ايكاو

Doc 9303

وثائق السفر المقروءة آلياً

الطبعة الثامنة – ٢٠٢١

الجزء ١٢: البنية الأساسية للمفاتيح العامة لوثائق السفر المقروءة آلياً

اعتمدتها الأمينة العامة ونُشرت بموجب سلطتها

منظمة الطيران المدني الدولي

ايكاو

Doc 9303

وثائق السفر المقروءة آلياً

الطبعة الثامنة – ٢٠٢١

الجزء ١٢: البنية الأساسية للمفاتيح العامة لوثائق 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/mrtd

الوثيقة Doc 9303، *وثائق السفر المقروءة آليا*
الجزء ١٢ — *البنية الأساسية للمفاتيح العامة لوثائق السفر المقروءة آلياً*
Order No.: 9303P12
ISBN 978-92-9265-560-0 (print version)

التعديلات

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

سجل التعديلات والتصويبات

التعديلات		
الرقم	التاريخ	أدخل بواسطة

التصويبات		
الرقم	التاريخ	أدخل بواسطة

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

جدول المحتويات

الصفحة

١ – المجال

يعرّف الجزء الثاني عشر من الوثيقة Doc 9303 البنية الأساسية للمفاتيح العامة (PKI) لتطبيق وثيقة السفر الالكترونية المقروءة آلياً. ويتم تحديد متطلبات دول أو منظمات الإصدار، بما في ذلك تشغيل سلطة لإصدار الترخيص (CA) تقوم بإصدار الشهادات وقوائم إلغاء الشهادات (CRLs). وتحدَّد أيضاً متطلبات دول القبول ونظمها للتفتيش التي تصادق على تلك الشهادات وقوائم إلغاء الشهادات.

وتتضمن الطبعة الثامنة من الوثيقة Doc 9303 المواصفات العامة للأختام الرقمية المرئية (VDS) وسجلات السفر الاختيارية، وتطبيقات سجلات التأشيرات وسمات الاستدلال البيولوجي الإضافية (المعروفة باسم LDS2) كامتداد للتطبيق الإلزامي لوثيقة السفر الإلكترونية المقروءة آلياً (المعروف باسم LDS1).

ويجب أن تُقرأ الوثيقة Doc 9303-12 بالإقتران مع ما يلي:

- الوثيقة Doc 9303-10 — بنية البيانات المنطقية (LDS) لخزن بيانات الاستدلال البيولوجي وغيرها في دائرة متكاملة لا تلامسية (IC)؛
- والوثيقة Doc 9303-11 — آليات أمن وثائق السفر المقروءة آلياً؛
- والوثيقة Doc 9303-13 — الأختام الرقمية المرئية.

٢ – نظرة عامة إلى البنية الأساسية للمفاتيح العامة

تُتيح البنية الأساسية للمفاتيح العامة (PKI) لوثائق السفر الالكترونية المقروءة آلياً الإنشاء والتحقق اللاحق من صحة التوقيعات الرقمية على مواد وثائق السفر الالكترونية المقروءة آلياً، بما في ذلك المادة الأمنية للوثيقة (SO_D) لضمان أن البيانات الموقّعة صحيحة ولم يتم تعديلها. ولا يؤدي إلغاء الشهادة أو الإخفاق في إجراءات المصادقة خلال سير الترخيص أو الإخفاق في التحقق من التوقيع الرقمي وحده للتسبب في اعتبار أن وثيقة سفر الكترونية مقروءة آلياً غير صحيحة. ومثل هذا الإخفاق يعني أن التحقق الالكتروني من سلامة وصحة بيانات بنية البيانات المنطقية قد أخفق ويمكن عندئذٍ استخدام آليات غير الكترونية أخرى للبتّ في تلك المسألة كجزءٍ من التفتيش الشامل لوثيقة السفر الالكترونية المقروءة آلياً.

البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً أبسط بكثير من البنى الأساسية للمفاتيح العامة متعددة التطبيقات الأعم مثل البنية الأساسية للمفاتيح العامة للانترنت المعرّفة في [RFC 5280]. وفي البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً، تقوم كل دولة / سلطة إصدار بإنشاء سلطة إصدار ترخيص (CA) منفردة تقوم بإصدار جميع الشهادات مباشرة للكيانات النهائية، بما في ذلك الجهات الموقّعة على الوثائق. ويُشار إلى سلطات إصدار الترخيص هذه بإسم السلطات الوطنية المعنية بالتوقيع على الشهادات (CSCAs). ولا توجد سلطات إصدار ترخيص أخرى في البنية الأساسية. وتبني دول القبول الثقة مباشرةً في مفاتيح / شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات لكل دولة أو منظمة إصدار.

تستند البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً إلى معايير عامة للبنية الأساسية للمفاتيح العامة تشمل [X.509] و[RFC 5280]. وتلك المعايير الأساسية للبنية الأساسية للمفاتيح العامة تحدّد مجموعة كبيرة من السمات الاختيارية وعلاقات الثقة المتشعبة بين سلطات إصدار الترخيص التي لا صلة لها بتطبيق وثيقة السفر الالكترونية المقروءة آلياً. ويُحدَّد في هذا الجزء من الوثيقة Doc 9303 شكلٌ لتلك المعايير، مصمم خصيصاً ليناسب تطبيق وثيقة السفر الالكترونية المقروءة آلياً. وبعض الجوانب الفريدة لتطبيق وثيقة السفر الالكترونية المقروءة آلياً تشمل ما يلي:

- توجد على وجه الدقة سلطة وطنية واحدة معنية بالتوقيع على الشهادات لكل دولة إصدار.

- مسارات الترخيص تشمل على وجه الدقة شهادة واحدة (مثلاً الموقّع على الوثيقة)
- يجي أن يكون التحقق من التوقيع ممكناً بعد ٥–١٠ سنوات من انشائه.
- تغير اسم السلطة الوطنية المعنية بالتوقيع على الشهادات مدعوم.
- شهادات الارتباط الصادرة عن السلطة الوطنية المعنية بالتوقيع على الشهادات لا تُعالَج بوصفها شهادات متوسطة في مسار للترخيص.

في أغلب الأحيان، تكون البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً متوافقة مع [RFC 5280]. ومع ذلك، فإن حقيقة أن السلطات الوطنية المعنية بالتوقيع على الشهادات يمكن أن تخضع لتغيير اسم تفرض متطلبات فريدة على البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً تكون غير متوافقة مع بعض إجراءات المصادقة على قائمة إلغاء الشهادات المعرّفة في [RFC 5280]. وقد تم الابقاء على هذه الاختلافات في الحد الأدنى وهي محددةٌ بوضوحٍ.

بالنسبة للأختام الرقمية المرئية والبنية LDS2، تعتبر البنية الأساسية للمفاتيح العامة للتواقيع الرقمية، التي توفر سلامة وصحة مواد البيانات، امتداداً للبنية الأساسية للمفاتيح العامة للبنية LDS1. أما الجهات الموقعة على الأختام الرقمية المرئية وسمات الاستدلال البيولوجي الإضافية فتُصدرها نفس السلطة الوطنية المعنية بالتوقيع على الشهادت التي تصدر الجهاة الموقعة على البنية LDS1. وتحدد هذه الوثيقة التغيرات التي أدخلت على المواصفات الموجزة للشهادات المتعلقة بهذه التطبيقات الجديدة. ويشار إلى هذه العوامل مجتمعة بالبنية الأساسية **للمفاتيح العامة لوثيقة السفر الإلكترونية المقروءة آلياً.**

تتألف المفاتيح العامة للتواقيع الرقمية من الكيانات التالية:

- السلطة الوطنية المعنية بالتوقيع على الشهادت؛
- شهادات الجهات الموقعة المستخدمة للتوقيع على المادة الأمنية للوثيقة؛
- شهادات الجهات الموقعة على LDS2، وتتألف مما يلي:
  - الجهة الموقعة على LDS2-TS وتوقع على أختام السفر المتعلقة بالبنية LDS2؛
  - والجهة الموقعة على LDS2-V وتوقع على التأشيرات الإلكترونية المتعلقة بالبنية LDS2؛
  - والجهة الموقعة على LDS2-B وتوقع على سمات الاستدلال البيولوجي الإضافية المتعلقة بالبنية LDS2؛
- شهادات الجهة الموقعة على رمز الأعمدة (BCSC)، ويعرّف من أجلها في الوثيقة النوعان المحددان التاليان:
  - شهادات الجهة الموقعة على التأشيرات (VSC)؛
  - شهادات الجهة الموقعة على وثائق السفر في حالات الطوارئ؛
- شهادات الجهة الموقعة على القائمة الرئيسية وتستخدم للتوقيع على القوائم الرئيسية؛
- شهادات الجهة الموقعة على قائمة الانحراقات وتستخدم للتوقيع على قوائم الانحرافات؛
- قائمة إلغاء الشهادات.

توقع على جميع أنواع الشهادات المختلفة نفس السلطة الوطنية المعنية بالتوقيع على الشهادات. وتوقع هذه السلطة أيضاً على قائمة إلغاء الشهادات، التي تحتوي على أي شهادة ملغاة بصرف النظر عن نوع الشهادة. ويشار بشكل جماعي إلى جميع الشهادات الصادرة عن السلطة الوطنية المعنية بالتوقيع على الشهادات باسم **شهادات الجهات الموقعة.**

بالنسبة لتطبيقات البنية LDS2، تعرّف **بنية أساسية للمفاتيح العامة للتراخيص.** وتمكّن البنية الأساسية للمفاتيح العامة للتراخيص دولة أو منظمة الإصدار من مراقبة وإدارة الدول الأجنبية التي أعطيت لها تراخيص كتابة مواد بيانات البنية LDS2 على وثائق السفر الإلكترونية المقروءة آلياً الخاصة بها وقراءة مواد البيانات هذه. ويجب على الدولة الأجنبية التي ترغب في قراءة أو كتابة بيانات البنية LDS2 أن تحصل على شهادة الترخيص مباشرة من دولة أو منظمة إصدار وثيقة السفر الإلكترونية المقروءة آلياً.

تستخدم البنية الأساسية للمفاتيح العامة للتراخيص بنية مختلفة للشهادات (شهادات البطاقات التي يمكن إثباتها ISO 7816) وتتطلب بالتالي مكونات إضافية للبنية الأساسية.

تقتضي البنية LDS2 من الوحدة الطرفية أن تثبت للدائرة المتكاملة اللا تلامسية أنها مخوّلة بكتابة مواد بيانات البنية LDS2 على الدائرة المتكاملة اللا تلامسية أو أنها مخوّلة بقراءة مواد بيانات البنية LDS2. وتكون هذه الوحدة الطرفية مجهزة بمفتاح خاص واحد على الأقل وبشهادة الوحدة الطرفية المقابلة له، وذلك لترميز المفتاح العام للوحدة الطرفية وحقوق الوصول. وبعد أن تثبت الوحدة الطرفية معرفتها بهذا المفتاح الخاص، تقوم رقاقة وثيقة السفر المقروءة آلياً بمنح الوحدة الطرفية حق قراءة/كتابة بيانات البنية LDS2 كما هو مبين في شهادة الوحدة الطرفية.

تتألف البنية الأساسية للمفاتيح العامة للتراخيص البنية LDS2 من الكيانات التالية:

- السلطة الوطنية المعنية بالتوقيع على الشهادت؛
- والجهات المتحققة من الوثائق؛
- والوحدات الطرفية؛
- ونقطة الاتصال المفردة (SPOC).

ويدار توزيع وإدارة شهادات الترخيص بين السلطات الوطنية المعنية بالتوقيع على الشهادت والجهات المتحققة من الوثائق بواسطة نقطة اتصال مفردة في كل دولة.

يُحدد هذا الجزء الثاني عشر من الوثيقة Doc 9303 الوصف الموجز للبنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً، والوصف الموجز للبنية الأساسية للمفاتيح العامة للتراخيص والمواد المقابلة بما في ذلك ما يلي:

- أدوار ومسؤوليات الكيانات في البنية الأساسية.
- خوارزميات التشفير وإدارة المفاتيح.
- محتوى الشهادة وقائمة إلغاء الشهادات.
- آليات توزيع الشهادات وقائمة إلغاء الشهادات.
- المصادقة على مسار الترخيص.

٣ الأدوار والمسؤوليات

يقدم هذا القسم معلومات مفصلة عن الكيانات وأدوار ومسؤوليات كل من البنية الأساسية للمفاتيح العامة لوثيقة السفر الإلكترونية المقروءة آلياً والبنية الأساسية للمفاتيح العامة للتراخيص.

٣-١ البنية الأساسية للمفاتيح العامة لوثيقة السفر الإلكترونية المقروءة آلياً

صحة وسلامة البيانات المخزنة في وثائق السفر الالكترونية المقروءة آلياً يحميهما التحقق السلبي من الصحة. وهذه الآلية الأمنية تستند إلى توقيعات رقمية وتشتمل على كيانات البنية الأساسية للمفاتيح العامة التالية الخاصة بالبنية الأساسية للمفاتيح العامة لوثيقة السفر الإلكترونية المقروءة آلياً:

- **السلطة الوطنية المعنية بالتوقيع على الشهادات (CSCA):** تُنشئ كل دولة / سلطة إصدار سلطة وطنية واحدة معنية بالتوقيع على الشهادات بوصفها نقطة الثقة الوطنية في سياق وثائق السفر الالكترونية المقروءة آلياً. وتُصدر السلطة الوطنية المعنية بالتوقيع على الشهادات شهادات مفاتيح عامة لواحدة أو أكثر من الجهات (الوطنية) الموقّعة على الوثائق واختياراً للكيانات النهائية الأخرى مثل الموقّعين على القائمة الرئيسية والموقّعين على قائمة الانحرافات. وتقوم السلطة الوطنية المعنية بالتوقيع على الشهادات أيضاً بإصدار قوائم دورية بإلغاء الشهادات (CRL) تُبين ما إذا كانت أي من الشهادات التي أُصدرت قد أُلغيت.
- **الجهات الموقّعة على الوثائق (DS):** تقوم أي جهة موقّعة على وثيقة بالتوقيع رقمياً على البيانات التي تخزن في وثائق السفر الالكترونية المقروءة آلياً، ويخزن هذا التوقيع في وثيقة السفر الالكترونية المقروءة آلياً في المادة الأمنية للوثيقة.
- **الجهات الموقعة على سمات الاستدلال البيولوجي الإضافية (LDS2):** تقوم الجهة الموقعة على LDS2 بالتوقيع رقمياً على مواد بيانات البنية LDS2 من نوع واحد أو أكثر.
- **الجهات الموقعة على رمز الأعمدة (BCS):** تقوم الجهة الموقعة على رمز الأعمدة بالتوقيع رقمياً على البيانات (العنوان والرسالة) المرمزة في رمز الأعمدة. ويخزن التوقيع أيضاً في رمز الأعمدة. وتحدد هذه الوثيقة نوعان من حالات الاستعمال الخاصة بالجهة الموقعة على رمز الأعمدة، viz، التأشيرة ووثيقة السفر في حالات الطوارئ.
- **نظم التفتيش (IS):** يتحقق نظام للتفتيش من التوقيع الرقمي، بما في ذلك المصادقة على مسار الترخيص للتحقق من صحة وسلامة البيانات الالكترونية المخزنة في وثيقة السفر الالكترونية المقروءة آلياً كجزء من التحقق السلبي من الصحة.
- **الموقّعون على القائمة الرئيسية:** الموقّع على قائمة رئيسية هو كيان اختياري يوقع رقمياً على قائمة بشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات (المحلية والأجنبية) دعماً لآلية التوزيع الثنائي لشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات.
- **الجهات الموقّعة على قائمة الانحرافات:** تستخدم الجهات الموقعة على قوائم الانحرافات للتوقيع على قوائم الانحرافات. وقوائم الانحرافات معرّفة في الوثيقة Doc 9303-3.

يجب أن تكون المرافق المأمونة لصنع أزواج المفاتيح خاضعة لرقابة دولة أو منظمة الإصدار. ويشمل كل زوج من المفاتيح مفتاحاً "خاصاً" ومفتاحاً "عاماً". **ويجب** أن توفر للمفاتيح الخاصة والأنظمة أو التجهيزات المرتبطة بها عن طريق التصميم الأصيل والتجهيزات الأمنية للبرمجيات حماية من أي اطلاع خارجي أو غير مرخص به.

في حين أن شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات تظل ثابتة نسبياً، فإنه سيتم بمرور الوقت انشاء عدد كبير من شهادات الجهة الموقّعة على الوثيقة.

تعمل السلطة الوطنية المعنية بالتوقيع على الشهادات لكل دولة أو منظمة إصدار بوصفها النقطة الجديرة بالثقة لدولة القبول. وتقوم دولة أو منظمة الإصدار بتوزيع المفتاح العام للسلطة الوطنية المعنية بالتوقيع على الشهادات على دول القبول في شكل شهادة. وتقوم دولة القبول باثبات أن هذه الشهادة (والمفتاح المرخص به) "جديران بالثقة" من خلال وسائل خارج النطاق، وتخزّن "كياناً جديراً بالثقة" من أجل ذلك المفتاح الجدير بالثقة / الشهادة الجديرة بالثقة. **ويجب** أن تكون هذه الشهادات للسلطة الوطنية المعنية بالتوقيع على الشهادات شهادات موقّعة ذاتياً أصدرتها مباشرة السلطة الوطنية المعنية بالتوقيع على الشهادات. **ويجب** ألا تكون شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات في مرتبة أدنى أو شهادات متبادلة في بنية أساسية أكبر للمفاتيح العامة. ويجوز أيضاً إصدار شهادات الربط التي تصدرها ذاتياً

السلطة الوطنية المعنية بالتوقيع على الشهادات لمساعدة دولة القبول في إنشاء الثقة في مفتاح جديد / شهادة جديدة للسلطة الوطنية المعنية بالتوقيع على الشهادات عقب ترنح أحد المفاتيح.

ملاحظة — يوجد في بعض الدول اقتضاء أن يكون مراقب مركزي لسلطة إصدار الترخيص (CCA) السلطة العليا لنشر الشهادات الموقّعة ذاتياً لجميع الطلبات. وفي هذه الحالات، يتمثل حلّ ممكن في أن تنشئ السلطة الوطنية المعنية بالتوقيع على الشهادات شهادة موقعة ذاتياً (تفي بمقتضيات وثيقة الإيكاو Doc 9303) وجعل تلك الشهادة يصدق على توقيعها مراقب سلطة إصدار الترخيص (للوفاء باقتضاء أن يقوم بذلك مراقب سلطة إصدار الترخيص الخاص بالدولة). غير أن هذه الشهادات المصدق على توقيعها ليست جزءاً من البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً وقد لاتُوزّع على دول القبول.

٣-١-١ السلطة الوطنية المعنية بالتوقيع على الشهادات

يوصى بإنشاء أزواج مفاتيح السلطة الوطنية المعنية بالتوقيع على الشهادات (KPu_{CSCA}, KPr_{CSCA}) وتخزينها في بنية أساسية عالية الحماية، خارج الخط لسلطة إصدار الترخيص.

يُستخدم المفتاح الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات (KPr_{CSCA}) للتوقيع على شهادات الجهة الموقّعة على الوثيقة (C_{DS})، وشهادات أخرى وقوائم إلغاء الشهادات.

تستخدم شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات (C_{CSCA}) للمصادقة على شهادات الجهة الموقّعة على الوثيقة وشهادات الموقّع على القائمة الرئيسية وشهادات الموقّع على قائمة الانحرافات وقوائم إلغاء الشهادات والشهادات الأخرى التي تصدرها السلطة الوطنية المعنية بالتوقيع على الشهادات.

يجب أن تمتثل جميع الشهادات وقوائم إلغاء الشهادات للصور الجانبية المحددة في القسم ٧ و**يجب** توزيعها باستخدام آليات التوزيع حسب ما هي محددة في القسم ٥.

بالنسبة للمشاركين في دليل المفاتيح العامة، **يجب** أيضاً إرسال كل شهادة من السلطة الوطنية المعنية بالتوقيع على الشهادات بواسطة هيئة إصدار الشهادة إلى دليل المفاتيح العامة (لغرض المصادقة على شهادات الجهة الموقّعة على الوثيقة (C_{DS})).

يجب إصدار قوائم إلغاء الشهادات على أساسٍ دوري حسب ما هو محدد في القسم ٤.

٣-١-٢ الجهات الموقّعة على الوثيقة

يوصى بإنشاء أزواج مفاتيح الجهة الموقّعة على الوثيقة (KPu_{DS}, KPr_{DS}) وتخزينها في بنية أساسية ذات مستوى عالٍ من الحماية.

يستخدم المفتاح الخاص للجهة الموقّعة على الوثيقة (KPr_{DS}) للتوقيع على المواد الأمنية للوثائق (SO_D).

تستخدم شهادات الجهة الموقّعة على الوثيقة (C_{DS}) للمصادقة على المواد الأمنية للوثائق (SO_D).

يجب أن تمتثل كل شهادة للجهة الموقّعة على الوثيقة للصورة الجانبية الواردة في الشهادة المعرّفة في القسم ٧ و**يجب** تخزينها في الدائرة المتكاملة اللا تلامسية لكل وثيقة سفر الكترونية مقروءة آلياً تمّ التوقيع عليها بالمفتاح الخاص المناظر للجهة الموقّعة على الوثيقة (انظر الوثيقة Doc 9303-10 للاطلاع على التفاصيل). ويضمن هذا أن دولة القبول يُتاح لها الاطلاع على شهادة الجهة الموقّعة على الوثيقة ذات الصلة بكل وثيقة سفر الكترونية مقروءة آلياً.

ينبغي أن تُرسل إلى الإيكاو أيضاً بواسطة جهة إصدار الشهادات شهادات الجهات الموقّعة على الوثائق المشاركة في دليل المفاتيح العامة من أجل النشر في دليل الإيكاو للمفاتيح العامة (PKD).

٣-١-٣ الجهات الموقّعة على البنية LDS2

تقوم الجهة الموقّعة على البنية LDS2 بالتوقيع رقمياً على مواد بيانات البنية LDS2 من نوع واحد أو أكثر.

وحيثما تدعو الحاجة إلى الإشارة إلى الجهات الموقعة على البنية LDS2 باعتبارها الجهة التي توقع على نوع خاص من مواد بيانات البنية LDS2، يشار إليها على النحو التالي:

- الجهة الموقعة على LDS2-TS وتوقع على أختام السفر المتعلقة بالبنية LDS2؛
- والجهة الموقعة على LDS2-V وتوقع على التأشيرات الإلكترونية المتعلقة بالبنية LDS2؛
- والجهة الموقعة على LDS2-B وتوقع على سمات الاستدلال البيولوجي الإضافية المتعلقة بالبنية LDS2؛

و**يوصى** بأن لا يكون لدى كل دولة أكثر من جهة موقعة واحدة على أختام السفر المتعلقة بالبنية LDS2، وجهة موقعة واحدة على التأشيرات الإلكترونية المتعلقة بالبنية LDS2، وجهة موقعة واحدة على سمات الاستدلال البيولوجي الإضافية المتعلقة بالبنية LDS2. ويمكن أيضاً لجهة موقعة واحدة على البنية LDS2 أن تجمع بعض هذه الأدوار أو جميعها.

وإذا كان المطلوب زيادة التمييز، من قبيل الموقع الذي أضيف منه ختم السفر، أو الموظف الذي أعطى تصريحاً لأحد المسافرين، أو الموظف الذي أعطى التأشيرة، أو الموقع الذي أضيفت فيه سمات الاستدلال البيولوجي الإضافية، يمكن إدراجه في خانة الملكية ضمن مادة بيانات LDS2 نفسها الخاصة بها.

٣-١-٤ الجهات الموقّعة على رمز الأعمدة

يوصى بإنشاء أزواج مفاتيح الجهة الموقّعة على رمز الأعمدة (KPu_{BCS}, KPr_{BCS}) وتخزينها في بنية أساسية محمية للغاية.

يستخدم المفتاح الخاص للجهة الموقعة على رمز الأعمدة (KPr_{BCS}) للتوقيع على البيانات (العنوان والرسالة) المرمزة في رمز الأعمدة. ويخزن التوقيع أيضاً في رمز الأعمدة.

تستخدم شهادات الجهة الموقعة على رمز الأعمدة (C_{BCS}) للمصادقة على البيانات (العنوان والرسالة) المرمزة في رمز الأعمدة.

و**يجب** أن تمتثل كل شهادة من شهادات الجهة الموقعة على رمز الأعمدة (C_{BCS}) للوصف الموجز للشهادة المعرّف في القسم ٧. ولا ترد شهادات الجهة الموقعة على رمز الأعمدة في الختم الرقمي نفسه. وبالتالي **يجب** على البلد الذي يصدر وثائق محمية بأختام رقمية أن ينشر جميع شهادات الجهة الموقعة على رمز الأعمدة الخاص به. وتكون قناة التوزيع الأولية لشهادات الجهة الموقعة على رمز الأعمدة عبارة عن دليل المفاتيح العامة الثنائي. وتعتبر الآليات الأخرى، مثل النشر على شبكة الويب، قنوات ثانوية.

و**ينبغي** أيضاً أن ترسل شهادات الجهة الموقعة على رمز الأعمدة للمشاركين في دليل المفاتيح العامة بواسطة هيئة إصدار الشهادة إلى الإيكاو لنشرها في دليل الإيكاو للمفاتيح العامة.

وتعتبر الجهة الموقعة على التأشيرات والجهة الموقعة على وثائق السفر في حالات الطوارئ حالات خاصة للجهة الموقعة على رمز الأعمدة.

٣-١-٥ نظام التفتيش

تقوم منظمة تفتيش بالتحقق السلبي من الصحة لضمان سلامة وصحة البيانات المخزنة على الدائرة المتكاملة اللا تلامسية لوثيقة السفر الالكترونية المقروءة آلياً. وكجزءٍ من تلك العملية، **يجب** أن تؤدي نظم التفتيش التحقق من صحة مسار الترخيص على النحو المبين في القسم ٦.

٣-١-٦ الجهة الموقّعة على القائمة الرئيسية

يُستخدم المفتاح الخاص للموقّع على القائمة الرئيسية للتوقيع على القوائم الرئيسية للسلطة الوطنية المعنية بالتوقيع على الشهادات.

تُستخدم شهادات الموقّع على القائمة الرئيسية لاعتماد القوائم الرئيسية للسلطة الوطنية المعنية بالتوقيع على الشهادات.

٣-١-٧ الجهة الموقّعة على قائمة الانحرافات

يُستخدم المفتاح الخاص للموقّع على قائمة الانحرافات للتوقيع على قوائم الانحرافات.

- تُستخدم شهادات الموقّع على قائمة الانحرافات لاعتماد قوائم الانحرافات.

٣-٢ البنية الأساسية للمفاتيح العامة للتراخيص

يكتب تطبيق البنية LDS2 على الدائرة المتكاملة اللا تلامسية لوثيقة سفر إلكترونية مقروءة آلياً بواسطة دولة أو منظمة الإصدار وقت إضفاء الطابع الشخصي.

وقبل أن تتمكن دولة أخرى من كتابة مواد البنية LDS2 على الدائرة المتكاملة اللا تلامسية، **يجب** أن تحصل من دولة أو منظمة الإصدار على ترخيص للقيام بذلك. وتكون كل مادة بيانات للبنية LDS2 موقعة رقمياً من جانب الجهة الموقعة على البنية LDS2 في الدولة القائمة بالكتابة وتكتب لاحقاً على الدائرة المتكاملة اللا تلامسية بواسطة وحدة طرفية مرخصة في الدولة القائمة بالكتابة. وتشبه العملية المكونة من خطوتين المتمثلة بالتوقيع من قبل الجهة الموقعة والكتابة بواسطة وحدة طرفية مرخصة مفهوم البنية LDS1 حيث تقوم الجهة الموقعة على الوثيقة بالتوقيع رقمياً على المواد الأمنية للوثيقة ولكن هذه المواد تكتب لاحقاً على الدائرة المتكاملة اللا تلامسية من خلال عملية إضفاء الطابع الشخصي، كما هو موضّح في الشكل ١. وتتم القراءة اللاحقة لمواد البنية LDS2 من الدائرة المتكاملة اللا تلامسية من خلا وحدات طرفية مرخصة لقراءة البنية LDS2 الخاصة بالنوع المعني للمادة LDS2.

تمكّن البنية الأساسية للمفاتيح العامة للتراخيص دولة أو منظمة إصدار وثيقة السفر إلكترونية المقروءة آلياً من مراقبة الوصول (القراءة والكتابة) إلى بيانات LDS2 على الدوائر المتكاملة اللا تلامسية لوثائق السفر الإلكترونية المقروءة آلياً التي تصدرها.

٣-٢-١ السلطة الوطنية للتحقق من الشهادات

يجب على كل دولة او منظمة إصدار تسمح بإضافة بيانات LDS2 إلى وثائق السفر الإلكترونية المقروءة آلياً أن تنشئ سلطة وطنية واحدة للتحقق من الشهادات (CVCA). وهذه السلطة هي سلطة لإصدار للتراخيص (CA) تعتبر كيان الثقة للبنية الأساسية للمفاتيح العامة للتراخيص لتلك الدولة أو المنظمة وتغطي جميع تطبيقات LDS2. وقد تكون السلطة الوطنية للتحقق من الشهادات بمثابة كيان قائم بذاته أو مدمجة مع السلطة الوطنية المعنية بالتوقيع على الشهادات التابعة لتلك الدولة أو المنظمة ذاتها. غير أنه إذا كانتا تشتركان في نفس الموقع، **يجب** على السلطة الوطنية للتحقق من الشهادات أن تستخدم زوج مفاتيح مختلف عن زوج المفاتيح الخاص بالسلطة الوطنية المعنية بالتوقيع على الشهادات. وتحدد السلطة الوطنية للتحقق من الشهادات حقوق الوصول التي ستمنح إلى جميع المتحققين من الوثائق، المحلية منها والأجنبية، وتصدر شهادات تحتوي على التراخيص الفردية لكل واحد من المتحققين من الوثائق.

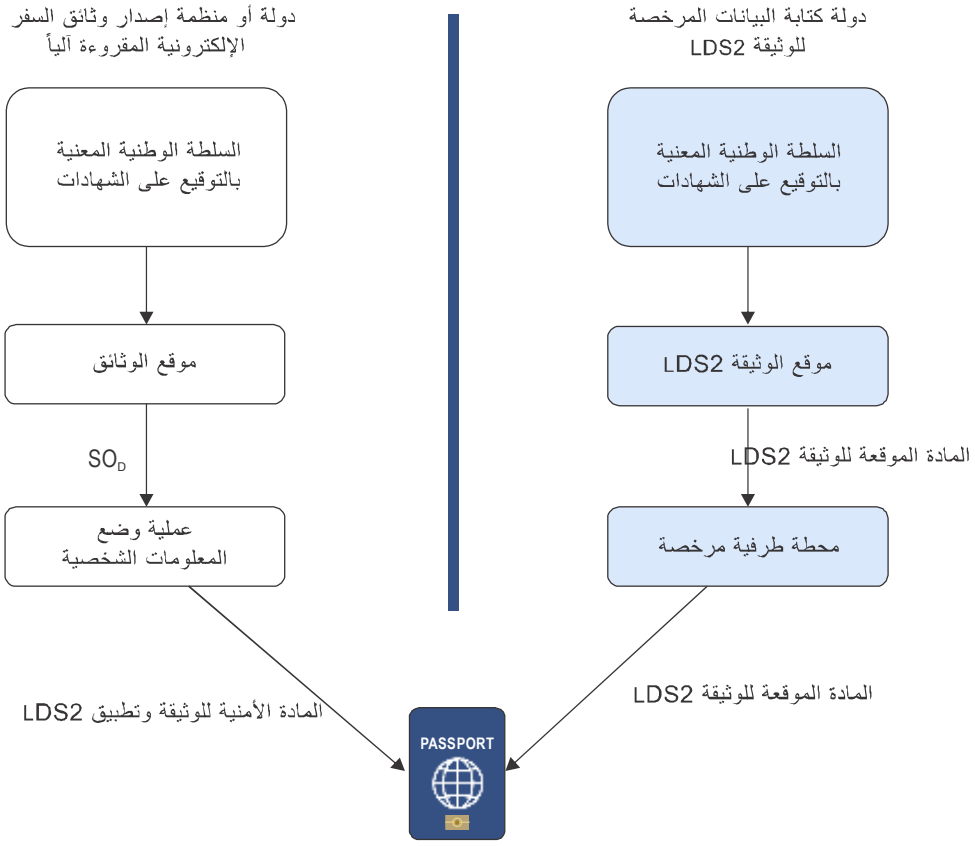
٣-٢-٢ المتحقق من الوثائق

المتحقق من الوثائق هو سلطة إصدار للتراخيص تقوم، بوصفها جزءاً من وحدة تنظيمية، بإدارة مجموعة من الوحدات الطرفية (مثل الوحدات الطرفية التي يشغلها حراس حدود الدولة) وإصدار شهادات ترخيص لهذه الوحدات الطرفية. ويجب أن يكون المتحقق من الوثائق قد تلقى بالفعل شهادة ترخيص من السلطة الوطنية المسؤولة للتحقق من الشهادات قبل أن يتمكن من إصدار شهادات مرتبطة بوحداته الطرفية. و**يجوز** للشهادات الصادرة عن المتحقق من الوثائق أن تحتوي على الترخيص نفسه، أو على مجموعة فرعية منه، يمكن منحها إلى المتحقق من الوثائق. و**يجب ألا** تحتوي على أي ترخيص يتخطى الترخيص المعطى للمتحقق من الوثائق.

٣-٢-٣ الوحدة الطرفية/نظام التفتيش

ضمن سياق البنية الأساسية للمفاتيح العامة للتراخيص، الوحدة الطرفية هي كيان يمكنه الوصول إلى الدائرة المتكاملة اللا تلامسية لوثيقة سفر إلكترونية مقروءة آلياً ويكتب مادة بيانات موقعة رقمياً للبنية LDS2، أو يقرأ مادة بيانات للبنية LDS2. و**يجب** أن يكون للوحدة الطرفية شهادة

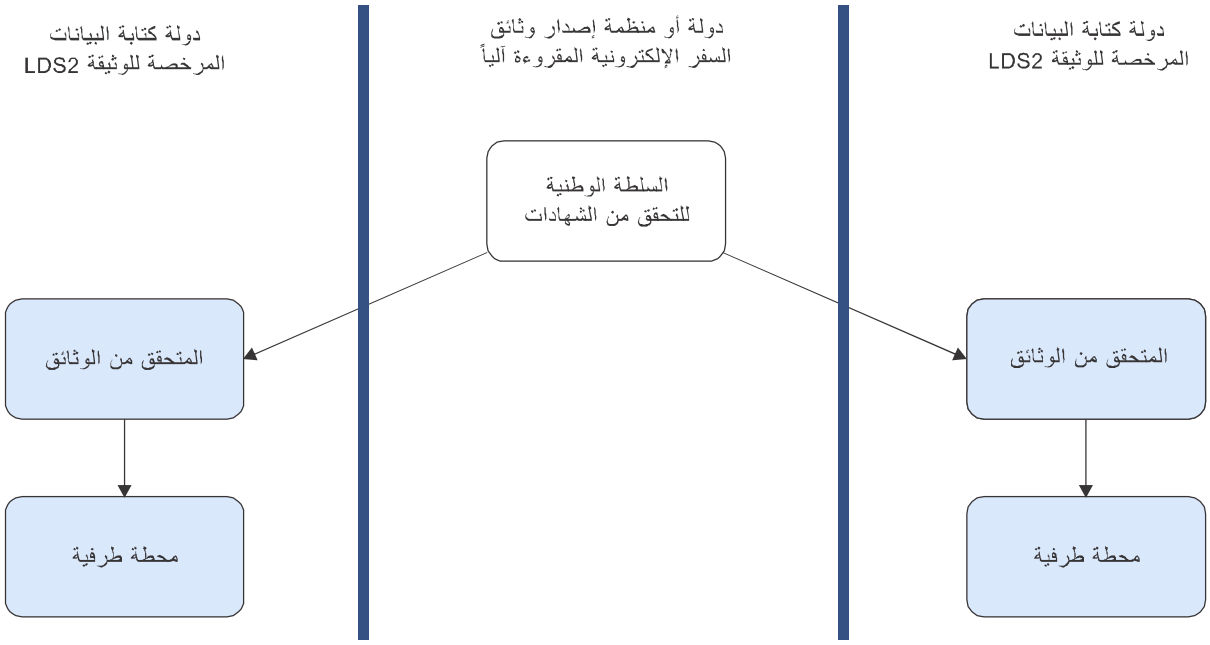
ترخيص صادرة لها من جانب المتحقق المحلي من الوثائق الخاص بها الذي يمنح الترخيص المطلوب. ويشار أيضاً إلى الوحدة الطرفية باسم نظام التفتيش.



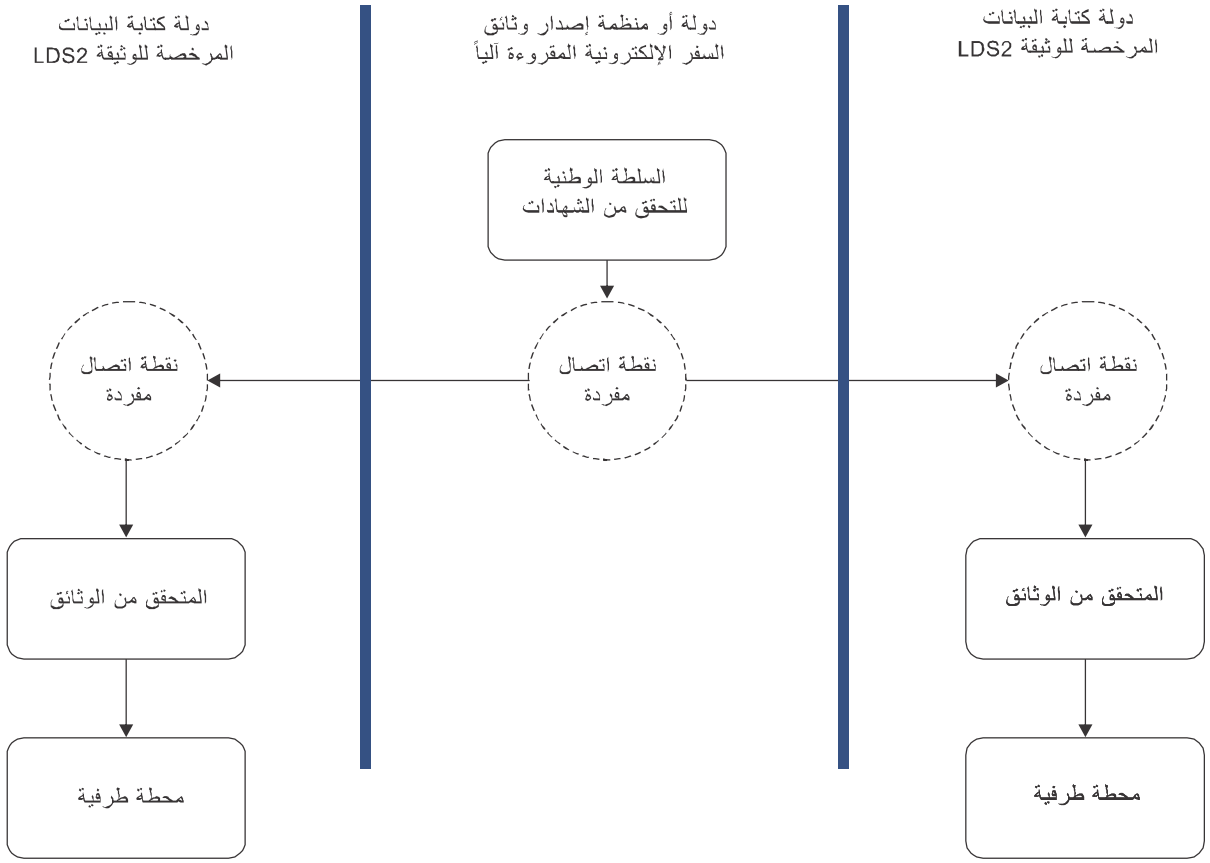
الشكل ١ – نموذج الثقة في البنية LDS2 وهيكل الكتابة

٣-٢-٤ *نقطة الاتصال المفردة (SPOC)*

يجب على كل دولة تشارك في البنية الأساسية للمفاتيح العامة للتراخيص في البنية LDS2 أن تنشئ نقطة اتصال مفردة واحدة. وهذه النقطة هي الواجهة التي تستخدم لجميع الاتصالات بين السلطة الوطنية للتحقق من الشهادات في إحدى الدول والمتحققين من الوثائق في دولة أخرى. وتنقل الطلبات على الشهادات والردود عليها بين نقاط الاتصال المفردة في كل دولة باستخدام بروتوكول نقطة الاتصال المفردة المحدد في القسم ٨.



الشكل ٢ — نموذج الثقة للبنية الأساسية للمفاتيح العامة للتراخيص



الشكل ٣ — دور نقطة الاتصال المفردة

٤ – إدارة المفاتيح

يتم تعريف إدارة المفاتيح بالنسبة للبنيتين الأساسيتين للمفاتيح العامة بشكل منفصل.

٤ – ١ البنية الأساسية للمفاتيح العامة لوثيقة السفر الإلكترونية المقروءة آلياً

يجب أن يكون لدى دول أو منظمات الإصدار نوعان من أزواج المفاتيح على الأقل:

- زوج مفاتيح السلطة الوطنية المعنية بالتوقيع على الشهادات؛
- وزوج مفاتيح الجهة الموقّعة على الوثيقة.

يجوز أن يكون لدى دول أو منظمات الإصدار أنواع من أزواج المفاتيح الإضافية:

- زوج مفاتيح الموقّع على القائمة الرئيسية،

- وزوج مفاتيح الموقّع على قائمة الانحرافات؛
- وزوج مفاتيح الموقع على البنية LDS2؛
- وزوج مفاتيح عميل نقطة الاتصال المفردة؛
- وزوج مفاتيح مخدذم نقطة الاتصال المفردة؛
- وزوج مفاتيح الموقّع على التأشيرات/زوج مفاتيح الموقعّ على وثيقة السفر في حالات الطوارئ (وهما نوعان من الجهات الموقعة على رمز الأعمدة).

يتم إصدار المفاتيح العامة للسلطة الوطنية المعنية بالتوقيع على الشهادات وشهادة الجهة الموقّعة وشهادة نقطة الاتصال المفردة باستخدام شهادات [X.509]. وتُستخدم المفاتيح العامة التي تحتوي عليها شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات للتحقق من توقيع السلطة الوطنية المعنية بالتوقيع على الشهادات على شهادات الجهة الموقعة وشهادات نقطة الاتصال المفردة التي تم إصدارها، والسلطة الوطنية المعنية بالتوقيع على الشهادات، وعلى قوائم إلغاء الشهادات التي تم إصدارها.

بالنسبة للموقّع على القائمة الرئيسية والموقّع على قائمة الانحرافات ومفاتيح وشهادات الاتصالات، يُترك عمر المفتاح الخاص وفترة صلاحية الشهادة لتقدير دولة أو منظمة الإصدار.

يُربَط كل من شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات وشهادات الجهة الموقّعة على الوثيقة باستخدام مفتاح خاص وفترة صلاحية مفتاح عام على النحو المبين في الجدول ١.

الجدول ١ — استخدام المفاتيح وصلاحيتها

	استخدام المفتاح الخاص	**صلاحية المفتاح العام (على افتراض سريان جوازات السفر لفترة ١٠ سنوات)**
السلطة الوطنية المعنية بالتوقيع على الشهادات	٣–٥ سنوات	١٣–١٥ سنة
الجهة الموقّعة على الوثيقة	حتى ٣ شهور[1]	١٠ سنوات تقريباً
الجهة الموقّعة على ختم السفر في البنية LDS2	١–٢ سنة	١٠ سنوات + ٣ أشهر
الجهة الموقّعة على المتحقق من البنية LDS2	١–٢ سنة	١٠ سنوات + ٣ أشهر
الجهة الموقّعة على رمز الأعمدة في البنية LDS2	١–٢ سنة	١٠ سنوات + ٣ أشهر
عميل نقطة الاتصال المفردة	غير محدد	٦–١٨ شهراً
مخدّم نقطة الاتصال المفردة	غير محدد	٦–١٨ شهراً
الجهة الموقعة على رمز الأعمدة في التأشيرة	١–٢ سنة	مدة استخدام المفتاح الخاص + مدة صلاحية التأشيرة

1 لاحظ لامتداد المناظر `privateKeyUsage` في شهادة الجهة الكوقعة على الوثيقة قد يكون أطول بقليل للسماح بالتداخل أو متطلبات الانتاج.

	استخدام المفتاح الخاص	صلاحية المفتاح العام (على افتراض سريان جوازات السفر لفترة ١٠ سنوات)
الجهة الموقعة على رمز الأعمدة في وثيقة السفر في حالات الطوارئ	سنة + شهران (الشهران من أجل التجديد)	مدة استخدام المفتاح الخاص + الإطار الزمني لصلاحية وثيقة السفر في حالات الطوارئ
الموقّع على القائمة الرئيسية	تقدير دولة أو منظمة الإصدار	تقدير دولة أو منظمة الإصدار
الموقّع على قائمة الانحرافات	تقدير دولة أو منظمة الإصدار	تقدير دولة أو منظمة الإصدار
الاتصال	تقدير دولة أو منظمة الإصدار	تقدير دولة أو منظمة الإصدار

٤-١-١ *مفاتيح وشهادات الجهة الموقّعة على الوثيقة*

فترة استخدام المفتاح الخاص للجهة الموقّعة على الوثيقة أقصر بكثير من فترة صلاحية شهادة الجهة الموقّعة على الوثيقة للمفتاح العام المناظر.

٤-١-١-١ *صلاحية المفتاح العام للجهة الموقّعة على الوثيقة*

عمر، أي فترة صلاحية الشهادة، للمفتاح العام للجهة الموقّعة على الوثيقة يُحدد بسلسلة الفترتين التاليتين:

- طول الوقت الذي سيُستخدم فيه المفتاح الخاص المناظر لإصدار وثائق سفر الكترونية مقروءة آلياً،
- مع أطول فترة صلاحية لأي وثيقة سفر الكترونية مقروءة آلياً تم إصدارها بواسطة ذلك المفتاح[٢]..

يجب أن تكون شهادة الجهة الموقّعة على الوثيقة (C_{DS}) صالحةً لهذه الفترة الاجمالية لإتاحة التحقق من صحة وثائق السفر الالكترونية المقروءة آلياً. غير أن المفتاح الخاص المناظر **ينبغي** استخدامه فقط لإصدار وثائق لفترة محدودة، بمجرد انتهاء صلاحية الوثيقة الأخيرة التي استُخدم لإصدارها، إذ أن المفتاح العام لا يعود مطلوباً.

٤-١-١-٢ *فترة إصدار المفتاح الخاص للجهة الموقّعة على الوثائق*

عندما تقوم دول أو منظمات الإصدار بنشر نظمها، قد ترغب في مراعاة عدد الوثائق التي سيتم التوقيع عليها بواسطة مفتاح خاص منفرد للجهة الموقّعة على الوثيقة.

يجوز لأي دولة أو منظمة إصدار نشر واحدة أو أكثر من الجهات الموقّعة على الوثائق، تكون كل منها مزودة بزوج مفاتيحها الخاصة الفريدة، الناشطَين في أي وقت معين.

بغية خفض تكاليف استمرار الأعمال إلى الحد الأدنى في حالة إلغاء شهادة الجهة الموقّعة على الوثيقة، قد ترغب دولة أو منظمة إصدار تُصدر عدداً كبيراً من وثائق السفر الالكترونية المقروءة آلياً في اليوم فيما يلي:

- استخدام فترة استخدام قصيرة للغاية للمفتاح الخاص، و/أو
- نشر عدة جهات متزامنة موقعة على الوثائق ناشطة في الوقت ذاته، يكون لكلٍّ منها مفتاحها الخاص الفريد الخاص بها وشهادة مفتاح عام.

---

2 قد تصدر بعض دول أو منظمات الإصدار وثائق سفر الكترونية مقروءة آلياً قبل أن تصبح صالحة، مثلاً عند تغيير الاسم عند الزواج. وفي هذه الحالات، فإن "أطول فترة صلاحية لأي وثيقة سفر الكترونية مقروءة آلياً" تشمل الصلاحية الفعلية لوثيقة السفر الالكترونية المقروءة آلياً (مثلاً ١٠ سنوات) زائداً الوقت الأقصى بين إصدار وثيقة السفر الالكترونية المقروءة آلياً والوقت الذي تصبح فيه صالحةً.

يجوز لأي دولة أو منظمة إصدار تصدر عدداً صغيراً من وثائق السفر الإلكترونية المقروءة آلياً في اليوم أي تختار نشر جهة موقّعة غلى الوثائق منفردة ويجوز أيضاً الارتياح مع وجود فترة أطول بقليل لاستخدام مفتاح خاص.

بصرف النظر عن عدد وثائق السفر الالكترونية المقروءة آلياً الصادرة في اليوم، أو عدد الجهات الموقّعة على الوثائق الناشطة في الوقت ذاته، **يوصى** بأن تكون الفترة القصوى التي يستخدم فيها مفتاح خاص لجهة موقعة على الوثائق للتوقيع على وثائق سفر الكترونية مقروءة آلياً ثلاثة أشهر.

بمجرد انتاج آخر وثيقة موقّع عليها بمفتاح خاص معين، **يوصى** بأن تمحو دول أو منظمات الإصدار المفتاح الخاص بطريقة يمكن مراجعتها وتقديم حساب عنها.

٤-١-٢ *مفاتيح وشهادات الجهة الموقّعة على سمات الاستدلال البيولوجي*

تشبه أزواج مفاتيح الجهة الموقّعة على سمات الاستدلال البيولوجي (LDS2) أزواج مفاتيح الجهة الموقّعة على الوثائق من حيث أن فترة استعمال المفاتيح الخاصة أقصر بكثير من فترة صلاحية الشهادة المقابلة. و**يجب** أن تبقى الشهادات صالحة خلال عمر وثيقة السفر الإلكترونية المقروءة آلياً أو المادة الموقّعة للبنية LDS2 (أيهما أطول). وبما أن مواد البيانات الموقّعة ستكتب على وثائق السفر الإلكترونية المقروءة آلياً من قبل دول مختلفة، **يجب** أن تكون هذه الشهادات صالحة لمدة لا تقل عن أطول عمر لوثيقة السفر الإلكترونية المقروءة آلياً (أي ١٠ سنوات).

٤-١-٢-١ *فترة صلاحية المفتاح الخاص للجهة الموقّعة على البنية LDS2*

يحدد عمر المفتاح الخاص للجهة الموقّعة على البنية LDS2، أي فترة صلاحية الشهادة، عن طريق ربط الفترتين التاليتين معاً:

- المدة التي سيستخدم فيها المفتاح الخاص المقابل للتوقيع على مواد البينة LDS2، مع
- فترة صلاحية الوثيقة الأطول مما يلي:
  - أي وثيقة سفر إلكترونية مقروءة آلياً ستخزن مادة LDS2 الموقعة بذلك المفتاح؛ أو
  - أي مادة LDS2 موقعة بذلك المفتاح. ويلاحظ أنه في حالة تأشيرة إلكترونية من النوع LDS2، من الممكن تمديد فترة صلاحية التأشيرة الإلكترونية الموقّعة إلى ما بعد فترة صلاحية وثيقة السفر الإلكترونية المقروءة آلياً التي تتضمن تلك التأشيرة.

٤-١-٣ *مفاتيح وشهادات الجهة الموقّعة على رمز الأعمدة*

الجهة الموقّعة على رمز الأعمدة هي نوع محدد من مخدّمات التوقيع المستخدمة للتوقيع على فئة وحية من أنواع الوثائق، مثل التأشيرة، ووثيقة السفر في حالات الطوارئ وما إلى ذلك. ولاتباع أفضل الممارسات في هذا المجال، **يوصى** باستخدام عدد محدود فقط من مفاتيح التوقيع (أقل عدد مؤلف من رقم واحد) بشكل متواز لإنشاء تواقيع للأختام الرقمية، ما لم تحتم المتطلبات التشغيلية استخدام عدد أكبر من المفاتيح بشكل مطلق. ولضمان توافر الجهة الموقعة على رمز الأعمدة في حالة حادث أمني متعلق بمفاتيح التوقيع، **يوصى** بأن يكون هناك تدابير لضمان استمرارية الأعمال (مثل إعداد مفاتيح احتياطية، وموقع احتياطي وما إلى ذلك).

ولتسهيل التعامل مع الشهادات المقابلة (انظر القسم ٥)، **يجب** أن يكون عدد مفاتيح صلاحية التواقيع محدوداً بخمسة مفاتيح تواقيع في السنة.

٤-١-٣-١ *فترة صلاحية المفتاح الخاص للجهة الموقّعة على رمز الأعمدة*

يطبق هذا القسم على جميع الجهات الموقعة على رمز الأعمدة، بما في ذلك الجهة الموقعة على التأشيرات والجهة الموقعة على وثائق السفر في حالات الطوارئ.

يحدد عمر المفتاح الخاص للجهة الموقّعة على رمز الأعمدة، أي فترة صلاحية الشهادة، عن طريق ربط الفترتين التاليتين معاً:

- المدة التي سيستخدم فيها المفتاح الخاص المقابل لإصدار تأشيرة أو وثيقة سفر في حالات الطوارئ، مع

- أطول فترة صلاحية لأي وثيقة تصدر بواسطة هذا المفتاح[٣].

و**يجب** أن تكون شهادة الجهة الموقّعة على رمز الأعمدة صالحة لهذه الفترة الإجمالية لإتاحة التحقق من صحة الوثيقة. ومع ذلك، **ينبغي** ألا يستخدم المفتاح الخاص إلا لإصدار وثائق لفترة محدودة، وبعد انتهاء صلاحية الوثيقة الأخيرة التي استخدمت للإصدار، لم يعد هناك حاجة للمفتاح الخاص.

مدة استخدام المفتاح الخاص:	حسب الوصف الموجز للوثيقة
صلاحية الشهادة:	مدة استخدام المفتاح الخاص + الإطار الزمني لفترة صلاحية الوثيقة

مثال

ملاحظة — لا يترتب أي توصيات على فترات الصلاحية المستخدمة في الحسابات المتضمنة في هذا المثال.

لنفترض أن مدة صلاحية الوثائق التي تم إصدارها ٥ سنوات، وأن مدة استخدام المفتاح الخاص لشهادة الجهة الموقّعة على رمز الأعمدة هي سنة واحدة. عندئذ تكون فترة صلاحية شهادة الجهة الموقّعة على رمز الأعمدة ١ + ٥ = ٦ سنوات. وإذا كنت مدة استخدام المفتاح الخاص لشهادة السلطة المعنية بالتوقيع على الشهادات ٣ سنوات، تكون فترة صلاحية شهادة السلطة المعنية بالتوقيع على الشهادات ٣ + ٦ = ٩ سنوات.

٤-١-٤ مفاتيح وشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات

فترة استخدام مفتاح الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات أقصر بكثير من فترة صلاحية شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات للمفتاح العام المناظر.

٤-١-٤-١ صلاحية المفتاح العام للسلطة الوطنية المعنية بالتوقيع على الشهادات

يُحدّد عمر، أي صلاحية شهادة، المفتاح العام للسلطة الوطنية المعنية بالتوقيع على الشهادات عن طريق ربط الفترتين التاليتين معاً:

- طول الوقت الذي سيستخدم فيه المفتاح الخاص المناظر للسلطة الوطنية المعنية بالتوقيع على الشهادات للتوقيع على أي شهادة تحت السلطة الوطنية المعنية بالتوقيع على الشهادات،
- والعمر الأقصى لأي شهادة تصدر تحت السلطة الوطنية المعنية بالتوقيع على الشهادات.

٤-١-٤-٢ فترة إصدار المفتاح الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات

فترة استخدام المفتاح الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات لتوقيع شهادات وقوائم إلغاء الشهادات هي توازن دقيق بين العوامل التالية:

- في الحدث غير المحتمل المتمثل في أن يتعرض مفتاح سلطة إصدار الترخيص الخاص للتوقيع في البلد بواسطة دولة أو منظمة للخطر، فإن صلاحية جميع وثائق السفر الالكترونية المقروءة آلياً التي أُصدرت باستخدام مفاتيح الجهة الموقّعة على الوثيقة التي تم توقيع شهاداتها بالمفتاح الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات الذي تعرّض للخطر يكون مشكوكاً فيه. وبالتالي **يجوز** أن ترغب دول أو منظمات الإصدار في الإبقاء على فترة إصدار قصيرة تماماً،
- غير أن الابقاء على فترة الإصدار قصيرة للغاية سيؤدي إلى وجود عدد كبير جداً من المفاتيح العامة السارية للسلطة الوطنية المعنية بالتوقيع على الشهادات في أي وقت معين. ويمكن أن يؤدي هذا إلى إدارة شهادات أكثر تعقيداً داخل نظم المعالجة عند الحدود.

---

[٣] قد تصدر بعض دول أو منظمات الإصدار وثائق سفر إلكترونية مقروءة آلياً قبل أن تصبح صالحة، وعلى سبيل المثال عند تغيير اسم بعد الزواج. وفي هذه الحالات، فإن "أطول فترة صلاحية لوثيقة سفر إلكترونية مقروءة آلياً" تشمل الصلاحية الفعلية لوثيقة السفر الإلكترونية المقروءة آلياً (مثلاً ١٠ سنوات) زائد المدة القصوى بين وقت إصدار وثيقة السفر الإلكترونية المقروءة آلياً والوقت الذي تصبح عنده صالحة.

لذلك **يوصى** بأن يتم كل ثلاث إلى خمس سنوات استبدال زوج مفاتيح السلطة الوطنية المعنية بالتوقيع على الشهادات لدولة أو منظمة إصدار.

٤-١-٤-٣ المفتاح المُعاد صنعه للسلطة الوطنية المعنية بالتوقيع على الشهادات

توفر مفاتيح السلطة الوطنية المعنية بالتوقيع على الشهادات نقاط ثقة في النظام بأكمله وبدون هذه قد ينهار النظام. ولذلك **ينبغي** أن تخطط دول ومنظمات الإصدار للاستعاضة بعناية عن زوج مفاتيحها للسلطة الوطنية المعنية بالتوقيع على الشهادات. وبمجرد انقضاء فترة الإصدار لمفتاح التوقيع الخاص الأصلي للسلطة الوطنية المعنية بالتوقيع على الشهادات، سيكون لدى أي دولة أو منظمة إصدار دائماً اثنتان على الأقل من شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات (CCSCA) ساريتان في أي وقت معين.

يجب على دول أو منظمات الإصدار اخطار دول القبول بأنه يجري التخطيط لتمديد مفتاح للسلطة الوطنية المعنية بالتوقيع على الشهادات. و**يجب** تقديم هذا الإخطار قبل تمديد المفتاح بتسعين يوماً. وبمجرد حدوث تمديد المفتاح يتم توزيع الشهادة الجديدة للسلطة الوطنية المعنية بالتوقيع على الشهادات (التي تشهد بالمفتاح العام الجديد للسلطة الوطنية المعنية بالتوقيع على الشهادات) على دول القبول.

إذا كانت شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات شهادة جديدة موقعة ذاتياً، ينبغي القيام بالتحقق من صحة تلك الشهادة باستخدام أسلوب خارج النطاق.

عند حدوث تمديد لمفتاحٍ للسلطة الوطنية المعنية بالتوقيع على الشهادات **يجب** إصدار شهادة تربط المفتاح الجديد بالمفتاح القديم لتوفير انتقال مأمون للأطراف المعتمِدة. وعموماً يُحقَّق هذا من خلال إصدار شهادة مُصدَرة ذاتياً تكون فيها خانة هيئة الإصدار وخانة الموضوع متطابقتين لكن المفتاح المستخدم للتحقق من التوقيع يمثل زوج المفاتيح القديم والمفتاح العام المعتمد يمثل زوج المفاتيح الجديد. وهذه الشهادات للربط الخاصة بالسلطة الوطنية المعنية بالتوقيع على الشهادات لا تحتاج إلى تحقق باستخدام أسلوب خارج النطاق نظراً لأن التوقيع على شهادة الربط بالسلطة الوطنية المعنية بالتوقيع على الشهادات يتم التحقق منه باستخدام مفتاح عام موثوق به بالفعل بالنسبة لتلك السلطة الوطنية المعنية بالتوقيع على الشهادات. ويمكن أيضاً استخدام القوائم الرئيسية لتوزيع الربط بالسلطة الوطنية المعنية بالتوقيع على الشهادات والاجتهادات الأساسية الموقّعة ذاتياً للسلطة الوطنية المعنية بالتوقيع على الشهادات.

ينبغي أن تمتنع دول أو منظمات الإصدار عن استخدام مفتاحها الخاص الجديد للسلطة الوطنية المعنية بالتوقيع على الشهادات لليومين الأولين بعد تمديد مفتاح السلطة الوطنية المذكورة، للتأكد من أن المفتاح العام الجديد المناظر للسلطة الوطنية المذكورة قد تم توزيعه بنجاح.

يجب على دول ومنظمات الإصدار أن تستخدم المفتاح الخاص الأحدث للسلطة الوطنية المعنية بالتوقيع على جميع الشهادات، ولتوقيع قوائم إلغاء الشهادات.

٤-١-٥ إلغاء الشهادات

قد تحتاج دول أو منظمات الإصدار لإلغاء شهادات في حالة واقعةٍ (مثل انكشاف مفتاح).

يجب على جميع السلطات الوطنية المعنية بالتوقيع على الشهادات إصدار معلومات إلغاء دورية في شكل قائمة إلغاء الشهادات (CRL).

يجب على السلطات الوطنية المعنية بالتوقيع على الشهادات أن تصدر قائمة إلغاء شهادات واحدة على الأقل كل ٩٠ يوماً، حتى لو لم يتم إلغاء أي شهادات منذ أن أُصدرت قائمة إلغاء الشهادات السابقة. و**يجوز** إصدار قوائم إلغاء الشهادات بتواتر أكثر من إصدارها كل٩٠ يوماً ولكن ليس بتواتر يتجاوز إصدارها كل ٤٨ ساعةً.

إذا تم إلغاء الشهادة، **يجب** توزيع قائمة إلغاء الشهادات تُبين ذلك الإلغاء في غضون ٤٨ ساعةً.

يمكن إلغاء الشهادات فقط، ليس المواد الأمنية للوثائق. ويقتصر استخدام قوائم إلغاء الشهادات على الإخطارات بالشهادات الملغاة التي أصدرتها السلطة الوطنية المعنية بالتوقيع على الشهادات التي أصدرت قائمة إلغاء الشهادات (بما في ذلك الاشعارات بالإلغاء لشهادات

السلطة الوطنية المعنية بالتوقيع على الشهادات وشهادات الجهة الموقّعة على الوثيقة وشهادات الموقّع على القائمة الرئيسية وشهادات الموقّع على قائمة الانحرافات وأي أنواع أخرى من الشهادات التي أصدرتها تلك السلطة لإصدار الترخيص).

لا تُستخدم قوائم إلغاء الشهادات المقسمة في تطبيق وثيقة السفر الالكترونية المقروءة آلياً. وجميع الشهادات التي ألغتها سلطة وطنية معنية بالتوقيع على الشهادات، بما في ذلك شهادات الجهة الموقّعة على الوثيقة وشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات وشهادات الموقّع على القائمة الرئيسية وشهادات الموقّع على قائمة الانحرافات، ترد قائمة بها على نفس قائمة إلغاء الشهادات. وعلى الرغم من أن قائمة إلغاء الشهادات يتم دائماً التوقيع عليها بأحدث مفتاح توقيع خاص (حالي) للسلطة الوطنية المعنية بالتوقيع على الشهادات، تشمل قائمة إلغاء الشهادات إشعارات بإلغاء شهادات تم التوقيع عليها بذلك المفتاح الخاص نفسه فضلاً عن شهادات تم التوقيع عليها بمفاتيح توقيع سابقة خاصة للسلطة الوطنية المعنية بالتوقيع على الشهادات.

٤-١-٥-١ إلغاء شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات

إلغاء شهادة للسلطة الوطنية المعنية بالتوقيع على الشهادات هو متطرفٌ وصعبٌ في الوقت ذاته. وعند إخطار دولة قبول بأن الشهادة للسلطة الوطنية المعنية بالتوقيع على الشهادات قد أُلغيت، فإن جميع الشهادات الأخرى الموقّعة باستخدام المفتاح الخاص المناظر للسلطة الوطنية المعنية بالتوقيع على الشهادات تُلغى بالفعل.

حيث يكون قد تمّ التوقيع على شهادة وصل لسلطة وطنية معنية بالتوقيع على الشهادات باستخدام مفتاح خاص قديم للسلطة الوطنية المعنية بالتوقيع على الشهادات للمصادقة على مفتاح عام جديد للسلطة الوطنية المعنية بالتوقيع على الشهادات (انظر "المفتاح المعاد صنعه للتوقيع الوطني" في ٤-١-٤-٣)، يلغي الشهادة القديمة للسلطة الوطنية المعنية بالتوقيع على الشهادات **يجب** أن يلغي أيضاً الشهادة الجديدة للسلطة الوطنية المعنية بالتوقيع على الشهادات.

إذا كانت شهادة للسلطة الوطنية المعنية بالتوقيع على الشهادات في حاجة إلى إلغاء، يجوز للسلطة الوطنية المذكورة إصدار قائمة إلغاء الشهادات موقعة بمفتاح خاص مناظر للمفتاح العام الذي يتم إلغاءه، نظراً لأن هذا هو المفتاح الوحيد الذي سيكون مستخدمو قائمة إلغاء الشهادات قادرين على التحقق منه في ذلك الوقت. وينبغي اعتبار المفتاح العام للسلطة الوطنية المذكورة صالحاً فقط لغرض التحقق من أن توقيع قائمة إلغاء الشهادات صالحٌ. وبمجرد أن يتمّ تحقق مستخدم لقائمة إلغاء الشهادات من صحة توقيع قائمة إلغاء الشهادات، يُعتبر مفتاح التوقيع الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات تعرّض للخطر وتُلغى الشهادة بالنسبة لجميع عمليات التحقق من الصحة المستقبلية.

لإصدار وثائق جديدة، **يجب** أن تلجأ دولة أو منظمة الإصدار إلى تأهيل عمليتها للتحقق من الصحة منذ البداية، عن طريق إصدار شهادة جذرية جديدة للسلطة الوطنية المعنية بالتوقيع على الشهادات وتوزيع تلك الشهادة على دول القبول وتأييد التأكيد خارج النطاق أن الشهادة التي تسلمتها كل دولة قبول هي في الحقيقة الشهادة الأصلية الحالية للسلطة الوطنية المعنية بالتوقيع على الشهادات.

٤-١-٥-٢ إلغاء الشهادات الأخرى

عندما ترغب دولة أو منظمة إصدار في إلغاء شهادة جهة موقعة تم إصدارها تحت السلطة الوطنية المعنية بالتوقيع على الشهادات، فإنها لا تحتاج إلى الانتظار حتى فترة `nextUpdate` في قائمة إلغاء الشهادات الحالية حان وقت إصدارها لقائمة إلغاء شهادات جديدة. و**يوصى** بإصدار قائمة إلغاء الشهادات في غضون فترة ٤٨ ساعة من الإشعار بالإلغاء.

٤-١-٦ خوارزميات التشفير

يجوز أن تدعم دولة أو منظمة الإصدار خوارزمية مختلفة للاستخدام في مفاتيحها لسلطتها الوطنية المعنية بالتوقيع على الشهادات ولمفاتيح شهادات التوقيع. وعلى سبيل المثال، ربما تكون السلطة الوطنية المعنية بالتوقيع على الشهادات قد صدرت باستخدام ريفست وشمير وأدلمان، ولكن قد تكون شهادات الجهة الموقعة خوارزمية التوقيع الرقمي للمنحنى الإهليلجي والعكس بالعكس.

يجب أن تختار دول أو منظمات الإصدار أطوال مفاتيح ملائمة تتيح حماية من الهجمات و**ينبغي** أن تُؤخذ بعين الاعتبار كتالوجات تشفير مناسبة.

يجب أن تدعم دول القبول جميع الخوارزميات في النقاط حيث ترغب في التحقق من صحة التوقيع على وثائق السفر الالكترونية المقروءة آلياً.

يجب أن تدعم دول أو منظمات الإصدار واحدة من الخوارزميات أدناه للاستخدام في سلطتها الوطنية المعنية بالتوقيع على الشهادات ومفاتيح التوقيع، وعند الاقتضاء، المواد الأمنية للوثائق.

٤-١-٦-١ ريفست وشمير وأدلمان

دول أو منظمات الإصدار تلك التي تنفذ خوارزمية ريفست وشمير وأدلمان لإنشاء التوقيع أو التحقق من صحة الشهادات والمادة الأمنية للوثيقة (SO_D) **يجب** أن تستخدم [RFC 4055]. ويحدد [RFC 4055] آليتين للتوقيع، RSASSA-PSS و RSASSA-PKCS1_v15. و**يوصى** بأن تُنشئ دول أو منظمات الإصدار التوقيعات وفقاً لـ RSASSA-PSS، لكن دول القبول **يجب** أن تكون على استعداد أيضاً للتحقق من صحة التوقيعات وفقاً لـ RSASSA-PKCS1_v15.

٤-١-٦-٢ خوارزمية التوقيع الرقمي

دول أو منظمات الإصدار تلك التي تنفّذ خوارزمية التوقيع الرقمي لإنشاء التوقيع أو التحقق من صحته **يجب** أن تستخدم [FIPS (القاعدة القياسية الاتحادية لمعالجة المعلومات) 4-186].

٤-١-٦-٣ خوارزمية التوقيع الرقمي للمنحنى الاهليلجي

دول أو منظمات الإصدار تلك التي تنفذ خوارزمية التوقيع الرقمي للمنحنى الاهليلجي لإنشاء التوقيع أو التحقق من صحته **يجب** أن تستخدم [X9.62] أو [ISO/IEC 15946]. ومعايير نطاق المنحنى الاهليلجي المستخدمة لانشاء زوج مفاتيح خوارزمية التوقيع الرقمي للمنحنى الاهليلجي **يجب** وصفها صراحة في معايير المفتاح العام، أي أن المعايير يجب أن تكون من نوع معايير المنحنى الاهليلجي (لا منحنيات مسمات، لا معايير ضمنية) و**يجب** أن تتضمن العامل المشترك الاختياري. و**يجب** أن تكون نقاط المنحنى الاهليلجي في شكل غير مضغوط.

يوصى باتباع التوجيه [TR 03111].

٤-١-٦-٤ خوارزميات استخدام البصمة الرقمية

SHA-224, SHA-256, SHA-384 and SHA-512، هي الخوارزميات الوحيدة المسموح بها لاستخدام البصمة الرقمية. انظر [القاعدة القياسية الاتحادية لمعالجة المعلومات FIPS 180-2].

٤-١-٧ خوارزميات التشفير لشهادات الجهة الموقعة على البنية LDS2

بما أن شهادات البنية LDS2 والمواد الموقّعة تكون مخزنة على الدائرة المتكاملة اللا تلامسية، فعليها أن تكون متراصّة قدر الإمكان. لذلك يجب أن تستخدم الجهات الموقعة على البنية LDS2 خوارزمية التوقيع الرقمي للمنحنى الإهليلجي، بصرف النظر عن الخوارزمية المستخدمة في السلطة الوطنية المعنية بالتوقيع على الشهادات ومفاتيح التوقيع على الوثائق.

٤-٢ البنية الأساسية للمفاتيح العامة للتراخيص

يجب أن يكون لدى دول أو منظمات الإصدار التي تنفّذ البنية LDS2 أنواع أزواج المفاتيح التالية:

- زوج مفاتيح السلطة الوطنية المعنية بالتوقيع على الشهادات؛
- وزوج مفاتيح المتحقق من الوثائق؛

- وزوج مفاتيح الوحدة الطرفية.

تصدّق السلطة الوطنية المعنية بالتوقيع على الشهادات على المفاتيح العامة للسلطة الوطنية المعنية بالتوقيع على الشهادات والمفاتيح العامة للمتحقق من الوثائق. ويصدق المتحقق من الوثائق على المفاتيح العامة للوحدة الطرفية. والمفاتيح العامة لكل من السلطة الوطنية المعنية بالتوقيع على الشهادات والمتحقق من الوثائق والوحدة الطرفية هي شهادات يمكن التحقق بواسطة بطاقة و**يجب** أن تمتثل للأوصاف الموجزة للشهادات المقابلة لها المعرّفة في القسم ٧. ولا يوجد آلية إلغاء لشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات أو شهادات المتحقق من الوثائق أو شهادات الوحدة الطرفية. ولذلك تكون فترات صلاحيتها أقصر بكثير من فترة صلاحية الشهادة X.509.

لا تحدد فترة استخدام المفتاح الخاص وتخضع لتقدير الدولة. ومع ذلك، **يجب** أن تكون فترة استخدام المفتاح الخاص مساوية على الأكثر لفترة صلاحية المفتاح العام. ويوضح الجدول ٢ فترة صلاحية المفاتيح العامة لأزواج مفاتيح السلطة الوطنية المعنية بالتوقيع على الشهادات والمتحقق من الوثائق والوحدة الطرفية.

الجدول ٢ — صلاحية الشهادة القابلة للتحقق بواسطة بطاقة لاستخدام المفتاح

	صلاحية المفتاح العام
السلطة الوطنية المعنية بالتوقيع على الشهادات	٦ أشهر – ٣ سنوات
المتحقق من الوثائق	أسبوعان – ٣ أشهر
الوحدة الطرفية	يوم واحد – شهر واحد

٤-٢-١ *خوارزميات التشفير للتحقق من صحة الوحدة الطرفية*

تحدد السلطة الوطنية المعنية بالتوقيع على الشهادات التابعة لدولة إصدار وثيقة السفر الإلكترونية المقروءة آلياً الخوارزمية المستخدمة في التحقق من صحة الوحدة الطرفية في البنية الأساسية للمفاتيح العامة للتراخيص. و**يجب** أن تستخدم خوارزمية التوقيع وبارامترات النطاق وأحجام المفاتيح نفسها ضمن سلسلة الشهادات (أي لشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات وشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية بالنسبة لترخيص معين). ونتيجة لذلك، يتعين أن يكون المتحققون من الوثائق والوحدات الطرفية مجهزين بعدة أزواج من المفاتيح. و**يجوز** لشهادات الربط بالسلطة الوطنية المعنية بالتوقيع على الشهادات أن تشمل مفتاحاً عاماً ينحرف عن البارامترات الحالية، أي **يجوز** للسلطة الوطنية المعنية بالتوقيع على الشهادات أن تتحول إلى خوارزمية توقيع جديدة أو بارامترات نطاق جديدة أو أحجام مفاتيح حديدة.

وبالنسبة للتحقق من صحة الوحدة الطرفية، يجوز استخدام خوارزمية التوقيع الرقمي أو خوارزمية التوقيع الرقمي للمنحنى الإهليلجي. وترد التفاصيل في الوثيقة Doc 9303-11.

٤-٢-٢ *خوارزميات التشفير لنقطة الاتصال المفردة*

ترد في الجدول ٣ مجموعات التشفير المقرر استخدامها في بروتوكول نقطة الاتصال المفردة.

الجدول ٣ — مجموعات تشفير أمن طبقة النقل

خوارزمية تبادل الشهادات والمفاتيح	مجموعة الشفرات
RSA	TLS_RSA_WITH_AES_128_CBC_SHA
DHE_RSA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
RSA	TLS_RSA_WITH_AES_256_CBC_SHA
DHE_RSA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
ECDHE_ECDSA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE_ECDSA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

وفي نطاق التفاوض بإقامة اتصال بأمن طبقة النقل، **يجب** على العميل أن يدعم مجموعات شفرات أمن طبقة النقل المحددة في الجدول ٣. ويجب على كل من المخدّم والعميل أن يدعم التحقق من صحة خوارزمية التوقيع الرقمي أو خوارزمية التوقيع الرقمي للمنحنى الإهليلجي. ويسمح للمخدّم بطلب شهادة عميل من نوع مختلف عن شهادة المخدّم وللعميل أيضاً بإرسالها.

ويعتبر استخدام اتفاق مفاتيح ECDHE_ECDSA في اتصال أمن طبقة النقل متوافقاً مع الإضافات المحددة في [TLSECC] و[TLS1.2] و[TLSEXT]. و**يجب** على كل من العميل والمخدّم أن يدعم الامتدادات المناسبة للمنحنيات الإهليلجية حسبما هو محدد في المواصفة [TLSECC] في نطاق اتصال أمن طبقة النقل. وتحدد المنحنيات الإهليلجية المدعومة وأشكال نقاط المنحنيات الإهليلجية في القسم ٥ من [TLSECC]. و**يجب** أن يكون استخدام مجموعات شفرات أمن طبقة النقل المحددة في الجدول ٣، التي تستخدم القاعدة القياسية للتشفير المتقدم للتشفير متوافقة مع المواصفة [TLSAES].

٥- آليات التوزيع

بالنسبة للبنية الأساسية للمفاتيح العامة لوثائق السفر الإلكترونية المقروءة آلياً، ثمة حاجة لتوزيع مواد البنية الأساسية للمفاتيح العامة على دول القبول. ويُستخدم عدد من آليات التوزيع المختلفة، يتوقف على نوع المادة والمتطلبات التشغيلية. ومن المهم ملاحظة أن توزيع هذه المواد **لا** يُنشئ ائتماناً لتلك المواد، أو مفاتيح خاصة / عامة مرتبطة بها. وآليات إنشاء الإئتمان محددة في القسم ٦-١.

ويغطي القسم ٨ آلية توزيع البنية الأساسية للمفاتيح العامة.

المواد التي ثمة حاجة لتوزيعها من دول أو منظمات الإصدار على دول القبول تشمل ما يلي:

- شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات؛
- وشهادات الربط بالسلطة الوطنية المعنية بالتوقيع على الشهادات؛
- وشهادات الجهة الموقّعة على الوثيقة؛
- وشهادات الجهة الموقعة على البنية LDS2؛
- والشهادات الأولية للسلطة الوطنية للتحقق من الشهادات؛
- وشهادات الربط بالسلطة الوطنية للتحقق من الشهادات؛
- وشهادات المتحقق من الوثائق؛

- وشهادات الجهة الموقعة على رمز الأعمدة؛
- وقوائم إلغاء الشهادات (الباطل وغير الباطل).
- وشهادات الموقّع على القائمة الرئيسية، القوائم الرئيسية؛
- وشهادات الجهة الموقّعة على قائمة الانحرافات.

آليات التوزيع المستخدمة في البنية الأساسية للمفاتيح العامة لوثائق السفر الالكترونية المقروءة آلياً والتراخيص تشمل ما يلي:

- دليل المفاتيح العامة؛
- والتبادل الثنائي؛
- ونقطة الاتصال المفردة؛
- والقوائم الرئيسية؛
- وقوائم الانحرافات؛
- والدائرة المتكاملة اللا تلامسية لوثيقة السفر الالكترونية المقروءة آلياً.

تحدد آلية توزيع أولي وثانوي (حيث يكون ملائماً) لكل مادة على النحو المبين في الجدول ٤.

الجدول ٤ — توزيع مواد البنية الأساسية للمفاتيح العامة

	الدائرة المتكاملة اللا تلامسية	نقطة الاتصال المفردة	ثنائي	دليل المفاتيح العامة	قائمة الانحرافات	القائمة الرئيسية	ملاحظات
شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات			نعم (أولي)			نعم (ثانوي)	
وشهادات الجهة الموقعة على الوثائق	نعم (أولي)			نعم (ثانوي)			شهادات مكتوبة في الوقت الذي تكتب فيه SOD
شهادات الجهة الموقعة على البنية LDS2	نعم						شهادات مكتوبة في الوقت الذي تكتب فيه الحاجة الموقّعة
الشهادة الأولية للسلطة الوطنية للتحقق من الشهادات	نعم						شهادات مكتوبة في الوقت الذي تكتب فيه المواصفات الشخصية لوثيقة السفر الإلكترونية المقروءة آلياً
شهادات الربط بالسلطة الوطنية للتحقق من الشهادات	نعم	نعم					شهادات توزع على المتحققين من الوثائق عن طريق كيان جدير بالثقة لنقطة الاتصال المفردة والسلطة الوطنية للتحقق من الشهادات يتم تحديثه على الدائرة المتكاملة اللا تلامسية عند التحقق التالي

شهادات المتحقق من الوثائق		نعم					توزع فقط على المتحقق من وثائق الموضوع
قوائم إلغاء الشهادات (الباطل وغير الباطل).			نعم (ثانوي)	نعم (أولي)			تشمل قوائم إلغاء الشهادات التي تصدرها السلطة الوطنية المعنية بالتوقيع على الشهادات معلومات الإلغاء ذات الصلة بمواد البنية الأساسية للمفاتيح العامة للبنية LDS2
شهادات الجهة الموقّعة على القائمة الرئيسية					نعم		
شهادات الجهة الموقعة على رمز الأعمدة			نعم (ثانوي)	نعم (أولي)			لا يتم ترميز الجهات الموقّعة على رمز الأعمدة في رمز الأعمدة وبالتالي يجب أن يكون التوزيع مكفولاً للتحقق من رمز الأعمدة
القوائم الرئيسية			نعم	نعم			
شهادات الجهة الموقّعة على قائمة الانحرافات					نعم		

من الناحية التشغيلية، دول القبول غير ملزمة باستخدام كلٍّ من المصدر الأولي والثانوي. وفي التشغيل اليومي لنظام تفتيش، يُترك لتقدير سلطة التفتيش ما إذا كان يتعين استخدام المصدر الأولي أو الثانوي. وإذا استخدمت سلطة دولة القبول المصدر الثانوي لشهادة أو قائمة إلغاء الشهادات في عملياتها اليومية، ينبغي أن تكون على استعداد لدعم المصدر الأولي كذلك.

دول أو منظمات الإصدار تحتاج لتخطيط استراتيجيات تمديد فترة استخدام زوج مفاتيحها بالنسبة لكل من مفاتيح السلطة الوطنية المعنية بالتوقيع على الشهادات ومفاتيح الجهة الموقّعة بغية اتاحة نشر الشهادات **و**قوائم إلغاء الشهادات إلى داخل أنظمة مراقبة حدود دول القبول في الوقت المناسب. والوضع الأمثل هو أن الانتشار سيحدث في غضون ٤٨ ساعةً، لكن بعض دول القبول قد تكون لديها نقاط خارجية نائية وضعيفة التوصيل قد يستغرق انتشار الشهادات وقوائم إلغاء الشهادات عليها وقتاً أطول. و**ينبغي** أن تبذل دول القبول كل جهد لتوزيع هذه الشهادات وقوائم إلغاء الشهادات على جميع محطات الحدود في غضون ٤٨ ساعةً.

ينبغي أن تتوقع دول أو منظمات الإصدار أن شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات (C_{CSCA}) سيتم نشرها بواسطة دول القبول في غضون ٤٨ ساعةً.

تضمن دول أو منظمات الإصدار أن يتم في الوقت المناسب نشر شهادات الجهات الموقّعة على الوثائق (C_{DS}) عن طريق إرفاق شهادة الجهة الموقّعة على الوثيقة (C_{DS}) داخل المادة الأمنية للوثيقة (SO_D). وينبغي أن تتوقع أن شهادة الجهة الموقّعة على الوثيقة (C_{DS}) المنشورة في دليل المفاتيح العامة سيتم أيضاً تعميمها على المحطات الحدودية في غضون ٤٨ ساعةً.

ولا ترد شهادات الجهة الموقّعة على رمز الأعمدة في الختم الرقمي نفسه. وبالتالي **يجب** على البلد الذي يصدر وثائق محمية بأختام رقمية أن ينشر شهادات الجهة الموقعة على رمز الأعمدة الخاصة به. وقناة التوزيع الأولية لشهادات الجهة الموقعة على رمز الأعمدة هي دليل المفاتيح العامة الثنائي. ما بالنسبة للآليات الأخرى، مثل النشر على موقع شبكي، فهي قنوات ثانوية.

للجهات الموقعة على رمز الأعمدة، **يجب** أن يتقيد النشر بالمبدأين التاليين:

- حالما يتم إنشاء شهادة جديدة، **يجب** تعميمها بتأخير لا يزيد على ٤٨ ساعة؛
- و**يجب** أن تبقى الشهادة منشورة إلى حين انتهاء صلاحيتها أو إلغائها.

ينبغي أن تبذل دول القبول كل محاولة سواءً الكترونياً أو بوسيلة أخرى للعمل وفقاً لقوائم إلغاء الشهادات، بما في ذلك تلك القوائم بإلغاء الشهادات الصادرة في ظروف استثنائية.

يُضمن النشر في الوقت المناسب لشهادات الموقّع على القائمة الرئيسية عن طريق إدراجها في كل قائمةٍ رئيسيةٍ.

٥-١ آلية توزيع دليل المفاتيح العامة

تُقدّم الإيكاو دليل خدمة دليل المفاتيح العامة (PKD). و**يجب** أن تقبل هذه الخدمة مواد دليل المفاتيح العامة، بما في ذلك الشهادات وقوائم إلغاء الشهادات والقوائم الرئيسية، من المشاركين في دليل المفاتيح العامة، وتخزنها في دليل وتجعلها متاحةً لجميع دول القبول.

لا تُخزَّن شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات (CCSCA) فردياً كجزء من خدمة دليل المفاتيح العامة للإيكاو. غير أنها قد تكون موجودة في دليل المفاتيح العامة إذا كانت القوائم الرئيسية تحتوي عليها.

تظل كل شهادة في دليل المفاتيح العامة حتى تنقضي فترة صلاحية شهادتها، بصرف النظر عمّا إذا كان أم لم يكن المفتاح الخاص المناظر لا يزال مستخدماً.

الشهادات وقوائم إلغاء الشهادات والقوائم الرئيسية المخزنة في دليل المفاتيح العامة بواسطة جميع المشاركين في دليل المفاتيح العامة **يجب** إتاحتها لجميع الأطراف (شاملة غير المشاركين في دليل المفاتيح العامة) التي تحتاج إلى هذه المعلومات للمصادقة على صحة وسلامة بيانات وثيقة السفر الالكترونية المقروءة آلياً المخزنة رقمياً. مواد البنية LDS2 ومواد الأختام الرقمية المرئية.

٥-١-١ تحميل دليل المفاتيح العامة

يجوز للمشاركين في دليل المفاتيح العامة فقط تحميل الشهادات وقوائم إلغاء الشهادات والقوائم الرئيسية على دليل المفاتيح العامة. و**يجب** أن تمتثل جميع الشهادات وقوائم إلغاء الشهادات للأوصاف الموجزة الواردة في القسم ٧. و**يجب** أن تمتثل جميع القوائم الرئيسية للمواصفات الواردة في القسم ٩.

يتكون دليل المفاتيح العامة من "دليل للكتابة" و"دليل للقراءة". و**يجب** على المشاركين في دليل المفاتيح العامة استخدام Lightweight Directory Access Protocol (LDAP) (بروتوكول الاطلاع على الدليل الخفيف الوزن) لتحميل موادهم على دليل الكتابة. وبمجرد أن يتم التحقق من التوقيع الرقمي على مادة، وإكمال عمليات التدقيق الأخرى التي تقتضيها العناية الواجبة، تُنشر المادة في دليل القراءة.

٥-١-٢ تنزيل دليل المفاتيح العامة

الاطلاع بالقراءة على جميع الشهادات وقوائم إلغاء الشهادات والقوائم الرئيسية المنشورة في دليل المفاتيح العامة **يجب** أن يكون متاحاً للمشتركين في دليل المفاتيح العامة وغير المشتركين. و**يجب ألا** تنفذ مراقبة الاطلاع بالنسبة للاطلاع بالقراءة على دليل المفاتيح العامة.

تقع على عاتق دولة القبول المسؤولية عن توزيع المواد المنزّلة من دليل المفاتيح العامة على نظمها للتفتيش والاحتفاظ بذاكرةٍ مخبئةٍ لقائمة إلغاء الشهادات جارية إلى جانب الشهادات اللازمة للتحقق من التوقيعات على بيانات وثيقة السفر الالكترونية المقروءة آلياً.

٥-٢ آلية توزيع التبادل الثنائي

بالنسبة لقوائم إلغاء الشهادات وشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات (CCSCA)، فإن قناة التوزيع الاولية هي التبادل الثنائي بين دول أو منظمات الإصدار ودول القبول. ويمكن أيضاً استخدام التبادل الثنائي لتوزيع القوائم الرئيسية.

قد تتفاوت التكنولوجيا المحدّدة المستخدمة لذلك التبادل الثنائي على نحو يتوقف على سياسات كل دولة أو منظمة إصدار تحتاج إلى توزيع شهاداتها وقوائمها لإلغاء الشهادات وقوائمها الرئيسية، فضلاً عن سياسات كل دولة قبول تحتاج إلى الاطلاع على تلك المواد. وبعض أمثلة التكنولوجيات التي قد تُستخدم في التبادل الثنائي تشمل ما يلي:

- البريد الدبلوماسي / الحقيبة الدبلوماسية،
- وتبادل البريد الالكتروني،
- وتنزيل من موقع الكتروني مرتبط بالسلطة الوطنية المعنية بالتوقيع على الشهادات التي قامت بالإصدار،
- والتنزيل من مزود لبروتوكول الاطلاع على الدليل الخفيف الوزن مرتبط بالسلطة الوطنية المعنية بالتوقيع على الشهادات التي قامت بالإصدار.

هذه ليست قائمة شاملة وقد تُستخدم أيضاً تكنولوجيات أخرى.

٥-٣ آلية توزيع القائمة الرئيسية

القوائم الرئيسية هي تكنولوجيا داعمة لخطة التوزيع الثنائي. وتوزيع شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات عن طريق قوائم رئيسية بصفته هذه هو فرع من خطة التوزيع الثنائي.

القائمة الرئيسية هي قائمة موقعة رقمياً بشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات التي "تثق فيها" دولة أو منظمة القبول التي أصدرت القائمة الرئيسية. ويجوز أن تُدرج في قائمة رئيسية الشهادات الجذرية الموقّعة ذاتياً بواسطة السلطة الوطنية المعنية بالتوقيع على الشهادات وشهادات الربط الصادرة عن السلطة الوطنية المعنية بالتوقيع على الشهادات. وبنية وشكل القائمة الرئيسية معرفان في القسم ٨. ونشر قائمة رئيسية يمكّن دول أو منظمات القبول الأخرى من الحصول على مجموعة من شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات من مصدر منفرد (هيئة إصدار القائمة الرئيسية) بدلاً عن انشاء اتفاق تبادل ثنائي مباشر مع كلٍّ من سلطات أو منظمات الإصدار الممثلة على تلك القائمة.

أي موقّع على قائمة رئيسية مصرَّح له من السلطة الوطنية المعنية بالتوقيع على الشهادات بتأليف القوائم الرئيسية والتوقيع عليها رقمياً وإصدارها. والقوائم الرئيسية **يجب** ألا تقوم السلطة الوطنية المعنية بالتوقيع على الشهادات بالتوقيع عليها وإصدارها بنفسها مباشرةً. و**يجب** أن تمتثل الشهادات الموقّعة على القائمة الرئيسية لمظهر الشهادة المعرّف في القسم ٧.

قبل أن يُصدر الموقّع على القائمة الرئيسية القائم بالإصدار قائمةً رئيسيةً **ينبغي** أن يقوم على نطاق واسع بالمصادقة على شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات المراد التصديق على توقيعها، بما في ذلك ضمان أن الشهادات تملكها حقاً السلطات الوطنية المعنية بالتوقيع على الشهادات التي تمّ تحديدها. و**ينبغي** للاجراءات المستخدمة لهذه المصادقة خارج النطاق أن تُعكس في سياسات الشهادات المنشورة للسلطة الوطنية المعنية بالتوقيع على الشهادات التي أصدرت شهادة الموقّع على القائمة الرئيسية.

يجب أن تحتوي كل قائمة رئيسية على شهادة الموقّع على القائمة الرئيسية التي ستستخدم للتحقق من التوقيع على القائمة الرئيسية فضلاً عن شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات للسلطة المذكورة التي أصدرت شهادة الموقّع على القائمة الرئيسية.

إذا تسلمت دولة القبول شهادات جديدة للسلطة الوطنية المعنية بالتوقيع على الشهادات، وتمّ إكمال إجراءات المصادقة عليها، **يوصى** بتحرير قائمة رئيسية جديدة وإصدارها.

استخدام قائمة رئيسية لا يُتيح التوزيع بمزيد من الكفاءة لشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات بالنسبة لبعض دول القبول. غير أن أي دولة قبول تستفيد من قوائم رئيسية لا يزال **يجب** عليها أن تحدّد سياساتها الخاصة لإنشاء الثقة في الشهادات التي تحتوي عليها تلك القائمة (انظر القسم ٦ للاطلاع على التفاصيل).

٦- ائتمان البنية الأساسية للمفاتيح العامة والمصادقة عليها

يختلف ائتمان البنية الأساسية للمفاتيح العامة والمصادقة عليها بين البنية الأساسية للمفاتيح العامة لوثائق السفر الإلكترونية المقروءة آلياً والبنية الأساسية للمفاتيح العامة للتراخيص.

٦-١ البنية الأساسية للمفاتيح العامة لوثائق السفر الإلكترونية المقروءة آلياً

في بيئة البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً، تقوم نظم التفتيش في دول القبول بدور الأطراف المعولة على البنية الأساسية للمفاتيح العامة. هو التحقق بنجاح من صحة التوقيع الرقمي على المادة الأمنية لوثيقة سفر الكترونية مقروءة آلياً يضمن صحة وسلامة البيانات المخزنة في الدائرة المتكاملة اللا تلامسية لتلك الوثيقة الالكترونية للسفر المقروءة آلياً. وتلك العملية للتحقق من التوقيع تتطلب أن يثبت الطرف المعوّل أن المفتاح العام للجهة الموقّعة على الوثيقة المستخدم للتحقق من التوقيع هو ذاته "مؤتمنٌ".

تتيح آليات التوزيع المختلفة المعرَّفة في القسم ٥ لدول القبول الاطلاع على اجتهادات وقوائم إلغاء الشهادات التي تحتاج إليها للتحقق من التوقيعات الرقمية المعنية. غير أن هذه الخطط للتوزيع لا تُنشئ ائتمان تلك الشهادات أو قوائم إلغاء الشهادات أو المفاتيح العامة التي ستستخدم للتحقق من التوقيعات على تلك الشهادات وقوائم إلغاء الشهادات.

المفاتيح العامة التي تحتوي عليها شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات (C_{CSCA}) تُستخدم للتحقق من التوقيعات الرقمية على الشهادات وقوائم إلغاء الشهادات. ولذلك، لقبول وثيقة سفر الكترونية مقروءة آلياً من دولة إصدار أخرى، **يجب** أن تكون دولة القبول قد وضعت بالفعل في مخزن ائتمان بشكل ما، يستطيع نظامها لمراقبة الحدود الوصول إليه، نسخة مؤتمنة من شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات (C_{CSCA}) لدولة أو منظمة الإصدار، أو شكل آخر من معلومات مرتكز الإئتمان للمفتاح العام لتلك السلطة الوطنية المعنية بالتوقيع على الشهادات كما هو مستمد من الشهادة.

تقع على عاتق دولة القبول المسؤولية عن انشاء ائتمان في شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات (C_{CSCA}) وتخزين الشهادات (أو المعلومات من الشهادات) كمرتكزات للائتمان، بطريقة مأمونة لكي تستخدمها نظمها للتفتيش على الحدود.

٦-١-١ *إدارة مرتكز الإئتمان*

حسبما تم تحديده في [RFC 5280] يجب إنشاء مرتكز ائتمان يمكن استخدامه كمرتكز لاجراءات المصادقة على جهة معينة موقعة على الوثيقة أو الموقّع على القائمة الرئيسية أو الموقّع على قائمة الانحرافات أو شهادة من نوع آخر.

يتألف كل مرتكز ائتمان من مفتاح عام مؤتمن وأساسيات المعلومات المرتبطة به. و**يجب** أن تتضمن مرتكزات الإئتمان، كحدٍ أدنى ما يلي:

- المفتاح العام المؤتمن وأي أساسيات معلومات موتبطة بالمفتاح.
- خوارزمية المفتاح العام.
- اسم مالك المفتاح.
- قيمة امتداد `SubjectAltName` لشهادة السلطة الوطنية المعنية بالتوقيع على الشهادات التي تحتوي على الرمز ثلاثي الأحرف الذي خصصته الإيكاو لسلطة أو منظمة الإصدار. وعلى الرغم من أن هذا لا يستخدم في مسار الترخيص أو إجراءات المصادقة على قائمة إلغاء الشهادات، فهو يُستخدم في التحقق السلبي من الصحة المعرّف في الوثيقة Doc 9303-11.

في تطبيق وثيقة السفر الالكترونية المقروءة آلياً، يُنشأ مرتكز ائتمان منفصل لكل مفتاح عام لسلطة وطنية معينةٍ معنيةٍ بالتوقيع على الشهادات. وبالنسبة للمفتاح العام الأول الذي يتم الحصول عليه من سلطة وطنية معنية بالتوقيع على الشهادات، **يجب** إنشاء الائتمان من خلال آليةٍ خارج النطاق. ومثلاً، إذا تم تنزيل شهادة سلطة وطنية معنية بالتوقيع على الشهادات من مزوّد مرتبط بالسلطة الوطنية المعنية بالتوقيع على الشهادات، يمكن استخدام اتصال خارج النطاق (مثل الهاتف أو البريد الالكتروني) للتحقق من أن شهادة التنزيل هي في الواقع شهادة صحيحة لتلك السلطة الوطنية المعنية بالتوقيع على الشهادات. وكذلك، قد يجوز للطرف المعتَمِد أن يُحلّل سياسات السلطة الوطنية المعنية بالتوقيع على الشهادات التي قامت بالإصدار وإجراءاتها وممارساتها لتقرير ما إذا كانت مأمونة بقدرٍ كافٍ للوفاء بالمتطلبات المحلية لاستخدام الشهادات. وبمجرد إنشاء مرتكز ائتمان أولي لسلطةٍ وطنيةٍ معينةٍ معنية بالتوقيع على الشهادات، يمكن تبسيط العملية للمفاتيح التالية لتلك السلطة الوطنية نفسها. وإذا أصدرت السلطة الوطنية المعنية بالتوقيع على الشهادات شهادة ارتباط بسلطة وطنية معنية بالتوقيع على الشهادات، يمكن عندئذٍ إغفال إجراء اتصال خارج النطاق بالسلطة الوطنية المعنية بالتوقيع على الشهادات للتحقق من صحة الشهادة الجديدة لأنه يُستخدم بالفعل مفتاح عام مؤتمن لتلك السلطة الوطنية المعنية بالتوقيع على الشهادات نفسها للتحقق من صحة التوقيع على تلك الشهادة للارتباط بالسلطة الوطنية المعنية بالتوقيع على الشهادات.

يجوز تخزين معلومات مرتكز الائتمان كنسخة مؤتمنة من شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات نفسها، أو في شكل مؤتمن آخر ما.

لأن التوقيعات على الشهادات الصادرة عن سلطات وطنية معنية بالتوقيع على الشهادات في حاجة للتحقق من صحتها بعد قيام تلك السلطة الوطنية بتحديث زوجها من المفاتيح بوقتٍ طويل، فعادةً ما سيكون لدى أي دولة قبول أكثر من مرتكز ائتمان واحد لنفس السلطة الوطنية المعنية بالتوقيع على الشهادات في أي وقت معين. وإذا خضعت السلطة الوطنية المعنية بالتوقيع على الشهادات لتغيير اسمٍ، فإن بعض هذه المرتكزات للائتمان ستحتوي على اسم السلطة الوطنية القديمة المعنية بالتوقيع على الشهادات وستحتوي الأخريات على الاسم الجديد.

٦-١-٢ *الفحص للمصادقة على الشهادة / قائمة إلغاء الشهادات والإلغاء*

كجزءٍ من عملية التحقق من صحة وسلامة مواد البيانات في تطبيق وثيقة السفر الالكترونية المقروءة آلياً (مثل المواد الأمنية للوثيقة والقوائم الرئيسية وقوائم الانحرافات، أ ل خ.)، تقوم أي دولة قبول بما يلي:

- المصادقة على الشهادة المستخدمة للتحقق من صحة التوقيع على مادة البيانات (مثل شهادة الجهة الموقعة على الوثيقة، شهادة الموقع على القائمة الرئيسية، شهادة الموقع على قائمة الانحرافات)،
- المصادقة على قائمة إلغاء الشهادات المستخدمة لفحص وضع إلغاء الشهادة المعنية،
- معالجة قائمة إلغاء الشهادات للتحقق من وضع إلغاء الشهادة المعنية.

تتوافر عينات خوارزميات لهذه العمليات، مثل تلك المحدد في [RFC 5280]. ولا تحتاج دول القبول لتنفيذ الخوارزمية المحددة المعرّفة في RFC 5280، لكن **يجب** أن توفّر تشغيلاً مساوياً للسلوك الخارجي الناتج عن هذه الإجراءات. ويجوز استخدام أي خوارزمية عن طريق تنفيذ خاص طالما تستخلص النتيجة الصحيحة.

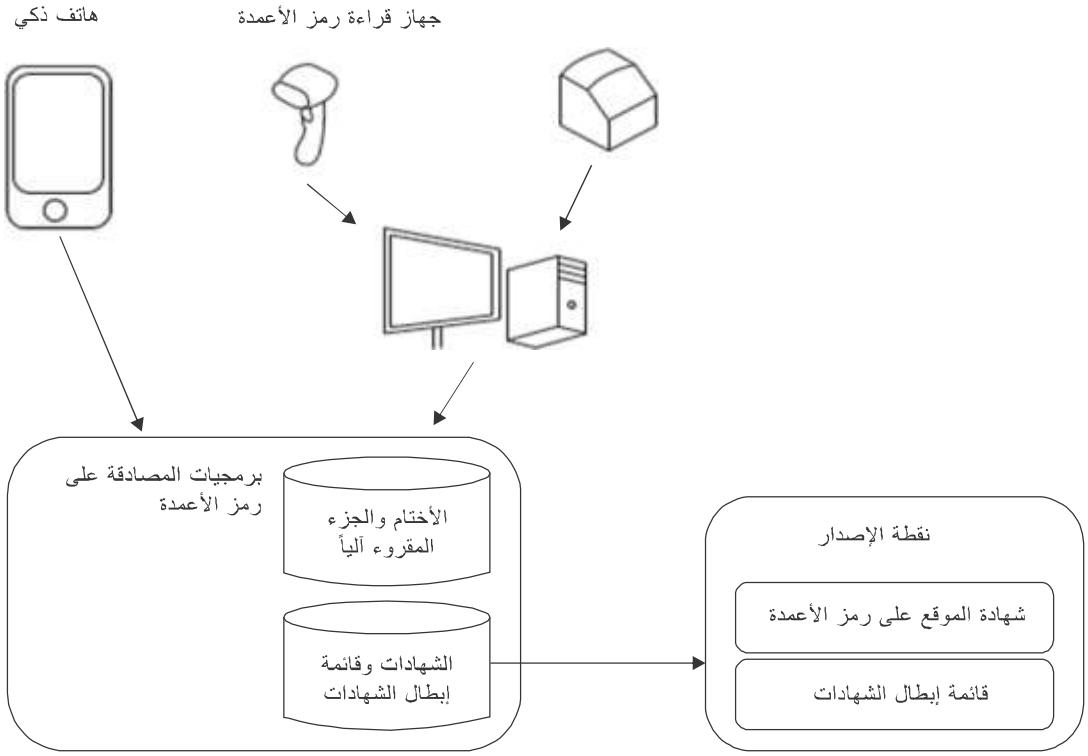
يقدم المرفق (د) ارشادات لدول القبول التي تختار اسناد خوارزميتها إلى تلك المحددة في [RFC 5280].

٦-١-٣ *سلطة المصادقة على رمز الأعمدة*

تقوم سلطة المصادقة على رمز الأعمدة بالمصادقة على ختم رقمي عن طريق تطبيق سياسة المصادقة. وتحدد الوثيق Dov 9303-13 بالتفصيل معايير وخوارزميات المصادقة من أجل توليد حالة مصادقة.

ويوضح الشكل ٤ الهيكلية الوظيفية لسلطة المصادقة على رمز الاعمدة. وتعتمد سلطة المصادقة على رمز الأعمدة على برمجيات المصادقة التي يمكن تشرها على أي حاسوب تستخدمه سلطات مراقبة الحدود.

تكون برمجيات المصادقة متصلة بجهاز قراءة يأخذ صورة لرمز الأعمدة لاستعادة رمز الأعمدة والجزء المقروء آلياً من الوثيقة، وأيضاً صورة للوثيقة لاستعادة جزئها المقروء آلياً. وللتحقق من صلاحية توقيع الختم الرقمي، **ينبغي** أن تكون برمجيات المصادقة متزامنة مع نقطة نشر البنية الأساسية للمفاتيح العامة كل ٢٤ ساعة على الأقل لاستعادة الشهادات الأخيرة للجهة الموقعة على رمز الأعمدة وقوائم إلغاء الشهادات.



الشكل ٤ — المصادقة على رمز الأعمدة

تقوم برمجيات المصادقة على رمز الأعمدة بترميز الختم الرقمي والأجزاء المقروءة آلياً لأي وثائق مرتبطة بها (مثلاً التأشيرة أو الجواز)، والمصادقة على توقيع الختم الرقمي، وتطبيق سياسة المصادقة (راجع الوثيقة Doc 9303-13) من أجل توليد حالة مصادقة على الوثيقة.

في سيناريوهات الأجهزة المتنقلة، يمكن أيضاً تنفيذ برمجيات المصادقة على هاتف ذكي. وبينما يمكن التحقق من صلاحية الختم بواسطة البرمجيات على الهاتف الذكي، **يجب** أن تتم المقارنة بين البيانات (الموقّعة) الموجودة داخل الختم والأجزاء المقروءة آلياً المطبوعة (مثل التأشيرة أو الجواز) إما يدوياً أو بواسطة القراءة بالمسح الضوئي للأجزاء المقروءة إلكترونياً خارج الصورة الملتقطة، حيث تعتبر الطريقة الأخيرة غالباً من أصعب المشاكل عملياً.

تعالج البيانات التالية بواسطة برمجيات المصادقة على رمز الأعمدة.

- بيانات الدخل التي توفرها أجهزة القراءة، مثل صور التأشيرات أو الجوازات؛
- والشهادات وقوائم إلغاء الشهادات.

٦-٢ البنية الأساسية للمفاتيح العامة للتراخيص

بالنسبة للبنية الأساسية للمفاتيح العامة للتراخيص، يتم التعامل مع مرتكز الثقة والمصادقة بشكل مختلف.

٦-٢-١ المصادقة على الشهادات التي يتم التحقق منها بالبطاقة

بالنسبة لشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية في البنية الأساسية للمفاتيح العامة للتراخيص، يكون مرتكز الثقة هو أحدث مفتاح عام للسلطة الوطنية للتحقق من الشهادات في الدولة التي أصدرت وثيقة السفر الإلكترونية المقروءة آلياً. و**يجب** أن يكون مرتكز الثقة الأولي مخزناً بطريقة آمنة في الدائرة المتكاملة اللا تلامسية لوثيقة السفر الإلكترونية المقروءة آلياً في مرحلة الإنتاج أو (ما قبل) إدخال المواصفات الشخصية. وبما أن زوج المفاتيح الذي تستعمله السلطة الوطنية للتحقق من الشهادات يتغير مع الوقت، تكون شهادات الربط بالسلطة الوطنية للتحقق من الشهادات منتجة. و**يجب** أن تقوم الدائرة المتكاملة اللا تلامسية لوثيقة السفر الإلكترونية المقروءة آلياً بتحديث مرتكز (مرتكزات) الثقة الخاص (الخاصة) بها داخلياً وفقاً لشهادات الربط الصالحة الواردة. ونظراً لبرمجة شهادات الربط بالسلطة الوطنية للتحقق من الشهادات، سوف تخزن مرتكزات الثقة على الدائرة المتكاملة اللا تلامسية في أي وقت من الأوقات.

وللمصادقة على شهادة وحدة طرفية، **يجب** أن تزود الدائرة المتكاملة اللا تلامسية لوثيقة السفر الإلكترونية المقروءة آلياً بسلسلة شهادات تبدأ في مرتكز الثقة المخزن على الدائرة المتكاملة اللا تلامسية لوثيقة السفر الإلكترونية المقروءة آلياً.

يكون إجراء المصادقة على شهادات المتحقق من الوثائق وشهادات الوحدة الطرفية خاصاً ببروتوكول التحقق من صحة البنية LDS2 ويحدد في الوثيقة Doc 9303-11).

٧- الأوصاف الموجزة للشهادة وقائمة إلغاء الشهادات

يرد تعريف الأوصاف الموجزة للشهادات لكل **من** البنية الأساسية للمفاتيح العامة لوثائق السفر الإلكترونية المقروءة آلياً والبنية الأساسية للمفاتيح العامة للتراخيص.

٧-١ البنية الأساسية للمفاتيح العامة لوثائق السفر الإلكترونية المقروءة آلياً

يجب على دول أو منظمات الإصدار إصدار شهادات وقوائم إلغاء شهادات تتفق مع الأوصاف الموجزة المحددة أدناه. و**يجب** انتاج جميع الشهادات وقوائم إلغاء الشهادات في شكل قاعدة التشفير المميز (DER) للحفاظ على سلامة التوقيعات داخلها. والأوصاف الموجزة لشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات والجهة الموقّعة على الوثيقة التي أُدرِجَت في الطبعة السادسة من هذه المواصفات تختلف في بعض المجالات عن الأوصاف الموجزة الحالية. و**يجب** أن تكون نظم التفتيش قادرة على معالجة الشهادات التي أُصدرت وفقاً لتلك الأوصاف الموجزة السابقة (انظر المرفق (ج)) وكذلك الأوصاف الموجزة الحالية.

تستند هذه الأوصاف الموجزة إلى اقتضاء أنه **يجب** أن تُنشئ كل دولة أو منظمة إصدار سلطةً وطنيةً واحدةً معنيةً بالتوقيع على الشهادات لغرض التوقيع على جميع وثائق السفر الالكترونية المقروءة آلياً الممتثلة للوثيقة Doc 9303.

الأوصاف الموجزة للشهادات معرّفة في هذا القسم لأنواع الشهادات التالية:

- سلطة إصدار الترخيص الموقّعة للبلد،
- الجهة الموقّعة على الوثيقة،
- الموقّع على القائمة الرئيسية للسلطة الوطنية المعنية بالتوقيع على الشهادات،
- الموقّع على قائمة الانحرافات،
- والاتصالات– على الرغم من أنها ليست هناك حاجة ماسة إليها اليوم. وهذه هي خطوة للاثبات في المستقبل. ويجوز استخدام هذه الشهادات للاطلاع على دليل المفاتيح العامة أو الاتصالات بروتوكول الاطلاع على الدليل الخفيف الوزن LDAP/EMAIL/HTTP بين الدول. ويُوصى بأن تُصدر هذه الشهادات السلطة الوطنية المعنية بالتوقيع على الشهادات.

سلطة إصدار الترخيص الموقّعة للبلد والجهة الموقّعة على الوثيقة والجهة الموقّعة على قائمة الانحرافات والجهة الموقّعة على القائمة الرئيسية للسلطة الوطنية المعنية بالتوقيع على الشهادات موادها معرّفة في القسم ٣.

الوصف الموجز لقائمة إلغاء الشهادات معّرف في القسم ٧-١-٤.

تستخدم الاوصاف الموجزة المصطلحات التالية لمتطلبات وجود كلٍّ من المكونات / الامتدادات التالية:

m إلزامي – **يجب** أن تكون الخانة موجودةً،
x لا تستخدمها – **يجب ألّا** تكون الخانة موجودةً،
o اختياري – **يجوز** أن تكون الخانة موجودةً.
C مشروط – **يجب** أن تكون الخانة موجودة في ظروف معينة.

تستخدم الأوصاف الموجزة المصطلحات التالية للمتطلبات الحرجة لامتداداتٍ يجوز / يجب تضمينها:

c حرجة – **يجب** أن تكون تطبيقات القبول قادرة على معالجة هذا الامتداد،
nc غير حرجة – تطبيقات القبول التي لا تفهم هذا الامتداد **يجوز** أن تتجاهله.

بعض المتطلبات المحددة في هذه الأوصاف الموجزة موروثةٌ على الأوصاف الموجزة الأساسية المعزّزة بالمراجع (مثل RFC 5280). وتوخياً للتسهيل، فإن النص المعني من الأوصاف الموجزة الأساسية التي تغطي المطلب المحدد مزدوجة في الجدول في المرفق (ب).

٧-١-١ *الأوصاف الموجزة للشهادات*

يحدد الجدول ٥ متطلبات الأوصاف الموجزة المشتركة لجميع الشهادات بالنسبة لخانات متن الشهادة. ويحدد الجدول ٦ المتطلبات بالنسبة لامتدادات الشهادة.

الجدول ٥ — الوصف الموجز لخانات الشهادة

Certificate Component	*Presence*	*Comments*
`Certificate`	m	
`TBSCertificate`	m	See Table 6
`signatureAlgorithm`	m	Value inserted here dependent on algorithm selected
`signatureValue`	m	Value inserted here dependent on algorithm selected
`TBSCertificate`		
`version`	m	MUST be `v3`
`serialNumber`	m	MUST be positive integer and maximum 20 Octets MUST use 2's complement encoding and be represented in the smallest number of octets
`signature`	m	Value inserted here MUST be the same as that in `signatureAlgorithm` component of `Certificate` sequence

Certificate Component	*Presence*	*Comments*
issuer	m	countryName and serialNumber, if present, MUST be PrintableString Other attributes that have DirectoryString syntax MUST be either PrintableString or UTF8String countryName MUST be Upper Case See 7.1.1 for naming conventions
validity	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in UTCTime UTCTime MUST be represented as YYMMDDHHMMSSZ Dates in 2050 and beyond MUST be in GeneralizedTime. GeneralizedTime MUST NOT have fractional seconds GeneralizedTime MUST be represented as YYYYMMDDHHMMSSZ
subject	m	countryName and serialNumber, if present, MUST be PrintableString Other attributes that have DirectoryString syntax MUST be either PrintableString or UTF8String countryName MUST be Upper Case countryName in issuer and subject fields MUST match See 7.1.1.1 for naming conventions
subjectPublicKeyInfo	m	
issuerUniqueID	x	
subjectUniqueID	x	
extensions	m	See Table 6 on which extensions should be present Default values for extensions MUST NOT be encoded

الجدول ٦ — الوصف الموجز لامتدادات الشهادة

Extension name	*CSCA Self-Signed Root*		*CSCA Link*		*Document Signer*		*Master List Signer and Deviation List Signer*		*Communication*		*Comments*
	Presence	*Criticality*	*Presence*	*Criticality*	*Presence*	*Criticality*	*Presence*	*Criticality*	*Presence*	*Criticality*	
AuthorityKeyIdentifier	**o**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	
keyIdentifier	m		m		m		m		m		
authorityCertIssuer	o		o		o		o		o		
authorityCertSerialNumber	o		o		o		o		o		
SubjectKeyIdentifier	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
subjectKeyIdentifier	m		m		m		m		m		
KeyUsage	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	
digitalSignature	x		x		m		m		o		Some communication certificates (e.g. TLS certificates) require that the keyUsage bits be set in accordance with the particular cipher suite used. Some cipher suites do, and some do not require the digitalSignature bit to be set.
nonRepudiation	x		x		x		x		x		
keyEncipherment	x		x		x		x		o		
dataEncipherment	x		x		x		x		x		
keyAgreement	x		x		x		x		o		
keyCertSign	m		m		x		x		x		
cRLSign	m		m		x		x		x		
encipherOnly	x		x		x		x		x		
decipherOnly	x		x		x		x		x		
PrivateKeyUsagePeriod	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	
notBefore	o		o		o		o		o		At least one of notBefore or notAfter MUST be present
notAfter	o		o		o		o		o		MUST be encoded as generalizedTime
CertificatePolicies	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
PolicyInformation	m		m		m		m		m		
policyIdentifier	m		m		m		m		m		
policyQualifiers	o		o		o		o		o		

Extension name	*CSCA Self-Signed Root*		*CSCA Link*		*Document Signer*		*Master List Signer and Deviation List Signer*		*Communication*		*Comments*
PolicyMappings	**x**		**x**		**x**		**x**		**x**		See Note 1
SubjectAltName	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	See 7.1.2
IssuerAltName	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	See 7.1.2
SubjectDirectoryAttributes	**x**		**x**		**x**		**x**		**x**		
Basic Constraints	**m**	**c**	**m**	**c**	**x**		**x**		**x**		
cA	m		m		x		x		x		
PathLenConstraint	m		m		x		x		x		MUST always be '0'
NameConstraints	**x**		**x**		**x**		**x**		**x**		See Note 1
PolicyConstraints	**x**		**x**		**x**		**x**		**x**		See Note 1
ExtKeyUsage	**x**		**x**		**x**		**m**	**c**	**m**	**c**	See 7.1.3
CRLDistributionPoints	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	
distributionPoint	m		m		m		m		m		MUST be ldap, http or https See 7.1.4
reasons	x		x		x		x		x		
cRLIssuer	x		x		x		x		x		
InhibitAnyPolicy	**x**		**x**		**x**		**x**		**x**		See Note 1
FreshestCRL	**x**		**x**		**x**		**x**		**x**		See Note 2
privateInternetExtensions	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	See Note 3
NameChange	**o**	**nc**	**o**	**nc**	**x**		**x**		**x**		See 7.1.1.5
DocumentType	**x**		**x**		**m**	**nc**	**x**		**x**		See 7.1.1.6
Netscape Certificate Type	**x**		**x**		**x**		**x**		**x**		See Note 4
other private extensions	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	

ملاحظة ١ — يمكن أن يرد الامتداد، بحكم تعريفه، فقط في شهادات سلطة إصدار الترخيص المتوسطة (الشهادات التي أصدرتها سلطة إصدار ترخيص واحدة إلى سلطة إصدار ترخيص أخرى). ولا تُستخدم شهادات سلطة إصدار الترخيص المتوسطة في البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً. ولذلك فإن هذا الامتداد يُمنع من شهادات وثيقة السفر الالكترونية المقروءة آلياً.

ملاحظة ٢ — يُستخدم أحدث امتداد لقائمة إلغاء الشهادات للإشارة إلى قائمة إلغاء الشهادات دلتا. وقوائم إلغاء الشهادات دلتا غير مدعومة في البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً. ولذلك فإن هذا الامتداد ممنوعٌ.

ملاحظة ٣ — يوجد امتدادان خاصان للانترنت (الاطلاع على معلومات السلطة والاطلاع على معلومات الموضوع) معرّفان في RFC 5280 يُستخدمان للاشارة إلى المعلومات عن هيئة الإصدار أو موضوع شهادة. وهذان الامتدادان غير مطلوبين في البنية الأساسية للمفاتيح العامة لوثيقة السفر الالكترونية المقروءة آلياً. غير أنه نظراً لأنهما لا يؤثران على القابلية للتشغيل البيني، وهما غير حرجين، فيجوز اختيارياً إدراجهما في شهادات وثائق السفر الالكترونية المقروءة آلياً.

ملاحظة ٤ — يمكن استخدام امتداد نتسكيب (Netscape) من نوع الشهادة للحدّ من الأغراض التي يمكن أن تُستخدم فيها شهادة. والامتدادان `extKeyUsage and basicConstraints` *هما الآن الامتدادان القياسيان لتلك الأغراض ويُستخدمان في تطبيق وثيقة السفر الالكترونية المقروءة آلياً. وبسبب التضارب المحتمل بين القيم في الامتدادات القياسية وفي امتداد نتسكيب (Netscape) الخاضع للملكية، فإن امتداد نتسكيب (Netscape) محظورّ.*

٧-١-١-١ متطلبات هيئة الإصدار وخانة الموضوع

تكون خانة هيئة الإصدار وخانة الموضوع مشتركتين بين جميع الشهادات، علماً بأن هناك قيوداً محددة تطبق على شهادات الجهة الموقعة على البنية LDS2.

٧-١-١-١-١ المتطلبات العامة

التقاليد التالية للتسمية والعنونة لخانتي هيئة الإصدار والموضوع **مطلوبةٌ**.

- الخانة `countryName` **يجب** أن تكون موجودةً. وتحتوي القيمة على رمز بلد **يجب** أن يتبع شكل حرفي رمزي البلد، المحددين في الوثيقة Doc 9303-3.
- الخانة `commonName` **يجب** أن تكون موجودةً.

يجوز أيضاً إدراج سمات أخرى حسب تقدير دولة أو منظمة الإصدار.

٧-١-١-١-٢ متطلبات شهادات الجهة الموقّعة على البنية LDS2

يجب على شهادات الجهة الموقّعة على البنية LDS2 أن تمتثل للوصف الموجز لشهادة الجهة الموقّعة على الوثائق المعرّفة أعلاه باستثناء ما هو محدد في ٧-١-٢.

٧-١-١-٢ متطلبات هيئة الإصدار والاسم البديل للموضوع

لأن الوظائف التي تخدمها الأسماء البديلة في تطبيق وثيقة السفر الالكترونية المقروءة آلياً محددة لهذا التطبيق ومختلفة عن تلك المحددة من أجل البنية الأساسية للمفاتيح العامة للانترنت في [RFC 5280]، فإن القيم في امتداد الاسم البديل لموضوع شهادات وثائق السفر الالكترونية المقروءة آلياً لا تحدد عموماً بشكلٍ لا لبس فيه موضوع الشهادة.

في تطبيق وثيقة السفر الالكترونية المقروءة آلياً، تخدم الأسماء البديلة الوظيفتين التاليتين.

الوظيفة الأولى هي تقديم معلومات اتصال من أجل الموضوع و / أو هيئة إصدار الشهادة. ولذلك الغرض **ينبغي** أن تتضمن على الأقل واحداً مما يلي:

- `rfc822Name`،
- `dNSName`،
- `uniformResourceIdentifier`.

الوظيفة الثانية هي توفير سلسلة دالّة من الرموز التي خصصتها الإيكاو للبلدان. ولهذا الغرض فإن الشهادات المصدرة باستخدام هذا الشكل **يجب** أن تتضمن فضلاً عن ذلك اسماً دالّاً مكوناً على النحو التالي:

- `localityName` يحتوي على رمز الإيكاو للبلد كما يظهر في الجزء المقروء آلياً،
- إذا كان هذا الرمز للبلد لا يعرِّف على نحوٍ فريد دولة أو منظمة الإصدار، **يجب** استخدام الصفة `stateOrProvinceName` للدلالة على الرمز ثلاثي الأحرف الذي خصصته الإيكاو لدولة أو منظمة الإصدار.

- الصفات الأخرى غير مسموح بها.

في الشهادات الأصلية الموقّعة ذاتياً من السلطة الوطنية المعنية بالتوقيع على الشهادات، **يجب** أن يكون الامتدادان IssuerAltName وSubjectAltName متطابقين.

في شهادات الربط الصادرة عن السلطة الوطنية المعنية بالتوقيع على الشهادات، **قد** تختلف القيم. ومثلاً، إذا حدث تغيير عن طريق rfc822Name للسلطة الوطنية المعنية بالتوقيع على الشهادات مباشرةً قبل إصدار شهادة ربط عن السلطة الوطنية المعنية بالتوقيع على الشهادات، سيتضمن الامتداد IssuerAltName rfc822Name القديم وسيتضمن الامتداد SubjectAltName الصيغة الجديدة rfc822Name. وأي شهادات ربط لاحقة صادرة عن السلطة الوطنية المعنية بالتوقيع على الشهادات ستحتوي على الصيغة الجديدة rfc822Name في كلا الامتدادين.

٧-١-١-٣ *متطلبات تمديد استخدام المفتاح الممتد*

معرّف البند الذي يجب ادراجه في الامتداد extendedKeyUsage من أجل شهادات الموقّع على القائمة الرئيسية هو 2.23.136.1.1.3.

معرّف البند الذي يجب ادراجه في امتداد extendedKeyUsage من أجل شهادات الموقّع على قائمة الانحرافات هو 2.23.136.1.1.8.

بالنسبة لشهادات الاتصال تتوقف قيمة هذا الامتداد على بروتوكول الاتصال المستخدم (see RFC 5280, section 4.2.1.12).

٧-١-١-٤ *متطلبات تمديد نقاط توزيع قائمة إلغاء الشهادات*

يجوز للسلطات الوطنية المعنية بالتوقيع على الشهادات نشر قوائمها لإلغاء الشهادات في عدة أماكن بما في ذلك دليل المفاتيح العامة وموقعها الخاص على الانترنت، أ ل خ.

بالنسبة لقوائم إلغاء الشهادات المنشورة في أماكن غير دليل المفاتيح العامة (مثلاً موقع على الانترنت أو مزوّد محلي لبروتوكول الاطلاع على الدليل الخفيف الوزن)، فإن القيم التي يتعين إدراجها في هذا الامتداد تخضع لمراقبة السلطة الوطنية المعنية بالتوقيع على الشهادات التي أصدرت الشهادات وقائمة إلغاء الشهادات المعنية.

بالنسبة لقوائم إلغاء الشهادات التي قُدمت إلى دليل المفاتيح العامة، **يجوز** للمشاركين في دليل المفاتيح العامة إدراج قيمتين لعنوان الموقع على الانترنت من أجل قوائمهم لإلغاء الشهادات باستخدام النموذج التالي (replace “CountryCode” with the issuing State or organization ICAO assigned three-letter code). وإذا كان هذا الرمز للبلاد لا يحدد بصورة فريدة دولة أو منظمة الإصدار، سيتم إنشاء القيد بارفاق الرمز "_" برمز البلد ثلاثي الأحرف في الجزء المقروء آلياً، ثم الرمز ثلاثي الأحرف المخصص من الإيكاو لدولة او منظمة الإصدار الذي يحدد دولة أو منظمة الإصدار على نحو فريدٍ:
https://pkddownload1.icao.int/CRLs/CountryCode.crl
https://pkddownload2.icao.int/CRLs/CountryCode.crl

هذا هو امتداد إلزامي، وفحوص وضع الإلغاء هي جزء إلزامي من إجراء المصادقة. ولذلك **يجب** على الأقل تدوين قيمة واحدة.

- قيم دليل المفاتيح العامة قد تكون القيم الوحيدة في الامتداد.
- قد توجد قيم إضافية (مثلاً قد تختار سلطة وطنية معنية بالتوقيع على الشهادات أيضاً نشر قائمتها لإلغاء الشهادات بموقع على الانترنت وإرفاق مؤشر إلى ذلك المصدر).
- يجوز أيضاً أن تختار سلطة وطنية معنية بالتوقيع على الشهادات أن تُدرج قيمةً منفردةً فقط (مثلاً مؤشر إلى موقعها على الانترنت كمصدرٍ) حتى إذا كانت تُرفق أيضاً قائمتها لإلغاء الشهادات إلى دليل المفاتيح العامة.

تُبين الأمثلة التالية قيم دليل المفاتيح العامة التي سيتم ملؤها في الشهادات الصادرة عن سلطة الإصدار لسنغافورة ولهونغ كونغ:

Singapore PKD example:
https://pkddownload1.icao.int/CRLs/SGP.crl
https://pkddownload2.icao.int/CRLs/SGP.crl

Hong Kong example:
https://pkddownload1.icao.int/CRLs/CHN_HKG.crl
https://pkddownload2.icao.int/CRLs/CHN_HKG.crl

٧-١-١-٥ *امتداد تغيير الاسم*

عند ترنّح مفتاح سلطة وطنية معنية بالتوقيع على الشهادات، **يجب** إصدار شهادة تربط المفتاح القديم بالمفتاح العام الجديد لتوفير انتقال مأمون للأطراف المعتمدة على ذلك. وعموماً يتم تحقيق هذا من خلال إصدار شهادة مُصدرة ذاتياً حيث تكون خانتا issuer وsubject متطابقتين لكن المفتاح المستخدم للتحقق من التوقيع يمثل زوج المفاتيح القديم والمفتاح العام المُعتمد يمثّل زوج المفاتيح الجديد.

يُوصى بألّا تغير السلطات الوطنية المعنية بالتوقيع على الشهادات اسمها المميّز (DN) بلا ضرورة نظراً لأنه يوجد تأثير سلبي على الأطراف المعتمِدة (يجب أن تحتفظ بكلا الاسمين القديم والجديد بوصفهما سلطات وطنية معنية بالتوقيع على الشهادات لنفس دولة أو منظمة الإصدار إلى أن تنتهي صلاحية جميع جوازات السفر الالكترونية المقروءة آلياً الموقّع عليها بالاسم القديم). غير أنه، إذا كان تغيير الاسم ضرورياً، **فيجب** إبلاغ هذا للأطراف المعتمِدة من خلال إصدار شهادة ربط بسلطة وطنية معنية بالتوقيع على الشهادات حيث تحتوي خانة issuer على الاسم القديم وتحتوي خانة subject على الاسم الجديد. وهذه الشهادة للربط بسلطة وطنية معنية بالتوقيع على الشهادات تنقل أيضاً ترنّح مفتاح حيث أن المفتاح المستخدم للتحقق من التوقيع يمثل الزوج القديم من المفاتيح والمفتاح العام المُعتمَد يمثل الزوج الجديد من المفاتيح. والشهادات التي تنقل كلاً من تَغيّر اسم سلطة وطنية معنية بالتوقيع على الشهادات و ترنّح مفتاح من أجل تلك السلطة **يجب** أن تتضمن امتداد الـ NameChange. للتعرّف على الشهادة بصفتها تلك. وهذا ليس له تأثير على PathLengthConstraint، فهو يظل `0`.

بالإضافة إلى ذلك، **يجوز** أيضاً ادراج امتداد NameChange في الشهادة الجديدة الموقّعة ذاتياً للسلطة الوطنية المعنية بالتوقيع على الشهادات التي أُنشأت عند تغيير الاسم المميّز للسلطة الوطنية المعنية بالتوقيع على الشهادات. وفي مثل هذه الشهادة الأساسية الموقّعة ذاتياً بواسطة السلطة الوطنية المعنية بالتوقيع على الشهادات، تحتوي كلٌّ من خانتي issuer وsubject على الاسم المميز الجديد. وعلى عكس شهادة الربط التي أصدرتها ذاتياً السلطة الوطنية المعنية بالتوقيع على الشهادات، المحتوية على كلٍّ من الاسم المميّز القديم والجديد للسلطة الوطنية المعنية المذكورة، فإن إدراج الامتداد NameChange في الشهادة الأساسية الموقعة ذاتياً من السلطة الوطنية المعنية بالتوقيع على الشهادات يبين ببساطة أن تغييراً للاسم قد حدث ولا يربط الاسم المميّز القديم بالاسم المميّز الجديد.

يجب ألّا تعيد أي سلطة وطنية معنية بالتوقيع على الشهادات استخدام الأرقام التسلسلية للشهادات. وكل شهادة تُصدرها سلطة وطنية معنية بالتوقيع على الشهادات، بصرف النظر عمّا إذا كانت تلك السلطة الوطنية قد خضعت لتغير اسمٍ أم لا، **يجب** أن تكون فريدةً.

مجموعة الرموز الأولى لتركيب الخلاصات من أجل امتداد تغيير الاسم:

```
nameChange EXTENSION ::= {
   SYNTAX                NULL
   IDENTIFIED BY     id-icao-mrtd-security-extensions-nameChange}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::=
{id-icao-
mrtd-security-extensions 1}
```

٧-١-١-٦ امتداد نوع الوثيقة

The DocumentType extension MUST be used to indicate the document types, as they appear in the MRZ, that the corresponding Document Signer is allowed to produce. This extension MUST always be set to non-critical.

ASN.1 for Document Type List extension:

```
documentTypeList EXTENSION ::= {
   SYNTAX                DocumentTypeListSyntax
   IDENTIFIED BY     id-icao-mrtd-security-extensions-
documentTypeList}

DocumentTypeListSyntax ::= SEQUENCE {
   version           DocumentTypeListVersion,
   docTypeList       SET OF DocumentType }

DocumentTypeListVersion ::= INTEGER {v0(0)}

-- Document Type as contained in MRZ, e.g. “P” or “ID” where a
-- single letter denotes all document types starting with that letter
DocumentType ::= PrintableString (size(1..2))

id-icao-mrtd-security-extensions-documentTypeList OBJECT
IDENTIFIER ::= {id-icao-mrtd-security-extensions 2}
```

٧-١-٢ وصف موجز لشهادات الجهة الموقّعة على البنية LDS2

يجب على شهادات الجهة الموقّعة على البنية LDS2 أن تمتثل للوصف الموجز لشهادة الجهة الموقّعة على الوثائق المعرّفة في ٧-١-١ باستثناء ما يلي:

خانة الموضوع:

يجب أن تملأ خانة "الموضوع" في شهادات الجهة الموقّعة على البنية LDS2 على النحو التالي:

- countryName (اسم البلد): **يجب** أن يكون موجوداً. وتحتوي القيمة على رمز البلد الذي يجب أن يتبع شكل رموز البلدان المكونة من حرفين، كما هو محدد في الوثيقة Doc 9303-3.
- commonName (الاسم الشائع): **يجب** أن يكون موجوداً. و**يجب ألا** يتجاوز طول القيمة في هذا النعت ٩ حروف.
- **يجب عدم** إدراج النعوت الأخرى.

امتدادات الشهادة:

يجب أن تحتوي شهادات الجهة الموقّعة على البنية LDS2 على امتدادات الشهادة المعرّفة في الجدول ٧ أدناه. و**يجب عدم** إدراج امتدادات الشهادة الأخرى.

الجدول ٧ — امتدادات الشهادة الإلزامية للبنية LDS2

Extension name	LDS2 Signer		Comments
	Presence	Criticality	
AuthorityKeyIdentifier	**m**	**nc**	
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
ExtKeyUsage	**m**	**c**	See Note 1

*ملاحظة ١ — **يجب** أن يملأ امتداد استخدام المفتاح الممتد لكل نوع من أنواع شهادة الجهة الموقّعة على البنية LDS2 على النحو المبيّن أدناه. ويلاحظ أنه يمكن ترخيص جهة موقعة واحدة على البنية LDS2 على جميع لتوقيع عدة أنواع من مواد بيانات LDS2. وفي هذه الحالة قد يحتوي امتداد استخدام المفتاح الممتد على جميع معرّفات البنود المتصلة بهذه الجهة الموقّعة.*

```
id-icao-mrtd-security-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}
                    id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-
                                                          security-lds2 8}
```

- LDS2 Travel Stamp Signer (LDS2-TS) certificates

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

- LDS2 Visa Signer (LDS2-V) certificates:

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

- LDS2 Biometrics Signer (LDS2-B) certificates:

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

*ملاحظة ٢ — **يجب** أن تمتثل شهادة الجهة الموقّعة على البنية LDS2 لقيود الحجم التي يفرضها الملف الأولي EF.Certificates في الوثيقة Doc 9303-10.*

وعلى الرغم من أن امتداد نقاط توزيع قائمة إلغاء الشهادات غير مدرج في هذه الشهادات، من الضروري فحص حالة الإلغاء بالنسبة لكل شهادة كجزء من عملية المصادقة العادية. وقائمة إلغاء الشهادات التي تصدرها السلطة الوطنية المعنية بالتوقيع على الشهادات التي أصدرت الشهادة هي قائمة إلغاء الشهادات التي استخدمت للتحقق من حالة الإلغاء.

٧-١-٣ وصف موجز لشهادات الجهة الموقّعة على رمز الأعمدة

يجب على شهادات الجهة الموقّعة على رمز الأعمدة أن تمتثل للوصف الموجز لشهادة الجهة الموقّعة على البنية LDS2. وبما أن شهادات الجهة الموقّعة على رمز الأعمدة تقوم بدور مختلف عن دور شهادات LDS2، فإن وصفها الموجز يختلف عنه في بعض النواحي. وبوجه خاص، يوجد متطلبات محددة للاسم المميز للموضوع (subjectDN) الخاص بشهادة الجهة الموقّعة على رمز الأعمدة والرقم التسلسلي (انظر الوثيقة Doc 9303-13).

خانة الموضوع:

يجب أن تملأ خانة "الموضوع" في شهادات الجهة الموقّعة على رمز الأعمدة على النحو التالي:

- commonName (اسم البلد): **يجب** أن يكون موجوداً. و**يجب** أن يتألف من حرفين كبيرين بشكل سلسلة قابلة للطبع، تحدد بشكل فريد الجهة الموقّعة على رمز الأعمدة، و**يجب** أن يتطابق مع الحرفين الثالث والرابع لمعرّف الجهة الموقّعة في رمز الأعمدة كما هو محدد في الوثيقة Doc 9303-13).
- countryName (الاسم الشائع): **يجب** أن يتألف من رمز البلد المكون من حرفين (انظر الوثيقة Doc 9303-3) للجهة الموقعة على رمز الأعمدة، ومن حروف كبيرة، بشكل سلسلة قابلة للطبع، و**يجب** أن يتطابق مع الحرفين الأول والثاني لمعرّف الجهة الموقّعة في رمز الأعمدة كما هو محدد في الوثيقة Doc 9303-13).
- **يجب عدم** إدراج النعوت الأخرى.

امتدادات الشهادة:

يجب أن تحتوي شهادات الجهة الموقّعة على رمز الأعمدة على امتدادات الشهادة المعرّفة في الجدول ٨ أدناه. و**يجب عدم** إدراج امتدادات الشهادة الأخرى.

الجدول ٨ — الامتدادات المسموح بها لشهادة الجهة الموقّعة على رمز الأعمدة

Extension name	LDS2 Signer		Comments
	Presence	Criticality	
AuthorityKeyIdentifier	**m**	**nc**	
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
DocumentType	**o**		This extension indicates the document type, which the Bar Code Signer is allowed to produce
ExtKeyUsage	**m**	**c**	See note below

*ملاحظة — **يجب** أن يملأ امتداد استخدام المفتاح الممتد لكل نوع من أنواع شهادة الجهة الموقّعة على رمز الأعمدة على النحو المبيّن أدناه.*

```
id-icao-mrtd-security-vds OBJECT IDENTIFIER ::= {id-icao-mrtd-security 11}
id-icao-vdsSigner OBJECT IDENTIFIER ::= {id-icao-mrtd-security-vds 1}
```

٧-١-٤ وصف موجز لقائمة إلغاء الشهادات

يحدد الجدول ٩ متطلبات الوصف الموجز لقائمة إلغاء الشهادات بالنسبة لخانات متن قائمة إلغاء الشهادات. ويحدد الجدول ١٠ متطلبات الوصف الموجز لقائمة إلغاء الشهادات وامتدادات بنود قائمة إلغاء الشهادات.

الجدول ٩ — وصف موجز لخانات قائمة إلغاء الشهادات

Certificate List Component	*CSCA CRL*	*Comments*
CertificateList	m	
tBSCertList	m	See Table 10
signatureAlgorithm	m	Value inserted here dependent on algorithm selected
signatureValue	m	Value inserted here dependent on algorithm selected
tBSCertList		
Version	m	MUST be v2
Signature	m	value inserted here MUST be the same as that in signatureAlgorithm component of CertificateList sequence
Issuer	m	countryName and serialNumber, if present, MUST be PrintableString Other attributes that have DirectoryString syntax MUST be either PrintableString or UTF8String countryName MUST be Upper Case
thisUpdate	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in UTCTime UTCTime MUST be represented as YYMMDDHHMMSSZ Dates in 2050 and beyond MUST be in GeneralizedTime. GeneralizedTime MUST NOT have fractional seconds GeneralizedTime MUST be represented as YYYYMMDDHHMMSSZ
nextUpdate	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in UTCTime UTCTime MUST be represented as YYMMDDHHMMSSZ Dates in 2050 and beyond MUST be in GeneralizedTime. GeneralizedTime MUST NOT have fractional seconds GeneralizedTime MUST be represented as YYYYMMDDHHMMSSZ
revokedCertificates	c	SHALL be present if there are revoked certificates. If there are no revoked certificates it SHALL NOT be present. If present, MUST NOT be empty
crlExtensions	m	See Table 10 on which extensions should be present Default values for extensions MUST NOT be encoded

الجدول ١٠ — قائمة إلغاء الشهادات والوصف الموجز لامدادات مدخل قائمة إلغاء الشهادات

Extension Name	*CSCA CRL*	*Criticality*	*Comments*
CRL Extensions			
authorityKeyIdentifier	**m**	**nc**	This MUST be the same value as the subjectKeyIdentifier field in the CRL issuer's certificate.
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
issuerAlternativeName	**o**	**nc**	See Note 1
cRLNumber	**m**	**nc**	MUST be non-negative integer and maximum 20 Octets MUST use 2's complement encoding and be represented in the smallest number of octets
deltaCRLIndicator	**x**		
issuingDistributionPoint	**x**		
freshestCRL	**x**		
CRL Entry Extensions			
reasonCode	**x**		
holdInstructionCode	**x**		
invalidityDate	**x**		
certificateIssuer	**x**		
other private extensions	o	**nc**	

*ملاحظة ١ — إذا خضعت سلطة وطنية معنية بالتوقيع على الشهادات لتغيير اسمٍ، **يجوز** إدراج هذا الامتداد في قوائم إلغاء الشهادات الصادرة عقب تغيير اسم السلطة الوطنية المعنية بالتوقيع على الشهادات. وإذا كانت القيمة (القيم) موجودةً، **فيجب** أن تكون القيمة (القيم) في هذا الامتداد مطابقة لخانة issuer من الشهادات التي أصدرتها السلطة الوطنية المعنية بالتوقيع على الشهادات بذلك الاسم السابق. وبمجرد انتهاء فترة صلاحية جميع الشهادات التي أُصدرت باسمٍ سابقٍ للسلطة الوطنية المعنية بالتوقيع على الشهادات، يمكن استبعاد اسم تلك السلطة من قوائم إلغاء الشهادات اللاحقة. وأنظمة التفتيش غير مطلوبة لمعالجة هذا الامتداد. ونظراً إلى أن وثيقة اللايكاو Doc 9303 تفرض*

سلطة وطنية واحدة معنية بالتوقيع على الشهادات لكل بلد، فإن مكون الـ countryName لخانةهيئة الإصدار يكفي ليحدد السلطة الوطنية المعنية بالتوقيع على الشهادات بشكل فريد. ويُستخدم آخر مفتاح عام لتلك السلطة الوطنية المعنية بالتوقيع على الشهادات للتحقق من صحة توقيع قائمة إلغاء الشهادات. ونظراً لأن أي سلطة وطنية معنية بالتوقيع على الشهادات تُصدر قائمة واحدة لإلغاء الشهادات، فإن هذه القائمة لإلغاء الشهادات تشمل جميع الشهادات الصادرة بإسم ذلك countryName*. وبالإضافة إلى ذلك التحقق الإلزامي،* **فيجوز** *أيضاً إجراء تحقق اختياري من أن خانة الـ issuer من تلك الشهادة مساوية لخانة الـ issuer لقائمة إلغاء الشهادات أو إحدى قيم امتداد issuerAltName في قائمة إلغاء الشهادات.*

ملاحظة ٢ — يمكن أن تحتوي قائمة إلغاء الشهادات على معلومات إلغاء أخرى فيما يتعلق، مثلاً، بمشغّل النظام أو بشهادات سلطة التسجيل.

٧-٢ البنية الأساسية للمفاتيح العامة للتراخيص

تشمل البنية الأساسية للمفاتيح العامة للتراخيص شهادات X.509 لنقطة الاتصال المفردة وشهادات يمكن التحقق منها بواسطة البطاقة للسلطة الوطنية للتحقق من الشهادات والمتحقق من الشهادات والوحدات الطرفية. ويحدد هذا القسم الأوصاف الموجزة لشهادات نقطة الاتصال المفردة وشهادات السلطة الوطنية للتحقق من الشهادات والمتحقق من الشهادات ونظام التفتيش. وتتوفر نظرة عامة على مواد البيانات الواردة في الشهادات القابلة للتحقق بواسطة البطاقة وتتم أيضاً تغطية ترميز تلك المواد.

٧-٢-١ وصف موجز لشهادة نقطة الاتصال المفردة

يمكن استخدام جهاز منفصل لسلطة إصدار التراخيص من أجل إصدار شهادات نقطة الاتصال المفردة بشكل مباشر مع التقييدات التالية على الوصف الموجز لشهادات سلطة إصدار التراخيص الموقّعة ذاتياً.

- **يجب** أن تتوافق شهادة سلطة إصدار التراخيص مع [RFC 5280]؛
- SHA-224 وSHA-256 وSHA-384 وSHA-512 هي خوارزميات البصمة الرقمية الوحيد المسموح بها؛
- **يجب** أن يكون countryName موجوداً في خانة الموضوع.

يجب أن تمتثل شهادات نقطة الاتصال المفردة من النوع LDS2 (العميل والمخدّم) للوصف الموجز لشهادة الاتصال المحدد في القسم ٧-١، مع التقييدات التالية:

خانة هيئة الإصدار:

شهادات نقطة الاتصال المفردة تصدرها إما السلطة الوطنية المعنية بالتوقيع على الشهادات أو سلطة منفصلة لإصدار التراخيص تحدد خصيصاً لإصدار شهادات نقطة الاتصال المفردة.

خانة الموضوع:

بالنسبة لشهادات نقطة الاتصال المفردة ذات البنية LDS2، **يجب** أن تملأ خانة الموضوع على النحو التالي:

- countryName (اسم البلد): **يجب** أن يكون موجوداً. وتحتوي القيمة على رمز البلد الذي **يجب** أن يتبع شكل رموز البلدان المكونة من حرفين، كما هو محدد في الوثيقة Doc 9303-3.
- commonName (الاسم الشائع): **يجب** أن يكون موجوداً. وبالنسبة لشهادات عميل أمن طبقة النقل لنقطة الاتصال المفردة، **ينبغي** أن تكون القيمة "SPOC TLS client". وبالنسبة لشهادات مخدّم أمن طبقة النقل لنقطة الاتصال المفردة، **ينبغي** أن تكون القيمة "SPOC TLS server".

- **يجوز** أيضاً إدراج نعوت أخرى تبعاً لتقدير دولة أو منظمة الإصدار.

امتدادات استخدام المفاتيح:

بالنسبة لشهادات نقطة الاتصال المفردة، تعتمد القيمة (القيم) على مجموعة الشفرات المستعملة.

امتدادات الأسماء البديلة للموضوع:

بالإضافة إلى القيم المبينة في الوصف الموجز لشهادة الاتصال، **يجب** أيضاً أن تحتوي شهادات مخدم أمن طبقة النقل لنقطة الاتصال المفردة على قيمة DNSName التي هي الجزء المضيف لعنوان الموقع الإلكتروني لنقطة الاتصال المفردة.

امتدادات استخدام المفتاح الممتد:

بالنسبة لشهادات عميل ومخدّم نقطة الاتصال المفردة، **يجب** أن تدرج القيمة ذات الصلة الواردة أدناه:

- شهادات عميل نقطة الاتصال المفردة: معرّف البنود هو 2.23.136.1.1.10.1؛
- شهادات مخدّم نقطة الاتصال المفردة: معرّف البنود هو 2.23.136.1.1.10.2.

امتدادات نقطة توزيع قائمة إلغاء الشهادات:

هذا الامتداد إلزامي في شهادات عميل ومخدّم نقطة الاتصال المفردة.

٧-٢-٢ الأوصاف الموجزة لشهادات السلطة الوطنية للتحقق من الشهادات والمتحقق من الشهادات والوحدة الطرفية

يجب أن تصدّق الدوائر المتكاملة على شهادات السلطة الوطنية للتحقق من الشهادات وشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية. وبسبب القيود الحسابية المفروضة على تلك الرقاقات، **يجب** أن تكون الشهادات بشكل قابل للتحقق بواسطة البطاقة (شهادات السيرة الذاتية).

ويجب استخدام الشكل والوصف الموجز للشهادة المحددان في الجدول ١١. ويمكن الاطلاع على تفاصيل قيم الترميز في الوثيقة Doc 9303-11.

الجدول ١١ — الوصف الموجز لشهادة

Data Object	Certificate Presence
CV Certificate	m
Certificate Body	m
Certificate Profile Identifier	m
Certification Authority Reference	m
Public Key	m
Certificate Holder Reference	m
Certificate Holder Authorization Template	m
Certificate Effective Date	m
Certificate Expiration Date	m
Certificate Extensions	o
Signature	m

٧-٢-٢-١ معرّف الوصف الموجز للشهادة

يستدل على نسخة الوصف الموجز من معرّف الوصف الموجز للشهادة. و**يجب** استخدام الإصدار ١ ويتم تحديده بواسطة القيمة ٠.

٧-٢-٢-٢ معرّف الوصف الموجز للشهادة

يجب على كل شهادة من شهادات السيرة الذاتية أن تحتوي على مرجعين للمفاتيح العامة (مرجع لصاحب الشهادة ومرجع لسلطة إصدار الشهادات).

ومرجع سلطة إصدار الشهادة هو مرجع المفتاح العام (الخارجي) لسلطة إصدار الشهادات (السلطة الوطنية للتحقق من الشهادات أو المتحقق من الوثائق) الذي **يجب** استخدامه للتحقق من التوقيع على الشهادة.

ومرجع صاحب الشهادة هو معرّف للمفتاح العام المتوفر في الشهادة الذي **يجب** استخدامه للإشارة إلى هذا المفتاح العام.

*ملاحظة — نتيجة لذلك، **يجب** أن يكون مرجع سلطة إصدار الشهادات الوارد في شهادة معينة مساوياً لمرجع صاحب الشهادة في الشهادة المقابلة لسلطة إصدار الشهادات.*

و**يجب** أن يتألف مرجع صاحب الشهادة من العناصر المتسلسلة التالية: رمز البلد، واسم تذكيري لصاحب الشهادة، ورقم تسلسلي. و**يجب** أن يتم اختيار هذه العناصر وفقاً للجدول ١٢ والقواعد التالية:

(أ) رمز البلد

- **يجب** أن يكون رمز البلد الرمز المكون من حرفين لبلد صاحب الشهادة الوارد في الوثيقة Doc 9303-3.

(ب) اسم تذكيري لصاحب الشهادة:

- **يجب** أن يتم تعيين الاسم التذكيري لصاحب الشهادة كمعرّف وحيد على النحو التالي:
  - الاسم التذكيري لصاحب شهادة السلطة الوطنية للتحقق من الشهادات **يجب** أن تعينه السلطة الوطنية للتحقق من الشهادات نفسها؛
  - والاسم التذكيري لصاحب شهادة المتحقق من الوثائق **يجب** أن تعينه السلطة الوطنية المحلية للتحقق من الشهادات التابعة له؛
  - والاسم التذكيري لصاحب شهادة نظام التفتيش **يجب** أن يعينه المتحقق من الوثائق المشرف.

(ج) الرقم التسلسلي:

- **يجب** أن يعين صاحب الشهادة الرقم التسلسلي؛
- و**يجب** أن يكون الرقم التسلسلي عددياً أو أبجدياً عددياً؛
  - **يجب** أن يكون الرقم التسلسلي العددي مؤلفاً من الأرقام "٠...٩".
  - **يجب** أن يكون الرقم التسلسلي الأبجدي العددي مؤلفاً من الأرقام "٠...٩" ومن الحروف "A...Z" .
- و**يجب** أن يبدأ الرقم المتسلسل برمز البلد المكوّن من حرفين الوارد في الوثيقة Doc 9303-3 لبلد سلطة إصدار الشهادات، و**يجب** أن تعين الحروف الثلاثة الباقية كرقم تسلسلي أبجدي عددي؛
- و**يجوز** إعادة ضبط الرقم التسلسلي إذا استنفدت جميع الأرقام التسلسلية المتوفرة.

الجدول ١٢ — الوصف الموجز لشهادة

	الترميز	الطول
رمز البلد	Doc 9303-3	2F
الاسم التذكيري لصاحب الشهادة	ISO/IEC 8859-1	9V
الرقم التسلسلي	ISO/IEC 8859-1	5F

٧-٢-٢-٣ المفتاح العام

تحتوي الخانة على المفتاح العام الذي يجري اعتماده.

يجب أن تحتوي الشهادات الموقّعة ذاتياً للسلطة الوطنية للتحقق من الشهادات على بارامترات النطاق. و**يجوز** لشهادات الربط بالسلطة الوطنية للتحقق من الشهادات أن تحتوي على بارامترات النطاق، باستثناء الحالة التي تتغير فيها بارامترات النطاق. وفي هذه الحالات، **يجب** أن تحتوي شهادات الربط بالسلطة الوطنية للتحقق من الشهادات على بارامترات جديدة للنطاق.

و**يجب ألا** تحتوي شهادات المتحقق من الوثائق وشهادات الوحدة الطرفية على بارامترات نطاق. و**يجب** أن ترد بارامترات نطاق المفاتيح العامة للمتحقق من الوثائق والوحدة الطرفية من المفتاح العام للسلطة العامة المقابلة للتحقق من الشهادات.

٧-٢-٢-٤ نموذج الترخيص لصاحب الشهادة

يجب أن بتم ترميز دور وترخيص صاحب الشهادة في نموذج الترخيص لصاحب الشهادة. وهذا النموذج هو تسلسل مكون من مواد البانات التالية:

- معرّف مواد بحدد نوع الوحدة الطرفية وشكل النموذج؛
- مادة بيانات تقديرية ترمّز الترخيص، أي دور وترخيص صاحب الشهادة بالنسبة لسلطة إصدار الشهادات.

وتحدد الوثيقة Doc 9303-10 القيم المحددة.

٧-٢-٢-٥ التاريخ الفعلي للشهادة وتاريخ انتهاء صلاحية الشهادة

تدل مجموعة هذين التاريخين على فترة صلاحية الشهادة. و**يجب** أن يكون التاريخ الفعلي للشهادة تاريخ إنتاج الشهادة. وتاريخ انتهاء صلاحية الشهادة هو التاريخ الذي تنتهي بعده صلاحية الشهادة.

٧-٢-٢-٦ امتدادات الشهادة (امتدادات الترخيص)

يجوز أن تدرج امتدادات الترخيص في شهادات السلطة الوطنية للتحقق من الشهادات وشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية. وهذه الامتدادات تنقل التراخيص المضافة إلى تلك الموجودة في نموذج ترخيص صاحب الشهادة إلى الشهادة.

وامتداد الترخيص هو تسلسل نماذج بيانات تقديرية، حيث **يجب** أن يحتوي كل نموذج بيانات تقديري على مواد البيانات التالية كما هو مبين في الجدول ١٣.

أ) معرّف مواد يحدد محتوى وشكل الامتداد؛

ب) ومادة بيانات خاصة بالسياق تحتوي على الترخيص المرمّز.

الجدول ١٣ — امتدادات الشهادة

Data Object
Certificate Extensions
Discretionary Data Template
Object Identifier
Context Specific Data Object
Discretionary Data Template
Object Identifier
Context Specific Data Object
…

*ملاحظة — لا يأخذ إجراء المصادقة على الشهادة الوارد في الوثيقة Doc 9303-11 في الاعتبار امتدادات الشهادة. وبالتالي، فإن الامتدادات هي نعوت غير حرجة و**يجب ألا** ترفض الدائرة المتكاملة الشهادات بسبب امتدادات غير معروفة.*

٧-٢-٢-٧ التوقيع

يجب أن ينشأ التوقيع على الشهادة فوق متن الشهادة المرمّز (أي بما في ذلك الوسم والطول). و**يجب** أن يحدد مرجع سلطة إصدار الشهادات المفتاح العام المقرر استخدامه للتحقق من التوقيع.

٧-٢-٣ مواد البيانات

ترد في الجدول ١٤ لمحة عامة عن وسوم وأطوال وقيم مواد البيانات المستخدمة في شهادات السلطة الوطنية للتحقق من الشهادات وشهادات المتحقق من الوثائق وشهادات الوحدة الطرفية.

الجدول ١٤ — لمحة عامة عن مواد البيانات (مصنّفة بحسب الوسم)

الاسم	الوسم	الطول	القيمة	تعليق
معرّف المواد	0x06	V	معرّف مواد	–
مرجع سلطة إصدار الشهادات	0x42	16V	سلسلة حروف	يحدد المفتاح العام للسلطة المصدرة للشهادات في الشهادة.
بيانات تقديرية	0x53	V	سلسلة ثمانيات	يحتوي على بيانات اعتباطية.
مرجع صاحب الشهادة	0x5F20	16V	سلسلة حروف	يربط المفتاح العام الوارد في الشهادة بأحد المعرّفات.
تاريخ انتهاء صلاحية الشهادة	0x5F24	6F	تاريخ	التاريخ الذي تنتهي بعده صلاحية الشهادة.
التاريخ الفعلي للشهادة	0x5F25	6F	تاريخ	تاريخ توليد الشهادة.
معرّف الوصف الموجز للشهادة	0x5F29	1F	عدد صحيح غير جبري	إصدار الشهادة وشكل طلب الشهادة.

الاسم	الوسم	الطول	القيمة	تعليق
التوقيع	0x5F37	V	سلسلة ثمانيات	توقيع رقمي تنتجه خوارزمية تشفيرية لا تناظرية.
امتدادات الشهادة	0x65	V	متتالية	تحتوي على امتدادات الشهادة.
التحقق من الصحة	0x67	V	متتالية	يحتوي على مواد بيانات متعلقة بالتحقق من الصحة.
نموذج البيانات التقديرية	0x73	V	متتالية	يحتوي على مواد بيانات اعتباطية.
شهادة السيرة الذاتية	0x7F21	V	متتالية	تحتوي على متن الشهادة والتوقيع.
المفتاح العام	0x7F49	V	متتالية	يحتوي على قيمة المفتاح العام وبارامترات النطلق.
نموذج ترخيص صاحب الشهادة	0x7F4C	V	متتالية	يرمّز دور صاحب الشهادة (أي السلطة الوطنية للتحقق من الشهادات، المتحقق من الوثائق، الوحدة الطرفية) ويعيّن حقوق الوصول إلى القراءة/الكتابة.
متن الشهادة	0x7F4E	V	متتالية	يحدد مواد بيانات متن الشهادة.

F: fixed length (exact number of octets), V: variable length (up to number of octets).

٧-٢-٣-١ قيم الترميز

أنواع القيم الأساسية المستخدمة في هذه المواصفة هي التالية: الأعداد الصحيحة (غير الجبرية)، ونقاط المنحنى الإهليلجي، وتواريخ، وسلاسل الحروف، وسلاسل الثمانيات، ومعرّفات المواد، والمتتاليات.

٧-٢-٣-١-١ الأعداد الصحيحة (غير الجبرية)

جميع الأعداد الصحيحة المستخدمة في هذه المواصفة هي أعداد صحيحة غير جبرية. و**يجب** تحويل عدد صحيح غير جبري إلى سلسلة ثمانيات باستخدام التمثيل الثنائي للعدد الصحيح في شكل البايتات الأكثر دلالة. ويجب استخدام العدد الأدنى من الثمانيات، أي **يجب عدم** استخدام الثمانيات الطليعية ذات القيمة 0x00.

ملاحظة — بالمقابل، فإن العدد الصحيح من نوع ASN.1 هو دائماً عدد صحيح جبري.

٧-٢-٣-١-٢ نقاط المنحنى الإهليلجي

يحدد [TR-03111] تحويل نقاط المنحنى الإهليلجي إلى سلاسل ثمانيات. و**يجب** استخدام الشكل غير المضغوط.

٧-٢-٣-١-٣ التواريخ

يتم ترميز التاريخ بواسطة ٦ أرقام "d1…d6" بالشكل YYMMDD باستخدام نطاق غرينتش الزمني. ويتم تحويله إلى سلسلة ثمانيات 'o1….o6' عن طريق ترميز كل ثمانية oj على شكل أرقام مرمزة ثنائياً غير مضغوطة ($1 \le j \le 6$).

يتم ترميز السنة YY برقمين ويتعين تفسيرها على أنها 20YY، أي إن السنة تقع ضمن النطاق ٢٠٠٠ إلى ٢٠٩٩.

٧-٢-٣-١-٤ سلاسل الحروف

سلسلة الحروف "c1….cn" هي تسلسل لعدد n من الحروف cj حيث $n \geq j \geq 1$. **ويجب** تحويلها إلى سلسلة ثمانيات 'o1…on' عن طريق تحويل كل حرف cj إلى ثمانية oj باستخدام مجموعة الحروف ISO/IEC 8859-1.

لا يكون رمزا الحروف 0x00-0x1F و0x7F-0x9F مخصصين **ويجب عدم** استعمالهما. وتحويل ثمانية إلى حرف غير مخصص **ويجب** أن ينتج عنه خطا.

٧-٢-٣-١-٥ سلاسل الثمانيات

سلسلة الثمانيات "o1…on" هي تسلسل لعدد n من الثمانيات oj حيث $n \geq j \geq 1$. وتتألف كل ثمانية من ٨ بتات.

٧-٢-٣-١-٦ معرّفات المواد

يتم ترميز معرّف المواد "i1, i2…in" على شكل قائمة مرتبة من n إعداد صحيحة غير جبرية ij حيث $n \geq j \geq 1$. **ويجب** تحويله غلى سلسلة ثمانيات "o1….on" باستخدام الإجراء التالي:

١) يُرصّ أول عددين صحيحين i1 وi2 في عدد صحيح مفرد j يتم بعد ذلك تحويله إلى سلسلة الثمانيات o1. تحسب القيمة j كما يلي:

$$i=i1 \cdot 40+i2$$

٢) تحول الأعداد الصحيحة الباقية ij مباشرة الى سلاسل الثمانيات oj – 1 حيث $n \geq j \geq 3$.

ملاحظة — يتم ترميز الأعداد الصحيحة غير الجبرية على شكل سلاسل ثمانيات باستخدام الشكل ذي البايتات الأكثر دلالة كما هو محدد في الوثيقة Doc 9303-11، ومع ذلك لا تستخدم سوى البتات 7-1 من كل ثمانية. أما البتة ٨ (البتة في أقصى اليسار) التي تضبط على واحد فتستخدم للدلالة على أن هذه الثمانية ليست آخر ثمانية في السلسلة.

٧-٢-٣-١-٦ المتتاليات

المتتالية "D1…Dn" هي قائمة مرتبة من مواد بيانات Dj يبلغ عددها n حيث $n \geq j \geq 1$. ويجب أن يتم تحويل المتتالية إلى قائمة متسلسلة من سلاسل الثمانيات "o1….on" بواسطة ترميز كل مادة بيانات Dj إلى سلسلة الثمانيات oj بواسطة قاعدة التشفير المميز.

٧-٢-٣-٢ ترميز مواد بيانات المفاتيح العامة

تحتوي مادة بيانات المفاتيح العامة على متتالية من معرّف مواد وعدة مواد بيانات خاصة بالسياق:

- معرّف المواد هو معرّف خاص بالتطبيق ويشير ليس فقط إلى شكل المفتاح العام (أي مواد البيانات الخاصة بالسياق) بل إلى استخامه أيضاً.
- تعرّف مواد البيانات الخاصة يالسياق بواسطة معرّف المواد وتحتوي على قيمة المقتاح العام وبارامترات النطاق.

ويرد أدناه وصف لمواد بيانات المفاتيح العامة المستخدمة في هذه المواصفة.

٧-٢-٣-٢-١ المفاتيح العامة ريفست وشمير وأدلمان

يبين الجدول ١٥ مواد البيانات الواردة في المفتاح العام ريفست وشمير وأدلمان. ويكون ترتيب مواد البيانات ثابتاً.

الجدول ١٥ — المفتاح العام ريفست وشمير وأدلمان

مادة البيانات	الاختصار	الوسم	النوع	شهادة السيرة الذاتية
معرّف المواد		0x06	معرّف المواد	m
معامل مركّب	n	0x81	عدد صحيح غير جبري	m
أسّ عام	e	0x82	عدد صحيح غير جبري	m

٧-٢-٣-٢-٢ المفاتيح العامة للمنحنى الإهليلجي

يبين الجدول ١٦ مواد البيانات الواردة في المفتاح العام للمنحنى الإهليلجي. ويكون ترتيب مواد البيانات ثابتاً. و**يجب** أن تكون بارامترات النطاق **المشروطة** موجودة جميعها، ما عدا العامل المشترك، أو غائبة جميعها على النحو التالي:

- يجب أن تحتوي شهادات السلطة الوطنية للتحقق من الشهادات الموقّعة ذاتياً على بارامترات النطاق؛
- **يجوز** أن تحتوي شهادات الربط بالسلطة الوطنية للتحقق من الشهادات على بارامترات النطاق؛
- و**يجب ألا** تحتوي شهادات المتحقق من الوثائق وشهادات الوحدة الطرفية على بارامترات النطاق. و**يجب** أن ترد بارامترات النطاق للمفاتيح العامة للمتحقق من الوثائق والوحدة الطرفية من المفتاح العام المقابل للسلطة الوطنية للتحقق من الشهادات؛
- و**يجب** أن تحتوي طلبات الشهادات دائماً على بارامترات النطاق.

الجدول ١٦ — المفتاح العام للمنحنى الإهليلجي

مادة البيانات	الاختصار	الوسم	النوع	شهادة السيرة الذاتية
معرّف المواد		0x06	معرّف المواد	m
معامل عدد أولي	p	0x81	عدد صحيح غير جبري	c
المعامل الاول	a	0x82	عدد صحيح غير جبري	c
المعامل الثاني	b	0x83	عدد صحيح غير جبري	c
نقطة الاساس	G	0x84	نقطة المنحنى الإهليلجي	c
ترتيب النقطة	r	0x85	عدد صحيح غير جبري	c
نقطة عامة	Y	0x86	نقطة المنحنى الإهليلجي	m
العامل المشترك	f	0x87	عدد صحيح غير جبري	c

٨- بروتوكول نقطة الاتصال المفردة (SPOC)

نقطة الاتصال المفردة (SPOC) هي الواجهة الوحيدة التي تعرضها الدولة لعمليات إدارة المفاتيح التي تجريها مع الدول الأجنبية من أجل البنية الأساسية للمفاتيح العامة للتراخيص من النوع LDS2. وبروتوكول نقطة الاتصال المفردة هو بروتوكول إدارة المفاتيح المتعلقة بالعمليات بين السلطات الوطنية للتحقق من الشهادات والمتحققين من الوثائق في الدول المختلفة. وعلى الرغم من **إمكانية** استخدام بروتوكول نقطة الاتصال المفردة أيضاً في الاتصالات الداخلية بين السلطة الوطنية للتحقق من الشهادات والمتحققين الداخليين من الوثائق التابعين لها وبين أحد المتحققين من الوثائق ومجموعة الوحدات الطرفية الداخلية التي يديرها، فإنه غير مطلوب. ويمكن استخدام بروتوكولات أخرى لإدارة المفاتيح من أجل الإدارة الداخلية للمفاتيح.

يستخدم بروتوكول نقطة الاتصال المفردة لتبادل المفاتيح والشهادات، من أجل ما يلي:

- أن يتمكن المتحقق من الوثائق من إرسال طلب شهادة إلى السلطة الوطنية الأجنبية للتحقق من الشهادات؛
- وأن تتمكن السلطة الوطنية للتحقق من الشهادات من إرسال الشهادة الصادرة إلى المتحقق من الوثائق المطالب؛
- وأن تتمكن الوطنية للتحقق من الشهادات والمتحققين من الوثائق من طلب مجموعة من الشهادات الصالحة من إحدى السلطات الوطنية الأجنبية للتحقق من الشهادات؛
- وأن يكون من الممكن تبادل الرسائل العامة بين المتحققين من الوثائق والسلطات الوطنية للتحقق من الشهادات.

داخل الدولة:

- **يجب** أن تستعمل السلطة الوطنية للتحقق من الشهادات بروتوكول نقطة الاتصال المفردة الداخلية التابعة لها لقبول الطلبات الواردة لإصدار الشهادات الأجنبية ولإرسال الشهادات الناتجة أو التبليغات بالفشل إلى الجهة الطالبة؛
- و**يجب** أن يستعمل المتحققون من الوثائق بروتوكول نقطة الاتصال المفردة الداخلية التابعة لهم لإرسالطلبات الشهادات إلى السلطات الوطنية الأجنبية للتحقق من الشهادات واستقبال الشهادات الناتجة أو التبليغات بالفشل؛
- و**يجب** أن يجمع بروتوكول نقطة الاتصال المفردة الطلبات والردود الواردة من السلطة الوطنية الداخلية للتحقق من الشهادات والمتحققين من الوثائق وأن يرسلها إلى بروتوكول نقطة الاتصال المفردة التابع للدولة المتلقية؛
- و**يجب** أن يجمع بروتوكول نقطة الاتصال المفردة الطلبات والردود الواردة من بروتوكولات نقاط الاتصال المفردة للدول الأخرى وأن يرسلها إلى السلطة الوطنية الداخلية للتحقق من الشهادات ذات الصلة أو إلى المتحقق الداخلي من الوثائق ذي الصلة.

يجب أن تستخدم اتصالات خدمة الويب في بروتوكول نقطة الاتصال المفردة البروتوكول HTTPS مع التحقق من صحة أمن طبقة النقل لكل من العميل والمخدّم.

ملاحظة — بروتوكولات نقطة الاتصال المفردة هي محاور اتصالات بين كيانات البنية الأساسية للمفاتيح العامة للتراخيص التي ينبغي أن تكون بالتالي متوفرة على مدار الساعة وأن يتيسر الوصول إليها من بروتوكولات نقاط الاتصال المفردة الأجنبية.

يتسجل كل بروتوكول من بروتوكولات نقطة الاتصال المفردة بشكل منفصل مع جميع بروتوكولات نقاط الاتصال المفردة الأخرى، مقدماً المعلومات التالية على الأقل:

- دولة بروتوكول نقطة الاتصال المفردة – الدولة التي يقدم فيها بروتوكول نقطة الاتصال المفردة واجهة الاتصالات؛
- وعنوان الموقع الشبكي لبروتوكول نقطة الاتصال المفردة – العنوان الإلكتروني للغة WSDL، ويصف واجهة البروتوكول وموقع الخدمة؛

- وشهادة هيئة إصدار الشهادات التابعة لبروتوكول نقطة الاتصال المفردة – الشهادة (الشهادات) المستخدمة للتحقق من شهادات الاتصال ببروتوكول نقطة الاتصال المفردة.

٨-١ البنى المتعلقة بنقطة الاتصال المفردة

تعرّف البنى التالية لاستخدامها في رسائل بروتوكول نقطة الاتصال المفردة.

٨-١-١ بنية طلب الشهادة

طلبات الشهادات هي عبارة عن شهادات مختصرة قابلة للتحقق بواسطة بطاقة ويمكن أن تحمل توقيعاً إضافياً. و**يجب** استخدام الوصف الموجز لطلب الشهادة المحدد في الجدول ١٧.

الجدول ١٧ — الوصف الموجز لطلب شهادة السيرة الذاتية

Data Object	Certificate Presence
Authentication	c
CV Certificate	m
Certificate Body	m
Certificate Profile Identifier	m
Certification Authority Reference	r
Public Key	m
Certificate Holder Reference	m
Signature	m
Certification Authority Reference	c
Signature	c

٨-١-١-١ معرّف الوصف الموجز للشهادة

رقم الإصدار هو ١، ويحدد بالقيمة ٠.

٨-١-١-٢ مرجع سلطة إصدار الشهادات

ينبغي أن يستخدم مرجع سلطة إصدار الشهادات لإبلاغ سلطة إصدار الشهادات عن المفتاح الخاص الذي يتوقع أن يستخدمه مقدم الطلب للتوقيع على الشهادة. وفي حال انحراف سلطة إصدار الشهادات الواردة في الطلب عن مرجع سلطة إصدار الشهادات الوارد في الشهادة الصادرة (أي أن الشهادة الصادرة موقّعة بواسطة مفتاح خاص لا يتوقعه مقدم الطلب)، **ينبغي** أن تقدم الشهادة المقابلة لسلطة إصدار الشهادات إلى مقدم الطلب رداً على ذلك.

٨-١-١-٣ المفتاح العام

يجب أن تحتوي طلبات الشهادات دائماً على بارامترات نطاق.

٨-١-١-٤ مرجع صاحب الشهادة

يستخدم مرجع صاحب الشهادة لتحديد المفتاح العام الوارد في الطلب والشهادة الناتجة.

٨-١-١-٥ التوقيع (التواقيع)

يمكن أن يصل عدد التواقيع على طلب الشهادة إلى توقيعين، توقيع داخلي وتوقيع خارجي.

التوقيع الداخلي (مطلوب)

يكون متن الشهادة موقع ذاتياً، أي **يجب** أن يكون التوقيع الداخلي قابلاً للتحقق بواسطة مفتاح عام وارد في طلب الشهادة. و**يجب** أن ينشأ التوقيع فوق دسم الشهادة المرمّز (أي بما في ذلك الوسم والطول).

التوقيع الخارجي (مشروط)

- يكون التوقيع **مشروطاً** إذا تقدم كيان بطلب الشهادة الأولية. وفي هذه الحالة **يجوز** أن يكون الطلب موقعاً بشكل إضافي من كيان آخر موثوق من السلطة المتلقية لإصدار الشهادات (مثلاً يمكن للسلطة الوطنية للتحقق من الشهادات أن تتحقق من صحة الطلب المقدم من المتحقق من الوثائق والمرسل إلى السلطة الوطنية الأجنبية للتحقق من الشهادات).
- يكون التوقيع **مطلوباً** إذاً تقدم كيان بطلب شهادة متتالية. وفي هذه الحالة **يجب** أن يكون الطلب موقعاً بشكل إضافي من صاحب الطلب باستخدام زوج مفاتيح حديث تم تسجيله سابقاً لدى السلطة المتلقية لإصدار الشهادات.

إذا كان التوقيع الخارجي مستخدماً، **يجب** استخدام مادة بيانات التحقق من الصحة لوضع شهادة السيرة الذاتية (الطلب)، ومرجع سلطة إصدار الشهادات، والتوقيع الإضافي. و**يجب** على مرجع سلطة إصدار الشهادات أن يحدد المفتاح العام المقرر استخدامه للتحقق من التوقيع الإضافي. و**يجب** أن ينشأ التوقيع فوق تسلسل شهادة السيرة الذاتية المرمّزة ومرجع سلطة إصدار الشهادات المرمّز (أي يشمل كل منهما الوسم والطول).

٨-٢ البنى المتعلقة بنقطة الاتصال المفردة

يعرض هذا القسم تفاصيل الرسائل المستخدمة في بروتوكول نقطة الاتصال المفردة.

٨-٢-١ رسالة طلب الشهادة

الاستخدام المقصود:

تستخدم نقطة الاتصال المفردة رسالة طلب الشهادة (RequestCertificate) لطلب توليد شهادة جديدة لأحد المتحققين من الوثائق التابعين لها من سلطة وطنية أجنبية للتحقق من الشهادات.

بارامترات الدخل:

callerID: (إلزامي)

يحتوي هذا البارامتر على معرّف للدولة المصدرة للطلب. و**يجب** أن تكون القيمة هي رمز البلد المكون من حرفين وفقاً للوثيقة Doc 9303-3. و**يجب** أن تتحقق نقطة الاتصال المفردة المتلقية من قيمة callerID بمقارنتها بالقيمة التي تسجلها نقطة الاتصال المفردة المصدرة أثناء تسجيلها.

messageID: (إلزامي)

يحتوي هذا البارامتر على تعريف للرسالة. و**يجب** أن يحدد الرسالة بشكل فريد ضمن جميع الرسائل الصادرة عن المرسل. وإذا كان لا بد من إرسال رسالة رد إلى مُصدر الطلب نتيجة لهذه الرسالة، فإن الرسالة الجوابية ستحتوي على نفس messageID (معرّف الرسالة). وبالتالي يمكن أن تخصص رسالة رد واردة للرسالة الأصلية الصحيحة. وقد يبتّ مُصدر الرسالة بإنشاء وتعيين messageID ولا يتم التحقق من ذلك من قبل الطرف المتلقي.

certReq: (إلزامي)

يحتوي هذا البارامتر على الطلب الفعلي للشهادة. و**يجب** إنشاؤه وفقاً للقسم ٨-١-١. و**يجب** أن يتقيد الترميز بالمواصفات الواردة في القسم ٧-٢-٣-١.

بارامترات الخرج:

certificateSeq: (مشروط)

يحتوي هذا البارامتر على النتيجة (شهادة واحدة أو أكثر) بعد معالجة هذه الرسالة إذا تمت معالجة الرسالة بنجاح وبشكل متزامن من قبل المتلقي. وهذا الأمر **مطلوب** إذا كان لا بد من إرسال الشهادات مع الردّ. و**يجب** أن يكون غير موجود إذا لم ترسل أي شهادة مع الرسالة.

الرموز المرتجعة:

- ok_cert_available: تمت معالجة هذه الرسالة بنجاح وبصورة متزامنة. يحتوي بارامتر الخرج certificateSeq على شهادة واحدة أو أكثر.
- ok_reception_ack: يوجد إشعار باستلام هذه الرسالة. لم تتم بعد زيادة التحقق من الرسالة. وستتم معالجة الرسالة بشكل غير متزامن. وترسل نتيجة المعالجة إلى العنوان الشبكي المسجل باستخدام الرسالة SendCertificates.
- failure_inner_signature: فشل التحقق من التوقيع الداخلي للطلب الفعلي للشهادة.
- failure_outer_signature: فشل التحقق من التوقيع الخارجي للطلب الفعلي للشهادة.
- failure_syntax: الرسالة غير صحيحة من ناحية التركيب النحوي.
- failure_request_not_accepted: تمت معالجة الرسالة بصورة صحيحة ولكن الطلب لم يقبل.
- failure_request_syntax: طلب الشهادة غير صحيح (مثلاً لناحية النحو أو الشكل).
- failure_expired: انتهاء صلاحية الشهادة المقرر استعمالها للتحقق من التوقيع الخارجي للطلب.
- failure_domain_parameters: بارامترات النطاق الواردة في الطلب غير مطابقة لبارامترات النطاق المتعلقة بشهادة السلطة الوطنية للتحقق من الشهادات المخصصة لتوقيع الشهادة المطلوبة للمتحقق من الوثائق.
- failure_internal_error: خطأ غير الأخطاء الواردة أعلاه.

ملاحظات:

ينبغي أن يحتوي متن طلب الشهادة على مرجع سلطة إصدار الشهادات لإطلاع السلطة الوطنية للتحقق من الشهادات على المفتاح الخاص الذي يتوقع أن يستخدمه الطالب للتوقيع على الشهادة. وإذا اختلف مرجع سلطة إصدار الشهادات في الطلب عن المرجع في الشهادة الصادرة، **يجب** أن يتوفر أيضاً في الرد الشهادة المقابلة الخاصة بالسلطة الوطنية للتحقق من الشهادات. في هذه الحالة، وإذا تمت معالجة الرسالة بصورة متزامنة، **يجب** أن تكون الشهادة الخاصة بالسلطة الوطنية للتحقق من الشهادات جزءاً من البارامتر الخارجي certificateSeq. و**يجب** أن تكون شهادة المتحقق من الوثائق أول شهادة في المتتالية. و**يجب** ترتيب شهادات السلطة الوطنية للتحقق من الشهادات (الأساسية و/أو المرتبطة بها) بحسب التاريخ الفعلي (التصاعدي) في المتتالية.

٨-٢-٢ *رسالة إرسال الشهادات*

الاستخدام المقصود:

تستخدم نقطة الاتصال المفردة الرسالة (SendCertificates) لإرسال الشهادة الجديدة أو سلسلة الشهادات إلى نقطة الاتصال المفردة الطالبة. ويجب توليد هذه الرسالة جواباً على:

- RequestCertificate: فور معالجة ناجحة وغير متزامنة للطلب بعد إصدار الشهادة؛
- GetCACertificates.

بالإضافة إلى ذلك، **يجب** استخدام الرسالة عند إنشاء شهادة جديدة (أساسية أو متصلة بالسلطة الوطنية للتحقق من الشهادات) لدفع الشهادات إلى نقطة الاتصال المفردة الاجنبية المسجلة.

بارامترات الدخل:

callerID: (إلزامي)

يحتوي هذا البارامتر على معرّف للدولة المصدرة. و**يجب** أن تكون القيمة هي رمز البلد المكون من حرفين وفقاً للوثيقة Doc 9303-3. و**يجب** أن تتحقق نقطة الاتصال المفردة المتلقية من قيمة callerID بمقارنتها بالقيمة التي تسجلها نقطة الاتصال المفردة المصدرة أثناء تسجيلها.

messageID: (مشروطا)

عند توليد الرسالة رداً على رسالة الطلب، **يجب** أن يحتوي هذا البارامتر على القيمة نفسها الواردة في البارامتر message ID الوارد في رسالة الطلب. وعند إطلاق عملية توليد الرسائل دون تدخل خارجي (المفتاح المعاد صنعه لشهادة السلطة الوطنية للتحقق من الشهادات)، **يجب** أن تكون statusInfo بقيمة new_cert_available_notification و**يجوز** إغفال البارامتر messageID و**يجب** تجاهله في حال وجوده.

statusInfo: (إلزامي)

يحتوي هذا البارامتر على رمز لحالة نتيجة معالجة الرسالة المقابلة. وفيما يلي الحالات المحتملة:

- new_cert_available_notification: ترغب نقطة الاتصال المفردة في الإبلاغ بأن شهادة (شهادات) جديدة للسلطة الوطنية للتحقق من الشهادات متوفرة دون تقديم طلب لذلك.
- ok_cert_available: تمت معالجة الطلب بنجاح. يحتوي البارامتر الداخلي certificateSeq على شهادة واحدة أو أكثر.
- failure_inner_signature: فشل التحقق من التوقيع الداخلي للطلب الفعلي للشهادة.
- failure_outer_signature: فشل التحقق من التوقيع الخارجي للطلب الفعلي للشهادة.
- failure_syntax: الرسالة غير صحيحة من ناحية التركيب النحوي.
- failure_request_not_accepted: تمت معالجة الرسالة بصورة صحيحة ولكن الطلب لم يقبل.
- failure_certificate: واحدة أو أكثر من الشهادات المرسلة ليست صحيحة (لناحية التركيب النحوي أو التوقيع)
- failure_internal_error: خطأ غير الأخطاء الواردة أعلاه (مشروط).

يكون هذا البارامتر **مطلوباً** إذا كان لا بد من إرسال الشهادات مع الرسالة. و**يجب** أن يكون غائباً في حال عدم إرسال شهادات مع الرسالة. و**يجب** أن تكون الشهادات ثنائية TLV DER ومرمّزة على النحو المحدد في القسم ٧-٢-٣.

عند توليد الرسالة كردّ على الرسالة GetCACertificates، أو بسبب وجود شهادة جديدة، **يجب** أن تحتوي المتتالية على قائمة شهادات سلطة إصدار الشهادات. و**يجب** أن تكون القائمة مرتّبة. ويجب أن تكون شهادات السلطة الوطنية للتحقق من الشهادات (الأساسية والمرتبطة بها) مرتبة بحسب التاريخ الفعلي في المتتالية. وإذا كانت المتتالية تحتوي على شهادات ذات بارامترات نطاق مختلفة، **يجب** أن توجد شهادة واحدة على الأقل ذات بارامترات نطاق مدرجة لكل نوع من بارامترات النطاق. و**يجب** أن تكون جميع الشهادات الحالية لسلطة إصدار الشهادات مدرجة.

وعند توليد الرسالة كردّ على الرسالة RequestCertificate، يكون محتوى المتتالية هو نفسه الوارد في الرد المتزامن للطلب RequestCertificate.

بارامترات الخرج:

لا يوجد.

الرموز المرتجعة:

- ok_received_correctly: تم تلقي الرسالة بشكل صحيح.
- failure_syntax: الرسالة غير صحيحة من ناحية التركيب النحوي.
- failure_messageID_unknown: لا يمكن مطابقة messageID الوارد مع الرسالة التي أرسلت سابقاً.
- failure_internal_error: خطأ غير الأخطاء الواردة أعلاه.

٨-٢-٣ *رسالة الحصول على شهادات سلطة إصدار الشهادات*

الاستخدام المقصود:

ترسل هذه الرسالة بواسطة البروتوكول SPOC إلى بروتوكول SPOC أجنبي للحصول على شهادات صالحة للسلطة الوطنية للتحقق من الشهادات (شهادات مرتبطة لها وشهادات موقّعة ذاتياً) في تلك الدولة.

بارامترات الدخل:

callerID: (إلزامي)

يحتوي هذا البارامتر على معرّف للدولة المصدرة. و**يجب** أن تكون القيمة هي رمز البلد المكون من حرفين وفقاً للوثيقة Doc 9303-3. و**يجب** أن يتحقق بروتوكول SPOC المتلقي من قيمة callerID بمقارنتها بالقيمة التي يسجلها البروتوكول SPOC المصدر أثناء تسجيله.

messageID: (إلزامي)

يحتوي هذا البارامتر على تعريف للرسالة. و**يجب** أن يعرّف الرسالة بصورة فريدة ضمن جميع الرسائل الصادرة. وإذا كان لا بد من إرسال رسالة جوابية إلى المرسل كنتيجة لهذه الرسالة، يجب أن تحتوي الرسالة الجوابية على نفس messageID. وبالتالي يمكن تخصيص رسالة جوابية واردة إلى الرسالة الأصلية الصحيحة. ويمكن البتّ بإنشاء وتخصيص messageID بواسطة مُصدر الرسالة.

بارامترات الخرج:

certificateSeq: (مشروط)

يحتوي هذا البارامتر على النتيجة (شهادة واحدة أو أكثر) بعد معالجة هذه الرسالة إذا تمت معالجة الرسالة بنجاح وبشكل متزامن من قبل المتلقي. وهذا الأمر **مطلوب** إذا كان لا بد من إرسال الشهادات مع الردّ. و**يجب** أن يكون غير موجود إذا لم ترسل أي شهادة مع الرسالة.

الرموز المرتجعة:

- ok_cert_available: تمت معالجة هذه الرسالة بنجاح وبصورة متزامنة. يحتوي بارامتر الخرج certificateSeq على شهادة واحدة أو أكثر من شهادات سلطة إصدار الشهادات.
- ok_reception_ack: يوجد إشعار باستلام هذه الرسالة. لم تتم بعد زيادة التحقق من الرسالة. وستتم معالجة الرسالة بشكل غير متزامن. وترسل نتيجة المعالجة إلى العنوان الشبكي المسجل باستخدام الرسالة SendCertificates.

- failure_syntax: الرسالة غير صحيحة من ناحية التركيب النحوي.
- failure_internal_error: خطأ غير الأخطاء الواردة أعلاه.

ملاحظات:

إذا تمت معالجة الرسالة بنجاح وتم قبولها، **يجب** على السلطة الوطنية للتحقق من الشهادات أن ترسل ضمن الردّ جميع الشهادات الصالحة للسلطة الوطنية للتحقق من الشهادات، إما في بارامتر الخرج certificateSeq (معالجة متزامنة) أو في الرسالة الجوابية المقابلة SendCertificates (معالجة غير متزامنة)

٨-٢-٤ *الرسائل العامة*

الاستخدام المقصود:

ترسل هذه الرسالة بواسطة البروتوكول SPOC إلى بروتوكول SPOC أجنبي من أجل إرسال تبليغ أو رسالة نصية عامة مقروءة من البشر.

بارامترات الدخل:

callerID: (إلزامي)

يحتوي هذا البارامتر على معرّف للدولة المصدرة. و**يجب** أن تكون القيمة هي رمز البلد المكون من حرفين وفقاً للوثيقة Doc 9303-3. و**يجب** أن يتحقق بروتوكول SPOC المتلقي من قيمة callerID بمقارنتها بالقيمة التي يسجلها البروتوكول SPOC المصدر أثناء تسجيله، بما في ذلك السمات الأمنية للرسالة (شهادة التوقيع الرقمي/ شهادة عميل أمن طبقة مسجلة بالنسبة للدولة ذات الصلة).

messageID: (إلزامي)

يحتوي هذا البارامتر على تعريف للرسالة. و**يجب** أن يعرّف الرسالة بصورة فريدة ضمن جميع الرسائل الصادرة. وإذا كان لا بد من إرسال رسالة جوابية إلى المرسل كنتيجة لهذه الرسالة، يجب أن تحتوي الرسالة الجوابية على نفس messageID. وبالتالي يمكن تخصيص رسالة جوابية واردة إلى الرسالة الأصلية الصحيحة. ويمكن البتّ بإنشاء وتخصيص messageID بواسطة مُصدر الرسالة.

subject: (إلزامي)

يحتوي هذا البارامتر على موضوع الرسالة. و**ينبغي** أن يصف الموضوع محتوى متن الرسالة. و**يجب** استخدام اللغة الإنجليزية للموضوع.

المتن: (إلزامي)

يحتوي هذا البارامتر على متن الرسالة. و**ينبغي** أن يكون المتن عبارة عن نص بسيط مقروء من البشر وأن لا يكون مخصصاً للمعالجة الآلية المباشرة. و**يجب** استخدام اللغة الإنجليزية للمتن.

الرموز المرتجعة:

- ok: تم قبول الرسالة للتسليم.
- failure_syntax: الرسالة غير صحيحة من ناحية التركيب النحوي.
- failure_internal_error: خطأ غير الأخطاء الواردة أعلاه.

٨-٣ خدمة شبكة الويب

واجهة خدمة شبكة الويب هي الواجهة المتعلقة بالتبادل الروتيني السلكي للبيانات فيما بين نقاط الامتثال المفردة. و**يجب** أن تستخدم الواجهة البروتوكول [SOAP] فوق البروتوكول [HTTPS]. و**يجب** أن تمتثل واجهة خدمة شبكة الويب SOAP للغة WSDL المحددة في القسم ٨-٣-٣.

٨-٣-١ استخدام البروتوكول SOAP

يجب استخدام البروتوكول [SOAP] الصرف فوق [HTTPS] لتنفيذ واجهات خدمة شبكة الويب. و**يجب عدم** استخدام امتدادات SOAP الأخرى (مثل WS-Addressing، وWS-Security، وWS-Secure Conversation، وWS-Authorizatio، وWS-Federation، وWSAuthorization، وWS-Policy، وWS-Trust ، وWS-Privacy، وWS-Test، وغير ذلك من امتدادات خدمات الويب).

و**يجب عدم** استخدام نوع عقد SOAP المتوسطة. ويجب فقط استخدام تشكيلة مباشرة من نقطة الاتصال المفردة للعميل ونقطة الاتصال المفردة للمخدّم.

و**يجب** عدم استخدام عنصر الخطأ في SOAP إلا عند حدوث خطأ في طبقة النقل لا تشمله هذه المواصفة. و**يجب** الإبلاغ عن أخطاء مستوى التطبيق كردود عادية للبروتوكول SOAP باستخدام آلية الخطأ على النحو المحدد في كل رسالة.

و**يوصى** بتنفيذ واجهة خدمة الويب وفقاً لـ [WS-IBP] و[WSI-SSBP].

ويجب أن تمتثل واجهة البروتوكول SOAP في نقطة الاتصال المفردة لتعاريف لغة WSDL المحددة في القسم ٨-٣-٣.

٨-٣-٢ الاعتبارات الأمنية

يجب أن تستخدم اتصالات خدمة الويب لنقطة الاتصال المفردة قناة آمنة ومتحقق من صحتها. و**يجب** استخدام البروتوكول [SOAP] فوق [HTTPS]. و**يجب** استخدام الإصدار ١,٢ لأمن طبقة النقل.

و**يجب** أن يقوم عميل أمن طبقة النقل بعمليات التحقق التالية:

- **يجب** المصادقة تماماً على شهادة المخدّم وفقاً لـ[RFC5280] بما في ذلك حالة الإلغاء؛
- و**يجب** أن يكون امتداد شهادة المخدّم ExtKeyUsage موجوداً و**يجب** أن يحتوي على معرّفات المواد وفقاً لشهادة مخدّم أمن طبقة النقل الواردة في القسم ٧-٢-١؛
- و**يجب** أن يكون بلد موضوع شهادة المخدّم مساوياً لقيمة البارامتر callerID. وفي حال الفشل **يجب** على عميل أمن طيقة النقل أن يقطع الاتصال.

و**يجب** أن يقوم مخدّم أمن طبقة النقل بعمليات التحقق التالية:

- **يجب** المصادقة تماماً على العميل باستخدام الشهادة؛
- و**يجب** المصادقة تماماً على شهادة العميل وفقاً لـ[RFC5280] بما في ذلك حالة الإلغاء؛
- و**يجب** أن يكون امتداد شهادة العميل ExtKeyUsage موجوداً و**يجب** أن يحتوي على معرّفات المواد وفقاً لشهادة عميل أمن طبقة النقل الواردة في للقسم ٧-٢-١؛
- و**يجب** أن يكون بلد موضوع شهادة العميل مقابلاً للموضوع المقصود.

في حال فشل بعض عمليات التحقق **يجب** رفض الطلب باستخدام رمز الردّ غير المرخّص في البروتوكول HTTP 401.

وفي نطاق التفاوض بإقامة اتصال بأمن طبقة النقل، **يجب** على العميل أن يدعم مجموعات شفرات أمن طبقة النقل المحددة في القسم ٤-٢-٢. و**يجب** على كل من المخدّم والعميل أن يدعم التحق من صحة خوارزمية التوقيع الرقمي أو خوارزمية التوقيع الرقمي للمنحنى الإهليلجي. ويسمح للمخدّم بطلب شهادة عميل من نوع مختلف عن شهادة المخدّم وللعميل أيضاً بإرسالها.

ويعتبر استخدام اتفاق مفاتيح ECDHE_ECDSA في اتصال أمن طبقة النقل متوافقاً مع الإضافات المحددة في [TLSECC] و[TLS1.2] و[TLSEXT]. و**يجب** على كل من العميل والمخدّم أن يدعم الامتدادات المناسبة للمنحنيات الإهليلجية حسبما هو محدد في المواصفة [TLSECC] في نطاق اتصال أمن طبقة النقل. وتحدد المنحنيات الإهليلجية المدعومة وأشكال نقاط المنحنيات الإهليلجية في القسم ٥ من [TLSECC]. و**يجب** أن يكون استخدام مجموعات شفرات أمن طبقة النقل المحددة في القسم ٤-٢-٢، التي تستخدم القاعدة القياسية للتشفير المتقدم للتشفير متوافقة مع المواصفة [TLSAES].

٨-٣-٣ لغة *WDSL من أجل واجهة خدمة الويب*

التالية:WSDL لنقطة الاتصال المفردة مع تعاريف لغة SOAP **يجب** أن تتطابق واجهة البروتوكول

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:SPOC="http://namespaces.icao.int/lds2"
  targetNamespace="http://namespaces. icao.int/lds2">

  <wsdl:types>
    <xs:schema xmlns="http://namespaces.icao.int/lds2"
      targetNamespace="http://namespaces." elementFormDefault="qualified"
      attributeFormDefault="unqualified">
      <xs:element name="certificateSequence">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="certificate" type="xs:base64Binary" minOccurs="1"
maxOccurs="unbounded"/>
          </xs:sequence>
      </xs:complexType>
      </xs:element>
      <xs:element name="RequestCertificateRequest">
      <xs:complexType>
        <xs:sequence>
            <xs:element name="callerID" type="xs:string"/>
            <xs:element name="messageID" type="xs:string"/>
            <xs:element name="certificateRequest" type="xs:base64Binary"/>
        </xs:sequence>
      </xs:complexType>
      </xs:element>
      <xs:element name="RequestCertificateResponse">
      <xs:complexType>
        <xs:sequence>
            <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
            <xs:element name="result">
           <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:enumeration value="ok_cert_available"/>
                <xs:enumeration value="ok_reception_ack"/>
                <xs:enumeration value="failure_inner_signature"/>
                <xs:enumeration value="failure_outer_signature"/>
                <xs:enumeration value="failure_syntax"/>
                <xs:enumeration value="failure_request_not_accepted"/>
```

```
            <xs:enumeration value="failure_request_syntax"/>
            <xs:enumeration value="failure_expired"/>
            <xs:enumeration value="failure_domain_parameters"/>
            <xs:enumeration value="failure_internal_error"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
 </xs:element>
 <xs:element name="SendCertificatesRequest">
<xs:complexType>
  <xs:sequence>
      <xs:element name="callerID" type="xs:string"/>
      <xs:element name="messageID" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
      <xs:element name="statusInfo">
     <xs:simpleType>
         <xs:restriction base="xs:string">
           <xs:enumeration value="new_cert_available_notification"/>
           <xs:enumeration value="ok_cert_available"/>
           <xs:enumeration value="failure_inner_signature"/>
           <xs:enumeration value="failure_outer_signature"/>
           <xs:enumeration value="failure_syntax"/>
           <xs:enumeration value="failure_request_not_accepted"/>
           <xs:enumeration value="failure_certificate"/>
           <xs:enumeration value="failure_internal_error"/>
       </xs:restriction>
     </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
 </xs:element>
 <xs:element name="SendCertificatesResponse">
<xs:complexType>
      <xs:sequence>
      <xs:element name="result">
     <xs:simpleType>
         <xs:restriction base="xs:string">
           <xs:enumeration value="ok_received_correctly"/>
           <xs:enumeration value="failure_syntax"/>
           <xs:enumeration value="failure_messageID_unknown"/>
           <xs:enumeration value="failure_internal_error"/>
       </xs:restriction>
     </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
 </xs:element>
 <xs:element name="GetCACertificatesRequest">
<xs:complexType>
  <xs:sequence>
      <xs:element name="callerID" type="xs:string"/>
      <xs:element name="messageID" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
 </xs:element>
 <xs:element name="GetCACertificatesResponse">
<xs:complexType>
  <xs:sequence>
      <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
      <xs:element name="result">
     <xs:simpleType>
         <xs:restriction base="xs:string">
           <xs:enumeration value="ok_cert_available"/>
           <xs:enumeration value="ok_reception_ack"/>
           <xs:enumeration value="failure_syntax"/>
           <xs:enumeration value="failure_internal_error"/>
```

```
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
   </xs:element>
   <xs:element name="GeneralMessageRequest">
    <xs:complexType>
      <xs:sequence>
          <xs:element name="callerID" type="xs:string"/>
          <xs:element name="messageID" type="xs:string"/>
          <xs:element name="subject" type="xs:string"/>
          <xs:element name="body" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
   </xs:element>
   <xs:element name="GeneralMessageResponse">
    <xs:complexType>
      <xs:sequence>
          <xs:element name="result">
          <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:enumeration value="ok"/>
                <xs:enumeration value="failure_syntax"/>
                <xs:enumeration value="failure_internal_error"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  </xs:schema>
</wsdl:types>

<wsdl:message name="RequestCertificateRequest">
  <wsdl:part name="RequestCertificateRequest" element="SPOC:RequestCertificateRequest"/>
</wsdl:message>
<wsdl:message name="RequestCertificateResponse">
  <wsdl:part name="RequestCertificateResponse" element="SPOC:RequestCertificateResponse"/>
</wsdl:message>

<wsdl:message name="SendCertificatesRequest">
  <wsdl:part name="SendCertificatesRequest" element="SPOC:SendCertificatesRequest"/>
</wsdl:message>
<wsdl:message name="SendCertificatesResponse">
  <wsdl:part name="SendCertificatesResponse" element="SPOC:SendCertificatesResponse"/>
</wsdl:message>

<wsdl:message name="GetCACertificatesRequest">
  <wsdl:part name="GetCACertificatesRequest" element="SPOC:GetCACertificatesRequest"/>
</wsdl:message>
<wsdl:message name="GetCACertificatesResponse">
  <wsdl:part name="GetCACertificatesResponse" element="SPOC:GetCACertificatesResponse"/>
</wsdl:message>

<wsdl:message name="GeneralMessageRequest">
  <wsdl:part name="GeneralMessageRequest" element="SPOC:GeneralMessageRequest"/>
</wsdl:message>
<wsdl:message name="GeneralMessageResponse">
  <wsdl:part name="GeneralMessageResponse" element="SPOC:GeneralMessageResponse"/>
</wsdl:message>

<wsdl:portType name="SPOCPortType">
  <wsdl:operation name="RequestCertificate">
    <wsdl:input message="SPOC:RequestCertificateRequest"/>
    <wsdl:output message="SPOC:RequestCertificateResponse"/>
  </wsdl:operation>
  <wsdl:operation name="SendCertificates">
```

```
    <wsdl:input message="SPOC:SendCertificatesRequest"/>
    <wsdl:output message="SPOC:SendCertificatesResponse"/>
   </wsdl:operation>
   <wsdl:operation name="GetCACertificates">
    <wsdl:input message="SPOC:GetCACertificatesRequest"/>
    <wsdl:output message="SPOC:GetCACertificatesResponse"/>
   </wsdl:operation>
   <wsdl:operation name="GeneralMessage">
    <wsdl:input message="SPOC:GeneralMessageRequest"/>
    <wsdl:output message="SPOC:GeneralMessageResponse"/>
   </wsdl:operation>
  </wsdl:portType>

  <wsdl:binding name="SPOCSOAPBinding" type="SPOC:SPOCPortType">
   <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
   <wsdl:operation name="RequestCertificate">
    <soap:operation soapAction="RequestCertificate"/>
  <wsdl:input>
        <soap:body parts="RequestCertificateRequest" use="literal"/>
    </wsdl:input>
    <wsdl:output>
     <soap:body parts="RequestCertificateResponse" use="literal"/>
    </wsdl:output>
 </wsdl:operation>
   <wsdl:operation name="SendCertificates">
    <soap:operation soapAction="SendCertificates"/>
    <wsdl:input>
     <soap:body parts="SendCertificatesRequest" use="literal"/>
  </wsdl:input>
    <wsdl:output>
     <soap:body parts="SendCertificatesResponse" use="literal"/>
    </wsdl:output>
 </wsdl:operation>
   <wsdl:operation name="GetCACertificates">
    <soap:operation soapAction="GetCACertificates"/>
    <wsdl:input>
     <soap:body parts="GetCACertificatesRequest" use="literal"/>
  </wsdl:input>
    <wsdl:output>
     <soap:body parts="GetCACertificatesResponse" use="literal"/>
    </wsdl:output>
 </wsdl:operation>
   <wsdl:operation name="GeneralMessage">
    <soap:operation soapAction="GeneralMessage"/>
    <wsdl:input>
     <soap:body parts="GeneralMessageRequest" use="literal"/>
  </wsdl:input>
    <wsdl:output>
     <soap:body parts="GeneralMessageResponse" use="literal"/>
    </wsdl:output>
 </wsdl:operation>
  </wsdl:binding>

  <wsdl:service name="SPOC">
   <wsdl:port name="SPOCPort" binding="SPOC:SPOCSOAPBinding">
    <soap:address location="http://spoc-server/SPOC"/>
   </wsdl:port>
  </wsdl:service>
 </wsdl:definitions>
```

٩- بنية القائمة الرئيسية للسلطة الوطنية المعنية بالتوقيع على الشهادات

Master Lists are implemented as instances of the `ContentInfo` Type, as specified in [RFC 5652]. The `ContentInfo` MUST contain a single instance of the `SignedData` Type as profiled below. No other data types are included in the `ContentInfo`. All Master Lists MUST be produced in DER format to preserve the integrity of the signatures within them.

9.1 SignedData Type

تطبق قواعد المعالجة الواردة في [RFC 3852]:

The specification of Master List structure uses the following terminology for presence requirements of each field.

m mandatory — the field MUST be present
r recommended — the field SHOULD be present
x do not use — the field MUST NOT be present
o optional — the field MAY be present.

الجدول ١٨ — القائمة الرئيسية

Value		*Comments*
`SignedData`		
`Version`	m	Value = `v3`
`digestAlgorithms`	m	
`encapContentInfo`	m	
`eContentType`	m	`id-icao-cscaMasterList`
`eContent`	m	The encoded contents of an `cscaMasterList`
`Certificates`	m	The Master List Signer certificate MUST be included and the CSCA certificate, which can be used to verify the signature in the `signerInfos` field SHOULD be included.
`Crls`	x	
`signerInfos`	m	It is RECOMMENDED that States only provide 1 `signerinfo` within this field.
`SignerInfo`	m	
`Version`	m	The value of this field is dictated by the `sid` field. See [RFC 5652] for rules regarding this field
`Sid`	m	
`subjectKeyIdentifier`	r	It is RECOMMENDED that this field be supported rather than `issuerandSerialNumber`.
`digestAlgorithm`	m	The algorithm identifier of the algorithm used to produce the hash value over `encapsulatedContent` and `SignedAttrs`. See note below.

Value		*Comments*
`signedAttrs`	m	Additional attributes may be included. However these do not have to be processed by Receiving States except to verify the signature value. `signedAttrs` MUST include signing time (see [PKCS #9]).
`signatureAlgorithm`	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters. See note below.
`signature`	m	The result of the signature generation process.
`unsignedAttrs`	o	Although this field MAY be included, Receiving States may choose to ignore it.

Note.— `DigestAlgorithmIdentifiers` MUST omit "`NULL`" parameters, while the `SignatureAlgorithmIdentifier` (as defined in RFC 3447) MUST include `NULL` as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Implementations MUST accept `DigestAlgorithmIdentifiers` with both conditions, absent parameters or with `NULL` parameters.

9.2 ASN.1 Master List Specification

```
CscaMasterList
{ joint-iso-itu-t(2) international-organization(23) icao(136) mrtd(1)
security(1) masterlist(2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

 -- Imports from RFC 5280 [PROFILE], Appendix A.1
     Certificate
       FROM PKIX1Explicit88
         { iso(1) identified-organization(3) dod(6)
           internet(1) security(5) mechanisms(5) pkix(7)
             mod(0) pkix1-explicit(18) };
-- CSCA Master List

CscaMasterListVersion ::= INTEGER {v0(0)}

CscaMasterList ::= SEQUENCE {
  version            CscaMasterListVersion,
  certList           SET OF Certificate }

-- Object Identifiers

id-icao-cscaMasterList OBJECT IDENTIFIER ::=
                                  {id-icao-mrtd-security 2}
id-icao-cscaMasterListSigningKey OBJECT IDENTIFIER ::=
                                  {id-icao-mrtd-security 3}
END
```

١٠- بنية قائمة الانحرافات

يتم تنفيذ قائمة الانحرافات على شكل نوع بيانات موقّعة SignedData، كما هو محدد في [RFC 3852]. ويجب أن تُعدّ جميع قوائم الانحرافات بشكل قاعدة الترميز المميّز (DER) للحفاظ على سلامة التواقيع الموجودة فيها.

يكون مدى الانحرافات محدوداً بما يلي:

- مدى البيانات (بما في ذلك تاريخ الإصدار وتاريخ انتهاء الصلاحية)؛
- اسم هيئة الإصدار ورقمه التسلسلي؛
- معرّف مفتاح الموضوع الخاص بشهادة التوقيع الرقمي؛
- قائمة أرقام وثائق السفر الإلكترونية المقروءة آلياً.
- وتستخدم توليفات مناسبة من هذه القيم للحد بدقة من مدى وثائق السفر الإلكترونية المقروءة آلياً المتأثرة. وعند الجمع بين القيم، يتعين معالجتها كما لو أنها مجموعة بالعامل "AND". وليس هناك خيار لمعالجة القيم المجموعة بالعامل "OR".

١٠-١ نوع البيانات الموقّعة

تطبق قواعد المعالجة الواردة في [RFC 3852]:

m mandatory — the field MUST be present
r recommended — the field SHOULD be present
x do not use — the field MUST NOT be present
o optional — the field MAY be present.

الجدول ١٩ — قائمة الانحرافات

Value		Comments
SignedData		
version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-DeviationList
eContent	m	The encoded contents DeviationList
certificates	m	States MUST include the Deviation List Signer certificate and SHOULD include the CSCA certificate, which can be used to verify the signature in the signerInfos field.
crls	x	
signerInfos	m	It is RECOMMENDED that States provide only 1 signerInfo within this field.
SignerInfo	m	

Value		Comments
version	m	The value of this field is dictated by the sid field. See [RFC 3852] Section 5.3 for rules regarding this field.
sid	m	
subjectKeyIdentifier	r	It is RECOMMENDED that States support this field over issuerandSerialNumber.
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value. signedAttrs MUST include signing time (ref. PKCS#9).
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters.
signature	m	The result of the signature generation process.
unsignedAttrs	x	

٢-١٠ المواصفة ASN.1

```
DeviationList
{ joint-iso-itu-t (2) international-organization(23) icao(136) mrtd(1) security(1)
deviationlist(7)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

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

  -- Imports from RFC 3852
       SubjectKeyIdentifier, Digest, IssuerAndSerialNumber
          FROM CryptographicMessageSyntax2004
                 { iso(1) member-body(2) us(840) rsadsi(113549)
                   pkcs(1) pkcs-9(9) smime(16) modules(0)
                   cms-2004(24) };

DeviationListVersion ::= INTEGER {v0(0)}

DeviationList ::= SEQUENCE {
 version      DeviationListVersion,
 digestAlgorithm AlgorithmIdentifier OPTIONAL,
 deviations   SET OF Deviation
}

Deviation ::= SEQUENCE{
 documents       DeviationDocuments,
 descriptions SET OF DeviationDescription
}

DeviationDescription ::= SEQUENCE{
 description     PrintableString OPTIONAL,
```

```
 deviationType   OBJECT IDENTIFIER,
 parameters  [0] ANY DEFINED BY deviationType OPTIONAL,
 nationalUse     [1] ANY OPTIONAL

 -- The nationalUse field is for internal State use, and is not governed
 -- by an ICAO specification.
}

DeviationDocuments ::= SEQUENCE {
 documentType    [0] PrintableString (SIZE(2)) OPTIONAL,
          -- per MRZ, e.g. 'P'
 dscIdentifier   DocumentSignerIdentifier OPTIONAL,
 issuingDate     [4] IssuancePeriod OPTIONAL,
 documentNumbers    [5] SET OF PrintableString OPTIONAL
}

DocumentSignerIdentifier ::= CHOICE{
 issuerAndSerialNumber [1] IssuerAndSerialNumber,
 subjectKeyIdentifier [2] SubjectKeyIdentifier,
 certificateDigest  [3] Digest   -- if used, digestAlgorithm must be present in
DeviationList
}

IssuancePeriod ::= SEQUENCE {
 firstIssued   GeneralizedTime,
 lastIssued   GeneralizedTime
}

-- CertField is used to define which part of a certificate is
  affected by a coding error. Parts of the Body are identified by
  the corresponding value of CertificateBodyField, extensions
  by the corresponding OID identifying the extension.

CertField ::= CHOICE {
 body  CertificateBodyField,
 extension OBJECT IDENTIFIER
}
CertificateBodyField ::= INTEGER {
 generic(0), version(1), serialNumber(2), signature(3), issuer(4),
 validity(5), subject(6), subjectPublicKeyInfo(7),
 issuerUniqueID(8), subjectUniqueID(9)
}

Datagroup ::= INTEGER
              {dg1(1), dg2(2), dg3(3), dg4(4), dg5(5), dg6(6),
               dg7(7), dg8(8), dg9(9), dg10(10), dg11(11),
               dg12(12), dg13(13), dg14(14), dg15(15), dg16(16),
               sod(20), com(21)}

MRZField ::= INTEGER
             {generic(0), documentCode(1), issuingState(2), personName(3),
              documentNumber(4), nationality(5), dateOfBirth(6),
              sex(7), dateOfExpiry(8), optionalData(9)}

-- Base Object Identifiers

id-icao OBJECT IDENTIFIER ::= {2 23 136 }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-security 8}

-- Deviation Object Identifiers and Parameter Definitions

id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}
id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 1}
id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 2}
id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 3}
id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 4}
```

```
id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}
id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}
id-Deviation-LDS-DGHashWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 2}
id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 3}
id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}
id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}
id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

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

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

END
```

١١- المراجع (معيارية)

FIPS 180-2	FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, *Secure Hash Standard*, August 2002.
FIPS 186-4	FIPS 186-4, Federal Information Processing Standards Publication (FIPS PUB) 186-4, *Digital Signature Standard (DSS)*, July 2013 (Supersedes FIPS PUB 186-3 dated June 2009).
ISO 3166-1	ISO/IEC 3166-1: 2006, Codes for the representation of names of countries and their subdivisions — Part 1: Country Codes.
ISO/IEC 15946	ISO/IEC 15946: 2002, Information technology — Security techniques — Cryptographic techniques based on elliptic curves.
RFC 3280	RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.
RFC 4055	RFC 4055, J. Schaad, B. Kaliski, R. Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, June 2005.
RFC 5652	RFC 5652, R. Housley, Cryptographic Message Syntax, September 2009.
RFC 5280	RFC 5280, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May, 2008.
TR 03111	BSI TR-03111: Elliptic Curve Cryptography v 2.0, 2012.
X9.62	X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 7 January 1999.
X.509	ITU-T X.509 | ISO/IEC 9594-8, 2008: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
X.690	ITU-T X.690 2008: Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
RFC-RSA	Jonsson, Jakob and Kaliski, Burt RFC 3447, Public-key cryptography standards (PKCS)#1: RSA cryptography specifications version 2.1, 2003
PKCS#1	RSA Laboratories RSA Laboratories Technical Note, PKCS#1 v2.2: RSA cryptography standard, 2012
TLSAES	Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002

TLSECC	Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006
TLS1.2	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008
TLSEXT	Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006
SOAP	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation 27 April 2007
HTTPS	E. Rescorla., "HTTP Over TLS", RFC 2818, May 2000
WSI-BP	WS-I Basic Profile available at http://www.ws-i.org/Profiles/BasicProfile-1.1.html
WSI-SSBP	WS-I Basic Binding available at http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html

— — — — — — — —

المرفق (أ) بالجزء ١٢

الأعمار (إعلامية)

تبيّن الأمثلة التالية حساب فترات استخدام المفتاح الخاص وصلاحية شهادة المفتاح العام للسيناريوهات المختلفة على النحو الموصوف في القسم ٤.

أ-١ المثال ١

يبيّن المثال الأول سيناريو تكون فيه وثائق السفر الالكترونية المقروءة آلياً صالحة لخمس سنوات. ولأن عدداً كبيراً نسبياً من وثائق السفر الالكترونية المقروءة آلياً يصدر في اليوم، فإن السياسة هي ابقاء فترات استخدام المفتاح الخاص وصلاحية شهادة المفتاح العام في حدٍّ أدنى. ولهذا المثال، فإن فترة الاستخدام الدنيا للمفتاح الخاص لشهادات الجهة الموقّعة على الوثيقة هي شهر واحد.

البند	فترة الاستخدام / الصلاحية
صلاحية وثيقة السفر الالكترونية المقروءة آلياً	٥ سنوات
فترة استخدام المفتاح الخاص للجهة الموقّعة على الوثيقة	١ شهر
صلاحية شهادة الجهة الموقّعة على الوثيقة	خمس سنوات + ١ شهر
فترة استخدام المفتاح الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات	٣ سنوات
صلاحية شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات	٨ سنوات + ١ شهر

نتائج هذا المثال هي أنه في الوقت الذي تصبح فيه أول شهادة للسلطة الوطنية المعنية بالتوقيع على الشهادات غير صالحة فإنه ستكون قد أُصدرَت ٣٦ شهادة على الأقل للجهة الموقّعة على الوثيقة (واحدة مناظرة لكل مفتاح خاص له فترة استخدام لشهر واحد). وفي الأشهر القليلة الأخيرة قبل أن تصبح شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات غير صالحة، ستوجد على الأقل شهادتان إضافيتان صادرتان عن السلطة الوطنية المعنية بالتوقيع على الشهادات (واحدة مناظرة لكل مفتاح خاص له فترة استخدام لثلاث سنوات).

أ-٢ المثال ٢

يبيّن المثال الثاني سيناريو تكون فيه وثائق السفر الالكترونية المقروءة آلياً صالحة لعشر سنوات. والسياسة هي ابقاء صلاحية فترات استخدام المفتاح الخاص وصلاحية شهادة المفتاح العام لطولٍ متوسطٍ.

البند	الاستخدام / فترة الصلاحية
صلاحية وثيقة السفر الالكترونية المقروءة آلياً	١٠ سنوات

البند	الاستخدام / فترة الصلاحية
فترة استخدام المفتاح الخاص للجهة الموقّعة على الوثيقة	٢ شهران
صلاحية شهادة الجهة الموقّعة على الوثيقة	١٠ سنوات + ٢ شهران
فترة استخدام المفتاح الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات	٤ سنوات
صلاحية شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات	١٤ سنة + ٢ شهران

نتائج هذا المثال هي أنه بحلول الوقت الذي تصبح فيه الشهادة الأولى للسلطة الوطنية المعنية بالتوقيع على الشهادات غير صالحة ستكون قد أُصدرت على الأقل ٢٤ شهادةً للجهة الموقّعة على الوثيقة (واحدة مناظرة لكل مفتاح خاص له فترة استخدام طولها شهران). وفي الأشهر القليلة الأخيرة قبل أن تصبح الشهادة الأولى للسلطة الوطنية المعنية بالتوقيع على الشهادات غير صالحة، ستكون موجودةً على الأقل ثلاث شهادات صادرة إضافية للسلطة الوطنية المعنية بالتوقيع على الشهادات (واحدة مناظرة لكل مفتاح خاص له فترة استخدام طولها أربع سنوات).

أ-٣ المثال ٣

يبيّن المثال الأخير سيناريو تكون فيه وثائق السفر الالكترونية المقروءة آلياً صالحةً لعشر سنوات، والسياسة هي استخدام فترات استخدام المفتاح الخاص القصوى وصلاحية شهادة المفتاح العام.

البند	الاستخدام / فترة الصلاحية
صلاحية وثيقة السفر الالكترونية المقروءة آلياً	١٠ سنوات
فترة استخدام المفتاح الخاص للجهة الموقّعة على الوثيقة	٣ أشهر
صلاحية شهادة الجهة الموقّعة على الوثيقة	١٠ سنوات + ٣ أشهر
فترة استخدام المفتاح الخاص للسلطة الوطنية المعنية بالتوقيع على الشهادات	٥ سنوات
صلاحية شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات	١٥ سنة + ٣ أشهر

نتائج هذا المثال هي أنه بحلول الوقت الذي تصبح فيه الشهادة الأولى للسلطة الوطنية المعنية بالتوقيع على الشهادات غير صالحة ستكون قد أُصدرت على الأقل ٢٠ شهادةً للجهة الموقّعة على الوثيقة (واحدة مناظرة لكل مفتاح خاص له فترة استخدام طولها ٣ أشهر). وفي الأشهر القليلة الأخيرة قبل أن تصبح الشهادة الأولى للسلطة الوطنية المعنية بالتوقيع على الشهادات غير صالحة، ستوجد على الأقل ثلاث شهادات إضافية للسلطة الوطنية المعنية بالتوقيع على الشهادات تم إصدارها (واحدة مناظرة لكل مفتاح خاص له فترة استخدام طولها أربع سنوات).

— — — — — — — —

المرفق (ب) بالجزء ١٢

النص المرجعي للوصف الموجز للشهادة وقائمة إلغاء الشهادات

(إعلامي)

تستند الشهادة والأوصاف الموجزة لقائمة إلغاء الشهادات المعرّفة في القسم ٧ إلى التعاريف ومتطلبات الوصف الموجز الأساسي المحددة في الوثائق ذات المراجع. وترد في الجدولين أدناه نسخة طبق الأصل من المقتطفات الموجزة من بعض الأقسام ذات الصلة من هذه الوثائق المصدرية (كما هي في وقت الكتابة). وهذه المقتطفات مقدمة لمساعدة القارئ على فهم خلفية بعض المتطلبات المحددة في شهادة وثيقة السفر الالكترونية المقروءة آلياً والأوصاف الموجزة لقائمة إلغاء الشهادات. ولا يُقصد الاعتماد عليها عوضاً عن الوثائق ذات المراجع. وفي جميع الحالات، للحصول على المواصفة الكاملة للمكون / للامتداد الوارد في المرجع وللحصول على أحدث مواصفة، **يجب** استخدام الوثائق الفعلية ذات المراجع.

الجدول ب–١ — خانات وامتدادات الشهادات

Component / Extension	*Reference*	*Relevant Excerpts*
`Certificate`	RFC 5280 – 4.1.1	
`TBSCertificate`	RFC 5280 – 4.1.1.1	
`signatureAlgorithm`	RFC 5280 – 4.1.1.2	
`signatureValue`	RFC 5280 – 4.1.1.3	
`TBSCertificate`	RFC 5280 – 4.1.2	
`version`	RFC 5280 – 4.1.2.1	When extensions are used, as expected in this profile, version MUST be 3 (value is `2`).
`serialNumber`	RFC 5280 – 4.1.2.2	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the `serialNumber` to be a non-negative integer. Given the uniqueness requirements above, serial numbers can be expected to contain long integers. Certificate users MUST be able to handle `serialNumber` values up to 20 octets. Conformant CAs MUST NOT use `serialNumber` values longer than 20 octets.
	X.690 – 8.3.2	If the contents octets of an integer value encoding consist of more than one octet, then the bits of the first octet and bit 8 of the second octet:

Component / Extension	*Reference*	*Relevant Excerpts*
		a) shall not all be ones; and b) shall not all be zero. *Note*. — These rules ensure that an integer value is always encoded in the smallest possible number of octets.
	X.690 – 8.3.3	The contents octets shall be a two's complement binary number equal to the integer value, and consisting of bits 8 to 1 of the first octet, followed by bits 8 to 1 of the second octet, followed by bits 8 to 1 of each octet in turn up to and including the last octet of the contents octets.
`signature`	RFC 5280 – 4.1.1.2	This field MUST contain the same algorithm identifier as the `signatureAlgorithm` field in the sequence `Certificate`.
`issuer`	RFC 5280 – Appendix A.1	`X520countryName ::= PrintableString (SIZE (2))` `X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))`
	RFC 5280 – 4.1.2.4	CAs conforming to this profile MUST use either the `PrintableString` or `UTF8String` encoding of `DirectoryString`.
	ISO 3166-1	
`validity`	RFC 5280 – 4.1.2.5	Both `notBefore` and `notAfter` may be encoded as `UTCTime` or `GeneralizedTime`. CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as `UTCTime`. Certificate validity dates in 2050 or later MUST be encoded as `GeneralizedTime`.
`(if encoded as UTCTime)`	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on `UTCTime`.
	X.690 – 11.8.2	The seconds element shall always be present.
`(if encoded as GeneralizedTime)`	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 | ISO/IEC 8824-1 clause on `GeneralizedTime`.
	X.690 – 11.7.2	The seconds element shall always be present.
	RFC 5280 – 4.1.2.5.2	`GeneralizedTime` values MUST NOT include fractional seconds. For the purposes of this profile, `GeneralizedTime` values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.

Component / Extension	*Reference*	*Relevant Excerpts*
subject	RFC 5280 – Appendix A.1	`X520countryName ::= PrintableString (SIZE (2))` `X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))`
	RFC 5280 – 4.1.2.6	CAs conforming to this profile MUST use either the `PrintableString` or `UTF8String` encoding of `DirectoryString`.
subjectPublicKeyInfo	RFC 5280 – 4.1.2.7	
issuerUniqueID	RFC 5280 – 4.1.2.8	CAs conforming to this profile MUST NOT generate certificates with unique identifiers.
subjectUniqueID	RFC 5280 – 4.1.2.8	CAs conforming to this profile MUST NOT generate certificates with unique identifiers.
extensions	X.690 – 11.5	The encoding of a `set` value or `sequence` value shall not include an encoding for any component value which is equal to its default value.
AuthorityKeyIdentifier	RFC 5280 – 4.2.1.1	The `keyIdentifier` field of the `authorityKeyIdentifier` extension MUST be included in all certificates generated by conforming CAs to facilitate certification path construction. There is one exception. Where a CA distributes its public key in the form of a "self-signed" certificate, the authority key identifier MAY be omitted.
keyIdentifier		
authorityCertIssuer		
authorityCertSerialNumber		
SubjectKeyIdentifier	RFC 5280 – 4.2.1.2	To facilitate certification path construction, this extension MUST appear in all conforming CA certificates, that is, all certificates including the basic constraints extension (section 4.2.1.9) where the value of `cA` is `TRUE`.
subjectKeyIdentifier		
KeyUsage	RFC 5280 – 4.2.1.3	The usage restriction might be employed when a key that could be used for more than one operation is to be restricted.
digitalSignature		The `digitalSignature` bit is asserted when the subject public key is used with a digital signature mechanism to support security services other than certificate signing (bit 5), or CRL signing (bit 6).
nonRepudiation		

Component / Extension	*Reference*	*Relevant Excerpts*
keyEncipherment		
dataEncipherment		
keyAgreement		
keyCertSign		The keyCertSign bit is asserted when the subject public key is used for verifying a signature on public key certificates.
cRLSign		The cRLSign bit is asserted when the subject public key is used for verifying a signature on certificate revocation list (e.g., a CRL, delta CRL, or an ARL). This bit MUST be asserted in certificates that are used to verify signatures on CRLs.
encipherOnly		
decipherOnly		
PrivateKeyUsagePeriod	RFC 3280 – 4.2.1.4	CAs conforming to this profile MUST NOT generate certificates with private key usage period extensions unless at least one of the two components is present and the extension is non-critical.
notBefore		Where used, notBefore and notAfter are represented as GeneralizedTime and MUST be specified and interpreted as defined in section 4.1.2.5.2.
notAfter		
CertificatePolicies	RFC 5280 – 4.2.1.4	If this extension is critical, the path validation software MUST be able to interpret this extension (including the optional qualifier), or MUST reject the certificate.
PolicyInformation		
policyIdentifier		
policyQualifiers		
PolicyMappings	RFC 5280 – 4.2.1.5	
SubjectAltName	RFC 5280 – 4.2.1.6	
IssuerAltName	RFC 5280 – 4.2.1.7	
SubjectDirectoryAttributes	RFC 5280 – 4.2.1.8	
Basic Constraints	RFC 5280 – 4.2.1.9	The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. Conforming CAs MUST include this extension in all CA certificates that contain public keys used to validate digital signatures on certificates and MUST mark the extension as critical in such certificates.

Component / Extension	*Reference*	*Relevant Excerpts*
cA		The cA boolean indicates whether the certified public key belongs to a CA. If the cA boolean is not asserted, then the keyCertSign bit in the key usage extension MUST NOT be asserted.
PathLenConstraint		
NameConstraints	RFC 5280 – 4.2.1.10	
PolicyConstraints	RFC 5280 – 4.2.1.11	
ExtKeyUsage	RFC 5280 – 4.2.1.12	This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.
CRLDistributionPoints	RFC 5280 – 4.2.1.13	
distributionPoint		
reasons		
cRLIssuer		
InhibitAnyPolicy	RFC 5280 – 4.2.1.14	
FreshestCRL	RFC 5280 – 4.2.1.15	
privateInternetExtensions	RFC 5280 – 4.2.2	
NameChange		
DocumentType		
Netscape Certificate Type		
other private extensions		

الجدول ب–٢ — خانات وامتدادات قوائم إلغاء الشهادات

Component / Extension	*Reference*	*Relevant Excerpts*
CertificateList	RFC 5280 – 5.1.1	
tBSCertList	RFC 5280 – 5.1.1.1	
signatureAlgorithm	RFC 5280 – 5.1.1.2	
signatureValue	RFC 5280 – 5.1.1.3	

Component / Extension	*Reference*	*Relevant Excerpts*
	RFC 5280 – 5.1.2	
`version`	RFC 5280 – 5.1.2.1	This optional field describes the version of the encoded CRL. When extensions are used, as required by this profile, this field MUST be present and MUST specify version 2 (the integer value is `1`).
`signature`	RFC 5280 – 5.1.2.2	This field MUST contain the same algorithm identifier as the signature field in the sequence `CertificateList`.
`issuer`	RFC 5280 – Appendix A.1	`X520countryName ::= PrintableString (SIZE (2))` `X520SerialNumber ::= PrintableString (SIZE 1..ub-serial-number))`
	RFC 5280 – 5.1.2.3 and 4.1.2.4	CAs conforming to this profile MUST use either the `PrintableString` or `UTF8String` encoding of `DirectoryString`.
`thisUpdate`	RFC 5280 – 5.1.2.4	CRL issuers conforming to this profile MUST encode `thisUpdate` as `UTCTime` for dates through the year 2049. CRL issuers conforming to this profile MUST encode `thisUpdate` as `GeneralizedTime` for dates in the year 2050 or later.
`(if encoded as UTCTime)`	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on `UTCTime`.
	X.690 – 11.8.2	The seconds element shall always be present.
`(if encoded as GeneralizedTime)`	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 | ISO/IEC 8824-1 clause on `GeneralizedTime`.
	X.690 – 11.7.2	The seconds element shall always be present.
	RFC 5280 – 4.1.2.5.2	`GeneralizedTime` values MUST NOT include fractional seconds. For the purposes of this profile, `GeneralizedTime` values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.
`nextUpdate`	5.1.2.5	CRL issuers conforming to this profile MUST encode `nextUpdate` as `UTCTime` for dates through the year 2049. CRL issuers conforming to this profile MUST encode `nextUpdate` as `GeneralizedTime` for dates in the year 2050 or later.
`(if encoded at UTCTime)`	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on `UTCTime`.
	X.690 – 11.8.2	The seconds element shall always be present.
`(if encoded at`	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T

Component / Extension	*Reference*	*Relevant Excerpts*
`GeneralizedTime)`		Rec. X.680 | ISO/IEC 8824-1 clause on `GeneralizedTime`.
	X.690 – 11.7.2	The seconds element shall always be present.
	RFC 5280 – 4.1.2.5.2	`GeneralizedTime` values MUST NOT include fractional seconds. For the purposes of this profile, `GeneralizedTime` values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.
`revokedCertificates`	RFC 5280 – 5.1.2.6	When there are no revoked certificates, the revoked certificates list MUST be absent. Otherwise, revoked certificates are listed by their serial numbers.
`crlExtensions`	RFC 5280 – 5.2	Conforming CRL issuers are REQUIRED to include the authority key identifier (Section 5.2.1) and the CRL number (Section 5.2.3) extensions in all CRLs issued.
	X.690 – 11.5	The encoding of a `set` value or `sequence` value shall not include an encoding for any component value which is equal to its default value.
`authorityKeyIdentifier`	RFC 5280 – 5.2.1	Conforming CRL issuers MUST use the key identifier method, and MUST include this extension in all CRLs issued.
`issuerAlternativeName`	RFC 5280 – 5.2.2	
`cRLNumber`	RFC 5280 – 5.2.3	CRL issuers conforming to this profile MUST include this extension in all CRLs and MUST mark this extension as non-critical. `CRLNumber ::= INTEGER (0..MAX)` Given the requirements above, CRL numbers can be expected to contain long integers. CRL verifiers MUST be able to handle `CRLNumber` values up to 20 octets. Conforming CRL issuers MUST NOT use `CRLNumber` values longer than 20 octets.
	X.690 – 8.3.2	If the contents octets of an integer value encoding consist of more than one octet, then the bits of the first octet and bit 8 of the second octet: a) shall not all be ones; and b) shall not all be zero. *Note*.— These rules ensure that an integer value is always encoded in the smallest possible number of octets.
	X.690 – 8.3.3	The contents octets shall be a two's complement binary number equal to the integer value, and consisting of bits 8 to 1 of the first octet, followed by bits 8 to 1 of the second octet, followed by bits 8 to 1 of each octet in turn up to and including the last octet of the contents octets.

Component / Extension	*Reference*	*Relevant Excerpts*
`deltaCRLIndicator`	RFC 5280 – 5.2.4	
`issuingDistribution Point`	RFC 5280 – 5.2.5	
`freshestCRL`	RFC 5280 – 5.2.6	
`reasonCode`	RFC 5280 – 5.3.1	
`holdInstructionCode`	RFC 5280 – 5.3.2	
`invalidityDate`	RFC 5280 – 5.3.3	
`certificateIssuer`	RFC 5280 – 5.3.4	

— — — — — — — —

المرفق (ج) بالجزء ١٢

الأوصاف الموجزة للشهادات الصادرة في الماضي (إعلامية)

الأوصاف الموجزة للشهادات في هذا المرفق حُددت في الطبعة السادسة من وثيقة الإيكاو Doc 9303. وعلى الرغم من أنه **يجب** على السلطات الوطنية المعنية بالتوقيع على الشهادات إصدار شهادات ممتثلة للأوصاف الموجزة الحالية كما هي محددة في القسم ٧، والأوصاف الموجزة السابقة مدرجة هنا للاعلام فقط نظراً لأن الشهادات التي أُصدرت امتثالاً للأوصاف الموجزة السابقة ستكون متداولةً، وتعالجها نظم التفتيش لعدة سنوات.

الجدول ج-١ — هيئة الشهادة

Certificate Component	*Section in RFC 3280*	*Country Signing CA Certificate*	*Document Signer Certificate*	*Comments*
`Certificate`	4.1.1	m	m	
`TBSCertificate`	4.1.1.1	m	m	See Table C-2
`SignatureAlgorithm`	4.1.1.2	m	m	Value inserted here dependent on algorithm selected
`SignatureValue`	4.1.1.3	m	m	Value inserted here dependent on algorithm selected
`TBSCertificate`	4.1.2			
`version`	4.1.2.1	m	m	SHALL be `v3`
`serialNumber`	4.1.2.2	m	m	
`signature`	4.1.2.3	m	m	Value inserted here SHALL match the OID in `signatureAlgorithm`
`issuer`	4.1.2.4	m	m	
`validity`	4.1.2.5	m	m	Implementations SHALL specify using UTC time until 2049 from then on using `GeneralizedTime`
`subject`	4.1.2.6	m	m	

Certificate Component	*Section in RFC 3280*	*Country Signing CA Certificate*	*Document Signer Certificate*	*Comments*
subjectPublicKeyInfo	4.1.2.7	m	m	
issuerUniqueID	4.1.2.8	x	x	
subjectUniqueID	4.1.2.8	x	x	
extensions	4.1.2.9	m	m	See Table C-2 on which extensions SHOULD be present

الجدول ج-٢ — الامتدادات

Extension name	*Paragraph in RFC 3280*	*Country Signing CA Certificate*	*Document Signer Certificate*	*Comments*
AuthorityKeyIdentifier	4.2.1.1	o	m	Mandatory in all certificates except for self-signed CSCA certificates
SubjectKeyIdentifier	4.2.1.2	m	o	
KeyUsage	4.2.1.3	mc	mc	This extension SHALL be marked CRITICAL
PrivateKeyUsagePeriod	4.2.1.4	o	o	This would be the issuing period of the private key
CertificatePolicies	4.2.1.5	o	o	
PolicyMappings	4.2.1.6	x	x	
SubjectAltName	4.2.1.7	x	x	
IssuerAltName	4.2.1.8	x	x	
SubjectDirectoryAttributes	4.2.1.9	x	x	
BasicConstraints	4.2.1.10	mc	x	This extension SHALL be marked CRITICAL
NameConstraints	4.2.1.11	x	x	
PolicyConstraints	4.2.1.12	x	x	
ExtKeyUsage	4.2.1.13	x	x	

Extension name	*Paragraph in RFC 3280*	*Country Signing CA Certificate*	*Document Signer Certificate*	*Comments*
CRLDistributionPoints	4.2.1.14	o	o	If issuing States or organizations choose to use this extension they SHALL include the ICAO PKD as a distribution point. Implementations may also include relative CRL DPs for local purposes; these may be ignored by other receiving States.
InhibitAnyPolicy	4.2.1.15	x	x	
FreshestCRL	4.2.1.16	x	x	
privateInternetExtensions	4.2.2	x	x	
other private extensions	N/A	o	o	If any private extension is included for national purposes then it SHALL NOT be marked. Issuing States or organizations are discouraged from including any private extensions.
AuthorityKeyIdentifier	4.2.1.1			
keyIdentifier		m	m	If this extension is used this field SHALL be supported as a minimum
authorityCertIssuer		o	o	
authorityCertSerialNumber		o	o	
SubjectKeyIdentifier	4.2.1.2			
subjectKeyIdentifier		m	m	
KeyUsage	4.2.1.3			
digitalSignature		x	m	
nonRepudiation		x	x	
keyEncipherment		x	x	
dataEncipherment		x	x	
keyAgreement		x	x	
keyCertSign		m	x	
cRLSign		m	x	
encipherOnly		x	x	

Extension name	*Paragraph in RFC 3280*	*Country Signing CA Certificate*	*Document Signer Certificate*	*Comments*
decipherOnly		x	x	
BasicConstraints	4.2.1.10			
cA		m	x	TRUE for CA certificates
PathLenConstraint		m	x	0 for New CSCA certificate, 1 for Linked CSCA certificate
CRLDistributionPoints	4.2.1.14			
distributionPoint		m	x	
reasons		m	x	
cRLIssuer		m	x	
CertificatePolicies	4.2.1.5			
PolicyInformation				
policyIdentifier		m	m	
policyQualifiers		o	o	

— — — — — — — —

المرفق (د) بالجزء ١٢

المعيار RFC 5280 توافق الاعتماد (إعلامي)

This appendix provides guidance to receiving States wishing to use systems that implement the [RFC 5280] certification path and CRL validation algorithms.

The eMRTD PKI trust model is a subset of that covered by the validation procedures defined in [RFC 5280]. Section D.1 identifies the subset of steps from the [RFC 5280] definition that are required for the eMRTD application and provides the necessary inputs and initialization values and processes for certification path validation, CRL validation and revocation checking.

Section D.2 covers the remaining steps from the [RFC 5280] definition that are not relevant to the eMRTD application. The inputs and initialization values for certification path validation and CRL validation are provided. The guidance in this section is for use in situations where the tools implement the full [RFC 5280] algorithms, rather than just the subset described in D.1.

Section D.3 provides guidance to support the extension of [RFC 5280] based CRL processing to cover revocation checking after a CSCA has undergone a name change.

D.1 STEPS RELEVANT TO eMRTD

The eMRTD certification path validation procedure defined here is based on the procedure described in [RFC 5280].The same terminology and process descriptions are used. The eMRTD certificate profiles restrict certification paths to a single certificate and prohibit use of many optional features that are used in other applications, such as the Internet PKI defined in [RFC 5280]. Path validation steps associated with these features are omitted from the eMRTD certification path validation procedure.

D.1.1 Certification Path Validation Procedure

D.1.1.1 Inputs

[RFC 5280] defines a set of nine inputs to the path validation algorithm. Only the following three are relevant to the eMRTD application:

- certification path: A single certificate (e.g. the Document Signer certificate);
- current date/time; and
- Trust Anchor information, including:
    - trusted issuer name: If the Trust Anchor is in the form of a CSCA certificate, the trusted issuer name is the value of the `subject` field of that certificate;
    - trusted public key algorithm: If the Trust Anchor is in the form of a CSCA certificate, the trusted public key algorithm is taken from the `SubjectPublicKeyInfo` field of that certificate;
    - trusted public key: If the Trust Anchor is in the form of a CSCA certificate, the trusted public key is taken from the `SubjectPublicKeyInfo` field of that certificate; and

- trusted public key parameters: This is an optional input that is included only if the trusted public key algorithm requires parameters. If the Trust Anchor is in the form of a CSCA certificate, these parameters are taken from the `SubjectPublicKeyInfo` field of that certificate.

If an implementation requires that the additional six inputs be supplied, recommendations for these are provided in D.2.

There could be several Trust Anchors for the CSCA that issued the certificate being validated. Of these Trust Anchors, the one that MUST be used is the one that contains the public key that matches the value of the Authority Key Identifier extension in the certificate being validated.

D.1.1.2 Initialization

There are eleven State variables defined in [RFC 5280]. Only the following five are relevant to the eMRTD application:

- application: max_path_length: Initialize to "0";
- working_issuer_name: Initialize to the value of the trusted issuer name;
- working_public_key_algorithm: Initialize to the value of the trusted public key algorithm;
- working_public_key: Initialize to the value of the trusted public key; and
- working_public_key_parameters: Initialize to the value of the trusted public key parameters.

If an implementation requires that the additional six variables be initialized, recommendations for these are provided in D.2.

D.1.1.3 Certificate processing

eMRTD certificate processing steps are a subset of those defined in [RFC 5280]. The result of processing an eMRTD certificate using this simplified process will be consistent with the result using the full RFC 5280 algorithm. If the additional inputs and State variables are configured as described in D.2:

a) Verify the basic certificate information. The certificate MUST satisfy each of the following:

- the signature on the certificate can be verified using working_public_key_algorithm, the working_public_key, and the working_public_key_parameters;
- the certificate validity period includes the current time;
- at the current time, the certificate is not revoked (see 6.3 for details); and
- the certificate issuer name is the working_issuer_name.

b) Assign the certificate `subjectPublicKey` to working_public_key.

c) If the `subjectPublicKeyInfo` field of the certificate contains an algorithm field with non-null parameters, assign the parameters to the working_public_key_parameters variable. If the `subjectPublicKeyInfo` field of the certificate contains an algorithm field with null parameters or parameters are omitted, compare the certificate `subjectPublicKey` algorithm to the working_public_key_algorithm. If the certificate `subjectPublicKey` algorithm and the working_public_key_algorithm are different, set the working_public_key_parameters to null.

d) Assign the certificate `subjectPublicKey` algorithm to the working_public_key_algorithm variable.

e) Recognize and process any other critical extensions present in the certificate.

f) Process any other recognized non-critical extensions present in the certificate.

If any of the checks in step a) fail or if there are any unrecognized critical extensions in the certificate that cannot be processed, the path validation procedure fails. Otherwise the procedure succeeds.

D.1.1.4 Outputs

If path validation succeeds, the procedure terminates, returning a success indication together with the working_public_key, the working_public_key_algorithm, and the working_public_key_parameters.

If path validation fails, the procedure terminates, returning a failure indication and an appropriate reason.

D.1.2 CRL Validation and Revocation Checking

The CRL validation algorithm in [REC 5280] covers various types of CRLs including delta CRLs, partitioned CRLs, indirect CRLs, etc. The CRL profile for the eMRTD application is very restrictive and prohibits use of any of these features. Use of the `issuingDistributionPoint` extension as well as all of the standardized CRL-entry extensions is also prohibited. As a result, CRL validation and revocation checking for the eMRTD application is relatively simple.

D.1.2.1 Inputs

[RFC 5280] defines two inputs to the CRL validation algorithm. Only the following one of these is relevant to the eMRTD application. If an implementation requires that the additional input be supplied, a recommendation for this is provided in D.2.

- certificate: certificate serial number and issuer name

D.1.2.2 Initialization

There are three State variables defined in [RFC 5280]. Only the following one of these is relevant to the eMRTD application. If an implementation requires that the additional two variables be initialized, recommendations for these are provided in D.2.

- cert_status : initialize to the value UNREVOKED.

D.1.2.3 CRL Processing

All CRLs in the eMRTD application are complete CRLs that cover all current certificates issued by the CSCA that issued the CRL. There are no partitioned, delta or indirect CRLs. The steps in the CRL processing algorithm for the eMRTD application are:

a) Obtain the current CRL for the CSCA that issued the certificate. If the CRL cannot be obtained, the cert_status variable is set to UNDETERMINED, and processing is stopped.

b) Verify that the CRL issuer is the same CSCA that issued the certificate in question. Because there is a single CSCA in each country, and the eMRTD application is a closed application with Inspection Systems retaining a cache of CRLs that is unique to this application, verifying that the country name is the same in the issuer field of the CRL and the issuer field of the certificate is sufficient.

- If the CSCA has not undergone a name change since the certificate was issued, the issuer field in the CRL and the issuer field in the certificate will be identical.

- If the CSCA has undergone a name change since the certificate was issued, the country attribute of the name in the issuer field of the certificate and in the issuer field of the CRL will be the same, but some other attributes may be different.

- If the relying party wishes to verify that substitution of some non eMRTD CRL has not happened, it may optionally verify that it has Trust Anchors for both CSCA names and that those Trust Anchors are for the same CSCA. If the CSCA has undergone a name change and has included the optional `issuerAltName` extension in the CRL, the relying party MAY optionally verify that the issuer field in the certificate is identical to one of the values in this extension.

If the CRL issuer is not the CSCA that issued the certificate, the cert_status variable is set to UNDETERMINED, and processing is stopped.

c) Validate the certification path for the issuer of the CRL. Note that in the eMRTD application all CRLs are issued by CSCAs that are the Trust Anchors for the respective paths. Unlike the algorithm in [RFC 5280], the eMRTD application does NOT require that the Trust Anchor used to validate the CRL certification path be the same Trust Anchor that was used to validate the target certificate. However, if the Trust Anchors are different, they MUST both be Trust Anchors for the same CSCA. Unlike [RFC 5280], the eMRTD application has multiple Trust Anchors for a given CSCA that are valid at the same time. If the certification path cannot be successfully validated, the cert_status variable is set to UNDETERMINED, and processing is stopped.

d) Verify the signature on the CRL. If the signature cannot be successfully verified, the cert_status variable is set to UNDETERMINED, and processing is stopped.

e) Search for the certificate on the CRL. If an entry is found that matches the certificate issuer and serial number, then the cert_status variable is set to UNSPECIFIED.

D.1.2.4 Output

Return the cert_status. If steps a), b), c) or d) failed, the status will be UNDETERMINED. If the certificate was listed as revoked on the CRL, the status will be UNSPECIFIED. If CRL validation succeeded, but the certificate was not listed on the CRL, the status will be UNREVOKED.

D.2 STEPS NOT REQUIRED BY eMRTD

D.2.1 Certification Path Validation

Settings for additional inputs that are not relevant to eMRTD validation include:

- initial-policy-mapping-inhibit: Set to inhibit policy mapping;
- initial-any-policy-inhibit: Set to inhibit processing of the any-policy value;
- initial-permitted-subtrees: Set to permit all subtrees;
- initial-excluded-subtrees: Set to exclude no subtrees;
- initial-explicit-policy: This should NOT be set; and
- user-initial-policy-set: Set to the special value “any-policy”.

Initialization of State variables that are not relevant to the eMRTD application include:

- permitted_subtrees: Initialize to permit all subtrees;
- excluded_subtrees: Initialize to exclude no subtrees;
- inhibit_any_policy: If initial-any-policy-inhibit is set, initialize to “0”. Otherwise, set to the value 1 or any value greater than that;
- policy_mapping: Initialize to “0”;
- explicit_policy: Initialize to “2”; and
- valid_policy_tree: Initialize the valid_policy element to “anyPolicy”, the qualifier_set element to empty and the expected_policy_set to “anyPolicy”.

D.2.2 CRL Validation

Settings for additional inputs that are not relevant to eMRTD validation include:

- use-deltas: Set to prohibit use of deltas.

Initialization of State variables that are not relevant to the eMRTD application include:

- reasons_mask: Initialize to an empty set; and
- Interim_reasons_mask: Initialize to the special value “all-reasons”.

D.3 MODIFICATIONS REQUIRED TO PROCESS CRLS

CRL validation systems that comply with the CRL validation procedure in [RFC 5280] are not intended to support environments where a CA has undergone a name change, such as the eMRTD application environment. Therefore these systems require some modification to handle this special case, as described below:

a) In clause 6.3.3, step a) of the [RFC 5280] CRL validation procedure, the name in the distribution point field of the CRL Distribution Points extension of the certificate in question is used to update the local cache with the relevant CRL(s). For the eMRTD application, this step would need to be modified and only the `countryName` attribute of the distribution point field should be used to identify and obtain the appropriate CRL.

b) In clause 6.3.3, step f) of the [RFC 5280] CRL validation procedure, there is a requirement that the same Trust Anchor be used to validate the certification path for the CRL issuer that was used to validate the target certificate. This is NOT a requirement for the eMRTD application because independent Trust Anchors are established for each public key of the CSCA.

The Trust Anchor used for validation of the CRL issuer will be the one for the CSCA’s public key that corresponds to the private key used to sign the CRL. The Trust Anchor used to validate the certification path for the target certificate may be for an earlier CSCA key pair.

— — — — — — — —

المرفق (هـ) بالجزء ١٢

مثال على البنية LDS2 (إعلامي)

يوضح المثال التالي التفاعلات الحاصلة بين مختلف مكونات معرف المفتاح الخاص لتوقيع الوثيقة LDS2 ومعرّف المفتاح الخاص لترخيص الوثيقة LDS2.

ولتوضيح التفاعلات والأمور التمهيدية التي يتطلبها السيناريو النموذجي للأعمال، لننظر في السيناريو الذي يريد فيه البلد Dystopia كتابة أختام سفر على جوازات مواطني البلد Utopia. وفيما بعد، يريد البلد Atlantis قراءة أختام السفر التي وضعتها Dystopia على جوازات Utopia.

وترد فيما يلي الملاحظات التمهيدية:

- قامت Utopia بتثبيت تطبيق ختم السفر LDS2 على جوازاتها.
- حددت كل من Dystopia وUtopia معرّف المفتاح الخاص بها لترخيص LDS2.
- حددت Dystopia معرّف المفتاح الخاص بها للتوقيع على وثائق LDS1 من أجل إصدار شهادات موقّع الوثائق LDS2.
- تم تبادل شهادات السلطة الوطنية للتحقق من الشهادات وشهادات عميل ومخدّم نقطة الاتصال المفردة (SPOC) بطريقة موثوقة بين Utopia وDystopia في وقت معين. (فيما بعد، يمكن تبادل الشهادات الجديدة للسلطة الوطنية للتحقق من الشهادات وشهادات SPOC بصورة مباشرة عن طريق نقطة الاتصال المفردة).
- تم تبادل شهادات السلطة الوطنية للتحقق من الشهادات وشهادات عميل ومخدّم نقطة الاتصال المفردة (SPOC) بطريقة موثوقة بين Utopia وAtlantis في وقت معين (فيما بعد، يمكن تبادل الشهادات الجديدة للسلطة الوطنية للتحقق من الشهادات وشهادات SPOC بصورة مباشرة عن طريق نقطة الاتصال المفردة). وإذا كان تطبيق ختم السفر LDS2 مفتوحاً للقراءة، أي إذا كان بإمكان أي بلد أن يقرأ أختام السفر LDS2 (لا حاجة للإذن إلا للكتابة)، يمكن إغفال هذه الخطوة.
- تم تبادل شهادات السلطة الوطنية المعنية بالتوقيع على الشهادات بطريقة موثوقة بين Dystopia وAtlantis في وقت معين.

وترد فيما يلي عملية التكرار اللازمة لتمكين Dystopia من ختم وثائق السفر الإلكترونية المقروءة آلياً الخاصة بـUtopia في وقت معين:

- تطلب Dystopia من Utopia شهادة متحقق من الوثائق.
- تستخدم نقطة الاتصال المفردة في Dystopia شهادة عميل نقطة الاتصال المفردة الخاصة بها وشهادة مخدّم نقطة الاتصال المفردة الخاصة بـUtopia لبدء اتصال مع نقطة الاتصال المفردة. بعد ذلك، ينشأ طلب من المتحقق من الوثائق في Dystopia ويرسل من نقطة اتصال مفردة إلى أخرى. وبناء على الطلب، تنشئ Utopia شهادة متحقق أجنبي من الوثائق مع منح Dystopia إمكانية القراءة/الكتابة، ثم تعاد الشهادة عن طريق نقطة اتصال مفردة إلى أخرى.
- بعد تلقي شهادة المتحقق من الوثائق من نقطة الاتصال المفردة الخاصة به، ينشئ المتحقق من الوثائق في Dystopia شهادات محطة طرفية من أجل الوحدات الطرفية عند حدودها. ولدى الاتصال بالجواز، تتحقق الدائرة المتكاملة الموجودة على جوازات Utopia من شهادة المحطة الطرفية في Dystopia بواسطة شهادة المتحقق من الوثائق في Dystopia، ومن شهادة المتحقق من الوثائق بواسطة شهادة السلطة الوطنية للتحقق من الشهادات في Utopia. بعد ذلك تمنح الدائرة المتكاملة للمحطة الطرفية في Dystopia إمكانية القراءة/الكتابة فى تطبيق ختم السفر LDS2.

وفيما يلي عملية وضع ختم إلكتروني على وثيقة سفر إلكترونية مقروءة آلياً:

- تنشئ Dystopia ختم سفر إلكترونياً، وتوقّعه بواسطة المفتاح الخاص المناظر للمفتاح العام المخزّن في شهادة موقّع (ختم السفر) LDS2 الخاصة بمعرّف المفتاح الخاص لتوقيع LDS2 في Dystopia. وتخزّن شهادة الموقّع على LDS2 في الدائرة المتكاملة اللا تلامسية الموجودة في جواز Utopia.

وبعد المصادقة على جواز Utopian عند حدود Atlantis:

- إذا تطلبت قراءة أختام السفر الموجودة على جوازات Utopia شهادة من المحطة الطرفية مع إمكانية للقراءة، يرسل طلب شهادة من Atlantis إلى Utopia عن طريق نقطة اتصال مفردة إلى أخرى. وبناء على الطلب، تنشئ Utopia شهادة متحقق أجنبي من الوثائق مع إمكانية قراءتها من Atlantis وترسل هذه الشهادة إلى Atlantis عن طريق نقطة اتصال مفردة إلى أخرى. وباستخدام شهادة المتحقق من الوثائق هذه، تنشئ Atlantis شهادات للوحدات الطرفية مع إمكانية قراءة جوازات Utopia في الوحدات الطرفية في Atlantis. وإذا استطاعت محطة طرفية أن تقرأ أختام السفر الموجودة على جوازات Utopia، يمكن إغفال هذه الخطوة.
- للتحقق من ختم سفر وضعته Dystopia على الجواز، تستخدم Atlantis معرّف المفتاح الخاص في Dystopia للتوقيع على LDS1: وتستخدم شهادة الموقّع على LDS2 في Dystopia المخزّنة في الجواز للتحقق من ختم السفر. بعد ذلك، تستكمل السلسلة، أي يتم التحقق من شهادة الموقع على LDS2 في Dystopia بواسطة شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات في Dystopia التي تم تلقيها بصورة أولية.

— انتهـــى —

ISBN 978-92-9265-560-0