ايكاو

Doc 9303

وثائق السفر المقروءة آلياً

الطبعة الثامنة – ٢٠٢١

الجزء ١١: آليات أمن وثائق السفر المقروءة آلياً

اعتمدتها الأمينة العامة ونُشرت بموجب سلطتها

منظمة الطيران المدني الدولي

ايكاو

Doc 9303

وثائق السفر المقروءة آلياً

الطبعة الثامنة – ٢٠٢١

الجزء ١١: آليات أمن وثائق السفر المقروءة آلياً

اعتمدتها الأمينة العامة ونُشرت بموجب سلطتها

منظمة الطيران المدني الدولي

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

تتوافر التنزيلات والمعلومات الإضافية على الرابط www.icao.int/Security/FAL/TRIP

الوثيقة Doc 9303، وثائق السفر المقروءة آليا
الجزء ١١ — آليات أمن وثائق السفر المقروءة آلياً
Order No.: 9303P11
ISBN 978-92-9265-553-2 (النسخة المطبوعة)
ISBN 978-92-9275-580-5 (النسخة الإلكترونية)

التعديلات

تعلن التعديلات في ملاحق كتالوج المنتجات والخدمات. ويمكن الاطلاع على الكتالوج وملاحقه في موقع الإيكاو على الإنترنت www.icao.int. والجدول أدناه مخصص لتسجيل مثل هذه التعديلات.

سجل التعديلات والتصويبات

التعديلات		
الرقم	التاريخ	أدخل بواسطة
١	٢٠٢٤/٦/١٤	

التصويبات		
الرقم	التاريخ	أدخل بواسطة

جدول المحتويات

١ – المجال

يوفّر الجزء الحادي عشر من الوثيقة Doc 9303 مواصفات فنية لتمكين الدول والمورّدين من تطبيق السمات الأمنية المشفّرة لوثائق السفر الإلكترونية المقروءة آلياً ("eMRTDs") التي توفّر دائرة متكاملة لاتلامسية (IC). وتحدَّد البروتوكولات المشفّرة من أجل ما يلي:

- منع استخلاص البيانات من الدائرة المتكاملة اللاتلامسية.
- منع التنصت على الاتصالات بين الدائرة المتكاملة اللاتلامسية والجهاز القارئ.
- توفير التحقق من صحة البيانات المخزّنة على الدائرة المتكاملة اللاتلامسية بالاستناد إلى البنية الأساسية للمفاتيح العامة (PKI) الموصوفة في الجزء ١٢.
- توفير التحقق من صحة الدائرة المتكاملة اللاتلامسية ذاتها.

وتتضمن الطبعة الثامنة من الوثيقة Doc 9303 مواصفات التطبيقات الاختيارية لسجلات السفر وسجلات التأشيرات وسمات الاستدلال البيولوجي الإضافية (المعروفة باسم تطبيقات البنية LDS2) بوصفها امتداداً اختيارياً لوثيقة السفر الإلكترونية المقروءة آلياً. ويشمل هذا الجزء من الوثيقة Doc 9303 البروتوكولات الضرورية لمراقبة الوصول الموسّعة من أجل الحماية من كتابة وقراءة البيانات المتعلقة بتطبيقات LDS2 الخاصة بها. كما يمكن استخدام بروتوكولات مراقبة الاطلاع هذه لحماية سمات الاستدلال البيولوجي الثانوية في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً.

التحقق من صحة بيانات المخزّنة على الدائرة المتكاملة اللاتلامسية هو السمة الأمنية الأساسية للتمكين من استخدام الدائرة المتكاملة للتفتيش اليدوي و/أو الآلي. ولذلك فإن هذه السمة **مطلوبة**.

تنفيذ بروتوكول لمنع استخلاص البيانات المخزّنة على الدائرة المتكاملة اللاتلامسية ولمنع التنصت على الاتصالات بين الدائرة المتكاملة والمحطة الطرفية **مطلوب**.

تنفيذ البروتوكولات الأخرى **اختياري**، يسمح لدولة أو منظمة الاصدار بأن تقرر بشأن المجموعة اللازمة من السمات الأمنية وفقاً للوائح/للطلبات الوطنية.

يجب أن يُقرأ الجزء الحادي عشر بالاقتران مع الأجزاء التالية من الوثيقة Doc 9303:

- الجزء ١ — *المقدمة*؛
- الجزء ١٠ — *بنية البيانات المنطقية لخزن بيانات الاستدلال البيولوجي وغيرها في دائرة متكاملة لاتلامسية*؛
- الجزء ١٢ — *البنية الأساسية للمفاتيح العامة لوثائق السفر المقروءة آلياً*.

٢ – الافتراضات والحواشي

من المفترض أن قارئ هذه الوثيقة معتاد على المفاهيم والآليات التي يوفرها تشفير المفتاح العام وبنى المفاتيح العامة.

في حين أن استخدام تقنيات تشفير المفتاح العام يضيف بعض التعقيد إلى تنفيذ وثائق السفر الإلكترونية المقروءة آلياً، فإن مثل هذه التقنيات تضيف قيمة من حيث أنها ستزوّد نقاط مراقبة الحدود على الخط الأمامي بتدبير إضافي لتقرير صحة وثيقة السفر الإلكترونية المقروءة آلياً. ويُفترض أن استخدام مثل هذه التقنية ليس هو التدبير الوحيد لتحديد الصحة و**لا ينبغي** الاعتماد عليها كعامل وحيد للتحديد.

وفي حالة تعذر استخدام البيانات من الدائرة المتكاملة اللاتلامسية، مثلاً كنتيجة لإلغاء شهادة أو التحقق من توقيع باطل أو إذا تُركت الدائرة المتكاملة اللاتلامسية غفلاً عمداً (انظر القسم ٤-٥-٤ من الوثيقة Doc 9303-10)، لا تُبطل وثيقة السفر الإلكترونية المقروءة آلياً بالضرورة. وفي مثل هذه الحالات فإنه **يجوز** لأي دولة مستقبِلة أن تعتمد على السمات الأمنية لوثيقة أخرى لأغراض التحقق من الصحة.

٢-١ متطلبات الرقاقات والوحدات الطرفية لوثيقة السفر الإلكترونية المقروءة آلياً

يحدد هذا الجزء من الوثيقة Doc 9303 متطلبات تطبيقات رقاقات وثيقة السفر الإلكترونية المقروءة آلياً (أو، بشكل مكافئ، الدائرة المتكاملة ووحداتها الطرفية (أو نظم التفتيش). وفي حين أن رقاقات وثيقة السفر الإلكترونية المقروءة آلياً يجب أن تمتثل لتلك المتطلبات وفقاً للمصطلحات الموصوفة في الوثيقة Doc 9303-1، فإن تفسير المتطلبات للوحدات الطرفية بأنها إرشادات، أي أن التشغيل المتبادل لرقاقة وثيقة السفر الإلكترونية المقروءة آلياً ووحدتها الطرفية يُضمنان فقط إذا امتثلت الوحدة الطرفية لتلك المتطلبات، وبخلاف ذلك فإن التفاعل مع رقاقة وثيقة السفر الإلكترونية المقروءة آلياً إما سيفشل أو سيكون سلوك رقاقة وثيقة السفر الإلكترونية المقروءة آلياً غير محدد. وبصفة عامة، ليس من الضروري أن تستوفي رقاقة وثيقة السفر الإلكترونية المقروءة آلياً المتطلبات المتصلة بالوحدات الطرفية مع لم يتأثر أمن رقاقة وثيقة السفر الإلكترونية المقروءة آلياً بصورة مباشرة.

٢-٢ الحواشي

تُستخدم الحواشي التالية للدلالة على أوليات علم الشفرة بطريقة مستقلة عن الخوارزميات:

- Encryption of clear text S with symmetric key K: **E**(K, S);
- Decryption of cipher text C with symmetric key K: **D**(K, C);
- The operation for computing a hash over a message *m* is denoted by **H***(m)*.
- Computing a Message Authentication Code with symmetric key K over message M: **MAC**(K,M);
- Key agreement based on asymmetric key pairs (SK, PK) and (SK', PK') and domain parameters D: **KA**(SK,PK',D) / **KA**(SK',PK,D);
- Key derivation from a shared secret S: **KDF**(S);
- Signing a message *m* with private key SK_{IFD} is denoted by *s* = **Sign***(SK_{IFD}, m)*;
- Verifying the resulting signature *s* with public key PK_{IFD} and message *m*: **Verify***(PK_{IFD}, s, m*).
- Computing a compressed representation of a public key *PK*: **Comp***(PK).*

٣- تأمين البيانات الإلكترونية

إلى جانب التحقق السلبي من الصحة بواسطة التوقيعات الرقمية ومراقبة الوصول إلى الرقاقة، **يجوز** لدول أو منظمات الإصدار اختيار إجراء أمني اضافي، باستخدام مزيد من الطرائق المتشعّبة لتأمين الدائرة المتكاملة اللاتلامسية وبياناتها.

ينطوي الاطلاع على أي وثيقة سفر إلكترونية مقروءة آلياً من الخطوات التالية:

١) الاطلاع على الدائرة المتكاملة اللاتلامسية لوثيقة السفر الإلكترونية المقروءة آلياً (القسم ٤)

٢) التحقق من صحة البيانات (القسم ٥)

٣) التحقق من صحة الرقاقة (القسم ٦)

٤) آليات مراقبة الاطلاع الاضافي (القسم ٧)

٥) قراءة البيانات (انظر الوثيقة Doc 9303-10).

تتوافر بروتوكولات مختلفة للخطوات المختلفة. والتشكيلة الدقيقة لأي وثيقة سفر إلكترونية مقروءة آلياً تقوم باختيارها دولة أو منظمة الاصدار. ويمكن الجمع بشكل مناسب بين الخيارات المعطاة في الجدول ١ لتحقيق أمن إضافي وفقاً لمتطلبات جهات الاصدار.

وترد في المرفق (ي) إجراءات التفتيش المتعلقة بمختلف تشكيلات وثائق السفر الإلكترونية المقروءة آلياً.

الجدول ١ — تأمين البيانات الإلكترونية (موجز)

Method	***Contactless IC***	***Inspection System***	***Benefits***	***Note***
BASELINE SECURITY METHOD				
Passive Authentication (Section 5.1)	m	m	Proves that the contents of the SO_D and the LDS are authentic and not changed.	Does not prevent an exact copy or IC substitution. Does not prevent unauthorized access. Does not prevent skimming.
ADVANCED SECURITY METHODS				
Comparison of conventional MRZ(OCR-B) and IC-based MRZ(LDS)	n/a	o	Proves that contactless IC's content and physical eMRTD belong together.	Adds (minor) complexity. Does not prevent an exact copy of contactless IC and conventional document.
Active Authentication (Section 6.1)	o	o	Prevents copying the SO_D and proves that it has been read from the authentic contactless IC. Proves that the contactless IC has not been substituted.	Does not prevent unauthorized access. Adds complexity. Chip Authentication is REQUIRED for LDS2.
Chip Authentication (Section 6.2)	o/c	o		

Method	*Contactless IC*	*Inspection System*	*Benefits*	*Note*
Basic Access Control (BAC) (Section 4.3)	c (see also 4.1)	m (see also 4.1)	Prevents skimming and misuse. Prevents eavesdropping on the communications between eMRTD and inspection system (when used to set up encrypted session channel).	Does not prevent an exact copy or IC substitution (requires also copying of the conventional document). Adds complexity. At least one of BAC or PACE SHALL be supported by the eMRTD. PACE is REQUIRED for LDS2. PACE offers better protection against eavesdropping than BAC. See also Appendix A.
Password Authenticated Connection Establishment (PACE) (Section 4.4)	r/c (see also 4.1)	m (see also 4.1)		
Terminal Authentication (Section 7.1)	o/c	o	Prevents unauthorized access to sensitive data. Prevents skimming of sensitive data.	Requires additional key management. Does not prevent an exact copy or IC substitution (requires also copying of the conventional document). Adds complexity. Terminal Authentication is REQUIRED for LDS2.
Data Encryption (Section 7.2)	o	o	Secures additional biometrics. Does not require processor-ICs.	Requires complex decryption key management. Does not prevent an exact copy or IC substitution. Adds complexity.
m = REQUIRED, r = RECOMMENDED, o = OPTIONAL, c = CONDITIONAL, n/a = not applicable.				

ملاحظة — انظر القسم ٤ للاطلاع على تفاصيل التشكيلات الممتثلة للدوائر المتكاملة اللاتلامسية فيما يتعلق بتنفيذ مراقبة الاطلاع الأساسي وفتح الاتصال بكلمة سر مصدّق عليها.

لا يؤثر تنفيذ الطرق الأمنية المتقدمة كما هي مدرجة في الجدول ١ على الامتثال لأحكام الإيكاو.

٤- الوصول إلى الدائرة المتكاملة اللاتلامسية

إن إضافة دائرة متكاملة لاتلامسية بدون مراقبة الاطلاع على وثيقة سفر إلكترونية مقروءة آلياً تتيح إمكانيتين جديدتين للهجوم:

- البيانات المخزنة في الدائرة المتكاملة اللاتلامسية يمكن قراءتها الكترونياً بدون الترخيص بهذه القراءة للوثيقة (الاستخلاص)؛
- الاتصال غير المشفّر بين دائرة متكاملة لاتلامسية وجهاز قارئ يمكن التنصت عليه من مسافة عدة أمتار.

بينما توجد تدابير مادية ممكنة مضادة للاستخلاص (مثل التغطية باستخدام شبكة معدنية في غلاف دفتر جواز السفر)، فإن هذه لا تعالج التنصت. ولذلك، من المفهوم أن دول أو منظمات الاصدار **يجب** أن تختار تنفيذ آلية لمراقبة الاطلاع على الرقاقة، أي آلية مراقبة اضطلاع تتطلب في الواقع أن يعرف صاحب وثيقة السفر الإلكترونية المقروءة آلياً أن البيانات المخزنة في الدائرة المتكاملة اللاتلامسية تتم قراءتها بطريقة مأمونة. وهذه الآلية لمراقبة الاطلاع على الرقاقة تمنع الاستخلاص وكذلك التنصت.

أي دائرة متكاملة لاتلامسية محمية بآلية لمراقبة الاطلاع على الرقاقة تمنع الاطلاع على محتوياتها ما لم يكن بمقدور نظام التفتيش أن يثبت أنه مرخّص له بولوج الدائرة المتكاملة اللاتلامسية. وهذا الاثبات يُعطى في بروتوكول تشفير، حيث يثبت نظام التفتيش معرفة المعلومات المستمدة من الوثيقة المادية.

يجب أن يكون نظام التفتيش مزوّداً بهذه المعلومات قبل أن يتمكن من قراءة الدائرة المتكاملة اللاتلامسية. ويتعين استرجاع المعلومات ضوئياً/بصرياً من وثيقة السفر الإلكترونية المقروءة آلياً (مثلاً من الجزء المقروء آلياً). و**يجب** أيضاً أن يتمكن مفتش من إدخال هذه المعلومات يدوياً في نظام التفتيش في حالة عدم إمكان القراءة الآلية للمعلومات.

على افتراض أن المعلومات من الوثيقة المادية لا يمكن الحصول عليها من وثيقة غير منظورة (مثلاً بالنظر إلى أن المعلومات مستمدة من الجزء المقروء آلياً المقروء ضوئياً)، من المقبول أن وثيقة السفر الإلكترونية المقروءة آلياً قد سُلِّمت للتفتيش مع العلم بذلك. وبسبب تشفير القناة، فإن التنصت أثناء الاتصال قد يتطلب جهداً كبيراً.

يعرّف هذا القسم آليتين لمراقبة ولوج الرقاقة:

- مراقبة الاطلاع الأساسي (القسم ٤–٣)، التي تستند حصراً إلى تشفير تماثلي؛
- الاتصال باستخدام كلمة سرّ مصدّق عليها (PACE، القسم ٤–٤)، الذي يستعمل التشفير اللاتماثلي لتوفير مفاتيح دورات انتروبيا أعلى.

انظر أيضاً المرفق (أ) للحصول على معلومات إضافية بشأن قوة مفاتيح الدورات.

٤–١ التشكيلات الممتثلة

تمتثل التشكيلات التالية لهذه المواصفة الفنية:

- رقاقات وثائق السفر الإلكترونية المقروءة آلياً التي تتيح مراقبة الاطلاع الأساسي فقط؛
- رقاقات وثائق السفر الإلكترونية المقروءة آلياً التي تنفّذ فتح الاتصال بكلمة سر مصدّق عليها ومراقبة الاطلاع الأساسي؛
- رقاقات وثائق السفر الإلكترونية المقروءة آلياً التي تتيح فتح الاتصال بكلمة سر مصدّق عليها فقط.

والتأمين الذي تتيحه مراقبة الاطلاع الأساسي مقيد بتصميم البروتوكول، على النحو الذي يرد شرحه في المرفق (أ). ومن المتوقع أن تؤدي زيادة قوة أجهزة الكمبيوتر مع مرور السنوات إلى التمكّن من شن هجمات بواسطة مراقبة الاطلاع الأساسي والتي سيكون من الممكن إجراؤها بشكل ناجح حال توافر قدر معقول من الإمكانيات المالية وفي ظل مهلة زمنية معقولة. لذلك، تم الاتفاق على التحول تدريجياً من مراقبة الاطلاع الأساسي إلى فتح اتصال بكلمة سر مصدّق عليها.

وحُددت فترة الانتقال التالية:

- من ٢٠٢٧/١/١، يجب أن تنفذ رقاقات وثائق السفر الإلكترونية المقروءة آلياً فتح الاتصال بكلمة سر مصدّق عليها، أما تلك التي تتيح مراقبة الاطلاع الأساسي فقط فسيجري إيقاف العمل بها. وجميع رقاقات وثائق السفر الإلكترونية المقروءة آلياً التي تتيح مراقبة الاطلاع الأساسي فقط والصادرة قبل ٢٠٢٧/١/١ ستظل متوافقة طوال فترة صلاحيتها.
- اعتباراً من ٢٠٢٨/١/١، سيجري إيقاف العمل بنظام مراقبة الاطلاع الأساسي، وسيلزم أن تنفذ رقاقات وثائق السفر الإلكترونية المقروءة آلياً فقط فتح الاتصال بكلمة سر مصدّق عليها. وجميع رقاقات وثائق السفر الإلكترونية المقروءة آلياً التي تنفّذ فتح الاتصال بكلمة سر مصدّق عليها ومراقبة الاطلاع الأساسي الصادرة قبل ٢٠٢٨/١/١ ستظل متوافقة طوال فترة صلاحيتها. و**يجب** أن تيسر نظم التفتيش الممتثلة جميع تشكيلات وثيقة السفر الإلكترونية المقروءة آلياً الممتثلة. وإذا كانت وثيقة سفر إلكترونية مقروءة آلياً تيسّر كلاً من فتح الاتصال بكلمة سر مصدّق عليها والمراقبة الأساسية للوصول، **يجب** أن يستخدم نظام التفتيش إما المراقبة الأساسية للاطلاع وإما فتح الاتصال بكلمة سر مصدّق عليها لكن ليس كلاً منهما في نفس الدورة.

*الملاحظة ١ — أتاحت الإصدارات السابقة للوثيقة Doc 9303 لرقاقات وثائق السفر الإلكترونية المقروءة آلياً تنفيذ عدم وجود مراقبة أساسية للاطلاع (وثائق السفر الإلكترونية المقروءة آلياً البسيطة). وهذا أمر مشجوب في الطبعة الإنجليزية. ومع ذلك، **يجب** على نظم التفتيش الممتثلة أن تدعم وثائق السفر الإلكترونية المقروءة آلياً من دون مراقبة أساسية للاطلاع.*

ملاحظة ٢ — للوصول إلى تطبيقات LDS2، يجب أن تتطلب الدائرة المتكاملة تنفيذ فتح الاتصال بكلمة سر مصدّق عليها

٤-٢ إجراءات الاطلاع على الرقاقة

تتكوّن إجراءات الاطلاع على الرقاقة للتحقق من صحة نظام التفتيش من الخطوات التالية.

1. **Read EF.CardAccess** **(REQUIRED)**

If PACE is supported by the eMRTD, the eMRTD chip MUST provide the parameters to be used for PACE in the file EF.CardAccess.

If EF.CardAccess is available, the inspection system SHALL read the file EF.CardAccess (cf. Section 9.2.11) to determine the parameters (i.e. symmetric ciphers, key agreement algorithms, domain parameters, and mappings) supported by the eMRTD chip. The inspection system may select any of those paramet

If the file EF.CardAccess is not available or does not contain parameters for PACE, the inspection system SHOULD try to read the eMRTD with Basic Access Control (skip to Step 4)

2. **Read EF.DIR** **(OPTIONAL)**

The Inspection System MAY read EF.DIR (if present) to retrieve a list of applications present on the eMRTD chip.

3. **PACE** **(CONDITIONAL)**

This step is RECOMMENDED if PACE is supported by the eMRTD chip. This step is REQUIRED if access to LDS2 applications is intended.

- The inspection system SHOULD derive the key K_π from the MRZ. It MAY use the CAN instead of the MRZ if the CAN is known to the inspection system.
- The eMRTD chip SHALL accept the MRZ as passwords for PACE. It MAY additionally accept the CAN instead of the MRZ.
- The inspection system and the eMRTD chip mutually authenticate using K_π and derive session keys KS_{Enc} and KS_{MAC}. The PACE protocol as described in Section 4.4 SHALL be used.

If successful, the eMRTD chip performs the following:

- It SHALL start Secure Messaging.
- It SHALL grant access to less sensitive data (e.g. EF.DG1, EF.DG2, EF.DG14, EF.DG15, etc. of the eMRTD Application, and the Document Security Object. For the definition of "sensitive data" see Doc 9303-1).
- It SHALL restrict access rights to require Secure Messaging.

The inspection system MUST verify the authenticity of the contents of EF.CardAccess using EF.DG14 or EF.CardSecurity, and of EF.DIR (if present and read) using EF.CardSecurity.

Note.— If no LDS2 application is present on the eMRTD chip, EF.CardSecurity may not contain a secured copy of EF.DIR.

4. **Basic Access Control** **(CONDITIONAL)**

This step is REQUIRED if Chip Access Control is enforced by the eMRTD chip and PACE has not been used. If PACE was successfully performed or if the eMRTD does not enforce Chip Access Control, this step is skipped.

The eMRTD Application MUST be selected before Basic Access Control is performed.

- The inspection system SHOULD derive the Document Basic Access Keys (K_{Enc} and K_{MAC}) from the MRZ.

- The inspection system and the eMRTD chip mutually authenticate using the Document Basic Access Keys and derive session keys KS_{Enc} and KS_{MAC}.

If successful, the eMRTD chip performs the following:

- It SHALL start Secure Messaging.
- It SHALL grant access to less sensitive data (e.g. EF.DG1, EF.DG2, EF.DG14, EF.DG15, etc. of the eMRTD Application, and the Document Security Object).
- It SHALL restrict access rights to require Secure Messaging.

Note.— As a result of the Chip Access Procedure, the Current DF can be either the Master File (if PACE was used) or the eMRTD Application (if BAC was used).

٤-٣ المراقبة الأساسية للوصول

٤-٣-١ *المواصفة الفنية للبروتوكول*

يتم توفير التحقق من الصحة وإنشاء المفاتيح بواسطة بروتوكول ثلاثي المراحل للتحدي والاستجابة وفقاً لـ [ISO/IEC 11770-2] آلية إنشاء المفاتيح ٦ باستخدام 3DES [FIPS 46-3] كشفرة كتلة. وثمة مجموع تحقق للتشفير وفقاً لـ [ISO/IEC 9797-1]، الخوارزمية ٣ لرمز التحقق من صحة الرسالة تُحسب فوق نصوص الشفرة وتلحق بها. و**يجب** استخدام طرائق التشغيل الموصوفة في القسم ٤-٣-٣. و**يجب** أن يكون حجم الأرقام المستخدمة مرة واحدة ٨ بتات، و**يجب** أن يكون حجم مواد استخدام المفاتيح المتبادلة ١٦ بتات. و**يجب ألا** يستخدم جهاز التوصيل (أي نظام التفتيش) والدائرة المتكاملة اللاتلامسية معرّفات مميزة كأرقام تُستخدم مرة واحدة.

بمزيد من التفصيل، **يجب** أن يتضمن جهاز التوصيل والدائرة المتكاملة الخطوات التالية:

1) The IFD requests a challenge RND.IC by sending the GET CHALLENGE command. The IC generates and responds with a nonce RND.IC.

2) The IFD performs the following operations:

   a) generate a nonce RND.IFD and keying material K.IFD.

   b) generate the concatenation S = RND.IFD || RND.IC || K.IFD.

   c) compute the cryptogram $E_{IFD} = \mathbf{E}(K_{Enc}, S)$.

   d) compute the checksum $M_{IFD} = \mathbf{MAC}(K_{MAC}, E_{IFD})$.

   e) send the EXTERNAL AUTHENTICATE command with mutual authenticate function using the data E_{IFD} || M_{IFD}.

3) The IC performs the following operations:

   a) check the checksum MIFD of the cryptogram EIFD.

   b) decrypt the cryptogram EIFD.

   c) extract RND.IC from S and check if IFD returned the correct value.

   d) generate keying material K.IC.

   e) generate the concatenation R = RND.IC || RND.IFD || K.IC.

   f) compute the cryptogram EIC = E(KEnc, R).

   g) compute the checksum MIC = MAC(KMAC, EIC).

h) send the response using the data EIC || MIC.

4) The IFD performs the following operations:

a) check the checksum M_{IC} of the cryptogram E_{IC}.

b) decrypt the cryptogram E_{IC}.

c) extract RND.IFD from R and check if IC returned the correct value.

5) The IFD and the IC derive session keys KSEnc and KSMAC using the key derivation mechanism described in Sections 9.7.1 and 9.7.4 with (K.IC xor K.IFD) as shared secret.

٤-٣-٢ عملية التفتيش

عند تقديم وثيقة سفر إلكترونية مقروءة آلياً مزوّدة بالمراقبة الأساسية للوصول إلى نظام التفتيش، تُستخدم المعلومات المقروءة ضوئياً أو بصرياً لاستخلاص المفتاحين الأساسيين للاطلاع على الوثيقة (K_{Enc} و K_{MAC}) للتمكن من الوصول إلى الدائرة المتكاملة اللاتلامسية ولإقامة قناة اتصالات مأمونة بين الدائرة المتكاملة اللاتلامسية لوثيقة السفر الإلكترونية المقروءة آلياً ونظام التفتيش.

أي دائرة متكاملة لاتلامسية لوثيقة سفر إلكترونية مقروءة آلياً تدعم مراقبة الاطلاع الأساسي **يجب** أن تستجيب لمحاولات القراءة التي لم يتم التحقق من صحتها، أي محاولات القراءة المرسلة بدون مراسلات مأمونة (بما في ذلك اختيار الملفات (المحمية) في بنية البيانات المنطقية)، مع "عدم إرضاء الوضع الأمني" (0x6982) بمجرد إنشاء قناة مأمونة. وإذا تسلّمت الدائرة المتكاملة أمر اختيار بسيط، أي بدون تطبيق المراسلات المأمونة، في القناة المأمونة، **يجب** أن تلغي الدائرة المتكاملة القناة المأمونة. وعند إرسال أمر اختيار بسيط قبل إنشاء القناة المأمونة، أو عندما يكون قد تم إلغاء القناة المأمونة، **يجوز** أن تعيد الدائرة المتكاملة كلاً من 0x6982 and 0x9000، أي هما استجابتان مطابقتان لمعايير الايكاو.

للتحقق من صحة نظام التفتيش **يجب** أداء الخطوات التالية:

1) The inspection system reads the “MRZ_information”. The “MRZ_information” consists of the concatenation of Document Number, Date of Birth and Date of Expiry, including their respective check digits, as described in Doc 9303-4, Doc 9303-5 or Doc 9303-6 for document form factors TD3, TD1 and TD2, respectively, from the MRZ using an OCR-B reader. Alternatively, the required information can be typed in; in this case it SHALL be typed in as it appears in the MRZ. The most significant 16 bytes of the SHA-1 hash of this “MRZ_information” are used as key seed to derive the Document Basic Access Keys using the key derivation mechanism described in Section 9.7.2.

2) The inspection system and the eMRTD’s contactless IC mutually authenticate and derive session keys. The authentication and key establishment protocol described above MUST be used.

3) After a successful execution of the authentication protocol both the IFD and the IC compute session keys KS_{Enc} and KS_{MAC} using the key derivation mechanism described in Sections 9.7.1 and 9.7.4 with (K.IC xor K.IFD) as shared secret. All subsequent communication MUST be protected by Secure Messaging as described in Section 9.8.

٤-٣-٣ المواصفات الفنية للتشفير

٤-٣-٣-١ *تشفير التحدي والاستجابة*

مفتاحان ٣ للقاعدة القياسية لتشفير البيانات بطريقة CBC مع صفر IV (أي 00 00 00 00 00 00 00 00) وفقاً لـ [ISO/IEC 11568-2] **يجب** استخدامهما لحساب E_{IFD} and E_{IC}. **ويجب عدم** استخدام الحشو للبيانات المدخلة عند أداء أمر EXTERNAL AUTHENTICATE.

٤-٣-٣-٢ *التحقق من صحة التحدي والاستجابة*

يجب حساب مجموعي التحقق من التشفير M_{IFD} and M_{IC} باستخدام [ISO/IEC 9797-1] خوارزمية رمز التحقق من صحة الرسالة ٣ مع شفرة كتلة القاعدة القياسية لتشفير البيانات وصفر IV (8 bytes) وأسلوب الحشو ٢ لـ [ISO/IEC 9797-1]. و**يجب** أن يكون طول رمز التحقق من صحة الرسالة ٨ بايتات.

٤-٣-٤ وحدات بيانات بروتوكول التطبيق

يتم أداء مراقبة الاطلاع الأساسي باستخدام الأمرين GET CHALLENGE و EXTERNAL AUTHENTICATE مع وظيفة التحقق من الصحة المتبادلة. و**يجب** تشفير الأوامر على النحو المحدد في [ISO/IEC 7816-4].

٤-٣-٤-١ *التحدّي*

Command			
CLA		Context specific	
INS	0x84	GET CHALLENGE	
P1/P2	0x0000	–	
Data		*Absent*	
Response			
Data	Random Nonce		
Status Bytes	0x9000	*Normal processing* Random Nonce successfully generated and transmitted.	
	Other	*Operating system dependent error* Random Nonce could not be transmitted.	

٤-٣-٤-٢ *التحقق الخارجي من الصحة*

Command			
CLA		Context specific	
INS	0x82	EXTERNAL AUTHENTICATE	
P1/P2	0x0000	–	
Data		Command data E_{IFD} || M_{IFD}	REQUIRED
Response			
Data		Response data E_{IC} || M_{IC}	REQUIRED
Status Bytes	0x9000	*Normal processing* The protocol has been performed successfully.	
	Other	*Operating system dependent error* The protocol failed.	

٤-٤ فتح الاتصال بكلمة سر مصدّق عليها

فتح الاتصال بكلمة سر مصدّق عليها هو بروتوكول اتفاق رئيسي Diffie-Hellman تم التحقق من صحته بكلمة سر يوفّر اتصالاً مأموناً والتحقق بالاستناد إلى كلمة سر من صحة رقاقة وثيقة السفر الإلكترونية المقروءة آلياً ونظام التفتيش (أي أن رقاقة وثيقة السفر الإلكترونية المقروءة آلياً ونظام التفتيش يتشاركان في نفس كلمة السر π).

ينشئ فتح الاتصال بكلمة سر مصدّق عليها تبادل رسائل مأمون بين رقاقة وثيقة سفر إلكترونية مقروءة آلياً ونظام تفتيش مستند إلى كلمات سر ضعيفة (قصيرة). ويُنشأ سياق الأمن في الملف الرئيسي. ويمكّن البروتوكول رقاقة وثيقة السفر الإلكترونية المقروءة آلياً من التحقق من أن نظام التفتيش مرخّص له بالاطلاع على البيانات المخزّنة ويتسم بالسمتين التاليتين:

- توفّر مفاتيح دورة قوية مستقلة عن قوة كلمة سر.
- انتروبيا كلمة السر (كلمات السر) المستخدمة للتحقق من صحة نظام التفتيش يمكن أن تكون منخفضة (مثلاً ٦ أرقام تكفي بصفة عامة.

فتح الاتصال بكلمة سر مصدّق عليها يستخدم مفاتيح K_π مستنتجة من كلمات سر مع وظيفة استنتاج مفاتيح $\mathbf{KDF}_\pi$ (انظر القسم ٩-٧-٣). من أجل وثائق السفر المقروءة آلياً القابلة للتشغيل المتبادل عالمياً تتوافر كلمتا السر التاليتان والمفتاحان المقابلان:

- MRZ: The key K_π defined by $K_\pi = \mathbf{KDF}_\pi(\text{MRZ})$ is REQUIRED. It is derived from the Machine Readable Zone (MRZ) similar to Basic Access Control, i.e. the key is derived from the Document Number, the Date of Birth and the Date of Expiry.

- CAN: The key K_π defined by $K_\pi = \mathbf{KDF}_\pi(\text{CAN})$ is OPTIONAL. It is derived from the Card Access Number (CAN). The CAN is a number printed on the document and MUST be chosen randomly or pseudo-randomly (e.g. using a cryptographically strong pseudo-random function). Doc 9303, Parts 4,5 and 6 specify the CAN field.

ملاحظة — على النقيض من الجزء المقروء آلياً (رقم الوثيقة، تاريخ الميلاد، تاريخ انتهاء الصلاحية) يتسم رقم الاطلاع على البطاقة بميزة أنه يمكن طباعته يدوياً بسهولة.

يدعم فتح الاتصال بكلمة سر مصدّق عليها تحديد المجالات المختلفة كجزء من تنفيذ البروتوكول:

- تحديد المجالات العام المستند إلى اتفاق مفتاح Diffie-Hellman؛
- تحديد المجالات المتكامل المستند إلى تحديد المجالات المباشر لعنصر خانة لمجموعة التشفير؛
- يمدّد تحديد المجالات للتحقق من صحة الرقاقة تحديد المجالات العام ويدمج التحقق من صحة الرقاقة في بروتوكول فتح الاتصال بكلمة سر مصدّق عليها.

إذا كانت الرقاقة تدعم تحديد المجالات للتحقق من صحة الرقاقة، **فيجب** أن تدعم الرقاقة أيضاً واحداً على الأقل من تحديد المجالات العام أو تحديد المجالات المتكامل والتحقق من صحة الرقاقة. وهذا يدل ضمنياً على أنه بالنسبة لنظم التفتيش الداعمة لفتح الاتصال بكلمة سر مصدّق عليها، **من المطلوب** فقط الدعم لتحديد المجالات العام وتحديد المجالات المتكامل. ودعم تحديد المجالات للتحقق من صحة الرقاقة هو **اختياري**.

٤-٤-١ المواصفة الفنية للبروتوكول

يقرأ نظام التفتيش البارامترات لفتح الاتصال بكلمة سر مصدّق عليها التي تدعمها رقاقة وثيقة السفر الإلكترونية المقروءة آلياً من الملف EF.CardAccess (انظر القسم ٩-٢-١١) ويختار البارامترات التي تُستخدم، ويلي ذلك تنفيذ البروتوكول.

يجب استخدام الأوامر التالية:

- READ BINARY as specified in Doc 9303-10;
- MSE:Set AT (MANAGE SECURITY ENVIRONMENT command with Set Authentication Template function) as specified in Section 4.4.4.1;
- The following steps SHALL be performed by the inspection system and the eMRTD chip using a chain of GENERALAUTHENTICATE commands as specified in Section 4.4.4.2:

1) The eMRTD chip randomly and uniformly chooses a nonce s, encrypts the nonce to $z = \mathbf{E}(K_\pi,s)$, where $K_\pi = \mathbf{KDF}_\pi(\pi)$ is derived from the shared password π, and sends the ciphertext z to the inspection system.

2) The inspection system recovers the plaintext $s = \mathbf{D}(K_\pi,z)$ with the help of the shared password π.

3) Both the eMRTD chip and the inspection system perform the following steps:

a) They exchange additional data required for the mapping of the nonce:

i) for the generic mapping, the eMRTD chip and the inspection system exchange ephemeral key public keys.

ii) for the integrated mapping, the inspection system sends an additional nonce to the eMRTD chip.

b) They compute the ephemeral domain parameters $D = \mathbf{Map}(D_{IC},s,\ldots)$ as described in Section 4.4.3.3.

c) They perform an anonymous Diffie-Hellman key agreement (cf. Section 9.6) based on the ephemeral domain parameters and generate the shared secret $K = \mathbf{KA}(SK_{DH,IC}, PK_{DH,IFD},D) = \mathbf{KA}(SK_{DH,IFD},PK_{DH,IC},D)$.

d) During Diffie-Hellman key agreement, the IC and the inspection system SHOULD check that the two public keys $PK_{DH,IC}$ and $PK_{DH,IFD}$ differ.

e) They derive session keys $KS_{MAC} = \mathbf{KDF}_{\mathrm{MAC}}(K)$ and $KS_{Enc} = \mathbf{KDF}_{\mathrm{Enc}}(K)$ as described in Section 9.7.1.

f) They exchange and verify the authentication token $T_{IFD} = \mathbf{MAC}(KS_{MAC},PK_{DH,IC})$ and $T_{IC} = \mathbf{MAC}(KS_{MAC},PK_{DH,IFD})$ as described in Section 4.4.3.4.

4) Conditionally, the eMRTD chip computes Chip Authentication Data CA_{IC}, encrypts them $A_{IC} = \mathbf{E}(KS_{Enc}, CA_{IC})$ and sends them to the terminal (cf. Section 4.4.3.5.1). The terminal decrypts A_{IC} and verifies the authenticity of the chip using the recovered Chip Authentication Data CA_{IC} (cf. Section 4.4.3.5.2).

تبيَّن أيضاً في الشكل ١ نسخة مبسّطة من البروتوكول.

Chip denoted as IC		***Inspection system denoted as IFD***
Static domain parameters D_{IC} Choose random nonce s Compute z = **E**(K_π,s)		
	— z →	
		Compute s = **D**(K_π,z)
	← additional data for **Map** →	
D = **Map**(D_{IC},s,…) Choose random ephemeral key pair ($SK_{DH,IC}$, $PK_{DH,IC}$,D)		D = **Map**(D_{IC},s,…) Choose random ephemeral key pair ($SK_{DH,IFD}$,$PK_{DH,IFD}$,D)
	← $PK_{DH,IC}$, $PK_{DH,IFD}$ →	
Check $PK_{DH,IC} \neq PK_{DH,IFD}$ K = **KA**($SK_{DH,IC}$, $PK_{DH,IFD}$,D) Compute T_{IC} = **MAC**(KS_{MAC},$PK_{DH,IFD}$) [compute CA_{IC} and encrypt as A_{IC} = **E**(KS_{Enc}, CA_{IC}).]		Check $PK_{DH,IC} \neq PK_{DH,IFD}$ K = **KA**($SK_{DH,IFD}$,$PK_{DH,IC}$,D) Compute T_{IFD} = **MAC**(KS_{MAC},$PK_{DH,IC}$)
	← T_{IC}, T_{IFD} → [— A_{IC} →]	
Verify T_{IFD}		Verify T_{IC} [decrypt A_{IC} and authenticate chip]

الشكل ١ — فتح الاتصال بكلمة سر مصدّق عليها

٤-٤-٢ حالة الأمن

رقاقة أي وثيقة سفر إلكترونية مقروءة آلياً تدعم فتح الاتصال بكلمة سر مصدّق عليها **يجب** أن تستجيب لمحاولات القراءة غير المتحقق من صحتها (بما في ذلك اختيار الملفات (المحمية) في بنية البيانات المنطقية) بعبارة (0x6982) "Security status not satisfied".

ملاحظة — هذه المواصفة أكثر تقييداً من المواصفة المناظرة من أجل وثائق السفر الإلكترونية المقروءة آلياً لمراقبة الاطلاع الأساسي فقط.

إذا تم بنجاح أداء فتح الاتصال بكلمة سر مصدّق عليها فمن ثم فإن رقاقة وثيقة السفر الإلكترونية المقروءة آلياً قد تحققت من صحة كلمة السر المستخدمة. وتُبدأ المراسلات المأمونة باستخدام مفتاحي الدورة المشتقين KS_{MAC} and KS_{Enc}.

٤-٤-٣ مواصفات التشفير

يحتوي هذا القسم على تفاصيل التشفير للمواصفات.

تقوم دولة أو منظمة الإصدار باختيار خوارزميات خاصة. و**يجب** أن يدعم نظام التفتيش جميع التوليفات الموصوفة في الأقسام الفرعية التالية، باستثناء تحديد المجالات للتحقق من صحة الرقاقة، الذي يكون اختيارياً. و**يجوز** لرقاقة وثيقة السفر المقروءة آلياً أن تدعم أكثر من توليفة واحدة من الخوارزميات.

ملاحظة — بعض الخوارزميات غير متاحة لتحديد مجالات التحقق من صحة الرقاقة: لأسباب أمنية، فإن استخدام القاعدة القياسية لتشفير البيانات 3DES لم يعد موصى به. ومختلف أشكال بروتوكول ديفي–هلمان لم تعد متوافرة لخفض عدد الأشكال المختلفة التي يتعين أن تنفذها الوحدات الطرفية.

٤-٤-٣-١ بروتوكول ديفي–هلمان

من أجل فتح الاتصال بكلمة سر مصدّق عليها ببروتوكول ديفي–هلمان **يجب** استخدام الخوارزميات والأشكال الخاصة بكل من القسم ٩-٦ والجدول ٢.

الجدول ٢ — الخوارزميات والأشكال لبروتوكول ديفي–هلمان

OID	*Mapping*	*Sym. Cipher*	*Key-length*	*Secure Messaging*	*Auth. Token*
id-PACE-DH-GM-3DES-CBC-CBC	Generic	3DES	112	CBC / CBC	CBC
id-PACE-DH-GM-AES-CBC-CMAC-128	Generic	AES	128	CBC / CMAC	CMAC
id-PACE-DH-GM-AES-CBC-CMAC-192	Generic	AES	192	CBC / CMAC	CMAC
id-PACE-DH-GM-AES-CBC-CMAC-256	Generic	AES	256	CBC / CMAC	CMAC
id-PACE-DH-IM-3DES-CBC-CBC	Integrated	3DES	112	CBC / CBC	CBC
id-PACE-DH-IM-AES-CBC-CMAC-128	Integrated	AES	128	CBC / CMAC	CMAC
id-PACE-DH-IM-AES-CBC-CMAC-192	Integrated	AES	192	CBC / CMAC	CMAC
id-PACE-DH-IM-AES-CBC-CMAC-256	Integrated	AES	256	CBC / CMAC	CMAC

٤–٤–٣–٢ *بروتوكول ديفي–هيلمان للمنحنى الاهليلجي*

لفتح الاتصال بكلمة سر مصدّق عليها ببروتوكول ديفي–هيلمان للمنحنى الاهليلجي **يجب** استخدام كل من الخوارزميات والأشكال من القسم ٩–٦ والجدول ٣.

يجب أن تُستخدم فقط المنحنيات الرئيسية ذات النقاط غير المضغوطة. و**ينبغي** أن تُستخدم معايير النطاق الموحدة الموصوفة في القسم **Error! Reference source not found.**9.5.1.

الجدول ٣ — الخوارزميات والأشكال لبروتوكول ديفي–هيلمان للمنحنى الاهليلجي

OID	*Mapping*	*Sym. Cipher*	*Key-length*	*Secure Messaging*	*Auth. Token*
id-PACE-ECDH-GM-3DES-CBC-CBC	Generic	3DES	112	CBC / CBC	CBC
id-PACE-ECDH-GM-AES-CBC-CMAC-128	Generic	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-GM-AES-CBC-CMAC-192	Generic	AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-GM-AES-CBC-CMAC-256	Generic	AES	256	CBC / CMAC	CMAC
id-PACE-ECDH-IM-3DES-CBC-CBC	Integrated	3DES	112	CBC / CBC	CBC
id-PACE-ECDH-IM-AES-CBC-CMAC-128	Integrated	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-IM-AES-CBC-CMAC-192	Integrated	AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-IM-AES-CBC-CMAC-256	Integrated	AES	256	CBC / CMAC	CMAC
id-PACE-ECDH-CAM-AES-CBC-CMAC-128	Chip Authenti-cation	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-CAM-AES-CBC-CMAC-192		AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-CAM-AES-CBC-CMAC-256		AES	256	CBC / CMAC	CMAC

٤–٤–٣–٣ *تشفير وتحديد مجالات الأرقام التي تُستخدم مرة واحدة*

يجب أن تقوم رقاقة وثيقة السفر الإلكترونية المقروءة آلياً بشكل عشوائي وموحّد باختيار الرقم الذي يُستخدم مرة واحدة s كسلسلة ثنائية من البتات طولها /، حيث أن / هي مضاعف حجم الكتلة بالبتات لشيفرة الكتلة المختصة **E**() التي اختارتها رقاقة وثيقة السفر الإلكترونية المقروءة آلياً.

- الرقم المُستخدم مرة واحدة s **يجب** تشفيره بطريقة CBC وفقاً لـ [ISO/IEC 10116] باستخدام المفتاح $K_\pi = KDF_\pi(\pi)$ المستمد من كلمة السر π و IV المحددة للسلسلة all-0.
- **يجب** تحويل الرقم الذي يستخدم مرة واحدة s إلى مولد عشوائي يستخدم وظيفة تحديد مجالات محددة بخوارزمية **Map**.
- بالنسبة لتحديد المجالات المتكامل **يجب** اختيار الرقم الذي يُستخدم مرة واحدة الاضافي بشكل عشوائي ومتسق كسلسلة من البتات الثنائية ذات الطول k وتُرسل في صيغة واضحة. وفي هذه الحالة فإن k هو حجم المفتاح بالبتات لشيفرة الكتلة المناظرة **E**() و / **يجب** أن يكون أصغر مضاعف لحجم الكتلة **E**() بحيث أن $l \geq k$.

الرقم الذي يُستخدم مرة واحدة لتحديد المجالات s أو الرقمين اللذين يستخدمان مرة واحدة s, t إلى داخل مجموعة التشفير **يجب** استخدام واحد من أشكال تحديد المجالات التالية:

- تحديد المجالات العامة (القسم ٤-٤-٣-٣-١)؛
- تحديد المجالات المتكامل (القسم ٤-٤-٣-٣-٢)؛
- تحديد المجالات للتحقق من صحة الرقاقة (القسم ٤-٤-٣-٣-٣).

٤-٤-٣-٣-١ *تحديد المجالات العام*

بروتوكول ديفي-هيلمان للمنحنى الاهليلجي

The function **Map**:G → Ĝ is defined as Ĝ = s×G+H, where H in <G> is chosen such that $\log_G H$ is unknown. The point H SHALL be calculated by an anonymous Diffie-Hellman Key Agreement [TR-03111] as H = **KA**$(SK_{Map,IC}, PK_{Map,IFD}, D_{IC})$ = **KA**$(SK_{Map,IFD}, PK_{Map,IC}, D_{IC})$.

ملاحظة — خوارزمية اتفاق المفاتيح ECKA تحول دون هجمات المجموعات الفرعية الصغيرة عن طريق استخدام العامل المتوافق للضرب.

بروتوكول ديفي-هيلمان

The function **Map**:g → ĝ is defined as ĝ =g^s×h, where h in <g> is chosen such that $\log_g h$ is unknown. The group element h SHALL be calculated by an anonymous Diffie-Hellman Key Agreement as h = **KA**$(SK_{Map,IC}, PK_{Map,IFD}, D_{IC})$ = **KA**$(SK_{Map,IFD}, PK_{Map,IC}, D_{IC})$.

*ملاحظة — **يجب** استخدام أسلوب المصادقة على المفتاح العام الموصوف في [RFC 2631] لمنع هجمات المجموعات الفرعية الصغيرة.*

٤-٤-٣-٣-٢ *تحديد المجالات المتكامل*

بروتوكول ديفي-هيلمان للمنحنى الاهليلجي

The function **Map**:G → Ĝ is defined as Ĝ = $f_G(\mathbf{R}_p(s,t))$, where $\mathbf{R}_p$() is a pseudo-random function that maps octet strings to elements of GF(p) and f_G() is a function that maps elements of GF(p) to <G>. The random nonce t SHALL be chosen randomly by the inspection system and sent to the eMRTD chip. The pseudo-random function $\mathbf{R}_p$()is described below. The function f_G() is defined in [BCIMRT2010]. An informative description is given in Appendix B.

بروتوكول ديفي-هيلمان

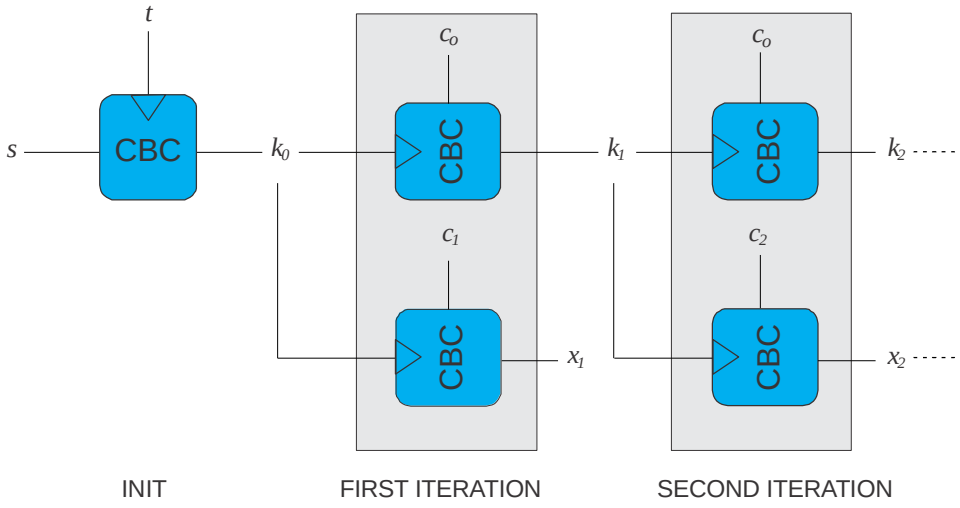
The function **Map**:g → ĝ is defined as ĝ = $f_g(\mathbf{R}_p(s,t))$, where $\mathbf{R}_p$() is a pseudo-random function that maps octet strings to elements of GF(p) and f_g() is a function that maps elements of GF(p) to <g>. The random nonce t SHALL be chosen randomly by the inspection system and sent to the eMRTD chip. The pseudo-random function $\mathbf{R}_p$() is described below. The function f_g() is defined as $f_g(x)=x^a \bmod p$, and a = (p-1)/q is the cofactor. Implementations MUST check that ĝ ≠ 1.

تحديد مجالات الأرقام العشوائي الزائف

The function $\mathbf{R}_p(s,t)$ is a function that maps octet strings s (of bit length l) and t (of bit length k) to an element $int(x_1||x_2||...||x_n)$ mod p of GF(p). The function $\mathbf{R}_p(s,t)$ is specified below in Figure 2.

The construction is based on the respective block cipher **E**() in CBC mode according to [ISO/IEC 10116] with IV=0, where k is the key size (in bits) of **E**(). Where required, the output k_i MUST be truncated to key size *k*. The value *n* SHALL be selected as smallest number, such that $n*l \geq \log_2 p + 64$.

ملاحظة — الاقتطاع لازم فقط بالنسبة إلى AES-192. استخدم الثمانينات من ١ إلى ٢٤ من k_i، ولا تُستخدم الثمانينات الاضافية. وفي حالة القاعدة القياسية لتشفير البيانات، تُعتبر k مساوية لـ ١٢٨ بتات، ويجب أن يكون مُخرج R(s,t) هو ١٢٨ بتات.



الشكل ٢ — تحديد مجالات الأرقام العشوائي الزائف

The constants c_0 and c_1 are defined as follows:

- For 3DES and AES-128 (l=128):
  - `c0=0xa668892a7c41e3ca739f40b057d85904`
  - `c1=0xa4e136ac725f738b01c1f60217c188ad`
- For AES-192 and AES-256 (l=256):
  - `c0= 0xd463d65234124ef7897054986dca0a174e28df758cbaa03f240616414d5a1676`
  - `c1= 0x54bd7255f0aaf831bec3423fcf39d69b6cbf066677d0faae5aadd99df8e53517`

٤-٤-٣-٣-٣ تحديد المجالات للتحقق من صحة الرقاقة

مرحلة تحديد المجالات لنظام تحسين الأداء والكفاءة – التصنيع بمساعدة الحاسوب مطابقة لمرحلة تحديد المجالات لنظام تحسين الأداء والكفاءة – تحديد المجالات العام (النظر القسم ٤-٤-٣-٣-١).

٤-٤-٣-٤ رمز التحقق من الصحة

يجب حساب رمز التحقق من الصحة فوق موضوع بيانات لمفتاح عام (انظر القسم ٩-٤) يتضمن محدد الموضوع كما هو مبيّن في MSE:Set AT (انظر القسم ٤-٤-١)، والمفتاح العام سريع الزوال المستلم (أي باستبعاد بارامترات النطاق، انظر القسم ٩-٤-٥) مع استخدام رمز للتحقق من الصحة والمفتاح KS_{MAC} المستمد من اتفاق المفاتيح.

ملاحظة — يتم أداء الحشو داخلياً بواسطة رمز للتحقق من صحة الرسالة، أي لا يتم أداء حشو محدد للتطبيق.

التشفير الثلاثي للبيانات

يجب استخدام التشفير الثلاثي للبيانات [القاعدة القياسية الاتحادية لمعالجة المعلومات ٤٦-٣] في طريقة التقسيط وفقاً لـ [ISO/IEC 9797-1] خوارزمية رمز التحقق من صحة الرسالة / 3 أسلوب الحشو ٢ مع شيفرة الكتلة بالقاعدة القياسية لتشفير البيانات و IV=0.

القاعدة القياسية للتشفير المتقدم

يجب استخدام القاعدة القياسية للتشفير المتقدم [القاعدة القياسية الاتحادية لمعالجة المعلومات ١٩٧] في طريقة رمز التحقق من صحة الرسالة القائم على الشيفرة [SP 800-38B] مع طول رمز تحقق من صحة الرسالة قدره ٨ بايت.

٤-٤-٣-٥ بيانات التحقق من صحة الرقاقة المشفّرة

يجب أن توفّر رقاقة وثيقة السفر الإلكترونية المقروءة آلياً زوج (أزواج) المفاتيح الساكنة SK_{IC}, PK_{IC} على النحو الموصوف في القسم ٦-٢. وبيانات التحقق من صحة الرقاقة المشفّرة **مطلوبة** من أجل فتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات للتحقق من صحة الرقاقة.

٤-٤-٣-٥-١ الصنع برقاقة وثيقة السفر الإلكترونية المقروءة آلياً

يجب حساب بيانات التحقق من صحة الرقاقة بوصفها $CA_{IC} = (SK_{IC})^{-1} * SK_{Map,IC} \bmod p$، حيث أن SK_{IC} هو المفتاح الخاص الساكن للرقاقة، و $SK_{Map,IC}$ هو المفتاح الخاص سريع الزوال الذي تستخدمه الرقاقة للحاسوب H في مرحلة تحديد مجالات فتح الاتصال بكلمة سر مصدّق عليها (راجع القسم ٤-٤-٣-٣-١) و p هو ترتيب مجموعة التشفير المستخدمة. و**يجب** تشفير بيانات التحقق من صحة الرقاقة باستخدام المفتاح KS_{Enc} المستمد من اتفاق المفاتيح بوصفه $A_{IC} = \mathbf{E}(KS_{Enc}, CA_{IC})$ لإنتاج البيانات المشفّرة للتحقق من صحة الرقاقة.

ملاحظة — $(SK_{IC})^{-1}$ يمكن حسابه مسبقاً خلال إضافة البيانات الشخصية لرقاقة وثيقة السفر الإلكترونية المقروءة آلياً وتخزينها بشكل مأمون في الرقاقة، لتفادي انعكاس الوحدات أثناء وقت التشغيل.

٤-٤-٣-٥-٢ التحقق من الصحة بواسطة الوحدة الطرفية

يجب أن تفك الوحدة الطرفية تشفير A_{IC} لاسترداد CA_{IC} والتحقق من $PK_{Map,IC} = \mathbf{KA}(CA_{IC}, PK_{IC}, D_{IC})$، حيث أن PK_{IC} هو المفتاح العام الساكن لرقاقة وثيقة السفر الإلكترونية المقروءة آلياً.

*ملاحظة — **يجب** أداء التحقق السلبي من الصحة بالاقتران مع تحديد مجالات التحقق من صحة الرقاقة. وبعد التحقق بنجاح من صلاحية المادة الأمنية المختصة فقط يجوز اعتبار رقاقة وثيقة السفر الإلكترونية المقروءة آلياً حقيقية.*

٤-٤-٣-٥-٣ الحشو

يجب حشو البيانات التي يتعين تشفيرها وفقاً لـ [ISO/IEC 9797-1] "طريقة الحشو ٢".

٤-٤-٣-٥-٤ AES

AES [19] SHALL be used in CBC-mode according to [ISO/IEC 10116] with $IV=E(KS_{Enc},-1)$, where *-1* is the bit string of length 128 with all bits set to 1.

٤-٤-٤ وحدات بيانات بروتوكول التطبيق

يجب استخدام السلسلة التالية من الأوامر لتنفيذ فتح الاتصال بكلمة سر مصدّق عليها:

1. MSE:Set AT
2. GENERAL AUTHENTICATE

4.4.4.1 MSE:Set AT

The command MSE:Set AT is used to select and initialize the PACE protocol. The use of MSE:Set AT for PACE is indicated by a PACE Object Identifier (see Sections 4.4.3 and 9.2.3) contained as cryptographic mechanism reference with tag 0x80, see table below.

Command			
CLA		Context specific	
INS	0x22	Manage Security Environment	
P1/P2	0xC1A4	Set Authentication Template for mutual authentication	
Data	0x80	*Cryptographic mechanism reference* Object Identifier of the protocol to select (value only, Tag 0x06 is omitted).	REQUIRED
	0x83	*Reference of a public key / secret key* The password to be used is indicated by the following values in this data object: 0x01: MRZ_information 0x02: CAN	REQUIRED
	0x84	*Reference of a private key / Reference for computing a session key* This data object is REQUIRED to indicate the identifier of the domain parameters to be used if the domain parameters are ambiguous, i.e. more than one set of domain parameters is available for PACE.	CONDITIONAL
	0x7F4C	*Certificate Holder Authorization Template* This data object (defined in Doc 9303-12) MUST be present if the terminal requests Certification Authority Reference(s) for use in Terminal Authentication to be returned as part of PACE (cf. Section 4.4.5). The Object Identifier contained in this data object SHALL be set to id-IS (cf. Doc 9303-10). The access bits in the discretionary data template SHALL all be set to 1 by the terminal.	CONDITIONAL
Response			
Data	–	Absent	
Status Bytes	0x9000	*Normal processing* The protocol has been selected and initialized.	
	0x6A80	*Incorrect parameters in the command data field* Algorithm not supported or initialization failed.	
	0x6A88	*Referenced data not found* The referenced data (i.e. password or domain parameter) is not available.	
	other	*Operating system dependent error* The initialization of the protocol failed.	

الملاحظة ١ — بعض نظم التشغيل تقبل اختيار مفتاح غير متوافر وتفيد بخطأ فقط عند استخدام المفتاح للغرض المختار.

*الملاحظة ٢ — بالنسبة للأمر NSE.Set، **ينبغي** أن تتجاهل الدائرة المتكاملة مواد البيانات التي تكون وسومها غير محددة بالنسبة لهذا الأمر. وينبغي **ألا تشمل** الوحدة الطرفية مواد بيانات ذات وسوم من غير المعروف أنها مفهومة من الدائرة المتكاملة.*

٤-٤-٤-٢ *التحقق العام من الصحة (GENERAL AUTHENTICATE)*

تُستخدم سلسلة من أوامر التحقق العام من الصحة (GENERAL AUTHENTICATE) لأداء بروتوكول فتح الاتصال بكلمة سر مصدّق عليها.

Command			
CLA		Context specific.	
INS	0x86	GENERAL AUTHENTICATE	
P1/P2	0x0000	Keys and protocol implicitly known	
Data	0x7C	*Dynamic Authentication Data* Protocol specific data objects	REQUIRED
Response			
Data	0x7C	*Dynamic Authentication Data* Protocol specific data objects as described in Section 4.4.5.	REQUIRED
Status Bytes	0x9000	*Normal processing* The protocol (step) was successful.	
	0x6300	*Authentication failed* The protocol (step) failed.	
	0x6A80	*Incorrect parameters in command data field* Provided data is invalid.	
	other	*Operating system dependent error* The protocol (step) failed.	

٤-٤-٤-٣ *تسلسل الأوامر*

يجب استخدام تسلسل الأوامر من أجل أمر التحقق العام من الصحة (GENERAL AUTHENTICATE) لربط تسلسل الأوامر بتنفيذ البروتوكول. و**يجب عدم** استخدام تسلسل الأوامر لأغراض أخرى ما لم تشر الرقاقة بذلك بوضوح. وللتفاصيل بشأن تسلسل الأوامر انظر [ISO/IEC 7816-4].

٤-٤-٥ البيانات المتبادلة

يجب تبادل مواد البيانات المحددة للبروتوكول في سلسلة من أوامر التحقق العام من الصحة (GENERAL AUTHENTICATE)، مع أمر محدد للبروتوكول وبيانات استجابة مغلّفة في مادة بيانات التحقق الدينامي من الصحة (انظر القسم ٤-٤-٤-٢) مع وسوم محددة للسياق على النحو المبيّن في الجدول ٤:

الجدول ٤ — البيانات المتبادلة لفتح الاتصال بكلمة سر مصدّق عليها

الخطوة	*الوصف*	*بيانات أمر البروتوكول*		*بيانات الاستجابة للبروتوكول*	
١–	رقم مشفّر يُستخدم مرة واحدة	-	لا توجد[1]	0x80	رقم مشفّر يُستخدم مرة واحدة
٢–	رقم يُستخدم مرة واحدة لتحديد المجالات	0x81	بيانات تحديد المجالات	0x82	بيانات تحديد المجالات
٣–	أداء اتفاق المفاتيح	0x83	مفتاح عام سريع الزوال	0x84	مفتاح عام سريع الزوال
٤–	التحقق المتبادل من الصحة	0x85	رمز التحقق من الصحة	0x86	رمز التحقق من الصحة
				0x87	مرجع السلطة المعنية بإصدار الشهادات (مشروط)
				0x88	مرجع السلطة المعنية بإصدار الشهادات (مشروط)
				0x8A	بيانات التحقق من صحة الرقاقة المشفّرة (مشروطة)

يجب أن يكون مرجع أو مراجع السلطة المعنية بإصدار الشهادات موجودة إذا أرسلت مادة البيانات 0x7F4C إلى الدائرة المتكاملة أثناء فتح الاتصال بكلمة سر مصدّق عليها (انظر القسم ٤–٤–١) وكان التحقق من صحة الوحدة الطرفية مدعوماً من الدائرة المتكاملة. وفي هذه الحالة **يجب** أن تحتوي مادة البيانات 0x87 على أحدث مرجع للسلطة المعنية بإصدار الشهادات. و**يجوز** أن تحتوي مادة البيانات 0x88 على المرجع السابق للسلطة المعنية بإصدار الشهادات.

يجب أن تكون بيانات التحقق من صحة الرقاقة المشفّرة (انظر القسم ٤–٤–٣–٥) موجودة إذا استُخدم تحديد مجالات التحقق من صحة الرقاقة و**يجب ألا** تكون موجودة بخلاف ذلك.

٤–٤–٥–١ الرقم المشفّر الذي يُستخدم مرة واحدة

الرقم المشفّر الذي يُستخدم مرة واحدة (انظر القسم ٤–٤–٣–٣) **يجب** ترميزه كسلسلة من المجموعات الثمانية.

٤–٤–٥–٢ بيانات تحديد المجالات

البيانات المتبادلة مخصصة لتحديد المجالات المستخدم:

٤–٤–٥–٢–١ تحديد المجالات العام

يجب ترميز المفاتيح العامة العابرة (راجع القسم ٤–٤–٣–٣ والقسم ٩–٤–٥) بوصفها نقطة منحنى اهليلجي (ECDH) أو عدداً صحيحاً غير موقّع (DH).

٤–٤–٥–٢–٢ تحديد المجالات المتكامل

1. يدل هذا على وجود مادة بيانات تحقق من الصحة دينامية فارغة.

يجب ترميز الرقم الذي يُستخدم مرة واحدة *t* بوصفه سلسلة ثمانية.

ملاحظة — سياق مادة البيانات المحددة 0x82 **يجب** *أن يكون خالياً من تحديد المجالات المتكامل.*

٤-٤-٥-٢-٣ تحديد المجالات للتحقق من صحة الرقاقة

ترميز بيانات تحديد المجالات مطابق لتحديد المجالات العام (راجع القسم ٤-٤-٥-٢-١).

٤-٤-٥-٣ المفاتيح العامة

يجب ترميز المفاتيح العامة على النحو المبيّن في القسم ٩-٤-٥.

٤-٤-٥-٤ رمز التحقق من الصحة

يجب ترميز رمز التحقق من الصحة (راجع القسم ٤-٤-٣-٤) كسلسلة من المجموعات الثمانية.

٤-٤-٥-٥ مرجع السلطة المعنية بإصدار الشهادات

يجب أن ترمّز مواد البيانات المتعلقة بمرجع سلطة إصدار الشهادات على النحو المحدد في الوثيقة Doc 9303-12.

٤-٤-٥-٦ بيانات التحقق من صحة الرقاقة المشفّرة

يجب ترميز بيانات التحقق من صحة الرقاقة كسلسلة من المجموعات الثمانية باستخدام الوظيفة FE2OS() المحددة في [TR-03111] قبل التشفير. ولاحظ أن FE2OS() تتطلب الترميز بنفس العدد من المجموعات الثمانية كالترتيب الأولي للمجموعة، أي من الممكن أن يشمل 0x00's الرائدة. و**ترميز** بيانات التحقق من صحة الرقاقة المشفّرة كسلسلة من المجموعات الثمانية.

٥- التحقق من صحة البيانات

بالإضافة إلى مجموعات بيانات بنية البيانات المنطقية، تحتوي الدائرة المتكاملة اللاتلامسية أيضاً على مادة أمنية للوثيقة (SO_D). وهذه المادة موقّعة رقمياً بواسطة دولة أو منظمة الاصدار وتتضمن تمثيلات ببصمات رقمية لمحتويات بنية البيانات المنطقية (انظر الوثيقة Doc 9303-10).

ثمة نظام تفتيش، يحتوي على المفتاح العام للجهة الموقّعة على الوثيقة لكل دولة، أو قرأ شهادة الجهة الموقعة على الوثيقة (C_{DS}) من وثيقة السفر الإلكترونية المقروءة آلياً، سيتمكن من التحقق من المادة الأمنية للوثيقة (SO_D). وبهذه الطريقة، من خلال محتويات المادة الأمنية للوثيقة (SO_D)، يتم التحقق من صحة محتويات بنية البيانات المنطقية.

هذه الآلية للتحقق لا تتطلب قدرات معالجة الدائرة المتكاملة اللاتلامسية في وثيقة السفر الإلكترونية المقروءة آلياً. لذلك تسمى "التحقق السلبي من صحة" محتويات الدائرة المتكاملة اللاتلامسية.

يثبت التحقق السلبي من الصحة أن محتويات المادة الأمنية للوثيقة (SO_D) وبنية البيانات المنطقية صحيحة ولم يتم تغييرها. وهي لا تحول دون النسخ الدقيق لمحتوى الدائرة المتكاملة اللاتلامسية أو استبدال الرقاقة.

لذلك **ينبغي** دعم التحقق السلبي من الصحة بتفتيش مادي إضافي على وثيقة السفر الإلكترونية المقروءة آلياً.

٥-١ التحقق السلبي من الصحة

٥-١-١ عملية التفتيش

ينفّذ نظام التفتيش الخطوات التالية:

١) **يجب** أن يقرأ نظام التفتيش المادة الأمنية للوثيقة (SO_D) (التي **يجب** أن تحتوي على شهادة الجهة الموقعة على الوثيقة (C_{DS})، انظر أيضاً الوثيقة Doc 9303-10) من الدائرة المتكاملة اللاتلامسية.

٢) **يجب** أن يبني نظام التفتيش ويصادق على مسار لإصدار الترخيص من كيان جدير بالثقة إلى شهادة الجهة الموقعة على الوثيقة يُستخدم للتوقيع على المادة الأمنية للوثيقة (SO_D) وفقاً للوثيقة Doc 9303-12.

٣) **يجب** أن يستخدم نظام التفتيش المفتاح العام الذي تم التحقق منه للجهة الموقعة على الوثيقة للتحقق من توقيع المادة الأمنية للوثيقة (SO_D).

٤) **يجوز** لنظام التفتيش أن يقرأ مجموعات البيانات ذات الصلة من الدائرة المتكاملة اللاتلامسية.

٥) **يجب** أن يضمن نظام التفتيش أن محتويات مجموعة البيانات صحيحة ولم يغيّرها وضع بصمات رقمية على المحتويات ومقارنة النتيجة بقيمة البصمة الرقمية المناظرة في المادة الأمنية للوثيقة (SO_D).

تُعتبر الفحوص الاضافية التالية أفضل ممارسة:

١) **ينبغي** أن يقوم نظام التفتيش أو المسؤول عن التفتيش بالتحقق من وجود امتداد من نوع الوثيقة في شهادة الجهة الموقعة على الوثيقة.

- إذا كانت الإجابة بنعم، **ينبغي** أن يتحقق نظام التفتيش من تطابق الامتداد من نوع الوثيقة ونوع الوثيقة من مجموعة البيانات ١ ونوع الوثيقة من الجزء المقروء آلياً البصري (انظر الوثائق Docs 9303-12 و 9303-10 و 9303-3، على التوالي).
- إذا كانت الإجابة بلا، **ينبغي** أن يتحقق نظام التفتيش من أن الاستخدام الرئيسي لشهادة الجهة الموقعة على الوثيقة مضبوط على توقيع رقمي ومن أن شهادة الجهة الموقعة على الوثيقة تحتوي على امتداد استخدام بمفتاح ممدد (انظر الوثيقة Doc 9303-12).

٢) **ينبغي** أن يتحقق نظام التفتيش أو المسؤول عن التفتيش من تطابق رموز البلد من:

- خانة الموضوع و، إذا كان موجوداً، الاسم البديل لموضوع شهادة الجهة الموقعة على الوثيقة؛
- خانة الموضوع و، إذا كان موجوداً، الاسم البديل لموضوع الكيان الجدير بالثقة (شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات)؛
- مجموعة البيانات الأولى حسب ما تُقرأ من الدائرة المتكاملة اللاتلامسية؛
- الجزء المقروء آلياً البصري.

بالإضافة إلى ذلك، **يجوز** لجهاز التفتيش أو المسؤول عن التفتيش مقارنة محتويات مجموعة البيانات الأولى بالجزء المقروء آلياً البصري (انظر الوثائق Docs 9303-12 و 9303-10 و 9303-3، على التوالي)

٣) **ينبغي** أن يتحقق جهاز التفتيش من أن تاريخ إصدار وثيقة السفر الإلكترونية المقروءة آلياً مشمول في فترة استخدام المفتاح الخاص التي تحتوي عليها شهادة الجهة الموقعة على الوثيقة (انظر الوثيقة Doc 9303-12).

يمكن الآن استخدام معلومات الاستدلال البيولوجي لإجراء التحقق من سمات الاستدلال البيولوجي لدى الشخص الذي يعرض وثيقة السفر الإلكترونية المقروءة آلياً.

٥-١-٢ *عملية التفتيش الإضافية لتطبيقات LDS2*

لا تكون البيانات المكتوبة بعد إصدار وثيقة السفر الإلكترونية المقروءة آلياً محمية بالمادة الأمنية للوثيقة، التي توقعها جهة إصدار الوثيقة. وللتحقق من موثوقية البيانات التي تكتب بعد الإصدار، **يجب** أن يقوم نظام التفتيش بما يلي بالنسبة لكل مادة من مواد البيانات المكتوبة:

١) **يجب** أن يقوم نظام التفتيش بإنشاء مسار لإصدار الشهادات والتحقق من صحته، يبدأ من الكيان الجدير بالثقة إلى شهادة الجهة الموقّعة المستخدمة لتوقيع مادة البيانات وفقاً للوثيقة Doc 9303-12. و**يجوز** لنظام التفتيش أن يستخدم الشهادتين المعروفتين سلفاً والشهادات المستعادة من الرقاقة لإنشاء المسار (انظر الوثيقة Doc 9303-10).

٢) **يجب** على نظام التفتيش أن يستخدم المفتاح العام الذي تم التحقق منه للجهة الموقعة للتحقق من توقيع مادة البيانات.

ملاحظة — يمكن أن تتخطى هذا الإجراء مواد البيانات التي لا تعتبر ذات صلة بعملية التفتيش التي تقوم بها الدولة أو المنظمة المستقبِلة.

٦- التحقق من صحة الدائرة المتكاملة اللاتلامسية

يجوز لأي دولة أو منظمة إصدار أن تختار حماية وثائقها الإلكترونية المقروءة آلياً من استبدال الرقاقة.

تتوافر الآليات التالية للتحقق من صحة الرقاقة.

١) *التحقق الإيجابي من الصحة*، حسب ما هو معرَّف في القسم ٦-١ دعم التحقق الإيجابي من الصحة يدل عليه وجود EF.DG15. وإذا توافر، **يجوز** للوحدة الطرفية قراءة والتحقق من EF.DG15 وإجراء التحقق الإيجابي من الصحة.

٢) *التحقق من صحة الرقاقة*، حسب ما هو معرَّف في القسم ٦-٢ دعم التحقق من صحة الرقاقة يبيّنه وجود `SecurityInfos` (معلومات أمنية) مناظرة في EF.DG14/EF.CardSecurity. و**يجوز** للوحدة الطرفية، إذا توافرت، قراءة والتحقق من EF.DG14/EF.CardSecurity وأداء تحقق من صحة الرقاقة.

٣) فتح الاتصال بكلمة سر مصدّق عليها مع *تحديد المجالات للتحقق من صحة الرقاقة* (PACE-CAM) على النحو المعرَّف في القسم ٤-٤. والدعم مبيّن بوجود بنية `PACEInfo` مناظرة في الاطلاع على البطاقة EF.CardAccess. وإذا تم بنجاح أداء فتح الاتصال بكلمة سر مصدّق عليها – تحديد المجالات للتحقق من صحة الرقاقة في إجراءات الاطلاع على الرقاقة، **يجوز** للوحدة الطرفية أداء ما يلي للتحقق من صحة الرقاقة:

- قراءة والتحقق من أمن البطاقة EF.CardSecurity.
- استخدام مفتاح عام من أمن البطاقة مع بيانات تحديد المجالات وبيانات التحقق من صحة الرقاقة المستلمة كجزء من فتح الاتصال بكلمة سر مصدّق عليها – تحديد المجالات للتحقق من صحة الرقاقة وذلك للتحقق من صحة الرقاقة (القسم ٤-٤-٣-٥-٢).

٦-١ التحقق الإيجابي من الصحة

التحقق الإيجابي من الصحة يتحقق من صحة الدائرة المتكاملة اللاتلامسية عن طريق التوقيع على تحدٍّ مرسلٍ من جهاز التوصيل (جهاز التفتيش) مع مفتاح خاص معروف للدائرة المتكاملة فقط.

لهذا الغرض تحتوي الدائرة المتكاملة اللاتلامسية على زوجها الخاص من مفاتيح التحقق الإيجابي من الصحة (KPr_{AA} and KPu_{AA}). ويُخزن تمثيل بالبصمات الرقمية لمجموعة البيانات ١٥ (معلومات المفتاح العام) (KPu_{AA}) في المادة الأمنية للوثيقة (SO_D) ولذلك يتم التحقق من صحته بواسطة التوقيع الرقمي لجهة الاصدار. ويُخزن المفتاح الخاص المناظر (KPr_{AA}) في الذاكرة المؤمّنة للدائرة المتكاملة اللاتلامسية.

عن طريق التحقق من صحة الجزء المقروء آلياً البصري (عن طريق الجزء المقروء آلياً ذي البصمة الرقمية في المادة الأمنية للوثيقة (SO_D)) بالاقتران مع الاستجابة للتحدي، باستخدام زوج مفاتيح التحقق الإيجابي من الصحة لوثيقة السفر الإلكترونية المقروءة آلياً (KPr_{AA} and KPu_{AA})، يتحقق نظام التفتيش من أن المادة الأمنية للوثيقة (SO_D) قد قُرئت من دائرة متكاملة لاتلامسية حقيقية، مخزّنة في وثيقة سفر إلكترونية مقروءة آلياً حقيقية.

يتطلب التحقق الإيجابي من الصحة قدرات لمعالجة الدائرة المتكاملة اللاتلامسية لوثيقة السفر الإلكترونية المقروءة آلياً.

٦-١-١ *مواصفة البروتوكول*

يتم التحقق الإيجابي من الصحة باستخدام INTERNAL AUTHENTICATE command [ISO/IEC 7816-4].

إذا تم التحقق الإيجابي من الصحة بعد إثبات المراسلات المأمونة، **يجب** إرسال جميع الأوامر والاستجابات كمراسلات مأمونة كوحدات بيانات بروتوكول التطبيق وفقاً للقسم ٩-٨.

بمزيد من التفصيل، فإن جهاز التوصيل (جهاز التفتيش) والدائرة المتكاملة (الدائرة المتكاملة اللاتلامسية لوثيقة السفر الإلكترونية المقروءة آلياً) يقومان بالخطوات التالية:

١) يصدر جهاز التوصيل رقماً يُستخدم مرة واحدة RND.IFD ويرسله إلى الدائرة المتكاملة باستخدام الأمر INTERNAL AUTHENTICATE.

٢) تقوم الدائرة المتكاملة بالعمليات التالية:

أ) إصدار الرسالة M؛

ب) حساب h(M)؛

ج) حساب التوقيع σ وإرسال الاستجابة إلى جهاز التوصيل.

٣) يتحقق جهاز التوصيل من الاستجابة للأمر المرسَل INTERNAL AUTHENTICATE ويتحقق مما إذا كانت الدائرة المتكاملة قد عادت إلى القيمة الصحيحة.

٦-١-٢ *مواصفات علم الشيفرة*

٦-١-٢-١ *الرقم الذي يُستخدم مرة واحدة*

المُدخل هو رقم يُستخدم مرة واحدة (RND.IFD) **يجب** أن يكون ٨ بايتات.

*ملاحظة — **يجب ألا** يعاد استخدام الأرقام التي تُستخدم مرة واحدة، مثلاً الرقم الذي يُستخدم مرة واحدة من أجل مراقبة الوصول الأساسي/فتح الاتصال بكلمة سر مصدّق عليها **يجب ألا** يعاد استخدامه من أجل التحقق الإيجابي من الصحة.*

٦-١-٢-٢ *رفست وشمير وأدلمن*

يجب أن تحسب الدائرة المتكاملة توقيعاً، عند استخدام آلية قائمة على تحليل عدد صحيح إلى عوامل، وفقاً لـ [ISO/IEC 9796-2] خطة التوقيع الرقمي ١.

فيما يلي، k يدل على طول المفتاح لإنتاج التوقيع ويدل L_h على طول ناتج وظيفة البصمة الرقمية H المستخدمة خلال صنع التوقيع. و**يجب** استخدام خيار الخانة الملحقة ١ (وضبط t على ١) إذا استُخدمت SHA-1 خلال صنع التوقيع، **يجب** أن يُستخدم بدلاً عن ذلك خيار الخانة الملحقة ٢ (وضبط t على ٢).

و**يجب** أن تستخدم القيم التالية للخانة الملحقة بالنسبة للخيار ٢:

Hash function	SHA-224	SHA-256	SHA-384	SHA-512
Trailer field	0x38CC	0x34CC	0x36CC	0x35CC

ولأسباب تتعلق بالتشغيل المتبادل، يتم فقط دعم SHA-1 وSHA-224 وSHA-256 وSHA-384 وSHA-512 باعتبارها دوال بصمات رقمية للتحقق الفعال بواسطة ريفست وشمير وأدلمان.

الرسالة M التي يتعين التوقيع عليها **يجب** أن تكون سلسلة لـ M1 و M2، حيث **يجب** أن تكون M1 رقماً يُستخدم مرة واحدة طوله c - 4 بيتات (RND.IC) صنعته وثيقة السفر الإلكترونية المقروءة آلياً، حيث c *(القدرة الاستيعابية للتوقيع)* معطاة عن طريق $c = k - L_h - (8 \times t) - 4$، و M2 هي RND.IFD من صنع جهاز التفتيش.

نتيجة حساب التوقيع **يجب** أن تكون توقيعاً σ بدون جزء الرسالة غير القابل للاسترداد M2.

ينبغي أن تنفّذ وثائق السفر الإلكترونية المقروءة آلياً خطة صنع التوقيع المحددة في [ISO/IEC 9796-2] الفقرة B.6 و**لا ينبغي** أن تستفيد من خطة صنع التوقيع المحددة في [ISO/IEC 9796-2] الفقرة B.4. و**يجب ألا** تنفّذ وثائق السفر الإلكترونية المقروءة آلياً خططاً أخرى لصنع التوقيع.

يجب أن تنفّذ أجهزة التفتيش خطة صنع التوقيع المحددة في [ISO/IEC 9796-2] الفقرة B.6 و**ينبغي** أن تنفّذ خطة صنع التوقيع المحددة في [ISO/IEC 9796-2] الفقرة B.4.

٦-١-٢-٣ *خوارزمية التوقيع الرقمي للمنحنى الاهليلجي*

بالنسبة لخوارزمية التوقيع الرقمي للمنحنى الاهليلجي، **يجب** استخدام شكل التوقيع البسيط وفقاً لـ [TR-03111]. و**يجب** أن تُستخدم فقط منحنيات أولية ذات نقاط غير مضغوطة. و**يجب** أن تُستخدم خوارزمية بصمة رقمية، طولها المُخرج هو نفس طول أو أقصر من طول المفتاح المُستخدم لخوارزمية التوقيع الرقمي للمنحنى الاهليلجي. ويتم فقط دعم SHA-224 وSHA-256 وSHA-384 وSHA-512 باعتبارها دوال بصمات رقمية. **ويجب عدم** استخدام RIPEMD-160 وSHA-1.

الرسالة M التي يتعين التوقيع عليها هي الرقم الذي يُستخدم مرة واحدة RND.IFD الذي يوفّره جهاز التفتيش.

٦-١-٣ ***وحدات بيانات بروتوكول التطبيق***

يؤدى التحقق الإيجابي من الصحة عن طريق استدعاء واحد للأمر INTERNAL AUTHENTICATE حسبما هو محدد في [ISO/IEC 7816-4].

Command			
CLA		Context specific	
INS	0x88	INTERNAL AUTHENTICATE	
P1/P2	0x0000	--	
Data		*RND.IFD*	REQUIRED
Response			

Data		Signature σ generated by the IC	REQUIRED
Status Bytes	0x9000	*Normal processing* The protocol has been performed successfully.	
	Other	*Operating system dependent error* The protocol failed.	

٦-١-٤ مفاتيح التحقق الإيجابي من الصحة

يجب أن يتم بطريقة مأمونة صنع زوج مفتاحي التحقق الإيجابي من الصحة (KPr_{AA} and KPu_{AA}).

يُخزن كل من المفتاح العام للتحقق الإيجابي من الصحة (KPu_{AA}) والمفتاح الخاص للتحقق الإيجابي من الصحة (KPr_{AA}) في الدائرة المتكاملة اللاتلامسية لوثيقة السفر الإلكترونية المقروءة آلياً. وبعد ذلك، لا تنطبق أي إدارة مفاتيح لهذين المفتاحين.

ملاحظة — ينبغي ملاحظة أنه عند استخدام أطوال مفاتيح تتجاوز ١ ٨٤٨ بتات (إذا استُخدمت المراسلة المؤمّنة بواسطة القاعدة القياسية ٣ لتشفير البيانات) / ١ ٧٩٢ بتات (إذا استُخدمت المراسلة المؤمّنة بواسطة القاعدة القياسية للتشفير المتقدم) في التحقق الإيجابي من الصحة بواسطة المراسلة المؤمّنة، فإن وحدات بيانات بروتوكول التطبيق ذات الطول الممدد **يجب** *أن تدعمها رقاقة وثيقة السفر الإلكترونية المقروءة آلياً وجهاز التفتيش.*

يجب أن تختار دول أو منظمات الاصدار أطوال مفاتيح ملائمة تتيح الحماية من الهجمات طوال عمر وثيقة السفر الإلكترونية المقروءة آلياً. و**ينبغي** أن تؤخذ بعين الاعتبار كتالوجات التشفير المناسبة.

٦-١-٥ معلومات المفتاح العام للتحقق الإيجابي من الصحة

يُخزَّن المفتاح العام للتحقق الإيجابي من الصحة في المجموعة ١٥ لبيانات بنية البيانات المنطقية. وشكل البنية (`SubjectPublicKeyInfo`) محدد في [RFC 5280]، انظر القسم ٩-١. و**يجب** إنتاج جميع المواد الأمنية في شكل قاعدة التشفير المميّز (DER) للحفاظ على سلامة التوقيعات داخلها.

```
ActiveAuthenticationPublicKeyInfo ::= SubjectPublicKeyInfo
```

٦-١-٦ عملية التفتيش

عند عرض وثيقة سفر إلكترونية مقروءة آلياً مع مجموعة البيانات ١٥ على جهاز التفتيش، **يجوز** أداء آلية التحقق الإيجابي من الصحة لضمان أن البيانات تُقرأ من دائرة متكاملة لاتلامسية حقيقية وأن الدائرة المتكاملة اللاتلامسية والوثيقة المادية تنتميان كل منهما إلى الأخرى.

يؤدي جهاز التفتيش والدائرة المتكاملة اللاتلامسية الخطوات التالية:

١) يُقرأ الجزء المقروء آلياً بأكمله بصرياً من وثيقة السفر الإلكترونية المقروءة آلياً (إذا لم يُقرأ بالفعل كجزء من إجراءات مراقبة الوصول الأساسي) ويُقارن بقيمة الجزء المقروء آلياً في مجموعة البيانات ١. ونظراً لأن صحة وسلامة مجموعة البيانات ١ تم التحقق منهما من خلال التحقق السلبي من الصحة، بالمثل يضمن أن الجزء المقروء آلياً البصري صحيح ولم يتم تغييره.

٢) أثبت التحقق السلبي من الصحة أيضاً صحة وسلامة مجموعة البيانات ١٥. وهذا يضمن أن المفتاح العام للتحقق الإيجابي من الصحة (KPu_{AA}) صحيح ولم يتم تغييره).

٣) لضمان أن المادة الأمنية للوثيقة (SO_D) ليست نسخة، يستخدم جهاز التفتيش زوج مفاتيح التحقق الإيجابي من الصحة لوثيقة السفر الإلكترونية المقروءة آلياً (KPr_{AA} and KPu_{AA}) في بروتوكول للاستجابة للتحدي مع الدائرة المتكاملة اللاتلامسية لوثيقة السفر الإلكترونية المقروءة آلياً على النحو الموصوف أعلاه.

بعد تشغيل بروتوكول الاستجابة للتحدي بنجاح، يُثبت أن المادة الأمنية للوثيقة (SO_D) تنتمي إلى الوثيقة المادية وأن الدائرة المتكاملة اللاتلامسية حقيقية والدائرة المتكاملة اللاتلامسية والوثيقة المادية تنتمي كل منهما إلى الأخرى.

٦-٢ التحقق من صحة الرقاقة

بروتوكول التحقق من صحة الرقاقة هو بروتوكول اتفاق مفتاح ديفي-هيلمان سريع الزوال/ساكن يوفّر اتصالاً آمناً وتحققاً من طرف واحد من صحة رقاقة وثيقة السفر الإلكترونية المقروءة آلياً.

الاختلافان الرئيسيان عن التحقق الإيجابي من الصحة هما:

- يتم منع دلالات التحدي لأن النسخ التي يُنتجها هذا البروتوكول غير قابلة للتحويل.
- إلى جانب التحقق من صحة رقاقة وثيقة السفر الإلكترونية المقروءة آلياً يوفّر هذا البروتوكول أيضاً مفاتيح دورات زمنية قوية.

يرد في المرفق (ج) وصف تفاصيل دلالات التحدي.

يجب تخزين زوج (أزواج) مفاتيح التحقق السكوني من صحة الرقاقة على رقاقة وثيقة السفر الإلكترونية المقروءة آلياً.

- **يجب** تخزين المفتاح الخاص بشكل مأمون في ذاكرة رقاقة وثيقة السفر الإلكترونية المقروءة آلياً.
- **يجب** توفير المفتاح العام بوصفه `SubjectPublicKeyInfo` في بنية `ChipAuthenticationPublicKeyInfo` (انظر القسم ٩-٢-٦).

يوفّر البروتوكول تحققاً ضمنياً من صحة كل من رقاقة وثيقة السفر الإلكترونية المقروءة آلياً ذاتها والبيانات المخزونة بواسطة أداء المراسلة المأمونة باستخدام مفاتيح الدورات الزمنية الجديدة.

وإذا كانت الدائرة المتكاملة تدعم التحقق من صحة الرقاقة، **يجوز** للدائرة المتكاملة أن تدعم التحقق من صحة الرقاقة في الملف الرئيسي و/أو **يجوز** لها أن تدعم التحقق من صحة الرقاقة في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً. وإذا استخدم التحقق من صحة الرقاقة بالترافق مع الاطلاع على مجموعات البيانات في تطبيقات LDS2، **يجب** على الدائرة المتكاملة أن تدعم التحقق من صحة الرقاقة في الملف الرئيسي.

*ملاحظة — إذا كان التوافق مع مراقبة الاطلاع الموسّعة للاتحاد الأوروبي (TR-03110) مطلوباً، **يجب** على الدائرة المتكاملة أن تدعم التحقق من صحة الرقاقة في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً.*

حيث أن تطبيق وثيقة السفر الإلكترونية المقروءة آلياً يتم اختياره نتيجة لإجراءات الوصول إلى الرقاقة، يتم أداء التحقق من صحة الرقاقة في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً.

٦-٢-١ *مواصفة البروتوكول*

تؤدي الوحدة الطرفية ورقاقة وثيقة السفر الإلكترونية المقروءة آلياً الخطوات التالية.

١) ترسل رقاقة وثيقة السفر الإلكترونية المقروءة آلياً مفتاحها العام السكوني ديفي-هيلمان PK_{IC}، ومعايير النطاق D_{IC} إلى الوحدة الطرفية.

٢) تصنع الوحدة الطرفية زوجاً سريع الزوال من مفاتيح ديفي–هيلمان $(SK_{DH,IFD}, PK_{DH.IFD}, D_{IC})$ وترسل المفتاح العام سريع الزوال $PK_{DH,IFD}$ إلى رقاقة وثيقة السفر الإلكترونية المقروءة آلياً.

٣) يحب كل من رقاقة وثيقة السفر الإلكترونية المقروءة آلياً والوحدة الطرفية ما يلي:

أ) الحرف K السرّي المشترك $\mathbf{KA}(SK_{IC}, PK_{DH,IFD}, D_{IC}) = \mathbf{KA}(SK_{DH,IFD}, PK_{IC}, D_{IC})$ =.

ب) مفاتيح الدورات الزمنية $KS_{MAC} = \mathbf{KDF}_{MAC}(K)$ and $KS_{Enc} = \mathbf{KDF}_{Enc}(K)$ المستمدة من K من أجل المراسلات المأمونة.

تبيَّن نسخة مبسّطة في الشكل ٣:

IC (chip)		***IFD (Inspection system)***
Static key pair $(SK_{IC}, PK_{IC}, D_{IC})$		
	— PK_{IC}, D_{IC} →	
		Choose random ephemeral key pair $(SK_{DH,IFD}, PK_{DH,IFD}, D_{IC})$
	← $PK_{DH,IFD}$ —	
$K = \mathbf{KA}(SK_{IC}, PK_{DH,IFD}, D_{IC})$		$K = \mathbf{KA}(SK_{DH,IFD}, PK_{IC}, D_{IC})$

الشكل ٣ التحقق من صحة الرقاقة

للتحقق من صحة الـ PK_{IC} **يجب** أن تؤدي الوحدة الطرفية التحقق السلبي من الصحة.

٦-٢-٢ *الوضع الأمني*

إذا تم بنجاح أداء التحقق من صحة الرقاقة، يعاد تشغيل المراسلات المأمونة باستخدام مفتاحي الدورات الزمنية المستمدين KS_{MAC} و KS_{Enc}. وبخلاف ذلك، تواصَل المراسلات المأمونة باستخدام مفتاحي الدورات الزمنية المؤسسين (فتح الاتصال بكلمة سر مصدّق عليها أو مراقبة الوصول الأساسي).

*ملاحظة — **يجب** أداء التحقق السلبي من الصحة بالاقتران مع التحقق من صحة الرقاقة. ولا يجوز اعتبار رقاقة وثيقة السفر الإلكترونية المقروءة آلياً حقيقية إلا بعد مصادقة ناجحة على المادة الأمنية الخاصة بها.*

٦-٢-٣ *مواصفات التشفير*

تقوم دولة أو منظمة الإصدار باختيار خوارزميات معيّنة. و**يجب** أن يدعم نظام التفتيش جميع التركيبات الموصوفة في الأقسام الفرعية التالية. و**يجوز** أن تدعم رقاقة وثيقة السفر الإلكترونية المقروءة آلياً أكثر من توليفة واحدة للخوارزميات.

٦-٢-٣-١ *التحقق من صحة الرقاقة ببروتوكول ديفي–هيلمان*

بالنسبة للتحقق من صحة الرقاقة ببروتوكول ديفي–هيلمان **يجب** استخدام الخوارزميات والأشكال ذات الصلة من القسم ٩-٦ والجدول ٥. وبالنسبة للمفاتيح العامة، **يجب** استخدام PKCS#3 [PKCS#3] بدلاً عن X9.42 [X9.42].

الجدول ٥ — معرّفات البنود للتحقق من صحة الرقاقة ببروتوكول ديفي–هيلمان

OID	***Sym. Cipher***	***Key Length***	***Secure Messaging***
id-CA-DH-3DES-CBC-CBC	3DES	112	CBC / CBC
id-CA-DH-AES-CBC-CMAC-128	AES	128	CBC / CMAC

id-CA-DH-AES-CBC-CMAC-192	AES	192	CBC / CMAC
id-CA-DH-AES-CBC-CMAC-256	AES	256	CBC / CMAC

٦-٢-٣-٢ *التحقق من صحة الرقاقة ببروتوكول ديفي–هيلمان للمنحنى الاهليلجي*

للتحقق من صحة الرقاقة ببروتوكول ديفي–هيلمان للمنحنى الاهليلجي **يجب** استخدام الخوارزميات والأشكال ذات الصلة من القسم ٦-٩ والجدول ٦.

الجدول ٦ — معرّفات البنود للتحقق من صحة الرقاقة ببروتوكول ديفي–هيلمان للمنحنى الاهليلجي

OID	***Sym. Cipher***	***Key Length***	***Secure Messaging***
id-CA-ECDH-3DES-CBC-CBC	3DES	112	CBC / CBC
id-CA-ECDH-AES-CBC-CMAC-128	AES	128	CBC / CMAC
id-CA-ECDH-AES-CBC-CMAC-192	AES	192	CBC / CMAC
id-CA-ECDH-AES-CBC-CMAC-256	AES	256	CBC / CMAC

٦-٢-٤ *تطبيقات وحدات بيانات البروتوكول*

حسب الخوارزمية التماثلية التي تُستخدم، يتوافر تنفيذان للتحقق من صحة الرقاقة.

- **يجب** استخدام الأمر التالي لتنفيذ التحقق من صحة الرقاقة عن طريق المراسلات المأمونة بالتشفير الثلاثي للبيانات:

  ١- MSE:Set KAT.

- **يجب** استخدام السلسلة التالية من الأوامر لتنفيذ التحقق من صحة الرقاقة بالمراسلات المأمونة للقاعدة القياسية للتشفير المتقدم و**يجوز** استخدامها لتنفيذ التحقق من صحة الرقاقة بالمراسلات المأمونة عن طريق التشفير الثلاثي للبيانات:

  ١- MSE:Set AT.

  ٢- GENERAL AUTHENTICATE

٦-٢-٤-١ *التنفيذ باستخدام MSE:Set KAT*

ملاحظة — MSE:Set KAT يجوز استخدامها فقط من أجل id-CA-DH-3DES-CBC-CBC و -id-CA-ECDH-3DES-CBC-CBC، أي أن المراسلة المأمونة مقتصرة على التشفير الثلاثي للبيانات.

Command		
CLA		Context specific
INS	0x22	Manage Security Environment
P1/P2	0x41A6	Set Key Agreement Template for computation.

Data	0x91	*Ephemeral Public Key* Ephemeral public key $PK_{DH,IFD}$ (cf. Section 9.4.5) encoded as plain public key value.	REQUIRED
	0x84	*Reference of a private key* This data object is REQUIRED if the private key is ambiguous, i.e. more than one key pair is available for Chip Authentication (cf. Section 6.2 and 9.2.6).	CONDITIONAL
Response			
Data	–	Absent	
Status Bytes	0x9000	*Normal processing* The key agreement operation was successfully performed. New session keys have been derived.	
	0x6A80	*Incorrect Parameters in the command data field* The validation of the ephemeral public key failed.	
	other	*Operating system dependent error* The previously established session keys remain valid.	

٦-٢-٤-٢ *التنفيذ باستخدام MSE:Set AT و*GENERAL AUTHENTICATE

١- **MSE:Set AT:** الأمر MSE:Set AT يُستخدم لاختيار وبدء البروتوكول. واستخدام الأمر MSE:Set AT للتحقق من صحة الرقاقة يبينه معرّف مادة التحقق من صحة الرقاقة (انظر القسمين ٦-٢-٣ و٩-٢-٧) الوارد كمرجع لآلية التشفير بالوسم tag 0x80، انظر الجدول أدناه.

Command			
CLA		Context specific	
INS	0x22	Manage Security Environment	
P1/P2	0x41A4	*Chip Authentication*: Set Authentication Template for internal authentication.	
Data	0x80	*Cryptographic mechanism reference* Object Identifier of the protocol to select (value only, Tag 0x06 is omitted).	REQUIRED
	0x84	*Reference of a private key* This data object is REQUIRED to indicate the identifier of the private key to be used if the private key is ambiguous, i.e. more than one private key is available for Chip Authentication.	CONDITIONAL
Response			
Data	–	Absent	
Status Bytes	0x9000	*Normal processing* The protocol has been selected and initialized.	
	0x6A80	*Incorrect parameters in the command data field* Algorithm not supported or initialization failed.	
	0x6A88	*Referenced data not found* The referenced data (i.e. private key) is not available.	

	other	*Operating system dependent error* The initialization of the protocol failed.

ملاحظة — بعض أنظمة التشغيل تقبل اختيار مفتاح غير متوافر والعودة إلى خطأ فقط عندما يُستخدم المفتاح للغرض المختار.

٢- **GENERAL AUTHENTICATE:** يُستخدم الأمر GENERAL AUTHENTICATE لأداء التحقق من صحة الرقاقة.

Command				
CLA		Context specific		
INS	0x86	GENERAL AUTHENTICATE		
P1/P2	0x0000	Keys and protocol implicitly known.		
Data	0x7C	*Dynamic Authentication Data* Protocol specific data objects.		REQUIRED
		0x80	Ephemeral Public Key	
Response				
Data	0x7C	*Dynamic Authentication Data* Protocol specific data objects		REQUIRED
Status Bytes	0x9000	*Normal processing* The protocol (step) was successful.		
	0x6300	*Authentication failed* The protocol (step) failed.		
	0x6A80	*Incorrect parameters in data field* Provided data is invalid.		
	0x6A88	*Referenced data not found* The referenced data (i.e. private key) is not available.		
	other	*Operating system dependent error* The protocol (step) failed.		

ملاحظة — المفاتيح العامة للتحقق من صحة الرقاقة المدعومة بالرقاقة يتم توفيرها في المادة الأمنية (انظر القسم ٩-٢-١١).
*وإذا كان يُدعم أكثر من مفتاح عام واحد، **يجب** أن تختار الوحدة الطرفية المفتاح الخاص المناظر للرقاقة التي تُستخدم داخل MSE:Set AT.*

٦-٢-٤-٣ *المفتاح العام سريع الزوال*

يجب ترميز المفاتيح العامة سريعة الزوال (راجع القسم ٩-٤-٥) كنقطة منحنى اهليلجي (بروتوكول ديفي-هيلمان للمنحنى الاهليلجي) أو عدد صحيح غير موقّع (بروتوكول ديفي-هيلمان).

٧- آليات مراقبة الوصول الإضافية

البيانات الشخصية المخزّنة في الدائرة المتكاملة اللاتلامسية حسبما تُعرَّف بأنها الحد الأدنى الالزامي للتشغيل المتبادل العالمي هي الجزء المقروء آلياً والصورة المخزّنة رقمياً لوجه حامل الوثيقة. وكلا الشيئين يمكن أيضاً رؤيتهما (قراءتهما) بصرياً بعد فتح وثيقة السفر الإلكترونية المقروءة آلياً وعرضها للتفتيش.

إلى جانب الصورة المخزّنة رقمياً للوجه بوصفها سمة الاستدلال البيولوجي الأولية للتشغيل المتبادل العالمي، أقرّت الايكاو استخدام الصور المخزّنة رقمياً للأصابع و/أو مخططات الحدقات بالإضافة إلى الوجه. وبالنسبة للاستخدام الوطني أو الثنائي الأطراف، **يجوز** للدول اختيار تخزين نماذج و/أو **يجوز** أن تختار حداً للوصول أو تشفير هذه البيانات، حسب ما تقرره الدول أنفسها.

ينبغي للوصول إلى هذه البيانات الشخصية الأكثر حساسية أن يكون أكثر تقييداً. ويمكن تحقيق هذا بطريقتين: المراقبة الموسّعة للوصول أو تشفير البيانات. ويحدد القسم ٧-١ التحقق من صحة الوحدة الطرفية كآلية قابلة للتشغيل المتبادل للمراقبة الموسعة للوصول. وإذا لم تكن قابلية التشغيل المتبادل مطلوبة، يمكن استخدام آليات أخرى.

٧-١ التحقق من صحة الوحدة الطرفية

آلية التحقق من صحة الوحدة الطرفية هي آلية **مشروطة**. ويعتبر التنفيذ **مطلوباً** بالنسبة لتطبيقات LDS2. و**يمكن** استخدام التحقق من صحة الوحدة الطرفية لحماية سمات الاستدلال البيولوجي الثانوية في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً.

وبروتوكول التحقق من صحة الوحدة الطرفية هو بروتوكول استجواب وإجابة من حركتين يوفر التحقق الصريح والأحادي الجانب من صحة الوحدة الطرفية ويقوم البروتوكول على مراقبة الوصول الموسعة على النحو المحدد في [TR-03110]. وإذا كان هذا البروتوكول مدعوماً من الدائرة المتكاملة، **يجب** أن يدعم التحقق من صحة الرقاقة أو فتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات للتحقق من صحة الرقاقة.

يمكّن البروتوكول الدائرة المتكاملة من التحقق من أن للوحدة الطرفية الحق في الاطلاع على البيانات الحساسة. وبما أن بإمكان الوحدة الطرفية الاطلاع على البيانات الحساسية فيما بعد، **يجب** أن تكون جميع الاتصالات الأخرى محمية بصورة مناسبة. لذلك فإن التحقق من صحة الوحدة الطرفية يقوم أيضاً بالتحقق من صحة مفتاح عام سريع الزوال قامت باختياره الوحدة الطرفية التي استخدمت لإعداد مراسلات مأمونة مع تحقق من صحة الرقاقة أو فتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات للتحقق من صحة الرقاقة. و**يجب** على الدائرة المتكاملة أن تربط حقوق اطلاع الوحدة الطرفية على المراسلات المأمونة التي حددها المفتاح العام سريع الزوال لوحدة الطرفية الذي تم التحقق من صحته.

و**يجوز** للدائرة المتكاملة أن تدعم التحقق من صحة الوحدة الطرفية في الملف الرئيسي و/أو تطبيق وثيقة السفر الإلكترونية المقروءة آلياً. وفي حال استخدام التحقق من صحة الوحدة الطرفية من أجل حماية مجموعات البيانات في تطبيقات أخرى خلاف تطبيق وثيقة السفر الإلكترونية المقروءة آلياً، **يجب** على الدائرة المتكاملة أن تدعم التحقق من صحة الوحدة الطرفية في الملف الرئيسي.

*ملاحظة — إذا كان التوافق مع مراقبة الاطلاع الموسّعة للاتحاد الأوروبي (TR-03110) مطلوباً، **يجب** على الدائرة المتكاملة أن تدعم التحقق من صحة الرقاقة في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً.*

٧-١-٢ *مواصفة البروتوكول*

تقوم الوحدة الطرفية والدائرة المتكاملة بالخطوات التالية:

١- ترسل الوحدة الطرفية سلسلة شهادات إلى الدائرة المتكاملة. تبدأ السلسلة بشهادة يمكن التحقق منها بواسطة المفتاح العام للسلطة الوطنية المعنية بالتحقق من الشهادات المخزّن على الرقاقة وتنتهي بشهادة الوحدة الطرفية.

٢- تتحقق الدائرة المتكاملة من الشهادات وتستخلص المفتاح العام للوحدة الطرفية PK_{IFD}.

٣- تختار الدائرة المتكاملة لطريقة عشوائية تحدياً r_{IC} وترسله إلى الوحدة الطرفية.

٤- تستجيب الوحدة الطرفية بالتوقيع s_{IFD} = **Sign**$(SK_{IFD}, ID_{IC}||r_{IC}||$**Comp**$(PK_{DH,IFD}))$.

٥- تتحقق الدائرة المتكاملة من أن **Verify**$(PK_{IFD}, s_{IFD}, ID_{IC}||r_{IC}||$**Comp**$(PKDH,IFD)) = true$.

*ملاحظة — يتولد المفتاح $PK_{DH,IFD}$ أثناء التحقق من صحة الرقاقة أو فتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات للتحقق من صحة الرقاقة. وإذا تم توليد أكثر من مفتاح واحد (مثلاً إذا تم إجراء التحقق من صحة الرقاقة بعد فتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات للتحقق من صحة الرقاقة)، **يجب** استخدام المفتاح الأحدث.*

في هذا البروتوكول، ID_{IC} هو أحد معرفات الدائرة المتكاملة.

- إذا استخدمت مراقبة الوصول الأساسية، يكون ID_{IC} رقم وثيقة السفر الإلكترونية المقروءة آلياً كما ورد في الجزء المقروء آلياً بما في ذلك رقم التدقيق.
- إذا استخدم فتح الاتصال بكلمة سر مصدّق عليها، يحسب ID_{IC} باستخدام المفتاح العام سريع الزوال لفتح الاتصال بكلمة سر مصدّق عليها، أي ID_{IC} = **Comp**$(PK_{DH,IC})$.

*ملاحظة — يكون التنفيذ الناجح لبروتوكول فتح الاتصال بكلمة سر مصدّق عليها **مطلوباً** قبل إجراء التحقق من صحة الوحدة الطرفية في الملف الرئيسي.*

وتظهر أدناه نسخة مبسطة:

IC (chip)		**IFD (inspection system)**
Choose r_{IC} randomly		
	— r_{IC} →	
		s_{IFD} = **Sign**$(SK_{IFD},ID_{IC}\|\|r_{IC}\|\|$**Comp**$(PK_{DH,IFD}))$
	← s_{IFD} —-	
Verify$(PK_{IFD}, s_{IFD}, ID_{IC}\|\|r_{IC}\|\|$**Comp**$(PK_{DH,IFD})) = true$		

الشكل ٤ التحقق من صحة الوحدة الطرفية

٧-١-٣ حالة الأمن

إذا تم التحقق من صحة الوحدة الطرفية بنجاح، **يجب** على الدائرة المتكاملة أن تمنح الوصول إلى البيانات الحساسة المخزنة وفقاً للترخيص الفعال للوحدة الطرفية التي تم التحقق منها. وإذا لم يمنح الترخيص الفعال حق الوصول إلى أي بيانات في تطبيق LDS2، **يجب** على الدائرة المتكاملة أن ترفض اختيار هذا التطبيق.

ومع ذلك، **يجب** على الدائرة المتكاملة أن تقصر حقوق الوصول على المراسلات الآمنة التي يحددها المفتاح العام سريع الزوال الذي تم التحقق منه، أي المفتاح العام سريع الزوال الذي توفره الوحدة الطرفية كجزء من التحقق من صحة الرقاقة أو فتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات للتحقق من صحة الرقاقة. و**يجب ألا** تقبل الدائرة المتكاملة أكثر من تنفيذ واحد للتحقق من صحة الوحدة الطرفية ضمن الدورة الزمنية نفسها (راجع القسم ٩-٨-١ والقسم ٩-٨-٣ بشأن تعريف "الدورة الزمنية").

الملاحظة ١ — تكون حقوق الوصول صالحة ما دامت المراسلات الآمنة التي يحددها المفتاح العام سريع الزوال الذي تم التحقق منه فاعلة، ولذلك لا تتأثر حالة الأمن باختيار أو عدم اختيار التطبيقات.

*الملاحظة ٢ — لا تتأثر المراسلات الآمنة بالتحقق من صحة الوحدة الطرفية. و***يجب** *على رقاقة وثيقة السفر الإلكترونية المقروءة آلياً أن تحتفظ بالمراسلات الآمنة حتى ولو فشل التحقق من صحة الوحدة الطرفية (إلا إذا حدث خطأ في المراسلات الآمنة).*

٧-١-٤ المواصفات الفنية المشفرة

٧-١-٤-١ التحقق من صحة الوحدة الطرفية بمراقبة الوصول الأساسية

بالنسبة للتحقق من صحة الوحدة الطرفية بمراقبة الوصول الأساسية، **يجب** استخدام الخوارزميات والأشكال التالية:

٧-١-٤-١-١ خوارزمية التوقيع

يجب استخدام مراقبة الوصول الأساسية [PKCS#1] ,[RFC-3447] كما هي محددة في الجدول ٧.

الجدول ٧ — معرّفات المواد من أجل التحقق من صحة الوحدة الطرفية بواسطة مراقبة الوصول الأساسية

OID	Signature	Hash	Parameters
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	default
id-TA-RSA-PSS-SHA-512	RSASSA-PSS	SHA-512	default

وتعرّف البارامترات الأصلية المقرر استخدامها مع مراقبة الوصول الأساسية – خطة التواقيع الاحتمالية كما يلي:

- خوارزمية البصمة الرقمية: يتم اختيار خوارزمية البصمة الرقمية وفقاً للجدول ٧.
- خوارزمية توليد القناع: MGF1 [PKCS#1] ,[RFC-3447] باستخدام خوارزمية البصمة الرقمية التي تم اختيارها.
- طول "سولت": الطول بالثمانيات لخرج خوارزمية البصمة الرقمية التي تم اختيارها.
- الخانة الملحقة: 0xBC.

٧-١-٤-١-٢ شكل المفتاح العام

يجب استخدام الشكل TLV [ISO/IEC 7816-8] كما هو محدد في الوثيقة Doc 9303-12.

- **يجب** أن يؤخذ معرّف المواد من الجدول ٧.
- يجب أن يكون طول المُعامل بالبتات ٠٤٨ ٢ أو ٠٧٢ ٣.
- **يجب** أن يكون طول الأس بالبتات ٣٢ على الأكثر.

٧-١-٤-١-٣ ضغط المفتاح العام

يعرّف المفتاح العام سريع الزوال المضغوط للوحدة الطرفية (**Comp**($PK_{DH,IFD}$) بأنه البصمة الرقمية SHA-1 للقيمة العامة لبروتوكول ديفي هلمان، أي مجموعة ثمانيات بطول ثابت يساوي ٢٠.

٧-١-٤-٢ التحقق من صحة الوحدة الطرفية بخوارزمية التوقيع الرقمي للمنحنى الإهليلجي

بالنسبة للتحقق من صحة الوحدة الطرفية بخوارزمية التوقيع الرقمي للمنحنى الإهليلجي، **يجب** استخدام الخوارزميات والأشكال التالية:

٧-١-٤-٢-١ خوارزمية التوقيع

يجب استخدام خوارزمية التوقيع الرقمي للمنحنى الإهليلجي مع شكل توقيع بسيط [TR-03111] كما هو محدد في الجدول ٨.

الجدول ٨ — معرّفات المواد من أجل التحقق من صحة الوحدة الطرفية ببروتوكول ديفي هلمان للمنحنى الإهليلجي

Hash	Signature	OID
SHA-224	ECDSA	id-TA-ECDSA-SHA-224
SHA-256	ECDSA	id-TA-ECDSA-SHA-256
SHA-384	ECDSA	id-TA-ECDSA-SHA-384
SHA-512	ECDSA	id-TA-ECDSA-SHA-512

٧-١-٤-٢-٢ شكل المفتاح العام

يجب استخدام الشكل TLV [ISO/IEC 7816-8] كما هو محدد في الوثيقة Doc 9303-12.

- **يجب** أن يؤخذ معرّف المواد من الجدول ٨.
- **يجب** أن يكون طول المنحنى بالبتات ٢٢٤ أو ٢٥٦ أو ٣٢٠ أو ٣٨٤ أو ٥١٢.
- **يجب** أن تكون بارامترات النطاق ممتثلة لـ [TR-03111].

٧-١-٤-٢-٣ ضغط المفتاح العام

يعرّف المفتاح العام سريع الزوال المضغوط للوحدة الطرفية **Comp**($PK_{DH,IFD}$) بأنه الإحداثي x للنقطة العامة لبروتوكول ديفي هلمان للمنحنى الإهليلجي، أي مجموعة ثمانيات بطول ثابت يساوي ⌈log256p⌉.

٧-١-٤-٣ المصادقة على الشهادات

للمصادقة على شهادة الوحدة الطرفية، **يجب** أن تزوّد الدائرة المتكاملة بسلسلة شهادات تبدأ بنقطة ثقة مخزنة على الدائرة المتكاملة. وتعتبر نقاط الثقة هذه بمثابة مفاتيح عامة حديثة تقريباً للسلطة الوطنية لتحقق من الشهادات في الدائرة المتكاملة.

٧-١-٤-٣-١ الحالة الابتدائية لنقطة (نقاط) الثقة في الدائرة المتكاملة

يجب تخزين نقطة (نقاط) الثقة بطريقة آمنة في ذاكرة الدائرة المتكاملة في مرحلة الإنتاج أو مرحلة (ما قبل) إضافة البيانات الشخصية.

و**يجب** على موظف (ما قبل) إضافة البيانات الشخصية أن يقوم بما يلي:

- ضبط التاريخ الحالي للدائرة المتكاملة على تاريخ إضفاء الطابع الشخصي؛
- وإضافة البيانات الشخصية لمفتاح السلطة الوطنية للتحقق من الشهادات بأحدث تاريخ كنقطة ثقة.

ويجوز لموظف (ما قبل) إضافة البيانات الشخصية أن يضيف أيضاً البيانات الشخصية للمفتاح السابق كنقطة ثقة.

٧-١-٤-٣-٢ شهادات الربط

بما أن زوج المفاتيح الذي تستخدمه السلطة الوطنية للتحقق من الشهادات يتغير مع الوقت، يتعين إنشاء شهادات ربط بالسلطة الوطنية للتحقق من الشهادات. و**يجب** أن تكون شهادات الربط بالسلطة الوطنية للتحقق من الشهادات موقعة بالمفتاح السابق للسلطة الوطنية للتحقق من الشهادات، أي مفتاح السلطة الوطنية للتحقق من الشهادات لآخر تاريخ فعلي. و**يتعين** على الدائرة المتكاملة أن تحدث داخلياً نقطة (نقاط) الثقة وفقاً لشهادات الربط الصالحة الواردة.

و**يجب** أن تكون الدائرة المتكاملة قادرة على تخزين ما يصل إلى نقطتي من نقاط الثقة.

ملاحظة — نظراً للجدول الزمني لشهادات الربط بالسلطة الوطنية للتحقق من الشهادات (انظر الوثيقة Doc 9303-12)، يتعين تخزين نقطتي ثقة على الأكثر في الدائرة المتكاملة.

٧-١-٤-٣-٣ التاريخ الحالي

يجب على الدائرة المتكاملة أن تقبل شهادات الربط بالسلطة الوطنية للتحقق من الشهادات ولكن **يجب ألا** تقبل شهادات المتحقق من الوثائق وشهادات الوحدة الطرفية. ولتحديد ما إذا كانت الشهادة منتهية الصلاحية، **يجب** على الدائرة المتكاملة أن تستخدم التاريخ الحالي.

التاريخ الحالي: إذا لم تكن الدائرة المتكاملة مجهزة بساعة داخلية، يجب أن يكون التاريخ الحالي لها تقريباً على النحو المحدد فيما يلي. ويحدد التاريخ بصورة تقريبية بواسطة الدائرة المتكاملة باستخدام آخر تاريخ فعلي للشهادة يرد في شهادة ربط صالحة بالسلطة الوطنية للتحقق من الشهادات، أو في شهادة المتحقق من الوثائق أو في شهادة دقيقة للوحدة الطرفية.

الشهادة الدقيقة للوحدة الطرفية: تكون شهادة الوحدة الطرفية دقيقة إذا كان المتحقق من إصدار الوثيقة يحظر بثقة الدائرة المتكاملة لإنتاج شهادات الوحدة الطرفية بالتاريخ الفعلي الصحيح للشهادة. و**يجب** أن تعتبر الدائرة المتكاملة أن شهادات الربط بالسلطة الوطنية للتحقق من الشهادات وشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية التي يصدرها متحقق محلي من الوثائق هي شهادات دقيقة. و**يجب ألا** تعتبر الشهادات الأخرى دقيقة.

ويجوز للوحدة الطرفية أن ترسل شهادات الربط بالسلطة الوطنية للتحقق من الشهادات وشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية إلى الدائرة المتكاملة من أجل تحديث التاريخ الحالي ونقطة الثقة المخزنة في الدائرة المتكاملة حتى إذا لم تكن غاية الدائرة المتكاملة الاستمرار في عملية التحقق من صحة الوحدة الطرفية أو لم تكن قادرة على ذلك.

ملاحظة — تتحقق الدائرة المتكاملة فقط من أن الشهادة حديثة ظاهرياً (أي بالنسبة للتاريخ الفعلي التقريبي)، إلا إذا كانت تحتوي على ساعة داخلية.

٧-١-٤-٣-٤ الإجراء العام للمصادقة

يتألف إجراء المصادقة على الشهادة من ثلاث مراحل:

١- **التحقق من الشهادة: يجب** أن يكون التوقيع صالحاً، وما لم تكن الشهادة هي شهادة ربط بالسلطة الوطنية للتحقق من الشهادات، **يجب ألا** تكون الشهادة منتهية الصلاحية، وإذا فشلت عملية التحقق، **يجب** إبطال الإجراء.

ملاحظة — لا يمكن لحالة شهادة ربط بالسلطة الوطنية للتحقق من الشهادات منتهية الصلاحية أن تحدث إلا إذا كان للدائرة المتكاملة مصدر زمني يتخطى التاريخ الفعلي التقريبي الوارد أعلاه.

٢- **تحديث الحالة الداخلية: يجب** تحديث التاريخ الحالي، و**يجب** استيراد المفتاح العام والنعوت (بما في ذلك امتدادات الشهادات ذات الصلة)، و**يجب** تفعيل نقاط الثقة، و**يجب** تعطيل نقاط الثقة المنتهية الصلاحية من أجل التحقق من شهادات المتحقق من الوثائق.

٣- **التنظيف: يجب** أن توفر الرقاقة نقطتي ثقة مفعلتين على الأكثر لكل تطبيق. وإذا بقي أكثر من نقطتي ثقة مفعلتين لكل تطبيق بعد تحديث الحالة الداخلية، **يجب** تعطيل نقطة الثقة ذات التاريخ الفعلي الأحدث.

يجب أن تنفذ *عملية تحديث* التاريخ الفعلي وعمليات *تفعيل وتعطيل* إحدى نقاط الثقة باعتبارها عملية ذرية.

تفعيل نقطة الثقة: يجب أن تضاف نقطة الثقة الجديدة إلى قائمة نقاط الثقة.

تعطيل نقطة الثقة: يجب ألا تستخدم نقاط الثقة للتحقق من شهادات المتحقق من الوثائق. وفي حالة الدارات المتكاملة التي قد يكون فيها التاريخ الفعلي متقدماً عن تاريخ انتهاء صلاحية نقطة الثقة، مثل الدارات المتكاملة التي تستخدم ساعة داخلية، **يجب** أن تظل نقاط الثقة قابلة للاستعمال من اجل التحقق من شهادات الربط بالسلطة الوطنية للتحقق من الشهادات. و**يجوز** أن تحذف نقاط الثقة المعطلة بعد الاستيراد الناجح لشهادات الربط المتتالية.

٧-١-٤-٣-٥ مثال على إجراء المصادقة

يمكن استخدام إجراء المصادقة التالي، الذي يعطى كمثال، للمصادقة على سلسلة شهادات. ولكل شهادة واردة، تقوم الدائرة المتكاملة بالخطوات التالية:

١- تتحقق الدائرة المتكاملة من التوقيع الموجود على الشهادة. وتفشل عملية التحقق إذا كان التوقيع غير صحيح.

٢- إذا لم تكن الشهادة من شهادات الربط بالسلطة الوطنية للتحقق من الشهادات، يقارن تاريخ انتهاء صلاحية الشهادة بالتاريخ الحالي للدائرة المتكاملة. فإذا كان تاريخ انتهاء الصلاحية قبل التاريخ الحالي، تفشل عملية التحقق.

٣- تعتبر الشهادة صالحة والمفتاح العام والنعوت (بما في ذلك امتدادات الشهادات ذات الصلة) الواردة في الشهادة مستوردة.

- بالنسبة لشهادات الربط بالسلطة الوطنية للتحقق من الشهادات وشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية. ويقارن التاريخ الفعلي للشهادة بالتاريخ الحالي للدائرة المتكاملة. فإذا كان التاريخ الحالي قبل التاريخ الفعلي، يتم تحديث التاريخ الحالي ليصبح التاريخ الفعلي.
- بالنسبة لشهادات الربط بالسلطة الوطنية للتحقق من الشهادات. يضاف المفتاح العام الجديد للسلطة الوطنية للتحقق من الشهادات إلى قائمة نقاط الثقة المخزنة بصورة آمنة في ذاكرة الدائرة المتكاملة. بعد ذلك يتم تفعيل نقطة الثقة الجديدة.
- بالنسبة لشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية. يستورد مؤقتاً المفتاح العام الجديد للمتحقق من الوثائق أو للوحدة الطرفية من أجل التحقق من الشهادات المتتالية أو التحقق من صحة الوحدة الطرفية. على التوالي.

٤- يتم تعطيل نقاط الثقة المنتهية الصلاحية المخزنة حالياً في ذاكرة الدائرة المتكاملة من أجل التحقق من شهادات المتحقق من الوثائق ويمكن إزالتها من قائمة نقاط الثقة.

٧-١-٤-٣-٦ الترخيص الفعلي

يجب أن تحتوي كل شهادة على نموذج ترخيص صاحب الشهادة (انظر الوثيقة Doc 9303-12) **ويجوز** أن تحتوي على امتدادات الترخيص (انظر الوثيقة Doc 9303-12، القسم ٧-٢-٢-٦).

- يحدد نموذج ترخيص صاحب الشهادة نوع الوحدة الطرفية (لا تأخذ هذه الواصفة في الاعتبار إلا نظم التفتيش، ولكن يمكن لمواصفات أخرى أن تستخدم أنواعاً مختلفة من الوحدات الطرفية).
- يحدد كل من نموذج ترخيص صاحب الشهادة وامتدادات الترخيص *النسبي* لصاحب الشهادة الذي عينته سلطة إصدار الشهادات.

ولتحديد الترخيص الفعلي لصاحب الشهادة، **يجب** أن تحسب الدائرة المتكاملة دالة بتات 'and' للترخيص النسبي الواردة في شهادة الوحدة الطرفية، وشهادة المتحقق من الوثائق المشار إليها وشهادة الربط بالسلطة الوطنية للتحقق من الشهادات المشار إليها.

و**يجب** أن تفسر الدائرة المتكاملة الترخيص الفعلي على النحو التالي:

- الدور الفعلي هو السلطة الوطنية للتحقق من الشهادات:
  - صدرت شهادة الربط عن السلطة الوطنية للتحقق من الشهادات.
  - **يجب** على الدائرة المتكاملة أن تحدث نقطة الثقة الداخلية الخاصة بها، أي المفتاح العام والترخيص الفعلي.
  - جهة اصدار الشهادة هي مصدر موثوق للوقت و**يجب** على الدائرة المتكاملة أن تحدّث تاريخها الحالي باستخدام التاريخ الفعلي للشهادة.

- **يجب ألا** تمنح الدائرة المتكاملة السلطة الوطنية للتحقق من الشهادات إمكانية الاطلاع على البيانات الحساسة (أي ينبغي تجاهل الترخيص الفعلي).

- الدور الفعلي هو المتحقق من الوثائق:
  - صدرت الشهادة عن السلطة الوطنية للتحقق من الشهادات بالنسبة لمتحقق من الوثائق مرخص.
  - جهة اصدار الشهادة هي مصدر موثوق للوقت و**يجب** على الدائرة المتكاملة أن تحدّث تاريخها الحالي باستخدام التاريخ الفعلي للشهادة.
  - **يجب ألا** تمنح الدائرة المتكاملة المتحقق من الوثائق إمكانية الاطلاع على البيانات الحساسة (أي ينبغي تجاهل الترخيص الفعلي.
- الدور الفعلي هو الوحدة الطرفية:
  - صدرت الشهادة عن متحقق محلي أو أجنبي من الوثائق.
  - إذا كانت الشهادة شهادة دقيقة لوحدة طرفية (راجع القسم ٧-١-٤-٣-٣)، تكون جهة الإصدار مصدراً موثوقاً للوقت و**يجب** على الدائرة المتكاملة أن تحدّث تاريخها الحالي باستخدام التاريخ الفعلي للشهادة.
  - **يجب** على الدائرة المتكاملة أن تمنح الوحدة الطرفية المتحقق من صحتها حق الاطلاع على البيانات الحساسة وفقاً للترخيص الفعلي.

*ملاحظة — قد يحتوي كل من نموذج ترخيص صاحب الشهادة وامتداد الترخيص بتات غير مخصصة لحق الوصول (بتات محجوزة للاستعمال في المستقبل). و**يجب** على الدائرة المتكاملة أن تتجاهل هذه البتات أثناء تقييم حقوق الوصول.*

٧-١-٤-٣-٧ استيراد المفتاح العام

تكون المفاتيح العامة المستوردة من إجراء المصادقة على الشهادة مخزنة إما بصورة مؤقتة أو دائمة على الدائرة المتكاملة.

و**ينبغي** أن ترفض الدائرة المتكاملة استيراد مفتاح عام، إذا كان مرجع صاحب الشهادة معروفاً بالفعل من جانب الدائرة المتكاملة.

الاستيراد الدائم: يجب أن تستورد الدائرة المتكاملة بصورة دائمة المفاتيح العامة الواردة في شهادات الربط بالسلطة الوطنية للتحقق من الشهادات و**يجب** تخزينها بشكل آمن في ذاكرة الدائرة المتكاملة. ويجب أن يستوفي كل من المفتاح العام الذي تم استيراده بصورة دائمة وبياناته الوصفية الشروط التالية:

- **قد** يحل محله بعد انتهاء الصلاحية مفتاح عام لاحق مستورد بصورة دائمة.
- إذا كان **لا بد** من أن يحل محل أي منهما مفتاح عام لاحق مستورد بصورة دائمة له المرجع نفسه لصاحب الشهادة أو **لا بد** من رفض الاستيراد.
- **يجب ألا** يحل محله مفتاح عام لاحق مستورد بصورة مؤقتة.

و**يجب** أن تكون عملية تفعيل وتعطيل مفتاح عام لاحق مستورد بصورة دائمة عملية ذرية.

الاستيراد المؤقت: يجب أن تستورد الدائرة المتكاملة بصورة مؤقتة المفاتيح العامة الواردة في شهادات المتحقق من الوثائق وشهادات الوحدة الطرفية و**يجب** تخزينها بشكل آمن في ذاكرة الدائرة المتكاملة. ويجب أن يستوفي كل من المفتاح العام الذي تم استيراده بصورة مؤقت/ وبياناته الوصفية الشروط التالية:

- **ألا يكون** قابلاً للانتقاء أو الاستخدام بعد انقطاع الطاقة عن الدائرة المتكاملة.

- **يجب** أن يظل قابلاً للاستخدام إلى حين انتهاء عملية التشفير اللاحقة بنجاح (أي PSO:Verify Certificate أو External Authenticate).
- **قد** يحل محله مفتاح عام لاحق مستورد بصورة مؤقتة.

و**يجب ألا** تستفيد الوحدة الطرفية من أي مفتاح عام مستورد بصورة مؤقتة ما عدا المفتاح المستورد مؤخراً.

البيانات الوصفية المستوردة: بالنسبة بكل مفتاح عام مستورد بصورة دائمة أو مؤقتة، يجب تخزين البيانات الإضافية التالية الواردة في الشهادة (انظر الوثيقة Doc 9303-12):

- مرجع صاحب الشهادة.
- ترخيص صاحب الشهادة (الدور الفعلي والترخيص الفعلي).
- التاريخ الفعلي للشهادة.
- تاريخ انتهاء صلاحية الشهادة.
- امتدادات الشهادة (عند الاقتضاء).

وترد في القسم ٧-١-٤-٣-٦ حسابات الدور الفعلي (السلطة الوطنية للتحقق من الشهادات، أو المتحقق من الوثائق، أو الوحدة الطرفية) والترخيص الفعلي لصاحب الشهادة.

ملاحظة — يعتمد شكل البيانات المخزنة على نظام التشغيل ولا يندرج ضمن نطاق هذه المواصفة.

٧-١-٥ وحدات بيانات بروتوكول التطبيق

يجب أن يُستخدم التسلسل التالي للأوامر مع المراسلات الآمنة لتنفيذ التحقق من صحة الوحدة الطرفية:

- MSE:Set DST
- PSO:Verify Certificate
- MSE:Set AT
- Get Challenge
- External Authenticate

تتكرر الخطوتان ١ و٢ لكل شهادة سيرة ذاتية من المقرر التحقق منها (شهادات الربط بالسلطة الوطنية للتحقق من الشهادات، أو شهادة المتحقق من الوثائق، أو شهادة الوحدة الطرفية).

٧-١-٥-١ الأمر *MSE:Set DST*

يستخدم الأمر MSE:Set DST لإعداد التحقق من الشهادة.

Command			
CLA		Context Specific	
INS	0x22	Manage Security Environment	
P1/P2	0x81B6	Set Digital Signature Template for verification.	
Data	0x83	*Reference of a public key* ISO 8859-1 encoded name of the public key to be set	REQUIRED

Response		
Data	–	Absent
Status Bytes	0x9000 0x6A88 other	*Normal Operation* The key has been selected for the given purpose. *Referenced data not found* The selection failed as the public key is not available. *Operating system dependent error* The key has not been selected.

ملاحظة — تقبل بعض نظم التشغيل اختيار مفتاح عام غير متوفر ولا تعيد الخطأ إلا عندما يستخدم المفتاح العام للغرض الذي تم اختياره.

٧-١-٥-٢ الأمر *PSO:Verify Certificate*

يستخدم الأمر PSO:Verify Certificate للتحقق من الشهادات واستيرادها.

Command			
CLA		Context Specific	
INS	0x2A	Perform Security Operation	
P1/P2	0x00BE	Verify self-descriptive certificate.	
Data	0x7F4E 0x5F37	*Certificate body* *The body of the certificate to be verified.* *Signature* *The signature of the certificate to be verified.*	REQUIRED REQUIRED

Response		
Data	–	Absent
Status Bytes	0x9000 other	*Normal processing* The certificate was successfully validated and the public key has been imported. *Operating system dependent error* The public key could not be imported (e.g. the certificate was not accepted).

٧-١-٥-٣ الأمر *MSE:Set AT*

يشار إلى استخدام الأمر MSE:Set AT من أجل التحقق من صحة الوحدة الطرفية بضبط P1/P2 على 0x81A4، انظر الجدول ادناه.

Command			
CLA		Context Specific	
INS	0x22	Manage Security Environment	
P1/P2	0x81A4	Terminal Authentication:	
Data	0x83	*Reference of a public key / secret key*	REQUIRED

		This data object is used to select the public key of the terminal by its ISO 8859-1 encoded name.	

Response		
Data	–	Absent
Status Bytes	0x9000 0x6A80 0x6A88 other	*Normal processing* *The protocol has been selected and initialized.* *Incorrect parameters in the command data field* Algorithm not supported or initialization failed. *Referenced data not found* The referenced data is not available. *Operating system dependent error* The initialization of the protocol failed.

ملاحظة — تقبل بعض نظم التشغيل اختيار مفتاح عام غير متوفر ولا تعيد الخطأ إلا عندما يستخدم المفتاح العام للغرض الذي تم اختياره.

٧-١-٥-٤ الأمر *Get Challenge*

Command			
CLA		Context Specific	
INS	0x84	Get Challenge	
P1/P2	0x0000		
Data	–	Absent	
Le	0x08		REQUIRED

Response		
Data	r_{IC}	8 bytes of randomness.
Status Bytes	0x9000 other	*Normal processing* *Operating system dependent error*

٧-١-٥-٥ الأمر *External Authenticate*

Command			
CLA		Context Specific	
INS	0x82	External Authenticate	
P1/P2	0x0000	Keys and Algorithms implicitly known.	
Data		Signature generated by the terminal.	REQUIRED

Response		
Data	–	Absent
Status Bytes	0x9000 0x6300	*Normal processing* The authentication was successful. Access to data groups will be granted according to the effective authorization of the corresponding verified certificate. *Warning* Signature verification failed.

	0x6982 other	*Security status not satisfied* The authentication failed as the current authentication level of the terminal does not allow to use Terminal Authentication (e.g. Terminal Authentication was already performed, etc.). *Operating system dependent error* The authentication failed.

٨-٧ تشفير سمات الاستدلال البيولوجي الإضافية

يجوز أيضاً تقييد الوصول إلى سمات الاستدلال البيولوجي الإضافية عن طريق تشفيرها. وللتمكن من فك تشفير البيانات المشفّرة، **يجب** تزويد جهاز التفتيش بمفتاح لفك التشفير. وتحديد خوارزمية التشفير/فك التشفير والمفاتيح التي تُستخدم متروك للدولة المنفّذة ويخرج عن نطاق هذه الوثيقة.

يعتمد تنفيذ حماية سمات الاستدلال البيولوجي الإضافية على المواصفات الداخلية للدولة أو المواصفات المتفق عليها ثنائياً بين الدول المتشاركة في هذه المعلومات.

٨- جهاز التفتيش

بغية دعم الوظيفية المطلوبة والخيارات المحددة التي يمكن تنفيذها على وثائق السفر الإلكترونية المقروءة آلياً التي ستُعرض، سيتعين على جهاز التفتيش الوفاء ببعض الشروط المسبقة.

٨-١ مراقبة الوصول الأساسية

يجب على أجهزة التفتيش الداعمة لمراقبة الوصول الأساسية أن تفي بالشرطين المسبقين التاليين:

١) جهاز التفتيش مزوّد بالوسائل اللازمة للحصول على الجزء المقروء آلياً من الوثيقة المادية لاشتقاق مفتاحي الوصول الأساسيين للوثيقة (K_{Enc} and K_{MAC}) من وثيقة السفر الإلكترونية المقروءة آلياً.

٢) تدعم برامجيات جهاز التفتيش البروتوكول الموصوف في القسم ٤-٣، في حالة أن توفَّر للجهاز وثيقة سفر إلكترونية مقروءة آلياً مع مراقبة وصول أساسية، بما في ذلك تشفير قناة الاتصال بالمراسلات المأمونة.

٨-٢ فتح الاتصال بكلمة سر مصدّق عليها

يجب أن تفي أجهزة التفتيش الداعمة لفتح الاتصال بكلمة سر مصدّق عليها بالشروط التالية:

١) جهاز التفتيش مزوّد بوسائل للحصول على الجزء المقروء آلياً و/أو رقم الاطلاع على البطاقة من الوثيقة المادية.

٢) تدعم برامج حاسوب جهاز التفتيش البروتوكول الموصوف في القسم ٤-٤، في حالة أن تقدَّم إلى الجهاز وثيقة سفر إلكترونية مقروءة آلياً مع فتح الاتصال بكلمة سر مصدّق عليها، بما في ذلك تشفير قناة الاتصال بالمراسلات المأمونة.

٨-٣ التحقق السلبي من الصحة

للتمكن من أداء تحقق سلبي من صحة البيانات المخزّنة في الدائرة المتكاملة اللاتلامسية لوثائق السفر الإلكترونية المقروءة آلياً، يحتاج جهاز التفتيش لمعرفة معلومات مفاتيح دول أو منظمات الاصدار:

١) بالنسبة لكل دولة أو منظمة إصدار أو البلد الموقّع على شهادة سلطة إصدار الترخيص أو المعلومات ذات الصلة المستخلصة من الشهادة **يجب** تخزينها بشكل مأمون في جهاز التفتيش.

٢) بدلاً من ذلك، بالنسبة لكل دولة أو منظمة إصدار أو شهادات موقّع الوثيقة (C_{DS}) أو المعلومات ذات الصلة المستخلصة من الشهادات **يجب** تخزينها بشكل مأمون في جهاز التفتيش.

قبل استخدام مفتاح عام لسلطة إصدار الترخيص الموقّعة بأحد البلدان لدولة أو منظمة إصدار، **يجب** إثبات الثقة في هذا المفتاح بواسطة دولة أو منظمة القبول.

قبل استخدام شهادة جهة موقّعة على وثيقة (C_{DS}) للتحقق من حافظة أمن الوثيقة، **يجب** أن يتحقق جهاز التفتيش من توقيعه الرقمي، باستخدام المفتاح العام لسلطة إصدار الترخيص في البلد الموقِّع.

بالإضافة إلى ذلك، **يجب** أن يتاح لأجهزة التفتيش الوصول إلى معلومات الالغاء التي تم التحقق منها.

٨-٤ التحقق الإيجابي من الصحة

دعم أجهزة التفتيش للتحقق الإيجابي من الصحة **اختياري**.

إذا كان جهاز التفتيش يدعم التحقق الإيجابي من الصحة، من **المطلوب** أن تكون لدى جهاز التفتيش القدرة على قراءة الجزء المقروء آلياً البصري.

إذا كان جهاز التفتيش يدعم التحقق الإيجابي من الصحة، **يجب** أن تدعم برامج حاسوب جهاز التفتيش بروتوكول التحقق الإيجابي من الصحة الموصوف في القسم ٦-١.

٨-٥ التحقق من صحة الرقاقة

دعم أجهزة التفتيش للتحقق من صحة الرقاقة **اختياري**.

إذا كان جهاز التفتيش يدعم التحقق من صحة الرقاقة، من **المطلوب** أن تكون لدى جهاز التفتيش القدرة على قراءة الجزء المقروء آلياً البصري.

إذا كان جهاز التفتيش يدعم التحقق الإيجابي من صحة الرقاقة، **يجب** أن تدعم برامج حاسوب جهاز التفتيش بروتوكول التحقق الإيجابي من صحة الرقاقة الموصوف في القسم ٦-٢.

٨-٦ التحقق من صحة الوحدة الطرفية

يعتبر دعم التحقق من صحة الوحدة الطرفية بواسطة نظم التفتيش اختيارياً.

وإذا كان نظام التفتيش يدعم التحقق منصحة الوحدة الطرفية، **من الضروري** أن يكون نظام التفتيش قادراً على تخزين المفتاح الخاص لنظام التفتيش بصورة آمنة. و**يجب** أن يكون لنظام التفتيش إمكانية الاطلاع على المتحقق من الوثائق الخاص به على فترات منتظمة لتجديد شهادة الوحدة الطرفية.

وإذا كان نظام التفتيش يدعم التحقق من صحة الوحدة الطرفية، **يجب** على برمجيات نظام التفتيش أن تدعم بروتوكول التحقق من صحة الوحدة الطرفية كما هو وارد في القسم ٧-١.

٨-٧ فك تشفير سمات الاستدلال البيولوجي الإضافية

يعتمد تنفيذ حماية سمات الاستدلال البيولوجي الإضافية الاختيارية على المواصفات الداخلية للدولة أو المواصفات المتفق عليها ثنائياً بين دولتين متشاركتين في هذه المعلومات.

٩- المواصفات المشتركة

٩-١ بنى مجموعة الرموز الأولى لتركيب الخلاصات

بنى البيانات SubjectPublicKeyInfo و AlgorithmIdentifier معرّفة على النحو التالي:

```
SubjectPublicKeyInfo ::= SEQUENCE {
  algorithm  AlgorithmIdentifier,
  SubjectPublicKey    BIT STRING
}

AlgorithmIdentifier ::= SEQUENCE {
  algorithm OBJECT IDENTIFIER,
  parameters ANY DEFINED BY algorithm OPTIONAL
}
```

يمكن العثور على تفاصيل البارامترات في [TR-03111] and [X9.42].

٩-٢ المعلومات عن البروتوكولات والتطبيقات المدعومة

بنية بيانات مجموعة الرموز الأولى لتركيب الخلاصات SecurityInfos **يجب** توفيرها عن طريق رقاقة وثيقة السفر الإلكترونية المقروءة آلياً لبيان البروتوكولات الأمنية المدعومة. وتُحدد بنية البيانات كما يلي:

```
SecurityInfos  ::= SET OF SecurityInfo

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

العناصر الواردة في بنية بيانات SecurityInfo لها المعنى التالي:

- يعرّف معرِّف البند protocol البروتوكول المدعوم.
- النوع المفتوح requiredData يحتوي على بيانات إلزامية محددة للبروتوكول.
- النوع المفتوح optionalData يحتوي على بيانات اختيارية محددة للبروتوكول.

معلومات أمنية لفتح الاتصال بكلمة سر مصدّق عليها

لبيان الدعم لفتح الاتصال بكلمة سر مصدّق عليها يجوز أن تحتوي SecurityInfos على المدخلات التالية:

- **يجب** أن تكون موجودة واحدة على الأقل من PACEInfo باستخدام معيار نطاق موحّد.
- لكل مجموعة مدعومة من معايير النطاق الصريحة **يجب** أن تكون PACEDomainParameterInfo موجودة.

المعلومات الأمنية للتحقق الإيجابي من الصحة

إذا استُخدمت خوارزمية توقيع مستندة إلى خوارزمية التوقيع الرقمي للمنحنى الاهليلجي للتحقق الإيجابي من الصحة بواسطة رقاقة وثيقة السفر الإلكترونية المقروءة آلياً، **يجب** أن تحتوي الـ SecurityInfos على مدخل SecurityInfo التالي:

- ActiveAuthenticationInfo

المعلومات الأمنية للتحقق من صحة الرقاقة

لبيان الدعم للتحقق من صحة الرقاقة قد تحتوي SecurityInfos على المدخلات التالية:

- على الأقل واحدة من ChipAuthenticationInfo وChipAuthenticationPublicKeyInfo المناظرة **يجب** أن تكون معايير النطاق الصريحة موجودة.

المعلومات الأمنية للتحقق من صحة الوحدة الطرفية

لبيان الدعم للتحقق من صحة الوحدة الطرفية قد تحتوي SecurityInfos على المدخلات التالية:

- على الأقل واحدة من TerminalAuthenticationInfo يجب أن تكون موجودة.

المعلومات الأمنية للتطبيقات الموجودة

يوصي القسم ٣-١١-٢ من الوثيقة Doc 9303-10 بوجود ملف شفاف EF.DIR لبيان التطبيقات المدعومة. وهذا الملف إلزامي في حال وجود أي من تطبيقات LDS2. وبما أن الملف EF.DIR غير موقّع ويمكن بالتالي العبث به، مثلاً لإخفاء تطبيق قائم عن جهاز توصيل، تتوفر نسخة ثانية من الملف EF.DIR على شكل SecurityInfo في حال وجود أي تطبيق من تطبيقات LDS2.

المعلومات الأمنية للبروتوكولات الأخرى

يجوز أن تحتوي SecurityInfos على مدخلات إضافية تبيّن دعم بروتوكولات أخرى أو توفر معلومات أخرى. و**يجوز** أن يستبعد جهاز التفتيش أي مدخل غير معروف.

٩-٢-١ *معلومات فتح الاتصال بكلمة سر مصدّق عليها*

توفّر هذه البنية للبيانات معلومات مفصّلة عن تنفيذ فتح الاتصال بكلمة سر مصدّق عليها.

- **يجب** أن يعرّف protocol معرّف البند الخوارزميات التي تُستخدم (أي اتفاق المفاتيح والشيفرة التماثلية ورمز التحقق من صحة الرسالة).
- **يجب** أن تحدد version الصحيحة نسخة البروتوكول. وتُدعم النسخة ٢ فقط بهذه المواصفة.
- تُستخدم parameterId الصحيحة لبيان معرّف معيار النطاق. و**يجب** استخدامه إذا كانت رقاقة وثيقة السفر الإلكترونية المقروءة آلياً تستخدم بارامترات النطاق الموحّدة (راجع القسم ٩-٥-١)، ويوفّر معايير نطاق صريحة متعددة من أجل فتح الاتصال بكلمة سر مصدّق عليها أو protocol هو واحد من *-CAM-* معرّفات البنود. وفي حالة فتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات للتحقق من صحة الرقاقة، تدل parameterID أيضاً على هوية المفتاح المُستخدم للتحقق من صحة الرقاقة، أي **يجب** أن توفّر الرقاقة ChipAuthenticationPublicKeyInfo مع keyID مساوية لـ parameterID من هذه البنية للبيانات.

```
PACEInfo ::= SEQUENCE {
    Protocol    OBJECT IDENTIFIER(
```

```
                    id-PACE-DH-GM-3DES-CBC-CBC |
                    id-PACE-DH-GM-AES-CBC-CMAC-128 |
                    id-PACE-DH-GM-AES-CBC-CMAC-192 |
                    id-PACE-DH-GM-AES-CBC-CMAC-256 |
                    id-PACE-ECDH-GM-3DES-CBC-CBC |
                    id-PACE-ECDH-GM-AES-CBC-CMAC-128 |
                    id-PACE-ECDH-GM-AES-CBC-CMAC-192 |
                    id-PACE-ECDH-GM-AES-CBC-CMAC-256 |
                    id-PACE-DH-IM-3DES-CBC-CBC |
                    id-PACE-DH-IM-AES-CBC-CMAC-128 |
                    id-PACE-DH-IM-AES-CBC-CMAC-192 |
                    id-PACE-DH-IM-AES-CBC-CMAC-256 |
                    id-PACE-ECDH-IM-3DES-CBC-CBC |
                    id-PACE-ECDH-IM-AES-CBC-CMAC-128 |
                    id-PACE-ECDH-IM-AES-CBC-CMAC-192 |
                    id-PACE-ECDH-IM-AES-CBC-CMAC-256
                    id-PACE-ECDH-CAM-AES-CBC-CMAC-128 |
                    id-PACE-ECDH-CAM-AES-CBC-CMAC-192 |
                    id-PACE-ECDH-CAM-AES-CBC-CMAC-256),
    version     INTEGER, -- MUST be 2
    parameterId INTEGER OPTIONAL
}
```

٩-٢-٢ معلومات معايير نطاق فتح الاتصال بكلمة سر مصدّق عليها

هذه البنية للبيانات **مطلوبة** إذا كانت رقاقة وثيقة السفر الإلكترونية المقروءة آلياً توفّر معايير نطاق صريحة لفتح الاتصال بكلمة سر مصدّق عليها و**يجب** حذفها بخلاف ذلك.

- **يجب** أن يحدد الـ `protocol` المعرّف للمادة نوع معايير النطاق (أي بروتوكول ديفي–هيلمان أو بروتوكول ديفي–هيلمان للمنحنى الاهليلجي).
- **يجب** أن يحتوي تسلسل `domainParameter` على معايير النطاق.
- **يجوز** استخدام `parameterId` الصحيح لبيان معرّف معيار النطاق المحلي. و**يجب** استخدامه إذا كانت رقاقة وثيقة السفر الإلكترونية المقروءة آلياً توفّر عدة معايير نطاق صريحة من أجل فتح الاتصال بكلمة سر مصدّق عليها.

```
PACEDomainParameterInfo ::= SEQUENCE {
  protocol          OBJECT IDENTIFIER(
                    id-PACE-DH-GM |
                    id-PACE-ECDH-GM |
                    id-PACE-DH-IM |
                    id-PACE-ECDH-IM
                    id-PACE-ECDH-CAM),
  domainParameter   AlgorithmIdentifier,
  parameterId       INTEGER OPTIONAL
}
```

*ملاحظة — **يجوز** أن تدعم رقاقة وثيقة السفر الإلكترونية المقروءة آلياً أكثر من مجموعة واحدة من معايير النطاق الصريحة (أي أن الرقاقة يجوز أن تدعم خوارزميات و/أو أطوال مفاتيح مختلفة). وفي هذه الحالة **يجب** الكشف عن المعرّف في `PACEDomainParameterInfo` المناظرة.*

معايير النطاق التي تحتوي عليها *`PACEDomainParameterInfo`* غير محمية ويجوز أن تكون غير مأمونة. وسيؤدي استخدام معايير نطاق غير مأمونة لفتح الاتصال بكلمة سر مصدّق عليها إلى تسرّب كلمة السر المستخدمة. و**يجب** دعم رقائق وثائق السفر الإلكترونية المقروءة

آلياً بمجموعة واحدة على الأقل من معايير النطاق الموحّدة على النحو المحدد في القسم ٩-٥-١. **ويجب** ألا تستخدم أجهزة التفتيش معايير النطاق الصريحة التي تقدمها رقاقة وثيقة السفر الإلكترونية المقروءة آلياً ما لم تكن تلك المعايير للنطاق معروفة صراحة من قبل أجهزة التفتيش بأنها مأمونة.

يجب تبادل المفاتيح العامة سريعة الزوال كقيم مفاتيح عامة بسيطة. ويمكن العثور على مزيد من المعلومات بشأن الترميز في القسم ٩-٤-٥.

٩-٢-٣ معرّف مادة فتح الاتصال بكلمة سر مصدّق عليها

يحتوي البند الفرعي لـ bsi-de على معرّفات المادة المستخدمة لفتح الاتصال بكلمة سر مصدّق عليها:

```
bsi-de OBJECT IDENTIFIER ::= {
    itu-t(0) identified-organization(4) etsi(0)
    reserved(127) etsi-identified-organization(0) 7
}
```

يجب استخدام معرّف المادة التالي:

```
id-PACE OBJECT IDENTIFIER ::= {
    bsi-de protocols(2) smartcard(2) 4
}

id-PACE-DH-GM                     OBJECT IDENTIFIER ::= {id-PACE 1}
id-PACE-DH-GM-3DES-CBC-CBC        OBJECT IDENTIFIER ::= {id-PACE-DH-GM 1}
id-PACE-DH-GM-AES-CBC-CMAC-128    OBJECT IDENTIFIER ::= {id-PACE-DH-GM 2}
id-PACE-DH-GM-AES-CBC-CMAC-192    OBJECT IDENTIFIER ::= {id-PACE-DH-GM 3}
id-PACE-DH-GM-AES-CBC-CMAC-256    OBJECT IDENTIFIER ::= {id-PACE-DH-GM 4}

id-PACE-ECDH-GM                   OBJECT IDENTIFIER ::= {id-PACE 2}
id-PACE-ECDH-GM-3DES-CBC-CBC      OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 1}
id-PACE-ECDH-GM-AES-CBC-CMAC-128  OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 2}
id-PACE-ECDH-GM-AES-CBC-CMAC-192  OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 3}
id-PACE-ECDH-GM-AES-CBC-CMAC-256  OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 4}

id-PACE-DH-IM                     OBJECT IDENTIFIER ::= {id-PACE 3}
id-PACE-DH-IM-3DES-CBC-CBC        OBJECT IDENTIFIER ::= {id-PACE-DH-IM 1}
id-PACE-DH-IM-AES-CBC-CMAC-128    OBJECT IDENTIFIER ::= {id-PACE-DH-IM 2}
id-PACE-DH-IM-AES-CBC-CMAC-192    OBJECT IDENTIFIER ::= {id-PACE-DH-IM 3}
id-PACE-DH-IM-AES-CBC-CMAC-256    OBJECT IDENTIFIER ::= {id-PACE-DH-IM 4}

id-PACE-ECDH-IM                   OBJECT IDENTIFIER ::= {id-PACE 4}
id-PACE-ECDH-IM-3DES-CBC-CBC      OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 1}
id-PACE-ECDH-IM-AES-CBC-CMAC-128  OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 2}
id-PACE-ECDH-IM-AES-CBC-CMAC-192  OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 3}
id-PACE-ECDH-IM-AES-CBC-CMAC-256  OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 4}

id-PACE-ECDH-CAM                  OBJECT IDENTIFIER ::= {id-PACE 6}
id-PACE-ECDH-CAM-AES-CBC-CMAC-128 OBJECT IDENTIFIER ::= {id-PACE-ECDH-CAM 2}
id-PACE-ECDH-CAM-AES-CBC-CMAC-192 OBJECT IDENTIFIER ::= {id-PACE-ECDH-CAM 3}
id-PACE-ECDH-CAM-AES-CBC-CMAC-256 OBJECT IDENTIFIER ::= {id-PACE-ECDH-CAM 4}
```

٩-٢-٤ معلومات التحقق الإيجابي من الصحة

إذا استُخدمت خوارزمية توقيع مستندة إلى خوارزمية التوقيع الرقمي للمنحنى الاهليلجي من أجل التحقق الإيجابي من صحة رقاقة وثيقة السفر الإلكترونية المقروءة آلياً، فإن SecurityInfos في مجموعة البيانات ١٤ من بنية البيانات المنطقية لرقاقة وثيقة السفر الإلكترونية المقروءة آلياً **يجب** أن تحتوي على مدخل SecurityInfo:

```
ActiveAuthenticationInfo ::= SEQUENCE {
    Protocol     OBJECT IDENTIFIER (id-icao-mrtd-security-aaProtocolObject)
    version      INTEGER -- MUST be 1
    signatureAlgorithm OBJECT IDENTIFIER
}

id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::=
                                    { id-icao-mrtd-security 5 }
```

بالنسبة إلى signatureAlgorithm، **يجب** استخدام معرّفات المادة المعرّفة في [TR-03111].

ملاحظة — معرّف المادة id-icao-mrtd-security معرَّف في الوثيقة Doc 9303-10.

٩-٢-٥ معلومات التحقق الإيجابي من صحة الرقاقة

تقدّم هذه البنية للبيانات معلومات مفصّلة بشأن تنفيذ للتحقق من صحة الرقاقة.

- **يجب** أن يحدد protocol معرّف المادة الخوارزميات التي يتعين استخدامها (أي اتفاق المفاتيح والشيفرة التماثلية ورمز التحقق من صحة الرسالة).
- **يجب** أن تحدد الـ version الصحيحة نسخة البروتوكول. وفي الوقت الراهن، فإن النسخة ١ فقط هي التي تدعمها هذه المواصفة.
- **يجوز** استخدام keyId الصحيحة لبيان معرّف المفتاح المحلي. و**يجب** استخدامه إذا كانت رقاقة وثيقة السفر المقروءة آلياً توفّر عدة مفاتيح عامة للتحقق من صحة الرقاقة.

```
ChipAuthenticationInfo ::= SEQUENCE {
  protocol   OBJECT IDENTIFIER(
             id-CA-DH-3DES-CBC-CBC |
             id-CA-DH-AES-CBC-CMAC-128 |
             id-CA-DH-AES-CBC-CMAC-192 |
             id-CA-DH-AES-CBC-CMAC-256 |
             id-CA-ECDH-3DES-CBC-CBC |
             id-CA-ECDH-AES-CBC-CMAC-128 |
             id-CA-ECDH-AES-CBC-CMAC-192 |
             id-CA-ECDH-AES-CBC-CMAC-256),
  version    INTEGER, -- MUST be 1
  keyId      INTEGER OPTIONAL
}
```

٩-٢-٦ معلومات المفتاح العام للتحقق من صحة الرقاقة

توفّر هذه البنية من البيانات مفتاحاً عاماً للتحقق من صحة الرقاقة أو فتح الاتصال بكلمة سر مصدّق عليها مع تحديد مجالات التحقق من صحة الرقاقة لرقاقة وثيقة السفر الإلكترونية المقروءة آلياً.

- **يجب** أن يعرّف معرّف المادة protocol نوع المفتاح العام (أي بروتوكول ديفي-هيلمان أو بروتوكول ديفي-هيلمان للمنحنى الاهليلجي).
- **يجب** أن يحتوي التسلسل chipAuthenticationPublicKey على المفتاح العام في شكل مرمَّز.
- **يجوز** استخدام keyId الصحيحة لبيان معرّف المفتاح المحلي. و**يجب** استخدامه إذا كانت رقاقة وثيقة السفر الإلكترونية المقروءة آلياً توفر عدة مفاتيح عامة للتحقق من صحة الرقاقة أو إذا كان هذا المفتاح يُستخدم لفتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات للتحقق من صحة الرقاقة.

```
ChipAuthenticationPublicKeyInfo ::= SEQUENCE {
    protocol                    OBJECT IDENTIFIER(id-PK-DH | id-PK-ECDH),
    chipAuthenticationPublicKey SubjectPublicKeyInfo,
    keyId                       INTEGER OPTIONAL
}
```

*ملاحظة — **يجوز** أن تدعم رقاقة وثيقة السفر الإلكترونية المقروءة آلياً أكثر من زوج واحد من المفاتيح للتحقق من صحة الرقاقة (أي أن الرقاقة قد تدعم خوارزميات و/أو أطوال مفاتيح مختلفة). وفي هذه الحالة **يجب** الكشف عن معرّف المفتاح المحلي في ChipAuthenticationInfo و ChipAuthenticationPublicKeyInfo المناظرين.*

٩-٢-٧ معرّف مادة التحقق من صحة الرقاقة

يجب استخدام معرّف المادة التالي:

```
id-PK OBJECT IDENTIFIER ::= {
  bsi-de protocols(2) smartcard(2) 1
}

id-PK-DH                    OBJECT IDENTIFIER ::= {id-PK 1}
id-PK-ECDH                  OBJECT IDENTIFIER ::= {id-PK 2}

id-CA OBJECT IDENTIFIER ::= {
  bsi-de protocols(2) smartcard(2) 3
}

id-CA-DH                    OBJECT IDENTIFIER ::= {id-CA 1}
id-CA-DH-3DES-CBC-CBC       OBJECT IDENTIFIER ::= {id-CA-DH 1}
id-CA-DH-AES-CBC-CMAC-128   OBJECT IDENTIFIER ::= {id-CA-DH 2}
id-CA-DH-AES-CBC-CMAC-192   OBJECT IDENTIFIER ::= {id-CA-DH 3}
id-CA-DH-AES-CBC-CMAC-256   OBJECT IDENTIFIER ::= {id-CA-DH 4}

id-CA-ECDH                  OBJECT IDENTIFIER ::= {id-CA 2}
id-CA-ECDH-3DES-CBC-CBC     OBJECT IDENTIFIER ::= {id-CA-ECDH 1}
id-CA-ECDH-AES-CBC-CMAC-128 OBJECT IDENTIFIER ::= {id-CA-ECDH 2}
id-CA-ECDH-AES-CBC-CMAC-192 OBJECT IDENTIFIER ::= {id-CA-ECDH 3}
id-CA-ECDH-AES-CBC-CMAC-256 OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

٩-٢-٨ معلومات التحقق من صحة الوحدة الطرفية

توفر بنية البيانات معلومات مفصلة عن تنفيذ التحقق من صحة الوحدة الطرفية.

- **يجب** على معرّف المواد `protocol` أن يحدد البروتوكول *العام* للتحقق من صحة الوحدة الطرفية نظراً لتغير البروتوكول المحدد مع الوقت.
- **يجب** على إصدار `version` العدد الصحيح أن تحدد إصدار البروتوكول. وحالياً تدعم هذه المواصفة الإصدار ١. وتجدر الإشارة إلى أن الإصدارات الأخيرة لـ [TR-03110] تعرّف الإصدار ٢ لهذا البروتوكول، وهو لا يندرج ضمن نطاق هذه المواصفة.

```
TerminalAuthenticationInfo ::= SEQUENCE {
    protocol OBJECT IDENTIFIER(id-TA),
    version  INTEGER        -- MUST be 1

        }
```

٩-٢-٩ معرفات مواد التحقق من صحة الوحدة الطرفية

يجب استخدام معرّف المواد التالي:

```
id-TA OBJECT IDENTIFIER ::= {
  bsi-de protocols(2) smartcard(2) 2
}

id-TA-RSA               OBJECT IDENTIFIER ::= {id-TA 1}
id-TA-RSA-PSS-SHA-256   OBJECT IDENTIFIER ::= {id-TA-RSA 4}
id-TA-RSA-PSS-SHA-512   OBJECT IDENTIFIER ::= {id-TA-RSA 6}

id-TA-ECDSA             OBJECT IDENTIFIER ::= {id-TA 2}
id-TA-ECDSA-SHA-224     OBJECT IDENTIFIER ::= {id-TA-ECDSA 2}
id-TA-ECDSA-SHA-256     OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}
id-TA-ECDSA-SHA-384     OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}
id-TA-ECDSA-SHA-512     OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

٩-٢-١٠ *EFDIRInfo*

تغلف بنية البيانات نسخة كاملة عن محتوى الملف الأولي الشفاف EF.DIR الوارد في الملف الرئيسي.

```
  EFDIRInfo ::= SEQUENCE {
      protocol                        OBJECT IDENTIFIER(id-EFDIR),
      eFDIR                           OCTET STRING
  }

id-EFDIR OBJECT IDENTIFIER ::={
  id-icao-mrtd-security 13
}
```

٩-٢-١١ *التخزين على الرقاقة*

لبيان دعم البروتوكولات والمعايير المدعومة، **يجب** أن توفّر رقاقة وثيقة السفر الإلكترونية المقروءة آلياً `SecurityInfos` في الملفات الأولية الشفافة (يمكن العثور على البنية العامة لهذه الملفات في الوثيقة Doc 9303-10):

- الملف EF.CardAccess الوارد في الملف الرئيسي **مطلوب** إذا كان فتح الاتصال بكلمة سر مصدّق عليها مدعوماً برقاقة وثيقة السفر الإلكترونية المقروءة آلياً و**يجب** أن يحتوي على `SecurityInfos` ذات الصلة المطلوبة لفتح الاتصال بكلمة سر مصدّق عليها:
  - `PACEInfo`
  - `PACEDomainParameterInfo`
- الملف EF.CardSecurity الوارد في الملف الرئيسي **مطلوب** إذا:

- كان فتح الاتصال بكلمة سر مصدّق عليها مع تحديد مجالات التحقق من صحة الرقاقة مدعوماً برقاقة وثيقة السفر الإلكترونية المقروءة آلياً، أو
- إذا كان التحقق من صحة الوحدة الطرفية في الملف الرئيسي مدعوماً برقاقة وثيقة السفر الإلكترونية المقروءة آلياً، أو
- إذا كان التحقق من صحة الرقاقة في الملف الرئيسي مدعوماً بوثيقة السفر الإلكترونية المقروءة آلياً،

و**يجب** أن يحتوي على SecurityInfos:

- ChipAuthenticationInfo حسبما يطلبه للتحقق من صحة الرقاقة
- ChipAuthenticationPublicKeyInfo حسبما هو مطلوب للتحقق من صحة PACE-CAM/Chip
- TermninalAuthenticationInfo حسبما يطلبه التحقق من صحة الوحدة الطرفية
- EFDIRInfo إذا كان أكثر من تطبيق وثيقة السفر الإلكترونية المقروءة آلياً موجوداً على الرقاقة
- SecurityInfos الوارد في الملف الأولي EF.CardAccess

- الملف الرئيسي EF.DG14 الوارد في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً مطلوب إذا
- كان فتح الاتصال بكلمة سر مصدّق عليها مع تحديد المجالات العام/المتكامل مدعوماً برقاقة تطبيق وثيقة السفر الإلكترونية المقروءة آلياً، أو
- كان التحقق من صحة الوحدة الطرفية في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً مدعوماً برقاقة تطبيق وثيقة السفر الإلكترونية المقروءة آلياً، أو
- كان التحقق من صحة الرقاقة في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً مدعوماً برقاقة تطبيق وثيقة السفر الإلكترونية المقروءة آلياً

و**يجب** أن يحتوي على SecurityInfos التالية:

- ChipAuthenticationInfo كما هي مطلوبة من أجل التحقق من صحة الرقاقة
- ChipAuthenticationPublicKeyInfo حسبما هو مطلوب من أجل التحقق من صحة الرقاقة
- TermninalAuthenticationInfo حسبما هو مطلوب من أجل التحقق من صحة الوحدة الطرفية
- SecurityInfos التي يحتوي عليها الملف الأولي للاطلاع على البطاقة EF.CardAccess.

- المجموعة الكاملة من SecurityInfos (بما في ذلك SecurityInfos التي يحتوي عليها EF.CardAccess غير المحددة في الوثيقة Doc 9303) **يجب** تخزينها إضافياً في الملف الأولي لمجموعة البيانات ١٤ (EF.DG14) لتطبيق وثيقة السفر الإلكترونية المقروءة آلياً (انظر الوثيقة Doc 9303-10).

يجوز أن تحتوي الملفات على SecurityInfos خارج نطاق هذه المواصفة.

ملاحظة — في حين أن صحة SecurityInfos المخزّنة في الملف الأولي لمجموعة البيانات ١٤ والملف الأولي لأمن البطاقة محمية بالتحقق السلبي من الصحة، فإن الملف EF.CardAccess غير محمي.

٩-٣ وحدات بيانات بروتوكول التطبيق

٩-٣-١ *الطول الممدد*

اعتماداً على حجم مواد التشفير (المفاتيح العامة، التوقيعات)، **يجب** استخدام وحدات بيانات بروتوكول التطبيق ذات حقول الطول الممتدة لإرسال هذه البيانات إلى رقاقة وثيقة السفر الإلكترونية المقروءة آلياً وللاطلاع على تفاصيل الطول الممد انظر [ISO/IEC 7816-4].

٩-٣-١-١ رقاقات وثيقة السفر الإلكترونية المقروءة آلياً

بالنسبة لرقاقات وثيقة السفر الإلكترونية المقروءة آلياً، فإن دعم الطول الممدد **مشروط**. وإذا كانت خوارزميات الشيفرة وأحكام المفاتيح التي اختارتها دولة الاصدار تتطلب استخدام طول ممدد، **يجب** أن تدعم رقاقات وثيقة السفر الإلكترونية المقروءة آلياً الطول الممدد. وإذا كانت رقاقة وثيقة السفر الإلكترونية المقروءة آلياً تدعم الطول الممدد، **فيجب** بيان هذا في ATR/ATS أو في EF.ATR/INFO على النحو المحدد في [ISO/IEC 7816-4].

٩-٣-١-٢ الوحدات الطرفية

بالنسبة للوحدات الطرفية، فإن دعم الطول الممدد **مطلوب**. و**ينبغي** أن تفحص أي وحدة طرفية ما إذا كان أو لم يكن الدعم للطول الممدد مبيّناً في ATR/ATS لرقاقة وثيقة السفر الإلكترونية المقروءة آلياً أو في EF.ATR/INFO قبل استخدام هذا الخيار. و**يجب ألا** تستخدم الوحدة الطرفية الطول الممدد من أجل وحدات بيانات بروتوكول التطبيق لغير الأوامر التالية ما لم يبيَّن صراحة في ATR/ATS أو في EF.ATR/INFO المدخَل والمخرَج بالضبط لأحجام الحماية لرقاقة وثيقة السفر الإلكترونية المقروءة آلياً.

- MSE:Set KAT
- GENERAL AUTHENTICATE

٩-٣-٢ *سلسلة الأوامر*

- **يجب** استخدام سلسلة الأوامر من أجل أمر التحقق العام من الصحة (GENERAL AUTHENTICATE) لربط سلسلة الأوامر بتنفيذ بروتوكول فتح الاتصال بكلمة سر مصدق عليها. و**يجب ألا** تُستخدم سلسلة الأوامر لأغراض أخرى ما لم تبيّن الرقاقة ذلك بوضوح. وللاطلاع على التفاصيل بشأن سلسلة الأوامر انظر [ISO/IEC 7816-4].

٩-٣-٣ *مواد البيانات*

يجب على مرسل وحدة بيانات بروتوكول تطبيق الأمر أو الاستجابة أو يرسل مواد البيانات في خانة التاريخ بالترتيب المحدد في وصف وحدة بيانات بروتوكول التطبيق.

ملاحظة — ليس المطلوب أن تقبل مواد البيانات بأي ترتيب ولكن تحسين إمكانية التشغيل المتبادل، مثلاً من أجل MSE:Set AT/GENERAL AUTHENTICATE. ومع ذلك، ينبغي توخي الحذر في حالة أوامر مثل PSO:Verify Certifcate، حيث يكون الترتيب ثابتاً لأسباب تشفيرية.

٩-٤ مواد بيانات المفتاح العام

مادة بيانات مفتاح عام هي بنية قواعد التشفير الأساسية قيمة طول الوسم مشيّدة تحتوي على معرّف للمادة وعدة مواد بيانات محددة للسياق محفوظة داخل نموذج المفتاح العام لحامل البطاقة 0x7F49.

- معرّف المادة هو محدَّد حسب التطبيق ويشير لا إلى شكل المفتاح العام فقط (أي سياق مواد البيانات المحددة) لكن أيضاً إلى استخدامه.
- مواد البيانات المحددة حسب السياق يعرّفها معرّف المادة وتحتوي على قيمة المفتاح العام ومعايير النطاق.

يرد أدناه وصف شكل مواد بيانات المفاتيح العامة المستخدمة في هذه المواصفة.

٩-٤-١ ترميز مادة البيانات

يجب تحويل عدد صحيح غير موقّع إلى سلسلة ثمانية باستخدام التمثيل الثنائي للعدد الصحيح في شكل ذي نهاية كبيرة. و**يجب** استخدام العدد الأدنى من الثمانيات، أي **يجب ألا** تُستخدم الثمانيات الرئيسية ذات القيمة 0x00.

لترميز نقاط منحنى اهليلجي، **يجب** استخدام ترميز غير مضغوط وفقاً لـ [TR-03111].

٩-٤-٢ المفاتيح العامة ريفست وشمير وأدلمان

ترد في الجدول ٩ مواد البيانات الواردة في المفاتيح العامة ريفست وشمير وأدلمان. ويكون ترتيب مواد البيانات ثابتاً.

الجدول ٩ — المفتاح العام ريفست وشمير وأدلمان

Data Object	Notation	Tag	Type	CV Certificate
Object Identifier		0x06	Object Identifier	m
Composite modulus	*n*	0x81	Unsigned Integer	m
Public exponent	*e*	0x82	Unsigned Integer	m

٩-٤-٣ المفاتيح العامة لديفي–هيلمان

مواد البيانات التي يحتوي عليها مفتاح عام لديفي–هيلمان مبيّنة في الجدول ١٠. ويكون ترتيب مواد البيانات ثابتاً.

الجدول ١٠ — مواد البيانات للمفاتيح العامة لديفي–هيلمان

Data Object	Notation	Tag	Type
Object Identifier		0x06	Object Identifier
Prime modulus	p	0x81	Unsigned Integer
Order of the subgroup	q	0x82	Unsigned Integer
Generator	g	0x83	Unsigned Integer
Public Value	y	0x84	Unsigned Integer

ملاحظة — ترميز مكوّنات المفتاح كعدد صحيح غير موقّع يعني ضمنياً أن كلاً منهم مرمّز فوق العدد الأدنى من البايتات الممكنة، أي بدون ضبط البايتات السابقة على 0x00. وبصفة خاصة، فإن المفتاح العام ديفي–هيلمان يجوز ترميزه فوق عدد من البايتات أصغر من عدد بايتات الرئيسي.

٩-٤-٤ المفاتيح العامة للمنحنى الاهليلجي

مواد البيانات التي يحتوي عليها مفتاح عام لمنحنى اهليلجي مبيّنة في الجدول ١١. وترتيب مواد البيانات ثابت، ومعايير النطاق **المشروطة** **يجب** إما تكون كلها موجودة، باستثناء العامل المرافق، أو كلها غير موجودة على النحو التالي:

الجدول ١١ — مواد البيانات لمفاتيح عامة لبروتوكول ديفي–هيلمان للمنحنى الاهليلجي

Data Object	Notation	Tag	Type
Object Identifier		0x06	Object Identifier
Prime modulus	p	0x81	Unsigned Integer
First coefficient	a	0x82	Unsigned Integer
Second coefficient	b	0x83	Unsigned Integer
Base point	G	0x84	Elliptic Curve Point
Order of the base point	r	0x85	Unsigned Integer
Public point	Y	0x86	Elliptic Curve Point
Cofactor	f	0x87	Unsigned Integer

٩-٤-٥ المفاتيح العامة العابرة

بالنسبة للمفاتيح العامة العابرة فإن الشكل ومعايير النطاق معروفة بالفعل. ولذلك، فإن قيمة المفاتيح العامة البسيطة فقط، أي القيمة العامة y للمفاتيح العامة ديفي–هيلمان والنقطة العامة Y للمفاتيح العامة للمنحنى الاهليلجي، تُستخدم لنقل المفتاح العام العابر في مادة بيانات محددة السياق.

*ملاحظة — **يوصى** بالتحقق من المفاتيح العامة العابرة. وبالنسبة لديفي–هيلمان، فإن خوارزمية التحقق تتطلب أن تكون لدى رقاقة وثيقة السفر الإلكترونية المقروءة آلياً معرفة بمعايير النطاق (أي ترتيب المجموعة الفرعية المستخدمة) أكثر تفصيلاً مما يقدَّم عادة بواسطة PKCS#3.*

٩-٥ معايير النطاق

باستثناء معايير النطاق التي تحتوي عليها PACEInfo، **يجب** توفير جميع معايير النطاق بوصفها AlgorithmIdentifier (راجع القسم ٩-١).

داخل PACEInfo، **يجب** استخدام مرجع مباشر إلى معرّف معايير النطاق الموحدة الموصوفة في الجدول ١٢. و**يجب ألا** تستخدم معايير النطاق الصريحة التي توفرها PACEDomainParameterInfo تلك المعرّفات المحجوزة من أجل معايير النطاق الموحدة.

٩-٥-١ معايير النطاق الموحدة

ينبغي استخدام معرّفات معايير النطاق الموحدة الموصوفة في الجدول أدناه. و**يجب ألا** تستخدم معايير النطاق الصريحة تلك المعرّفات المحجوزة لمعايير النطاق الموحدة.

ينبغي استخدام معرّف المواد التالي للإشارة إلى معايير النطاق الموحدة في AlgorithmIdentifier (راجع القسم ٩-١):

```
standardizedDomainParameters OBJECT IDENTIFIER ::= {
  bsi-de algorithms(1) 2
}
```

داخل AlgorithmIdentifier **يجب** أن يحيل هذا المعرّف للمواد معرّف معيار النطاق الموحّد حسب ما يرد في الجدول ٩ بوصفه INTEGER، الوارد بوصفه parameters في AlgorithmIdentifier.

الجدول ١٢ — معايير النطاق الموحّدة

ID	*Name*	*Size (bit)*	*Type*	*Reference*
0	1024-bit MODP Group with 160-bit Prime Order Subgroup	1024/160	GFP	[RFC 5114]
1	2048-bit MODP Group with 224-bit Prime Order Subgroup	2048/224	GFP	[RFC 5114]
2	2048-bit MODP Group with 256-bit Prime Order Subgroup	2048/256	GFP	[RFC 5114]
3-7	RFU			
8	NIST P-192 (secp192r1)	192	ECP	[RFC 5114], [FIPS 186-4]
9	BrainpoolP192r1	192	ECP	[RFC 5639]
10	NIST P-224 (secp224r1) *	224	ECP	[RFC 5114], [FIPS 186-4]
11	BrainpoolP224r1	224	ECP	[RFC 5639]
12	NIST P-256 (secp256r1)	256	ECP	[RFC 5114], [FIPS 186-4]
13	BrainpoolP256r1	256	ECP	[RFC 5639]
14	BrainpoolP320r1	320	ECP	[RFC 5639]
15	NIST P-384 (secp384r1)	384	ECP	[RFC 5114], [FIPS 186-4]
16	BrainpoolP384r1	384	ECP	[RFC 5639]
17	BrainpoolP512r1	512	ECP	[RFC 5639]
18	NIST P-521 (secp521r1)	521	ECP	[RFC 5114], [FIPS 186-4]
19-31	RFU			

* لا يمكن استخدام هذا المنحنى مع تحديد المجالات المتكامل.

٩-٥-٢ *معايير النطاق الصريحة*

معرّف المادة dhpublicnumber أو ecPublicKey من أجل بروتوكول ديفي-هيلمان أو بروتوكول ديفي-هيلمان للمنحنى الاهليلجي، على التوالي، **يجب** استخدامهما للإشارة إلى معايير النطاق الصريحة في AlgorithmIdentifier (راجع القسم ٩-١):

```
dhpublicnumber OBJECT IDENTIFIER ::= {
```

```
  iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1
}

ecPublicKey OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) 1
}
```

في حالة المنحنيات الاهليلجية، **يجب** وصف معايير النطاق بصراحة في بنية `ECParameters`، الواردة بوصفها `parameters` في الـ `AlgorithmIdentifier`، أي **يجب ألا** تُستخدم المنحنيات المسماة ومعايير النطاق المضمّنة.

٩-٦ خوارزميات اتفاق المفاتيح

تدعم هذه المواصفة اتفاق مفاتيح ديفي–هيلمان وديفي–هيلمان للمنحنى الاهليلجي على النحو الملخص في الجدول التالي:

الجدول ١٣ — خوارزميات اتفاق المفاتيح

Algorithm / Format	***DH***	***ECDH***
Key Agreement Algorithm	[PKCS#3]	ECKA [TR-03111]
X.509 Public Key Format	[X9.42]	[TR-03111]
TLV Public Key Format	TLV, cf. Section 9.4.2	TLV, cf. Section 9.4.3
Ephemeral Public Key Validation	[RFC 2631]	[TR-03111]

٩-٧ آلية اشتقاق المفاتيح

٩-٧-١ وظيفة اشتقاق المفاتيح

وظيفة اشتقاق المفاتيح **KDF**(K,c)، معرّفة على النحو التالي:

المُدخل: المُدخلات التالية مطلوبة:

- القيمة السرّية المشتركة K **(مطلوبة)**
- A 32-bit, big-endian integer counter c **(مطلوبة)**

المُخرج: An octet string keydata.

الإجراءات: تؤدى الإجراءات التالية:

- keydata = **H**(K || c)
- Output octet string keydata

وظيفة اشتقاق المفتاح **KDF**(K,c) تتطلب دالة بصمة رقمية مناسبة يُرمز إليها بـ **H**()، أي أن طول البت لدالة البصمة الرقمية **يجب** أن يكون أكبر من أو مساوياً لطول بت المفتاح المشتق. و**يجب** تفسير قيمة البصمة الرقمية بوصفها مُخرجة لـ big-endian byte.

*ملاحظة — حرف K السرّي المشترك يُعرَّف بأنه سلسلة ثمانية. وإذا تولّد سر مشترك بواسطة اتفاق مفاتيح المنحنيات الاهليلجية [TR-03111]، **يجب** استخدام س-تنسيق من النقطة المولّدة.*

٩-٧-١-١ التشفير الثلاثي للبيانات

لاشتقاق مفاتيح ١٢٨-بت (١١٢-بت باستثناء بتات التعادل) للتشفير الثلاثي للبيانات [القاعدة القياسية الاتحادية لمعالجة المعلومات ٤٦-٣] **يجب** استخدام دالة البصمة الرقمية خوارزمية البصمة الرقمية المؤمّنة-١ [القاعدة القياسية الاتحادية لمعالجة المعلومات ١٨٠-٢] و**يجب** أداء الخطوات الاضافية التالية:

- استخدم من ١ إلى ٨ ثمانيات لتكوين البيانات الرئيسية أ والثمانيات من ٩ إلى ١٦ من البيانات الرئيسية ب.
- اضبط بتات التعادل للبيانات الرئيسية أ والبيانات الرئيسية ب لتكوين مفاتيح القاعدة القياسية لتشفير البيانات الصحيحة (اختيارية).

٩-٧-١-٢ القاعدة القياسية للتشفير المتقدم

لاشتقاق مفاتيح ١٢٨-بت القاعدة القياسية للتشفير المتقدم [القاعدة القياسية الاتحادية لمعالجة المعلومات ١٩٧] **يجب** استخدام دالة البصمة الرقمية خوارزمية البصمة الرقمية المؤمنة-١ [القاعدة القياسية الاتحادية لمعالجة المعلومات ١٨٠-٢] و**يجب** أداء الخطوة الإضافية التالية:

- استخدِم الثمانيات من ١ إلى ١٦ من البيانات الرئيسية، ولا تُستخدم ثمانيات إضافية.

لاشتقاق ١٩٢-بت و٢٥٦-بت القاعدة القياسية للتشفير المتقدم [القاعدة القياسية الاتحادية لمعالجة المعلومات ١٩٧] **يجب** استخدام المفاتيح خوارزمية البصمة الرقمية المؤمنة-٢٥٦ [القاعدة القياسية الاتحادية لمعالجة المعلومات ١٨٠-٢]. وبالنسبة لمفاتيح ١٩٢-بت القاعدة القياسية للتشفير المتقدم **يجب** أداء الخطوة الإضافية التالية:

- استخدِم الثمانيات من ١ إلى ٢٤ من البيانات الرئيسية، ولا تُستخدم ثمانيات إضافية.

٩-٧-٢ المفاتيح الأساسية للاطلاع على الوثيقة

حساب مفتاحين للتشفير الثلاثي للبيانات من مفتاح مبدئي (K) يُستخدم في إنشاء المفاتيح الأساسية للاطلاع على الوثيقة $K_{Enc} = \mathbf{KDF}(K,1)$ and $K_{MAC} = \mathbf{KDF}(K,2)$.

٩-٧-٣ فتح الاتصال بكلمة سرّ مصدّق عليها

لنجعل $\mathbf{KDF}_{\pi}(\pi) = \mathbf{KDF}(f(\pi),3)$ مفتاحاً لوظيفة الاشتقاق لاشتقاق مفاتيح تشفير من كلمة سر π. وترميز كلمات السر، أي $K= f(\pi)$ محدد في الجدول ١٤:

الجدول ١٤ ترميزات كلمة السر

كلمة السر	الترميز
الجزء المقروء آلياً	SHA-1(Document Number || Date of Birth || Date of Expiry)
رقم الاطلاع على البطاقة	[ISO/IEC 8859-1] encoded character string

ملاحظة — إن رقم الوثيقة المقرر استخدامه كدخل TD يكون دائماً رقم الوثيقة الكاملة. وفي حالة الوثائق من الحجم ١ (TD1) التي يكون رقمها أطول من تسعة حروف، يتعين أن يكون رقم الوثيقة متسلسلاً من خانة رقم الوثيقة وخانة البيانات الاختيارية في الجزء المقروء آلياً باستثناء حرف الحشو. انظر أيضاً الملاحظة ي) في الوثيقة القسم ٤-٢-٢ من الوثيقة Doc 9303-5.

٩-٧-٤ مفاتيح المراسلات المأمونية

مفاتيح التشفير والتحقق من الصحة مشتقّة مع $\mathbf{KDF}_{Enc}(K) = \mathbf{KDF}(K,1)$ and $\mathbf{KDF}_{MAC}(K) = \mathbf{KDF}(K,2)$ على التوالي، من K سرّي مشترك.

٩-٨ المراسلات المأمونة

٩-٨-١ بدء دورة زمنية

تُبدأ دورة زمنية عند إنشاء مراسلات مأمونة. وضمن دورة يجوز تغيير مفاتيح المراسلات المأمونة (أي المُنشأة بواسطة مراقبة الاضطلاع الأساسي أو فتح الاتصال بكلمة سر مصدّق عليها أو التحقق من صحة الرقاقة).

تستند المراسلات المأمونة إما إلى التشفير الثلاثي للبيانات [القاعدة القياسية الاتحادية لمعالجة المعلومات ٤٦-٣] أو القاعدة القياسية للتشفير المتقدم [القاعدة القياسية الاتحادية لمعالجة المعلومات ١٩٧] بطريقة قم بالتشفير ثم تحقق من الصحة، أي يتم حشو البيانات وتشفيرها وبعد ذلك يتم إدخال البيانات المشفّرة المشكّلة في حساب التحقق من الصحة. و**يجب** اشتقاق مفاتيح الدورة الزمنية باستخدام وظيفة اشتقاق المفاتيح الموصوفة في القسم ٩-٧-١.

ملاحظة — يتم الحشو دائماً بواسطة طبقة المراسلات المأمونة، لذلك لا حاجة لأن يؤدي رمز التحقق من صحة الرسالة الكامن أي حشو داخلي.

٩-٨-٢ عداد تتابع الارسال

يجب استخدام عدد صحيح غير موقّع كعداد لتتابع الارسال. و**يجب** أن يكون حجم بت عداد تتابع الارسال مساوياً لحجم الكتلة لشيفرة الكتلة المستخدمة لتأمين المراسلات، أي، ٦٤ بت بالنسبة إلى التشفير الثلاثي للبيانات و١٢٨ بت بالنسبة إلى القاعدة القياسية للتشفير المتقدم.

يجب زيادة عداد تتابع الارسال كل مرة قبل إصدار أمر أو استجابة من وحدة بيانات بروتوكول التطبيق، أي، إذا كانت قيمة البدء هي x، في الأمر الأول فإن قيمة عداد تتابع الارسال هي x+1. وقيمة عداد تتابع الارسال بالنسبة للاستجابة الأولى هي x+2.

إذا أعيد تشغيل المراسلات المأمونة، يُستخدم عداد تتابع الارسال على النحو التالي:

- الأوامر المستخدمة لاتفاق المفاتيح تُحمى بمفاتيح الدورة الزمنية القديمة وعداد تتابع الارسال القديم. وينطبق هذا بصفة خاصة بالنسبة للاستجابة للأمر الأخير المُستخدم لاتفاق مفتاح الدورة الزمنية.
- عداد تتابع الارسال مضبوط على قيمة تشغيله الجديدة، انظر القسم ٩-٨-٦-٣ بالنسبة إلى التشفير الثلاثي للبيانات/ القسم ٩-٨-٧-٣ بالنسبة إلى القاعدة القياسية للتشفير المتقدم.
- تُستخدم مفاتيح الدورة الزمنية الجديدة وعداد تتابع الارسال الجديد لحماية الأوامر/الاستجابات اللاحقة.

٩-٨-٣ إنهاء الدورة الزمنية

يجب أن تقوم رقاقة وثيقة السفر الإلكترونية المقروءة آلياً بإلغاء المراسلات المأمونة إذا وفقط إذا حدث خطأ في مراسلة مأمونة أو تم تسلّم أمر بسيط من وحدة بيانات بروتوكول التطبيق.

في حالة إلغاء المراسلات المأمونة، **يجب** أن تحذف رقاقة وثيقة السفر الإلكترونية المقروءة آلياً مفاتيح الدورة الزمنية المخزّنة وأن تعيد حقوق الاطلاع على الوحدة الطرفية إلى الوضع السابق.

*ملاحظة — **يجوز** أن تختار رقاقة وثيقة السفر الإلكترونية المقروءة آلياً بشكل ضمني الملف الرئيسي عند إنهاء دورة زمنية.*

٩-٨-٤ بنية المراسلة للمراسلات المأمونة الصادرة عن وحدات بيانات بروتوكول التطبيق

يجب استخدام مواد بيانات المراسلات المأمونة (انظر [ISO/IEC 7816-4]) بالترتيب التالي:

- أمر وحدة بيانات بروتوكول التطبيق: 'DO'8E' ['DO'97'] ['DO'85' or DO'87'].
- استجابة وحدة بيانات بروتوكول التطبيق: 'DO'8E' ['DO'99'] ['DO'85' or DO'87'].

في الحالة التي يكون فيها INS مزدوجاً، **يجب** استخدام مادة البيانات 'Do'87، وإذا كان INS مفرداً، **يجب** استخدام مادة البيانات 'Do'85.

يجب ترميز جميع مواد بيانات المراسلات المأمونة بقواعد التشفير الأساسية قيمة طول الوسم على النحو المحدد في [ISO/IEC 7816-4]. و**يجب** إدراج عنوان الأمر في حساب رمز التحقق من صحة الرسالة، لذلك **يجب** استخدام بايت الدرجة CLA = 0x0C.

سيتم تعديل القيمة الفعلية لـ Lc إلى 'Lc بعد تطبيق المراسلات المأمونة. وإذا كان ذلك مطلوباً، يجوز اختيارياً إدراج مادة بيانات ملائمة في الجزء الخاص ببيانات وحدة بيانات بروتوكول التطبيق بغية نقل القيمة الأصلية لـ Lc.

يبيّن الشكل ٤ تحويل أمر غير محمي لوحدة بيانات بروتوكول التطبيق إلى أمر محمي لوحدة بيانات بروتوكول التطبيق في حالة توافر البيانات وLe. وإذا لم تتوافر أي بيانات، استبعد بناء '87' DO. وإذا لم تتوافر Le، استبعد بناء '97' DO. ولتفادي الغموض **يوصى** بعدم استخدام خانة قيمة خالية من مادة بيانات Le (انظر أيضاً Section 10.4 of [ISO/IEC 7816-4]).

يبيّن الشكل ٥ تحوّل استجابة غير محمية لوحدة بيانات بروتوكول التطبيق إلى استجابة محمية لوحدة بيانات بروتوكول التطبيق في حالة توافر البيانات. وإذا لم تتوافر البيانات، استبعد بناء '87' DO.

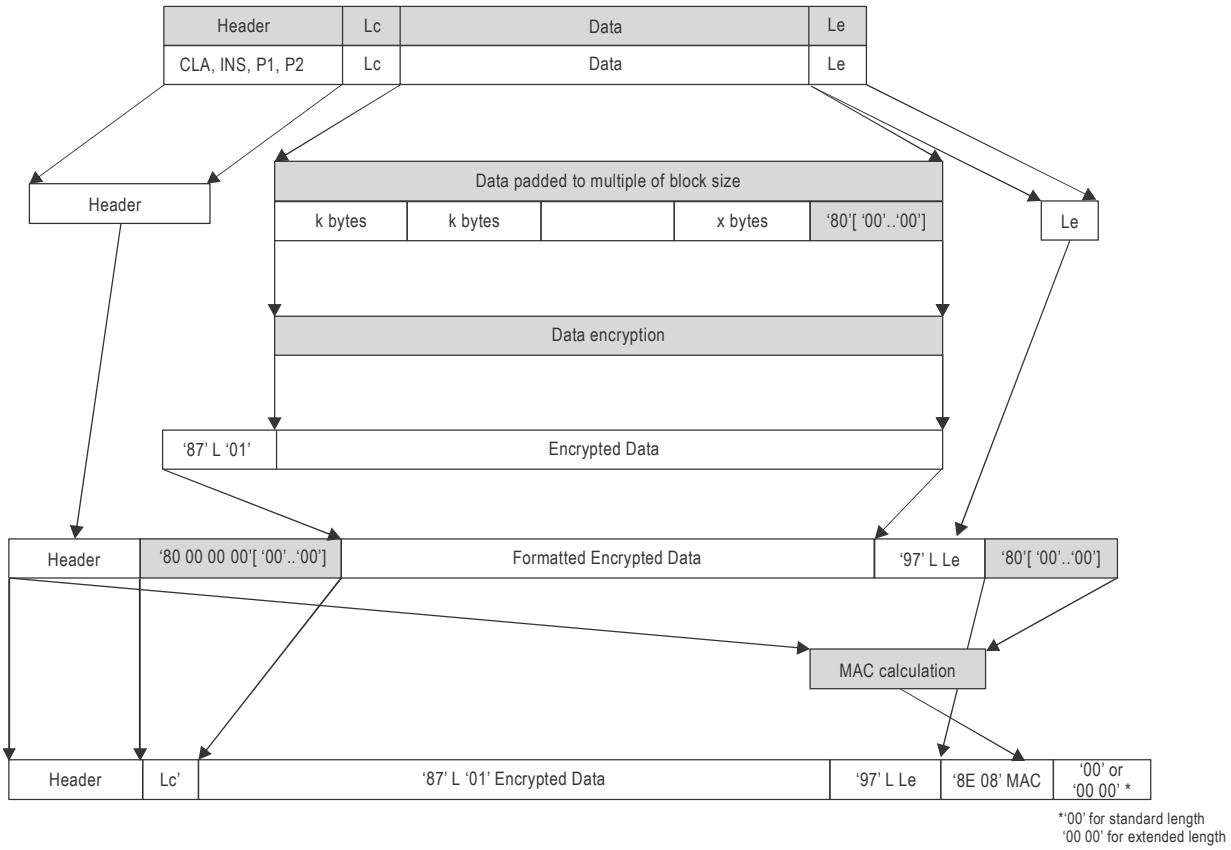
٩-٨-٥ *أخطاء المراسلات المأمونة*

إلغاء القناة المأمونة لتطبيق وثيقة السفر الإلكترونية المقروءة آلياً يحدث عندما:

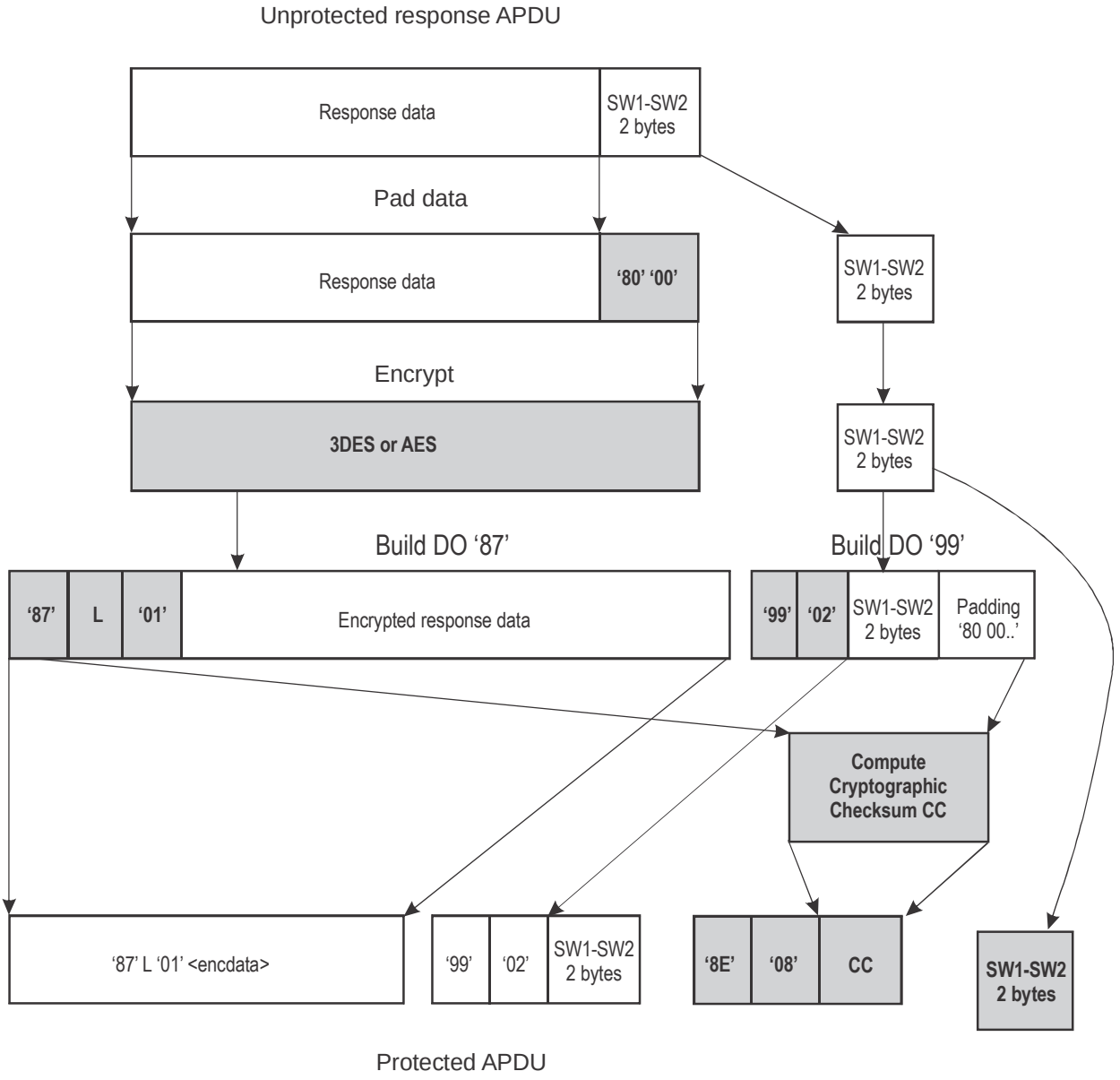
- يُقطع التيار الكهربائي عن الدائرة المتكاملة اللاتلامسية؛
- أو تتعرّف الدائرة المتكاملة اللاتلامسية على خطأ مراسلات مأمونة حين تفسّر أمراً. وفي هذه الحالة يجب الافادة بوضع البايتات بدون مراسلات مأمونة.

في حالة إلغاء المراسلات المأمونة، **يجب** أن تقوم رقاقة وثيقة السفر الإلكترونية المقروءة آلياً بحذف مفاتيح الدورة الزمنية المخزّنة وإعادة حقوق الاطلاع على الوحدة الطرفية للوضع السابق.

*ملاحظة — **يجوز** أن توجد ظروف أخرى تقوم فيها الدائرة المتكاملة اللاتلامسية بإلغاء الدورة الزمنية. وليس من الممكن تقديم قائمة كاملة بمثل هذه الظروف.*



الشكل ٥ حساب وحدة بيانات بروتوكول التطبيق لأمر مراسلات مأمونة لبايت تفتيش منتظم



الشكل ٦ حساب وحدة بيانات بروتوكول التطبيق لاستجابة مراسلات مأمونة لبايت تفتيش منتظم

٩-٨-٦ طرائق تشغيل التشفير الثلاثي للبيانات

٩-٨-٦-١ التشفير

يُستخدم التشفير الثلاثي للبيانات بمفتاحين في طريقة تسلسل كتلة الشيفرة مع zero IV (i.e. 0x00 00 00 00 00 00 00 00) وفقاً لـ [ISO/IEC 11568-2]. الحشو وفقاً لـ [ISO/IEC 9797-1] يُستخدم الأسلوب ٢ للحشو.

٩-٨-٦-٢ التحقق من صحة الرسالة

تُحسب تدقيقات المجموع التشفيرية باستخدام [ISO/IEC 9797-1] الخوارزمية ٣ لرمز التحقق من صحة الرسالة مع كتلة الشيفرة للقاعدة القياسية لتشفير البيانات، zero IV (٨ بايتات)، و [ISO/IEC 9797-1] الأسلوب ٢ للحشو. و**يجب** أن يكون طول رمز التحقق من صحة الرسالة ٨ بايتات.

بعد تحقق من الصحة بنجاح **يجب** أن يكون مخطط البيانات المراد أن يُطبَّق عليه رمز التحقق من صحة الرسالة مضافاً قبله عداد تتابع الارسال.

٩-٨-٦-٣ عداد تتابع الارسال

لتأمين المراسلات عقب مراقبة الاضطلاع الأساسي، **يجب** بدء تشغيل عداد تتابع الارسال عن طريق سلسلة البايتات الأربع الأقل أهمية من RND.IC و RND.IFD، على التوالي.

SSC = RND.IC (4 least significant bytes) || RND.IFD (4 least significant bytes).

In all other cases, the SSC SHALL be initialized to zero (i.e. 0x00 00 00 00 00 00 00 00).

٩-٨-٧ طرائق تشغيل القاعدة القياسية للتشفير المتقدم

٩-٨-٧-١ التشفير

من أجل تشفير الرسائل، **يجب** استخدام القاعدة القياسية للتشفير المتقدم [القاعدة القياسية الاتحادية لمعالجة المعلومات ١٩٧] بطريقة تسلسل كتلة الشيفرة وفقاً لـ [ISO/IEC 10116] مع المفتاح KS_{Enc} and IV = **E**(KS_{Enc}, SSC).

٩-٨-٧-٢ التحقق من صحة الرسائل

من أجل التحقق من صحة الرسائل، **يجب** استخدام القاعدة القياسية للتشفير المتقدم في [SP 800-38B] CMAC-mode مع KS_{MAC} مع رمز للتحقق من صحة الرسالة طوله ٨ بايتات. و**يجب** إضافة مخطط البيانات المراد التحقق من صحته مسبقاً بواسطة عداد تتابع الارسال.

٩-٨-٧-٣ عداد تتابع الارسال

يجب بدء تشغيل عداد تتابع الارسال لصفر (00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 i.e. 0x00).

١٠- المراجع (معيارية)

X9.42]	ANSI: X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, 1999
[ISO/IEC 7816-4]	ISO/IEC 7816-4:2013 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange
[ISO/IEC 7816-8]	ISO/IEC 7816-8:2019 Identification cards — Integrated circuit cards — Part 8: Commands and mechanisms for security operations
[ISO/IEC 8859-1]	ISO/IEC 8859-1:1998 Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1
[ISO/IEC 9796-2]	ISO/IEC 9796-2:2010 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms
[ISO/IEC 9797-1]	ISO/IEC 9797-1:2011 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
[ISO/IEC 10116]	ISO/IEC 10116:2017 Information technology — Security techniques — Modes of operation for an n-bit block cipher
[ISO/IEC 11568-2]	ISO/IEC 11568-2:2012 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle
[ISO/IEC 11770-2]	ISO/IEC 11770-2:2018 IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques
[FIPS 46-3]	NIST FIPS PUB 46-3, Data Encryption Standard (DES), 1999
[FIPS 180-4]	NIST FIPS PUB 180-4, Secure hash standard, 2015
[FIPS 186-4]	NIST FIPS PUB 186-4, Digital Signature Standard (DSS), 2013
[FIPS 197]	NIST FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), 2001
[SP 800-38B]	NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
[RFC 2631]	Rescorla, Eric: RFC 2631 Diffie-Hellman key agreement method, 1999
[RFC 3447]	Jonsson, Jakob and Kaliski, Burt: RFC 3447, Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1, 2003
[RFC 5114]	Lepinski, Matt; Kent, Stephen: RFC 5114 Additional Diffie-Hellman Groups for Use with IETF Standards, 2008
[RFC 5280]	D. Cooper, S. Santesson, S. Farrell, S. Boyen, R. Housley, W. Polk, RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008
[RFC 5639]	Lochter, Manfred; Merkle, Johannes: RFC 5639 Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010
[TR-03110]	BSI: Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents
[TR-03111]	BSI: Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 2012
[PKCS#1]	RSA Laboratories, PKCS#1 v2.2: RSA Cryptography Standard, 2012
[PKCS#3]	RSA Laboratories, PKCS#3: Diffie-Hellman key-agreement standard, 1993
[Keesing2009]	J. Bender, D. Kügler: Introducing the PACE solution, in: Keesing Journal of Documents & Identity, Issue 30, Keesing, 2009.

[BFK2009] J. Bender, M. Fischlin, D. Kügler: Security Analysis of the PACE Key-Agreement Protocol, in: Proceedings ISC 2009, LNCS volume 5735, Springer, 2009.

[BCIMRT2010] Brier, Eric; Coron, Jean-Sébastien; Icart, Thomas; Madore, David; Randriam, Hugues; and Tibouch, Mehdi, Efficient Indifferentiable Hashing into Ordinary Elliptic Curves, Advances in Cryptology – CRYPTO 2010, Springer-Verlag, 2010

– – – – – – – – – – –

المرفق (أ) بالجزء ١١

انتروبيا مفاتيح الاطلاع المشتقة من الجزء المقروء آلياً (إعلامية)

تبيّن أن مراقبة الاطلاع الأساسي، بسبب بساطتها، هي بروتوكول ناجح للغاية ويُنفَّذ في كل جواز سفر الكتروني مقروء آلياً تقريباً.

الأمن الذي توفّره الاطلاع الأساسي محدود بواسطة تصميم البروتوكول. ويتم إنشاء المفتاحين للاطلاع الأساسي على الوثيقة (K_{Enc} and K_{MAC}) من بيانات مطبوعة بعشوائية محدودة للغاية. والبيانات التي تُستخدم لإنشاء المفتاحين هي رقم الوثيقة وتاريخ الميلاد وتاريخ انتهاء الصلاحية. ونتيجة لذلك فإن المفتاحين الناشئين عن ذلك لهما انتروبيا منخفضة نسبياً وهما ضعيفان تشفيرياً. وتعتمد الانتروبيا الفعلية بشكل رئيسي على نوع رقم الوثيقة. وبالنسبة لوثيقة سفر صالحة لعشر سنوات فإن القوة القصوى للمفتاحين هي تقريباً:

- ٥٦ بايت بالنسبة لرقم وثيقة عددي ($365^2 * 10^{12}$ إمكانيات)
- ٧٣ بايت بالنسبة لرقم وثيقة أبجدي عددي ($365^2*36^9*10^3$ إمكانيات).

في الحالة الثانية خاصة يتطلب هذا التقدير أن يكون قد تم اختيار رقم الوثيقة عشوائياً وبشكل موحد وليس هذا هو الحال في العادة. واعتماداً على معرفة الباحث بالتجريب، فإن الانتروبيا الفعلية لمفتاح الاطلاع الأساسي على الوثيقة قد تكون أدنى، مثلاً إذا كان الباحث بالتجريب يعرف جميع أرقام الوثائق المستخدمة أو يستطيع الربط بين أرقام الوثائق وتواريخ انتهاء الصلاحية.

لا توجد طريقة مباشرة لتقوية مراقبة الاطلاع الأساسي نظراً لأن حدوده ملازمة لتصميم البروتوكول استناداً إلى تشفير تماثلي ("مفتاح سرّي"). ويجب (بالإضافة إلى ذلك) أن تستخدم آلية مراقبة اضطلاع قوية تشفيرياً تشفيراً لا تماثلي ("مفتاح عام").

تمّ تصميم فتح الاتصال بكلمة سرّ مصدّق عليها (PACE) للتغلّب على هذه المشكلة. وهو يستخدم تشفيراً لا تماثلي لإنشاء مفاتيح الدورات الزمنية، التي قوتّها مستقلة عن انتروبيا كلمة السر المستخدمة. وإذا نُفِّذ فتح الاتصال بكلمة سر مصدّق عليها بتشفير المنحنى الاهليلجي بمنحنيات ٢٥٦ بت والقاعدة القياسية للتشفير المتقدم AES-128 (اختيار شائع)، تكون لمفاتيح الدورات الزمنية انتروبيا ١٢٨ بت.

يجب التمييز بين نوعين من الهجمات:

- الاستخلاص: هذه هي هجمة على الانترنت، أي يحاول الباحث بالتجريب الاطلاع على الدائرة المتكاملة اللاتلامسية في الوقت الحقيقي، مثلاً عن طريق تخمين كلمة السر. وإذا كان البروتوكول المستخدم لحماية الدائرة المتكاملة اللاتلامسية خالياً من ضعف تشفيري، فإن احتمال نجاح الباحث بالتجريب يُعطى بواسطة الوقت الذي يطلع فيه الباحث بالتجريب على الدائرة المتكاملة ومدة محاولة واحدة لتخمين كلمة السر وانتروبيا جواز السفر.
- اختلاس المعلومات: هذه هي هجمة خارج الانترنت، أي يحاول الباحث بالتجريب فك تشفير الاتصال الذي يتم التدخل غير المرخّص به فيه بدون الاطلاع على الدائرة المتكاملة اللاتلامسية. وإذا كان البروتوكول المستخدم لإنشاء مفتاحي الدورة الزمنية خالياً من ضعف تشفيري، فإن احتمال النجاح يُعطى بواسطة قوة مفتاحي الدورة الزمنية وقوة الحساب المتوافرة للباحث بالتجريب.

للمزيد من المعلومات انظر [Keesing2009] ولمناقشة عامة بشأن انتروبيا مفتاحي الدورة الزمنية ومقارنة لمراقبة الاطلاع الأساسي وفتح الاتصال بكلمة سر مصدّق عليها، و [BFK2009] لتحليل تشفيري لفتح الاتصال بكلمة سر مصدّق عليها.

– – – – – – – – – – –

المرفق (ب) بالجزء ١١

ترميز النقاط من أجل بروتوكول ديفي–هيلمان للمنحنى الاهليلجي — تحليل المجالات المتكامل (إعلامي)

B.1 HIGH-LEVEL DESCRIPTION OF THE POINT ENCODING METHOD

The algorithm takes as inputs the curve parameters (a, b, p, f) where (a, b) are the curve coefficients, p is the characteristic of the prime field over which the curve

$$E : y^2 \equiv x^3 + ax + b \ (mod\ p)$$

is defined. The order of E is always of the form fq for some prime q and f is called the co-factor. PACE v2 requires the generation of a point that belongs to the q-subgroup of E that we denote by $E[q]$. The point encoding also takes as input a number t such that

$$0 < t < p$$

and returns, in constant time, a point that belongs to $E[q]$. As described in [BCIMRT2010], point encoding comes in two flavours, depending on the coordinate system preferred by the implementation:

- A first implementation, described in Section B.2, outputs the elliptic curve point in affine coordinates (x, y);
- An alternate implementation, presented in Section B.3, outputs the same point in Jacobian coordinates (X, Y, Z).

Irrespective of the option taken, the generated point is identical in the sense that

$$x = XZ^{-2} \ mod\ p \ and \ y = YZ^{-3} \ mod\ p$$

and the implementation of the subsequent phase of PACE v2 (the elliptic curve Diffie-Hellman key exchange phase) can therefore take advantage of using the option that best fits the interface of the cryptographic API that performs elliptic-curve operations.

As noted hereafter, point encoding for affine coordinates roughly requires two modular exponentiations modulo p whereas point encoding for Jacobian coordinates requires only a single one.

Note that for the two available implementations, point encoding explicitly requires that $p \equiv 3 \ mod\ 4$.

B.2 IMPLEMENTATION FOR AFFINE COORDINATES

The algorithm is implemented as follows:
Inputs: curve parameters (a, b, p, f) and t such that $0 < t < p$
Output: a point (x, y) in the prime-order subgroup $E[q]$ of E

1. Compute $\alpha = -t^2 \ mod\ p$
2. Compute $X_2 = -ba^{-1}(1+(\alpha+\alpha^2)^{-1}) \ mod\ p$
3. Compute $X_3 = \alpha X_2 \ mod\ p$
4. Compute $h_2 = (X_2)^3 + a X_2 + b \ mod\ p$
5. Compute $h_3 = (X_3)^3 + a X_3 + b \ mod\ p$
6. Compute $U = t^3 h_2 \ mod\ p$

7. Compute $A = (h_2)^{p-1-(p+1)/4} \bmod p$
8. If $A^2 h_2 = 1 \bmod p$ define $(x, y) = (X_2, A\, h_2 \bmod p)$
9. Otherwise define $(x, y) = (X_3, A\, U \bmod p)$
10. Output $(x, y) = [f]\,(x, y)$.

Implementation Notes

Neglecting modular multiplications and additions, the execution time of the above implementation is dominated by two modular exponentiations:

- Step 2 can be rewritten

$$X_2 = -ba^{-1}(1+(\alpha+\alpha^2)^{-1}) = -b(1+\alpha+\alpha^2)\,(a(\alpha+\alpha^2))^{p-2} \bmod p$$

  which essentially amounts to a modular exponentiation with exponent $p-2$;

- Step 7 is a modular exponentiation with exponent $p-1-(p+1)/4$.

Note.— Step 10 requires a scalar multiplication by the co-factor f. *For many curves, the co-factor is equal to 1 so that this scalar multiplication can be avoided.*

B.3 IMPLEMENTATION FOR JACOBIAN COORDINATES

The algorithm is implemented as follows:

Inputs: curve parameters (a, b, p, f) and t such that $0 < t < p$

Output: a point (X, Y, Z) in the prime-order subgroup $E[q]$ of E

1. Compute $\alpha = -t^2 \bmod p$
2. Compute $Z = a(\alpha+\alpha^2) \bmod p$
3. Compute $X_2 = -bZ\,(1+\alpha+\alpha^2) \bmod p$
4. Compute $X_3 = \alpha\, X_2 \bmod p$
5. Compute $h_2 = (X_2)^3 + a\, X_2 Z^4 + b\, Z^6 \bmod p$
6. Compute $h_3 = (X_3)^3 + a\, X_3 Z^4 + b\, Z^6 \bmod p$
7. Compute $U = -\alpha\, t\, h_2 \bmod p$
8. Compute $A = (h_2)^{p-1-(p+1)/4} \bmod p$
9. If $A^2 h_2 = 1 \bmod p$ define $(X, Y, Z) = (X_2, A\, h_2 \bmod p, Z)$
10. Otherwise define $(X, Y, Z) = (X_3, A\, U \bmod p, Z)$
11 Output $(X, Y, Z) = [f](X, Y, Z)$.

Implementation Notes

Neglecting modular multiplications and additions, the execution time of the above implementation is dominated by the single modular exponentiation of Step 7. Therefore, it is expected to be roughly twice as fast as the implementation for affine coordinates.

Note.— The scalar multiplication in Step 10 can be completely avoided when the co-factor f *is equal to 1.*

– – – – – – – – – – –

المرفق (ج) بالجزء ١١

علم الدلالة للتحدّي (إعلامي)

تأمّل في بروتوكول تحدٍّ – استجابة مستند إلى توقيع بين رقاقة وثيقة سفر إلكترونية مقروءة آلياً (دائرة متكاملة) ووحدة طرفية (جهاز التقارن القربي)، حيث تريد رقاقة وثيقة السفر الإلكترونية المقروءة آلياً إثبات معرفة مفتاحها الخاص SK_{IC}:

- ترسل الوحدة الطرفية تحدياً تم اختياره عشوائياً c إلى رقاقة وثيقة السفر الإلكترونية المقروءة آلياً.
- تستجيب رقاقة وثيقة السفر الإلكترونية المقروءة آلياً بالتوقيع $s=\mathbf{Sign}(SK_{IC},c)$.

في حين أن هذا بروتوكول بسيط وفعال جداً، فإن رقاقة وثيقة السفر الإلكترونية المقروءة آلياً توقّع في الحقيقة على الرسالة c دون معرفة دلالة هذه الرسالة. ونظراً لأن التوقيعات تقدم دليلاً على الصحة قابلاً للإحالة، فإن أي طرف ثالث يمكنه – من حيث المبدأ – الاقتناع بأن رقاقة وثيقة السفر الإلكترونية المقروءة آلياً قد وقّعت على هذه الرسالة في الحقيقة.

على الرغم من أن c ينبغي أن تكون سلسلة بتات عشوائية، تستطيع الوحدة الطرفية كذلك توليد هذه السلسلة من البتات بطريقة لا يمكن التنبؤ بها لكن يمكن التحقق منها (علانية)، مثلاً، دع SK_{IFD} تكون المفتاح الخاص للوحدة الطرفية و

$$c = \mathbf{Sign}(SK_{IFD},ID_{IC}||Date||Time||Location)$$

تكون التحدّي المتولّد باستخدام خطة توقيع مع استرداد رسالة. ويضمن التوقيع أن الوحدة الطرفية قد أصدرت هذا التحدّي في الحقيقة. وبسبب قابلية توقيع الوحدة الطرفية للتحويل، فإن أي طرف ثالث لديه ثقة في الوحدة الطرفية ويعرف المفتاح العام المناظر PK_{IFD} يمكنه أن يتحقق من أن التحدّي قد أنشئ بشكل صحيح عن طريق التحقق من هذا التوقيع. وفضلاً عن هذا، بسبب إمكان تحويل توقيع رقاقة وثيقة السفر الإلكترونية المقروءة آلياً عند التحدّي، يمكن أن يستنتج الطرف الثالث أن الزعم أصبح حقيقة: في الواقع أن رقاقة وثيقة السفر الإلكترونية المقروءة آلياً كانت في تاريخ ووقت معينين في موقع معين.

من الناحية الإيجابية، يجوز أن تستخدم الدول علم الدلالة للتحدّي لاستخدامها الداخلي، مثلاً، لإثبات أن شخصاً معيّناً قد هاجر حقاً. ومن الناحية السلبية يمكن إساءة استخدام مثل هذه الأدلة لتتبع الأشخاص. وبصفة خاصة نظراً لأن التحقق الإيجابي لا يقتصر على الوحدات الطرفية المرخّصة، فإن إساءة الاستخدام ممكنة. وقد يكون أسوأ سيناريو هو أن تكون رقائق وثائق السفر الإلكترونية المقروءة آلياً التي توفّر التحقق الإيجابي بدون مراقبة اطلاع أساسي. وفي هذه الحالة قد يتم إنشاء نظام تتبع قوي للغاية عن طريق وضع وحدات معدات مأمونة في أماكن بارزة. ولا يمكن تزييف السجلات الناتجة عن ذلك بسبب التوقيعات. ومراقبة الاطلاع الأساسي تقلل من هذه المشكلة إلى حد ما، نظراً لأن التفاعل مع حامل الوثيقة مطلوب. ومع ذلك، تظل المشكلة قائمة، لكنها تقتصر على أماكن تتم فيها قراءة وثيقة سفر حامل الوثيقة على أي حال، مثلاً، بواسطة شركات الطيران أو الفنادق.

قد يعترض المرء بأنه خاصة في سيناريو لا تلامسي، قد يتم اختلاس المعلومات من التحديات وإعادة استخدامها في تاريخ أو وقت أو موقع مختلف وبالتالي يُجعل الدليل غير جدير بالثقة على الأقل. وفي حين أن اختلاس معلومات التحديات ممكن فنياً، فإن الحجة لا تزال غير صالحة. وبناء على افتراض فإن أي وحدة طرفية موثوق من أنها تنتج التحديات بشكل صحيح، ويمكن افتراض أنها تحققت من هوية رقاقة وثيقة السفر الإلكترونية المقروءة آلياً قبل بدء التحقق الإيجابي. وهكذا، سيتضمن التحدّي المختلسة منه المعلومات هوية مختلفة عن هوية القائم بالإثبات الموقّع على التحدّي.

– – – – – – – – – – –

المرفق (د) بالجزء ١١

مثال محلول: مراقبة الاطلاع الأساسي (إعلامي)

D.1 COMPUTE KEYS FROM KEY SEED (K_{SEED})

This Section provides an example for derivation of 3DES keys from a seed value K_{seed}. This procedure will be used as a "subroutine" in the examples for Basic Access Control.

Input:

K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'

Compute encryption key (c = '00000001'):

1. Concatenate K_{seed} and c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000001'

2. Calculate the SHA-1 hash of D:
   H_{SHA-1}(D) = 'AB94FCEDF2664EDFB9B291F85D7F77F27F2F4A9D'

3. Form DES keys K_a and K_b, intended to be used as first and second key for 3DES (i.e. the 3DES key is the concatenation of K_a and K_b):
   $K_{a'}$ = 'AB94FCEDF2664EDF'
   $K_{b'}$ = 'B9B291F85D7F77F2'

4. Adjust parity bits:
   K_a = 'AB94FDECF2674FDF'
   K_b = 'B9B391F85D7F76F2'

Compute MAC computation key (c = '00000002'):

1. Concatenate K_{seed} and c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000002'

2. Calculate the SHA-1 hash of D:
   H_{SHA-1}(D) = '7862D9ECE03C1BCD4D77089DCF131442814EA70A'

3. Form keys $K_{a'}$ and $K_{b'}$:
   $K_{a'}$ = '7862D9ECE03C1BCD'
   $K_{b'}$ = '4D77089DCF131442'

4. Adjust parity bits:
   K_a = '7962D9ECE03D1ACD'
   K_b = '4C76089DCE131543'

D.2 DERIVATION OF DOCUMENT BASIC ACCESS KEYS (K_{ENC} AND K_{MAC})

This section provides examples how the Basic Access Keys are derived from the MRZ.

TD2 MRZ, document number exceeds 9 characters

1. Read the MRZ
   MRZ = I<UTOSTEVENSON<<PETER<JOHN<<<<<<<<<<
   D23145890<UTO3407127M95071227349<<<8

2. Construct the 'MRZ information' from the MRZ

Document number	= D23145890734	check digit = 9
Date of Birth	= 340712	check digit = 7
Date of Expiry	= 950712	check digit = 2
MRZ_information	= D23145890734934071279507122	

Continue with step 3.

TD2 MRZ, document number 9 characters

1. Read the MRZ:

MRZ = I<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<
L898902C<3UTO6908061F9406236<<<<<<<8

2. Construct the 'MRZ_information' from the MRZ:

Document number	= L898902C<	check digit = 3
Date of birth	= 690806	check digit = 1
Date of expiry	= 940623	check digit = 6
MRZ_information	= L898902C<3690806194062 36	

Continue with step 3.

TD1 MRZ, document number exceeds 9 characters

1. Read the MRZ

MRZ = I<UTOD23145890<7349<<<<<<<<<<<
3407127M9507122UTO<<<<<<<<<<<2
STEVENSON<<PETER<JOHN<<<<<<<<<

2. Construct the 'MRZ information' from the MRZ

Document number	= D23145890734	check digit = 9
Date of Birth	= 340712	check digit = 7
Date of Expiry	= 950712	check digit = 2
MRZ_information	= D23145890734934071279507122	

Continue with step 3.

TD1 MRZ, document number 9 characters

1. Read the MRZ

MRZ = I<UTOL898902C<3<<<<<<<<<<<<<<
6908061F9406236UTO<<<<<<<<<<<1
ERIKSSON<<ANNA<MARIA<<<<<<<<<<

2. Construct the 'MRZ information' from the MRZ

Document number	= L898902C<	check digit = 3
Date of Birth	= 690806	check digit = 1
Date of Expiry	= 940623	check digit = 6
MRZ_information	= L898902C<3690806194062 36	

3. Calculate the SHA-1 hash of 'MRZ_information':

H_{SHA-1}(MRZ_information) = '239AB9CB282DAF66231DC5A4DF6BFBAEDF477565'

4. Take the most significant 16 bytes to form the K_{seed}:

K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'

5. Calculate the basic access keys (K_{Enc} and K_{MAC}) according to Section 9.7.1/Appendix D.1:

K_{Enc} = 'AB94FDECF2674FDFB9B391F85D7F76F2'

K_{MAC} = '7962D9ECE03D1ACD4C76089DCE131543'

D.3 AUTHENTICATION AND ESTABLISHMENT OF SESSION KEYS

This section provides an example for performing Basic Access Control.

Inspection system:

1. Request an 8 byte random number from the eMRTD's contactless IC:

Command APDU:				
CLA	**INS**	**P1**	**P2**	**Le**
00	84	00	00	08

Response APDU:	
Response data field	**SW1-SW2**
RND.IC	9000

RND.IC = '4608F91988702212'

2. Generate an 8 byte random and a 16 byte random:
   RND.IFD = '781723860C06C226'
   K_{IFD} = '0B795240CB7049B01C19B33E32804F0B'

3. Concatenate RND.IFD, RND.IC and K_{IFD}:
   S = '781723860C06C2264608F91988702212
   0B795240CB7049B01C19B33E32804F0B'

4. Encrypt S with 3DES key K_{Enc}:
   E_{IFD} = '72C29C2371CC9BDB65B779B8E8D37B29
   ECC154AA56A8799FAE2F498F76ED92F2'

5. Compute MAC over E_{IFD} with 3DES key K_{MAC}:
   M_{IFD} = '5F1448EEA8AD90A7'

6. Construct command data for EXTERNAL AUTHENTICATE and send command APDU to the eMRTD's contactless IC:
   cmd_data = '72C29C2371CC9BDB65B779B8E8D37B29ECC154AA
   56A8799FAE2F498F76ED92F25F1448EEA8AD90A7'

Command APDU:						
CLA	**INS**	**P1**	**P2**	**Lc**	**Command data field**	**Le**
00	82	00	00	28	cmd_data	28

eMRTD's contactless IC:

1. Decrypt and verify received data and compare RND.IC with response on GET CHALLENGE.

2. Generate a 16 byte random:
   K_{IC} = '0B4F80323EB3191CB04970CB4052790B'

3. Calculate XOR of K_{IFD} and K_{IC}:
   K_{seed} = '0036D272F5C350ACAC50C3F572D23600'

4. Calculate session keys (KS_{Enc} and KS_{MAC}) according to Section 9.7.1/Appendix D.1:
   KS_{Enc} = '979EC13B1CBFE9DCD01AB0FED307EAE5'
   KS_{MAC} = 'F1CB1F1FB5ADF208806B89DC579DC1F8'

5. Calculate send sequence counter:
   SSC = '887022120C06C226'

6. Concatenate RND.IC, RND.IFD and K_{IC}:
   R = '4608F919887022126781723860C06C226
   0B4F80323EB3191CB04970CB4052790B'

7. Encrypt R with 3DES key K_{Enc}:
E_{IC} = '46B9342A41396CD7386BF5803104D7CE
DC122B9132139BAF2EEDC94EE178534F'

8. Compute MAC over E_{IC} with 3DES key K_{MAC}:
M_{IC} = '2F2D235D074D7449'

9. Construct response data for EXTERNAL AUTHENTICATE and send response APDU to the inspection system:
resp_data = '46B9342A41396CD7386BF5803104D7CEDC122B91
32139BAF2EEDC94EE178534F2F2D235D074D7449'

Response APDU:	
Response data field	**SW1-SW2**
resp_data	9000

Inspection system:

1. Decrypt and verify received data and compare received RND.IFD with generated RND.IFD.

2. Calculate XOR of K_{IFD} and K_{IC}:
K_{seed} = '0036D272F5C350ACAC50C3F572D23600'

3. Calculate session keys (KS_{Enc} and KS_{MAC}) according to Section 9.7.1/Appendix D.1:
KS_{Enc} = '979EC13B1CBFE9DCD01AB0FED307EAE5'
KS_{MAC} = 'F1CB1F1FB5ADF208806B89DC579DC1F8'

4. Calculate send sequence counter:
SSC = '887022120C06C226'

D.4 SECURE MESSAGING

After authentication and establishment of the session keys, the inspection system selects the EF.COM (File ID = '011E') and reads the data using secure messaging. The calculated KS_{Enc}, KS_{MAC} and SSC (previous steps 3 and 4 of the inspection system) will be used.

First the EF.COM will be selected, then the first four bytes of this file will be read so that the length of the structure in the file can be determined and after that the remaining bytes are read.

1. Select EF.COM

Unprotected command APDU:

CLA	INS	P1	P2	Lc	Command data field
00	A4	02	0C	02	01 1E

a) Mask class byte and pad command header:
CmdHeader = '0CA4020C80000000'

b) Pad data:
Data = '011E800000000000'

c) Encrypt data with KS_{Enc}:
EncryptedData = '6375432908C044F6'

d) Build DO'87':
DO87 = '8709016375432908C044F6'

e) Concatenate CmdHeader and DO'87':
M = '0CA4020C800000008709016375432908C044F6'

f) Compute MAC of M:
i) Increment SSC with 1:
SSC = '887022120C06C227'

ii) Concatenate SSC and M and add padding:
N = ‘887022120C06C2270CA4020C80000000
8709016375432908C044F68000000000’

iii) Compute MAC over N with KS_{MAC}:
CC = ‘BF8B92D635FF24F8’

g) Build DO‘8E’:
DO8E = ‘8E08BF8B92D635FF24F8’

h) Construct and send protected APDU:
ProtectedAPDU = ‘0CA4020C158709016375432908C0
44F68E08BF8B92D635FF24F800’

i) Receive response APDU of eMRTD’s contactless IC:
RAPDU = ‘990290008E08FA855A5D4C50A8ED9000’

j) Verify RAPDU CC by computing MAC of DO‘99’:

i) Increment SSC with 1:
SSC = ‘887022120C06C228’

ii) Concatenate SSC and DO‘99’ and add padding:
K = ‘887022120C06C2289902900080000000’

iii) Compute MAC with KS_{MAC}:
CC’ = ‘FA855A5D4C50A8ED’

iv) Compare CC’ with data of DO‘8E’ of RAPDU.
‘FA855A5D4C50A8ED’ == ‘FA855A5D4C50A8ED’ ? YES.

2. Read Binary of first four bytes:

Unprotected command APDU:

CLA	INS	P1	P2	Le
00	B0	00	00	04

a) Mask class byte and pad command header:
CmdHeader = ‘0CB0000080000000’

b) Build DO‘97’:
DO97 = ‘970104’

c) Concatenate CmdHeader and DO‘97’:
M = ‘0CB0000080000000970104’

d) Compute MAC of M:

i) Increment SSC with 1:
SSC = ‘887022120C06C229’

ii) Concatenate SSC and M and add padding:
N = ‘887022120C06C2290CB00000
8000000097010480000000000’

iii) Compute MAC over N with KSMAC:
CC = ‘ED6705417E96BA55’

e) Build DO‘8E’:
DO8E = ‘8E08ED6705417E96BA55’

f) Construct and send protected APDU:
ProtectedAPDU = ‘0CB000000D9701048E08ED6705417E96BA5500’

g) Receive response APDU of eMRTD's contactless IC:
RAPDU = '8709019FF0EC34F992265199029000
8E08AD55CC17140B2DED9000'

h) Verify RAPDU CC by computing MAC of concatenation DO'87' and DO'99':

i) Increment SSC with 1:
SSC = '887022120C06C22A'

ii) Concatenate SSC, DO'87' and DO'99' and add padding:
K = '887022120C06C22A8709019F
F0EC34F99226519902900080'

iii) Compute MAC with KS_{MAC}:
CC' = 'AD55CC17140B2DED'

iv) Compare CC' with data of DO'8E' of RAPDU:
'AD55CC17140B2DED' == 'AD55CC17140B2DED' ? YES.

i) Decrypt data of DO'87' with KS_{Enc}:
DecryptedData = '60145F01'

j) Determine length of structure:
L = '14' + 2 = 22 bytes

3. Read Binary of remaining 18 bytes from offset 4:

Unprotected command APDU:

CLA	INS	P1	P2	Le
00	B0	00	04	12

a) Mask class byte and pad command header:
CmdHeader = '0CB0000480000000'

b) Build DO'97':
DO97 = '970112'

c) Concatenate CmdHeader and DO'97':
M = '0CB000048000000970112'

d) Compute MAC of M:

i) Increment SSC with 1:
SSC = '887022120C06C22B'

ii) Concatenate SSC and M and add padding:
N = '887022120C06C22B0CB00004
8000000097011280000000000'

iii) Compute MAC over N with KS_{MAC}:
CC = '2EA28A70F3C7B535'

e) Build DO'8E':
DO8E = '8E082EA28A70F3C7B535'

f) Construct and send protected APDU:
ProtectedAPDU = '0CB000040D9701128E082EA28A70F3C7B53500'

g) Receive response APDU of eMRTD's contactless IC:
RAPDU = '871901FB9235F4E4037F2327DCC8964F1F9B8C30F42
C8E2FFF224A990290008E08C8B2787EAEA07D749000'

h) Verify RAPDU CC by computing MAC of concatenation DO‘87’ and DO‘99’:

i) Increment SSC with 1:
SSC = ‘887022120C06C22C’

ii) Concatenate SSC, DO‘87’ and DO‘99’ and add padding:
K = ‘887022120C06C22C871901FB9235F4E4037F232
7DCC8964F1F9B8C30F42C8E2FFF224A99029000’

iii) Compute MAC with KS_{MAC}:
CC’ = ‘C8B2787EAEA07D74’

iv) Compare CC’ with data of DO‘8E’ of RAPDU:
‘C8B2787EAEA07D74’ == ‘C8B2787EAEA07D74’ ? YES.

i) Decrypt data of DO‘87’ with KS_{Enc}:
DecryptedData = ‘04303130365F36063034303030305C026175’

RESULT:

EF.COM data = ‘60145F0104303130365F36063034303030305C026175’

– – – – – – – – – – –

المرفق (هـ) بالجزء ١١

مثال محلول: التحقق السلبي من الصحة (إعلامي)

الخطوة ١: اقرأ المادة الأمنية للوثيقة (SO_D) (التي تحتوي اختيارياً على شهادة الجهة الموقّعة على الوثيقة (C_{DS})) من الدائرة المتكاملة اللاتلامسية.

الخطوة ٢: اقرأ الجهة الموقّعة على الوثيقة (DS) من المادة الأمنية للوثيقة (SO_D).

الخطوة ٣: يتحقق نظام التفتيش من (SO_D) باستخدام المفتاح العام للجهة الموقّعة على الوثيقة.

الخطوة ٤: يتحقق نظام التفتيش من الجهة الموقّعة على الوثيقة C_{DS} باستخدام المفتاح العام للسلطة الوطنية المعنية بالتوقيع على الشهادات.

إذا كان التحققان في الخطوتين ٣ و٤ كلاهما صحيحين، يضمن هذا من ثم أنه يمكن الثقة في محتويات المادة الأمنية للوثيقة ويمكن استخدامها في عمليات التفتيش.

الخطوة ٥: اقرأ مجموعات البيانات ذات الصلة من بنية البيانات المنطقية.

الخطوة ٦: احسب البصمات الرقمية لمجموعات البيانات ذات الصلة.

الخطوة ٧: قارن البصمات الرقمية المحسوبة بقيم البصمات الرقمية المناظرة في المادة الأمنية للوثيقة.

إذا كانت قيم البصمات الرقمية في الخطوة ٧ متطابقة، يضمن هذا أن محتويات مجموعة البيانات ولم تتغيّر.

– – – – – – – – – – –

المرفق (و) بالجزء ١١

مثال محلول: التحقق الإيجابي من الصحة (إعلامي)

This worked example uses the following settings:

1.	Integer factorization-based mechanism:	RSA
2.	Modulus length (k):	1 024 bits (128 bytes)
3.	Hash algorithm:	SHA-1

Inspection system:

Step 1. Generate an 8 byte random:
RND.IFD = 'F173589974BF40C6'

Step 2. Construct command for internal authenticate and send command APDU to the eMRTD's contactless IC:

Command APDU

CLA	INS	P1	P2	Lc	Command data field	Le
00	88	00	00	08	RND.IFD	00

eMRTD's contactless IC:

Step 3. Determine M_2 from incoming APDU:
M_2 = 'F173589974BF40C6'

Step 4. Create the trailer:
T = 'BC' (i.e. SHA-1)
t (length of T in octets) = 1

Step 5. Determine lengths:
a. $c = k - L_h - 8t - 4 = 1024 - 160 - 8 - 4 = 852$ bits
b. $L_{M1} = c - 4 = 848$ bits

Step 6. Generate nonce M_1 of length L_{M1}:
M_1 = '9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8'

Step 7. Create M:
$M = M_1 \mid M_2$ = '9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF

40C6′

Step 8. Calculate SHA-1 digest of M:
H = SHA-1(M) = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127′

Step 9.[1] Construct the message representative:
F = ‘6A′ | M_1 | H | T =
‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
4E7292E2DCDA3024B47DA8C063AA1E6D
22FBD976AB0FE73D94D2D9C6D88127BC′

Step 10. Encrypt F with the Active Authentication Private Key to form the signature:
S = ‘756B683B036A6368F4A2EB29EA700F96
E26100AFC0809F60A91733BA29CAB362
8CB1A017190A85DADE83F0B977BB513F
C9C672E5C93EFEBBE250FE1B722C7CEE
F35D26FC8F19219C92D362758FA8CB0F
F68CEF320A8753913ED25F69F7CEE772
6923B2C43437800BBC9BC028C49806CF
2E47D16AE2B2CC1678F2A4456EF98FC9′

Step 11. Construct response data for INTERNAL AUTHENTICATE and send response APDU to the inspection system:

Response APDU:

Response data field	SW1-SW2
S	9000

Inspection system:

Step 12. Decrypt the signature with the public key:
F = ‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
4E7292E2DCDA3024B47DA8C063AA1E6D
22FBD976AB0FE73D94D2D9C6D88127BC′

Step 13. Determine hash algorithm by trailer T*:
T = ‘BC′ (i.e. SHA-1)

Step 14. Extract digest:
D = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127′

Step 15. Extract M_1:
M_1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98

[1] Since the known part (RND.IFD) is not returned, but must be appended by the IFD itself, Partial Recovery applies (‘6A’).

599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8'

Step 16. Header indicates partial recovery but signature has modulus length so concatenate M_1 with known M_2 (i.e. RND.IFD):

M* = '9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6'

Step 17. Calculate SHA-1 digest of M*:

D* = 'C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127'

Step 18. Compare D and D*:

D is equal to D* so verification successful.

– – – – – – – – – – –

المرفق (ز) بالجزء ١١

مثال محلول: فتح الاتصال بكلمة سر مصدّق عليها – تحديد المجالات العام (إعلامي)

WORKED EXAMPLE: PACE – GENERIC MAPPING (INFORMATIVE)

This Appendix provides two worked examples for the PACE protocol as defined in Section 4.4 using the generic mapping. The first example is based on ECDH while the second one uses DH. All numbers contained in the tables are noted hexadecimal.

In both examples, the MRZ is used as password. This also leads to the same symmetric key K_π. The relevant data fields of the MRZ including the check digits are:

- Document Number: T220001293;
- Date of Birth: 6408125;
- Date of Expiry: 1010318.

Hence, the encoding K of the MRZ and the derived encryption key K_π are

K	7E2D2A41 C74EA0B3 8CD36F86 3939BFA8 E9032AAD
K_π	89DED1B2 6624EC1E 634C1989 302849DD

ز–١ مثال قائم على بروتوكول ديفي هلمان للمنحنى الإهليلجي (ECDH)

This example is based on ECDH applying the standardized BrainpoolP256r1 domain parameters (see [RFC 5639]).

The first section introduces the corresponding `PACEInfo`. Subsequently, the exchanged APDUs including all generated nonces and ephemeral keys are listed and examined.

Elliptic Curve Parameters

Using standardized domain parameters, all information required to perform PACE is given by the data structure `PACEInfo`. In particular, no `PACEDomainParameterInfo` is needed.

PACEInfo	3012060A 04007F00 07020204 02020201 0202010D

The detailed structure of `PACEInfo` is itemized in the following table.

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
30	12		SEQUENCE	PACEInfo
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
02	01	02	INTEGER	Version 2
02	01	0D	INTEGER	Brainpool P256r1 Standardized Domain Parameters

For convenience, an ASN.1 encoding of the BrainpoolP256r1domain parameters is given below.

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
30	81 EC		SEQUENCE	Domain parameter
06	07	2A 86 48 CE 3D 02 01	OBJECT IDENTIFIER	Algorithm id-ecPublicKey
30	81 E0		SEQUENCE	Domain Parameter
02	01	01	INTEGER	Version
30	2C		SEQUENCE	Underlying field
06	07	2A 86 48 CE 3D 01 01	OBJECT IDENTIFIER	Prime field
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 72 6E 3B F6 23 D5 26 20 28 20 13 48 1D 1F 6E 53 77	INTEGER	Prime p
30	44		SEQUENCE	Curve equation
04	20	7D 5A 09 75 FC 2C 30 57 EE F6 75 30 41 7A FF E7 FB 80 55 C1 26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9	OCTET STRING	Parameter a
04	20	26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9 BB D7 7C BF 95 84 16 29 5C F7 E1 CE 6B CC DC 18 FF 8C 07 B6	OCTET STRING	Parameter b

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
04	41		OCTET STRING	Group generator G
		04	-	Uncompressed point
		8B D2 AE B9 CB 7E 57 CB 2C 4B 48 2F FC 81 B7 AF B9 DE 27 E1 E3 BD 23 C2 3A 44 53 BD 9A CE 32 62	-	x-coordinate
		54 7E F8 35 C3 DA C4 FD 97 F8 46 1A 14 61 1D C9 C2 77 45 13 2D ED 8E 54 5C 1D 54 C7 2F 04 69 97	-	y-coordinate
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 71 8C 39 7A A3 B5 61 A6 F7 90 1E 0E 82 97 48 56 A7	INTEGER	Group order n
02	01	01	INTEGER	Cofactor f

Application flow of the ECDH-based example

To initialize PACE, the terminal sends the command MSE:Set AT to the chip.

T>C:	`00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 02 02 83 01 01`
C>T:	`90 00`

Here, T>C is an abbreviation for an APDU sent from terminal to chip while C>T denotes the corresponding response sent by the chip to the terminal. The encoding of the command is explained in the next table.

Command				
CLA	00		Plain	
INS	22		Manage security environment	
P1/P2	C1 A4		Set Authentication Template for mutual authentication	
Lc	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 02 02	Cryptographic mechanism: PACE with ECDH, generic mapping and AES128 session keys
	83	01	01	Password: MRZ
Response				
Status Bytes	90 00		Normal processing	

Encrypted Nonce

Next, the chip randomly generates the nonce s and encrypts it by means of K_π.

Decrypted Nonce s	3F00C4D3 9D153F2B 2A214A07 8D899B22
Encrypted Nonce z	95A3A016 522EE98D 01E76CB6 B98B42C3

The encrypted nonce is queried by the terminal.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 95 A3 A0 16 52 2E E9 8D 01 E7 6C B6 B9 8B 42 C3 90 00

The encoding of the command APDU and the corresponding response can be found in the following table.

Command				
CLA	10		Command chaining	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data
	80	10	95 A3 A0 16 52 2E E9 8D 01 E7 6C B6 B9 8B 42 C3	Encrypted Nonce
Status Bytes	90 00		Normal processing	

Map Nonce

The nonce is mapped to an ephemeral group generator via generic mapping. The required randomly chosen ephemeral keys are also collected in the next table.

Terminal's Private Key	7F4EF07B 9EA82FD7 8AD689B3 8D0BC78C F21F249D 953BC46F 4C6E1925 9C010F99
Terminal's Public Key	7ACF3EFC 982EC455 65A4B155 129EFBC7 4650DCBF A6362D89 6FC70262 E0C2CC5E, 544552DC B6725218 799115B5 5C9BAA6D 9F6BC3A9 618E70C2 5AF71777 A9C4922D
Chip's Private Key	498FF497 56F2DC15 87840041 839A8598 2BE7761D 14715FB0 91EFA7BC E9058560
Chip's Public Key	824FBA91 C9CBE26B EF53A0EB E7342A3B F178CEA9 F45DE0B7 0AA60165 1FBA3F57, 30D8C879 AAA9C9F7 3991E61B 58F4D52E

	B87A0A0C 709A49DC 63719363 CCD13C54
Shared secret H	60332EF2 450B5D24 7EF6D386 8397D398 852ED6E8 CAF6FFEE F6BF85CA 57057FD5, 0840CA74 15BAF3E4 3BD414D3 5AA4608B 93A2CAF3 A4E3EA4E 82C9C13D 03EB7181
Mapped generator $\tilde{G}$	8CED63C9 1426D4F0 EB1435E7 CB1D74A4 6723A0AF 21C89634 F65A9AE8 7A9265E2, 8C879506 743F8611 AC33645C 5B985C80 B5F09A0B 83407C1B 6A4D857A E76FE522

The following APDUs are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 45 7C 43 81 41 04 7A CF 3E FC 98 2E C4 55 65 A4 B1 55 12 9E FB C7 46 50 DC BF A6 36 2D 89 6F C7 02 62 E0 C2 CC 5E 54 45 52 DC B6 72 52 18 79 91 15 B5 5C 9B AA 6D 9F 6B C3 A9 61 8E 70 C2 5A F7 17 77 A9 C4 92 2D 00
C>T :	7C 43 82 41 04 82 4F BA 91 C9 CB E2 6B EF 53 A0 EB E7 34 2A 3B F1 78 CE A9 F4 5D E0 B7 0A A6 01 65 1F BA 3F 57 30 D8 C8 79 AA A9 C9 F7 39 91 E6 1B 58 F4 D5 2E B8 7A 0A 0C 70 9A 49 DC 63 71 93 63 CC D1 3C 54 90 00

The structure of the APDUs can be described as follows:

Command				
CLA	10		Command chaining	
INS	86		GENARAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	45		Length of data	
Data	Tag	Length	Value	Comment
	7C	43	-	Dynamic Authentication Data
	81	41		Mapping Data
			04	Uncompressed Point
			7A CF 3E FC 98 2E ... C2 CC 5E	x-coordinate
			54 45 52 DC B6 72 ... C4 92 2D	y-coordinate
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	43		Dynamic Authentication Data
	82	41		Mapping Data

			04		Uncompressed Point
			82 4F BA 91 C9 CB ... BA 3F 57		x-coordinate
			30 D8 C8 79 AA A9 ... D1 3C 54		y-coordinate
Status Bytes	90 00		Normal processing		

Perform Key Agreement

In the third step, chip and terminal perform an anonymous ECDH key agreement using the new domain parameters determined by the ephemeral group generator of the previous step. Only the x-coordinate is required as shared secret since the KDF uses only the first coordinate to derive the session keys.

Terminal's Private Key	A73FB703 AC1436A1 8E0CFA5A BB3F7BEC 7A070E7A 6788486B EE230C4A 22762595
Terminal's Public Key	2DB7A64C 0355044E C9DF1905 14C625CB A2CEA487 54887122 F3A5EF0D 5EDD301C, 3556F3B3 B186DF10 B857B58F 6A7EB80F 20BA5DC7 BE1D43D9 BF850149 FBB36462
Chip's Private Key	107CF586 96EF6155 053340FD 633392BA 81909DF7 B9706F22 6F32086C 7AFF974A
Chip's Public Key	9E880F84 2905B8B3 181F7AF7 CAA9F0EF B743847F 44A306D2 D28C1D9E C65DF6DB, 7764B222 77A2EDDC 3C265A9F 018F9CB8 52E111B7 68B32690 4B59A019 3776F094
Shared Secret	28768D20 701247DA E81804C9 E780EDE5 82A9996D B4A31502 0B273319 7DB84925

The key agreement is performed as follows:

T>C :	10 86 00 00 45 7C 43 83 41 04 2D B7 A6 4C 03 55 04 4E C9 DF 19 05 14 C6 25 CB A2 CE A4 87 54 88 71 22 F3 A5 EF 0D 5E DD 30 1C 35 56 F3 B3 B1 86 DF 10 B8 57 B5 8F 6A 7E B8 0F 20 BA 5D C7 BE 1D 43 D9 BF 85 01 49 FB B3 64 62 00
C>T :	7C 43 84 41 04 9E 88 0F 84 29 05 B8 B3 18 1F 7A F7 CA A9 F0 EF B7 43 84 7F 44 A3 06 D2 D2 8C 1D 9E C6 5D F6 DB 77 64 B2 22 77 A2 ED DC 3C 26 5A 9F 01 8F 9C B8 52 E1 11 B7 68 B3 26 90 4B 59 A0 19 37 76 F0 94 90 00

The encoding of the key agreement is examined in the following table:

Command		
CLA	10	Command chaining
INS	86	GENARAL AUTHENTICATE
P1/P2	00 00	Keys and protocol implicitly known

Lc	45		Length of data		
Data	Tag	Length	Value	Comment	
	7C	43	-	Dynamic Authentication Data	
	83	41		Terminal's Ephemeral Public Key	
			04		Uncompressed Point
			2D B7 A6 4C 03 55 ... DD 30 1C		x-coordinate
			35 56 F3 B3 B1 86 ... B3 64 62		y-coordinate
Le	00		Expected maximal byte length of the response data field is 256		
Response					
Data	Tag	Length	Value	Comment	
	7C	43		Dynamic Authentication Data	
	84	41		Chip's Ephemeral Public Key	
			04		Uncompressed Point
			9E 88 0F 84 29 05 ... 5D F6 DB		x-coordinate
			77 64 B2 22 77 A2 ... 76 F0 94		y-coordinate
Status Bytes	90 00		Normal processing		

By means of the KDF, the AES 128 session keys KS_{Enc} and KS_{MAC} are derived from the shared secret. These are

KS_{Enc}	F5F0E35C 0D7161EE 6724EE51 3A0D9A7F
KS_{MAC}	FE251C78 58B356B2 4514B3BD 5F4297D1

Mutual Authentication

The authentication tokens are derived by means of KS_{MAC} using

Input Data for T_{IFD}	7F494F06 0A04007F 00070202 04020286 41049E88 0F842905 B8B3181F 7AF7CAA9 F0EFB743 847F44A3 06D2D28C 1D9EC65D F6DB7764 B22277A2 EDDC3C26 5A9F018F 9CB852E1 11B768B3 26904B59 A0193776 F094
Input Data for T_{IC}	7F494F06 0A04007F 00070202 04020286 41042DB7 A64C0355 044EC9DF 190514C6 25CBA2CE A4875488 7122F3A5 EF0D5EDD 301C3556 F3B3B186 DF10B857 B58F6A7E B80F20BA 5DC7BE1D 43D9BF85 0149FBB3 6462

as input. The encoding of the input data is shown below

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
7F49	4F		PUBLIC KEY	Input data for T_{IFD}
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Chip's Ephemeral Public Point
		04		Uncompressed Point
		9E 88 0F 84 29 ... 5D F6 DB		x-coordinate
		77 64 B2 22 77 ... 76 F0 94		y-coordinate

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
7F49	4F		PUBLIC KEY	Input data for T_{IC}
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Terminal's Ephemeral Public Point
		04		Uncompressed Point
		2D B7 A6 4C 03 ... DD 30 1C		x-coordinate
		35 56 F3 B3 B1 ... B3 64 62		y-coordinate

The computed authentication tokens are:

T_{IFD}	C2B0BD78 D94BA866
T_{IC}	3ABB9674 BCE93C08

Finally, these tokens are exchanged and verified.

T>C :	00 86 00 00 0C 7C 0A 85 08 C2 B0 BD 78 D9 4B A8 66 00
C>T :	7C 0A 86 08 3A BB 96 74 BC E9 3C 08 90 00

ز–٢ مثال قائم على بروتوكول ديفي هلمان (DH)

The second example is based on DH using the 1024-bit MODP Group with 160-bit Prime Order Subgroup specified by [RFC 5114]. The parameters of the group are:

Prime *p*	B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123 24975C3C D49B83BF

	ACCBDD7D 90C4BD70 98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371
Subgroup Generator *g*	A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213 160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5
Prime Order *q* of *g*	F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

The first section introduces the PACEInfo. Subsequently, the exchanged APDUs including all generated nonces and ephemeral keys are listed and examined.

Diffie Hellman Parameters

The relevant information for PACE is given by the data structure PACEInfo.

PACEInfo	3012060A 04007F00 07020204 01020201 02020100

The detailed structure of PACEInfo is:

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***	
30	12		SEQUENCE	PACEInfo	
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER		OID: PACE with DH, generic mapping and AES 128 session keys
02	01	02	INTEGER		Version 2
02	01	00	INTEGER		Standardized 1024-bit Group specified by RFC 5114

Application flow of the DH-based example

To initialize PACE, the terminal sends the command MSE:AT to the chip.

T>C :	00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 01 02 83 01 01
C>T :	90 00

The encoding of the command is described in the next table.

Command		
CLA	00	Plain
INS	22	Manage security environment
P1/P2	C1 A4	Set Authentication Template for mutual authentication

Lc	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 01 02	OID: Cryptographic mechanism: PACE with DH, generic mapping and AES128
	83	01	01	Password: MRZ
Response				
Status Bytes	90 00		Normal processing	

Encrypted Nonce

Next, the terminal queries a nonce from the chip.

Decrypted Nonce s	FA5B7E3E 49753A0D B9178B7B 9BD898C8
Encrypted Nonce z	854D8DF5 827FA685 2D1A4FA7 01CDDDCA

The communication looks as follows.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 85 4D 8D F5 82 7F A6 85 2D 1A 4F A7 01 CD DD CA 90 00

The encoding of the command APDU and the corresponding response is described in the following table.

Command				
CLA	10		Command chaining	
INS	86		GENARAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data
	80	10	85 4D 8D F5 82 7F A6 85 2D 1A 4F A7 01 CD DD CA	Encrypted Nonce
Status Bytes	90 00		Normal processing	

Map Nonce

By means of the generic mapping, the nonce is mapped to an ephemeral group generator. For that purpose, the following ephemeral keys are randomly generated by terminal and chip.

Terminal's Private Key	5265030F 751F4AD1 8B08AC56 5FC7AC95 2E41618D
Terminal's Public Key	23FB3749 EA030D2A 25B278D2 A562047A DE3F01B7 4F17A154 02CB7352 CA7D2B3E B71C343D B13D1DEB CE9A3666 DBCFC920 B49174A6 02CB4796 5CAA73DC 702489A4 4D41DB91 4DE9613D C5E98C94 160551C0 DF86274B 9359BC04 90D01B03 AD54022D CB4F57FA D6322497 D7A1E28D 46710F46 1AFE710F BBBC5F8B A166F431 1975EC6C
Chip's Private Key	78879F57 225AA808 0D52ED0F C890A4B2 5336F699 AA89A2D3 A189654A F70729E6 23EA5738 B26381E4 DA19E004 706FACE7 B235C2DB F2F38748 312F3C98 C2DD4882 A41947B3 24AA1259 AC22579D B93F7085 655AF308 89DBB845 D9E6783F E42C9F24 49400306 254C8AE8 EE9DD812 A804C0B6 6E8CAFC1 4F84D825 8950A91B 44126EE6
Chip's Public Key	5BABEBEF 5B74E5BA 94B5C063 FDA15F1F 1CDE9487 3EE0A5D3 A2FCAB49 F258D07F 544F13CB 66658C3A FEE9E727 389BE3F6 CBBBD321 28A8C21D D6EEA3CF 7091CDDF B08B8D00 7D40318D CCA4FFBF 51208790 FB4BD111 E5A968ED 6B6F08B2 6CA87C41 0B3CE0C3 10CE104E ABD16629 AA48620C 1279270C B0750C0D 37C57FFF E302AE7F
Shared secret H	7C9CBFE9 8F9FBDDA 8D143506 FA7D9306 F4CB17E3 C71707AF F5E1C1A1 23702496 84D64EE3 7AF44B8D BD9D45BF 6023919C BAA027AB 97ACC771 666C8E98 FF483301 BFA4872D EDE9034E DFACB708 14166B7F 36067682 9B826BEA 57291B5A D69FBC84 EF1E7790 32A30580 3F743417 93E86974 2D401325 B37EE856 5FFCDEE6 18342DC5
Mapped generator $\hat{G}$	7C9CBFE9 8F9FBDDA 8D143506 FA7D9306 F4CB17E3 C71707AF F5E1C1A1 23702496 84D64EE3 7AF44B8D BD9D45BF 6023919C BAA027AB 97ACC771 666C8E98 FF483301 BFA4872D EDE9034E DFACB708 14166B7F 36067682 9B826BEA 57291B5A D69FBC84 EF1E7790 32A30580 3F743417 93E86974 2D401325 B37EE856 5FFCDEE6 18342DC5

The following APDUs are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 86 7C 81 83 81 81 80 23 FB 37 49 EA 03 0D 2A 25 B2 78 D2 A5 62 04 7A DE 3F 01 B7 4F 17 A1 54 02 CB 73 52 CA 7D 2B 3E B7 1C 34 3D B1 3D 1D EB CE 9A 36 66 DB CF C9 20 B4 91 74 A6 02 CB 47 96 5C AA 73 DC 70 24 89 A4 4D 41 DB 91 4D E9 61 3D C5 E9 8C 94 16 05 51 C0 DF 86 27 4B 93 59 BC 04 90 D0 1B 03 AD 54 02 2D CB 4F 57 FA D6 32 24 97 D7 A1 E2 8D 46 71 0F 46 1A FE 71 0F BB BC 5F 8B A1 66 F4 31 19 75 EC 6C 00
C>T :	7C 81 83 82 81 80 78 87 9F 57 22 5A A8 08 0D 52 ED 0F C8 90 A4 B2 53 36 F6 99 AA 89 A2 D3 A1 89 65 4A F7 07 29 E6 23 EA 57 38 B2 63 81 E4 DA 1 9E0 04 70 6F AC E7 B2 35 C2 DB F2 F3 87 48 31 2F 3C 98 C2 DD 48 82 A4 19 47 B3 24 AA 12 59 AC 22 57 9D B9 3F 70 85 65 5A F3 08 89 DB B8 45 D9 E6 78 3F E4 2C 9F 24 49 40 03 06 25 4C 8A E8 EE 9D D8 12 A8 04 C0 B6 6E 8C AF C1 4F 84 D8 25 89 50 A9 1B 44 12 6E E6 90 00

The structure of the APDUs can be described as follows:

Command				
CLA	10		Command chaining	
INS	86		GENARAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	86		Length of data	
Data	Tag	Length	Value	Comment
	7C	81 83	-	Dynamic Authentication Data
	81	81 80	23 FB 37 49 EA 03 ... 75 EC 6C	Mapping Data
Le	00		Expected maximal byte length of the response data field is 256	

Response				
Data	Tag	Length	Value	Comment
	7C	81 83		Dynamic Authentication Data
	82	81 80	ED 0F C8 90 A4 B2 ... 12 6E E6	Mapping Data
Status Bytes	90 00		Normal processing	

Perform Key Agreement

Subsequently, chip and terminal perform an anonymous DH key agreement using the new domain parameters determined by the ephemeral group generator of the previous step.

Terminal's Private Key	89CCB99И 0У8B3И1A 11У1296B СФ68УС53 411CA2СФ
Terminal's Public Key	00907D89 E2D425A1 78AA81AF 4A7774EC 8E388C11 5CAE6703 1E85EECE 520BD911 551B9AE4 D04369F2 9A02626C 86FBC674 7CC7BC35 2645B616 1A2A42D4 4EDA80A0 8FA8D61B 76D3A154 AD8A5A51 786B0BC0 71470578 71A92221 2C5F67F4 31731722 36B7747D 1671E6D6 92A3C7D4 0A0C3C5C E397545D 015C175E B5130551 EDBC2EE5 D4
Chip's Private Key	020F018C 7284B047 FA7721A3 37EFB7AC B1440BB3 0C5252BD 41C97C30 C994BB78 E9F0C5B3 2744D840 17D21FFA 6878396A 6469CA28 3EF5C000 DAF7D261 A39AB886 0ED4610A B5343390 897AAB5A 7787E4FA EFA0649C 6A94FDF8 2D991E8E 3FC332F5 142729E7 040A3F7D 5A4D3CD7 5CBEE1F0 43C1CAD2 DD484FEB 4ED22B59 7D36688E
Chip's Public Key	A5B78012 6B7C980E 9FCEA1D4 539DA1D2 7C342DFA
Shared Secret	6BABC7B3 A72BCD7E A385E4C6 2DB2625B D8613B24 149E146A 629311C4 CA6698E3 8B834B6A 9E9CD718 4BA8834A FF5043D4 36950C4C 1E783236 7C10CB8C 314D40E5 990B0DF7 013E64B4 549E2270 923D06F0 8CFF6BD3 E977DDE6 ABE4C31D 55C0FA2E 465E553E 77BDF75E 3193D383 4FC26E8E B1EE2FA1 E4FC97C1 8C3F6CFF FE2607FD

The key agreement is performed as follows:

T>C :	10 86 00 00 86 7C 81 83 83 81 80 90 7D 89 E2 D4 25 A1 78 AA 81 AF 4A 77 74 EC 8E 38 8C 11 5C AE 67 03 1E 85 EE CE 52 0B D9 11 55 1B 9A E4 D0 43 69 F2 9A 02 62 6C 86 FB C6 74 7C C7 BC 35 26 45 B6 16 1A 2A 42 D4 4E DA 80 A0 8F A8 D6 1B 76 D3 A1 54 AD 8A 5A 51 78 6B 0B C0 71 47 05 78 71 A9 22 21 2C 5F 67 F4 31 73 17 22 36 B7 74 7D 16 71 E6 D6 92 A3 C7 D4 0A 0C 3C 5C E3 97 54 5D 01 5C 17 5E B5 13 05 51 ED BC 2E E5 D4 00
C>T :	7C 81 83 84 81 80 07 56 93 D9 AE 94 18 77 57 3E 63 4B 6E 64 4F 8E 60 AF 17 A0 07 6B 8B 12 3D 92 01 07 4D 36 15 2B D8 B3 A2 13 F5 38 20 C4 2A DC 79 AB 5D 0A EE C3 AE FB 91 39 4D A4 76 BD 97 B9 B1 4D 0A 65 C1 FC 71 A0 E0 19 CB 08 AF 55 E1 F7 29 00 5F BA 7E 3F A5 DC 41 89 92 38 A2 50 76 7A 6D 46 DB 97 40 64 38 6C D4 56 74 35 85 F8 E5 D9 0C C8 B4 00 4B 1F 6D 86 6C 79 CE 05 84 E4 96 87 FF 61 BC 29 AE A1 90 00

Command				
CLA	10		Command chaining	
INS	86		GENARAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	86		Length of data	
Data	Tag	Length	Value	Comment
	7C	81 83	-	Dynamic Authentication Data
	83	81 80	90 7D 89 E2 D4 25 ... 2E E5 D4	Terminal's Ephemeral Public Key
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	81 83		Dynamic Authentication Data
	84	81 80	07 56 93 D9 AE 94 ... 29 AE A1	Chip's Ephemeral Public Key
Status Bytes	90 00		Normal processing	

The AES 128 session keys KS_{Enc} and KS_{MAC} are derived from the shared secret using the KDF.

KS_{Enc}	2F7F46AD CC9E7E52 1B45D192 FAFA9126
KS_{MAC}	805A1D27 D45A5116 F73C5446 9462B7D8

Mutual Authentication

The authentication tokens are constructed from the following input data.

Input Data for T_{IFD}	7F49818F 060A0400 7F000702 02040102 84818007 5693D9AE 94187757 3E634B6E 644F8E60 AF17A007 6B8B123D 9201074D 36152BD8 B3A213F5 3820C42A DC79AB5D

	0AEEC3AE FB91394D A476BD97 B9B14D0A 65C1FC71 A0E019CB 08AF55E1 F729005F BA7E3FA5 DC418992 38A25076 7A6D46DB 97406438 6CD45674 3585F8E5 D90CC8B4 004B1F6D 866C79CE 0584E496 87FF61BC 29AEA1
Input Data for T_{IC}	7F49818F 060A0400 7F000702 02040102 84818090 7D89E2D4 25A178AA 81AF4A77 74EC8E38 8C115CAE 67031E85 EECE520B D911551B 9AE4D043 69F29A02 626C86FB C6747CC7 BC352645 B6161A2A 42D44EDA 80A08FA8 D61B76D3 A154AD8A 5A51786B 0BC07147 057871A9 22212C5F 67F43173 172236B7 747D1671 E6D692A3 C7D40A0C 3C5CE397 545D015C 175EB513 0551EDBC 2EE5D4

The encoding of the input data is shown below:

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***	
7F49	81 8F		PUBLIC KEY	Input data for T_{IFD}	
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER		PACE with DH, generic mapping and AES 128 session keys
84	81 80	07 56 93 D9 AE ... 29 AE A1	UNSIGNED INTEGER		Chip's Ephemeral Public Key

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***	
7F49	81 8F		PUBLIC KEY	Input data for T_{IC}	
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER		PACE with DH, generic mapping and AES 128 session keys
84	81 80	90 7D 89 E2 D4 ... 2E E5 D4	UNSIGNED INTEGER		Terminal's Ephemeral Public Key

The computed authentication tokens are:

T_{IFD}	B46DD9BD 4D98381F
T_{IC}	917F37B5 C0E6D8D1

Finally, these tokens are exchanged and verified.

T>C :	00 86 00 00 0C 7C 0A 85 08 B4 6D D9 BD 4D 98 38 1F 00
C>T :	7C 1B 86 08 91 7F 37 B5 C0 E6 D8 D1 87 0F 44 45 54 45 53 54 43 56 43 41 30 30 30 30 33

Command				
CLA	00		Plain	
INS	86		GENARAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	0C		Length of data	
Data	Tag	Length	Value	Comment
	7C	0A	-	Dynamic Authentication Data
	85	08	B4 6D D9 BD 4D 98 38 1F	Terminal's Authentication Token
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	0A		Dynamic Authentication Data
	86	08	91 7F 37 B5 C0 E6 D8 D1	Chip's Authentication Token
Status Bytes	90 00		Normal processing	

– – – – – – – – – – –

المرفق (ح) بالجزء ١١

مثال محلول: فتح الاتصال بكلمة سر مصدّق عليها – تحديد المجالات المتكامل (إعلامي)

WORKED EXAMPLE: PACE – INTEGRATED MAPPING (INFORMATIVE)

This Appendix provides two examples for the PACE protocol with Integrated Mapping. The first one is based on Elliptic Curve Diffie-Hellman (ECDH) and the second one on Diffie-Hellman (DH). The MRZ-derived key *K* from the previous Example is used.

H.1 ECDH BASED EXAMPLE

This example is based on the BrainpoolP256r1 elliptic curve. The block cipher used in this example is AES-128. For reminder, the curve parameters are the following:

Prime p	A9FB57DB A1EEA9BC 3E660A90 9D838D72 6E3BF623 D5262028 2013481D 1F6E5377
Parameter a	7D5A0975 FC2C3057 EEF67530 417AFFE7 FB8055C1 26DC5C6C E94A4B44 F330B5D9
Parameter b	26DC5C6C E94A4B44 F330B5D9 BBD77CBF 95841629 5CF7E1CE 6BCCDC18 FF8C07B6
x-coordinate of the group generator G	8BD2AEB9 CB7E57CB 2C4B482F FC81B7AF B9DE27E1 E3BD23C2 3A4453BD 9ACE3262
y-coordinate of the group generator G	547EF835 C3DAC4FD 97F8461A 14611DC9 C2774513 2DED8E54 5C1D54C7 2F046997
Group order n	A9FB57DB A1EEA9BC 3E660A90 9D838D71 8C397AA3 B561A6F7 901E0E82 974856A7
Cofactor f	01

The encryption key is the following:

K_π	591468CD A83D6521 9CCCB856 0233600F

Encrypted Nonce

A nonce s is randomly chosen by the chip and encrypted using K_π. The encrypted nonce z is then sent to the terminal.

Decrypted Nonce s	2923BE84 E16CD6AE 529049F1 F1BBE9EB
Encrypted Nonce z	143DC40C 08C8E891 FBED7DED B92B64AD

Map Nonce

A nonce t is randomly chosen and sent in clear. t and s are then used to compute the Integrated Mapping. First, the pseudo-random function R_p, derived from AES, is applied to s and t. Then, the point encoding f_G is used on the result to compute the Mapped Generator $\hat{G}=f_G(R_p(s,t))$.

Nonce t	5DD4CBFC 96F5453B 130D890A 1CDBAE32
Pseudo-random R(s,t)	E4447E2D FB3586BA C05DDB00 156B57FB B2179A39 49294C97 25418980 0C517BAA 8DA0FF39 7ED8C445 D3E421E4 FEB57322
$R_p(s,t)$	A2F8FF2D F50E52C6 599F386A DCB595D2 29F6A167 ADE2BE5F 2C3296AD D5B7430E
x-coordinate of the Mapped Generator $\hat{G}$	8E82D315 59ED0FDE 92A4D049 8ADD3C23 BABA94FB 77691E31 E90AEA77 FB17D427
y-coordinate of the Mapped Generator $\hat{G}$	4C1AE14B D0C3DBAC 0C871B7F 36081693 64437CA3 0AC243A0 89D3F266 C1E60FAD

Perform Key Agreement

The chip and the terminal perform an anonymous Diffie-Hellman key agreement using their secret keys and the mapped generator $\hat{G}$. The shared secret K is the x-coordinate of agreement.

Chip's private key SK_{IC}	107CF586 96EF6155 053340FD 633392BA 81909DF7 B9706F22 6F32086C 7AFF974A
Chip's public key PK_{IC}	67F78E5F 7F768608 2B293E8D 087E0569 16D0F74B C01A5F89 57D0DE45 691E51E8 932B69A9 62B52A09 85AD2C0A 271EE6A1 3A8ADDDC D1A3A994 B9DED257 F4D22753
Terminal's private key SK_{IFD}	A73FB703 AC1436A1 8E0CFA5A BB3F7BEC 7A070E7A 6788486B EE230C4A 22762595
Terminal's public key PK_{IFD}	89CBA23F FE96AA18 D824627C 3E934E54 A9FD0B87 A95D1471 DC1C0ABF DCD640D4 6755DE9B 7B778280 B6BEBD57 439ADFEB 0E21FD4E D6DF4257 8C13418A 59B34C37
Shared secret K	4F150FDE 1D4F0E38 E95017B8 91BAE171 33A0DF45 B0D3E18B 60BA7BEA FDC2C713

Using the specifications from [1], the session keys K_{Enc} and K_{MAC} are derived from K using the hash function SHA-1: K_{Enc}=SHA-1(K||0x00000001) and K_{MAC}=SHA-1(K||0x00000002). Then, only the first 16 octets of the digest are used with the following result:

K_{Enc}	0D3FEB33 251A6370 893D62AE 8DAAF51B
K_{MAC}	B01E89E3 D9E8719E 586B50B4 A7506E0B

Mutual Authentication

The authentication tokens are computed using a CMAC on the following inputs with the key K_{MAC}.

Input data for T_{IC}	7F494F06 0A04007F 00070202 04040286 410489CB A23FFE96 AA18D824 627C3E93

	4E54A9FD 0B87A95D 1471DC1C 0ABFDCD6 40D46755 DE9B7B77 8280B6BE BD57439A DFEB0E21 FD4ED6DF 42578C13 418A59B3 4C37
Input data for T_{IFD}	7F494F06 0A04007F 00070202 04040286 410467F7 8E5F7F76 86082B29 3E8D087E 056916D0 F74BC01A 5F8957D0 DE45691E 51E8932B 69A962B5 2A0985AD 2C0A271E E6A13A8A DDDCD1A3 A994B9DE D257F4D2 2753

The corresponding authentication tokens are:

T_{IC}	75D4D96E 8D5B0308
T_{IFD}	450F02B8 6F6A0909

H.2 DH BASED EXAMPLE

This example is based on the 1 024-bit MODP Group with 160-bit Prime Order Subgroup. The block cipher used in this example is AES-128.

The group parameters are:

Prime p	B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70 98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371
Subgroup generator g	A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213 160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5
Prime order q of g	F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

The following encryption key is used:

K_π	591468CD A83D6521 9CCCB856 0233600F

Encrypted Nonce

A nonce s is randomly chosen by the chip and encrypted using K_π. The encrypted nonce z is then sent to the terminal.

Decrypted Nonce s	FA5B7E3E 49753A0D B9178B7B 9BD898C8
Encrypted Nonce z	9ABB8864 CA0FF155 1E620D1E F4E13510

Map Nonce

A nonce t is randomly chosen and sent in clear. t and s are then used to compute the Integrated Mapping. First, the pseudo-random function R_p, derived from AES, is applied to s and t. Then, the point encoding f_g is used on the result.

Nonce t	B3A6DB3C 870C3E99 245E0D1C 06B747DE
Pseudo-random R(s,t)	EAB98D13 E0905295 2AA72990 7C3C9461 84DEA0FE 74AD2B3A F506F0A8 3018459C 38099CD1 F7FF4EA0 A078DB1F AC136550 5E3DC855 00EF95E2 0B4EEF2E 88489233 BEE0546B 472F994B 618D1687 02406791 DEEF3CB4 810932EC 278F3533 FDB860EB 4835C36F A4F1BF3F A0B828A7 18C96BDE 88FBA38A 3E6C35AA A1095925 1EB5FC71 0FC18725 8995944C 0F926E24 9373F485
$R_p(s,t)$	A0C7C50C 002061A5 1CC87D25 4EF38068 607417B6 EE1B3647 3CFB800D 2D2E5FA2 B6980F01 105D24FA B22ACD1B FA5C8A4C 093ECDFA FE6D7125 D42A843E 33860383 5CF19AFA FF75EFE2 1DC5F6AA 1F9AE46C 25087E73 68166FB0 8C1E4627 AFED7D93 570417B7 90FF7F74 7E57F432 B04E1236 819E0DFE F5B6E77C A4999925 328182D2
Mapped Generator $\hat{g}= f_g(R_p(s,t))$	1D7D767F 11E333BC D6DBAEF4 0E799E7A 926B9697 3550656F F3C83072 6D118D61 C276CDCC 61D475CF 03A98E0C 0E79CAEB A5BE2557 8BD4551D 0B109032 36F0B0F9 76852FA7 8EEA14EA 0ACA87D1 E91F688F E0DFF897 BBE35A47 2621D343 564B262F 34223AE8 FC59B664 BFEDFA2B FE7516CA 5510A6BB B633D517 EC25D4E0 BBAA16C2

Perform Key Agreement

The chip and the terminal perform an anonymous Diffie-Hellman key agreement using their secret keys and the mapped generator $\hat{g}$.

Chip's private key SK_{IC}	020F018C 7284B047 FA7721A3 37EFB7AC B1440BB3 0C5252BD 41C97C30 C994BB78 E9F0C5B3 2744D840 17D21FFA 6878396A 6469CA28 3EF5C000 DAF7D261 A39AB886 0ED4610A B5343390 897AAB5A 7787E4FA EFA0649C 6A94FDF8 2D991E8E 3FC332F5 142729E7 040A3F7D 5A4D3CD7 5CBEE1F0 43C1CAD2 DD484FEB 4ED22B59 7D36688E
Chip's public key PK_{IC}	928D9A0F 9DBA450F 13FC859C 6F290D1D 36E42431 138A4378 500BEB4E 0401854C FF111F71 CB6DC1D0 335807A1 1388CC8E AA87B079 07AAD9FB A6B169AF 6D8C26AF 8DDDC39A DC3AD2E3 FF882B84 D23E9768 E95A80E4 746FB07A 9767679F E92133B4

	D379935C 771BD7FB ED6C7BB4 B1708B27 5EA75679 524CDC9C 6A91370C C662A2F3
Terminal's private key SK_{IFD}	4BD0E547 40F9A028 E6A515BF DAF96784 8C4F5F5F FF65AA09 15947FFD 1A0DF2FA 6981271B C905F355 1457B7E0 3AC3B806 6DE4AA40 6C1171FB 43DD939C 4BA16175 103BA3DE E16419AA 248118F9 0CC36A3D 6F4C3736 52E0C3CC E7F0F1D0 C5425B36 00F0F0D6 A67F004C 8BBA33F2 B4733C72 52445C1D FC4F1107 203F71D2 EFB28161
Terminal's public key PK_{IFD}	0F0CC629 45A80292 51FB7EF3 C094E12E C68E4EF0 7F27CB9D 9CD04C5C 4250FAE0 E4F8A951 557E929A EB48E5C6 DD47F2F5 CD7C351A 9BD2CD72 2C07EDE1 66770F08 FFCB3702 62CF308D D7B07F2E 0DA9CAAA 1492344C 85290691 9538C98A 4BA4187E 76CE9D87 832386D3 19CE2E04 3C3343AE AE6EDBA1 A9894DC5 094D22F7 FE1351D5
Shared secret K	419410D6 C0A17A4C 07C54872 CE1CBCEB 0A2705C1 A434C8A8 9A4CFE41 F1D78124 CA7EC52B DE7615E5 345E48AB 1ABB6E7D 1D59A57F 3174084D 3CA45703 97C1F622 28BDFDB2 DA191EA2 239E2C06 0DBE3BBC 23C2FCD0 AF12E0F9 E0B99FCF 91FF1959 011D5798 B2FCBC1F 14FCC24E 441F4C8F 9B08D977 E9498560 E63E7FFA B3134EA7

The session keys K_{Enc} and K_{MAC} are derived from K using the hash function SHA-1: K_{Enc}=SHA-1(K||0x00000001) and K_{MAC}=SHA-1(K||0x00000002). Then, only the first 16 octets of the digest are used with the following result:

K_{Enc}	01AFC10C F87BE36D 8179E873 70171F07
K_{MAC}	23F0FBD0 5FD6C7B8 B88F4C83 09669061

Mutual Authentication

The authentication tokens are computed using a CMAC on the following inputs with the key K_{MAC}.

Input data for T_{IC}	7F49818F 060A0400 7F000702 02040302 8481800F 0CC62945 A8029251 FB7EF3C0 94E12EC6 8E4EF07F 27CB9D9C D04C5C42 50FAE0E4 F8A95155 7E929AEB 48E5C6DD 47F2F5CD 7C351A9B D2CD722C 07EDE166 770F08FF CB370262 CF308DD7 B07F2E0D A9CAAA14 92344C85 29069195 38C98A4B A4187E76 CE9D8783 2386D319 CE2E043C 3343AEAE 6EDBA1A9 894DC509 4D22F7FE 1351D5
Input data for T_{IFD}	7F49818F 060A0400 7F000702 02040302 84818092 8D9A0F9D BA450F13 FC859C6F 290D1D36 E4243113 8A437850 0BEB4E04 01854CFF 111F71CB 6DC1D033 5807A113 88CC8EAA 87B07907 AAD9FBA6 B169AF6D 8C26AF8D DDC39ADC 3AD2E3FF 882B84D2

	3E9768E9 5A80E474 6FB07A97 67679FE9 2133B4D3 79935C77 1BD7FBED 6C7BB4B1 708B275E A7567952 4CDC9C6A 91370CC6 62A2F3

The corresponding authentication tokens are:

T_{IC}	C2F04230 187E1525
T_{IFD}	55D61977 CBF5307E

\- - - - - - - - - - - -

المرفق (ط) بالجزء ١١

مثال محلول: فتح الاتصال بكلمة سر مصدّق عليها – تحديد المجالات المتكامل (إعلامي)

يوفر هذا المرفق مثالاً لبروتوكول PACE مع رقاقة التحقق من الصحة. تحديد المجالات بالاستناد إلى منحنى بيضاوي الشكل (ECDH) ديفي–هلمان. ويلاحظ أن جميع الأرقام التي تحتوي عليها الجداول عشرية.

يستخدم MRZ ككلمة سر. وخانات البيانات ذات الصلة لـ MRZ بما في ذلك أرقام التحقق هي:

- رقم الوثيقة: C11T002JM4؛
- تاريخ الميلاد: 9608122؛
- تاريخ انتهاء الصلاحية: 2310314.

ومن ثم، فإن K المشفرة لـ MRZ ومفتاح التشفير K_π المستمد هي

K	894D03F1 48C6265E 89845B21 8856EA34 D00EF8E8
K_π	4E6F6FBF 7BE748B9 32C7B741 61BBA9DF

ط–١ مثال مستند إلى ECDH

يستند هذا المثال إلى ECDH مع تطبيق بارامترات نطاق BrainpoolP256r1 (انظر [RFC 5639]):

يقدم القسم الأول PACEInfo المناظرة. وبعد ذلك، APDUs المتبادلة بما في ذلك جميع المناسبات الحالية المولدة ومفاتيح زائلة ترد قائمة بها وتفحص.

بارامترات المنحنيات البيضاوية

باستخدام بارامترات نطاق موحدة، تعطي بنية البيانات PACEInfo جميع المعلومات المطلوبة لأداء PACE. وبصفة خاصة، لا حاجة إلى PACEDomainParameterInfo.

PACEInfo	3012060A 04007F00 07020204 06020201 0202010D

البنية التفصيلية لـ PACEInfo مفصلة في الجدول التالي.

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
30	12		SEQUENCE	PACEInfo
06	0A	04 00 7F 00 07 02 02 04 06 02	OBJECT IDENTIFIER	PACE with ECDH, Chip Authentication Mapping and AES 128 session keys
02	01	02	INTEGER	Version 2
02	01	0D	INTEGER	Brainpool P256r1 Standardized Domain Parameters

توخياً للملاءمة، يُعطى أدناه تشفير بـ ASN.1 لبارامترات نطاق the BrainpoolP256r1.

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
30	81 EC		SEQUENCE	Domain parameter
06	07	2A 86 48 CE 3D 02 01	OBJECT IDENTIFIER	Algorithm id-ecPublicKey
30	81 E0		SEQUENCE	Domain Parameter
02	01	01	INTEGER	Version
30	2C		SEQUENCE	Underlying field
06	07	2A 86 48 CE 3D 01 01	OBJECT IDENTIFIER	Prime field
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 72 6E 3B F6 23 D5 26 20 28 20 13 48 1D 1F 6E 53 77	INTEGER	Prime p
30	44		SEQUENCE	Curve equation
04	20	7D 5A 09 75 FC 2C 30 57 EE F6 75 30 41 7A FF E7 FB 80 55 C1 26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9	OCTET STRING	Parameter a
04	20	26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9 BB D7 7C BF 95 84 16 29 5C F7 E1 CE 6B CC DC 18 FF 8C 07 B6	OCTET STRING	Parameter b

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
04	41		OCTET STRING	Group generator G
		04	-	Uncompressed point
		8B D2 AE B9 CB 7E 57 CB 2C 4B 48 2F FC 81 B7 AF B9 DE 27 E1 E3 BD 23 C2 3A 44 53 BD 9A CE 32 62	-	x-coordinate
		54 7E F8 35 C3 DA C4 FD 97 F8 46 1A 14 61 1D C9 C2 77 45 13 2D ED 8E 54 5C 1D 54 C7 2F 04 69 97	-	y-coordinate
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 71 8C 39 7A A3 B5 61 A6 F7 90 1E 0E 82 97 48 56 A7	INTEGER	Group order n
02	01	01	INTEGER	Cofactor f

انسياب تطبيق المثال المستند إلى ECDH

للبدء في استخدام PACE، ترسل المحطة النهائية أمر MSE:AT إلى الرقاقة.

T>C :	00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 06 02 83 01 01
C>T :	90 00

هنا، T>C هو اختصار لـ APDU مُرسَل من المحطة النهائية إلى الرقاقة في حين يعني C>T الاستجابة المطابقة المرسلة بواسطة الرقاقة إلى المحطة النهائية. وتشفير الأمر مشروح في الجدول التالي.

Command				
CLA	00		Plain	
INS	22		Manage security environment	
P1/P2	C1 A4		Set Authentication Template for mutual authentication	
Lc	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 06 02	Cryptographic mechanism: PACE with ECDH, Chip Authentication Mapping and AES128 session keys
	83	01	01	Password: MRZ
Response				
Status Bytes	90 00		Normal processing	

رقم مشفَّر يُستخدم مرة واحدة

بعد ذلك، تقوم الرقاقة عشوائياً بتوليد الرقم الذي يُستخدم مرة واحدة وبتشفيره بواسطة K_π.

Decrypted Nonce s	658B860B C94DF6F0 44FCE6D5 C82CF8E5
Encrypted Nonce z	CB60E8E0 D85B76A9 BD304747 C2AD42E2

تتساءل المحطة النهائية بشأن الرقم المشفَّر الذي يُستخدم مرة واحدة

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 СИ 60 У8 У0 В8 5И 76 Ф9 ИВ 30 47 47 С2 ФВ 42 У2 90 00

يمكن العثور في الجدول التالي على تشفير الأمر APDU والاستجابة المقابلة.

Command				
CLA	10		Command chaining	
INS	86		GENARAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data
	80	10	CB60E8E0 D85B76A9 BD304747 C2AD42E2	Encrypted Nonce
Status Bytes	90 00		Normal processing	

رقم الخريطة الذي يُستخدم مرة واحدة

يتم رسم خريطة للرقم الذي يستخدم مرة واحدة حسب مولّدة للمجموعات سريعة الزوال عن طريق رسم الخرائط العام. أما المفاتيح سريعة الزوال المطلوبة المختارة عشوائياً فيتم أيضاً جمعها في الجدول التالي.

Terminal's Private Key	5D8BB87B D74D985A 4B7D4325 B9F7B976 FE835122 77340079 8914AA22 738135CC
Terminal's Public Key	7F1D410A DB7DDB3B 84BF1030 800981A9 105D7457 B4A3ADE0 02384F30 86C67EDE 1AB88910 4A27DB6D 842B0190 20FBF3CE ACB0DC62 7F7BDCAC 29969E19 D0E553C1
Chip's Private Key	9E56A6B5 9C95D06E CE5CD10F 983BB2F4 F1943528 E577F238 81D89D8C 3BBEE0AA
Chip's Public Key	A234236A A9B9621E 8EFB73B5 245C0E09 D2576E52 77183C12 08BDD552 80CAE8B3 04F36571 3A356E65 A451E165 ECC9AC0A C46E3771 342C8FE5 AEDD0926 85338E23
Shared secret H	2C1DCC17 73346492 C6636A36 EE4B965E 292E9AAE 7EE37736 EF58B9D0 A043F348 403A8CF3 3CA7DC0D 9DF61D08 89CE2442 4FF97C1A AD48A5CA 2A554B07 1EF7638D
Mapped generator Ĝ	89A0И5УФ ИАЗИУ293 С75903Ф3 98613192 5С9А5И51 5СФ95ФА4 85ВС7У88 6А03245В 44ИУАИ2В В3Ф0ВИВ7 1СИ5У618 971СА474 7А12И79У 548379Ф4 0У45963И ФФА3У829

الـ APDUs التالية يتم تبادلها عن طريق المحطة النهائية والرقاقة لرسم خرائط لرقم الخريطة الذي يُستخدم مرة واحدة.

T>C :	10 86 00 00 45 7C 43 81 41 04 7F 1D 41 0A DB 7D DB 3B 84 BF 10 30 80 09 81 A9 10 5D 74 57 B4 A3 AD E0 02 38 4F 30 86 C6 7E DE 1A B8 89 10 4A 27 DB 6D 84 2B 01 90 20 FB F3 CE AC B0 DC 62 7F 7B DC AC 29 96 9E 19 D0 E5 53 C1 00
C>T :	7C 43 82 41 04 Ф2 34 23 6Ф Ф9 И9 62 1У 8У АИ 73 И5 24 5С 0У 09 В2 57 6У 52 77 18 3С 12 08 ИВ В5 52 80 СФ У8 И3 04 А3 65 71 3Ф 35 6У 65 Ф4 51 У1 65 УС С9 ФС 0Ф С4 6У 37 71 34 2С 8А У5 ФУ ВВ 09 26 85 33 8У 23 90 00

بنية الـ APDUs يمكن وصفها كما يلي:

Command					
CLA	10		Command chaining		
INS	86		GENARAL AUTHENTICATE		
P1/P2	00 00		Keys and protocol implicitly known		
Lc	45		Length of data		
Data	Tag	Length	Value	Comment	
	7C	43	-	Dynamic Authentication Data	
	81	41		Mapping Data	
			04		Uncompressed Point
			7F 1D 41 0A ... 86 C6 7E DE		x-coordinate
			1A B8 89 10... D0 E5 53 C1		y-coordinate
Le	00		Expected maximal byte length of the response data field is 256		
Response					
Data	Tag	Length	Value	Comment	
	7C	43		Dynamic Authentication Data	
	82	41		Mapping Data	
			04		Uncompressed Point
			A2 34 23 6A ... 80 CA E8 B3		x-coordinate
			04 F3 65 71... 85 33 8E 23		y-coordinate
Status Bytes	90 00		Normal processing		

اتفاق مفتاح قم بالأداء

في الخطوة الثالثة، تؤدي الرقاقة وقم بالأداء النهائي اتفاقاً لمفتاح ECDH مجهول الاسم باستخدام بارامترات النطاق الجديد التي حددتها المجموعة سريعة الزوال المولّدة للخطوة السابقة. والمطلوب نظير × فقط كسرّ مشترك نظراً لأن الـ KDF (الاشتقاق الرئيسي) فقط يستخدم النظير الأول فقط للحصول على مفاتيح الدورة.

Terminal's Private Key	76ECFDAA 9841C323 A3F5FC5E 88B88DB3 EFF7E35E BF57A7E6 946CB630 006C2120
Terminal's Public Key	446C9340 84D9DAB8 63944F21 9520076C 29EE3F7A E6722B11 FF319EC1 C7728F95 5483400B FF60BF0C 59292700 09277DC2 A515E125 75010AD9 BA916CF1 BF86FEFC
Chip's Private Key	CD626EF3 C256E235 FE8912CA C28279E6 26008EDA 6B3A05C4 CF862A3B DAB79E78
Chip's Public Key	02AD566F 3C6EC7F9 324509AD 50A51FA5 2030782A 4968FCFE DF737DAE A9933331 11C3B9B4 C2287789 BD137E7F 8AA882E2 A3C633CC D6ECC2C6 3C57AD40 1A09C2E1
Shared Secret	67950559 B0C06И4B 4И86972B 14460837 461087A8 419АВИС3 6ФФА6СУФ ФС462832

يتم أداء الاتفاق الرئيسي كما يلي:

T>C :	10 86 00 00 45 7C 43 83 41 04 44 6C 93 40 84 D9 DA B8 63 94 4F 21 95 20 07 6C 29 EE 3F 7A E6 72 2B 11 FF 31 9E C1 C7 72 8F 95 54 83 40 0B FF 60 BF 0C 59 29 27 00 09 27 7D C2 A5 15 E1 25 75 01 0A D9 BA 91 6C F1 BF 86 FE FC 00
C>T :	7C 43 84 41 04 02 AD 56 6F 3C 6E C7 F9 32 45 09 AD 50 A5 1F A5 20 30 78 2A 49 68 FC FE DF 73 7D AE A9 93 33 31 11 C3 B9 B4 C2 28 77 89 BD 13 7E 7F 8A A8 82 E2 A3 C6 33 CC D6 EC C2 C6 3C 57 AD 40 1A 09 C2 E1 90 00

يتم فحص تشفير الاتفاق الرئيسي في الجدول التالي:

Command					
CLA	10		Command chaining		
INS	86		GENARAL AUTHENTICATE		
P1/P2	00 00		Keys and protocol implicitly known		
Lc	45		Length of data		
Data	Tag	Length	Value	Comment	
	7C	43	-	Dynamic Authentication Data	
	83	41		Terminal's Ephemeral Public Key	
			04		Uncompressed Point
			44 6C 93 40 ... C7 72 8F 95		x-coordinate
			54 83 40 0B ... BF 86 FE FC		y-coordinate
Le	00		Expected maximal byte length of the response data field is 256		

Response					
Data	Tag	Length	Value	Comment	
	7C	43		Dynamic Authentication Data	
	84	41		Chip's Ephemeral Public Key	
			04		Uncompressed Point
			02 AD 56 6F ... A9 93 33 31		x-coordinate
			11 C3 B9 B4 ... 1A 09 C2 E1		y-coordinate
Status Bytes	90 00		Normal processing		

عن طريق الـ KDF، يُستمد مفتاحا الدورة AES 128، وهما KS_{Enc} و KS_{MAC} من السر المشترك. وهذان هما

KS_{Enc}	0A9DA4DB 03BDDE39 FC5202BC 44B2E89E
KS_{MAC}	4B1C0649 1ED5140C A2B537D3 44C6C0B1

المصادقة المتبادلة

تُستمد رموز المصادقة عن طريق استخدام KS_{MAC} كمُدخل. ويُبيَّن أدناه تشفير البيانات المُدخلة.

Input Data for T_{IFD}	7F494F06 0A04007F 00070202 04060286 410402AD 566F3C6E C7F93245 09AD50A5 1FA52030 782A4968 FCFEDF73 7DAEA993 333111C3 B9B4C228 7789BD13 7E7F8AA8 82E2A3C6 33CCD6EC C2C63C57 AD401A09 C2E1
Input Data for T_{IC}	7A494A06 0Ф04007A 00070202 04060286 4104446C 934084B9 ВФИ86394 4A219520 076C29УУ 3A7ФУ672 2И11АА31 9УС1С772 8A955483 400ИАА60 ИА0С5929 27000927 7ВС2Ф515 У1257501 0ФВ9ИФ91 6СА1ИА86 АУАС

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
7F49	4F		PUBLIC KEY	Input data for T_{IFD}
06	0A	04 00 7F 00 07 02 02 04 06 02	OBJECT IDENTIFIER	PACE with ECDH, Chip Authentication Mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Chip's Ephemeral Public Point
		04		Uncompressed Point
		02 AD 56 6F... A9 93 33 31		x-coordinate
		11 C3 B9 B4 ... 1A 09 C2 E1		y-coordinate

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
7F49	4F		PUBLIC KEY	Input data for T_{IC}
06	0A	04 00 7F 00 07 02 02 04 06 02	OBJECT IDENTIFIER	PACE with ECDH, Chip Authentication Mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Terminal's Ephemeral Public Point
		04		Uncompressed Point
		44 6C 93 40 ... C7 72 8F 95		x-coordinate
		54 83 40 0B ... BF 86 FE FC		y-coordinate

رموز التحقق من الصحة المحسوبة بالحاسوب هي:

T_{IFD}	E86BD060 18A1CD3B
T_{IC}	8596CF05 5C67C1A3

أخيراً، هذه الرموز يتم تبادلها ويتم التحقق من صحتها

T>C :	00 86 00 00 0C 7C 0A 85 08 E8 6B D0 60 18 A1 CD 3B 00
C>T :	7C 3C 86 08 85 96 CF 05 5C 67 C1 A3 8A 30 1E EA 96 4B ФФ У3 72 ФС 99 0У 3У АВ У6 33 33 53 ИА С8 9Ф 67 04 В9 3В Ф8 79 8С А7 7А 5И 7Ф 54 ИВ 10 СИ Ф3 72 И4 2И У0 И9 И5 А2 8Ф Ф8 ВУ 2А 4А 92 90 00

يتم في الجدول التالي فحص ترميز التحقق المتبادل من الصحة

Command					
CLA	00		No command chaining (last command in chain)		
INS	86		GENARAL AUTHENTICATE		
P1/P2	00 00		Keys and protocol implicitly known		
Lc	0C		Length of data		
Data	Tag	Length	Value	Comment	
	7C	0A	-	Dynamic Authentication Data	
	85	08		Terminal's Authentication Token	
			E8 6B D0 60 18 A1 CD 3B		T_{IFD}
Le	00		Expected maximal byte length of the response data field is 256		
Response					
Data	Tag	Length	Value	Comment	
	7C	3C		Dynamic Authentication Data	
	86	08		Chip's Authentication Token	
			85 96 CF 05 5C 67 C1 A3		T_{IC}
	8A	30			x-coordinate
			1E EA 96 4D … DE 2F 4F 92		Encrypted Chip Authentication Data
Status Bytes	90 00		Normal processing		

التحقق من صحة الرقاقة

وضع التحقق من صحة الرقاقة على المعلومات عن المفتاح العام من EF.CardSecurity

ChipAuthenticationPublicKeyInfo	30620609 04007F00 07020201 02305230 0C060704 007F0007 01020201 0D034200 04187270 9494399E 7470A643 1BE25E83 EEE24FEA 568C2ED2 8DB48E05 DB3A610D C884D256 A40E35EF CB59BF67 53D3A489 D28C7A4D 973C2DA1 38A6E7A4 A08F68E1 6F02010D

يتم وضع البنية المفصلة للتحقق من صحة معلومات المفتاح العام عن طريق الرقاقة في بنود في الجدول التالي.

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*	
30	62		SEQUENCE	ChipAuthenticationPublicKeyInfo	
06	09	04 00 7F 00 07 02 02 01 02	OBJECT IDENTIFIER		id-PK-ECDH
30	52		SEQUENCE		SubjectPublicKeyInfo
30	0C		SEQUENCE		Brainpool P256r1 Standardized Domain Parameters
06	07	04 00 7F 00 07 01 02	OBJECT IDENTIFIER		standardizedDomainParameters
02	01	0D	INTEGER		Brainpool256r1
03	42	00 04 18 72 70 … 8F 68 E1 6F	BIT STRING		CA Public Key
02	01	0D	INTEGER		keyID 13

تُستخدم البيانات التالية للتحقق من صحة الرقاقة.

Encrypted Chip Authentication Data	1EEA964D AAE372AC 990E3EFD E6333353 BFC89A67 04D93DA8 798CF77F 5B7A54BD 10CBA372 B42BE0B9 B5F28AA8 DE2F4F92
Decrypted Chip Authentication Data	85DC3FA9 3D0952BF A82F5FD1 89EE75BD 82F11D1F 0B8ED4BF 5319AC9B 53C426B3
IV for De-/Encryption of CA Data IV = $E(KS_{ENC}, -1)$	F6A3B75A1 E933941 DD7A13E2 520779DF
Chip's Public Key from GENERAL AUTHENTICATE Mapping Nonce $PK_{MAP,IC}$	A234236A A9B9621E 8EFB73B5 245C0E09 D2576E52 77183C12 08BDD552 80CAE8B3 04F36571 3A356E65 A451E165 ECC9AC0A C46E3771 342C8FE5 AEDD0926 85338E23
Chip's Public CA Key from ChipAuthenticationPublicKeyInfo PK_{IC}	18727094 94399E74 70A6431B E25E83EE E24FEA56 8C2ED28D B48E05DB 3A610DC8 84D256A4 0E35EFCB 59BF6753 D3A489D2 8C7A4D97 3C2DA138 A6E7A4A0 8F68E16F

يتحقق النهائي من أن $PK_{MAP,IC} = KA(CA_{IC}, PK_{IC}, D_{IC})$.

— — — — — — — —

المرفق (ي) بالجزء ١١

إجراءات التفتيش (إعلامي)

ي-١ إجراءات التفتيش المتعلقة بتطبيق وثيقة السفر الإلكترونية المقروءة آلياً

يصف هذا القسم أحد إجراءات التفتيش التي تتضمن تطبيق وثيقة السفر الإلكترونية المقروءة آلياً ("وثائق LDS1").

١- الوصول إلى الدائرة المتكاملة اللاتلامسية (انظر القسم ٤-٢)

- إذا كان الوصول إلى الدائرة المتكاملة محمياً، يمكن في هذه الخطوة استخدام فتح الاتصال بكلمة سر مصدق عليها أو مراقبة الوصول الأساسية، رغم أنه يوصى باستخدام فتح الاتصال بكلمة سر مصدق عليها لأسباب أمنية. وابتداء من ١ يناير ٢٠١٨، يمكن لوثائق السفر الإلكترونية المقروءة آلياً أن تدعم فتح الاتصال بكلمة سر مصدق عليها فقط.
- إذا كان الوصول مدعوماً بالدائرة المتكاملة والوحدة الطرفية، ينبغي استخدام فتح الاتصال بكلمة سر مصدق عليها مع تحديد مجالات التحقق من صحة الرقاقة لأسباب تتعلق بالأداء.
- إذا كانت الدائرة المتكاملة تمنح حق الوصول إلى بيانات أقل حساسية في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً وإلى الملف الأولي EF.CardSecurity في الملف الرئيسي، إن كان موجوداً.

٢- بدء التحقق من صحة البيانات

- قراءة المادة الأمنية للوثيقة والتحقق من التوقيع، بما في ذلك التحقق المتسلسل من شهادة الجهة الموقعة على الوثيقة.

٣- التحقق من صحة الرقاقة

- تبعاً للدعم الذي توفره الدائرة المتكاملة، إجراء التحقق من صحة الرقاقة أو التحقق الفعال. ويستدل على دعم التحقق الفعال من وجود الملف الأولي EF.DG15 في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً، وعلى دعم التحقق من صحة الرقاقة من وجود المعلومات الأمنية المقابلة `SecurityInfos` في الملف الأولي EF.DG14.
- يمكن أيضاً إجراء هذه الخطوة كجزء من الخطوة ١، إذا استخدم فتح الاتصال بكلمة سر مصدق عليها مع تحديد مجالات التحقق من صحة الرقاقة.
- لا يكتمل التحقق من الصحة إلا بالاقتران مع التحقق من صحة الملف الذي يحتوي على المفتاح العام (EF.CardSecurity، أو EF.DG14، أو EF.DG15) المستخدم في هذه الخطوة.

٤- مراقبة الوصول الإضافية

- يعتبر إجراء التحقق من صحة الوحدة الطرفية ضرورياً إذا كانت وثيقة السفر الإلكترونية المقروءة آلياً مشكلة بحيث تتطلب ذلك من أجل الوصول إلى البيانات الحساسة، أي EF.DG3 و/أو EF.DG4.

٥- قراءة البيانات

- يمكن البدء بقراءة البيانات فور منح حقوق الوصول الضرورية، مثلاً يمكن قراءة البيانات الحساسة بعد الخطوة ١.
- يجب عدم اعتبار البيانات أصلية من دون التحقق من صحة البيانات المقروءة (الخطوة ٢).

ي–٢ إجراءات التفتيش المتعلقة بوثائق السفر الإلكترونية المقروءة آلياً المتعددة التطبيقات

يصف هذا القسم أحد إجراءات التفتيش المصممة لوثائق السفر الإلكترونية المقروءة آلياً التي تحتوي على تطبيق واحد أو أكثر إلى جانب تطبيق وثيقة السفر الإلكترونية المقروءة آلياً ("وثائق LDS2"). ويمكن أيضاً استخدام هذا الإجراء للوصول إلى تطبيق وثيقة السفر الإلكترونية المقروءة آلياً فقط.

١– الوصول إلى الدائرة المتكاملة اللاتلامسية (انظر القسم ٤–٢)

- في هذا الترتيب، لا يتوفر سوى فتح الاتصال بكلمة سر مصدق عليها للوصول إلى الدائرة المتكاملة.
- إذا كان الوصول مدعوماً بالدائرة المتكاملة والوحدة الطرفية، ينبغي استخدام فتح الاتصال بكلمة سر مصدق عليها مع تحديد مجالات التحقق من صحة الرقاقة لأسباب تتعلق بالأداء.
- إذا كانت الدائرة المتكاملة تمنح حق الوصول إلى بيانات أقل حساسية في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً وإلى الملف الأولي EF.CardSecurity في الملف الرئيسي.

٢– التحقق من وجود الملف الأولي EF.CardSecurity

- إذا لم يكن الملف الأولي EF.CardSecurity موجوداً، لا تدعم وثيقة السفر الإلكترونية المقروءة آلياً عملية التحقق في الملف الرئيسي (ما يعني أن الدائرة المتكاملة لا تحتوي إلا على تطبيق وثيقة السفر الإلكترونية المقروءة آلياً). في هذه الحالة، يجب اختيار تطبيق وثيقة السفر الإلكترونية المقروءة آليا والاستمرار بالخطوة ٢ في القسم ي–١ من هذا المرفق.

٣– بدء التحقق من صحة البيانات

- قراءة الملف الأولي EF.CardSecurity للوثيقة والتحقق من التوقيع، بما في ذلك التحقق المتسلسل من شهادة الجهة الموقعة على الوثيقة.
- تكون البيانات الواردة من تطبيق وثيقة السفر الإلكترونية المقروءة آلياً محمية عن طريق المادة الأمنية للوثيقة، التي يجب التحقق منها عند قراءة البيانات الواردة من هذا التطبيق. وتكون البيانات الواردة من تطبيقات أخرى محمية بالتواقيع على البيانات، التي يجب أيضاً

٤– التحقق من صحة الرقاقة

- يجب إجراء التحقق من صحة الرقاقة في الملف الرئيسي. وإذا لم تكن المعلومات الضرورية واردة في المعلومات الأمنية `SecurityInfos` في الملف الأولي EF.CardSecurity، لا تدعم الدائرة المتكاملة التحقق من الصحة في الملف الرئيسي. وفي هذه الحالة، يجب اختيار تطبيق وثيقة السفر الإلكترونية المقروءة آلياً والمتابعة بالخطوة ٢ من الإجراء الوارد في القسم ي–١ من هذا المرفق.
- يمكن أيضاً إجراء هذه الخطوة كجزء من الخطوة ١، إذا استخدم فتح الاتصال بكلمة سر مصدق عليها مع تحديد مجالات التحقق من صحة الرقاقة.
- لا يكتمل التحقق من الصحة إلا بالاقتران مع التحقق من صحة الملف الذي يحتوي على المفتاح العام (EF.CardSecurity) المستخدم في هذه الخطوة.

٥- مراقبة الوصول الإضافية

- يجب إجراء التحقق من صحة الوحدة الطرفية.
- إذا كان المطلوب هو الوصول فقط إلى قراءة البيانات الحساسة الواردة في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً، يمكن تخطي هذه الخطوة.

٦- قراءة/كتابة البيانات

- تشمل قراءة/كتابة البيانات اختيار التطبيقات التي تتضمن هذه الملفات.
- يمكن البدء بقراءة البيانات فور منح حقوق الوصول الضرورية، مثلاً يمكن قراءة البيانات الأقل حساسية لتطبيق وثيقة السفر الإلكترونية المقروءة آليا بعد الخطوة ١.
- يجب عدم اعتبار البيانات أصلية من دون التحقق من صحة البيانات المقروءة (الخطوة ٣).

— — — — — — —

المرفق (ك) بالجزء ١١

مراقبة الوصول الموسعة للاتحاد الأوروبي (إعلامي)

يستند التحقق من صحة الوحدة الطرفية حسبما هو معرّف في هذه الوثيقة إلى مراقبة الوصول الموسّعة كما يستخدمها الاتحاد الأوروبي (انظر [TR-03110]) لحماية الوصول إلى البصمات المخزنة في تطبيق LDS1. ويبين هذا المرفق الفرق بين [TR-03110] والبروتوكولات المعرّفة في هذه الوثيقة.

تشمل إجراءات التفتيش المتقدمة المستخدمة للوصول إلى وثائق السفر الإلكترونية المقروءة آلياً المجهزة بالمراقبة الموسعة للوصول وفقاً لـ [TR-03110] الخطوات التالية:

١- القيام بإجراءات الوصول إلى الرقاقة (انظر القسم ٤-٢) واختيار تطبيق وثيقة السفر الإلكترونية المقروءة آلياً؛

٢- إجراء التحقق من صحة الرقاقة في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً (انظر القسم ٦-٢) وبدء التحقق السلبي من الصحة (انظر القسم ٥-١)؛

٣- إجراء التحقق من صحة الوحدة الطرفية (انظر أدناه) في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً (انظر القسم ٧-١).

ملاحظة — يتم التحقق من الرقاقة والوحدة الطرفية في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً في مراقبة الوصول الموسعة للاتحاد الأوروبي. وتسمح المواصفات الواردة في هذه الوثيقة بإجراء هذه البروتوكولات، تبعاً للسياق، في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً او في الملف الرئيسي.

ك-١ حقوق الوصول

الجدول ك-١ ترخيص نظم التفتيش

7	6	5	4	3	2	1	0	Description
x	x	-	-	-	-	-	-	Role (see Doc 9303-12)
-	-	x	x	x	x	x	x	Access Rights
-	-	x	x	x	x	-	-	RFU
-	-	-	-	-	-	1	-	Read access to eMRTD Application: DG4 (Iris)
-	-	-	-	-	-	-	1	Read access to eMRTD Application: DG3 (Fingerprint)

تنقل حقوق الوصول إلى مجموعات البيانات في تطبيقات خلاف تطبيق وثيقة السفر الإلكترونية المقروءة آلياً عن طريق امتدادات الترخيص حسبما هو محدد في الجزأين ١٢ و١٠ من الوثيقة Doc 9303. وتنقل حقوق الوصول إلى البصمات (والحدقة) عن طريق نموذج الترخيص لحامل الشهادة.

ولحساب حقوق الوصول الفعلية، انظر القسم ٧-١-٤-٣-٦.

ك-٢ الملف الأولي CVCA

وفقاً للمواصفة، ترسل نقاط الثقة (مراجع السلطة المعنية بالشهادات) المعروفة لدى الدائرة المتكاملة بالنسبة للتحقق من الشهادة كجزء من التحقق من صحة الوحدة الطرفية إلى جهاز التوصيل كجزء من بروتوكول فتح الاتصال بكلمة سر مصدق عليها (انظر القسم ٤-٤-٣-٥).

وبدلاً من ذلك، تعرّف مراقبة الوصول الموسعة للاتحاد الأوروبي الملف الأولي الشفاف EF.CVCA في وثيقة السفر الإلكترونية المقروءة آلياً. وترد المواصفة أدناه:

الجدول ك-٢ الملف الأولي EF.CVCA

File Name	EF.CVCA
File ID	0x011C (default)
Short File ID	0x1C (default)
Read Access	PACE
Write Access	NEVER (internally updated only)
Size	36 bytes (fixed) padded with octets of value 0x00
Content	[CARi][[||CARi-1][[||0x00..00]

إذا كانت الدائرة المتكاملة تدعم التحقق من صحة الوحدة الطرفية في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً، فيجب أن تجعل مراجع المفاتيح العامة للسلطة الوطنية للتحقق من الشهادات (CVCA) ملائمة لنظم التفتيش في الملف الأولي الشفاف EF.CVCA في تطبيق وثيقة السفر الإلكترونية المقروءة آلياً كما هو محدد في الجدول ك-٢.

و**يجب** أن يحتوي هذا الملف على سلسلة من مواد بيانات مراجع السلطة المعنية بالشهادات (انظر الوثيقة Doc 9303-12) تلائم التحقق من صحة الوحدة الطرفية.

- **يجب** أن تحتوي على الأكثر على مادتين من مواد بيانات مراجع السلطة المعنية بالشهادات.
- **يجب** أن يكون أحدث مرجع للسلطة المعنية بالشهادات أول مادة بيانات افي القائمة.
- **يجب** حشو الملف بإضافة ثمانيات بقيمة 0x00.

وللملف EF.CVCA معرّف أصلي للملف الأولي ومعرّف قصير للملف الأولي. وإذا كان استخدام القيم الأصلية غير ممكن، **يجب** تحديد المعرّف (قصير) للملف الأولي في البارامتر الاختياري efCVCA المتعلق بالمعلومات TerminalAuthenticationInfo. وإذا استخدم efCVCA لبيان معرّف الملف الأولي المقرر استخدامه، يمسح المعرف الأصلي للملف الأولي. وإذا لم يُعط معرّف قصير للملف الأولي في efCVCA، **يجب** اختيار الملف الأولي EF.CVCA بشكل واضح باستخدام المعرّف الوارد للملف الأولي.

```
TerminalAuthenticationInfo ::= SEQUENCE {
  protocol OBJECT IDENTIFIER(id-TA),
  version  INTEGER, -- MUST be 1
  efCVCA   FileID OPTIONAL
}

FileID ::= SEQUENCE {
  fid  OCTET STRING (SIZE(2)),
  sfid OCTET STRING (SIZE(1)) OPTIONAL
```

— انتهـــى —

ISBN 978-92-9275-580-5