ايكاو

# Doc 9303

## وثائق السفر المقروءة آلياً

الطبعة الثامنة – ٢٠٢١

## الجزء ١٣: الأختام الرقمية المرئية

اعتمدتها الأمينة العامة ونُشرت بموجب سلطتها

منظمة الطيران المدني الدولي

ايكاو

# Doc 9303

## وثائق السفر المقروءة آلياً

الطبعة الثامنة – ٢٠٢١

## الجزء ١٣: الأختام الرقمية المرئية

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 ١٣ – الأختام الرقمية المرئية**
Order No.: 9303P13
ISBN 978-92-9265-288-3 (النسخة المطبوعة)
ISBN 978-92-9275-582-9 (النسخة الإلكترونية)

## التعديلات

تعلن التعديلات في ملاحق كتالوج الإيكاو للمنتجات والخدمات، ويمكن الاطلاع على الكتالوج وملاحقة في مواقع الإيكاو على الانترنت عبر الرابط www.icao.int والجدول أدناه مخصص لتسجيل مثل هذه التعديلات

**سجل التعديلات والتصويبات**

| التعديلات | | |
|---|---|---|
| الرقم | التاريخ | أدخل بواسطة |
| ١ | ٢٠٢٤/٦/٤ | الإيكاو |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| التصويبات | | |
|---|---|---|
| الرقم | التاريخ | أدخل بواسطة |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# جدول المحتويات

# ١ – النطاق

يصف هذا الجزء ١٣ من الوثيقة Doc 9303 استخدام الختم الرقمي لضمان صحة وسلامة الوثائق غير الإلكترونية بطريقة غير مكلفة نسبياً ولكنها آمنة للغاية وذلك من خلال استخدام التشفير غير المتماثل. وينطوي هذا النظام على توقيع المعلومات الموجودة على الوثيقة غير الإلكتروني بشكل مشفر، وترميز التوقيع في شكل باركود ثنائي الأبعاد مطبوع على الوثيقة نفسها. ويوفر هذا النهج – *الختم الرقمي المرئي* – المزايا التالية:

- *عدم التماثل*. نظراً لاستخدام التشفير غير المتماثل، فإن تكلفة إرفاق ختم رقمي أعلى بكثير من تكلفة إصدار وثيقة محمية بختم رقمي. وبالتالي، على الرغم من أن تكلفة إصدار الوثيقة منخفضة للغاية، إلا أن تزوير أو تقليد البيانات الشخصية الخاصة بهذه الوثيقة أمر مكلف للغاية.
- *الطابع الشخصي*. يتيح كل ختم رقمي التحقق من المعلومات المطبوعة على الوثيقة المادية، وبالتالي فهو يرتبط بحامل الوثيقة. وليس هناك معادل مباشر لوثيقة خالية من البيانات، وبالتالي لا يمكن فقد أو سرقة أي وثائق خالية من البيانات.
- *سهولة التحقق*. حتى الأشخاص غير المدربين بمقدورهم التحقق من الوثيقة المحمية بختم رقمي باستخدام معدات منخفضة التكلفة، مثل أحد تطبيقات الهاتف الذكي. علاوة على ذلك، نظراً للطبيعة الثنائية للتوقيع الرقمي، فإن التمييز بين الوثائق الأصلية والمزورة أمر واضح ومباشر.

وفي حين يشكل الختم الرقمي تحسنا كبيراً على مستوى تأمين الوثائق (الورقية عادةً) التي لا تحتوي على رقاقة إلكترونية دقيقة، إلا أن له عيوباً كبيرة عند مقارنته بالوثائق القائمة على الشرائح الإلكترونية. فعادةً ما تقتصر سعة تخزين الأختام الرقمية على بضعة كيلوبايت على الأكثر ولا يمكن تحديث البيانات ولا مفاتيح تشفير الختم الرقمي أو مخططاته على الوثائق الموجودة. أي أن رشاقة التشفير غير متاحة. ولا يوفر الختم الرقمي أي حماية ضد الاستنساخ، ولا يتضمن وظيفة حماية الخصوصية، وهو أكثر عرضة للوقوع في الأخطاء بسبب التآكل والتلف مقارنة بالوثائق القائمة على الشريحة الدقيقة. وعلاوة على ذلك، فإن تعدد استخدامات رقائق التشفير يسمح بتنفيذ سمات إضافية، مثل مخططات التوقيع، والتحقق الطرفي، والطرق الثنائية للتحقق من الصحة القائمة على تقاسم الأسرار، مثل رقم الهوية الشخصي، أو بروتوكولات التشفير الآمنة القائمة على المخططات المتماثلة. ونظراً لأن الباركودات ثنائية الأبعاد لا يمكن أن تحل محل السمات الوظيفية أو التأمينية للرقائق الدقيقة، يجب أن تستخدم وثائق السفر الرقائق الدقيقة كلما كان ذلك ممكنًا.

# ٢ – تشفير الختم الرقمي

الختم الرقمي المرئي عبارة عن بنية بيانات موقعة بالتشفير تحتوي على سمات الوثيقة، في شكل باركود ثنائي الأبعاد ومطبوعة على الوثيقة. ويعرض هذا القسم وصفاً لتشفير وبنية الختم الرقمي المرئي.

## ٢–١ شكل الباركود ومتطلبات الطباعة الخاصة به

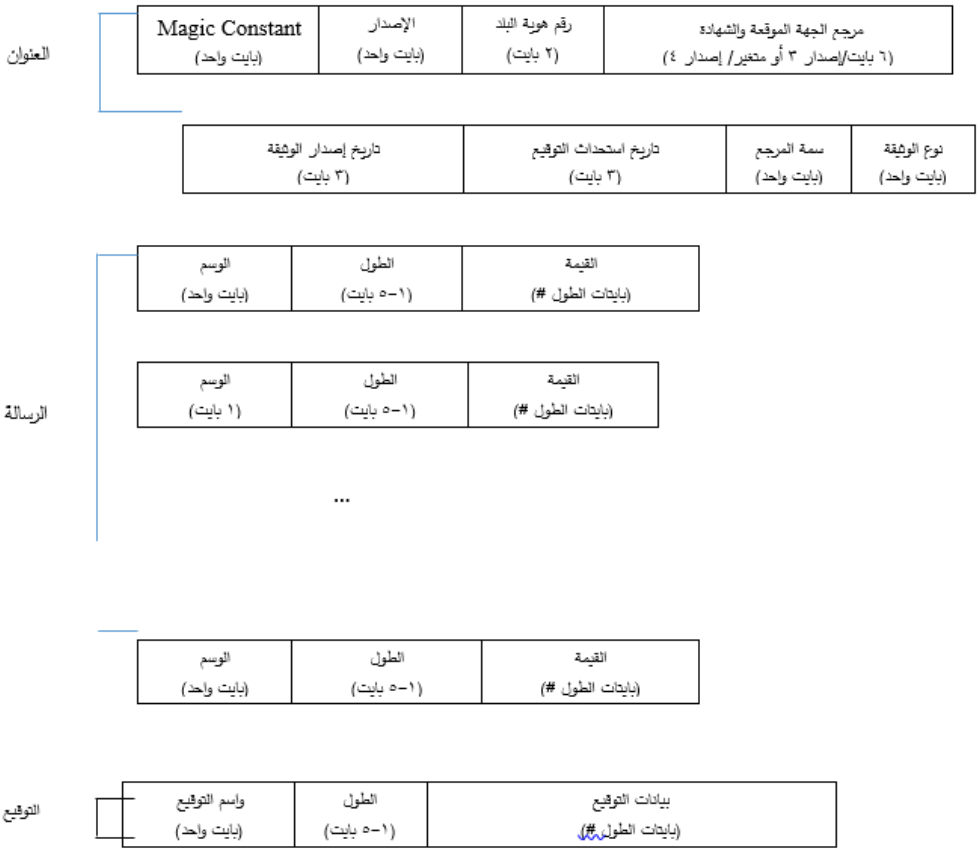
تحدد هذه الخاصية كيفية تشفير البيانات في شكل دفق من البايتات. والباركودات ثنائية الأبعاد التي صُنف نظامها الترميزي كقاعدة قياسية للمنظمة الدولية لتوحيد المقاييس (آيزو) هي وحدها التي **يجب** استخدامها. حيث إن نظم آيزو الترميزية القياسية المستخدمة في الباركودات ثنائية الأبعاد تشمل على سبيل المثال لا الحصر، "مصفوفة البيانات" DataMatrix [ISO/IEC 16022]، ورموز آزتيك Aztec [ISO / IEC 24778]، ورموز الاستجابة السريعة QR [ISO / IEC 18004].

و**ينبغي** طباعة الباركود بطريقة تسمح لمعدات القراءة (مثل الهواتف الذكية أو الماسحات الضوئية المتاحة في السوق التجارية) بفك شفرته بشكل موثوق؛ وعلى وجه الخصوص، **ينبغي** أن تؤخذ في الاعتبار القاعدة القياسية [ISO / IEC 15415] عند تقييم جودة الطباعة. وتعتمد متطلبات جودة الطباعة والمسح الضوئي المترتبة عن ذلك على الوثيقة؛ و**يجوز** تحديد التفاصيل الخاصة بسيناريو التطبيق في ملف تعريف.

ونظراً لأن جودة الطباعة والمسح الضوئي تؤثر على معدلات الخطأ وعلى قدرة التحقق من الختم الرقمي، **ينبغي** أن تضمن متطلبات الجودة هذه أنه يمكن التحقق بشكل موثوق من الباركود الذي يحتوي على الختم الرقمي وجميع سمات الوثيقة الإلزامية. وهناك مطلب هام آخر يتعلق بتباين الرموز في الباركود، لأن طباعة الختم الرقمي قد تجري على ورق مؤمَّن بخلفية ملونة (مثل الأخضر).

عند استخدام طابعات حبرية عادية، **يوصى** بألا يقل حجم الوحدة (حجم الحزمة الواحدة من الباركود ثنائي الأبعاد) عن ٠,٣٣٨٦ مم للطول الجانبي لكل وحدة، بما يعادل ٤ نقاط لكل طول جانبي للوحدة (أي ١٦ نقطة لكل وحدة) على طابعة تبلغ استبانتها ٣٠٠ نقطة في البوصة، أو ٨ نقاط لكل طول جانبي للوحدة (أي ٦٤ نقطة لكل وحدة) على طابعة باستبانة قدرها ٦٠٠ نقطة في البوصة. و**يجوز** قبول أحجام الطباعة الصغيرة، إذا تم استخدام طابعات عالية الاستبانة أو طابعات ليزر. لمعرفة موضع الباركود على الوثيقة، راجع الأجزاء ذات الصلة من الوثيقة Doc 9303.

يتكون الباركود المشفر من عنوان (انظر القسم ٢–٢) وجزء للرسائل (انظر القسم ٢–٣) وجزء للتوقيع (انظر القسم ٢–٤). ويعرض الشكل ١ بصورة مختصرة بنية الباركود.




**الشكل ١– بنية الختم الرقمي**

### ٢–٢ العنوان

يحتوي العنوان على بيانات تعريف بشأن الوثيقة والتشفير، مثل رقم الإصدار وتواريخ إصدار الوثيقة واستحداث التوقيع.

تحدد هذه الخاصية نسختين من العنوان، يُشار إليهما بواسطة معرّف الإصدار "٣" و "٤"، على التوالي. وتختلف الإصدارات في تعريف مرجع الشهادة (انظر أدناه) وطول ترميز سمات الوثيقة (انظر القسم ٢–٣).

الطول الإجمالي للعنوان هو ١٨ بايت للإصدار ٣ ومتغير للإصدار ٤. ويرد تعريف للعنوان في الجدول ١.

**الجدول ١– شكل العنوان**

| *موقع البداية* | *الطول (بايت)* | *المحتوى* |
|---|---|---|
| 0x00 | 1 | *Magic Constant*. لديه قيمة ثابتة قدرها 0xDC تحدد باركود يتوافق مع هذه الخاصية. |
| 0x01 | 1 | *الإصدار*. قيمة بالبايت تحدد رقم إصدار هذه الخاصية. يتم تحديد الإصدارات المحددة في هذه الخاصية بواسطة قيمة البايت 0x03 / 0x02، على التوالي. يشير الرقم *n* إلى الإصدار *1 + n*، حيث تشير القيمة صفر مثلاً إلى الإصدار ١. |
| 0x02 | 2 | *بلد الاصدار*. رمز من ثلاثة أحرف يحدد دولة أو منظمة الإصدار. الرمز المكون من ثلاثة أحرف يتحدد وفقاً للوثيقة *Doc 9303-3*. إذا كان رمز الأحرف الثلاثة يتكون من أقل من ثلاثة أحرف، **فيجب** أن يكون الرمز مبطنًا بأحرف حشو ("<")، على سبيل المثال "*D*" مبطن بـ "*D* <<". يتم ترميز الكود بواسطة القاعدة القياسية *C40* (انظر القسم ٢–٦) كتسلسل ثنائي البايت. |
| 0x04 | 6 / v | *معرف الموقع ومرجع الشهادة*.<br>الإصدار ٣: رمز من تسعة أحرف يحدد موقّع (الباركود) والشهادة.<br>الإصدار ٤: رمز حرف متغير الطول يحدد موقّع (الباركود) والشهادة (يشير الحرف "*v*" إلى الطول الإجمالي لهذا الحقل).<br>تم تشفير الرمز بواسطة *C40* (انظر القسم ٢–٦). للتشفير متغير الطول، انظر القسم ٢–٢–١. |
| 0x0A / 0x04+v | 3 | *تاريخ إصدار الوثيقة*. تاريخ إصدار الوثيقة.<br>مشفر كما هو محدد في القسم ٢–٣–١. |
| 0x0D / 0x07+v | 3 | *تاريخ إنشاء التوقيع*. تاريخ إنشاء التوقيع. مشفر كما هو محدد في القسم ٢–٣–١. |
| 0x10 / 0x0A+v | 1 | مرجع تعريف سمة الوثيقة. رمز مرجعي للوثيقة يحدد عدد سمات الوثيقة وتشفيرها. هذا التعريف مستقل عن كل فئة من فئات نوع الوثيقة، أي أن نفس الكود المرجعي لتعريف سمة الوثيقة قد يكون له معاني مختلفة لفئات نوع الوثيقة المختلفة. **يجب** أن تكون القيم في النطاق بين 01dec و254dec. |
| 0x11 / 0x0B+v | 1 | *فئة نوع الوثيقة*. فئة الوثيقة، سواء كانت تأشيرة، أو وثيقة سفر طارئة، أو شهادة ميلاد. **يجب** استخدام الأرقام الفردية في النطاق بين 01dec و253dec لفئات أنواع الوثائق المحددة من قبل الإيكاو. |
| الجملة | 18 / 12 + v | |

### ٢–٢–١ *معرِّف الجهة الموقعة ومرجع الشهادات*

بسبب قيود الحجم، من المستحيل تخزين الشهادات التي تحتوي على المفتاح العام المناظر للتوقيع داخل الباركود. لذلك، **يجب** الحصول على الشهادة على قناة مختلفة. ومن أجل التعرف تحديداً على الشهادة والجهة الموقِّعة التي هو موضوع الشهادة، وربط الشهادة بالباركود، يتم تخزين سلسلة تحتوي على معرِّف الجهة الموقِّعة ومرجع للشهادة في العنوان. وتتألف هذه السلسلة من:

أ) *مُعرّف الجهة الموقّعة*: توليفة مكونة من رمز البلد المكون من حرفين، على النحو الوارد في الوثيقة Doc 9303-3، لبلد الجهة الموقّعة وحرفين أبجديين رقميين لتحديد الجهة الموقّعة داخل البلد المحدد أعلاه. و**يجب** أن يقتصر معرّف الجهة الموقّعة على الجهة الموقّعة في البلد المعني.

ب) *مرجع الشهادة*:

١) لإصدار العنوان ٣: سلسلة سداسية تتألف من تسلسل من خمسة أحرف بالضبط هي التي يجب أن تحدد بشكل فريد بأن الشهادة تختص بجهة موقّعة معينة.

٢) بالنسبة لإصدار العنوان ٤: سلسلة سداسية تشتمل على تسلسل من:

١) حرفين بالضبط للدلالة على عدد الأحرف التالية، و

٢) الأحرف التي **يجب** أن تعرِّف، تحديدا، شهادة لموقّع معين.

لاحظ أنه بالنسبة لحالة الاستخدام المحددة للتأشيرات (انظر الوثيقة 7-9303 Doc)، تكون الجهة الموقّعة هي تلك *الموقّعة على التأشيرة*.

مرجع الشهادة 0 . . . 0 يتم حجزه لأغراض الاختبار **ويجب ألا** يُستخدم في الإنتاج.

**يجب** أن يتوافق معرّف الجهة الموقّعة (الباركود) ومرجع الشهادة مع الاسم المميز للموضوع (DN) والرقم التسلسلي لشهادة الموقّع على التوالي. وبالتالي، يمكن تحديد شهادة الموقع بشكل فريد عند فك تشفير العنوان.

### ٢-٢-٢ *مرجع تعريف سمات الوثيقة وفئة نوع الوثيقة*

التوليفة المكونة من مرجع *تعريف سمة الوثيقة وفئة نوع الوثيقة* تحدد مجموعة معينة من القواعد، مثل هذه الخاصية. وبالتالي يمكن في حالات الاستخدام المستقبلية إعادة استخدام نفس الباركود وشكل العنوان، ولكن مع الإشارة إلى تعريفات مختلفة للسمات (أي مرجع يصف قائمة المعلومات المضمنة في الباركود) أو فئات نوع الوثيقة. ويتيح هذا إعادة استخدام قواعد الرموز الموجودة، ويبسط عمليات التنفيذ ويزيد من إمكانية التشغيل البيني.

ويرد في الوثيقتين 7-9303 Doc و8-9303 Doc، على التوالي، مراجع تعريف سمات الوثائق وفئات نوع الوثيقة للتأشيرة ووثائق السفر في حالات الطوارئ.

## ٢-٣ الجزء الخاص بالرسائل

الجزء الخاص بالرسائل يأتي بعد العنوان ويتكون من سمات الوثيقة المشفرة رقمياً، كما هو محدد في هذا القسم. وطالما كانت جميع سمات الوثيقة الإلزامية موجودة فإن أي ترتيب لهذه السمات يكون صالحا.

وكل سمة من سمات الوثيقة تأتي مسبوقة بـ:

- وسم يحدد نوع السمة (بايت واحد)
- طول السمة (بايت واحد إلى خمسة بايت)

واعتماداً على معرف الإصدار (الذي يكون عند موضع البداية (0x01) في العنوان، انظر الجدول ١)، يجب التمييز بين نوعين من تشفير الطول:

- بالنسبة للإصدار رقم ٣ وما يليه، **يجب** تشفير الطول مباشرة في ١ بايت ("هذا البايت الطولي" هو البايت الثاني بعد "وسم" الرسالة مباشرة).
- بالنسبة للإصدار رقم ٤ وما فوق، يجب تشفير الطول باستخدام قيمة طول الوسم لقاعدة التشفير المميز (DER-TLV) وفقاً لـ [X.690].

بالنسبة لوثائق التأشيرة، **يوصى** باستخدام الإصدار رقم ٤ (أو أعلى) وبالتالي تشفير الطول DER-TLV. ويُعد استخدام الإصدار رقم ٣ (أو ما دونه) وبالتالي الترميز المباشر للطول صالحًا ولكن لا يُنصح به.

بالنسبة لوثائق السفر للطوارئ (ETD)، يجب استخدام الإصدار رقم ٤ (أو أعلى) وبالتالي التشفير الطولي لقيمة طول الوسم لقاعدة التشفير المميز (DER-TLV).

### ٢-٣-١ *التشفير الرقمي لسمات الوثيقة (التشفير الثنائي)*

يجري تشفير سمات الوثيقة بالطريقة التالية. نأخذ في الاعتبار الأنواع الأساسية التالية باعتبارها لبنات بناء:

أ) الأحرف الأبجدية الرقمية (*Alphanum*): سلاسل من أحرف أبجدية رقمية كبيرة[١] (مثل A–Z، ٠–٩ والمسافة)؛

ب) ثنائي (*Binary*): متواليات من البايتات؛

ج) عدد صحيح موجب (*Int*:)؛ و

د) التاريخ: (*Date*).

يتم تحويل هذه الأنواع الأساسية إلى متواليات من البايتات، على النحو التالي:

أ) يتم تشفير سلاسل الأحرف الأبجدية الرقمية على هيئة بايتات بواسطة ترميز C40 (انظر القسم ٢–٦).

ب) تؤخذ متواليات البايتات كما هي.

ج) بالنسبة للأعداد الصحيحة الموجبة، يتم أخذ تمثيلها كأعداد صحيحة بدون إشارة.

د) يتم تحويل التاريخ أولاً إلى عدد صحيح موجب عن طريق تجميع الشهر والأيام والسنة (معبر عنها بأربعة أرقام)، في شكل رقم متسلسل. ثم يتم تجميع هذا العدد الصحيح الموجب في تسلسل من ثلاثة بايت كما هو محدد في ج) أعلاه.

مثال: خذ التاريخ ٢٥ مارس ١٩٥٧. ينتج عن الربط التسلسلي للشهر والتاريخ والسنة العدد الصحيح ٠٣٢٥١٩٥٧، مما يسفر عن البايتات الثلاثة 0x31 0x9E 0xF5.

سمة الوثيقة الرقمي هي سلسلة من البايتات. لديها الهيكل التالي:

الوسم | الطول | القيمة

***الوسم*** هنا هي عدد صحيح في النطاق 0–254dec يعمل كمعرف فريد لسمة الوثيقة. لاحظ أن العلامة 255dec محجوزة للإشارة إلى بداية التوقيع. ويتكون ***الطول*** من واحد إلى خمسة بايت وفقاً لتشفير خانات قيمة طول الوسم لقاعدة التشفير المميز (DER-TLV). ويشير *الطول* إلى طول القيمة التالية. أما ***القيمة*** فهي نوع أساسي يتم تحويله إلى سلسلة من البايتات.

مثال: خذ سمة وثيقة تشفّر السلسلة "VISA01" بالوسم المخصص 0x0A. تسلسل البايت المشفر C40 (انظر القسم ٢–٦) بطول ٤ هو 0xDE515826. وبالتالي فإن سمة الوثيقة هي تسلسل البايت 0x0A04DE515826.

يجب أن تعزز حالة الاستخدام المحددة هذا التعريف من خلال تعداد سمات الوثيقة التي يجب أن تكون موجودة وتلك التي يمكن أن تكون موجودة بشكل اختياري، وتحديد قيم علاماتها ونطاقات الطول المسموح بها.

وقد تكون هناك سمات إضافية، مثل السمات ذات الأوسام غير المعروفة، على سبيل المثال للاستخدام الاختياري للكيان الذي يتولى الإصدار. **ويجب ألا** تستخدم هذه السمات الإضافية وسم خانة السمة الإضافية، أو وسم أي سمة اختيارية أو إلزامية أخرى. **يجب ألا** يؤثر وجود سمات ذات علامات غير معروفة على صلاحية الباركود، إذا تم الإقرار بصلاحية التوقيع.

[١] يرجع التقيد باستخدام الأحرف الكبيرة وحدها إلى محدودية سعة بيانات للباركود.

### ٢-٤ الجزء الخاص بالتوقيع

يشار إلى بداية منطقة التوقيع بواسطة علامة التوقيع التي لها القيمة 0xFF، المشفرة كبايت واحد، متبوعاً ببايت واحد إلى خمسة بايتات للإشارة إلى طول التوقيع (عدد البايتات) باستخدام مخطط تشفير خانات الطول لقيمة طول الوسم حسب قواعد التشفير المتميز (DER-TLV).

و**يجب** أن يكون إدخال خوارزمية التوقيع هو (البصمة الرقمية لـ) تسلسل العنوان والجزء الخاص بالرسائل بأكمله، باستثناء الوسم الذي يشير إلى بداية منطقة التوقيع أو طول التوقيع. وتحتوي منطقة التوقيع على التوقيع الناتج.

**يجب** استخدام خوارزميات التجزئة والتوقيع المذكورة في الوثيقة Doc 9303-12 فقط. ونظراً لحجم التوقيع الناتج، يُوصى باستخدام خوارزمية اتفاق مفاتيح المنحنيات الإهليلجية ECDSA) بمفتاح لا يقل طوله عن ٢٥٦ بت مع خوارزمية بصمة رقمية قدرها ٢٥٦ SHA-256 (في وقت إعداد هذه الوثيقة).

ينتج عن تطبيق خوارزمية التوقيع (ECDSA) زوج من الأعداد الصحيحة الموجبة (r، s). و**يجب** تخزين هذا التوقيع في شكل خام في الختم. ويتوافق طول البت r و s على التوالي مع طول المفتاح. وهكذا، على سبيل المثال، بالنسبة لـ ECDSA-256 ، يكون طول r و s بحد أقصى ٢٥٦ بت = ٣٢ بايت لكل منهما. **ويجب** تخزين التوقيع عن طريق حساب تمثيل العدد الصحيح بدون إشارة لـ r و s، مع إمكانية إضافة أصفار بادئة لملاءمة r و s لطولهما المتوقع (أي طول المفتاح)، وإلحاق القيمة الناتجة من s إلى قيمة r. انظر الملحق باء للتحويل بين ASN.1 والصيغة الخام لـ ( r، s).

وخوارزمية التجزئة المستخدمة في التوقيع ليست مشفرة في منظومة البيانات. بل لابد من استنتاج خوارزمية التجزئة من طول البت في عدد مرات تكرار نقطة أساس بناء المنحنى المستخدم في إنشاء التوقيع، لأغراض التوقيع والتحقق من صحة التوقيع.

ولاستنتاج خوارزمية التجزئة، لابد من القيام بالخطوات التالية:

- افتراض أن **τ** تشير إلى طول البت في عدد مرات تكرار نقطة أساس بناء المنحنى G. يمكن الحصول على عدد مرات التكرار **η** من بارامترات المنحنى الإهليجي في شهادة الموقّع وهو يعطي قيمة **τ**.
- يجب أن تكون قيمة **τ** أقل من أو مساوية لطول الناتج 'l' في خوارزمية التجزئة (**τ** <= l)

| خوارزمية التجزئة | فى حالة لو كان |
|---|---|
| SHA-224 | **τ** <=224 |
| SHA-256 | (**τ** <=256) AND (**τ** >224) |
| SHA-384 | (**τ** <=384) AND (**τ** >256) |
| SHA-512 | (**τ** <=512) AND (**τ** >384) |

### ٢-٥ الحشو

إذا كان العنوان والرسالة والتوقيع معًا لا يملآن المساحة المتاحة للباركود، **فيجب** إضافة أحرف للحشو بعد التوقيع. وتعرِّف جميع نظم ترميز الباركودات ثنائية الأبعاد ذات الصلة طرق الحشو في قواعدها القياسية، ويجب أن يتقيد الحشو بهذا التعريف.

### ٢-٦ ترميز السلاسل وفقا لمخطط الترميز C40

للاقتصاد في المساحة عند ترميز الأحرف الأبجدية الرقمية ورمز الحشو <، يتم استخدام مخطط الترميز C40، كما هو محدد في [ISO/IEC 16022]. ويرد أدناه وصف لكيفية استخدام هذه التعريفات في الإعداد الحالي. ينطبق التعريفان التاليان على سمات الوثائق وترميزها الرقمي:

أ) تتكون السلاسل فقط من الأحرف الكبيرة (upper case) والأرقام و <SPACE> والرمز '<'. ويُستخدم الأخير كرمز حشو للجزء المقروء آليًا (MRZ) لوثائق السفر. وإذا ظهر الرمز "<" في السلسلة، يتم استبدال جميع الحالات التي يرد فيها "<" بـ <SPACE> قبل الترميز. إذ **يجب ألا** تحتوي السلسلة على أي رموز أخرى.

ب) عند وجود سلسلة طولها L، فإن الطول (أي عدد البايتات) للترميز الرقمي المقابل هو أقل عدد زوجي أكبر من أو مساوي لـ L.

في العمليات الحسابية التالية، تم ضمنيا تحويل قيمة البايت وما يقابلها من عدد صحيح بدون إشارة. فمثلا، نحدد قيمة البايت بواسطة صيغة تتكون من عدد صحيح حسابي على قيم عدد صحيح.

#### ٢-٦-١ *الترميز*

يعمل ترميز سلسلة من الرموز في سلسلة من البايتات على النحو التالي: أولاً، يتم تجميع السلسلة في مجموعات من ثلاثة رموز، ويتم استبدال كل رمز بقيمة C40 المقابلة وفقاً للجدول ٢، مما ينتج عنه ثلاثي (U1، U2، U3). ثم يجري لكل ثلاثي احتساب القيمة

```
U = (1600 * U1) + (40 * U2) + U3 + 1
```

والنتيجة تقع في النطاق من ١ إلى ٦٤٠٠٠، مما يعطي قيمة عدد صحيح بدون إشارة ١٦ بت. وقيمة ١٦ بت I16 معبأة في وحدتي بايت

```
البايت ١ = (I16) div 256
```

```
البايت ٢ = (I16) mod 256
```

هنا يشير div إلى تقسيم عدد صحيح (بدون باقي)، ويشير mod إلى عملية باقي القسمة. لاحظ أنه يمكن تنفيذ هذه العمليات عن طريق تحويل البتات.

**الجدول ٢– خارطة التشفير بمخطط C40 ومقارنتها بالشفرة القياسية الأمريكية لتبادل المعلومات –آسكي (ASCII)**

| قيمة C40 | الرمز | قيمة آسكى | قيمة C40 | الرمز | قيمة آسكى |
|---|---|---|---|---|---|
| صفر | Shift 1 | لا ينطبق | ٢٠ | G | ٧١ |
| ١ | Shift 2 | لا ينطبق | ٢١ | H | ٧٢ |
| ٢ | Shift 3 | لا ينطبق | ٢٢ | I | ٧٣ |
| ٣ | <SPACE> | ٣٢ | ٢٣ | J | ٧٤ |
| ٤ | صفر | ٤٨ | ٢٤ | K | ٧٥ |
| ٥ | ١ | ٤٩ | ٢٥ | L | ٧٦ |
| ٦ | ٢ | ٥٠ | ٢٦ | M | ٧٧ |

| قيمة C40 | الرمز | قيمة آسكى | قيمة C40 | الرمز | قيمة آسكى |
|---|---|---|---|---|---|
| ٧ | ٣ | ٥١ | ٢٧ | N | ٧٨ |
| ٨ | ٤ | ٥٢ | ٢٨ | O | ٧٩ |
| ٩ | ٥ | ٥٣ | ٢٩ | P | ٨٠ |
| ١٠ | ٦ | ٥٤ | ٣٠ | Q | ٨١ |
| ١١ | ٧ | ٥٥ | ٣١ | R | ٨٢ |
| ١٢ | ٨ | ٥٦ | ٣٢ | S | ٨٣ |
| ١٣ | ٩ | ٥٧ | ٣٣ | T | ٨٤ |
| ١٤ | A | ٦٥ | ٣٤ | U | ٨٥ |
| ١٥ | B | ٦٦ | ٣٥ | V | ٨٦ |
| ١٦ | C | ٦٧ | ٣٦ | W | ٨٧ |
| ١٧ | D | ٦٨ | ٣٧ | X | ٨٨ |
| ١٨ | E | ٦٩ | ٣٨ | Y | ٨٩ |
| ١٩ | F | ٧٠ | ٣٩ | Z | ٩٠ |

**٢-٦-٢ فك الترميز**

يمكن عكس الترميز بسهولة. بافتراض وجود زوج من البايتات، دع (I1,I2) تدل على قيمها للأعداد الصحيحة بدون إشارة. وتجري إعادة حساب قيمة الـ ١٦ بت I16 كالآتي:

```
V16 = (I1 * 256) + I2
```

يمكن إعادة حساب الثلاثي (U1,U2,U3) بواسطة

```
U1 = (V16 - 1) div 1600

U2 = (V16 - (U1*1600) - 1) div 40

U3 = V16 - (U1*1600) - (U2*40) - 1
```

هنا مجدداً، تشير div إلى القسمة الصحيحة. ويمكن فك ترميز الرموز من الثلاثي (U1, U2, U3) بمجرد البحث عن القيم المقابلة في الجدول ٢.

**٢-٦-٣ الحشو**

لا يكون التعريف أعلاه واضح المعالم إلا إذا كان طول السلسلة المراد تشفيرها من مضاعفات العدد ثلاثة. على غرار تعريفات الحشو الواردة في [ISO / IEC 16022]، وتنطبق قواعد الحشو التالية:

أ) إذا بقيت قيمتان C40 (= رمزان) في نهاية سلسلة، يتم إكمال هاتين القيمتين C40 في ثلاثي قيمته بموجب الـ C40 صفرا (التحول ١). ويتم ترميز الثلاثي على النحو المحدد أعلاه.

ب) إذا بقيت قيمة C40 واحدة (= رمز واحد)، فإن البايت الأول له القيمة 254dec (0xFE). أما البايت الثاني فهو قيمة مخطط ترميز آسكي لـ "مصفوفة البيانات" DataMatrix للرمز المقابل لقيمته وفقا لـ C40. لاحظ أن مخطط ترميز آسكي في DataMatrix لأي رمز من رموز آسكي التي تقع في النطاق ٠-١٢٧ هو رمز آسكي مضافاً إليه ١.

# ٣- استخدام الختم الرقمي

يقدم هذا القسم وصفاً عاماً لاستخدام الختم الرقمي، والذي ينطبق على التأشيرة ووثائق السفر في حالات الطوارئ. يتم تحديد متطلبات محددة في ملفات التعريف المقابلة.

## ٣-١ قواعد المحتوى والترميز

***٣-١-١ العنوان***

يتم ترميز عنوان الأختام الرقمية وفقاً للقسم ٢-٢. وتعتمد قيمة آخر ٢ بايت لمرجع تعريف سمات الوثيقة وفئة نوع الوثيقة على ملف تعريف الوثيقة المحدد. ويجب أن تكون فئة نوع الوثيقة رقمًا فرديًا لملفات تعريف الإيكاو. **ويجوز** استخدام الأرقام الزوجية لملفات التعريف الوطنية التي لم تحددها الإيكاو.

**٣-١-٢ سمات الوثيقة المشفرة في الختم الرقمي**

سمات الوثيقة التي **يجب** تخزينها في الختم هي الجزء القابل للقراءة آلياً (MRZ):

**ويجب** أن يشفر الختم الرقمي الجزء القابل للقراءة آلياً للوثيقة. ويجوز لهذا الجزء أن يكون من أي نوع من الأنواع المحددة في الوثيقة Doc 9303. إلا أن ملفات تعريف الوثيقة المحددة يجوز لها أن تقيد فئات الأنواع المسموح بها من الأجزاء القابلة للقراءة آلياً.

**ويجوز** أن يحدد كل ملف تعريف الأجزاء الإضافية **المشروطة** و**الاختيارية**.

***٣-١-٣ قواعد الترميز لسمات الوثيقة***

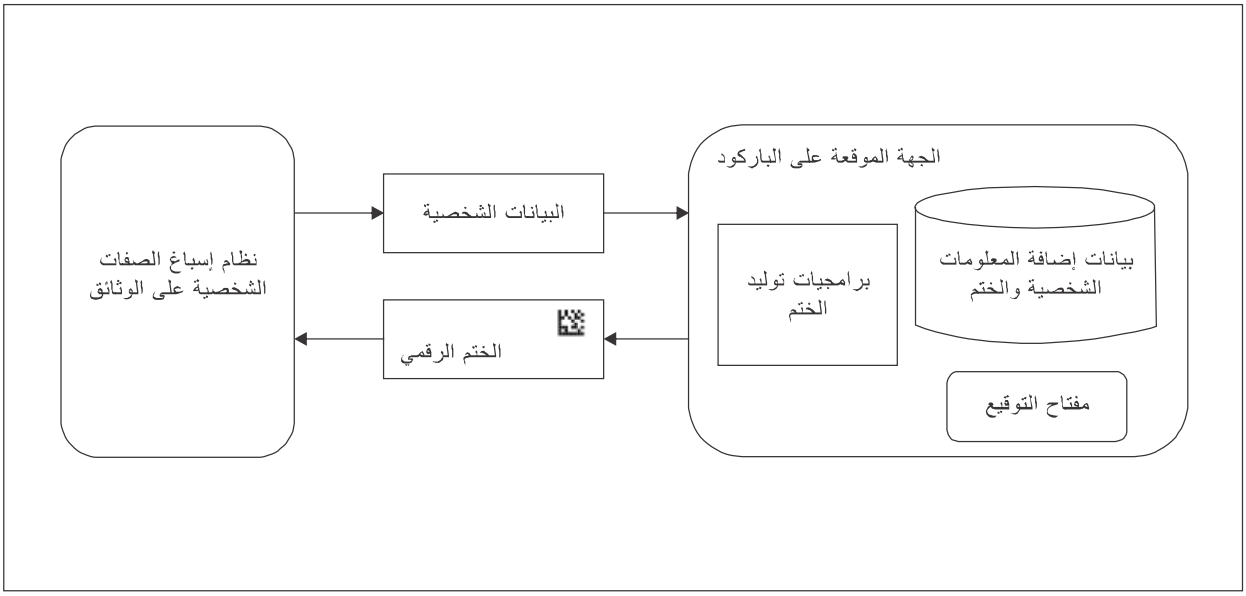
يعتمد ترميز سمات الوثيقة على مرجع تعريف سمات الوثيقة إلى جانب فئة نوع الوثيقة. يتم تحديد القيم المحددة في ملفات تعريف الوثائق المقابلة.

## ٣-٢ تصميم الجهة الموقعة على الباركود وختم الباركود

لإتاحة التحقق من الأختام الرقمية دون عناء، تستعين هذه الخاصية بقدرات البنية الأساسية للمفاتيح العامة (PKI) للسلطة الوطنية المعنية بالتوقيع على الشهادات (CSCA) الحالية لإصدار وتوزيع الشهادات بالإضافة إلى قوائم إلغاء الشهادات (CRLs). للحصول على تفاصيل وملفات تعريف الشهادات، انظر الوثيقة Doc 9303-12.

### ٣-٢-١ *بنية نظام الجهة الموقعة على الباركود*

تتلقى الجهة الموقّعة على الباركود من نظام إسباغ الصفات الشخصية على الوثائق بيانات تتيح تشفير ختم رقمي، وتستخدم مفتاح التوقيع لتوقيع الختم. ويوضح الشكل ٢ إحدى الطرق الممكنة لإنشاء الجهة الموقّعة على الباركود ونظام إسباغ الصفات الشخصية على الوثائق. الوثائق




**الشكل ٢- إضافة البيانات الشخصية للوثائق: سيناريو يتضمن وجود جهة مركزية للتوقيع على الباركود**

وتعتمد الجهة المُوقِّعة على الباركود على البرامجيات والبيانات التالية:

- ينتج *برنامج توليد الأختام* أختاماً رقمية مطابقة للمعيار الحالي. ويتلقى البيانات الشخصية التي يرسلها العميل، ويوقع على هذه البيانات بمفتاح توقيع خاص، ثم يقوم بترميز البيانات الشخصية والتوقيع في شكل باركود. والبيانات الشخصية والختم الرقمي هي بيانات الإدخال والإخراج، على التوالي، لبرامجيات توليد الختم. ويجب تخزين هذه البيانات مؤقتًا في الجهة الموقعة على الباركود أثناء عملية توليد الختم.
- تُستخدم *مفاتيح التوقيع* (المفتاح الخاص والعام) لتوقيع الختم الرقمي والتحقق منه. ومفتاح التوقيع الخاص هو أكثر البيانات أهمية للجهة الموقّعة على الباركود.

ورهناً بسيناريو النشر، لا يكون التمييز بين نظام البيانات الشخصية للوثائق والجهة الموقعة على الباركود دقيقاً دائماً. فعلى سبيل المثال، يمكن أن تكون الجهة المُوقِّعة على الباركود جزءاً من نظام البيانات الشخصية في سفارة ما. ويتمثل أحد السيناريوهات المحتملة في توسيع هذا النظام ليشمل توليد التوقيع، وتخزين مفاتيح التوقيع على بطاقة ذكية داخل السفارة. وهناك طريقة أخرى تتمثل في إيجاد جهة مركزية تتولى مهمة التوقيع على الباركود في البلد الأم، والسماح للسفارات بالاتصال بها عبر قناة آمنة. أخيراً، قد لا تقوم بعض السفارات بنفسها بإضافة البيانات الشخصية في الوثائق؛ وفي هذه الحالة يمكن أيضاً إعداد نظام البيانات الشخصية في البلد الأم ودمجه مع الجهة الموقعة على الباركود.

ونظراً لأن الجهة الموقعة على الباركود هي التي تقوم بإنتاج التوقيع، فهي تشكل مكوناً بالغ الأهمية. فالتوقيع يسمح بالتحقق من سلامة بيانات الباركود، أي ما إذا كان قد تم التلاعب بالبيانات، بالإضافة إلى صحتها، أي ما إذا كانت صادرة عن جهة معتمدة.

ومن أجل تحقيق مستوى تأمين عالٍ بما فيه الكفاية، **يوصى** بأن تكون الجهة المُوقِّع على الباركود إدارة مركزية، وألا يتم نشرها في السفارات، ما لم تحول أسباب تشغيلية أو تقنية أو لوجستية دون النشر المركزي. والغرض من هذا هو تركيز التدابير الأمنية في محيط محدود، مع مراعاة أفضل الممارسات التي تكفل إمكانية الاسترداد واستمرارية الأعمال. **ويجب** أن تتولى الجهة الموقّعة على الباركود تخزين مفاتيح التوقيع الخاصة بصورة مأمونة.

### ٣-٢-٢ *تأمين نظام توقيع الباركود*

**ينبغي** استضافة نظام توقيع الباركود وتشغيله وفقاً لأفضل الممارسات الأمنية في المجالات التالية: الأمن المادي؛ والبنية التحتية للخوادم والشبكات؛ وتطوير النظام وعمليات الدعم؛ والتحكم في إمكانية الوصول إلى المعلومات؛ وأمن العمليات. وإذا تم إعداد الجهة المُوقِّعة على الباركود كإدارة مركزية، **يوصى** بضمان الامتثال لـ [ISO/IEC 27002] في محيط الإدارة المسؤولة عن التُوقِيع على الباركود من أجل ضمان الامتثال لأفضل ممارسات الأمان هذه.

## ٤ – المراجع (معيارية)


[ISO/IEC 16022] ISO/IEC 16022 Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification, 2006

[ISO/IEC 18004] ISO/IEC 18004:2006: Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification, 2015

[ISO/IEC 24778] ISO/IEC 24778:2008: Information technology — Automatic identification and data capture techniques — Aztec Code bar code symbology specification, 2008

[ISO/IEC 27002] ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management, 2013

[ISO/IEC 15415] ISO/IEC 15415:2011: Information technology — Automatic identification and data capture techniques — Bar code symbol print quality test specification — Two-dimensional symbols, 2011

[X.690] ITU-T X.690 2008, DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS OSI networking and system aspects — Abstract Syntax Notation One (ASN.1) Information technology — ASN.1 encoding rules

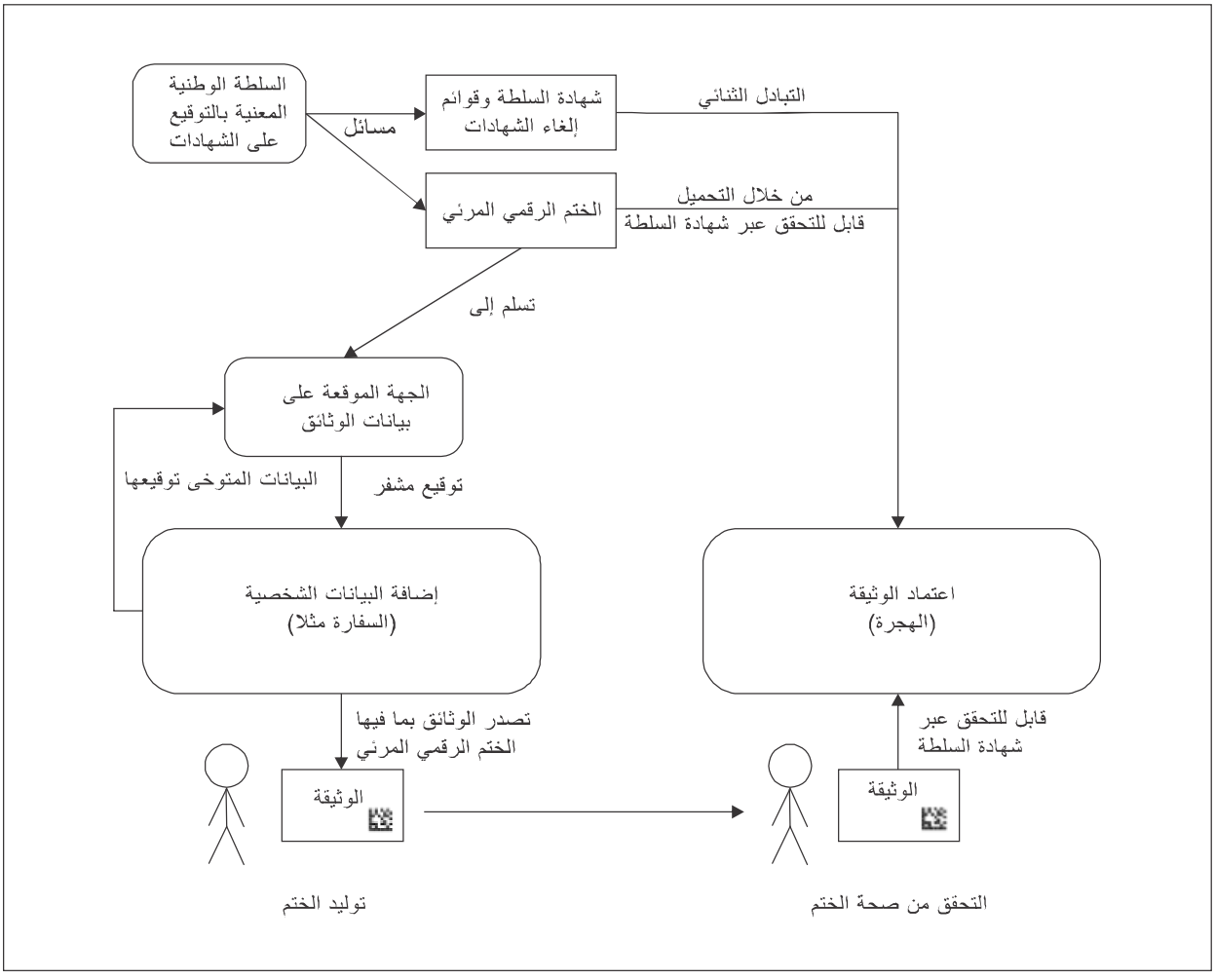

— — — — — — — —

# المرفق ألف بالجزء ١٣

# حالة الاستخدام النموذجي (إرشادي)

يقدم هذا القسم نظرة عامة على استخدام الختم الرقمي لحماية الوثائق غير الإلكترونية. وحالة الاستخدام قيد النظر هنا هي حماية وثيقة التأشيرة، على النحو الموضح في الشكل ألف– ١. ورغم أن التفاصيل الفنية قد تختلف بالنسبة لحالات الاستخدام الأخرى، إلا أن المبادئ العامة المنطبقة هي نفسها.

ويمكن تقسيم سير العمل العام إلى ثلاث خطوات. وكشرط أساسي، يجب استخراج شهادات الموقعين على التأشيرة (VSCs). وبعد ذلك، يجري توليد الأختام الرقمية، ثم التحقق من صحتها لاحقًا.




**الشكل ألف–١ حالة الاستخدام النموذجي للختم الرقمي المرئي**

### ألف–١ الشرط الأساسي: توليد شهادة الجهة الموقعة على التأشيرة

تستند البنية التحتية للمفاتيح العامة المتعلقة بتوقيع التأشيرة إلى إعداد البنية التحتية للمفاتيح العمومية لجوازات السفر الإلكترونية كما عرفتها الإيكاو. ونقطة الانطلاق لهذه العملية هي السلطة الوطنية المعنية بالتوقيع على الشهادات (CSCA) لكل بلد. وتقوم هذه السلطة بنشر الشهادات الخاصة بها التي تحتوي على مفتاحها العام. ولتعزيز الثقة بين البلدان، يتم توزيع شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات هذه بطريقة موثوقة عبر التبادل الثنائي، أو عبر القوائم الرئيسية.

الجهة الموقّعة على التأشيرة هي الهيئة التي توقع بالفعل على الأختام الرقمية. وتصدر الأختام الرقمية المرئية من قبل السلطة الوطنية المعنية بالتوقيع على الشهادات وبالتالي يمكن التحقق منها بواسطة شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات.

### ألف–٢ توليد الختم الرقمي

يتم توليد الختم الرقمي على خطوتين:

أ) يتقدم طالبو الحصول على التأشيرة بطلبهم في السفارة التي يقيمون فيها. وتقوم السفارة بتسجيل بيانات مقدم الطلب والتحقق مما إذا كان مقدم الطلب يفي بمتطلبات الحصول على التأشيرة. وإذا تم استيفاء المتطلبات، ترسل السفارة تمثيلًا رقمياً للبيانات المسجلة إلى الهية المعنية بالتوقيع على التأشيرات. ويمكن أن تكون هذه الجهة إما (١) كياناً مركزياً موجوداً في الدولة التي تصدر التأشيرة، وفي هذه الحالة تتصل السفارة بالجهة المعنية بالتوقيع على التأشيرات عبر قناة آمنة، أو (٢) كيانات لامركزية موجودة في كل سفارة تستخدم مثلا بطاقات ذكية تحتوي على مفاتيح تشفير متصلة مباشرة بنظام التخصيص. وفي كلتا الحالتين، يقوم الجهة المعنية بالتوقيع على التأشيرات بتوقيع البيانات المسجلة بشكل مشفر.

ب) للتوقيع، تستخدم الجهة المعنية بالتوقيع على الشهادات زوجاً من المفاتيح يتألف من مفتاح خاص ومفتاح عام. ويحدث التوقيع الفعلي باستخدام المفتاح الخاص، بينما يتم تخزين المفتاح العام في شهادة الجهة المعنية بالتوقيع على الشهادات. ويجري إرسال التوقيع الناتج مرة أخرى إلى نظام البيانات الشخصية للتأشيرات إذا لم تكن الجهة المُوقِّعة على التأشيرة جزءاً محلياً من النظام، وتتم طباعته على ملصق التأشيرة وإرفاقه بجواز سفر مقدم الطلب.

### ألف –٣ التحقق الرقمي من الختم

عند دخول طالبي الحصول على التأشيرة إلى البلد المُصدِر للتأشيرة، يقدمون تأشيراتهم إلى سلطة التحقق من التأشيرات (VVA)، مثل سلطة مراقبة الهجرة في بلد الإصدار. وتتحقق سلطة التحقق من التأشيرات من صحة وسلامة الختم الرقمي على التأشيرة من خلال التحقق من صحة التوقيع على الختم ومقارنة المعلومات المطبوعة على ملصق التأشيرة وعلى جواز السفر بالمعلومات الرقمية المخزنة في الختم. ويتم التحقق من توقيع الختم من خلال تحديد شهادة الجهة المعنية بالتوقيع على التأشيرات المسؤولة بمساعدة المعرِّف المخزن في عنوان الختم الرقمي، ثم استخدام المفتاح العام لشهادة الجهة المعنية بالتوقيع على التأشيرات. وكما هو موضح في الفقرات السابقة، يمكن التحقق من صلاحية شهادة هذه الجهة نفسها بواسطة شهادة السلطة الوطنية المعنية بالتوقيع على الشهادات.

**ملاحظة**

نظراً لأن جميع الشهادات متاحة للجمهور، يمكن التحقق من صحة التأشيرة من قبل *أي* طرف ثالث، وليس فقط من قبل الدولة المصدرة. وبالتالي يمكن لهذا النهج التعامل مع حالات الاستخدام لتجمعات البلدان، حيث تصدر دولة ما تأشيرة لدولة أخرى (كما هو الحال على سبيل المثال في الاتحاد الأوروبي). وهناك حالة استخدام أخرى تتمثل في التحقق من التأشيرات من قبل شركات الطيران قبل ركوب الطائرة.

**ملاحظة**

المعايير التي تحدد ما إذا كانت وثيقة التأشيرة يمكن الوثوق بها أم لا، بناءً على الختم الرقمي والأجزاء المقروءة آليا من التأشيرة وجواز السفر، يتم تعريفها في سياسة التحقق من صحة التأشيرة.

– – – – – – – – – – – –

# المرفق باء بالجزء ١٣

# تحويل أشكال توقيعات خوارزمية التوقيع الرقمي للمنحنى الإهليلجي (إرشادي)

### باء–١ تشفير العدد الصحيح وفقاً لقواعد التشفير الأساسية وقواعد التشفير المميزة

يتم ترميز الأعداد الصحيحة وفقاً لقواعد التشفير الأساسية (BER) وقواعد التشفير المميزة (DER) باعتبارها الترميز ذا النهاية الأكبر المميز بإشارة بأدنى حد من الطول، الذي يتم بعده تطبيق مخطط مقدار طول القسيمة (TLV). وتتميز هذه الأعداد بالحالات التالية:

أ) لنفترض أن قيمة العدد الصحيح موجبة، وأن الموضع الثنائي الأكثر أهمية (MSB) هو صفر في تمثيل العدد الصحيح الأدنى بدون إشارة. عليه يتخذ تمثيل العدد الصحيح بدون إشارة الشكل أدناه، وهو القيمة وفقا لقواعد التشفير الأساسية/ قواعد التشفير المتميزة:

```
|0bbbbbbb| ...
```

ب) لنفترض أن قيمة العدد الصحيح موجبة، وأن الموضع الثنائي الأكثر أهمية (MSB) هو إحدى تمثيلات العدد الصحيح الأدنى بدون إشارة، أي أن شكلها هو ...|1bbbbbbb|. إذن يتم وضع بايت يحتوي على أصفار في المقدمة وتكون القيمة وفقا لقواعد التشفير الأساسية/ قواعد التشفير المتميزة

```
|00000000|1bbbbbbb| ...
```

ج) لنفترض أن القيمة الصحيحة سالبة. في هذه الحالة يتم ترميز هذه القيمة كمكمل للاثنين، فمثلا عن طريق أخذ تمثيل العدد الصحيح الأدنى بدون إشارة، وعكسه، وإضافة واحد. بعد ذلك يتم ضبط الموضع الثنائي الأكثر أهمية (MSB) على واحد. فمثلا، بالنسبة إلى –٢٥٣٥٧، يكون تمثيل العدد الصحيح الأدنى بدون إشارة هو

```
|0110 0011|0000 1101|
```

ويتم عكس هذا إلى

```
|1001 1100|1111 0010|
```

ويُضاف واحد

```
|1001 1100|1111 0011|
```

مما ينتج عنه القيمة وفقا لقواعد التشفير الأساسية/ المتميزة. لاحظ أنه يمكن الاستدلال على أن الرقم سالب مباشرة من حقيقة أن الموضع الثنائي الأكثر أهمية (هنا أقصى اليسار) هو واحد.

أخيرًا، يحصل المرء على قيمة طول الوسم بوضع ٢ بايت أمام القيم المشفرة وفقا لقواعد التشفير الأساسية/ المتميزة أعلاه. البايت الأول هو الوسم ذات الثابت 0x02. ويحتوي البايت الثاني على طول (أي عدد بايتات) القيمة وفقا لقواعد التشفير الأساسية/ المتميزة المشفرة التالية. ويمكن فك التشفير ببساطة بسبل منها، على سبيل المثال، التمييز، وفقاً للموضع الثنائي الأكثر أهمية، بين ما إذا كان العدد المشفر صحيحًا سالبًا أم موجبًا، وتطبيق الخطوات المذكورة أعلاه في الاتجاه المعاكس.

### باء–٢ مثال

يعرض الجدول باء-١ بعض الأمثلة للأعداد الصحيحة المشفرة وفقا لقواعد التشفير الأساسية / المتميزة.

**الجدول باء– ١ أمثلة لتشفير بعض القيم الصحيحة وفقا لقواعد التشفير الأساسية/ المتميزة**

| *Value (dec)* | *Tag (hex)* | *Length (hex)* | *Value (hex)* | *Value (binary)* |
|---|---|---|---|---|
| **0** | **0x02** | **0x01** | **0x00** | **00000000** |
| **127** | **0x02** | **0x01** | **0x7F** | **01111111** |
| **128** | **0x02** | **0x02** | **0x00 0x80** | **00000000 10000000** |
| **-129** | **0x02** | **0x02** | **0xFF 0x7F** | **11111111 01111111** |

### باء–٣ توقيعات خوارزمية التوقيع الرقمي للمنحنى الإهليلجي وفقاً لقواعد التشفير المتميزة

وصف Abstract Syntax Notation One (ASN.1) لتوقيع خوارزمية التوقيع الرقمي للمنحنى الإهليلجي هو

```
Signature ::= SEQUENCE {
        r INTEGER, s INTEGER
}
```

يتم ترميز هذا التسلسل وفقاً لقواعد التشفير المتميزة باعتباره ثلاثي قيمة طول الوسم 0x30، بحيث يكون الطول عدد بايتات القيمة التالية، والقيمة كتسلسل ثلاثي قيمة طول الوسم لتشفير r المُلحق بتشفير s.

يرد في الجدول باء–٢ مثالان لتسلسلين – الأعداد الصحيحة r وs لتوقيع خوارزمية التوقيع الرقمي للمنحنى الإهليلجي هي بالطبع أكبر بكثير في الواقع العملي.

**الجدول باء– ٢ تسلسلان مشفران وفقاً لقواعد التشفير المتميزة لعددين صحيحين**

| *العدد الصحيح* | | *قيمة طول الوسم للتسلسل* | | |
|---|---|---|---|---|
| ***R*** | ***S*** | *الوسم* | *الطول* | *القيمة* |
| 127 | 1 | 0x30 | 0x06 | 0x02 0x01 0x7F 0x02 0x01 0x01 |
| 128 | 127 | 0x30 | 0x07 | 0x02 0x02 0x00 0x80 0x02 0x01 0x7F |

لاحظ أن r و s دائمًا أعداد صحيحة موجبة لتوقيع خوارزمية التوقيع الرقمي للمنحنى الإهليلجي. وبالتالي، للتحويل من توقيع خام إلى قواعد التشفير المتميزة، يتعين أولاً تقسيم التوقيع الأولي الخام إلى نصفين للحصول على r و s كل على حدة، ثم تشفيرهما على شكل تسلسل ASN.1 مشفر وفقاً لقواعد التشفير المتميزة حسب التعريف أعلاه. وعلى العكس من ذلك، لفك التشفير من توقيع بموجب خوارزمية التوقيع الرقمي للمنحنى الإهليلجي في قواعد التشفير المتميزة، يتعين أولاً فك تشفير التسلسل، واستخراج تمثيل العدد الصحيح بدون إشارة لـ r و s وضبط r و s بتمثيل طول ثابت (= طول حجم المفتاح) عن طريق تجريد أو إضافة بايتات الأصفار على اليسار إذا لزم الأمر (كمثال لذلك في حالة توقيع خوارزمية التوقيع الرقمي للمنحنى الإهليلجي بـ ٢٥٦ بت (ECDSA-256) يجب أن يكون طول كل من r و s ٢٥٦ بت = ٣٢ بايت)، وإلحاق القيمة الناتجة عن s بالقيمة الناتجة عن r.

– – – – – – – – – – – – –

# المرفق جيم بالجزء ١٣

# أمثلة للتشفير بمخطط الترميز C40 (إرشادي)

### جيم-١ المثال ١

بافتراض أنه يتعين ترميز السلسلة "XK<CD" . وبموجب تعريفها، تُستبدل جميع الحالات التي ترد فيها "<" بـ <SPACE> قبل الترميز. وبالتالي تصبح السلسلة الناتجة "XK CD" ، أي "XK<SPACE>CD " ( بإدخال مسافة واحدة). ويوضح الجدول جيم- ١ التشفير/ فك التشفير وفقا للمخطط C40 للسلسلة "XK<SPACE>CD ".

**الجدول جيم- ١ مثال لتشفير / فك تشفير السلسلة "XKCD"**

| ***Operation*** | ***Result*** | | | |
|---|---|---|---|---|
| original string | "XK<SPACE>CD" | | | |
| grouping into triples | (X, K, <SPACE>) | | (C, D, ) | |
| replacing with C40 values and padding | (37, 24, 3) | | (16, 17, padding) | |
| calculating the 16 bit integer value | 60164 | | 26281 | |
| | **Byte 1 (div)** | **Byte 2 (mod)** | **Byte 1 (div)** | **Byte 2 (mod)** |
| resulting byte sequence (decimal) | 235 | 4 | 102 | 169 |
| resulting byte sequence (hex) | 0xEB | 0x04 | 0x66 | 0xA9 |

### جيم-٢ المثال ٢

بافتراض أنه يتعين تشفير "XKCD". تتكون السلسلة فقط من أحرف كبيرة. يوضح الجدول جيم- ٢ التشفير/ فك التشفير وفقا للمخطط C40.

**الجدول جيم – ٢ مثال لتشفير/ فك تشفير السلسلة "XKCD"**

| ***Operation*** | ***Result*** | |
|---|---|---|
| original string | "XKCD" | |
| grouping into triples | (X, K, C) | (D, , ) |

| ***Operation*** | ***Result*** | | | |
|---|---|---|---|---|
| replacing with C40 values and padding | (37, 24, 16) | | (unlatch C40 and encode in ASCII) | |
| calculating the 16 bit integer value | 60177 | | | |
| | ***Byte 1 (div)*** | ***Byte 2 (mod)*** | ***Byte 1*** | ***Byte 2*** |
| resulting byte sequence (decimal) | 235 | 11 | 254 | 69 |
| resulting byte sequence (hex) | 0xEB | 0x11 | 0xFE | 0x45 |

– – – – – – – – – – – –

# المرفق دال بالجزء ١٣

# قواعد سياسة التحقق (إرشادي)

سياسة التحقق من الصحة هي عبارة عن مجموعة من قواعد التحقق التي تسمح بتحديد صلاحية الختم الموجود على الوثيقة. وينتج عن تطبيق سياسة التحقق من الصحة إشارة حالة بإحدى القيم التالية:

أ) **صالح**. تم تأكيد صحة الختم وسلامته. وتعني الصحة أن البيانات الموجودة في الختم قد تم توقيعها بالفعل بواسطة الجهة المعنية بالتوقيع على الباركود لبلد إصدار الوثيقة، وأن شهادة الموقّع على الباركود المعنية صالحة. وتعني السلامة أن بيانات الجزء المقروء آلياً الخاصة بالوثيقة المختوم لم يتم تعديلها، وأن الختم الرقمي لم يتم نقله من الوثيقة التي تم إرفاقه بها في الأصل.

ب) **غير صالح**. لم يتم التعرف على الختم على أنه صالح، وهناك حاجة إلى مزيد من التحقيق. قد يحدث البطلان للأسباب الثلاثة التالية:

١) *الاحتيال / التزوير*. يتضمن ذلك خلع الصفات الشخصية على وثيقة ما بصورة غير مصرح بها، باستخدام ملصق مسروق خال من الكتابة، أو إحداث تغييرات في البيانات الشخصية للوثيقة بناءً على ملصق أصلي، أو استبدال ملصق باركود من وثيقة مسروقة (مثل جواز السفر) بآخر، أو أي عمليات تزوير أخرى.

٢) *الضرر / التمزيق*. الأمر الذي يحول دون فك تشفير الباركود بسبب البلى أو التمزق أو البقع.

٣) *أخطاء غير معروفة و/ أو غير متوقعة*. ويشمل ذلك الأخطاء التي لا يمكن التنبؤ بها. مثل تلك التي تحدث بسبب الأخطاء الحاسوبية على مستوى تنفيذ البرنامج المستخدم لفك التشفير، أو الترميز الخاطئ أثناء اسباغ الصفات الشخصية على الوثيقة.

وإشعار الحالة **غير الصالح** يكون مصحوباً بإشعارات فرعية للحالة. وهذه توضح أسباب بطلان الختم. ونظراً لأن إمكانية الاحتيال تعتمد على هذه الأسباب، فمن المستحسن توصيف إشعارات الحالة والإشعارات الفرعية وفقاً لمستويات الثقة الثلاثة: "موثوقة" و "احتمالية احتيال متوسطة" و "احتمالية عالية للاحتيال". ويوضح الجدول دال –١ عملية التوصيف الموصى بها.

وتراعي سياسة التحقق العامة هذه دائماً الأسئلة التالية:

أ) هل الختم الرقمي المرئي صالح؟

ب) هل الجزء المقروء آليا بالوثيقة صالح؟

ج) هل يطابق الجزء المقروء آليا بالوثيقة الختم الرقمي المرئي؟

وفيما يلي قواعد التحقق من الصحة لكل نوع من أنواع الضوابط، وقائمة بمعايير التحقق، والنتائج المتوقعة لكل معيار، والإشعارات الفرعية للحالة الناتجة.

**التحقق من الختم الرقمي المرئي**

١ – التحقق من الشكل

- إذا كان شكل التشفير المادي غير متوافق مع المواصفات، أو إذا تعذر تصحيح الأخطاء الناجمة عن الضوضاء المادية، فهذا يعني أن الحالة **غير صالحة** مع الإشعار الفرعي READ_ERROR،

- إذا كان تنسيق الترميز (أي بنية الختم المكونة من العنوان والجزء الخاص بالرسائل والجزء الخاص بالتوقيع أو التشفير بمخطط الثنائي/ C40) غير متوافق مع المواصفات، أو
- إذا كانت القيم المتوقعة في العنوان غير معروفة، أو
- إذا كانت إحدى الخانات الإلزامية في الجزء الخاص بالرسائل مفقودة، أو
- إذا كان شكل الخانة في الجزء الخاص بالرسائل غير متوافق مع مواصفات الإصدار المحدد في العنوان فإن الحالة تكون غير صالحة مع الإشعار الفرعي WRONG_FORMAT، وفيما عدا ذلك، تابع، أو
- في حالة وجود خانة غير معروفة في الجزء الخاص بالرسائل، فيجب وضع الإشعار الفرعي UKNOWN_FEATURE. سيكون إشعار الحالة عندها **صالحًا** أو **غير صالح** اعتمادًا على صلاحية التوقيع الذي تم التحقق منه في الخطوات أدناه. لاحظ أنه إذا كان التوقيع صحيحًا، فإن وجود سمة غير معروفة وحده يجب ألا ينتهك صلاحية الختم.

٢- التحقق من صحة التوقيع

- إذا كانت شهادة الجهة الموقّعة على الباركود المشار إليها في عنوان الختم غير موجودة، فإن الحالة غير صالحة مع الإشعار الفرعي UNKNOWN_CERTIFICATE،
- إذا لم يتم توقيع شهادة الموقّع على الباركود المشار إليها في عنوان الختم من قبل السلطة الوطنية المعنية بالتوقيع على الشهادات، أو في حالة فشل التحقق من التوقيع، تكون الحالة غير صالحة مع الإشعار الفرعي UNTRUSTED_CERTIFICATE،
- إذا كانت شهادة الموقّع على الرمز الشريطي تحتوي على امتداد نوع الوثيقة وكان محتوى الباركود يحتوي على جزء مقروء آلياً، ولم يتم تضمين نوع وثيقة الجزء المقروء آلياً في ملحق نوع الوثيقة، تكون الحالة غير صالحة مع الإشعار الفرعي INVALID_DOCUMENTTYPE،
- إذا انتهت صلاحية شهادة الجهة الموقّعة على الباركود المشار إليها في عنوان الختم، تكون الحالة غير صالحة مع الإشعار الفرعي EXPIRED_CERTIFICATE،
- إذا تم إبطال شهادة الجهة الموقّعة على الباركود المشار إليها في عنوان الختم، فإن الحالة غير صالحة مع الإشعار الفرعي REVOKED_CERTIFICATE،
- إذا فشل التحقق من صحة العنوان والجزء الخاص بالرسائل باستخدام شهادة توقيع الباركود المشار إليها في عنوان الختم، تكون الحالة غير صالحة مع الإشعار الفرعي INVALID_SIGNATURE،
- فيما عدا ذلك، استمر.

**٣ - التحقق من صحة المُصدر**

- إذا لم تكن السلطة الوطنية المعنية بالتوقيع على الشهادات موثوقًا بها من قبل نظام التحقق من صحة الباركود في مجال الثقة الخاص به، تكون الحالة غير صالحة مع الإشعار الفرعي UNTRUSTED_CERTIFICATE، فيما عدا ذلك، استمر.

تغطي قواعد التحقق المذكورة أعلاه مقارنة البيانات المخزنة في الختم مقابل البيانات المخزنة في الجزء المقروء آليا للوثيقة. علاوة على ذلك، يمكن إجراء فحص يدوي لتلك البيانات المخزنة في الختم والمطبوعة على الوثيقة، ولكنها غير موجودة في الجزء المقروء آليا للوثيقة.

**الجدول دال– ١ مستويات الثقة الموصى بها للسياسة الخاصة بالوثائق**

| *إشعار الحالة* | *إشعار الحالة الفرعى* | *مستوى الثقة* |
|---|---|---|
| *صالحة* | - | *جدير بالثقة* |
| | UNKNOWN_FEATURE | |
| غير صالحة | READ_ERROR | *احتمالية احتيال متوسطة* |
| | EXPIRED_CERTIFICATE | |
| | WRONG_FORMAT | |
| | UNKNOWN_CERTIFICATE | *احتمالية احتيال عالية* |
| | UNTRUSTED_CERTIFICATE | |
| | INVALID_DOCUMENTTYPE | |
| | REVOKED_CERTIFICATE | |
| | INVALID_SIGNATURE | |

**— انتهى —**

ISBN 978-92-9275-582-9