المستخدمة للاتصال يجب أن تكون ممثلة تماماً لـ [ISO/IEC 14443] بصفة عامة، ولا توجد استثناءات أو اختلافات عن المعيار الأساسي، إلا بالنسبة لقوة المجال.

بالنسبة لوثيقة السفر الإلكترونية المقرورة آلياً المرتبطة بنظم تفتيش من النوع ١ و٢ و٣، يوصى أن تكون على الأقل 2 A/m بجميع المواقع للدرجة الأولى. وبالنسبة لوثيقة السفر الإلكترونية المقرورة آلياً ونظم التفتيش المرتبطة بها من النوع M، يجب أن تكون قوة المجال 1.5 A/m على الأقل بجميع الأوضاع بالنسبة للدرجة الأولى.

ملاحظة — قد يكون من المنشود بالنسبة لوثائق السفر الإلكترونية المقرورة آلياً الاتصال أيضاً بنظم التفتيش اللاسلكية الأخرى والأجهزة النقالة، مثل أجهزة الهاتف الذكية NFC تستخدم 1.5 A/m .

ج-٣ تسلسلات الاقتراع ووقت الكشف عن وثائق السفر الإلكترونية المقرورة آلياً

يجب أن يوفر نظام التفتيش المرتبط بتسلسل اقتراع وثيقة السفر الإلكترونية المقرورة آلياً 10 ms لناقل غير متغير قبل أي REQ/WUPA أو REQB/WUPB.

من أجل الاكتشاف والمعالجة السريعين، فإن نظام تفتيش وثيقة السفر الإلكترونية المقرورة آلياً:

- يجب أن يقترب لنوع A والنوع B مع حدوث مساو لطلبات لجميع الأنواع؛

بالنسبة لأنواع نظم التفتيش ١ و٢ و٣، ينبغي أن تحدث إعادة وضع بين أي REQ/WUP من نفس النوع؛

يجب أن يضمن أمر اقتراع واحد على الأقل لكل من النوع A والنوع B في غضون 150 ms من أجل أن تكون وثيقة سفر إلكترونية مقرورة آلياً موجودة بحجم التشغيل الإلزامي الأدنى وفقاً لـ [ISO/IEC 18745-2] بأي موقع.

يجوز لنظام تفتيش وثيقة السفر الإلكترونية المقرورة آلياً الاقتراع للمنتجات اللاسلكية من أي نوع آخر من التضمين على الناقل لـ 13.56 MHz طالما لم تبيت جميع المتطلبات أعلاه.

ملاحظة — الناقل غير المضمن لـ 10 ms مطلوب منه كشف جميع وثائق السفر الإلكترونية المقرورة آلياً في الخانة ويستند إلى مواصفات سابقة.

ج-٤ معدلات البت الإلزامية

يجب على نظام التفتيش المرتبط بوثيقة السفر الإلكترونية المقرورة آلياً أن يوفر إلزاماً 106 kbit/s و 424 kbit/s في كلا الاتجاهين من وثيقة السفر الإلكترونية المقرورة آلياً إلى نظام التفتيش المرتبط بمثيلتها والعكس بالعكس.

معدل البت 212 kbit/s، وكل معدلات البتات من 848 kbit/s إلى 6.78 Mbit/s لكلا الاتجاهين، ومن 10.17 Mbit/s إلى 27.12 Mbit/s من نظام التفتيش المرتبط بوثيقة السفر الإلكترونية المقرورة آلياً إلى وثيقة السفر المذكورة، حسبما هي معرفة في [ISO/IEC 14443-2]، هي اختيارية.

ج-٥ الاضطراب الكهرومغناطيسي (EMD)

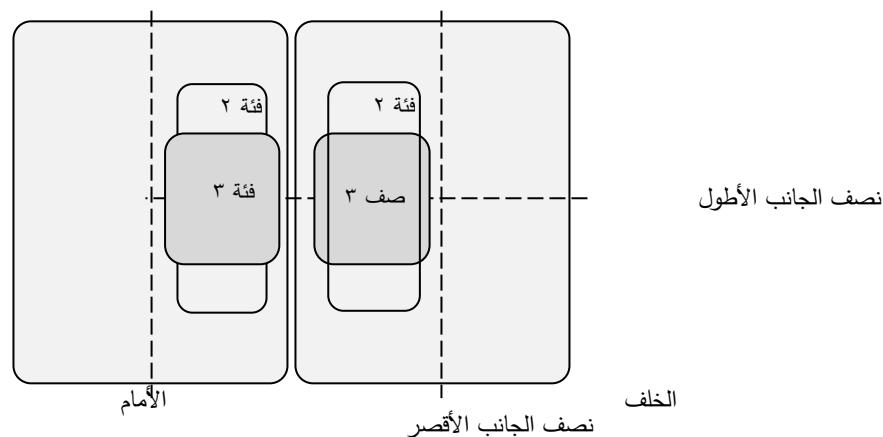
دعم الاضطراب الكهرومغناطيسي ليس إلزامياً.

ملاحظة — سمة الاضطراب الكهرومغناطيسي تعزز صلابة الاتصال اللا تلامسي بين وثيقة السفر الإلكترونية المقرورة آلياً والوثيقة المماثلة لها المرتبطة بنظام التفتيش المشترك ضد الإزعاج الكهرومغناطيسي المتولد عن وثيقة السفر الإلكترونية المقرورة آلياً. والوثيقة المذكورة تيارها الديناميكي خلال تنفيذ أحد الأوامر قد يسبب تأثير الشحنة الاستبدادية التضمينية (الذي قد لا يكون مقاوماً فقط) على المجال المغناطيسي. وفي بعض الحالات، فإن نظام التفتيش المشترك للنظام مع وثيقة السفر الإلكترونية المقرورة آلياً قد يسيء تفسير الاضطراب الكهرومغناطيسي بأنه بيانات أرسلتها الوثيقة المذكورة وهذا قد يؤثر سلبياً على الاستقبال السليم لاستجابة الوثيقة المذكورة.

ج-٦ فئات الهوائي المدعومة

سيقوم نظام التفتيش المشترك من النوع ١ والنوع ٢ لوثائق السفر الإلكترونية المقرورة آلياً بدعم فئة واحدة على الأقل لوثائق السفر المذكورة بالحجم اللازم للتشغيل.

وتعتبر الفئتان الثانية والثالثة إلزاميتين في ISO/IEC 14443، ولكن اختياريتين في نظام التفتيش على وثائق السفر الإلكترونية المقرورة آلياً.



الشكل ج-١ الموضع الإلزامية في كل سطح ID-3 تم فيه قراءة هوائي الفئة ٢ والفئة ٣ بواسطة نظام التفتيش المرتبط بوثائق السفر الإلكترونية المقرورة آلياً من النوع ١ و ٢.

ج- ٧ (اختياري) أحجام الأطر وتصويب الخطأ

يجوز اختيارياً أن يدعم نظام التفتيش المرتبط بوثيقة السفر الإلكترونية المقرورة آلياً جميع أحجام الأطر حتى ٤ كيلوبايت حسب ما هو معرف في [ISO/IEC 14443-3]. ويوصى باستخدام أطر مصوّبة الخطأ حسب ما هو معرف في [ISO/IEC 14443-3] لجميع أحجام الأطر المدعومة الأعلى من ١ كيلوبايت.

ملاحظة — من أجل نظم التفتيش المرتبطة بوثيقة السفر الإلكترونية المقرورة آلياً من النوع M، ليس من المتصور حالياً أحجام أطر أعلى من ٢٥٦ بايت.

ج- ٨ الدعم (الاختياري) للفئات الإضافية

جمعت وثائق السفر الإلكترونية المقرورة آلياً شمل نظم التفتيش ذات الصلة من جميع الأنواع ويجوز أن تدعم بالإضافة إلى ذلك الفئة ٤ والفئة ٥ والفئة ٦ لتكون ذات تشغيل متبادل، مثلاً، مع الأدوات المتحركة التي فيها ازدواج أقل مع نظام التفتيش المرتبط بوثيقة السفر الإلكترونية المقرورة آلياً المرتبطة بنظام تفتيش لغة سلك هوائي.

ج- ٩ معدلات البتات (اختيارية)

يوصى بأن نظام التفتيش المرتبط بوثيقة السفر الإلكترونية المقرورة آلياً يعمل مع درجات تتراوح من ١٠ إلى ٥٠ درجة مئوية.

ج- ١٠ الدعم (الموصى به) لوثائق السفر الإلكترونية المقرورة آلياً المتعددة والبطاقات أو الأشياء الأخرى أو المضييفين المتعددين

يوصى بشدة بتصميم نظام التفتيش لتداول الأيدي أكثر من وثيقة سفر إلكترونية مقرورة آلياً واحدة وأي بطاقة أخرى أو شيء آخر ممثل لـ [ISO/IEC 14443].

يجوز تطبيق إحدى القواعد أو المجموعات التالية أو توليفة، ضمن أخرى:

- تطبيق خوارزميات كاملة مضادة للاصطدام أم معرفة في [ISO/IEC 14443-3]؛
- تحقق من دعم [ISO/IEC 14443-4] وتخلص من جميع البطاقات غير الداعمة؛
- تتحقق من تطبيق لوثيقة سفر إلكترونية مقرورة آلياً؛
- استخدام معرف البطاقة (CID) وعنوان المذكرة (NAD).

ملاحظة — يجوز أيضاً استخدام NAD للأدوات المتحركة ذات المضييفين المتعددين.

ج- ١١ أحجام الأطر (الموصى بها)

أشركت وثيقة السفر الإلكترونية المقرورة آلياً إطار الدعم System MAY بأحجام تعلو إلى ٤ كيلوبايت وفقاً لـ [ISO/IEC 14443-3]. غير أنه يوصى بدعم أحجام أطر لا تقل عن ١ كيلوبايت أو أعلى، ويوصى باستخدام أطر ذات تصويب للخطأ كما عُرف في [ISO/IEC 14443-4].

يوصى بأداء أي فصل للحملة من طبقة التطبيق إلى داخل أدنى عدد من الأطر ذات الطول الفعال لحجم الأطر المنسوب الأقصى باستثناء الإطار الأخير.

ج- ١٢ استرداد الخطأ (الموصى به)

عقب نقل خطأ أو وثيقة سفر إلكترونية مقرورة آلياً غير مستجيبة، يوصى من أجل نظام التفتيش المرتبط بوثيقة السفر الإلكترونية المقرورة آلياً بإرسال كتلة R تحتوي على شعار استلام سلبي (NAK) R وفقاً للقاعدة ٤ من نظام التفتيش [ISO/IEC 14443-4].

ج- ١٣ الكشف عن الخطأ (الموصى به) وآلية الاسترداد

عند استخدام معدلات البت الاختيارية وكذلك أحجام الأطر الاختيارية الأعلى من ٢٥٦ بايت، في حالة عدد أعلى من المعتاد لأخطاء الإرسال، يوصى بخفض معدل البت وحجم إطار فعال.

المرفق (د) بالجزء ١٠

المادة الأمنية للوثيقة (EF.SOD) الإصدار V0 البنية LDS V1.7 (قديمة) (إعلامية)

لا تتضمن المادة الأمنية للوثيقة (EF.SOD) الإصدار V0 البنية LDS V1.7 معلومات عن بنية البيانات المنطقية وإصدار الرموز الموحدة .UNICODE

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

د- ١ البيانات الموقعة من أجل الوثيقة SOD V0

تنفذ المادة الأمنية للوثيقة كنوع من البيانات الموقعة SignedData، على النحو المحدد في [RFC 3369]. ويجب أن تنتج جميع المواد الأمنية على شكل قاعدة ترميز مميزة (DER) للحفاظ على سلامة التوقيع في داخلها.

m = MANDATORY — the field SHALL be present. — الملاحظة ١

x = do not use — the field SHOULD NOT be populated. — الملاحظة ٢

o = optional — the field MAY be present. — الملاحظة ٣

c = choice — the field content is a choice from alternatives. — الملاحظة ٤

الجدول د-١ — نوع البيانات الموقعة من أجل الوثيقة SO_D V0

Value		Comments
SignedData		
Version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
Certificates	o	States may choose to include the Document Signer Certificate (C _{Ds}) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States provide only 1 signerInfo within this field.
SignerInfo	m	
Version	m	The value of this field is dictated by the sid field. See RFC3369 Doc 9303-12 for rules regarding this field.
Sid	m	
issuerAndSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving States may choose to ignore them.

د-٢ وصف الترميز ASN.1 لبنية البيانات المنطقية للمادة الأمنية لـ الوثيقة SO_D V0

```

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

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

-- Imports from 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) };

-- Constants

ub-DataGroups INTEGER ::= 16

```

```
-- Object Identifiers
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}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {v0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

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

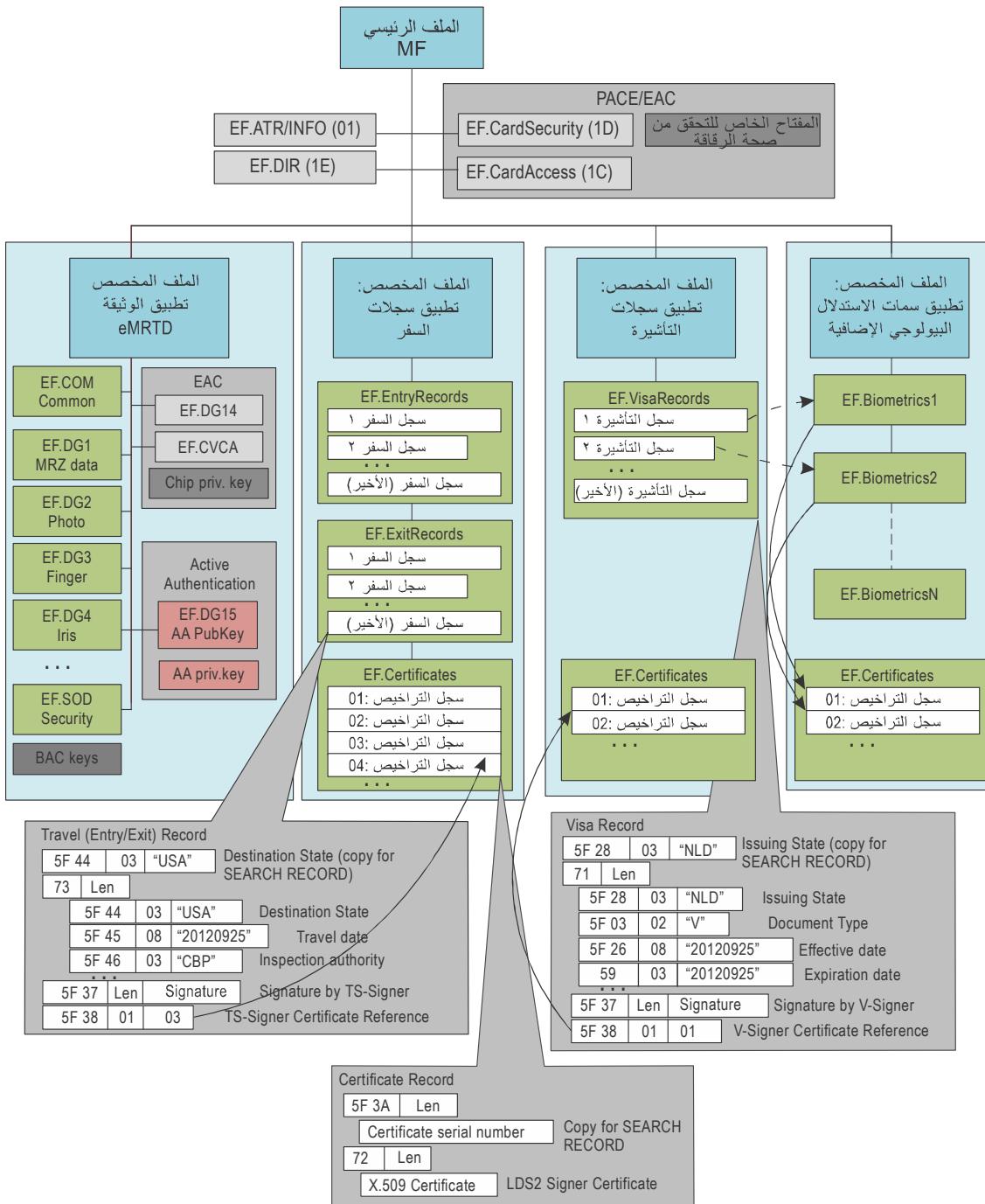
DataGroupHash ::= SEQUENCE {
    dataGroupNumber      DataGroupNumber,
    dataGroupHashValue   OCTET STRING }
DataGroupNumber ::= INTEGER {
    dataGroup1          (1),
    dataGroup2          (2),
    dataGroup3          (3),
    dataGroup4          (4),
    dataGroup5          (5),
    dataGroup6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

END
```

الملاحظة ١ — يحتوي الحقل `dataGroupHashValue` على البصمة الرقمية المحسوبة على كامل محتويات الملف الأولى لمجموعة البيانات، المحددة بواسطة `.dataGroupNumber`.

الملاحظة ٢ — يجب أن تغفل المعرفات `DigestAlgorithmIdentifiers` ببارامترات `NULL`، بينما يجب أن يتضمن المعرف `SignatureAlgorithmIdentifier` (كما هو محدد في `RFC 3447`) `NULL` كبارامتر في حال عدم وجود بارامترات، حتى عند استخدام خوارزميات `SHA2` وفقاً لـ `RFC 5754`. ويجب على نظام التقنيش أن يقبل الحقل `DigestAlgorithmIdentifiers` بكل الشرطية، أي البارامترات الغائبة وبارامترات `NULL`.

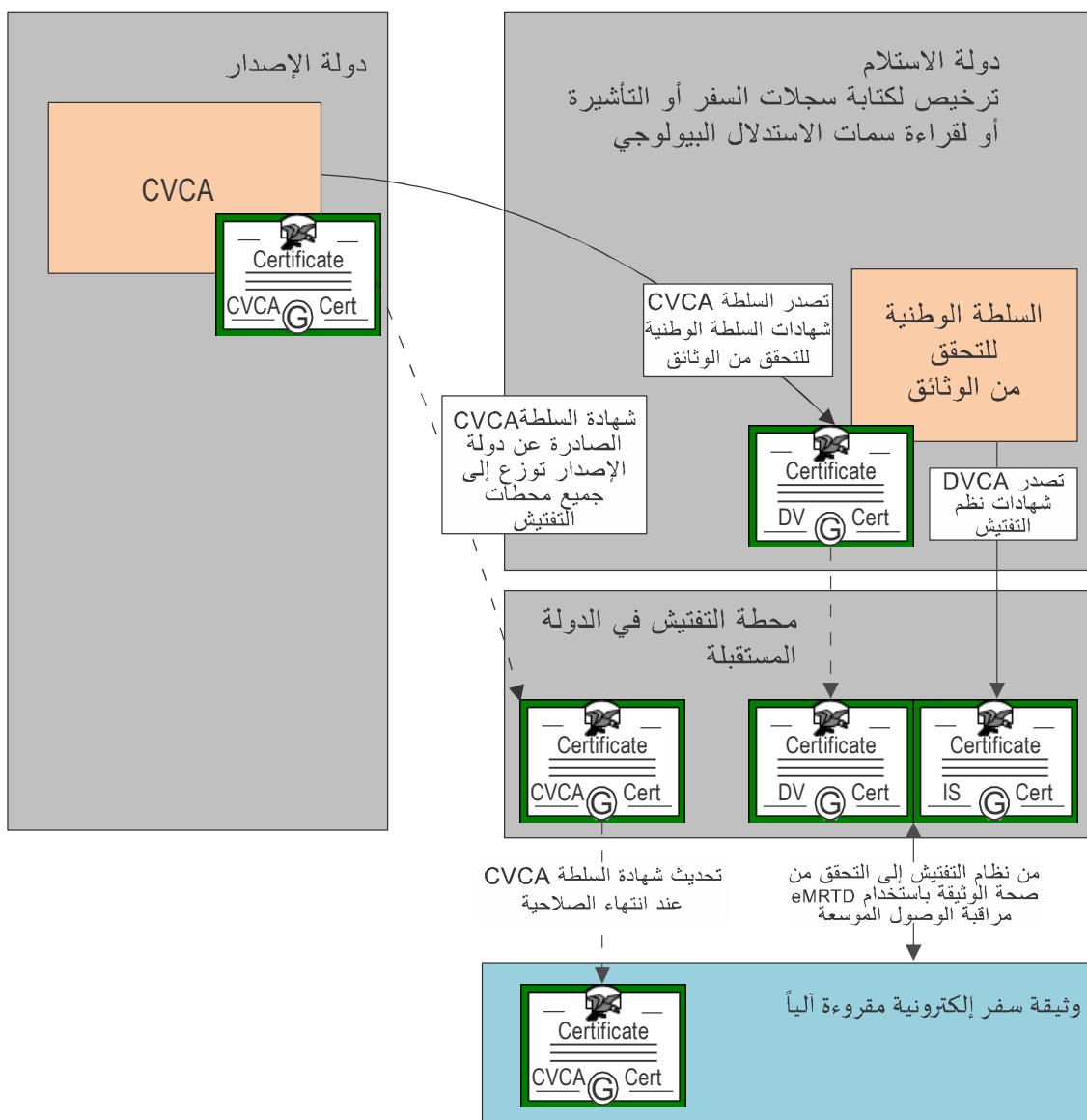
المرفق (هـ) بالجزء ١٠ موجز بنى الملفات (إعلامية)



الشكل ٥-١ — موجز بنى الملفات

المرفق (و) بالجزء ١٠

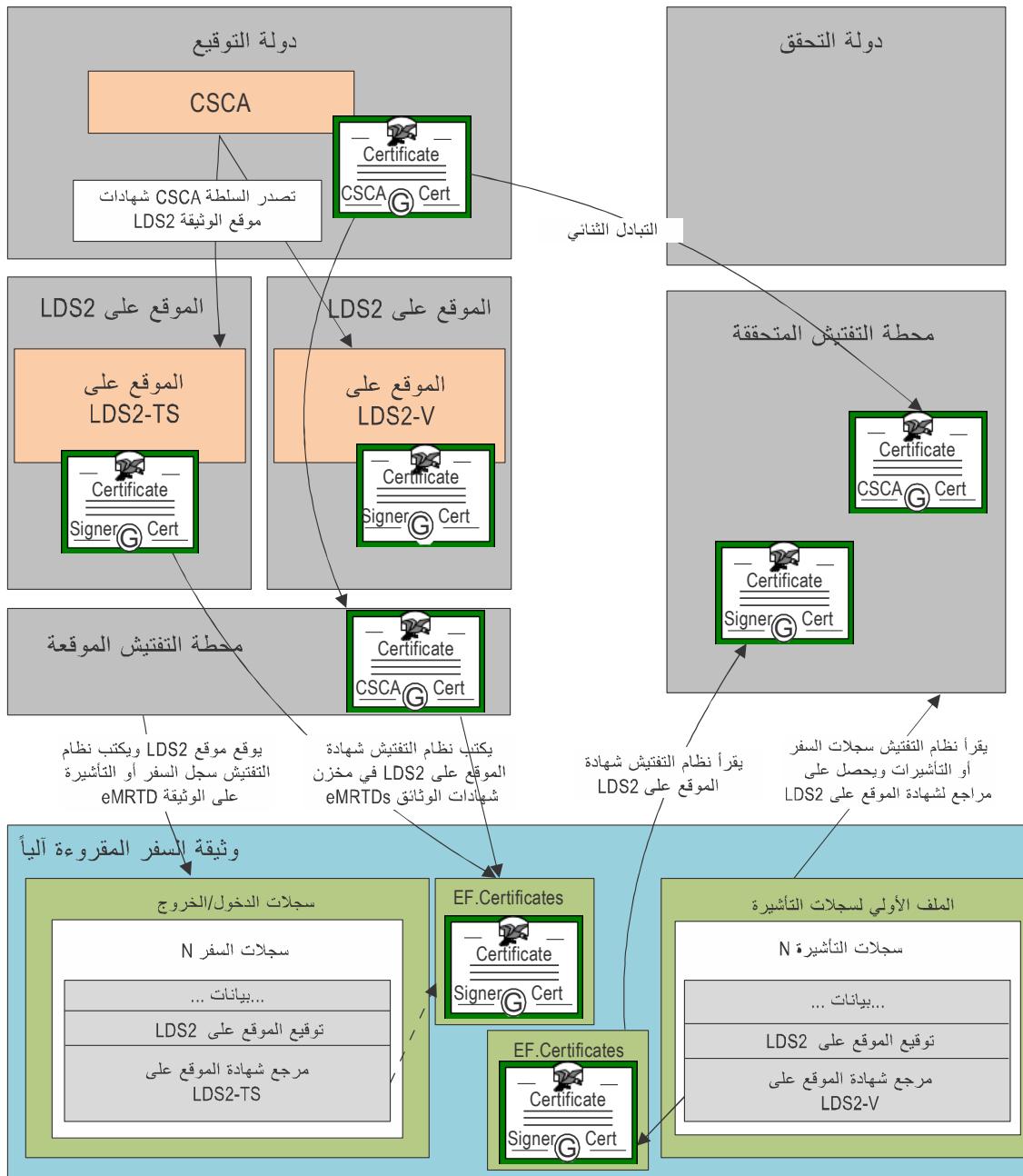
موجز أدوات بنية البيانات المنطقية (إعلامية)



الشكل و-١ — موجز أدوات بنية البيانات المنطقية

المرفق (ز) بالجزء ١٠

موجز التوقيع الرقمية لبنية البيانات المنطقية (إعلامية)



الشكل ز - ١ — موجز التوقيع الرقمية لبنيّة البيانات المنطقية

المرفق (ح) بالجزء ١٠

مثال لقراءة سجل السفر (علامية)

ح-١ الأمر FMM لاستعادة عدد سجلات الدخول

CLA	INS	P1	P2	Lc	Data	Le
‘80’	‘5E’	‘01’	‘04’	‘04’	‘51 02 01 01’	‘00’

CLA: Proprietary class / no secure messaging

INS:FMM

P1: ‘01’ — EF identifier in command data field

P2: ‘04’ — Return existing number of records in a record EF

Lc: ‘04’

Data: DO ‘51’ containing Entry Records EF identifier ‘0101’

Le: ‘00’ (Short Le)

الاستجابة: مادة الوثيقة FILE AND MEMORY MANAGEMENT التي تمثل عدد السجلات في الملف الأولي.

Data	SW1-SW2
‘83 01 FD’ ‘7F78 03’	‘90 00’

تحتوي مادة الوثيقة في بيانات الاستجابة على رقم السجل الأخير الذي يمكن استخدامه في الأمر READ RECORD التالي (P1).

وعلى سبيل المثال، يعني رقم السجل الأخير ‘00’ عدم وجود سجلات في هذا الملف، وتعني الاستجابة ‘FD’ أن عدد السجلات هو ٢٥٣ (العدد الأقصى للسجلات هو ٢٥٤).

ح-٢ الأمر READ RECORD لاستعادة سجل السفر الأخير من القائمة المستعادة

يمكن استخدام الأمر التالي لاستعادة سجل واحد باستخدام رقم السجل المستعاد بواسطة الأمر FMM.

CLA	INS	P1	P2	Le
‘00’	‘B2’	‘FD’	‘04’	‘00 00 00’

CLA: Interindustry class / no secure messaging

INS:READ RECORD(S)

P1: Record number from the previous command’s response

P2: Record number in P1 / read record P1

Le: ‘00 00 00’ (Extended Le), read entire record

الاستجابة: عدد السجلات هو ٢٥٣ (‘FD’).

Data	SW1-SW2
‘5F44’ ‘Len’ <Data> ‘73’ ‘Len’ <Data> ‘5F37’ ‘Len’ <Data> ‘5F38’ ‘Len’ <Data>	‘90 00’

ح-٣ الأمر READ RECORD لاستعادة سجلي السفر الآخرين من القائمة المستعادة

يمكن استخدام الأمر التالي لاستعادة سجلين (أو أكثر) من القائمة المستعادة بواسطة الأمر FMM. تسهم قراءة عدة سجلات في تبادل وحدة بيانات بروتوكول التطبيق في تحسين الأداء. ويمكن تحديد عدد السجلات التي يمكن استعادتها بواسطة أمر واحد من معلومات الطول الموسع في الملف الأولي EF.ATR/INFO والحجم الأقصى لسجل السفر.

CLA	INS	P1	P2	Le
‘00’	‘B2’	‘FC’	‘05’	‘00 00 00’

CLA: Interindustry class / no secure messaging

INS:READ RECORD(S)

P1: Decremented Record number from the FMM response ($253 - 1 = 252 = \text{‘FC’}$)

P2: Record number in P1 / read all records from P1 up to the last record

Le: ‘00 00 00’ (Extended Le), read entire record

الاستجابة: تمت استعادة السجلين الآخرين ٢٥٢ (‘FC’) و ٢٥٣ (‘FD’).

Data	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’

المرفق (ط) بالجزء ١٠

مثال لتفتيش السجلات بحسب الدولة (إعلامية)

ط-١ الأمر SERCH RECORD للبحث عن سجل (سجلات) السفر بحسب دولة المقصد

CLA	INS	P1	P2	Lc	Data	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: Interindustry class / no secure messaging

INS:SEARCH RECORD(S)

P1: record number = '00'

P2: Search through multiple EFs

Lc: length of command data field

Data: DO'7F76' - Record handling DO

DO'51' - File reference DO (EF.EntryRecords short identifier '01')

DO'A1' - Search configuration template

DO'80' - Search configuration parameter: '00' (search all records)

DO'B0' - Search window template

DO'02' - Offset: '03'

DO'02' - Number of bytes: '03'

DO'A3' - Search string template

DO'B1' - Search string DO

DO'81' - Search string (country code): xx xx xx

Le: '00' (Short Le)

Response: DO'7F76' – Record handling DO

DO'51' - EF.EntryRecords short identifier '01'

One or more DO'02' containing matching record numbers

Data	SW1-SW2
'7F 76' 'Len' '51 01 01' '02 01 03' '02 01 04'	'90 00'

المرفق (ي) بالجزء ١٠

مثال لكتابة سجل وشهادة السفر (إعلامية)

ي- ١ الأمر **SERCH RECORD** للبحث عن شهادات الملفات الأولية بحسب رقم الشهادة التسلسلي

يتتحقق IS مما إذا كانت شهادة موقع LDS2-TS مع الأرقام التسلسلي المطلوبة موجودة في الملف الأولي EF.Certificates. ويمكن استخدام الأمر التالي للبحث عن الشهادة:

CLA	INS	P1	P2	Lc	Data	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: Interindustry class / no secure messaging INS: SEARCH RECORD(S)

P1: record number = '00'

P2: Search through multiple EFs

Lc: length of command data field

Data: DO'7F76' - Record handling DO

DO'51' - File reference DO (EF.Certificates short identifier '1A')

DO'A1' - Search configuration template

DO'80' - Search configuration parameter: '30' (stop if record found)

DO'B0' - Search window template

DO'02' - Offset: '03'

DO'02' - Number of bytes: Search string size

DO'A3' - Search string template

DO'B1' - Search string DO

DO'81' - Search concatenation of country code and certificate

serial number: xx xx .. xx xx

Le: '00' (Short Le)

Response: DO'7F76' - Record handling DO
 DO'51' - EF.Certificates short identifier '1A'
 DO'02' - contains matching record number

Data	SW1-SW2
'7F 76 06' '51 01 1A' '02 01 01'	'90 00'

أو رمز التنبية '62.82' إذا لم يتطابق أي سجل مع معايير البحث:

SW1-SW2
'62 82'

إذا تطابق أحد سجلات EF.Certificate مع معايير البحث، يمكن لنظام التقتيش أن يستخدم بشكل اختياري رقم السجل المستعاد ('01)، في الأمر READ RECORD للتحقق مما إذا كانت الشهادة صحيحة. وإذا لم يتطابق أي سجل من سجلات EF.Certificate مع معايير البحث، يكتب نظام التقتيش الشهادة في الملف الأولي APPEND RECORD باستخدام الأمر EF.Certificates في القسم ي-٢ ويكتب أخيراً سجل الدخول باستخدام الأمر APPEND RECORD في القسم ي-٣.

ي-٢ الأمر APPEND RECORD لكتابة الشهادة

يكتب نظام التقتيش شهادة موقع LDS2-TS في الملف الأولي EF.Certificates. ويمكن استخدام الأمر التالي لكتابة الشهادة:

CLA	INS	P1	P2	Lc	Data	Le
'00'	'E2'	'00'	'D0'	'00' XX XX	'5F3A' 'Len' {certificate serial number} '72' 'Len' {X.509 certificate}'	Absent

CLA: Interindustry class / no secure messaging

INS:APPEND RECORD

P1: '00' (any other value is invalid)

P2: short EF identifier (= '1A')

Lc: Record length (Extended Lc)

Data: Record data

الاستجابة: رمز نجاح أو خطأ

SW1-SW2
'90 00'

ي- ٣ الأمر APPEND RECORD لكتابة سجل السفر

ينشئ نظام التفتيش سجل سفر باستخدام إشارة إلى شهادة موقع LDS2-TS ويكتبه في الملف الأولى EF.EntryRECORDS باستخدام الأمر التالي:

CLA	INS	P1	P2	Lc	Data	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: Interindustry class / no secure messaging

INS:APPEND RECORD

P1: '00' (any other value is invalid)

P2: short EF identifier (= '01')

Lc: Record length (Extended Lc)

Data: Record dat

الاستجابة: رمز نجاح أو خطأ

SW1-SW2
'90 00'

— انتهى —

ISBN 978-92-9275-581-2

A standard linear barcode representing the ISBN number 978-92-9275-581-2.

9 789292 755812