الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1341

(2015/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة – التوصيات ذات الصلة بالبنية التحتية للمفاتيح العمومية

بروتوكول نقل البريد المعتمد وبروتوكول مكتب البريد المعتمد

التوصية ITU-T X.1341

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات ذات الصلة بالبنية التحتية للمفاتيح العمومية	**X.1340-X.1349**
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1341

بروتوكول نقل البريد المعتمد وبروتوكول مكتب البريد المعتمد

ملخص

تعرِّف التوصية ITU-T X.1341 بروتوكول نقل البريد المعتمد (CMTP) وبروتوكول مكتب البريد المعتمد (CPOP) من أجل تعزيز تبادل رسائل البريد الإلكتروني المعتمد في العالم بطريقة آمنة من خلال توفير السرية وتحديد هوية المتراسلين وضمان السلامة وعدم التنصل.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1341	2015-09-17	17	11.1002/1000/12352

الكلمات الأساسية

بروتوكول نقل البريد المعتمد، بروتوكول مكتب البريد المعتمد، CMTP، السرية، CPOP، السلامة، عدم التنصل، POP، بروتوكول مكتب البريد، الأمن، بروتوكول نقل البريد البسيط، SMTP.

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بمعرف الهوية الفريد للتوصية. ومثال على ذلك http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، كان الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

مقدمة

تزيد هذه التوصية من قدرات بروتوكول نقل البريد البسيط (SMTP) والإصدار الثالث من بروتوكول مكتب البريد (POP3) بحيث يتسنى لهما دعم الاستيقان والأمن وعدم التنصل.

ولهذا الغرض، تم تحديد بروتوكولين:

- بروتوكول نقل البريد المعتمد (CMTP) الذي يعد امتداداً لبروتوكول نقل البريد البسيط (SMTP)، هو البروتوكول الذي يدعم الاتصالات بين مرسِل الرسائل الإلكترونية ومخدم البريد، الذي يطلق عليه اسم مخدم البريد المعتمد (Cmail)؛
- بروتوكول مكتب البريد المعتمد (CPOP) الذي يعد امتداداً للإصدار الثالث من بروتوكول مكتب البريد (POP3)، هو البروتوكول الذي يدعم الاتصالات بين مستقبِل الرسائل الإلكترونية ومخدم البريد المعتمد (Cmail).

وداخل البروتوكولين SMTP وPOP3، يتم تحديد نمط رسالة عن طريق أمر، أي كلمة مفتاحية لبدء الرسالة. وبالنسبة للبروتوكولين CMTP وCPOP، تم تحديد أوامر جديدة مع توسيع بعض أوامر البروتوكولين SMTP وPOP3. وتم توسيع بعض الأوامر بصفة خاصة تحمل إشعارات (وثائق إلكترونية) تسمح بتوثيق مختلف مراحل الاتصالات بين المرسِل والمستقبِل والتحقق منها.

كما يطرح البروتوكولان CMTP وCPOP مفهوم مخدم البريد المعتمد الذي يعد شريكاً نشطاً في الاتصالات بين المرسِل والمستقبِل يسمح بتأكيد الحدوث الفعلي لعملية التبادل بين الطرفين.

ويفترض البريد المعتمد وجود بنية تحتية للمفاتيح العمومية (PKI).

والملحق A، الذي يعد جزءاً لا يتجزأ من هذه التوصية، يوفر مواصفة رسمية للإشعارات التي تستخدم تقنية الترميز (XSD) تعريف مخطط لغة الوسم الموسع (XML).

والملحق B، الذي يعد جزءاً لا يتجزأ من هذه التوصية، يوفر مواصفة رسمية للإشعارات التي تستخدم قواعد التركيب المجردة (ASN.1).

والملحق C، الذي يعد جزءاً لا يتجزأ من هذه التوصية، يوصف متطلبات شهادات المفاتيح العمومية الصادرة للعملاء (مرسِل ومستقبِل الرسائل الإلكترونية) ولمخدمات البريد المعتمد.

والملحق D، الذي يعد جزءاً لا يتجزأ من هذه التوصية، يوصف متطلبات استعمال مواصفة أمن طبقة النقل (TLS).

والملحق E، الذي يعد جزءاً لا يتجزأ من هذه التوصية، يوصف معرفات هوية الأشياء المعرفة لمخدم البريد المعتمد.

بروتوكول نقل البريد المعتمد وبروتوكول مكتب البريد المعتمد

1 مجال التطبيق

توصِّف هذه التوصية كيفية جعل رسائل البريد الإلكتروني موثوقة من حيث تحديد الهوية والسرية.

ويمكن بروتوكول نقل البريد المعتمد/بروتوكول مكتب البريد المعتمد (CPOP/CMTP) من:

- حل مشكلات التنصل نظراً لاستعمال التوقيع الإلكتروني؛
- حل مشكلات الكتمان نظراً لاستعمال التجفير؛
- إعداد إشعارات موثوقة بالإيداع وأخرى بالعبور وأخرى بالاستلام؛
- استعمال مخدم البريد المعتمد (Cmail) لتتبع الرسائل المعتمدة لتفادي فقدانها خلال العملية؛
- استعمال توصيلة لأمن طبقة النقل (TLS) لتوفر تعرف أقوى للهوية. ويحتاج مخدم البريد المعتمد هذا المستوى الأقوى من تعرف الهوية.

ولا يؤخذ الالتزام بما تدعو إليه هذه التوصية كأي دليل من الأدلة للمطالبة بالامتثال لأي قانون أو لائحة أو سياسة على الصعيد الوطني أو الإقليمي. ولا تضمن الوسائل التقنية والتنظيمية والإجرائية التي يرد وصفها في هذه التوصية بأي شكل من الأشكال تشكيل أي مستوى من الأمن قد يُسنَد إلى مراسلات معينة بموجب قانون محدد أو لائحة محددة أو سياسة محددة على الصعيد الوطني أو الإقليمي.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.520] التوصية ITU-T X.520 (2012) | المعيار ISO/IEC 9594-6: 2014، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: أنماط نعوت منتقاة*.

[ITU-T X.680] التوصية ITU-T X.680 (2008) | المعيار ISO/IEC 8824-1: 2008، *تكنولوجيا المعلومات – الترميز واحد لقواعد التركيب المجردة (ASN.1): توصيف الترميز الأساسي*.

[ITU-T X.690] التوصية ITU-T X.690 (2008) | المعيار ISO/IEC 8825-1: 2008، *تكنولوجيا المعلومات – قواعد تشفير الترميز ASN.1: توصيف قواعد التشفير الأساسية (BER) وقواعد التشفير المقننة (CER) وقواعد التشفير المميزة (DER)*.

[ITU-T X.693] التوصية ITU-T X.693 (2008) | المعيار ISO/IEC 8825-4: 2008، *تكنولوجيا المعلومات – قواعد تشفير الترميز ASN.1: قواعد تشفير اللغة XML (XER)*.

[ISO 3166-1] المعيار ISO 3166-1: 2013، *شفرات لتمثيل أسماء البلدان وأقسامها الفرعية – الجزء 1: الرموز الدليلية للبلدان*.

[IETF RFC 822] المعيار IETF RFC 822 (1982)، *معيار خاص بنسق رسائل نصوص الإنترنت ARPA*.

[IETF RFC 1939] المعيار IETF RFC 1939 (1996)، *بروتوكول مكتب البريد، الإصدار 3*.

[IETF RFC 2045] المعيار IETF RFC 2045 (1996)، *تمديدات متعددة الأغراض لبريد الإنترنت (MIME)، الجزء 1: نسق من أجل هيئات رسائل الإنترنت*.

[IETF RFC 5246] المعيار IETF RFC 5246 (2008)، *بروتوكول أمن طبقة النقل (TLS) - الإصدار 1.2 من البروتوكول*.

[IETF RFC 5321] المعيار IETF RFC 5321 (2008)، *بروتوكول نقل البريد البسيط*.

[XML] التوصية W3C XML1.0 (2000)، *لاتحاد الشبكة العالمية، الإصدار 1.0 من لغة الوسم القابلة للتمديد (XML) (الطبعة الخامسة)*.

[XSD] التوصية W3C XML Schema (2001)، *لاتحاد الشبكة العالمية، الجزء 1 من مخطط اللغة XML: البنى*.

3 التعاريف

1.3 مصطلحات معرفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 سلطة إصدار الشهادة (certification authority) (CA) [b-ITU-T X.509]: سلطة تتمتع بثقة مستعمل واحد أو عدة مستعملين لكي تصدر شهادات المفاتيح العمومية وتخصصها. ويمكن، اختيارياً أن تنشئ مفاتيح المستعملين.

2.1.3 إقرار صلاحية الشهادة (certificate validation) [b-ITU-T X.509]: عملية التأكد من أن شهادة ما صالحة في لحظة معينة، وربما تضمن ذلك إنشاء ومعالجة مسار إصدار الشهادة، والتأكد من أن جميع الشهادات في هذا المسار صالحة حتى هذه اللحظة (أي أنها لم تنته صلاحيتها بعد ولم يجر إبطالها).

3.1.3 دالة الاختزال (hash function) [b-ITU-T X.509]: دالة (رياضية) تقابل قيم ميدان واسع (وربما واسع جداً) تقيم مدى أضيق. ودالة الاختزال "الجيدة" هي التي ينتج عن تطبيقها على مجموعة (واسعة) من القيم في الميدان قيماً موزعة بالتساوي (عشوائياً في الظاهر) عبر المدى.

4.1.3 المفتاح الخاص (private key) [b-ITU-T X.509]: (في نظام تجفير مفتاح عمومي)، هو المفتاح الذي لا يعرفه إلا الكيان فقط من زوج المفاتيح المخصص للكيان.

5.1.3 المفتاح العمومي (public key) [b-ITU-T X.509]: (في نظام تجفير مفتاح عمومي)، هو المفتاح المعروف للعامة من زوج المفاتيح المخصص للمستعمل.

6.1.3 شهادة المفتاح العمومي (public-key certificate) (PKC) [b-ITU-T X.509]: المفتاح العمومي للمستعمل مصحوباً ببعض المعلومات الأخرى، التي تعتبر غير قابلة للتزوير، عن طريق توقيع رقمي بالمفتاح الخاص الذي تصدره سلطة إصدار الشهادة.

7.1.3 البينة التحتية للمفتاح العمومي (public-key infrastructure) (PKI) [b-ITU-T X.509]: البنية التحتية التي بمقدورها دعم إدارة مفاتيح عمومية تستطيع دعم خدمات الاستيقان أو التجفير أو السلامة أو عدم التنصل.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 البريد المعتمد (certified mail): بريد إلكتروني يتم تبادله باستخدام بروتوكول نقل البريد المعتمد (CMTP) وبروتوكول مكتب البريد المعتمد (CPOP).

2.2.3 بروتوكول نقل البريد المعتمد (certified mail transfer protocol) (CMTP): بروتوكول طبقة تطبيق عبر توصيلة بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP) على أساس بروتوكول نقل البريد البسيط (SMTP) وهو يستخدم لإرسال البريد المعتمد.

3.2.3 بروتوكول مكتب البريد المعتمد (certified post office protocol) (CPOP): بروتوكول طبقة تطبيق عبر توصيلة بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP) على أساس الإصدار الثالث من بروتوكول مكتب البريد (POP3) وهو يستخدم لاستلام البريد المعتمد.

4.2.3 مخدم البريد المعتمد (Cmail server): كيان موثوق يشارك في عمليات تبادل البريد المعتمد.

5.2.3 إشعار بالإيداع (notice of deposit): وثيقة إلكترونية موقعة من المرسِل ومخدم البريد المعتمد تتضمن معلومات تسمح بتأكيد حدوث عملية إيداع لبريد معتمد.

6.2.3 إشعار بالاستلام (notice of reception): وثيقة إلكترونية موقعة من المستلم ومخدم البريد المعتمد تتضمن معلومات تسمح بتأكيد حدوث عملية استلام بريد معتمد.

7.2.3 إشعار بالعبور (notice of transit): وثيقة إلكترونية موقعة من مخدمات البريد المعتمد المشاركة في عملية التبادل وتتضمن معلومات تسمح بتأكيد إرسال بريد معتمد إلى مخدم البريد المعتمد.

8.2.3 الإصدار 3 من بروتوكول مكتب البريد (POP3): بروتوكول طبقة تطبيق عبر توصيلة بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP) وهو يستخدم لاستلام البريد الإلكتروني.

9.2.3 بروتوكول نقل البريد البسيط (SMTP): بروتوكول طبقة تطبيق عبر توصيلة بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP) وهو يستخدم لإرسال البريد الإلكتروني.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

AES معيار تجفير متقدم *(Advanced Encryption Standard)*

ASN.1 الترميز واحد لقواعد التركيب المجردة *(Abstract Syntax Notation One)*

CA سلطة إصدار الشهادات *(Certification Authority)*

CBC تسلسل فدرات التشفير *(Cipher Block Chaining)*

Cmail بريد معتمد *(Certified Mail)*

CMTP بروتوكول نقل البريد المعتمد *(Certified Mail Transfer Protocol)*

CPOP بروتوكول مكتب البريد المعتمد *(Certified Post Office Protocol)*

DER قواعد التشفير المميزة *(Distinguished Encoding Rules)*

DNS نظام أسماء الميادين *(Domain Name System)*

id الهوية *(Identity)*

MIME تمديدات بريد الإنترنت متعددة الأغراض *(Multipurpose Internet Mail Extensions)*

PKI البنية التحتية للمفتاح العمومي *(Public-Key Infrastructure)*

POP3 الإصدار 3 من بروتوكول مكتب البريد *(Post Office Protocol version 3)*

RSA خوارزمية ريفيست وشامير وأدليمان *(Rivest, Shamir and Adleman algorithm)*

RSCK مفتاح تشفير متناظر عشوائي *(Random Symmetric Cypher Key)*

S/MIME تمديدات بريد الإنترنت متعددة الأغراض الآمنة *(Secure/Multipurpose Internet Mail Extensions)*

SMTP بروتوكول نقل البريد البسيط *(Simple Mail Transfer Protocol)*

TCP/IP بروتوكول التحكم في الإرسال/بروتوكول الإنترنت *(Transmission Control Protocol/Internet Protocol)*

TLS أمن طبقة النقل *(Transport Layer Security)*

UTF-8 نسق تحويل مجموعة السمات 8-UCS *(Universal Character Set Transformation Format-8)*

XER قواعد تشفير اللغة XML *(XML Encoding Rules)*

XML لغة الوسم القابلة للتمديد *(eXtensible Markup Language)*

XSD تعريف مخطط اللغة XML *(XML Schema Definition)*

5 الاصطلاحات

لا توجد.

6 المفاهيم الأساسية للبريد المعتمد

في اتصالات البريد الإلكتروني التقليدية التي تستعمل بروتوكول نقل البريد البسيط (SMTP) والإصدار 3 من بروتوكول مكتب البريد (POP3)، يمكن لمستلم البريد الإلكتروني أن يرفض استلام هذا البريد. وهذه هي الحالة عند إضافة تمديدات بريد الإنترنت متعددة الأغراض/الآمنة (S/MIME) إلى كدسة البروتوكول. وتوفر التمديدات S/MIME إمكانية تشفير الرسائل واستيقان المرسِل، بيد أنها لا توفر إثبات على التسليم.

وتوصِّف هذه التوصية كدسة بروتوكول تسمى البريد المعتمد وتتألف من البروتوكولين CMTP وCPOP.

وفي أي اتصالات للبروتوكولين POP3/SMTP، لا يكون مخدم البريد عنصراً نشطاً في الاتصالات، بل مجرد أداة لتمرير الرسائل التي يستلمها كما هي عندما يوقع عليها المستلم لمخدم البريد. وتكون هذه هي الحالة عند استعمال التمديدات SMIME.

وفي حالة البريد المعتمد، يشارك مخدم البريد بنشاط في الاتصالات بين المرسِل والمستقبِل بما يمكن مخدم البريد المعتمد من التحقق من أن المستقبِل وافق على استلام البريد. ويرسل البريد مشفراً لكي لا يتسنى لمخدم البريد المعتمد قراءة المحتوى الفعلي للبريد الإلكتروني. وترد أدناه نظرة عامة على هذا الإجراء، في حين ترد المواصفة بالتفصيل في الفقرة 8.

وتوصف التبادلات بين المرسِل ومخدم البريد المعتمد في الفقرة 8.

في حين توصف التبادلات بين المستقبِل ومخدم البريد المعتمد في الفقرة 9.

7 أنماط أوامر البريد المعتمد

يستعمل البريد المعتمد توليفة من الأوامر الحالية للبروتوكولين SMTP وPOP3، وبعض أوامر هذين البروتوكولين المحسنة وبعض الأوامر الخاصة بالبريد المعتمد تحديداً. والأوامر الواردة في الجدولين 1 و2 وليس لها ما يناظرها من أوامر في البروتوكولين POP3/SMTP توصف بكلمة "إضافي". والأوامر المحسنة من أوامر البروتوكولين POP3/SMTP توصف بكلمة "معدل". والأوامر الخاصة بهذين البروتوكولين وتستخدم كما هي بدون تغيير توصف بكلمة "بدون تغيير".

ويعرف نمط الأمر بكلمة رئيسية باستعمال الحروف الكبيرة بحيث يعرف نمط معين من الرسائل مع بعض المواصفات الإضافية لنمط الرسالة.

1.7 أنماط أوامر بروتوكول نقل البريد المعتمد (CMTP)

الجدول 1 – أوامر البروتوكول CMTP

الأمر	وظيفة الأمر
CELO إضافي	يمكن المخدم من تحديد معالجته لأوامر البروتوكول CMTP.
DELV إضافي	يحدد أسلوب التسليم: بريد معتمد.
MAIL FROM معدل	يحدد مرسِل الرسالة؛ يستعمل في الصورة "MAIL FROM". وإذا كان الحساب موجوداً على المخدم، فإنه يرسل كلمة base64 من شهادة المفتاح العمومي للمرسِل المعروف.
RCPT TO معدل	يحدد مستقبِلي الرسالة؛ يستعمل في الصورة "RCPT TO". وإذا كان الحساب موجوداً على المخدم، فإنه يرسل كلمة base64 من شهادة المفتاح العمومي للمرسِل المعروف. وإذا كان الحساب موجوداً على مخدم CMTP آخر جرت معه عمليات تبادل للمفتاح، فإن المخدم يستعلم من المخدم الثاني ويرسل كلمة base64 من شهادة المفتاح العمومي الخاص بالمستقبِل المعروف مع الأمر CHCK RCPT.
CHCK RCPT إضافي	لا يرسل إلا إذا كان المستقبِل ملحقاً بمخدم بريد معتمد آخر خلاف مخدم المرسِل.
DATA معدل	يرسل العميل للبدء في نقل محتوى رسالة. يرد المخدم بإشعار إيداع موقع من المخدم لكي يقوم المرسِل بتوقيعه.
DEPO إضافي	يرسله العميل لبدء نقل إشعار إيداع المحتوى الموقع من المخدم ومن المرسِل في المقابل.
SEND EVLP إضافي	إحالة الغلاف من مخدم بريد معتمد إلى مخدم بريد معتمد آخر.
HELP بدون تغيير	إعادة قائمة بالأوامر التي يدعمها مخدم البروتوكول CMTP.
QUIT بدون تغيير	إنهاء الدورة.

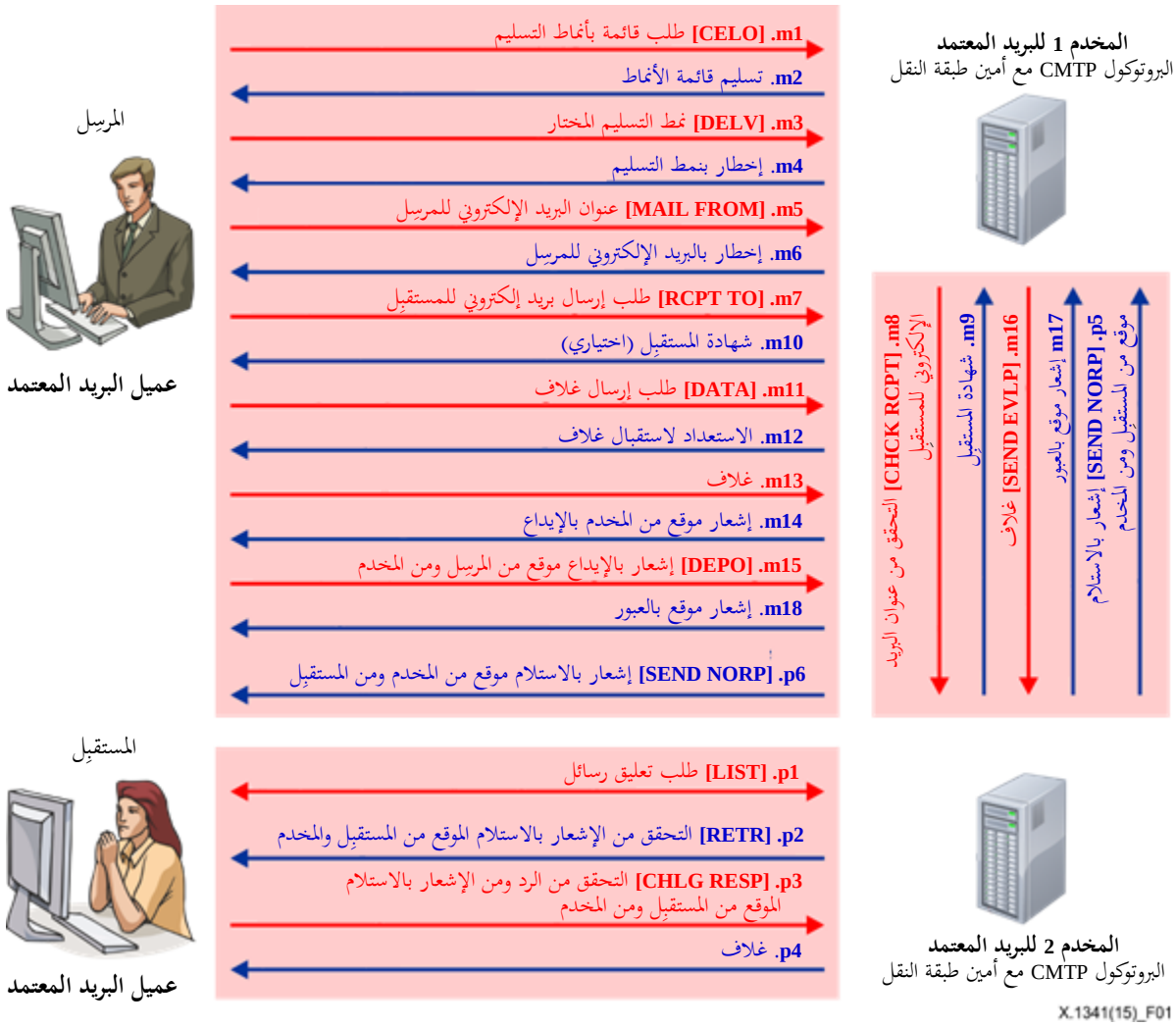
2.7 أنماط أوامر بروتوكول مكتب البريد المعتمد (CPOP)

الجدول 2 – أوامر البروتوكول CPOP

الأمر	وظيفة الأمر
USER بدون تغيير	يستعمل لتحديد اسم المستعمِل القائم بالتسجيل للدخول.
PASS بدون تغيير	كلمة المرور للمستعمِل القائم بالتسجيل للدخول.
LIST معدل	يستعمل لإعداد قائمة بالرسائل وحجمها. فمثلاً استعمال الأمر LIST بدون معلمات سيعيد رسالتين OK+2 (320 أثمون) مع قائمة بالرسائل: الهوية (id) والطول وأسلوب التسليم (إن وجد) مثل البريد المعتمد.

الجدول 2 – أوامر البروتوكول CPOP

الأمر	وظيفة الأمر
RETR معدل	بفرض *N* عدد بين 1 وآخر عدد يعاد بالأمر LIST. فإنه لا يمكن أن يستخدم هذا الأمر لاستعادة رسالة وسمت من قبل بأنها ملغاة. إذا لم يكن هناك أسلوب للتسليم، يرسل المخدم البريد الإلكتروني بتشفير التمديدات MIME. وفي حالة تحديد أسلوب التسليم، فمثلاً، مع البريد المعتمد، يقوم المخدم بمعالجة الرسالة حسب الأسلوب. يتحقق المخدم من المستقبِل قبل إرسال الغلاف باستخدام الأمر RCPT.
CHLG RESP إضافي	يرسل العميل لتقديم إشعار باستلام الرسالة مع الإجابة على السؤال السري. فإذا كانت الإجابة صحيحة، يرد المخدم بإرسال الغلاف MIME.
SEND NORP إضافي	إرسال إشعار موقع بالاستلام.
HELP بدون تغيير	إعادة قائمة بالأوامر التي يدعمها المخدم CPOP.
QUIT بدون تغيير	إنهاء الدورة.



الشكل 1 – نظرة عامة على تبادلات البروتوكول

الأوامر المسبوقة بحرف "m" تستخدم في البروتوكول CMTP والمسبوقة بحرف "p" تستخدم في البروتوكول CPOP. وتعرض الفقرات من 1.8 إلى 18.8 مواصفات تفصيلية للتبادلات من m 1 إلى m 18 المبينة في الشكل 1، في حين تعرض الفقرة 9 مواصفات تفصيلية للتبادلات من p1 إلى p6.

1.8 CELO: طلب قائمة بأنماط التسليم

يرسل نمط الأمر كرسالة SMTP مثل الأمر HELO يتبعه اسم ميدان كامل التأهيل. والغرض منه استعادة قائمة بأنماط التسليم.

2.8 قائمة بأنماط التسليم

تقدم قائمة أنماط التسليم استجابةً للأمر CELO. وهي نسق SMTP بالمحتوى التالي (لا يرتبط بالحالة):

250-<Fully qualified domain name of the Cmail server>
250-8BITMIME
250-Delivery-Types CertifiedMail <other delivery types>
250 OK

تقدم هذه التوصية مواصفات البريد المعتمد. يمكن للصيغ الأخرى أن تقدم مواصفات أنماط التسليم الأخرى.

3.8 نمط التسليم المختار

تحدد هذه الرسالة نمط التسليم من بين الأنماط المحددة في قائمة أنماط التسليم. ويكون على النسق (SMTP) التالي:

DELV <delivery type>

4.8 الإخطار بنمط التسليم

في حال الموافقة على نمط التسليم المختار، تكون هذه الرسالة على النسق SMTP التالي (لا يرتبط بالحالة):

250 Delivery-Type <delivery type>OK

ويكون الرد كالتالي في حالة وجود خطأ في قواعد تركيب رسالة نمط التسليم المختار:

501 Syntax: DELV <delivery type>

ويكون الرد كالتالي في حالة صدور رسالة نمط التسليم المختار خارج التسلسل:

501 Syntax: use CELO command first

ويكون الرد كالتالي عندما تكون رسالة نمط التسليم المختار غير معروفة:

501 Unknown Delivery-Type: <delivery type>

5.8 عنوان البريد الإلكتروني للمرسِل

ترسل هذه الرسالة إلى مخدم البريد المعتمد لطلب إرسال بريد معتمد مع إمكانية طلب شهادة المفتاح العمومي للمرسِل من مخدم البريد المعتمد.

MAIL FROM <sender's email address> [CertificateRequested]

6.8 إخطار بالبريد الإلكتروني للمرسِل

ترسل هذه الرسالة لتأكيد وجود عنوان البريد الإلكتروني للمرسِل في قاعدة بيانات مخدم البريد المعتمد. وإذا ما طلب المرسِل شهادة مفتاحه العمومي، تضاف هذه الشهادة:

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

7.8 طلب إرسال بريد إلكتروني للمستقبِل

ترسل هذه الرسالة إلى مخدم البريد المعتمد لطلب إرسال بريد معتمد إلى المستقبِل مع إمكانية طلب شهادة المفتاح العمومي للمستقبِل من مخدم البريد المعتمد:

RCPT TO <recipient's email address> [CertificateRequested]

يمكن استخدام هذا الأمر لأي عدد ممكن من المرات حسب الضرورة من أجل إضافة جميع المستقبِلين في حال تعددهم. والمعلومات التي تبين المستقبِل الأصلي (To) أو المرسَل إليه نسخة (CC) تدرج في رأسية الغلاف [IETF RFC 5321]. غير مسموح بإرسال نسخ لمستقبِلين متعددين (Cci).

8.8 التحقق من عنوان البريد الإلكتروني للمستقبِل من جانب مخدم البريد المعتمد البعيد

لا ترسل هذه الرسالة إلا إذا كان المستقبِل ملحق بمخدم بريد معتمد آخر خلاف المخدم الخاص بالمرسِل. وترسل من مخدم البريد المعتمد بالمرسِل إلى مخدم البريد المعتمد الخاص بالمستقبِل للتحقق من صلاحية عنوان البريد الإلكتروني مع إمكانية طلب شهادة المفتاح العمومي للمستقبِل.

CHCK RCPT <recipient's email address> [CertificateRequested]

9.8 الإخطار بعنوان البريد الإلكتروني للمستقبِل

ترسل هذه الرسالة رداً على الرسالة "التحقق من عنوان البريد الإلكتروني للمستقبِل من جانب مخدم البريد المعتمد البعيد".

والرسالة التالية تؤكد عنوان البريد الإلكتروني وتتضمن شهادة المفتاح العمومي للمستقبِل إذا طلب:

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

وفي حالة عدم القدرة على تأكيد عنوان البريد الإلكتروني، يمكن إرسال رسالة الخطأ التالية:

503 Sender already specified

ترسل إذا كانت رداً على طلب مزدوج.

501 Syntax: CHCK RCPT <address>

ترسل إذا كان هناك خطأ في قواعد تركيب عنوان البريد الإلكتروني للمستقبِل.

501 Syntax: CHCK RCPT <address> Error in parameters <parameter>

ترسل إذا لم يتم تمييز المعلمة التي تلي عنوان البريد الإلكتروني.

553 <email address> Invalid email address

ترسل إذا كان عنوان البريد الإلكتروني غير موجود في مخدم البريد المعتمد البعيد.

10.8 إخطار بالبريد الإلكتروني للمستقبِل

ترسل هذه الرسالة لتأكيد وجود عنوان البريد الإلكتروني للمستقبِل. وإذا طلب المرسِل شهادة المفتاح العمومي للمستقبِل، تضاف هذه الشهادة.

ما يلي يؤكد عنوان البريد الإلكتروني ويتضمن شهادة المفتاح العمومي للمستقبِل.

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

في حالة عدم القدرة على تأكيد عنوان البريد الإلكتروني، يمكن إرسال رسالة الخطأ التالية:

503 Error: need MAIL FROM command

ترسل في حالة إرسال الرسالة خارج التسلسل.

452 Error: too many recipients

ترسل في حالة تحديد عدد كبير جداً من المستقبِلين.

501-6.1.1 Syntax: RCPT TO <address>

ترسل في حالة وجود خطأ في قواعد تركيب عنوان البريد الإلكتروني للمستقبِل.

501-6.1.2 Syntax: RCPT TO <address> Error in parameters: <parameters>

ترسل في حالة عدم تمييز المعلمة بعد عنوان البريد الإلكتروني.

550-5.1.1 <email address> Invalid email address.

ترسل في حالة عدم وجود عنوان البريد الإلكتروني.

11.8 طلب إرسال غلاف

ترسل الرسالة التالية إذا كان مخدم البريد المعتمد مستعداً لاستقبال بيانات:

DATA

12.8 الاستعداد لاستقبال غلاف

ترسل الرسالة التالية إذا كان مخدم البريد المعتمد مستعداً لاستقبال بيانات:

354 Start mail input; end with <CRLF>.<CRLF>

وترسل الرسالة التالية في حالة عدم إرسال الأمر MAIL FROM:

503 Error: need MAIL FROM command

وترسل الرسالة التالية في حالة عدم إرسال الأمر RCPT TO:

503 Error: need RCPT TO command

وترسل الرسالة التالية في حالة عدم إرسال الأمر DELV:

503 Error: need DELV command

13.8 غلاف

يقوم العميل بما يلي:

1 ينشئ مفتاح تشفير متناظر عشوائي RSCK مثل معيار التشفير المتقدم (AES) 256؛

2 يقوم بتجفير متن الرسالة والمرفقات، إن وجدت، بهذا المفتاح؛

3 إنشاء رسالة MIME تتضمن جزءاً يطلق عليه اسم غلاف (ENVELOPE) يتضمن الرسالة المجفرة (انظر المعيار [IETF RFC 2045])؛

4 اختتام الرسالة بما يلي: <CR><LF>.<CR><LF>؛

5 إرسال الرسالة MIME.

14.8 إشعار بالإيداع موقع من المخدم

250 Notice-of-deposit:
<notice of deposit signed by the Cmail server encoded in base64>
250 Ok

يصدر المخدم إشعاراً بالإيداع يتضمن معلومات عن الغلاف (معرف هوية الغلاف ونمط التسليم ودالة الاختزال MIME) ويوقعه بمفتاحه الخاص.

15.8 إشعار بالإيداع موقع من المرسِل والمخدم

يقوم المرسِل:

1 بفك شفرة الإشعار بالإيداع المستلم؛

2 بالتحقق من كل مستقبِل؛

3 بتوقيع الإشعار بالإيداع الموقع من المخدم باستعمال مفتاحه العمومي؛

4 تشفير النتيجة بشفرة base64؛

5 إرسال النتيجة إلى مخدم البريد المعتمد بواسطة الأمر:

DEPO <notice of deposit base64 encoded>

يعرف التحقق في الملحق A، الشكل A.6.

يتضمن التحقق **SecretQuestion** و**CipherEnvelopeKey** وشهادة المفتاح العمومي للمستقبِل.

يتألف **SecretQuestion**: من طلب (**Request**) ورد (**Response**).

وقد يتضمن الطلب **RandomNumber**. ويتضمن الرد **AlgorithmIdentifier** يعيد المرسِل حسابه من أجل استلام ENVELOPE. ويعرف **AlgorithmIdentifier** هذا الخوارزمية المستخدمة في حساب دالة الاختزال (hash). ويشمل التحقق أولاً استعادة مفتاح الشفرة RSCK المشفر بالمفتاح العمومي للمستقبِل، ثم الربط بين **RandomNumber** وRSCK وحساب دالة الاختزال من أجل بناء الرد.

مثال على عملية تحقق بلغة الوسم القابلة للتمديد (XML):

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1"
Encoding="base64">5mYZWhtl0yxBa/wl7VLiiQ=</response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

الملاحظة 1 – يستطيع هذا التحقق استخدام قواعد التشفير المميزة (DER) للترميز ASN.1.

الملاحظة 2 – لا يستطيع المخدم إعادة حساب دالة الاختزال ما دام لا يعرف مفتاح التشفير. ومع ذلك، يعرف المخدم النتيجة المتوقعة فقط من حساب دالة الاختزال.

الملاحظة 3 – خلال التحقق مع المستقبِل، لا يرسل المخدم إلا السؤال السري وينتظر رد المستقبِل.

16.8 الغلاف (ENVELOPE) بين مخدمات البريد المعتمد

لا ترسل الرسالة المعرفة في الفقرة 13.8 إلى مخدم بريد معتمد آخر إلا إذا كان المرسِل والمستقبِل ملحقين بمخدمي بريد معتمد مختلفين (انظر البند m16 في الشكل 1).

SEND EVLP <MIME message>

17.8 الإشعار الموقع بالعبور بين مخدمات البريد المعتمد

يستخدم النسق التالي:

250 Notice-of-transit:
<notice of transit base64 encoded>

ترسل الرسالة التالية إذا استقبل مخدم البريد المعتمد إشعاراً بالعبور:

250 Ok

وترسل الرسالة التالية في حالة عدم صحة الإشعار بالعبور:

503 Error: incorrect Notice-of-transit

يعد الإشعار بالعبور البريد المعتمد الذي تسلم الغلاف (ENVELOPE).

ويقوم مخدم البريد المعتمد هذا بإعداد إشعار بالإيداع يتضمن معلومات عن الغلاف (معرف هوية الغلاف ونمط التسليم ودالة الاختزال MIME) ويوقعه بمفتاحه العمومي. وهذا الإشعار مماثل لإشعار الإيداع.

18.8 الإشعار الموقع بالعبور

يقوم المخدم مرسِل البريد المعتمد:

1 بفك شفرة الإشعار بالعبور المستلم؛

2 بتوقيع الإشعار بالعبور الموقع من المخدم باستعمال مفتاحه العمومي؛

3 بتشفير النتيجة بشفرة base64؛

4 بإرسال النتيجة إلى مخدم البريد المعتمد باستخدام الأمر:

250 Signed-notice-of-transit:
<signed notice of transit base64 encoded>
250 Signed-notice-of-deposit:
<signed notice of deposit base64 encoded>
250 Ok

9 بروتوكول صندوق البريد المعتمد (CPOP)

يرد في الفقرات من 1.9 إلى 6.9 شرح البنود p1 إلى p6 في الشكل 1.

1.9 طلب تعليق رسائل

تجهيز المعلومات بشأن تعليق الرسائل باستخدام الإجراء المحدد في الفقرة 5 تحت الأمر LIST في المعيار [IETF RFC 1939] مع معلمة إضافية. وبالنسبة إلى كل سطر يفصل رسالة معلقة، تضاف المعلمة الإضافية للإشارة إلى نمط التسليم إذا لم يكن بريداً إلكترونياً عادياً (انظر البند p1 في الشكل 1). مثال:

C: LIST
S: +OK 2 messages (320 octets)
S: 1 120
S: 2 200 CertifiedMail
S: .

يشمل هذا الإجراء أيضاً استعادة جميع الرسائل الإلكترونية العادية مع ترك الرسائل الموسومة فقط بنمط تسليم على مخدم البريد المعتمد.

2.9 التحقق من الإشعار بالاستلام الموقع من المستقبِل والمخدم

بالنسبة إلى الرسائل الموسومة بنمط التسليم لا يستعيد الأمر RETR الرسالة، بل يستعيد التحقق والإشعار بالاستلام الموقع من المخدم المشفر بالشفرة base64. ويتحقق العميل من التوقيع الرقمي ومن شهادة المرسِل الواردين بالإشعار بالاستلام.

مثال:

C: RETR 2

ترسل الرسالة التالية إذا أرسل مخدم البريد المعتمد الإشعار بالاستلام:

S: +OK 200 octets
S: <the Cmail server sends the notice of reception including the challenge>
S: .

وترسل الرسالة التالية عندما لا يتمكن المخدم من إرسال الإشعار بالاستلام:

503 Error: impossible to send Notice-of-reception

ويجد مخدم البريد المعتمد في الإشعار بالإيداع هوية العقدة **Entity** المتصلة بالمستلم. ويقوم مخدم البريد المعتمد بعد ذلك بنسخ هذه العقدة في الإشعار بالاستلام ويزيل محتوى عقدة **Response** الوارد في عقدة الهوية **Entity**.

مثال على عقدة في الإشعار بالإيداع:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1"
Encoding="base64">5mYZWhtl0yxBa/wl7VLiiQ=</response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

الملاحظة 1 – يمكن لهذا التحقق استخدام التشفير ASN.1 DER.

ويتم استنساخ نفس العقدة في الإشعار بالاستلام:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64" />
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

الملاحظة 2 – يمكن لهذا التحقق استخدام التشفير ASN.1 DER.

3.9 التحقق من الردود ومن الإشعار بالاستلام الموقع من المستقبِل ومن المخدم

يقوم المستقبِل:

1 بفك شفرة الإشعار بالاستلام الوارد؛

2 باستعادة المفتاح RSCK؛

3 بحساب الرد على التحقق؛

4 بالتوقيع على الإشعار بالاستلام الموقع من المخدم باستعمال مفتاحه الخاص؛

5 تشفير النتيجة بشفرة base64؛

6 إرسال النتيجة إلى مخدم البريد المعتمد باستخدام الأمر:

CHLG RESP <challenge response and recipient and server signed notice of reception>

يقوم المستقبِل بفك شفرة الرسالة كالتالي:

```
<Entity EmailAddress="john.doe@example.org" Type="to">
  <SecretQuestion>
    <Request RandomNumber="30987497498789739837"/>
   <Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64"></response>
  </SecretQuestion>
  <CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER"
KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>
  <Certificate
Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…
/gy7</Certificate>
</Entity>
```

ملاحظة – يمكن لهذا التحقق استخدام التشفير ASN.1 DER.

يستعيد المستقبِل المفتاح RSCK باستعمال مفتاحه العمومي بفك شفرة محتوى العقدة **CipherEnvelopeKey**. ويقوم المستقبِل بعد ذلك بالربط بين **RandomNumber** والمفتاح RSCK واختزالهما باستخدام المعرف **AlgorithmIdentifier** المحدد والحصول على نتيجة السؤال **SecretQuestion**.

ويقوم المستقبِل باستنساخ النتيجة في الإشعار الموقع بالاستلام، وتوقيتها وإرسالها إلى مخدم البريد المعتمد.

4.9 الغلاف (ENVELOPE)

إذا كان التحقق سليماً (OK)، يرسل مخدم البريد المعتمد الغلاف (ENVELOPE) بنفس الطريقة كنتيجة للأمر RETR. ولدى المستقبِل الآن الرسالة والمفتاح اللازم لفتحها.

وترسل الرسالة التالية إذا لم يتمكن المخدم من إرسال الغلاف:

503 Error: impossible to send ENVELOPE

5.9 إشعار بالاستلام موقع من المستلم ومن المخدم بين مخدمي البريد المعتمد (اختياري)

لا ترسل هذه الرسالة إلا عندما يكون المرسِل والمستقبِل ملحقين بمخدمي بريد معتمد مختلفين:

SEND NORP <base64 encoded Recipient and server signed notice of reception>

6.9 إشعار بالاستلام موقع من المستلم ومن المخدم

لا ترسل هذه الرسالة إلا عندما يكون المرسِل والمستقبِل ملحقين بمخدمي بريد معتمد مختلفين:

SEND NORP <base64 encoded Recipient and server signed notice of reception>

الملحق A

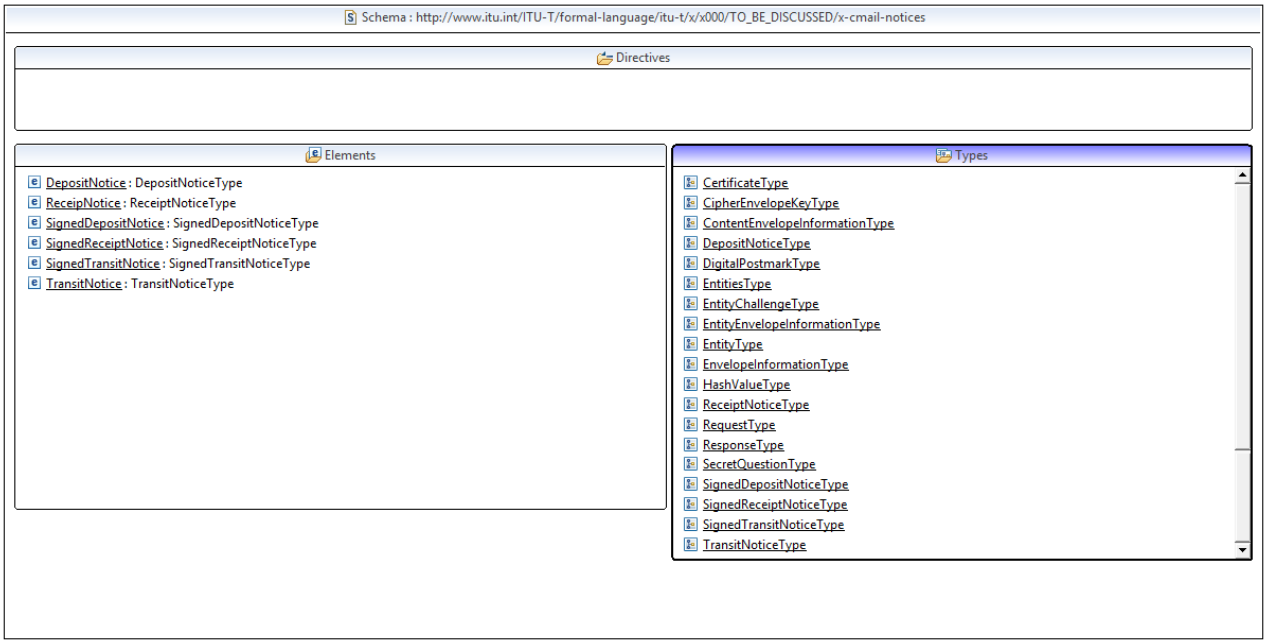
إشعارات بتعريف مخطط اللغة XML (XSD)

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

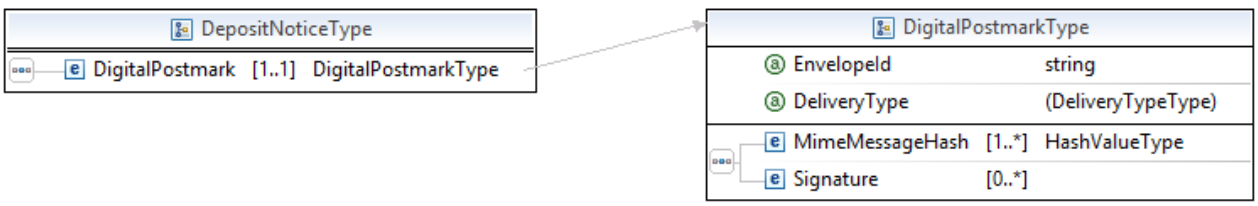
يوصِّف هذا الملحق مواصفة الإشعارات التي تستخدم تعريف مخطط اللغة XML كما هو موصف بالمواصفة [XSD]. هناك مثال للاتصالات مشفر باللغة XML كما هو موصف بالمواصفة [XML] ويجب أن يكون طبقاً لمواصفات التعريف XSD الواردة بهذا الملحق.

1.A استعراض شامل للتعريف XSD

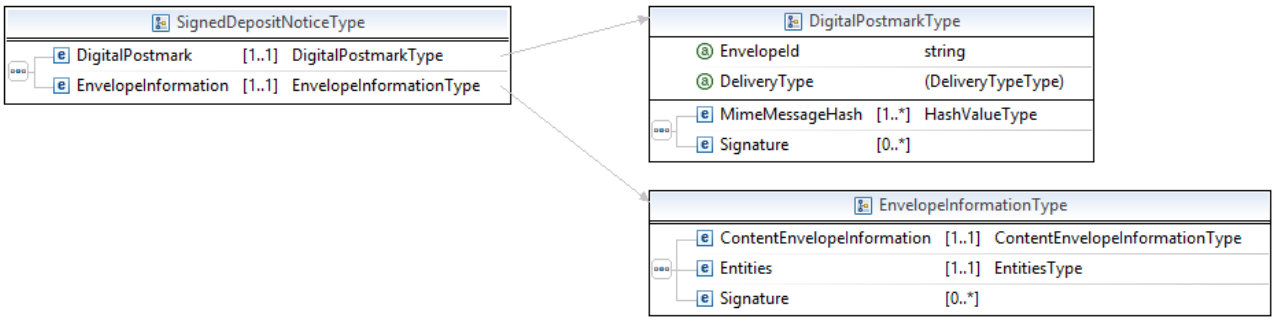
انظر الأشكال من 1.A حتى 10.A.



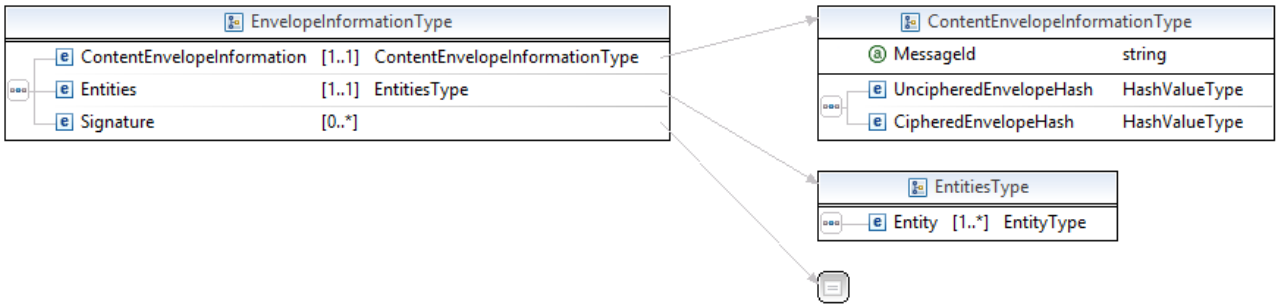
الشكل 1.A – العناصر وقائمة الأنماط



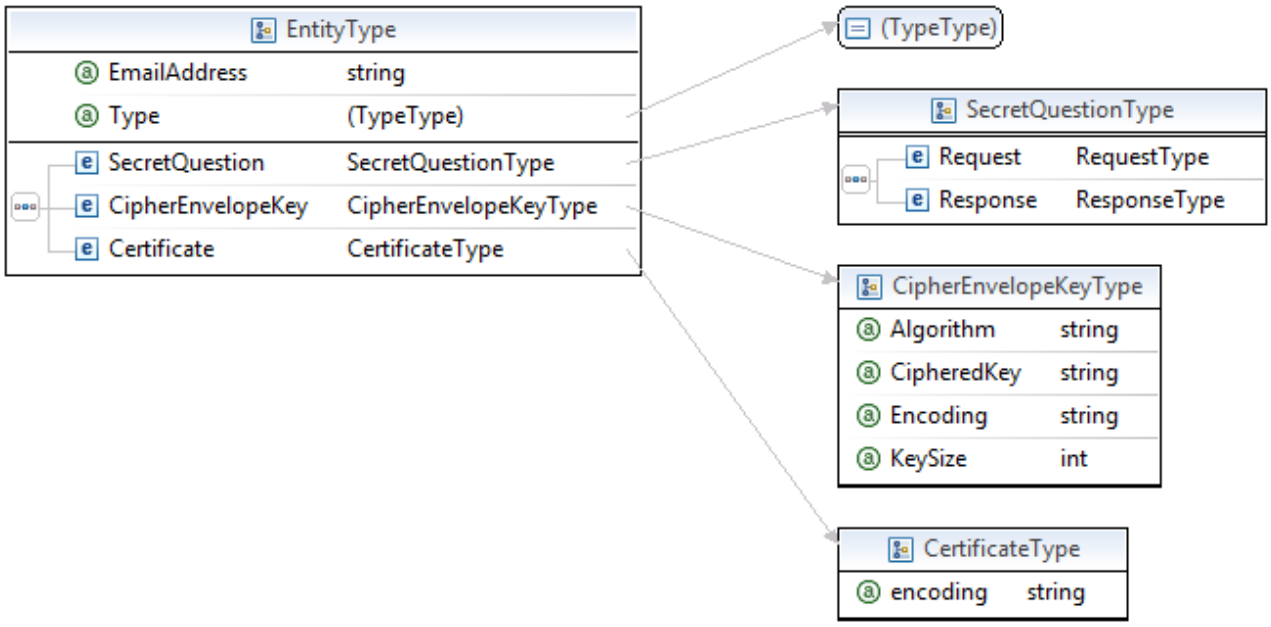
الشكل 2.A – الإشعار بالإيداع



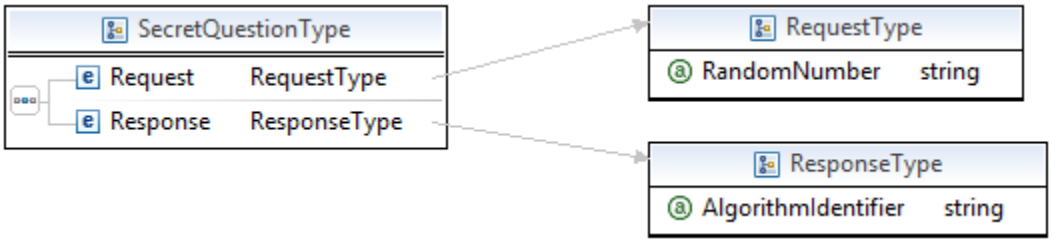
الشكل 3.A – الإشعار الموقع بالإيداع



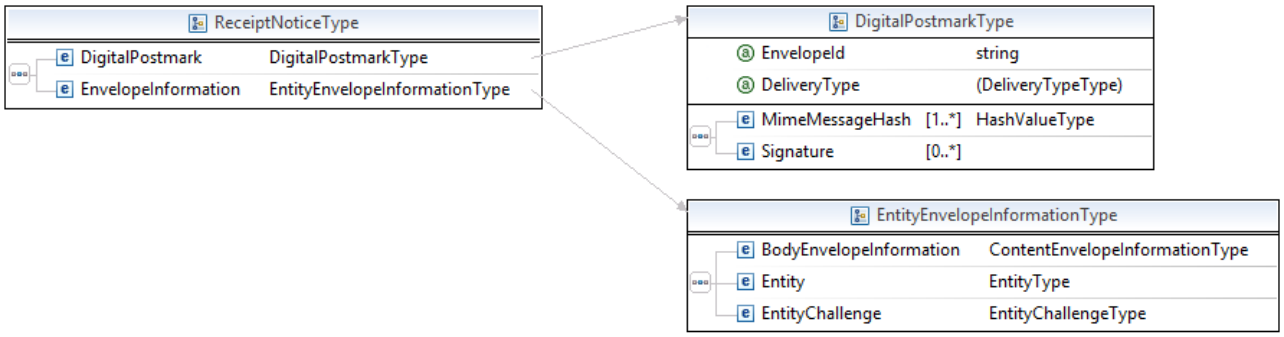
الشكل 4.A – نمط معلومات الغلاف



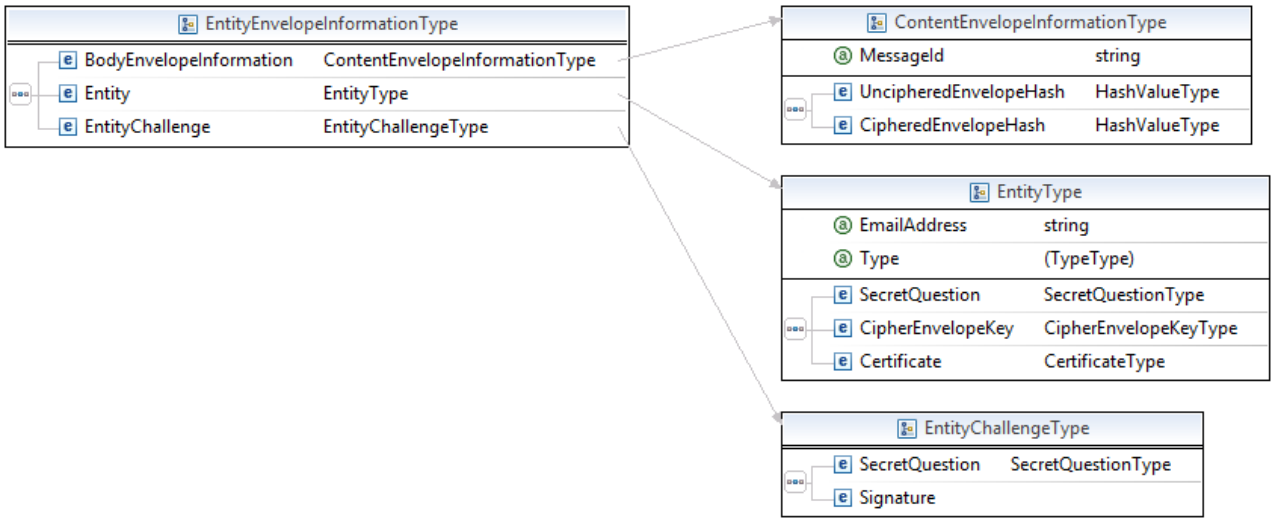
الشكل 5.A – نمط الكيان



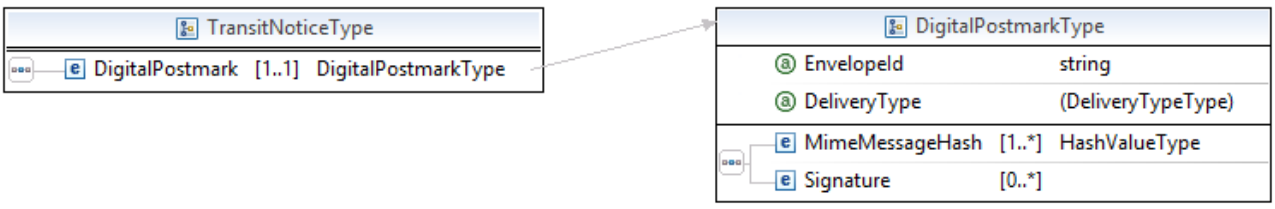
الشكل 6.A – التحقق



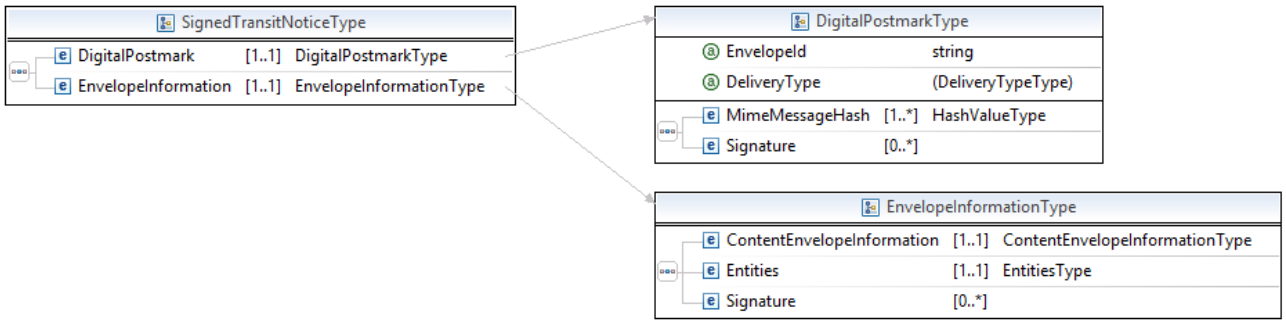
الشكل 7.A – الإشعار بالاستلام



الشكل 8.A – رد المستقبِل على التحقق



الشكل 9.A – الإشعار بالعبور



الشكل A.10 – الإشعار الموقع بالعبور

2.A المواصفة الرسمية للإشعارات بالتعريف XSD

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices"
     elementFormDefault="qualified" xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  <import namespace="http://www.w3.org/2009/xmldsig11#"
    schemaLocation="http://www.w3.org/TR/xmldsig-core1/xmldsig11-schema.xsd" />
  <import namespace="http://www.w3.org/2009/xmldsig-properties"
    schemaLocation="http://www.w3.org/TR/xmldsig-properties/xmldsig-properties.xsd" />

  <import namespace=http://www.w3.org/2000/09/xmldsig#
    schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd" />

  <element name="DepositNotice" type="tns:DepositNoticeType"></element>
  <element name="SignedDepositNotice" type="tns:SignedDepositNoticeType"></element>
  <element name="TransitNotice" type="tns:TransitNoticeType"></element>
  <element name="SignedTransitNotice" type="tns:SignedTransitNoticeType"></element>
  <element name="ReceipNotice" type="tns:ReceiptNoticeType"></element>
  <element name="SignedReceiptNotice" type="tns:SignedReceiptNoticeType"></element>

  <complexType name="DigitalPostmarkType">
    <sequence>
      <element name="MimeMessageHash" type="tns:HashValueType"
        maxOccurs="unbounded" minOccurs="1">
      </element>
      <element name="Signature" type="ds:SignatureType"
        maxOccurs="unbounded" minOccurs="0">
      </element>
    </sequence>
    <attribute name="EnvelopeId" type="string" use="required"></attribute>
    <attribute name="DeliveryType" use="required">
      <simpleType>
        <restriction base="string">
          <enumeration value="CertifiedMail"></enumeration>
        </restriction>
      </simpleType>
    </attribute>
  </complexType>

  <complexType name="EnvelopeInformationType">
    <sequence>
      <element name="ContentEnvelopeInformation"
        type="tns:ContentEnvelopeInformationType" maxOccurs="1" minOccurs="1">
      </element>
      <element name="Entities" type="tns:EntitiesType"
        maxOccurs="1" minOccurs="1">
      </element>
      <element name="Signature" type="ds:SignatureType"
        maxOccurs="unbounded" minOccurs="0">
```

```
    </element>
  </sequence>
</complexType>

<complexType name="ContentEnvelopeInformationType">
  <sequence>
    <element name="UncipheredEnvelopeHash" type="tns:HashValueType"></element>
    <element name="CipheredEnvelopeHash" type="tns:HashValueType"></element>
  </sequence>
  <attribute name="MessageId" type="string"></attribute>
</complexType>

<complexType name="SecretQuestionType">
  <sequence>
    <element name="Request" type="tns:RequestType"></element>
    <element name="Response" type="tns:ResponseType"></element>
  </sequence>
</complexType>

<complexType name="EntityType">
  <sequence>
    <element name="SecretQuestion" type="tns:SecretQuestionType"></element>
    <element name="CipherEnvelopeKey"
      type="tns:CipherEnvelopeKeyType">
    </element>
    <element name="Certificate" type="tns:CertificateType"></element>
  </sequence>
  <attribute name="EmailAddress" type="string" use="required">
    <annotation>
      <documentation>Email address has to be in RFC 822format</documentation>
    </annotation></attribute>
  <attribute name="Type" use="required">
    <simpleType>
      <restriction base="string">
        <enumeration value="from"></enumeration>
        <enumeration value="to"></enumeration>
        <enumeration value="cc"></enumeration>
        <enumeration value="transit"></enumeration>
      </restriction>
    </simpleType>
  </attribute>
</complexType>

<complexType name="CipherEnvelopeKeyType">
  <attribute name="Algorithm" type="string"></attribute>
  <attribute name="CipheredKey" type="string"></attribute>
  <attribute name="Encoding" type="string"></attribute>
  <attribute name="KeySize" type="int"></attribute>
</complexType>

<complexType name="CertificateType">
  <attribute name="encoding" type="string"></attribute>
</complexType>

<complexType name="EntitiesType">
  <sequence>
    <element name="Entity" type="tns:EntityType"
      maxOccurs="unbounded" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="SignedDepositNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
    <element name="EnvelopeInformation"
```

```
      type="tns:EnvelopeInformationType" maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="DepositNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="TransitNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="SignedTransitNoticeType">
  <sequence>
    <element name="DigitalPostmark" type="tns:DigitalPostmarkType"
      maxOccurs="1" minOccurs="1">
    </element>
    <element name="EnvelopeInformation"
      type="tns:EnvelopeInformationType" maxOccurs="1" minOccurs="1">
    </element>
  </sequence>
</complexType>

<complexType name="ReceiptNoticeType">
  <sequence>
    <element name="DigitalPostmark"
      type="tns:DigitalPostmarkType">
    </element>
    <element name="EnvelopeInformation"
      type="tns:EntityEnvelopeInformationType">
    </element>
  </sequence>
</complexType>

<complexType name="SignedReceiptNoticeType">
  <sequence>
    <element name="DigitalPostmark"
      type="tns:DigitalPostmarkType">
    </element>
    <element name="EnvelopeInformation"
      type="tns:EntityEnvelopeInformationType">
    </element>
  </sequence>
</complexType>

<complexType name="HashValueType">
  <attribute name="AlgorithmOID">
    <simpleType>
      <restriction base="string">
        <enumeration value="1.3.14.3.2.26"></enumeration>
        <enumeration value="2.16.840.1.101.3.4.2.1"></enumeration>
      </restriction>
    </simpleType>
  </attribute>
</complexType>

<complexType name="EntityEnvelopeInformationType">
  <sequence>
    <element name="BodyEnvelopeInformation" type="tns:ContentEnvelopeInformationType">
```

```
      </element>
      <element name="Entity" type="tns:EntityType"></element>
      <element name="EntityChallenge" type="tns:EntityChallengeType"></element>
    </sequence>
  </complexType>

  <complexType name="EntityChallengeType">
    <sequence>
      <element name="SecretQuestion" type="tns:SecretQuestionType"></element>
      <element name="Signature" type="ds:SignatureType"></element>
    </sequence>
  </complexType>

  <complexType name="RequestType">
    <attribute name="RandomNumber" type="string"></attribute>
  </complexType>

  <complexType name="ResponseType">
    <attribute name="AlgorithmIdentifier" type="string"></attribute>
  </complexType>

</schema>
```

الملحق B

الإشعارات بالترميز ASN.1

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

يقدم هذا الملحق مواصفة الإشعارات بالترميز ASN.1 كما هو موصف في [ITU-T X.680]. ويمكن تشفير هذه الإشعارات باستعمال قواعد التشفير المميز (DER) للترميز ASN.1 كما هو موصف في [ITU-T X.690] أو باستعمال التشفير باللغة XML الموسع (EXTENDED-XER) كما هو موصف في [ITU-T X.693]. وفي الحالة الأخيرة تتماثل النتيجة XML الناجمة عن هذا التشفير مع النتيجة XML المتولدة طبقاً للتعريف XDS كما هو موصف في الملحق A.

```
CMAIL {itu-t(0) recommendation(0) x(24) cmail(1341) asn1Module(1) cmail(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS String
     FROM XSDv2 {joint-iso-itu-t asn1(1) specification(0) modules(0)
          xsd-module(2) version2(2)};

DepositNotice         ::= DepositNoticeType

SignedDepositNotice   ::= SignedDepositNoticeType

TransitNotice         ::= TransitNoticeType

SignedTransitNotice   ::= SignedTransitNoticeType

ReceiptNotice         ::= ReceiptNoticeType

SignedReceiptNotice   ::= SignedReceiptNoticeType

DigitalPostmarkType   ::= SEQUENCE {
     mimeMessageHash SEQUENCE (SIZE(1..MAX)) OF
          mimeMessageHash HashValueType,
     signature  SEQUENCE (SIZE(0..MAX)) OF
          signature  SignatureType,
     envelopeId String,
     deliveryType    ENUMERATED {
          certifiedMail,
          ...
          }
     }

EnvelopeInformationType    ::= SEQUENCE {
     contentEnvelopeInformation ContentEnvelopeInformationType,
     entities              EntitiesType,
     signature        SEQUENCE (SIZE(0..MAX)) OF
          signature SignatureType
     }

ContentEnvelopeInformationType  ::= SEQUENCE {
     uncipheredEnvelopeHash     HashValueType,
     cipheredEnvelopeHash HashValueType,
     messageId        String
     }

SecretQuestionType    ::= SEQUENCE {
     request          RequestType,
     response   ResponseType
     }

EntityType ::= SEQUENCE {
     secretQuestion        SecretQuestionType,
```

```
      cipheredEnvelopeKey  CipheredEnvelopeKeyType,
      certificate          CertificateType,
      emailAddress         String
           (CONSTRAINED BY
           {-- "Email address has to be in IETF RFC 822 format --}),
      type ENUMERATED {
           from,
           to,
           cc,
           transit
           }
      }

CipheredEnvelopeKeyType    ::= SEQUENCE {
      algorithm  String,
      cipherededKey   String,
      encoding   String,
      keySize          String
      }

CertificateType ::= SEQUENCE {
      encoding   String
      }

EntitiesType     ::= SEQUENCE {
      entity           SEQUENCE(SIZE(1..MAX)) OF entity EntityType
      }

SignedDepositNoticeType    ::= SEQUENCE {
      digitalPostmark       DigitalPostmarkType,
      envelopeInformation   EnvelopeInformationType
      }

DepositNoticeType     ::= SEQUENCE {
      digitalPostmark       DigitalPostmarkType
      }

TransitNoticeType     ::= SEQUENCE {
      digitalPostmark       DigitalPostmarkType
      }

SignedTransitNoticeType    ::= SEQUENCE {
      digitalPostmark       DigitalPostmarkType,
      envelopeInformation   EnvelopeInformationType
      }

ReceiptNoticeType     ::= SEQUENCE {
      operatorPostmark      DigitalPostmarkType
      }

SignedReceiptNoticeType    ::= SEQUENCE {
      operatorPostmark      DigitalPostmarkType,
      envelopeInformation   EntityEnvelopeInformationType
      }

HashValueType    ::= SEQUENCE {
      algorithmOID     ENUMERATED {
           sha-1,
           sha-256
           }
      }

EntityEnvelopeInformationType   ::= SEQUENCE {
      bodyEnvelopeInformation    ContentEnvelopeInformationType,
      entity                EntityType,
      entityChallenge       EntityChallengeType
      }
```

```
EntityChallengeType  ::= SEQUENCE {
      secretQuestion _SecretQuestionType,
      signature  SignatureType
      }

RequestType     ::= SEQUENCE {
      randomNumer     String
      }

ResponseType    ::= SEQUENCE {
      algorithmIdentifier  String
      }

SignatureType   ::= String

ENCODING-CONTROL XER
      GLOBAL-DEFAULTS MODIFIED-ENCODINGS
      [NAME AS CAPITALIZED] DigitalPostmarkType.mimeMessageHash
      [UNTAGGED] DigitalPostmarkType.mimeMessageHash
      [NAME AS CAPITALIZED] DigitalPostmarkType.signature.*
      [UNTAGGED] DigitalPostmarkType.signature
      [NAME AS CAPITALIZED] DigitalPostmarkType.envelopeId
      [ATTRIBUTE] DigitalPostmarkType.envelopeId
      [NAME AS CAPITALIZED] DigitalPostmarkType.deliveryType
      [ATTRIBUTE] DigitalPostmarkType.deliveryType
      [TEXT AS CAPITALIZED] DigitalPostmarkType.delivetyType:certifiedMail
      [NAME AS CAPITALIZED] EnvelopeInformationType.contentEnvelopeInformation
      [NAME AS CAPITALIZED] EnvelopeInformationType.entities
      [NAME AS CAPITALIZED] EnvelopeInformationType.signature
      [UNTAGGED] EnvelopeInformationType.signature
      [NAME AS CAPITALIZED]
           ContentEnvelopeInformationType.uncipheredEnvelopeHash
      [NAME AS CAPITALIZED]
           ContentEnvelopeInformationType.cipheredEnvelopeHash
      [NAME AS CAPITALIZED] ContentEnvelopeInformationType.messageId
      [ATTRIBUTE] ContentEnvelopeInformationType.messageId
      [NAME AS CAPITALIZED] SecretQuestionType.request
      [NAME AS CAPITALIZED] SecretQuestionType.response
      [NAME AS CAPITALIZED] EntityType.secretQuestion
      [NAME AS CAPITALIZED] EntityType.cipheredEnvelopeKey
      [NAME AS CAPITALIZED] EntityType.certificate
      [NAME AS CAPITALIZED] EntityType.emailAddress
      [ATTRIBUTE] EntityType.emailAddress
      [NAME AS CAPITALIZED] EntityType.type
      [ATTRIBUTE] EntityType.type
      [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.algorithm
      [ATTRIBUTE] CipheredEnvelopeKeyType.algorithm
      [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.cipheredKey
      [ATTRIBUTE] CipheredEnvelopeKeyType.cipheredKey
      [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.encoding
      [ATTRIBUTE] CipheredEnvelopeKeyType.encoding
      [NAME AS CAPITALIZED] CipheredEnvelopeKeyType.keysize
      [ATTRIBUTE] CipheredEnvelopeKeyType.keysize
      [NAME AS CAPITALIZED] CertificateType.encoding
      [ATTRIBUTE] CertificateType.encoding
      [UNTAGGED] EntitiesType.entity
      [NAME AS CAPITALIZED] EntitiesType.entity.*
      [NAME AS CAPITALIZED] SignedDepositNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedDepositNoticeType.envelopeInformation
      [NAME AS CAPITALIZED] DepositNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] TransitNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedTransitNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedTransitNoticeType.envelopeInformation
      [NAME AS CAPITALIZED] ReceiptNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedReceiptNoticeType.digitalPostmark
      [NAME AS CAPITALIZED] SignedReceiptNoticeType.envelopeInformation
      [NAME AS CAPITALIZED] HashValueType.algorithmOID
      [ATTRIBUTE] HashValueType.algorithmOID
```

```
      [TEXT AS "1.3.14.3.2.26"] HashValueType.algorithmOID:sha-1
      [TEXT AS "2.16.840.1.101.3.4.2.1"] HashValueType.algorithmOID:sha-256
      [NAME AS CAPITALIZED]
           EntityEnvelopeInformationType.BodyEnvelopeInformation
      [NAME AS CAPITALIZED]
           EntityEnvelopeInformationType.entityChallenge
      [NAME AS CAPITALIZED] EntityChallengeType.secretQuestion
      [NAME AS CAPITALIZED] EntityChallengeType.signature
      [NAME AS CAPITALIZED] RequestType.randomNumber
      [ATTRIBUTE] RequestType.randomNumber
      [NAME AS CAPITALIZED] ResponseType.algorithmIdentifier
      [ATTRIBUTE] ResponseType.algorithmIdentifier

END
```

الملحق C

متطلبات بشأن مكونات البنى التحتية للمفاتيح العمومية

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

1.C المقدمة

يطرح هذا الملحق متطلبات بشأن شهادات المفاتيح العمومية الصادرة لمخدمات وعملاء البريد المعتمد.

2.C شهادات المفاتيح العمومية للكيان النهائي لمخدم البريد المعتمد

أي شهادة لمفتاح عمومي لكيان نهائي تصدر لمخدم من مخدمات البريد المعتمد، بحيث تتضمن المحتوى التالي:

أ) أن يحدد الإصدار 3.

ب) يجب أن تطرح سلطة إصدار الشهادات أرقام مسلسلة غير متتابعة.

ج) يجب أن يحمل حقل الموضوع اسم دليل مميز مع مكون وحيد يستخدم نمط النعت **dnsName** كما هو معرف في [ITU-T X.520]. ويجب أن تكون القيمة اسماً مسجلاً وفق نظام أسماء الميادين (DNS).

د) يجب أن يعرض تمديد الاسم البديل للموضوع مع عنصرين:

- **rfc822Name** البديل، يجب أن يؤخذ لأحد العنصرين ويجب أن يكون عنوان البريد الإلكتروني لمدير مخدم البريد المعتمد.
- **directoryName** البديل، يجب أن يؤخذ للعنصر الثاني ويجب أن يحمل اسماً مميزاً بالمكونات التالية:
  - يعرض **countryName** ويحمل الرمز المكون من ثلاثة أحرف (alpha-3) للمعيار [ISO 3166-1].
  - يعرض **organizationName** ويجب أن يحمل الاسم الموثوق للمنظمة التي تدير البريد المعتمد.
  - يعرض **streetAddress** ويحمل اسم الشارع ورقم المنزل.
  - يعرض **localityName** ويحمل اسم الحي.
  - يعرض **stateOrProvinceName** إذا لزم الأمر لأغراض تفرد تعرف الهوية. وخلاف ذلك لا يعرض.
  - يعرض **postalCode** ويجب أن يحمل الرمز البريدي للحي.

هـ) يعرض تمديد **certificatePolicies** ويجب أن يحمل على الأقل معرف هوية الشيء **{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailServer(1)}** للإشارة إلى أن شهادة المفتاح العمومي صدرت طبقاً لهذه التوصية.

3.C شهادات المفاتيح العمومية للكيانات النهائية لعملاء البريد المعتمد

شهادة المفتاح العمومي لكيان نهائي الصادرة لعميل من عملاء البريد المعتمد، يجب أن تتضمن المحتوى التالي:

أ) أن يحدد الإصدار 3.

ب) يجب أن تطرح سلطة إصدار الشهادات أرقام مسلسلة غير متتابعة.

ج) يجب أن يحمل حقل الموضوع اسم دليل مميز مع المكونات التالية:

- يعرض **surname** إذا كان العميل فرداً، ولا يعرض إذا كان العميل منظمة.
- يعرض **givenName** في حالة وجود **surname**. وخلاف ذلك لا يعرض.

- يمكن عرض **initials** في حالة وجود **surname**. وخلاف ذلك لا تعرض.
- يمكن عرض **generationQualifier** في حالة وجود **surname**. وخلاف ذلك لا تعرض.
- يعرض **organizationName** إذا لم يكن العميل أحد السكان. وخلاف ذلك لا يعرض. وفي حالة وجوده، يجب أن يحمل اسم موثوق للمنظمة التي ينتمي إليها العميل.
- يعرض **streetAddress** ويجب أن يحمل اسم الشارع ورقم العقار.
- يعرض **localityName** ويجب أن يحمل اسم الحي.
- يعرض **stateOrProvinceName** إذا لزم الأمر لأغراض تفرد تعرف الهوية. وخلاف ذلك لا يعرض.
- يعرض **postalCode** ويجب أن يحمل الرمز البريدي للحي.
- يعرض **countryCode3c** ويجب أن يحمل الرمز المكون من ثلاثة حروف (alpha-3) للمعيار [ISO 3166-1].

د) يعرض التمديد **subjectAltName**، ويجب أن يتضمن عنصراً واحداً كما هو مبين أدناه:

- **rfc822Name** ، يجب أن يحمل عنوان البريد الإلكتروني لمدير مخدم البريد المعتمد.

ه) يعرض تمديد certificatePolicies ويجب أن يحمل على الأقل معرف هوية الشيء **{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailClient(2)}** للإشارة إلى أن شهادة المفتاح العمومي صدرت طبقاً لهذه التوصية.

4.C متطلبات صلاحية المعلومات

يجب على جهة إصدار شهادات المفاتيح العمومية أن تتحقق قبل الإصدار ما يلي:

أ) أن الموضوع (مقدم الطلب) هو الحائز المسجل لاسم الميدان المقرر إدراجه في شهادة المفتاح العمومي؛

ب) الوجود الحقيقي للموضوع؛

ج) الوجود التشغيلي للموضوع (نشاط تجاري)؛

د) أن الموضوع كيان موثوق معتمد؛

ه) معلومات الاسم والعنوان المقرر إدراجها في شهادة المفتاح العمومي؛

و) أن **organizationName** المقرر إدراجه ضمن شهادة المفتاح العمومي اسم موثوق ومعتمد يعرِّف الموضوع.

الملحق D

متطلبات بشأن أمن طبقة النقل (TLS)

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

يجب دعم المعيار [IETF RFC 5246] أو أي إصدار بعده.

عند التفاوض، يجب ألا يقبل مخدم البريد المعتمد ولا العميل أي توصيل يشمل أي محاولة للتفاوض حول إصدار لأن طبقة النقل أقدم من الإصدار TLS 1.2.

ويجب أن يدعم التنفيذ كدسة الشفرة التالية:

- TLS_DH_RSA_WITH_AES_256_CBC_SHA256

الملحق E

معرفات هوية الأشياء المعرفة في هذه التوصية

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

تعرف هذه التوصية معرفات هوية الأشياء التالية:

أ) معرف هوية الشيء المرتبط بالوحدة النمطية ASN.1:

{itu-t recommendation(0) x(24) cmail(1341) asn1module(0) cmail(1)}

ب) معرف هوية الشيء المستخدم بواسطة تمديد certificatePolicies لمخدم البريد المعتمد:

{itu-t recommendation(0) x(24) cmail(1341) certificateProfile(2) cmailServer(1)}

ج) معرف هوية الشيء المستخدم بواسطة certificatePolicies لعميل البريد المعتمد:

{itu-t recommendation(0) x(24) cmail(1341) certificateProfile(2) cmailClient(2)}

التذييل I

نسق الغلاف والإشعارات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل أمثلة على تشفير الإشعارات.

1.I الإشعار بالإيداع

يتضمن الإشعار بالإيداع معلومات عن المرسِل والغلاف ويوقعه مخدم البريد المعتمد والمرسِل معاً.

وهو دليل على الإيداع يمكن للمرسِل استخدامه في الدعاوى القضائية.

ويمكن الاطلاع على المواصفة الرسمية للإشعار بالإيداع في الملحق A.

مثال: الملف "1373360283931.deposit.notice"

```
Received: from localhost ([127.0.0.1])
        by begmeil
        with SMTP (SubEthaSMTP null) id HIWV8HF9
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 10:58:14 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=depositNotice.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
bG9wZWQtc2lnbmF0dXJlIi8+CiAgICAgICAgICA8L1RyYW5zZm9ybXM+CiAgICAgICAgICA8RGln
...
ICAgPFJTQUtleVZhbHVlPgogICAgICAgICA8TW9kdWx1cz5tMkFSUURXUGJBMmgvMzJEQWs4
ICAgICAgICAgIDxFeHBvbmVudD5BUUFCPC9FeHBvbmVudD4KICAgICAgICAgIDwvUlNBS2V5VmFs
dWU+CiAgICAgICAgPC9LZXlWYWx1ZT4KICAgICAgICA8L1T4KICAgICAgICA8L9LZXlJbmZvPgogICAgPC9TaWduYXR1cmU+
CiAgPC9lbnZlbG9wSW5mb3JtYXRpb24+CjwvbGV0dGVyRGVwb3NpdFBvc3RtYXJrPgo=
```

2.I الإشعار بالاستلام

يتضمن الإشعار بالاستلام معلومات عن المرسِل والغلاف والتحقق من أجل فتح الغلاف ويوقعه مخدم البريد المعتمد والمستقبِل معاً.

وهو دليل على الاستلام يمكن أن يستخدمه المرسِل في الدعاوى القضائية.

ويمكن الاطلاع على المواصفة الرسمية للإشعار بالاستلام في الملحق A.

مثال: الملف "1373360283931.laura.prin@legalbox.com.receipt.notice"

```
Received: from begmeil get hostname ([127.0.0.1])
        by localhost
        with SMTP (LegalBox POP Server v1.0) id HIWX27L5
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 11:49:01 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=receiptNotice.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
PjEzNzMzNjAyODM5MzE8L2VudmVsb3BJZD4KICAgIDxkZWxpdmVyeU1vZGU+Y2VydGlmaWVkTGV0
dGVyPC9kZWxpdmVyeU1vZGU+CiAgICA8bWltZU1lc3NhZ2VIYXNoPgogICAgICA8c2hhMT5hNTVk
ZDhmYWU0Mzg2M2VmYWRmMWY3ZjM3MmEwYmU1MmEwMGRhYTFkPC9zaGExPgogICAgPC9taW1lTWVz
...
MDkwSDl0NFVkTTdWVU92bjY3WlU2aTJvVSt3b3lGR2tYMDJ3YkVMM2pDYmpJCm5VR1BwUGpoT3Zo
dzNPTy9mYmhKVk13dkM2NXB1MTl1cnA2M05kS0tHNlBuNjZtQkVnUldxZ2cvTVBITmZmWkhrOXFs
WExSSXhETi8Kb0ZnS285RmI0NExlSzBnZ3Vyb1Y2azNicm1TeGM1UnpYVWNxTzdwbldUN0FoNFl6
WXJJUHdYL1hjS1VqbXYxZi9JZjQ5VHVnWGtLcgpodklyOG9qUkdQcEdPdlB4cWR5QWNQR1BOUVRY
NFJrc29kSEVwdz09PC9Nb2R1bHVzPgogICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l
bnQ+CiAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICA8IDwvS2V5VmFsdWU+CiAgICAgIDwv
S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogIDwvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy
RGVwb3NpdFBvc3RtYXJrPgo=
```

3.I الإشعار بالعبور

يتضمن الإشعار بالعبور معلومات عن المرسِل والغلاف والتحقق لفتح الغلاف ويوقعه مخدما البريد المعتمد معاً.

وهو دليل بالعبور يمكن للمرسِل استخدامه في الدعاوى القضائية.

ويمكن الاطلاع على المواصفة الرسمية للإشعار بالعبور في الملحق A.

مثال: الملف "1373360283931.laura.prin@legalbox.com.receipt.notice"

```
Received: from begmeil get hostname ([127.0.0.1])
        by localhost
        with SMTP (LegalBox POP Server v1.0) id HIWX27L5
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 11:49:01 +0200 (CEST)
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=receiptNotice.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs
ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk
PjEzNzMzNjAyODM5MzE8L2VudmVsb3BJZD4KICAgIDxkZWxpdmVyeU1vZGU+Y2VydGlmaWVkTGV0
dGVyPC9kZWxpdmVyeU1vZGU+CiAgICA8bWltZU1lc3NhZ2VIYXNoPgogICAgICA8c2hhMT5hNTVk
ZDhmYWU0Mzg2M2VmYWRmMWY3ZjM3MmEwYmU1MmEwMGRhYTFkPC9zaGExPgogICAgPC9taW1lTWVz
...
MDkwSDl0NFVkTTdWVU92bjY3WlU2aTJvVSt3b3lGR2tYMDJ3YkVMM2pDYmpJCm5VR1BwUGpoT3Zo
dzNPTy9mYmhKVk13dkM2NXB1MTl1cnA2M05kS0tHNlBuNjZtQkVnUldxZ2cvTVBITmZmWkhrOXFs
WExSSXhETi8Kb0ZnS285RmI0NExlSzBnZ3Vyb1Y2azNicm1TeGM1UnpYVWNxTzdwbldUN0FoNFl6
WXJJUHdYL1hjS1VqbXYxZi9JZjQ5VHVnWGtLcgpodklyOG9qUkdQcEdPdlB4cWR5QWNQR1BOUVRY
NFJrc29kSEVwdz09PC9Nb2R1bHVzPgogICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l
bnQ+CiAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICA8IDwvS2V5VmFsdWU+CiAgICAgIDwv
S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogIDwvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy
RGVwb3NpdFBvc3RtYXJrPgo=
```

4.I الغلاف

الغلاف (ENVELOPE) عبارة عن رسالة MIME تتضمن محتوى البريد الإلكتروني مشفراً بالشفير AES.

مثال: الملف "1373360283931.certifiedLetter.msg"

```
Received: from localhost ([127.0.0.1])
        by begmeil
        with SMTP (SubEthaSMTP null) id HIWV8HF9
        for laura.prin@legalbox.com;
        Tue, 09 Jul 2013 10:58:03 +0200 (CEST)
Date: Tue, 9 Jul 2013 10:57:51 +0200 (CEST)
From: david.keller@legalbox.com
To: laura.prin@legalbox.com
Message-ID: proto_cmtp_1373360269856
Subject: =?UTF-8?Q?Bienvenue_=C3=A0_CMTP!?=
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_Part_1_1013939722.1373360271613"

------=_Part_1_1013939722.1373360271613
Content-Type: multipart/mixed;
        boundary="----=_Part_0_2062834323.1373360271584"

------=_Part_0_2062834323.1373360271584
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=envelop

RG44gUlyr1A/L+ps0R+yKMUpgPcJACmcRQdLZSMoLnm07gtRataSAWkG5qnc/f5Q

------=_Part_0_2062834323.1373360271584--

------=_Part_1_1013939722.1373360271613--
```

بيبليوغرافيا

[b-ITU-T X.509] التوصية ITU-T X.509 (2012) | المعيار الدولي ISO/IEC 9594-8:2014، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: أطر شهادات المفاتيح العمومية والنعوت*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، تغير المناخ، المخلفات الإلكترونية، كفاءة الطاقة، إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وجوانب بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2016