الاتحـــــاد الـــدولـــــي للاتصـــــــالات

ITU-T X.509

(2005/08)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات المعطيات، الاتصال بين الأنظمة المفتوحة وأمنها

الدليل

تِقَانة (تكنولوجيا) المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: الأطر العامة لشهادات المفتاح العمومي والنعت

التوصية ITU-T X.509

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات المعطيات والاتصالات بين الأنظمة المفتوحة والأمن

الشبكات العمومية للمعطيات	
الخدمات والمرافق	X.1–X.19
السطوح البينية	X.20–X.49
الإرسال والتشوير والتبديل	X.50–X.89
جوانب الشبكة	X.90–X.149
الصيانة	X.150–X.179
الترتيبات الإدارية	X.180–X.199
التوصيل البيني للأنظمة المفتوحة	
النموذج والترميز	X.200–X.209
تعاريف الخدمات	X.210–X.219
مواصفات البروتوكول بأسلوب التوصيل	X.220–X.229
مواصفات البروتوكول بأسلوب غياب التوصيل	X.230–X.239
جداول إعلان المطابقة (PICS)	X.240–X.259
تعرّف هوية البروتوكول	X.260–X.269
بروتوكولات الأمن	X.270–X.279
أشياء مسيرة على الطبقة	X.280–X.289
اختبار المطابقة	X.290–X.299
التشغيل البيني للشبكات	
اعتبارات عامة	X.300–X.349
الأنظمة الساتلية لإرسال البيانات	X.350–X.369
الشبكات القائمة على بروتوكول الإنترنت	X.370–X.379
أنظمة معالجة الرسائل	X.400–X.499
الدليل	**X.500–X.599**
التوصيل الشبكي في التوصيل البيني للأنظمة المفتوحة (OSI) وجوانب النظام	
التوصيل الشبكي	X.600–X.629
الفعالية	X.630–X.639
نوعية الخدمة	X.640–X.649
التسمية والعنونة والتسجيل	X.650–X.679
ترميز النظم المجرد واحد (ASN.1)	X.680–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	
الإطار والهيكل المعماري لإدارة الأنظمة	X.700–X.709
خدمة اتصالات الإدارة وبروتوكولاتها	X.710–X.719
هيكل معلومات الإدارة	X.720–X.729
وظائف الإدارة ووظائف الهيكل المعماري للإدارة الموزعة المفتوحة	X.730–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	
الالتزام والتلازم والاستعادة	X.850–X.859
معالجة المعاملات	X.860–X.879
العمليات البُعدية	X.880–X.889
التطبيقات التنوعية لترميز النظم المجرد واحد (ASN.1)	X.890–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن الاتصالات	X.1000–

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

المعيار الدولي ISO/IEC 9594-8
التوصية ITU-T X.509

تِقَانة (تكنولوجيا) المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: الأطر العامة لشهادات المفتاح العمومي والنعت

الموجـــز

تحدد هذه التوصية | هذا المعيار الدولي أطراً عامة لشهادات المفتاح العمومي وشهادات النعت. ويمكن أن تستخدم هذه الأطر هيئات تقييس أخرى لكي تحدد جانبيات (لاحات) طلباتها التي تقدمها للحصول على البنى التحتية للمفتاح العمومي (PKI) والبنى التحتية لإدارة الامتياز (PMI). كما تحدد هذه التوصية | هذا المعيار الدولي إطاراً يقدم الدليل ضمنه خدمات الاستيقان إلى مستعمليه. وهي تشرح سويتين من الاستيقان: الاستيقان البسيط الذي يستخدم كلمة سر للتحقق من الهوية المعلن عنها، والاستيقان المعمّق الذي يتطلب ثبوتيات تولدها التقنيات التجفيرية. وبينما يوفر الاستيقان البسيط بعض الحماية من النفاذات غير المرخص بها، فإن الاستيقان المعمق هو الوحيد الذي ينبغي استخدامه كأساس لتقديم خدمات مأمونة.

المصدر

وافقت لجنة الدراسات 17 (2005-2008) التابعة لقطاع تقييس الاتصالات بتاريخ 29 أغسطس 2005 على التوصية ITU-T X.509 بموجب الإجراء المحدد في التوصية ITU-T A.8. ونشر نص مطابق لهذا النص باعتباره المعيار الدولي ISO/IEC 9594-8.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. 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، يُشدد على توصية المسؤولين عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) على العنوان التالي: http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

المدخل

أعدّت هذه التوصية | هذا المعيار الدولي، مع غيرها من التوصيات | المعايير الدولية، لكي تسهّل التوصيل البيني لأنظمة معالجة المعلومات من أجل تقديم خدمات الدليل. وهذه المجموعة من الخدمات المتصاحبة مع المعلومات التي تحملها، يمكن اعتبارها كياناً متكاملاً يدعى *الدليل*. وتستعمل المعلومات التي يحملها الدليل، والمعروفة مجتمعة باسم قاعدة معلومات الدليل (DIB)، لكي تسهّل الاتصال بين أشياء وموضوعات أو معها أو حولها، مثل كيانات التطبيق والأفراد والمطاريف وقوائم التوزيع.

ويلعب الدليل دوراً مهماً في التوصيل البيني للأنظمة المفتوحة، وهو يرمي، باستخدامه حدّاً أدنى من الاتفاقات التقنية خارج معايير التوصيل البيني بالذات، إلى أن يتيح التوصيل البيني بين أنظمة معالجة المعلومات المتوفرة:

- من مزوّدين متنوعين؛
- تحت مسؤولية إدارات متنوعة؛
- بسويات تعقيد متنوعة؛
- بأعمار متنوعة.

وتحتاج تطبيقات عديدة إلى خدمات أمنية تحمي نفسها من التهديدات التي تقع على اتصال المعلومات. ومن الناحية العملية، تعتمد جميع الخدمات الأمنية على المعرفة الموثوقة بهويات الأطراف المشتركة في الاتصال، أي تعتمد على استيقان هذه الأطراف (التيقن من صحة هوياتها).

وتحدد هذه التوصية | هذا المعيار الدولي إطاراً عاماً لشهادات المفتاح العمومي. ويتضمن هذا الإطار مواصفات موضوعات المعطيات التي تستعمل لتمثيل الشهادات بالذات، ويتضمن كذلك التبليغات عن إبطال الشهادات الصادرة والتي ينبغي عدم الوثوق بها بعد الآن. وإطار شهادة المفتاح العمومي المشروح في هذه المواصفة يحدّد بعض المكوّنات الأساسية لبنية تحتية للمفتاح العمومي (PKI)، إلا أنه لا يحدد هذه البنية بكاملها. ومع ذلك توفر هذه المواصفة الأساس الذي يمكن أن تبنى عليه بنية تحتية PKI كاملة مع مواصفاتها.

وكذلك تحدد هذه التوصية | هذا المعيار الدولي إطاراً عاماً لشهادات النعت. ويتضمن هذا الإطار مواصفات موضوعات المعطيات التي تستعمل لتمثيل الشهادات بالذات، كما يتضمن التبليغات عن إبطال الشهادات الصادرة والتي ينبغي عدم الوثوق بها بعد الآن. وإطار شهادة النعت المشروح في هذه المواصفة يحدد بعض المكوّنات الأساسية لبنية تحتية لإدارة الامتياز (PMI)، إلا أنه لا يحدد هذه البنية بكاملها. ومع ذلك توفر هذه المواصفة الأساس الذي يمكن أن تبنى عليه بنى تحتية PMI كاملة مع مواصفاتها.

وتتحدد أيضاً موضوعات المعلومات التي تتيح تخوين موضوعات البنى التحتية PKI وPMI في الدليل، كما تتيح المقارنة بين القيم المعروضة والقيم المخزونة.

وكذلك تحدد هذه التوصية | هذا المعيار الدولي إطاراً لتقديم الدليل خدمات الاستيقان إلى مستعمليه.

وتقدم هذه التوصية | هذا المعيار الدولي الأطر الأساسية التي تسمح لهيئات تقييس أو منتديات صناعية أخرى بأن تحدد جانبيات صناعية خاصة بها. والعديد من الميزات التي يعتبر استعمالها اختياراً في هذه الأطر، يمكن أن تجعله الجانبيات إلزامياً في بعض البيئات. وهذه الطبعة الخامسة من هذه التوصية | هذا المعيار الدولي تراجع طبعتها الرابعة وتعززها تقنياً، ولكنها لا تحل محلها. وقد تبقى بعض التطبيقات تطالب بإعلان التطابق مع الطبعة الرابعة، إلا أن الطبعة الرابعة لن تعود معتمدة بعد تاريخ معين (أي إن التقارير التي تقدم بشأن بعض العيوب لن تدرس بعدئذ). ويوصى بأن تتوافق التطبيقات المختلفة مع هذه الطبعة الخامسة بأسرع ما يمكن.

وتحدد هذه الطبعة الخامسة الصيغ 1 و2 و3 لشهادات المفتاح العمومي والصيغتين 1 و2 لقوائم إبطال الشهادات. كما وتحدد هذه الطبعة الصيغة 2 لشهادات النعت.

وقد أضيفت وظيفة قابلية التوسع في طبعة سابقة مع الصيغة 3 لشهادة المفتاح العمومي، ومع الصيغة 2 لقائمة إبطال الشهادات، وأدمجت في شهادة النعت منذ صدورها الأول. وهذه الوظيفة محددة في البند 7. ومن المتوقع بمساعدة هذه الوظيفة استيعاب أي تطوير لهذه الطبعة وإدراجه فيها، وبذلك يجتنب إصدار صيغ جديدة.

يقدم الملحق A الذي يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي وحدات ترميز علم النحو المجرد 1 (أو ترميز قواعد التركيب المجرد 1) (ASN.1) التي تتضمن جميع التعريفات المصاحبة لأطر الاستيقان.

ويقدم الملحق B الذي يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي قواعد توليد ومعالجة قوائم إبطال الشهادات.

ويقدم الملحق C الذي لا يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي أمثلة من إصدار القوائم دلتا لإبطال الشهادات (delta-CRL).

ويقدم الملحق D الذي لا يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي أمثلة من قواعد النحو في سياسات الامتياز وأمثلة من نعوت الامتيازات.

ويقدم الملحق E الذي لا يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي مدخلاً إلى طريقة تجفير المفتاح العمومي.

ويعرّف الملحق F الذي يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي معرفات هوية الموضوعات المستندة إلى خوارزميات الاستيقان والتجفير، في غياب تسجيل رسمي.

ويحتوي الملحق G الذي لا يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي أمثلة من استخدام تقييدات مسيرة إصدار الشهادة.

ويقدم الملحق H الذي لا يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي توجيهات تتعلق بالتطبيقات الصالحة للبنى التحتية PKI، بشأن معالجة سياسة الشهادة أثناء عملية إقرار الصلاحية لمسيرة إصدار الشهادة.

ويقدم الملحق I الذي لا يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي توجيهات تتعلق باستخدام بتة الالتزام بالمحتوى (contentCommitment) في توسّع الشهادة استعمال المفتاح (keyUsage).

ويحتوي الملحق J الذي لا يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي على تعريفات عناصر المعلومات الموجودة في هذه المواصفة مرتبة في قائمة وفق الترتيب الهجائي.

ويقدم الملحق K الذي لا يشكل جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي قوائم بالتعديلات وبتقارير العيوب التي أدرجت في هذه الطبعة من هذه التوصية | هذا المعيار الدولي.

المعيار الدولي
توصية القطاع ITU-T

تِقَانة (تكنولوجيا) المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: الأطر العامة لشهادات المفتاح العمومي والنعت

القسم الأول – عموميات

1 مجال التطبيق

تتطرق هذه التوصية | هذا المعيار الدولي إلى بعض المتطلبات الأمنية في مجالات الاستيقان وغيره من الخدمات الأمنية، فتوفر مجموعة من الأطر يمكن أن تبنى عليها خدمات مكتملة. وتحدد هذه التوصية | هذا المعيار بصفة خاصة الأطر التالية:

- شهادات المفتاح العمومي؛
- شهادات النعت؛
- خدمات الاستيقان.

يشتمل إطار شهادة المفتاح العمومي المعرّف في هذه التوصية | هذا المعيار الدولي على تعريف موضوعات المعلومات اللازمة في البنية التحتية للمفتاح العمومي (PKI)، وهو يشمل شهادات المفتاح العمومي وقوائم إبطال الشهادات (CRL). ويشتمل إطار شهادة النعت على تعريف موضوعات المعلومات اللازمة في البنية التحتية لإدارة الامتياز (PMI)، وهو يشمل شهادات النعت وقوائم إبطال شهادات النعت (ACRL). كما تقدم هذه المواصفة الإطار اللازم لإصدار الشهادات وإدارتها واستعمالها وإبطالها. كما أدمجت آلية لقابلية التوسع في الأنساق المعرّفة لكلا نوعي الشهادات ولجميع أنماط قوائم الإبطال. وتحتوي هذه التوصية | هذا المعيار الدولي أيضاً على مجموعة مقيّسة من توسّعات كل نمط، ومن المتوقع أن تكون هذه المجموعة ذات فائدة عامة لعدد من تطبيقات البنى التحتية PKI وPMI. ومكوّنات التخطيطة التي تضم أصناف الموضوعات وأنماط النعوت وقواعد التواؤم من أجل تخزين موضوعات البنى التحتية PKI وPMI في الدليل، موجودة كذلك في هذه التوصية | هذا المعيار الدولي. ومن المتوقع أن تعرّف هيئات تقييس أخرى (مثل اللجنة TC 68 في المنظمة ISO وفريق المهام الهندسية في الإنترنت (TETF) وغيرها) عناصر أخرى إضافية من البنى التحتية PKI وPMI واقعة خارج هذه الأطر مثل بروتوكولات إدارة المفتاح والشهادة، أو البروتوكولات التشغيلية أو غيرها من توسّعات الشهادات والقوائم CRL.

وأسلوب الاستيقان المعرّف في هذه التوصية | هذا المعيار الدولي له صفة عمومية، يمكن تطبيقه على تطبيقات وبيئات متنوعة.

يستعمل الدليل شهادات المفتاح العمومي وشهادات النعت، والإطار الذي يستعمل الدليلُ ضمنه هذه التسهيلات محدد أيضاً في هذه التوصية | هذا المعيار الدولي. يستخدم الدليل تقانة المفتاح العمومي التي تشمل الشهادات، لكي يقدم استيقاناً معمقاً، وعمليات موقّعة و/أو مجفّرة، ولكي يختزن معطيات موقّعة و/أو مجفّرة. ويمكنه استعمال شهادات النعت لكي يقدم تحكماً في النفاذ مستنداً إلى قواعد. وعلى الرغم من أن الإطار المقابل لهذه الأمور متوفر في هذه المواصفة، إلا أن التعريف الكامل لاستخدام الدليل هذه الأطر، والخدمات المصاحبة التي يقدمها الدليل ومكوناته، فهي مقدمة في المجموعة الكاملة لمواصفات الدليل.

وتوضح هذه التوصية | هذا المعيار الدولي النقاط التالية أيضاً في إطار خدمات الاستيقان:

- مواصفة نسق معلومات الاستيقان الموجودة في الدليل؛
- وصف السبيل للحصول على معلومات الاستيقان من الدليل؛
- النص على الافتراضات المتّخذة بشأن كيفية إنشاء معلومات الاستيقان ووضعها في الدليل؛

– تعريف ثلاثة أساليب محتملة، تستعملها التطبيقات في استخدام معلومات الاستيقان من أجل القيام بعملية الاستيقان، ووصف الكيفية التي يستطيع الاستيقان بها دعم خدمات أمنية أخرى.

تشرح هذه التوصية | هذا المعيار الدولي سويتين من الاستيقان: الاستيقان البسيط الذي يستخدم كلمة سر للتحقق من الهوية المعلن عنها، والاستيقان المعمّق الذي يتطلب ثبوتيات تولدها التقنيات التجفيرية. وبينما يقدم الاستيقان البسيط بعض الحماية من النفاذات غير المرخصة، فإن الاستيقان المعمّق هو وحده الذي يجب أن يستخدم كأساس لتقديم خدمات مأمونة. وهو ليس مصمماً ليشكل بفعل ذلك إطاراً عاماً للاستيقان، ولكن يمكن استخدامه بصورة عامة في التطبيقات التي تعتبر هذه الأساليب وافية.

لا يمكن تقديم الاستيقان (مثل غيره من الخدمات الأمنية) إلا في سياق سياسة أمنية محددة. ويعود إلى مستخدمي أحد التطبيقات أن يحددوا سياستهم الأمنية الخاصة، التي قد يتم إخضاعها لقيود الخدمات المقدمة في إطار معيار معيّن.

ويعود إلى التطبيقات التي تحدد المعايير وتستخدم إطار الاستيقان أن تحدد تبادلات البروتوكول اللازمة لتحقيق استيقان، معتمد على معلومات الاستيقان المحسوبة من الدليل. وبروتوكول النفاذ إلى الدليل (DAP) الذي تستخدمه التطبيقات للحصول على الثبوتيات من الدليل، محدد في التوصية ITU-T X.519 | في المعيار ISO/IEC 9594-5.

2 المراجع المعيارية

تحتوي التوصيات والمعايير الدولية التالية على أحكام تصبح، بعد الإحالة إليها في هذا النص، أحكاماً سارية في التوصية | هذا المعيار الدولي. والطبعات المشار إليها كانت ما تزال سارية المفعول يوم نشرها. وجميع التوصيات والمعايير عرضة للمراجعة، لذلك تُشجَّع الأطراف المشاركة في الاتفاقيات المبنية على هذه التوصية | هذا المعيار الدولي على أن تفتش عن إمكانية تطبيق الطبعات الأكثر حداثة من التوصيات | المعايير المشار إليها أدناه. ويحتفظ أعضاء اللجنة TEC والمنظمة ISO بسجلات المعايير الدولية السارية المفعول حالياً. كما يحتفظ مكتب تقييس الاتصالات في الاتحاد قائمة محيّنة بتوصيات القطاع ITU-T النافذة.

1.2 التوصيات | المعايير الدولية المتطابقة

– ITU-T Recommendation X.411 (1999) | ISO/IEC 10021-4:2003, *Information technology – Message Handling Systems (MHS) – Message transfer system: Abstract service definition and procedures*.

– ITU-T Recommendation X.500 (2005) | ISO/IEC 9594-1:2005, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

– ITU-T Recommendation X.501 (2005) | ISO/IEC 9594-2:2005, *Information technology – Open Systems Interconnection – The Directory: Models*.

– ITU-T Recommendation X.511 (2005) | ISO/IEC 9594-3:2005, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.

– ITU-T Recommendation X.518 (2005) | ISO/IEC 9594-4:2005, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*.

– ITU-T Recommendation X.519 (2005) | ISO/IEC 9594-5:2005, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.

– ITU-T Recommendation X.520 (2005) | ISO/IEC 9594-6:2005, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.

– ITU-T Recommendation X.521 (2005) | ISO/IEC 9594-7:2005, *Information technology – Open Systems Interconnection – The Directory: Selected object classes*.

– ITU-T Recommendation X.525 (2005) | ISO/IEC 9594-9:2005, *Information technology – Open Systems Interconnection – The Directory: Replication*.

– ITU-T Recommendation X.530 (2005) | ISO/IEC 9594-10:2005, *Information technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory*.

– ITU-T Recommendation X.660 (2004) | ISO/IEC 9834-1:2005, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures, and top arcs of the ASN.1 Object Identifier tree*.

– ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

– ITU-T Recommendation X.681 (2002) | ISO/IEC 8824-2:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.

– ITU-T Recommendation X.682 (2002) | ISO/IEC 8824-3:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.

– ITU-T Recommendation X.683 (2002) | ISO/IEC 8824-4:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.

– ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

– ITU-T Recommendation X.691 (2002) | ISO/IEC 8825-2:2002, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*.

– ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

– ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

– ITU-T Recommendation X.880 (1994) | ISO/IEC 13712-1:1995, *Information technology – Remote Operations: Concepts, model and notation*.

– ITU-T Recommendation X.881 (1994) | ISO/IEC 13712-2:1995, *Information technology – Remote Operations: OSI realizations – Remote Operations Service Element (ROSE) service definition*.

2.2 أزواج التوصيات | المعايير الدولية المتكافئة في محتواها التقني

– CCITT Recommendation X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications*.

– ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

3 التعريفات

تطبق التعريفات التالية لأغراض هذه التوصية | هذا المعيار الدولي.

1.3 تعريفات تتعلق بمعمارية أمن النموذج المرجعي للتوصيل البيني للأنظمة المفتوحة (OSI)

المصطلحات التالية معرفة في التوصية CCITT X.800 | في المعيار ISO 7498-2:

أ) غير متناظر (تجفير)؛ *asymmetric (encipherment);*

ب) تبادل استيقاني؛ *authentication exchange;*

ج) معلومات استيقانية؛ *authentication information;*

د) السرّية؛ *confidentiality;*

هـ) ثبوتيات؛ *credentials;*

و) طريقة التجفير؛ *cryptography;*

ز) استيقان مَصْدر المعطيات؛ *data origin authentication;*

ح) فك التجفير؛ *decipherment;*
ط) توقيع رقمي؛ *digital signature;*
ي) تجفير؛ *encipherment;*
ك) مفتاح؛ *key;*
ل) كلمة سر؛ *password;*
م) استيقان الكيان الندّ؛ *peer-entity authentication;*
ن) متناظر (تجفير). *symmetric (encipherment).*

2.3 تعريفات تتعلق بنموذج الدليل

المصطلحات التالية معرفة في التوصية ITU-T X.501 | في المعيار ISO/IEC 9594-2:

أ) نعت؛ *attribute;*
ب) قاعدة معلومات الدليل (DIB)؛ *Directory Information Base;*
ج) شجرة معلومات الدليل (DIT)؛ *Directory Information Tree;*
د) وكيل نظام الدليل (DSA)؛ *Directory System Agent;*
هـ) وكيل مستعمل الدليل (DUA)؛ *Directory User Agent;*
و) اسم مميز؛ *distinguished name;*
ز) مَدْخل؛ *entry;*
ح) موضوع، شيء، هدف، غاية؛ *object;*
ط) جذر. *root.*

3.3 تعريفات

المصطلحات التالية معرفة في التوصية | هذا المعيار الدولي:

1.3.3 شهادة نعت (attribute certificate) (AC): بنية من المعطيات تحمل التوقيع الرقمي لسلطة نعت، وتربط بعض قيم النعت بمعلومات عن تعرّف هوية حامل الشهادة.

2.3.3 سلطة النعت (Attribute Authority) (AA): سلطة تمنح الامتيازات بإصدارها شهادات نعوت.

3.3.3 قائمة إبطال سلطات النعت (attribute authority revocation list) (AARL): قائمة إبطال تحتوي على قائمة من المراجع تحيل إلى شهادات نعت تخص سلطات نعت لم تعد السلطة المُصْدرة تعتبرها صالحة.

4.3.3 قائمة إبطال شهادات النعت (attribute certificate revocation list) (ACRL): قائمة إبطال تحتوي على قائمة من المراجع تحيل إلى شهادات نعت لم تعد السلطة المُصْدرة تعتبرها صالحة.

5.3.3 إذنة الاستيقان (الإذنة) (authentication token, (token)): معلومة منقولة أثناء تبادل الاستيقان المعمّق، يمكن استعمالها للتيقّن من مرسلها.

6.3.3 سلطة (authority): كيان مسؤول عن إصدار الشهادات. وتعرّف هذه المواصفة نمطين من السلطات: سلطة إصدار الشهادة التي تصدر شهادات المفتاح العمومي، وسلطة النعت التي تصدر شهادات النعت.

7.3.3 شهادة سلطة (authority certificate): شهادة صادرة إلى سلطة (إما سلطة إصدار شهادة وإما سلطة نعت).

8.3.3 قائمة أساسية لإبطال الشهادات (base CRL): قائمة إبطال الشهادات التي تعتبر أساساً لتوليد القائمة دلتا لإبطال الشهادات (dCRL).

9.3.3 شهادة صادرة من سلطة إصدار الشهادات (CA-certificate): شهادة صادرة من سلطة إصدار شهادة وموجهة إلى سلطة أخرى لإصدار شهادة.

10.3.3 سياسة الشهادة (certificate policy): مجموعة مسمّاة من القواعد، تبين قابلية انطباق الشهادة على جماعة خاصة و/أو على صنف خاص من التطبيقات، تتميز باحتياجات أمنية مشتركة. فمثلاً يمكن لسياسة شهادة خاصة أن تبين قابلية انطباق نمط من الشهادات على الاستيقان من معاملات تبادل المعطيات الإلكترونية التي تخص تجارة بعض السلع ضمن حدود معينة من الأسعار.

11.3.3 إعلان الممارسات في إصدار الشهادة (certification practice statement) (CPS): إعلان عن الممارسات التي تستخدمها إحدى سلطات إصدار الشهادة عند إصدارها الشهادة.

12.3.3 قائمة إبطال الشهادات (certificate revocation list) (CRL): قائمة موقعة تبين مجموعة من الشهادات لم يعد مُصْدرها يعتبرها صالحة. وإضافة إلى هذا الاسم العام للقائمة CRL، توجد أنماط خاصة من القائمة CRL معرفة لتغطي مجالات خاصة من التطبيق.

13.3.3 مستعمل الشهادة (certificate user): كيان يحتاج أن يعرف نعوت كيان آخر و/أو مفتاحه العمومي على نحو مؤكد.

14.3.3 رقم تسلسل الشهادات (certificate serial number): قيمة صحيحة وحيدة بالنسبة إلى سلطة الإصدار، ومصاحبة بلا لبس للشهادة التي تصدرها هذه السلطة.

15.3.3 نظام استعمال الشهادات (certificate-using system): تنفيذ تلك الوظائف التي يستخدمها مستعمل الشهادة، من الوظائف التي تعرفها مواصفة الدليل هذه.

16.3.3 إقرار صلاحية الشهادة (certificate validation): عملية التأكد من أن شهادة ما هي صالحة في لحظة معينة، وربما تضمّن ذلك إنشاء ومعالجة مسيرة إصدار الشهادة، وضمان كون جميع الشهادات في هذه المسيرة صالحة حتى هذه اللحظة (أي إنها لم تنته صلاحيتها بَعْد ولا جرى إبطالها).

17.3.3 سلطة إصدار الشهادة (certification authority) (CA): سلطة تتمتع بثقة مستعمل واحد أو عدة مستعملين لكي تنشئ شهادات المفتاح العمومي وتسندها. ويمكن بشكل اختياري أن تنشئ مفاتيح المستعمل.

18.3.3 قائمة إبطال سلطات إصدار الشهادة (certification authority revocation list) (CARL): قائمة إبطال تحتوي على قائمة من شهادات المفتاح العمومي الصادرة إلى سلطات إصدار شهادة، لم تعد سلطة إصدار الشهادة تعتبرها صالحة.

19.3.3 مسيرة إصدار الشهادة (certification path): تتابع مرتب من شهادات المفتاح العمومي لموضوعات موجودة في الشجرة DIT يمكن معالجته، انطلاقاً من المفتاح العمومي للموضوع البدائي في المسيرة، للحصول على المفتاح العمومي للموضوع النهائي في المسيرة.

20.3.3 نقطة توزيع القائمة CRL (CRL distribution point): مدخل في الدليل أو في مصدر آخر لتوزيع القائمة CRL. وقد تحتوي القائمة CRL على طريق نقطة توزيع القائمة CRL، على مداخل إبطال تخص فقط مجموعة فرعية من المجموعة الكاملة للشهادات الصادرة عن سلطة واحدة لإصدار الشهادة، أو إنها قد تحتوي على مداخل إبطال صادرة عن عدة سلطات لإصدار الشهادة.

21.3.3 شهادة متقاطعة (cross-certificate): شهادة مفتاح عمومي أو شهادة نعت يكون قيمها المُصْدر والصاحب/الحامل سلطتين مختلفتين CA أو AA على التوالي. وتصدر سلطات الشهادة (CA) وسلطات النعت (AA) شهادات متقاطعة موجهة لتغيرها من سلطات إصدار الشهادة أو النعت على التوالي، باعتبارها آلية ترخيص بوجود سلطة الإصدار الصاحبة (وذلك داخل تراتب صارم) أو باعتبارها آلية اعتراف بوجود سلطة الإصدار الصاحبة أو سلطة النعت الحاملة (كما في نموذج الثقة الموزع). وتستخدم بنية الشهادة المتقاطعة في كلتا الحالتين.

22.3.3 نظام التجفير (cryptographic system, cryptosystem): مجموعة من التحويلات تنقل النص الواضح إلى نص مرمّز وبالعكس، على أن يتم بواسطة المفاتيح انتقاء التحويلات الخاصة الواجب استعمالها. وتتحدد التحويلات عامة بخوارزمية رياضية.

23.3.3 سرّية المعطيات (data confidentiality): يمكن استعمال هذه الخدمة لتوفير حماية للمعطيات من إفشاء غير مرخص. وإطار الاستيقان هو الذي يدعم خدمة سرية المعطيات. ويمكن استعمال هذه الخدمة لحماية المعطيات من اعتراضها.

24.3.3 تفويض (delegation): نقل امتياز من كيان حائز عليه إلى كيان آخر.

25.3.3 مسيرة التفويض (delegation path): تتابع مرتّب من الشهادات يمكن معالجته، إضافة إلى الاستيقان من هوية مؤكّد الامتياز، من أجل التحقق من أصالة الامتياز الحائز عليه.

26.3.3 القائمة دلتا لإبطال الشهادات (delta-CRL) (dCRL): قائمة إبطال جزئي، تضم فقط المداخل إلى الشهادات التي جرى تعديل على وضع إبطالها القانوني، منذ إصدار القائمة الأساسية المرجعية لإبطال الشهادات.

27.3.3 الكيان النهائي (end entity): هو إما صاحب شهادة مفتاح عمومي يستخدم مفتاحه الخاص لغير أغراض توقيع الشهادات، وإما حامل شهادة نعت يستخدم نعوته للنفاذ إلى أحد الموارد، وإما كيان هو طرف واثق.

28.3.3 قائمة إبطال شهادات نعت صادرة لكيانات نهائية (end-entity attribute certificate revocation list) (EARL): قائمة إبطال تضم قائمة شهادات نعت صادرة إلى حامليها الذين ليسوا سلطات نعت (AA) و لم يعد مُصْدِر الشهادة يعتبرهم صالحين.

29.3.3 قائمة إبطال شهادات مفتاح عمومي صادرة لكيانات نهائية (end-entity public-key certificate revocation list) (EPRL): قائمة إبطال تضم قائمة شهادات مفتاح عمومي صادرة إلى أصحابها الذين ليسوا سلطات إصدار شهادة (CA) و لم يعد مُصْدِر الشهادة يعتبرهم صالحين.

30.3.3 متحولات بيئية (environmental variables): هي تلك الجوانب من السياسة اللازمة لاتخاذ قرار بالترخيص، وهي ليست موجودة في بنى ثابتة ولكنها يمكن أن تتيسر بوسائل محلية للمتحقق من امتياز (مثل اليوم والساعة أو الرصيد الحالي لحساب).

31.3.3 القائمة الكاملة لإبطال الشهادات (full CRL): قائمة إبطال كاملة تحتوي على مداخل جميع الشهادات التي أبطلت في مجال تطبيق معيّن.

32.3.3 دالّة الفرم (hash function): دالّة (رياضية) تقابل قيم مجال واسع (وربما واسع جداً) بقيم مجال أضيق. ودالّة الفرم "الجيدة" هي التي يعطي تطبيقها على مجموعة (واسعة) من القيم في المجال الأول قيماً موزعة بطريقة متساوية (عشوائية في الظاهر) في المجال الثاني.

33.3.3 حامل (holder): هو كيان تم تفويض امتياز إليه إما مباشرة من مَصْدر السلطة وإما بطريقة غير مباشرة عن طريق سلطة نعت أخرى.

34.3.3 قائمة غير مباشرة لإبطال الشهادات (indirect CRL) (iCRL): قائمة إبطال تحتوي على الأقل على معلومات إبطال تخص شهادات صادرة عن سلطات غير السلطة التي تصدر هذه القائمة.

35.3.3 اتفاق المفتاح (key agreement): طريقة للتفاوض على الخط بشأن قيمة للمفتاح، دون نقل المفتاح، ولو بشكل مجفّر، باستخدام تقنية ديفي–هِلْمان مثلاً (انظر المعيار ISO/IEC 11770-1 لمزيد من المعلومات حول آليات اتفاق المفتاح).

36.3.3 الطريقة الهدف (object method): عمل يمكن استدعاؤه بشأن مورد (مثلاً يمكن أن يتوفر لأسلوب الملفات الطرائق الأهداف للقراءة والكتابة والتنفيذ).

37.3.3 دالّة وحيدة الاتجاه (one-way function): دالّة (رياضية) f حسابها سهل، ولكن من الصعب إيجاد قيمة x في المجال المَصْدر تقابل قيمة ما y في المجال الصورة، بحيث يكون $y = f(x)$. وقد تكون هناك قلّة من قيم y لا يصعب إيجاد قيمة تقابلها x.

38.3.3 تقابل السياسات (policy mapping): الاعتراف بأنه عندما تصدّق سلطة إصدار الشهادة في أحد الميادين على سلطة إصدار الشهادة في ميدان آخر، يمكن أن تعتبر سلطة الميدان الأول سياسة شهادة خاصة صادرة في الميدان الثاني بأنها مكافئة (ولكنها ليست مطابقة من جميع الجوانب) لسياسة شهادة خاصة صادرة في الميدان الأول.

39.3.3 المفتاح الخاص، المفتاح السري (مصطلح متروك) (private key; secret key): (في نظام التجفير مع المفتاح العمومي) هو المفتاح الذي لا يعرفه إلا المستعمل وحده، من زوج مفاتيح المستعمل.

40.3.3 امتياز (privilege): هو نعت أو صفة تسندها سلطة ما إلى كيان ما.

41.3.3 مؤكد الامتياز (privilege asserter): صاحب امتياز يستخدم شهادة نعته أو شهادة مفتاحه العمومي ليؤكد امتيازه.

42.3.3 بنية تحتية لإدارة امتياز (PMI) (privilege management infrastructure): البنية التحتية التي تتحمل أعباء إدارة الامتيازات المقابلة لخدمة ترخيص كاملة ولها علاقة بالبنية التحتية للمفتاح العمومي.

43.3.3 سياسة الامتياز (privilege policy): السياسة التي تعيّن الخطوط العريضة للشروط التي يستطيع ضمنها المتحققون من الامتياز من تقديم أو أداء خدمات حساسة لصالح أو لحساب مؤكدي الامتيازات المؤهلين. وسياسة الامتياز مرتبطة بنعوت تخص الخدمة وكذلك بنعوت تخص مؤكدي الامتيازات.

44.3.3 متحقق من الامتياز (privilege verifier): كيان يتحقق من الشهادات وفق سياسة الامتياز.

45.3.3 المفتاح العمومي (public-key): (في نظام التجفير ذي المفتاح العمومي) هو المفتاح المعروف لدى العموم، من زوج مفاتيح المستعمل.

46.3.3 شهادة المفتاح العمومي (PKC) (public-key certificate): المفتاح العمومي لمستعمل، مصحوباً ببعض المعلومات الأخرى التي أصبحت غير قابلة للتزوير، عن طريق توقيع رقمي يستعمل فيه المفتاح الخاص الذي تصدره سلطة إصدار الشهادة.

47.3.3 بنية تحتية للمفتاح العمومي (PKI) (public key infrastructure): البنية التحتية التي تتحمل أعباء إدارة المفاتيح العمومية، لكي تقدم خدمات الاستيقان أو التجفير أو التكاملية أو عدم الرفض.

48.3.3 طرف واثق (relying party): مستعمل أو وكيل يثق بالمعطيات الواردة في شهادة ما عند اتخاذه القرارات.

49.3.3 شهادة إسناد الدور (role assignment certificate): شهادة تحتوي على نعت الدور، وتسند دوراً أو أكثر من دور، إلى صاحب الشهادة أو حاملها.

50.3.3 شهادة مواصفة الدور (role specification certificate): شهادة تحتوي على الامتيازات المسندة إلى دور ما.

51.3.3 الحساسية (sensitivity): خاصية أحد الموارد المرتبطة بقيمته أو بأهميته.

52.3.3 الاستيقان البسيط (simple authentication): استيقان عن طريق ترتيبات بسيطة لكلمة السر.

53.3.3 السياسة الأمنية (security policy): مجموعة من القواعد تضعها السلطة الأمنية التي يخضع لها استعمال وتقديم الخدمات والمرافق الأمنية.

54.3.3 شهادة (من سلطة) نعت صادرة لذاتها (self-issued AC): شهادة نعت يكون فيها مُصْدر الشهادة وحاملها هما نفس سلطة النعت. وتستطيع سلطة النعت استخدام شهادة نعت صادرة لذاتها، لكي تنشر مثلاً معلومات عن السياسة.

55.3.3 شهادة صادرة لذاتها (self-issued certificate): شهادة مفتاح عمومي يكون فيها مُصْدر الشهادة وصاحبها هما نفس سلطة إصدار الشهادة (CA). وتستطيع سلطة إصدار الشهادة استخدام شهادات صادرة لذاتها، أثناء عملية تجديد مفتاح مثلاً، من أجل نقل الثقة من المفتاح القديم إلى المفتاح الجديد.

56.3.3 شهادة موقّعة من ذاتها (self-signed certificate): حالة خاصة من الشهادات الصادرة لذاتها، حيث يكون فيها المفتاح الخاص الذي تستعمله سلطة إصدار الشهادة لتوقيع الشهادة مقابلاً للمفتاح العمومي المصدّق عليه داخل الشهادة. وتستطيع سلطة إصدار الشهادة استعمال شهادة موقعة من ذاتها، لكي تعلن مثلاً عن مفتاحها العمومي أو غيره من المعلومات الخاصة بتشغيلها.

ملاحظة: لا يقع استعمال الشهادات الصادرة لذاتها أو الموقّعة من ذاتها الصادرة من غير سلطات إصدار الشهادة ضمن مجال تطبيق هذه التوصية | هذا المعيار الدولي.

57.3.3 مَصْدر السلطة (source of authority) (SOA): سلطة نعت يستطيع متحقق من الامتياز أن يمنحها الثقة بشأن مورد معين، باعتبارها السلطة النهائية التي تسند مجموعة من الامتيازات.

58.3.3 الاستيقان المعمّق (strong authentication): استيقان يستخدم ثبوتيات حاصلة بوسائل تجفيرية.

59.3.3 الثقة (trust): يقال بصورة عامة بأن كياناً أول "يثق" بكيان ثانٍ، عندما يستطيع الكيان الأول أن يفترض أن الكيان الثاني سيتصرف تماماً كما يتوقع له الكيان الأول. ولا يمكن أن تنطبق هذه الثقة إلا على وظيفة معينة خاصة. ويكمن الدور الرئيسي للثقة في هذا الإطار في وصف العلاقة بين كيان يقوم بالاستيقان وبين سلطة، ويجب أن يكون الكيان متأكداً بأنه يستطيع أن يثق بكون السلطة لن تخلق إلا شهادات صالحة وموثوقة.

60.3.3 مرسِّخة الثقة (trust anchor): مرسِّخة الثقة هي مجموعة المعلومات التالية، إضافة إلى المفتاح العمومي: معرف هوية الخوارزمية، ومعلمات المفتاح العمومي (عند اللزوم)، والاسم المميز لحامل المفتاح الخاص المصاحب (أي صاحب الشهادة CA)، وبصورة اختيارية فترة الصلاحية. ويمكن أن تكون مرسِّخة الثقة بشكل شهادة موقعة من ذاتها. ويستطيع نظام يعتمد على الشهادات أن يثق بمرسِّخة ثقة، وأن تستخدم هذه الأخيرة لإقرار صلاحية شهادات في مسيرات إصدار الشهادات.

4 المختصرات

تطبق المختصرات التالية لأغراض هذه التوصية | هذا المعيار الدولي:

AA	سلطة النعت	Attribute Authority
AARL	قائمة إبطال سلطات النعت	Attribute Authority Revocation List
AC	شهادة نعت	Attribute Certificate
ACRL	قائمة إبطال شهادات النعت	Attribute Certificate Revocation List
CA	سلطة إصدار الشهادة	Certification Authority
CARL	قائمة إبطال سلطات إصدار الشهادة	Certification Authority Revocation List
CRL	قائمة إبطال الشهادات	Certificate Revocation List
dCRL	القائمة دلتا لإبطال الشهادات	Delta Certificate Revocation List
DIB	قاعدة معلومات الدليل	Directory Information Base
DIT	شجرة معلومات الدليل	Directory Information Tree
DSA	وكيل نظام الدليل	Directory System Agent
DUA	وكيل مستعمل الدليل	Directory User Agent
EARL	قائمة إبطال شهادات نعت صادرة لكيانات نهائية	End-entity Attribute certificate Revocation List
EPRL	قائمة إبطال شهادات مفتاح عمومي صادرة لكيانات نهائية	End-entity Public-key certificate Revocation List
iCRL	قائمة غير مباشرة لإبطال الشهادات	Indirect Certificate Revocation List

OCSP	بروتوكول وضع الشهادة القانوني على الخط	Online Certificate Status Protocol
PKC	شهادة المفتاح العمومي	Public-Key Certificate
PKCS	نظام تجفير بالمفتاح العمومي	Public-Key Cryptosystem
PKI	بنية تحتية للمفتاح العمومي	Public-Key Infrastructure
PMI	بنية تحتية لإدارة امتياز	Privilege Management Infrastructure
SOA	مَصْدر السلطة	Source of Authority

5 اصطلاحات

أعدّت مواصفة الدليل هذه طبقاً *لقواعد تقديم النصوص المشتركة بين ITU-T | ISO/IEC* المؤرخة في نوفمبر 2001، مع بعض الاستثناءات الطفيفة.

يجب أن يعتبر المصطلح "مواصفة الدليل" (كما في "مواصفة الدليل هذه") على أنه يقصد التوصية ITU-T X.509 | المعيار ISO/IEC 9594-8، كما يعتبر المصطلح "مواصفات الدليل" على أنه يقصد توصيات السلسلة X.500 وجميع أجزاء المعيار ISO/IEC 9594.

وتستخدم مواصفة الدليل هذه مصطلح *أنظمة الطبعة الأولى* لتشير إلى الأنظمة المطابقة للطبعة الأولى من مواصفات الدليل، أي طبعة عام 1988 من سلسلة التوصيات X.500 الصادرة عن اللجنة CCITT، وطبعة المعيار ISO/IEC 9594:1990. وتستخدم مواصفة الدليل هذه مصطلح *أنظمة الطبعة الثانية* لتشير إلى الأنظمة المطابقة للطبعة الثانية من مواصفات الدليل، أي طبعة عام 1993 من سلسلة التوصيات X.500 الصادرة عن القطاع ITU-T، وطبعة المعيار ISO/IEC 9594:1995. وتستخدم مواصفة الدليل هذه مصطلح *أنظمة الطبعة الثالثة* لتشير إلى الأنظمة المطابقة للطبعة الثالثة من مواصفات الدليل، أي طبعة عام 1997 من سلسلة التوصيات X.500 الصادرة عن القطاع ITU-T، وطبعة المعيار ISO/IEC 9594:1998. وتستخدم مواصفة الدليل هذه مصطلح *أنظمة الطبعة الرابعة* لتشير إلى الأنظمة المطابقة للطبعة الرابعة من مواصفات الدليل، أي طبعات عام 2001 من توصيات القطاع ITU-T ذات الأرقام X.500 وX.501 وX.511 وX.518 وX.519 وX.520 وX.521 وX.525 وX.530 وطبعة عام 2000 من التوصية ITU-T X.509، وكذلك الأجزاء من 1 إلى 10 من طبعة المعيار ISO/IEC 9594:2001.

وتستخدم مواصفة الدليل هذه مصطلح *أنظمة الطبعة الخامسة* لتشير إلى الأنظمة المطابقة للطبعة الخامسة من مواصفات الدليل، أي طبعات عام 2005 من توصيات القطاع ITU-T ذات الأرقام X.500 وX.501 وX.509 وX.518 وX.519 وX.520 وX.521 وX.525 وX.530 وكذلك الأجزاء من 1 إلى 10 من طبعة المعيار ISO/IEC 9594:2005.

تعرض مواصفة الدليل هذه ترميز علم النحو المجرد 1 (ASN.1) بالسمات Helvetica السوداء. وعندما يحال في النص العادي إلى أنماط وقيم من الترميز ASN.1 فإنها تميز عن النص العادي بعرضها بالسمات Helvetica السوداء. وتميز أسماء الإجراءات، التي تكون عادة موضوعاً لمرجع أثناء مواصفة معاني المعالجة، عن النص العادي بعرضها بالسمات Times السوداء. أما حالات السماح بالتحكم في النفاذ فتعرض بالسمات Times المائلة.

إذا كانت البنود في قائمة ما مرقّمة (بدلاً من أن تكون مسبوقة بشرطة "–" أو بحرف)، عندئذ تعتبر البنود خطوات في عملية ما.

ويحدد الجدول 1 التالي الترميز المستخدم في مواصفة الدليل هذه.

الجدول 1 – الترميز

الترميز	المعنى
Xp	المفتاح العمومي لمستعمل X.
Xs	المفتاح الخاص للمستعمل X.

الترميز	المعنى
Xp[I]	تجفير المعلومات I باستخدام المفتاح العمومي للمستعمل X.
Xs[I]	تجفير المعلومات I باستخدام المفتاح الخاص للمستعمل X.
X{I}	توقيع المستعمل X على المعلومات I. ويتألف من I مع إضافة موجز مجفّر.
CA(X)	سلطة إصدار الشهادة للمستعمل X.
$CA^n(X)$	(حيث n>1:CA(CA(...n مرة ...(X)))
$X_1<<X_2>>$	شهادة المستعمل X_2 تصدرها سلطة إصدار شهادة X_1.
$X_1<<X_2>>$ $X_2<<X_3>>$	سلسلة من الشهادات (من أي طول)، كل بند فيها شهادة لسلطة إصدار الشهادة التي أنتجت البند التالي. إنها مكافئة وظيفياً للشهادة التالية $X1<<X_{n+1}>>$. وامتلاك سلسلة الشهادات A<<B>>B<<C>> يوفر نفس الإمكانات مثل A<<C>>، أي إمكان إيجاد Cp من معرفة Ap.
$X_1p \circ X_1<<X_2>>$	عملية فتح شهادة (أو سلسلة شهادات) ونشرها لاستخراج مفتاح عمومي. وتتضمن العملية مؤثراً واسطاً يكون المتأثر اليساري به هو المفتاح العمومي لسلطة إصدار الشهادة، ويكون المتأثر اليميني به هو شهادة صادرة عن هذه السلطة لإصدار الشهادة. ويكون الناتج هو المفتاح العمومي للمستعمل الذي شهادته هي المتأثر اليميني. مثلاً: Ap ° A<<B>> B<<C>> يبين عملية استخدام مفتاح A العمومي للحصول على مفتاح B العمومي، Bp، من شهادته، تتبعها عملية استخدام المفتاح العمومي Bp لفتح شهادة C. وناتج العملية هو مفتاح C العمومي، Cp.
A→B	مسيرة إصدار الشهادة من A إلى B، المكوّنة من سلسلة من الشهادات تبدأ مع $CA(A)<<CA^2(A)>>$ وتنتهي مع CA(B)<<B>>.
ملاحظة – تمثل الرموز X وX_1 وX_2 ... في الجدول أسماء المستعملين، بينما يمثل الرمز I أيَّ معلومات.	

6 نظرة شاملة إلى الأطر

تحدد هذه المواصفة إطاراً يتيح الحصول على مفتاح عمومي لأحد الكيانات ثم الوثوق به، بغية تجفير المعلومات التي سيفكّ تجفيرها هذا الكيان، أو بغية التحقق من التوقيع الرقمي لهذا الكيان. ويشمل هذا الإطار إصدار شهادة مفتاح عمومي من سلطة إصدار الشهادة (CA) وإقرار صلاحية هذه الشهادة من مستعمل الشهادة. ويشمل إقرار الصلاحية:

- إقامة مسيرة موثوقة للشهادة بين مستعمل الشهادة وصاحب الشهادة؛
- التحقق من التوقيعات الرقمية على كل شهادة واقعة في المسيرة؛
- إقرار صلاحية جميع الشهادات الواقعة في المسيرة (أي إن صلاحيتها غير منتهية و لم يجر إبطالها في وقت ما).

وتحدد هذه المواصفة إطاراً يتيح الحصول على نعوت امتياز لأحد الكيانات ثم الوثوق بها، لتحديد ما إذا كانت مرخصة للنفاذ إلى مورد معين أم لا. ويشمل هذا الإطار إصدار شهادة من سلطة نعت (AA) وإقرار صلاحية هذه الشهادة من متحقق من الامتياز. ويشمل إقرار الصلاحية:

- التأكد من أن امتيازات هذه الشهادة كافية، عند النظر إليها من حيث سياسة الامتياز؛
- إقامة مسيرة موثوقة لتفويض الشهادات، عند اللزوم؛
- التحقق من التوقيعات الرقمية على كل شهادة واقعة في المسيرة؛
- التأكد من أن كل مُصْدر كان مرخصاً له تفويض الامتيازات؛
- التحقق من عدم انتهاء صلاحية هذه الشهادات ومن أن مُصْدريها لم يبطلوها.

وعلى الرغم من أن البنى التحتية PKI وMPI هي بنى منفصلة، ويمكن إنشاء كل منها بصورة مستقلة عن الأخرى، إلا إنها تتعلق ببعضها. وتوصي هذه المواصفة بأن يتم تعريف هوية حاملي شهادات النعت ومُصْدريها داخل شهادات النعت

بمؤشرات تبين شهادات مفاتيحهم العمومية المناسبة. ويجري استيقان مُصْدري شهادات النعت وحامليها، الضروري لضمان كون الكيانات المطالبة بالامتياز أو التي تصدره هي فعلاً الكيانات التي تدّعيها، عن طريق استخدام العملية العادية في البنية التحتية PKI لاستيقان الهويات. ولا تتكرر عملية الاستيقان هذه مرة ثانية في إطار شهادة النعت.

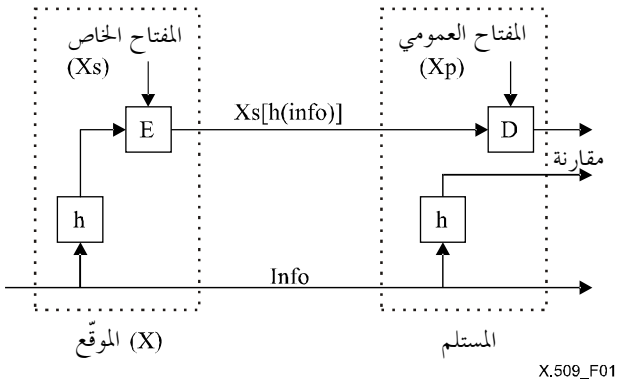
1.6 التوقيعات الرقمية

تستعمل التوقيعات الرقمية في كلا نوعي البنى التحتية PKI وMPI باعتبارها الآلية التي تصدّق بها السلطة التي تصدر الشهادة على الصلة الموجودة في الشهادة. وفي البنية التحتية PKI يصدّق التوقيع الرقمي على شهادة المفتاح العمومي لسلطة إصدار الشهادة التي أصدرتها، على العلاقة بين معلومات المفتاح العمومي وصاحب الشهادة. وفي البنية التحتية MPI، يصدّق التوقيع الرقمي لسلطة النعت المُصْدرة على العلاقة بين النعوت (الامتيازات) وحامل الشهادة. ويشرح هذا البند الفرعي التوقيعات الرقمية بشكل عام. ويناقش القسمان الثاني والثالث من هذه المواصفة استخدام التوقيعات الرقمية، خاصة في البنى PKI وMPI.

وهذا البند الفرعي ليس معدّاً ليحدّد معياراً للتوقيعات الرقمية بشكل عام، ولكنه يحدد الوسائل التي يتم بها توقيع الإذنات في البنى التحتية PKI وMPI وفي الدليل.

ويجري توقيع المعلومات (info) بتذييلها بموجز مجفّر للمعلومات. وينجز الموجز بواسطة دالّة فَرْم وحيدة الاتجاه، بينما يجري التجفير باستخدام المفتاح الخاص للموقّع (انظر الشكل 1). وينتج عن ذلك:

X{Info} = Info, Xs[h (Info)]



الشكل 1 – التوقيعات الرقمية

ملاحظة 1 – التجفير بالمفتاح الخاص يضمن عدم إمكانية تزوير التوقيع. وطبيعة كون دالّة الفَرْم وحيدة الاتجاه، تضمن عدم إمكانية الاستعاضة بمعلومات مزوّرة، جرى توليدها ليكون لها نتيجة فرم مطابقة (وبالتالي عدم إمكانية تقليد التوقيع).

إن مستلم المعلومات الموقّعة يتحقق من التوقيع كما يلي:

- يطبق دالّة الفرم وحيدة الاتجاه على المعلومات؛
- يقارن النتيجة بالنتيجة الحاصلة من فك تجفير التوقيع الحاصل باستخدام المفتاح العمومي للموقّع.

ولا تفرض هذه المواصفة دالّة فَرْم وحيدة الاتجاه واحدة لاستخدامها في التوقيع. إنها مصممة بحيث ينطبق الإطار على أي دالة فَرْم مناسبة، وبذلك يتحمل كل التغيرات التي تطرأ على الطرائق المستعملة في المستقبل بفعل التقدم الذي سيحصل في طريقة التجفير أو في التقنيات الرياضية أو في المقدرات الحسابية. وعليه إذا رغب مستعملان في استيقان كل منهما من الآخر، يكون عليهما أن يتحملا دالة الفَرْم نفسها لكي يجريا استيقاناً مضبوطاً. وعليه فإن اختيار دالّة واحدة في سياق مجموعة من التطبيقات المترابطة سوف يساعد إلى أقصى حد على تكبير جماعة المستعملين القادرين على استيقان بعضهم بعض والاتصال المأمون فيما بينهم.

وتشمل المعلومات الموقعة مؤشرات تعرّف بخوارزمية الفرم وخوارزمية التجفير المستعملتين لحساب التوقيع الرقمي.

ويمكن وصف تجفير أحد عناصر المعطيات باستخدام الترميز ASN.1 التالي:

```
ENCRYPTED { ToBeEnciphered } ::=   BIT STRING ( CONSTRAINED BY {
-- shall be the result of applying an encipherment procedure --
-- to the BER-encoded octets of a value of -- ToBeEnciphered } )
```

*-- يجب أن تكون نتيجة تطبيق إجراء التجفير على أثمونات التشفير BER (قواعد التشفير الأساسي) بقيمة -- **يطلب تجفيرها** --*

تولد قيمة سلسلة البتات بأخذ الأثمونات التي تشكل التشفير الكامل (باستخدام قواعد التشفير الأساسي في الترميز ASN.1 الوارد في التوصية ITU-T X.690 (2002) | في المعيار الدولي ISO/IEC 8825-1:2002) لقيمة النمط **يطلب تجفيره (ToBeEnciphered)**، وتطبيق إجراء التجفير عليها.

ملاحظة 2 – يتطلب إجراء التجفير اتفاقاً على الخوارزمية المطلوب تطبيقها، بما في ذلك معلمات الخوارزمية من مثل مجموعة المفاتيح اللازمة وقيم التدميث وتعليمات التحشية. وتقع المسؤولية على إجراءات التجفير لكي تحدد الوسائل التي تحقق التزامن بين مرسل المعطيات ومستقبلها والتي يمكنها أن تتضمن معلومات في البتات المطلوب إرسالها.

ملاحظة 3 – مطلوب من إجراءات التشفير أن تقبل مُدْخلاً هو سلسلة من الأثمونات وأن تولد سلسلة واحدة من البتات كنتيجة.

ملاحظة 4 – ليست الآليات المطلوبة للحصول على اتفاق موثوق بين مرسل المعطيات ومستقبلها بشأن خوارزمية التجفير ومعلماتها، واقعة في مجال تطبيق مواصفة الدليل هذه.

ويجري التوقيع على عنصر معطيات بتجفير تحويل مختصر أو "مفروم" لهذا العنصر، ويمكن وصفه باستخدام الترميز ASN.1 التالي:

```
HASH {ToBeHashed}          ::=   SEQUENCE {
algorithmIdentifier        AlgorithmIdentifier,
hashValue                  BIT STRING ( CONSTRAINED BY {
   -- shall be the result of applying a hashing procedure to the DER-encoded octets --
   -- of a value of -- ToBeHashed } ) }
```

*-- يجب أن تكون نتيجة تطبيق إجراء الفرم على أثمونات التشفير DER (قواعد التشفير المميزة) بقيمة -- **يطلب فرمها** --*

```
ENCRYPTED-HASH { ToBeSigned }    ::=          BIT STRING ( CONSTRAINED BY {
   -- shall be the result of applying a hashing procedure to the DER-encoded octets --
   -- of a value of -- ToBeSigned -- and then applying an encipherment procedure to those octets -- })
```

-- يجب أن تكون نتيجة تطبيق إجراء فرم على أثمونات التشفير DER (قواعد التشفير المميزة)
*-- بقيمة -- **يطلب توقيعها** – ثم تطبيق إجراء تجفير على هذه الأثمونات.*

```
SIGNATURE { ToBeSigned }      ::=          SEQUENCE {
   algorithmIdentifier        AlgorithmIdentifier,
   encrypted                  ENCRYPTED-HASH { ToBeSigned }}
```

ملاحظة 5 – يتطلب إجراء التجفير الاتفاقات المبينة في الملاحظة 2 وكذلك تتطلب اتفاقاً بشأن جعل الأثمونات المفرومة تجفّر مباشرة، أو بعد تشفيرها بشكل **سلسلة بتات BIT STRING** بواسطة قواعد التشفير الأساسي في الترميز ASN.1.

ويمكن استخدام الترميز ASN.1 التالي من أجل تعريف نمط المعطيات الذي ينتج من تطبيق توقيع على نمط معطيات معين، في حالة كون نمط المعطيات مطلوباً تذييله بالتوقيع.

```
SIGNED { ToBeSigned }          ::=          SEQUENCE {
   toBeSigned                  ToBeSigned,
   COMPONENTS OF               SIGNATURE { ToBeSigned }}
```

يلزم تشفير مميز لإقرار صلاحية النمطين **موقَّع (SIGNED)** و**توقيع (SIGNATURE)** في بيئة موزعة. ويمكن الحصول على تشفير مميز لمعطيات النمطين **موقّع** أو **توقيع** بتطبيق قواعد التشفير الأساسي المعرفة في التوصية ITU-T X.690 (2002) | في المعيار الدولي ISO/IEC 8825-1:2002، مع القيود التالية:

أ) يجب أن يستعمل شكل التشفير الواضح للطول، مشفراً بأصغر عدد ممكن من الأثمونات؛

ب) يجب ألا يستعمل شكل التشفير المركب لأنماط السلسلة؛

ج) إذا كانت قيمة أحد الأنماط هي قيمته بالتغيب، تعتبر قيمة غائبة؛

د) يجب أن تشفر مكوّنات النمط **مجموعة** (Set) وفق الترتيب التصاعدي لقيمة وَشْمها؛

ه) يجب أن تشفر مكونات النمط **مجموعة من** (Set-of) وفق الترتيب التصاعدي لقيمة أثمونها؛

و) إذا كانت قيمة نمط بولاني تساوي"صائبة"، يجب أن يحتوي التشفير على أثمون موضوع على 16"FF"؛

ز) كل بتة غير مستعملة في الأثمون النهائي من تشفير **سلسلة البتات**، إن وجدت، يجب أن توضع على الصفر؛

ح) يجب ألا يستعمل تشفير نمط حقيقي الأسس 8 و10 و16، ويجب أن يكون عامل المقايسة الاثنيني مساوياً الصفر؛

ط) يجب أن يشفّر التوقيت العالمي المنسق (UTC) كما هو محدد في التوصية ITU-T X.690 (2002) | في المعيار الدولي ISO/IEC 8825-1:2002؛

ي) يجب أن يشفّر التوقيت المعمّم كما هو محدد في التوصية ITU-T X.690 (2002) | في المعيار الدولي ISO/IEC 8825-1:2002.

يتطلب توليد تشفير مميّز أن يكون النحو المجرد للمعطيات المطلوب تشفيره مفهوماً بالكامل. وربما يكون استعمال الدليل ضرورياً للتوقيع على المعطيات أو للتحقق من توقيع المعطيات التي تحتوي على توسعات بروتوكول غير معروفة أو على قواعد نَحْو للنعت غير معروفة. ويتعين على الدليل أن يتّبع القواعد التالية:

- يجب أن يحتفظ بتشفير المعلومات المستقبلة التي لا يعرف هو نحوها المجرد بالكامل، والتي يتوقع أن عليه أن يوقّعها لاحقاً؛
- عندما يوقّع المعطيات المطلوب إرسالها، يرسل المعطيات التي يعرف نحوها بالكامل وهي مشفرة تشفيراً مميزاً، ويحتفظ بتشفير المعطيات الأخرى، ويتعين عليه أن يوقع التشفيرات التي يرسلها فعلاً؛
- عند التحقق من التوقيعات الموجودة في المعطيات المستقبلة، عليه أن يتحقق من التوقيعات بالنسبة إلى المعطيات المستقبلة فعلاً، قبل تحويلها إلى تشفير مميز.

القسم الثاني – إطار شهادة المفتاح العمومي

إطار شهادة المفتاح العمومي الموضح في هذه المواصفة معدّ لكي تستخدمه تطبيقات بحاجة إلى استيقان وتكاملية وسرية وعدم رفض.

وربط مفتاح عمومي بكيان ما، تقوم به سلطة عهن طريق بنية من المعطيات موقّعة رقمياً تدعى شهادة المفتاح العمومي. ونسق شهادات المفتاح العمومي موضح في هذه المواصفة وهو يشمل آلية لقابلية توسع مع مجموعة من التوسعات الخاصة في الشهادة. وإذا قامت سلطة ما، لأي سبب كان، بإبطال شهادة مفتاح عمومي صادرة سابقاً، يحتاج المستعملون أن يعلموا بحدوث هذا الإبطال، حتى لا يستعملوا شهادة ليست أهلاً للثقة بها. وقوائم الإبطال هي إحدى الوسائل الممكن استعمالها لتبليغ المستعملين بالإبطالات. ونسق قوائم الإبطال موضّح في هذه المواصفة، وهو يشمل آلية قابلية توسع مع مجموعة من التوسعات في قائمة الإبطال. وتستطيع هيئات أخرى أن تحدد توسعات إضافية في الشهادة وفي قائمة الإبطال على السواء، تكون مفيدة لها في بيئاتها الخاصة.

ويحتاج نظام استعمال شهادة المفتاح العمومي إلى إقرار صلاحية الشهادة قبل استخدامها في أي تطبيق. وإجراءات القيام بهذا الإقرار للصلاحية موضحة أيضاً في هذه المواصفة، وتشمل التحقق من تكاملية الشهادة بحد ذاتها، ومن وضع إبطالها القانوني، ومن صلاحيتها بالنسبة إلى الاستعمال المزمع.

يستخدم الدليل شهادات المفتاح العمومي لتقديم الخدمات الأمنية التالية:

- الاستيقان المعمق ما بين مكوّنات الدليل وخلالها؛
- استيقان عمليات الدليل وتكامليتها وسريتها؛
- تكاملية المعطيات المخزونة واستيقانها.

7 المفاتيح العمومية وشهادات المفتاح العمومي

يجب الحصول على المفتاح العمومي من مصدر موثوق، حتى يستطيع أحد المستعملين أن يثق بالمفتاح العمومي لمستعمل آخر، لكي يستيقن هوية هذا المستعمل مثلاً. ومثل هذا المصدر الذي يسمى سلطة إصدار الشهادة (CA) يصدّق على مفتاح عمومي بإصداره شهادة مفتاح عمومي تسند المفتاح العمومي إلى الكيان الذي يحمل المفتاح الخاص المقابل. وإن الإجراءات التي تستخدمها سلطة إصدار الشهادة للتأكيد على أن كياناً ما هو في الواقع مالك المفتاح الخاص، وغيرها من الإجراءات المتعلقة بإصدار شهادات المفتاح العمومي، تقع خارج نطاق هذه المواصفة. والشهادة التي يحدد هذا البند شكلها لاحقاً، تكون لها الصفات التالية:

- كل مستعمل له نفاذ إلى مفتاح عمومي تابع لسلطة إصدار الشهادة، يمكنه استعادة المفتاح العمومي الذي كان مصدّقاً عليه؛
- لا يستطيع أي طرف غير سلطة إصدار الشهادة أن يعدّل الشهادة من دون أن يُكْتشف عمله (لا يمكن تزوير الشهادات).

ولما كانت الشهادات غير قابلة للتزوير، يمكن نشرها في الدليل، دون أن يحتاج الدليل إلى بذل جهود خاصة لحمايتها.

ملاحظة 1 – على الرغم من أن سلطات إصدار الشهادة معرّفة دون لبس باسم مميز في شجرة معلومات الدليل (DIT)، فإن ذلك لا ينطوي على وجود أي علاقة بين هيئات سلطات إصدار الشهادة وشجرة معلومات الدليل.

وتصدر سلطة إصدار الشهادة شهادة لمستعمل ما بأن توقّع (انظر الفقرة 1.6) على مجموعة من المعلومات، تحتوي على الاسم المميز للمستعمل، والمفتاح العمومي، وكذلك على *معرف هوية وحيد* اختياري يحتوي على معلومات إضافية عن المستعمل. ولا توضّح هذه المواصفة الشكل المضبوط لمعرف الهوية الوحيد، وهو متروك لخيار سلطة إصدار الشهادة، فقد يكون مثلاً معرّف هوية شيء أو شهادة أو تاريخاً أو أي شكل آخر من التصديق على صلاحية الاسم المميز. ويكون الشكل التالي هو شكل شهادة مستعمل اسمه المميز هو A ومعرف هويته الوحيد هو UA، تنشرها سلطة إصدار شهادة اسمها هو CA ومعرف هويتها الوحيد هو UCA:

$$CA\langle\langle A\rangle\rangle = CA\{V,SN,AI,CA,UCA,A,UA,Ap,T^A\}$$

حيث V يمثل صيغة الشهادة، وSN يمثل رقم تسلسل الشهادة، وAI يمثل معرف هوية الخوارزمية المستعملة للتوقيع على الشهادة، وUCA يمثل معرف الهوية الوحيد الاختياري للسلطة CA، وUA يمثل معرف الهوية الوحيد الاختياري للمستعمل A، وT^A يدل على فترة صلاحية الشهادة، ويتكون من تاريخين هما أول وآخر تاريخ تبقى الشهادة صالحة بينهما. وفترة صلاحية الشهادة هي الفاصل الزمني الذي تكفل السلطة CA أثناءه أنها ستبقى تحتفظ بمعلومات الوضع القانوني للشهادة، أي نشر معطيات الإبطال. ولما كان من المفترض في T^A ألا يصيبه تغيير إلا في فترات لا تقل عن 24 ساعة، فمن المتوقع أن تستخدم الأنظمة التوقيت العالمي المنسق (UTC) كقاعدة زمنية مرجعية. وكل مستعمل يعرف المفتاح العمومي CAp للسلطة CA، يمكنه التحقق من صلاحية توقيع الشهادة. ويمكن استخدام النمط التالي من معطيات الترميز ASN.1 لتمثيل الشهادات:

```
Certificate                ::=  SIGNED { SEQUENCE {
    version           [0]      Version DEFAULT v1,
    serialNumber               CertificateSerialNumber,
    signature                  AlgorithmIdentifier,
    issuer                     Name,
    validity                   Validity,
    subject                    Name,
```

```
    subjectPublicKeyInfo        SubjectPublicKeyInfo,
    issuerUniqueIdentifier  [1] IMPLICIT UniqueIdentifier OPTIONAL,
                                -- if present, version shall be v2 or v3        -- إن وجدت تكون الصيغة v2 أو v3
    subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL,
                                -- if present, version shall be v2 or v3        -- إن وجدت تكون الصيغة v2 أو v3
    extensions              [3] Extensions OPTIONAL
                                -- if present, version shall be be v3 -- } }    -- إن وجدت تكون الصيغة v3 -- { {

    Version                     ::=     INTEGER { v1(0), v2(1), v3(2) }

    CertificateSerialNumber     ::=     INTEGER

AlgorithmIdentifier         ::=     SEQUENCE {
    algorithm           ALGORITHM.&id ({SupportedAlgorithms}),
    parameters          ALGORITHM.&Type ({SupportedAlgorithms}{ @algorithm}) OPTIONAL }
    -- Definition of the following information object set is deferred, perhaps to standardized
    -- profiles or to protocol implementation conformance statements. The set is required to
    -- specify a table constraint on the parameters component of AlgorithmIdentifier.
                                -- تعريف موضوع المعلومات التالية مؤجل، ربما حتى تتيسر الجانبيات المقيّسة أو الإعلانات عن التطابق مع تنفيذ
                                -- البروتوكول. والمجموعة لازمة لمواصفة جدول التقييدات على المعلمات المكوّنة لمعرّف هوية الخوارزمية --
--  SupportedAlgorithms         ALGORITHM           ::=  { ... }

Validity                    ::=     SEQUENCE {
    notBefore       Time,
    notAfter        Time }

SubjectPublicKeyInfo                ::=     SEQUENCE {
    algorithm               AlgorithmIdentifier,
    subjectPublicKey        BIT STRING }

Time ::= CHOICE {
    utcTime             UTCTime,
    generalizedTime     GeneralizedTime }

Extensions ::= SEQUENCE OF Extension

Extension ::=   SEQUENCE {
    extnId      EXTENSION.&id ({ExtensionSet}),
    critical    BOOLEAN DEFAULT FALSE,
    extnValue   OCTET STRING
                -- contains a DER encoding of a value of type &ExtnType
                -- for the extension object identified by extnId -- }
                                -- يحتوي على تشفير DER (قواعد التشفير المميزة) لقيمة من النمط &ExtnType
                                -- من أجل موضوع التوسع المعرّف بـ extnId -- {

ExtensionSet    EXTENSION       ::=     { ... }
```

قبل استخدام قيمة للنمط **توقيت (Time)** في كل عملية مقارنة، كجزء من قاعدة المواءمة أثناء البحث، وإذا كان النحو المختار للنمط **توقيت (Time)** هو نفس نحو النمط **التوقيت العالمي المنسّق (UTCTime)**، يجب تقييس قيمة حقل "السنة" ذات الرقمين بالطريقة التالية حيث تصبح قيمة السنة ذات أربعة أرقام:

- يضاف 2000 إذا كانت قيمة الرقمين محصورة بين 00 و49 (الطرفان ضمناً).
- يضاف 1900 إذا كانت قيمة الرقمين محصورة بين 50 و99 (الطرفان ضمناً).

ملاحظة 2 – إن استخدام النمط **التوقيت المعمّم (Generalized Time)** قد يعوق التشغيل البيني مع تطبيقات لا علم لها بإمكانية الاختيار بين **التوقيت العالمي المنسّق** و**التوقيت المعمّم**. ويقع على مسؤولية الأشخاص الذين يحددون الميادين التي ستستخدم فيها الشهادات المحددة في مواصفة الدليل هذه، أي الجماعات التي تعرّف الجانبيات، أن يعينوا متى يستخدم النمط **التوقيت المعمّم**. ولن يستخدم أبداً **التوقيت العالمي المنسّق** لتمثيل التواريخ، بعد عام 2049.

المكونة **الصيغة (version)** هي صيغة الشهادة المشفّرة. وإذا كانت المكوّنة **التوسعات** (extensions) موجودة في الشهادة، تكون صيغة الشهادة هي v3. أما إذا كانت المكوّنة **معرّف الهوية الوحيد للمُصْدر** (issuerUniqueIdentifier) هي الموجودة، فتكون الصيغة هي v2 أو v3.

المكونة **رقم التسلسل (serialNumber)** هي عدد صحيح مستند من سلطة إصدار الشهادة إلى كل شهادة. وعليه تكون قيمة رقم التسلسل وحيدة لكل شهادة صادرة عن سلطة معنية لإصدار الشهادة. (أي أن اسم المُصدر ورقم التسلسل يعرفان هوية شهادة وحيدة).

المكونة **التوقيع (signature)** تحتوي على معرف هوية الخوارزمية للخوارزمية وعلى دالّة الفرم اللتين تستعملهما سلطة إصدار الشهادة لتوقيع الشهادة (مثل md5WithRSAEncryption وsha-1WithRSAEncryption وid-dsa-with-sha1 وغيرها).

المكونة **المُصْدر (issuer)** تدل على الكيان الذي وقّع الشهادة وأصدرها.

المكونة **الصلاحية (validity)** هي الفاصل الزمني الذي تضمن فيه سلطة إصدار الشهادة أنها ستحتفظ بالمعلومات الخاصة بوضع الشهادة القانوني.

المكونة **الصاحب (subject)** تدل على الكيان المرتبط بالمفتاح العمومي الموجود في حقل "المفتاح العمومي للصاحب".

المكونة **معلومات المفتاح العمومي للصاحب (subjectPublicKeyInfo)** تستعمل لنقل المفتاح العمومي الجاري تصديقه، وللتعريف بالخوارزمية التي يشكل هذا المفتاح العمومي مطابقاً لها (مثل rsaEncryption وdhpublicnumber وid-dsa وغيرها).

المكونة **معرف الهوية الوحيد للمُصْدر (issuerUniqueIdentifier)** تستعمل للتعريف دون لبس بمُصدر، في حالة إعادة استخدام اسم.

المكونة **معرف الهوية الوحيد للصاحب (subjectUniqueIdentifier)** تستعمل للتعريف دون لبس بصاحب، في حالة إعادة استخدام اسم.

ملاحظة 3 – في الحالات التي ينبغي فيها لسلطة التسمية أن تسند من جديد اسماً مميزاً إلى مستعمل آخر، تستطيع سلطات إصدار الشهادة أن تستخدم معرف الهوية الوحيد من أجل التمييز بين مطابقات يعاد استعمالها. ومع ذلك إذا تلقى المستعمل نفسه شهادات صادرة من عدة سلطات لإصدار الشهادة، يوصى بأن تنسّق هذه السلطات فيما بينها لإسناد معرف هوية وحيد كجزء من إجراءاتها لتسجيل المستعمل.

الحقل **توسّعات (extensions)** يتيح إضافة حقول جديدة إلى البنية من دون إجراء أي تعديل في تعريف الترميز ASN.1. ويتكون حقل التوسع من معرف هوية التوسع، ومن راية الحرجية، ومن تشفير قيمة معطيات من نمط الترميز ASN.1 المصاحب للتوسع المعني. وعندما تكون رتبة التوسعات الافرادية داخل عبارة **التتابع (SEQUENCE)** ذات مغزى دلالي، فإن مواصفة هذه التوسعات الإفرادية سوف تحتوي على قواعد الدلالة على الرتبة المستعملة. وإذا لم يعترف تنفيذ ما بتوسع ما أثناء معالجته لشهادة، وكانت راية الحرجية موضوعة على "خاطئة"، يستطيع التنفيذ عندئذ تجاهل هذا التوسع. أما إذا كانت راية الحرجية موضوعة بالعكس على **"صائبة"**، فإن التوسعات غير المعترف بها ستتسبب في اعتبار البنية غير صالحة، وهذا يعني أن توسعاً حرجاً غير معترف به في شهادة، يؤدي إلى إفشال صلاحية التوقيع الذي يستعمل هذه الشهادة. وعندما يقوم تنفيذ يستعمل شهادات بالاعتراف بتوسّع وبكونه قادراً على معالجته، يجب عليه أن يعالج هذا التوسع مهما تكن قيمة راية الحرجية. وتجدر الملاحظة بأن كل توسع موسوم بأنه غير حرج يستدعي نوعين من السلوك متناقضين بين أنظمة استعمال الشهادات، فمن هذه الأنظمة ما يعالج التوسع، ومنها ما لا يعترف بالتوسع ويتجاهله.

وإذا وردت عناصر مجهولة في توسع ليس موسوماً بأنه حرج، يجب تجاهل هذه العناصر المجهولة طبقاً لقواعد قابلية التوسع الموثّقة في الفقرة 2.2.12 من التوصية ITU-T X.519 | في المعيار الدولي ISO/IEC 9594-5.

ويكون أمام سلطة إصدار الشهادة ثلاثة خيارات حيال توسع ما:

i) يمكنها إلغاء التوسع من الشهادة؛

ii) يمكن إدراج التوسع في الشهادة ووسمه بأنه غير حرج؛

iii) يمكنها إدراج التوسع في الشهادة ووسمه بأنه حرج.

وتستطيع آلية إقرار الصلاحية اتخاذ واحد من إجراءين حيال توسع ما:

i) يمكنها تجاهل التوسع وقبول الشهادة (مع بقاء الحالة كما هي من كل الوجوه الأخرى)؛

ii) يمكنها معالجة التوسع، وقبول أو رفض الشهادة حسب محتوى التوسع وحسب ظروف إجراء المعالجة (مع مراعاة القيم التي تأخذها متحولات معالجة المسيرة مثلاً).

لا يمكن لبعض التوسعات إلا أن توسم بأنها حرجة فقط. وفي هذه الحالات، فإن آلة إقرار الصلاحية التي تفهم التوسع تقوم بمعالجته، ويتوقف قبول الشهادة أو رفضها (ولو جزئياً) على محتوى التوسع. أما آلة إقرار الصلاحية التي لا تفهم التوسع فترفض الشهادة.

ولا يمكن لبعض التوسعات الأخرى إلا أن توسم بأنها غير حرجة فقط. وفي هذه الحالات، فإن آلة إقرار الصلاحية التي تفهم التوسع تقوم بمعالجته، ويتوقف قبول الشهادة أو رفضها (ولو جزئياً) على محتوى التوسع. أما آلة إقرار الصلاحية التي لا تفهم التوسع فتقبل الشهادة (ما لم تكن هناك عوامل أخرى غير التوسع المعتبر تؤدي إلى رفضها).

ويمكن لبعض التوسعات أن توسم بأنها حرجة أو غير حرجة. وفي هذه الحالات، فإن آلة إقرار الصلاحية التي تفهم التوسع تقوم بمعالجته، ويتوقف قبول الشهادة أو رفضها (ولو جزئياً) على محتوى التوسع، بصرف النظر عن راية الحرجية. أما آلة إقرار الصلاحية التي لا تفهم التوسع، فتقبل الشهادة إن كان التوسع موسوماً بأنه غير حرج (ما لم تكن هناك عوامل أخرى غير التوسع المعتبر تؤدي إلى رفضها)، ولكنها ترفض الشهادة إن كان التوسع موسوماً بأنه حرج.

عندما تزمع سلطة إصدار الشهادة إدماج توسع في شهادة، فهي تفعل ذلك معتقدة بأن إدماج هذا التوسع سوف يتم تقبله على نطاق واسع. وإذا وجدت سلطة إصدار الشهادة أن من اللازم تفحص محتوى التوسع قبل اعتماد أي شيء بشأن استعمال الشهادة، فإنها تسم التوسع بأنه حرج. وتفعل ذلك وهي مدركة أن أي آلة لإقرار الصلاحية لا تعالج التوسع سوف ترفض الشهادة (ربما عن طريق الحدّ من مجموعة التطبيقات التي تساعد على التحقق من الشهادة). وقد تسم سلطة إصدار الشهادة بعض التوسعات بأنها غير حرجة، لكي تؤمن المواءمة الخلفية مع بعض تطبيقات إقرار الصلاحية التي لا تستطيع معالجة التوسعات. وعندما يظهر أن الحاجة إلى المواءمة الخلفية وقابلية التشغيل البيني مع تطبيقات إقرار الصلاحية غير القادرة على معالجة التوسعات، هي أكثر أهمية حيوية من مقدرة سلطة إصدار الشهادة على تنفيذ التوسعات، عندئذ توسم هذه التوسعات، هي أكثر أهمية حيوية من مقدرة سلطة إصدار الشهادة على تنفيذ التوسعات، عندئذ توسم هذه التوسعات، التي وسمت اختيارياً بأنها حرجة، أنها غير حرجة. ومن المحتمل جداً أن تقوم سلطات إصدار الشهادة بوسم التوسعات الموسومة اختيارياً بأنها حرجة، على أنها غير حرجة خلال فترة انتقالية يجري فيها تحسين تطبيقات معالجة شهادات المتحققين، حتى تصبح تطبيقاتٍ قادرةً على معالجة التوسعات.

ويمكن تحديد توسعات خاصة في توصيات القطاع ITU-T | في المعايير الدولية أو عن طريق أي منظمة تشعر بالحاجة إليها. ويجب أن يتحدد معرف هوية الموضوع لتوسع ما وفقاً للتوصية ITU-T X.660 | ISO/IEC 9834-1. أما التوسعات المعيارية للشهادات فهي محددة في البند 8 من مواصفة الدليل هذه.

يستعمل صنف الموضوعات التالي لتحديد التوسعات الخاصة.

```
EXTENSION ::= CLASS {
    &id     OBJECT IDENTIFIER UNIQUE,
    &ExtnType }
WITH SYNTAX {
    SYNTAX              &ExtnType
    IDENTIFIED BY       &id }
```

وهناك نمطان أوليان من شهادات المفتاح العمومي: شهادات الكيان النهائي وشهادات سلطة إصدار الشهادة.

أما شهادة الكيان النهائي فهي شهادة تصدرها سلطة إصدار الشهادة لصاحب لا يصدر هو نفسه شهادات مفتاح عمومي أخرى.

وأما شهادة سلطة إصدار الشهادة (CA) فهي شهادة تصدرها سلطة CA لصاحب هو نفسه سلطة إصدار الشهادة (CA)، ولذلك فهو قادر على إصدار شهادات مفتاح عمومي. ويمكن تصنيف نفس شهادات سلطة إصدار الشهادة في فئات من الأنماط التالية:

- *شهادة صادرة لذاتها* – شهادة يكون فيها مُصْدر الشهادة وصاحبها هما نفس سلطة إصدار الشهادة (CA). وتستطيع سلطة إصدار الشهادة استعمال شهادة صادرة لأمرها أثناء عملية تجديد مفتاح مثلاً، من أجل نقل الثقة من المفتاح القديم إلى المفتاح الجديد.
- *شهادة موقعة من ذاتها* – حالة خاصة من الشهادات الصادرة لذاتها، حيث يكون فيها المفتاح الخاص الذي تستعمله سلطة إصدار الشهادة لتوقيع الشهادة مقابلاً للمفتاح العمومي المصدّق عليه داخل الشهادة. وتستطيع سلطة إصدار الشهادة استعمال شهادة موقعة من ذاتها لكي تعلن مثلاً عن مفتاحها العمومي أو عن غيره من المعلومات الخاصة بتشغيلها.
- *شهادة متقاطعة* – شهادة يكون فيها مُصْدر الشهادة وصاحبها سلطتي إصدار CA مختلفتين. وتصدر سلطات الإصدار CA شهادات إلى غيرها من سلطات الإصدار CA، إما باعتبارها آلية ترخيص بوجود سلطة الإصدار الصاحبة (وذلك داخل تراتب صارم)، وإما باعتبارها آلية اعتراف بوجود سلطة الإصدار الصاحبة (كما في نموذج الثقة الموزع). وتستخدم بنية الشهادة المتقاطعة في كلتا الحالتين. وفي بعض الحالات التي تحصل فيها متطلبات متناقضة أو متراكبة في موضوع التقييدات، كما في حالة تقييدات الأسماء، قد تضطر إحدى سلطات إصدار الشهادة (CA) إلى إصدار أكثر من شهادة متقاطعة لسلطة إصدار CA أخرى.

ومدخل كل مستعمل A في الدليل، مساهم في استيقان معمق، يحتوي على شهادة (شهادات) للمستعمل A. ومثل هذه الشهادة تولدها سلطة إصدار الشهادة للمستعمل A التي هي كيان في شجرة معلومات الدليل (DIT). ويرمز إلى سلطة إصدار الشهادة للمستعمل A، التي قد لا تكون وحيدة، بالرمز CA(A) أو فقط بالرمز CA، إن كان المستعمل A معروفاً ضمناً. وهكذا يستطيع أي مستعمل أن يكتشف المفتاح العمومي للمستعمل A، إن كان يعرف المفتاح العمومي للسلطة CA. وهكذا يكون اكتشاف المفاتيح العمومية تكرارياً.

وعندما يسعى مستعمل A إلى الحصول على المفتاح العمومي لمستعمل B، ويحصل على المفتاح العمومي للسلطة CA(B)، تكون العملية قد اكتملت. ومدخل كل سلطة إصدار X في الدليل يحتوي على عدد من الشهادات هي التي تتيح للمستعمل A الحصول على المفتاح العمومي للسلطة CA(B). وتكون هذه الشهادات على نمطين أولهما شهادات ذاهبة من السلطة X ولّدتها سلطات إصدار أخرى، والثاني شهادات عائدة إلى X ولدتها X نفسها، وهي المفاتيح العمومية المصدّقة التي تخص سلطات أخرى لإصدار الشهادة. ووجود هذه الشهادات يمكّن المستعملين من إنشاء مسيرات لإصدار الشهادات من نقطة إلى أخرى.

وقائمة الشهادات التي تتيح لمستعمل معين أن يحصل على المفتاح العمومي لمستعمل آخر تدعى *مسيرة إصدار الشهادة*. كل بند في هذه القائمة هو شهادة صادرة عن سلطة إصدار الشهادة للبند التالي في القائمة. ومسيرة إصدار الشهادة للبند التالي في القائمة. ومسيرة إصدار الشهادة من A إلى B والتي يرمز إليها بالرمز A→B:

- تبدأ بشهادة صادرة عن السلطة CA(A)، هي <<X1>>CA(A) لكيان ما X1؛
- تتبعها شهادات أخرى <<Xi+1>>Xi؛
- وتنتهي بشهادة المستعمل B.

ويستعمل حقلا **المُصْدر (issuer)** و**الصاحب (subject)** في كل شهادة ولو جزئياً للتعريف بمسيرة صالحة. وفي كل زوج من الشهادات المتجاورة من مسيرة صالحة لإصدار الشهادات، تكون قيمة حقل **الصاحب** في إحدى الشهادتين مقابلة بالضرورة لقيمة حقل **المُصدر** في الشهادة اللاحقة. وفوق ذلك فإن قيمة حقل **المُصدر** في الشهادة الأولى، يجب أن تطابق الاسم المميز (DN) في مرسخة الثقة. ولا تستخدم إلا الأسماء الموجودة في هذا الحقول عند التحقق من صلاحية مسيرة إصدار الشهادات. ولا تستخدم الأسماء الموجودة في توسعات الشهادات لهذا الغرض. وتشكل مسيرة إصدار الشهادة منطقياً سلسلة غير منقطعة من النقاط الموثوقة في شجرة معلومات الدليل بين مستعملين اثنين راغبين في الاستيقان. ويمكن أن تختلف الطريقة التي يستعملها بالضبط، مستعملان A وB للحصول على مسيرتي إصدار الشهادة من A إلى B ومن B إلى A. ومن السبل التي تسهل ذلك إقامة تراتب بين سلطات إصدار الشهادة، قد ينطبق أو لا ينطبق على تراتب الشجرة DIT كلياً أو جزئياً. ومن

فوائد هذا أن المستعملين الذين تكون سلطات إصدار شهاداتهم واقعة في التراتب، يمكنهم إقامة مسيرة إصدار الشهادة فيما بينهم باستخدام الدليل ودون أي معلومات مسبقة. ولكي تتمكن كل سلطة إصدار الشهادة من القيام بذلك، فإنها تستطيع اختزان شهادة ذاهبة وشهادة عائدة مسمّاة لكي تقابل سلطة إصدار شهادتها العلوية. وينبغي استعمال قاعدة التقابل **مواءمة الأسماء المميزة (distinguishedNameMatch)**، المعرفة في الفقرة 2.5.13 من التوصية ITU-T X.501 | ISO/IEC 9594-2، لمقارنة الاسم المميز (DN) الوارد في حقل **المُصْدر** من شهادة ما بالاسم المميز الوارد في حقل **الصاحب** من شهادة أخرى.

يستطيع المستعمل أن يحصل على شهادة واحدة أو أكثر من واحدة من سلطة واحدة لإصدار الشهادة أو من أكثر من سلطة. وتحمل كل شهادة اسم سلطة إصدار الشهادة التي أصدرتها. ويمكن استخدام أنماط معطيات الترميز ASN.1 التالية لتمثيل الشهادات ومسيرة إصدار الشهادة.

```
Certificates                ::=  SEQUENCE {
   userCertificate          Certificate,
   certificationPath        CertPath OPTIONAL }

CertificationPath           ::=  SEQUENCE {
   userCertificate          Certificate,
   theCACertificates        SEQUENCE OF CertificatePair OPTIONAL }
```

وعلاوة على ذلك يمكن استخدام نمط معطيات الترميز ASN.1 التالي لتمثيل مسيرات إصدار الشهادة الذاهبة. وتحتوي هذه المكوّنة على مسيرة إصدار الشهادة التي يمكن تسديدها نحو الخف إلى المُصْدر الأصلي.

```
CertPath  ::=  SEQUENCE OF CrossCertificates

CrossCertificates          ::=        SET OF Certificate

PkiPath  ::=  SEQUENCE OF Certificate
```

وفيها **مسيرة البنية التحتية للمفتاح العمومي (PkiPath)** تمثل مسيرة إصدار الشهادة. ويكون ترتيب الشهادات في التتابع بحيث يكون صاحب الشهادة الأولى هو مُصْدر الشهادة الثانية، وهكذا.

ويجب أن تكون كل شهادة في مسيرة إصدار الشهادة وحيدة. ولا يمكن أن تظهر أي شهادة أكثر من مرة واحدة في قيمة للمكوّنة **شهادات السلطة CA (the CACertificat)** من **مسيرة إصدار الشهادة (CertificationPath)**، أو في قيمة **شهادة (Certificate)** في المكوّنة **شهادات متقاطعة (CrossCertificates)** من مسيرة إصدار الشهادات **(CertPath)**، أو في قيمة **شهادة (Certificate)** في المسيرة **(PkiPath)**.

1.7 توليد أزواج المفاتيح

إن سياسة إدارة الأمن العام في أحد التطبيقات هي التي تحدد دورة الحياة لزوج المفاتيح، وبذلك فهي تقع خارج نطاق تطبيق هذا الإطار. ومع ذلك فإن من الأمور التي تكتسي أهمية حيوية بالنسبة إلى الأمن العام، أن تبقى جميع المفاتيح الخاصة معروفة فقط لدى المستعملين الذين يمتلكونها.

ليس سهلاً على الإنسان المستعمل أن يتذكر معطيات المفتاح، لذلك يجب استخدام طريقة مناسبة لتخزينها في وسيلة يمكن حملها وتنقيلها. وقد تكون إحدى هذه الوسائل الممكنة هي استعمال "بطاقة ذكية"، فهي تستطيع حمل مفتاحي المستعمل: الخاص واختيارياً العمومي، وشهادة المستعمل، ونسخة من المفتاح العمومي لسلطة إصدار الشهادة. ويمكن زيادة أمن استعمال هذه البطاقة عن طريق رقم تعريف الهوية الشخصية (PIN)، مما يزيد في أمن النظام عن طريق مطالبة المستعمل أن يمتلك البطاقة وأن يعرف كيف ينفذ إليها. غير أن الطريقة المضبوطة التي يجب اختيارها لتخزين مثل هذه المعطيات تقع خارج نطاق مواصفة الدليل هذه.

هناك ثلاثة سبل لإنتاج زوج المفاتيح للمستعمل، هي:

أ) المستعمل هو الذي يولد زوج مفاتيحه. وميزة هذه الطريقة أن المفتاح الخاص للمستعمل لا يترك أبداً عند كيان آخر، ولكنها تتطلب سوية معينة من كفاءة المستعمل.

ب) يولد طرف ثالث زوج المفاتيح. ويسلّم هذا الطرف الثالث المفتاح الخاص إلى المستعمل بطريقة آمنة مادياً، ثم يتلف إتلافاً فعّالاً جميع المعلومات المتعلقة بإنشاء زوج المفاتيح ويتلف كذلك المفتاحين ذاتيهما. وتتخذ تدابير مادية مناسبة للتأكد من أنه لا يمكن التأثير على الطرف الثالث ولا التلاعب بالعمليات التي أجريت على المعطيات.

ج) تولد سلطة إصدار الشهادة زوج المفاتيح، وهذه هي حالة خاصة من السبيل ب) وتنطبق عليها اعتبارات ذلك الوضع.

ملاحظة – تقدم سلطة إصدار الشهادة بالفعل وظائفيات موثوقة تجاه المستعمل، وتخضع للتدابير الأمنية المادية اللازمة. وميزة هذه الطريقة أنها لا تحتاج إلى نقل المعطيات بطريقة مأمونة إلى سلطة إصدار الشهادة للتصديق عليها.

ويفرض نظام التجفير المستعمل تقييدات (تقنية) خاصة على توليد المفاتيح.

2.7 إحداث شهادة المفتاح العمومي

تجمع شهادة المفتاح العمومي بين المفتاح العمومي واسم مميز وحيد للمستعمل المعني. وعليه:

أ) يجب أن تستوثق سلطة إصدار الشهادة من هوية المستعمل، قبل أن تحدث له شهادة.

ب) يجب ألا تصدر سلطة إصدار الشهادة شهادتين لمستعملين يحملان نفس الاسم.

ومن المهم ألا تتعرض المعلومات إلى أي خطر أثناء نقلها إلى سلطة إصدار الشهادة، ويجب اتخاذ التدابير الأمنية المادية المناسبة لحمايتها. وعليه:

أ) سيكون هناك خرق جسيم للأمن، إذا أصدرت سلطة الإصدار شهادة لمستعمل كان قد جرى تلاعب بمفتاحها العمومي.

ب) عند استعمال أسلوبي الفقرتين 1.7 ب) أو 1.7 ج) في توليد أزواج المفاتيح، يجب أن ينقل المفتاح الخاص للمستعمل بطريقة مأمونة إلى المستعمل.

ج) عند استعمال أسلوبي الفقرتين 1.7 ب) أو 1.7 ج) في توليد أزواج المفاتيح، يمكن للمستعمل أن يستخدم طرائق مختلفة (على الخط أو خارج الخط) لإيصال مفتاحه العمومي إلى سلطة إصدار الشهادة بطريقة مأمونة. وقد توفر الطرائق المباشرة (على الخط) بعض المرونة الإضافية للعمليات التي تؤدي عن بُعْد بين المستعمل وسلطة الإصدار.

إن شهادة المفتاح العمومي هي مجموعة من المعلومات متيسرة للعموم ولا تحتاج إلى أي تدبير خاص لحمايتها أثناء نقلها إلى الدليل. ولما كانت سلطة إصدار الشهادة تحدث الشهادة في وقت آجل نيابة عن مستعمل سوف يعطى نسخة عنها، فإن المستعمل لا يحتاج إلا إلى تخزين هذه المعلومات في مدخله في الدليل، عند نفاذه إليه في وقت لاحق. وفي حل بديل، تستطيع سلطة إصدار الشهادة إيداع الشهادة لدى وكيل للمستعمل، وفي هذه الحالة، يعطى هذا الوكيل حقوق النفاذ اللازمة.

3.7 صلاحية الشهادات

السلطات التي تصدر شهادات المفتاح العمومي أو شهادات النعت مسؤولة عن تبيان صلاحية الشهادات التي تصدرها. وتخضع الشهادات عامة إلى احتمال إبطالها لاحقاً. ويمكن أن يتم هذا الإبطال والتبليغ عن الإبطال إما مباشرة من نفس السلطة التي أصدرت الشهادة، وإما بطريقة غير مباشرة عن طريق سلطة أخرى توكّلها حسب الأصول نفس السلطة التي أصدرت الشهادة. ويطلب من السلطة التي تصدر الشهادة أن تبين عبر إعلان عام، هو واحد من ممارساتها، تورده في الشهادة ذاتها إن أمكن، أو عبر وسائل أخرى محددة، ما إذا:

– كان لا يمكن إبطال الشهادة؛ أو

- كان يمكن إبطال الشهادة عن طريق نفس سلطة إصدارها مباشرة؛ أو
- كانت سلطة إصدار الشهادة قد وكّلت كياناً آخر للقيام بالإبطال.

يتعين على السلطات التي تبطل الشهادات أن تعلن عبر وسائل مماثلة عن الآلية (الآليات) التي يمكن أن تستعملها الأطراف الواثقة، للحصول على معلومات الوضع القانوني للإبطال المتعلقة بالشهادات الصادرة عن هذه السلطات. وتحدد هذه المواصفة آلية لقائمة إبطال الشهادات (CRL)، ولكنها لا تمنع من استعمال غيرها. وبروتوكول الوضع القانوني للشهادة، على الخط (OCSP) المحدد في المعيار IETF RFC 2560[1] هو مثال من هذه الآلية البديلة، التي تسمح لطرف واثق (زبون) أن يطلب الوضع القانوني لإبطال شهادة صادرة عن مخدّم OCSP. وقد يتحقق المخدّم من الوضع القانوني للشهادة بعد مراجعة قوائم الإبطال CRL، أو باللجوء إلى وسائل أخرى، ويجيب الزبون وفقاً لذلك. إذا كان البروتوكول OCSP يتيح للأطراف الواثقة التحقق من الوضع القانوني لشهادة ما، عندئذ يحدد المعيار IETF RFC 3280[2] توسعاً في الشهادة (**نفاذ إلى معلومات السلطة Authority Info Access**) ينبغي أن يكون مدرجاً في مثل هذه الشهادة ويوفر معلومات كافية للوصول إلى مخدّم OCSP المناسب. وتقوم الأطراف الواثقة بالتحقق من معلومات الوضع القانوني للإبطال، كما ينبغي، بشأن جميع الشهادات، حتى تستطيع إقرار صلاحية إحدى الشهادات بتطبيق إجراءات معالجة المسيرة الموصوفة في البند 10 وإجراء مسيرة التفويض الموصوفة في البند 16.

ولا يجوز إلا لسلطة إصدار الشهادة المرخص لها بإصدار قوائم الإبطال CRL، أن تختار تفويض هذا الترخيص إلى كيان آخر. وإذا جرى التفويض، فيجب التحقق منه عند التحقق من الشهادة أو من قائمة إبطال الشهادات، ويجوز استخدام التوسع **نقاط توزيع قوائم الإبطال (cRLDistributionPoints)** لهذا الغرض. ويملأ حقل **مُصدر قوائم الإبطال (cRLIssuer)** في هذا التوسع بأسماء كل الكيانات، التي هي غير اسم مُصدر الشهادة نفسه، الذي كان مرخصاً له أن يصدر قوائم الإبطال CRL المعنية بالوضع القانوني لإبطال الشهادة المدروسة.

وجميع الشهادات، سواء شهادات المفتاح العمومي أو شهادات النعت، يجب أن يكون لها مدة عمر نافع تصاحب كلاً منها، تنتهي صلاحيتها بانتهاء هذه المدة. وفي سبيل تأمين استمرار الخدمة، يجب على السلطة أن تؤمن تيسر شهادات بديلة في الوقت المناسب، لكي تحل محل الشهادات المنتهية صلاحيتها أو التي هي في الطريق إلى الانتهاء. وتاريخ التبليغ عن إبطال هو تاريخ وساعة أول ظهور لتبليغ الإبطال عن الشهادة، في قائمة الإبطال، سواء كانت قائمة إبطال أساسية أو قائمة إبطال دلتا (dCRL). ويرد تاريخ التبليغ عن الإبطال في حقل **هذا التحيين (thisUpdate)** من القائمة CRL. ويكون تاريخ الإبطال هو تاريخ وساعة الإبطال الفعلي للشهادة الذي تحدده سلطة إصدار الشهادة، وقد يكون مختلفاً عن تاريخ أول ظهور للتبليغ في قائمة CRL. ويكون تاريخ الإبطال في القائمة CRL هو القيمة الواردة في مكوّنة **تاريخ الإبطال (revocationDate)**. ويكون تاريخ عدم الصلاحية هو تاريخ ووقت تعرّض المفتاح الخاص للخطر، المعروف أو المتوقع، أو هو التاريخ الذي ينبغي أن تعتبر فيه الشهادة غير صالحة. وقد يكون هذا التاريخ أبكر من تاريخ الإبطال. ويكون تاريخ عدم الصلاحية في القائمة CRL هو القيمة الواردة في توسع المدخل **تاريخ عدم الصلاحية (invalidityDate)**.

والنقطتان التاليتان ترتبطان بمدة عمر الشهادات النافع:

- يمكن أن تكون صلاحية الشهادات محددة بحيث تصبح كل واحدة منها صالحة في نفس الوقت الذي تنتهي فيه صلاحية سابقتها، أو يمكن أن يسمح بالتشابك. والطريقة الثانية الأخيرة تحمي السلطة من أن تقيم وتوزع عدداً كبيراً من الشهادات التي قد تصبح غير شغّالة في تاريخ انتهاء مشترك.
- الشهادات المنتهية صلاحيتها تزال عادة من الدليل. ويكون على السلطة أن تحمل العبء الأمني ومسؤولية الاحتفاظ بالشهادات القديمة لفترة زمنية معينة، في حالة توفر خدمة عدم رفض المعطيات.

---

[1] IETF RFC 2560، *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)*، (يونيو 1999).

[2] IETF RFC 3280، *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*، (أبريل 2002).

يمكن إبطال الشهادات قبل تاريخ انتهاء صلاحيتها، مثل الحالة التي يفترض فيها أن المفتاح الخاص للمستعمل كان قد تعرض للخطر، أو عندما لا تعود السلطة تثق بالمستعمل، أو عندما يفترض أن شهادة السلطة معرضة للخطر. ويجب على السلطة أن تعمل على الإخبار عن إبطال شهادة مستعمل أو شهادة سلطة، وأن تعمل على تيسر شهادة جديدة، عند اللزوم. ويمكن للسلطة أن تعلم حامل الشهادة إن إبطالها بعد ذلك باستخدامها إجراءً مؤجلاً خارج الخط.

كل سلطة تصدر الشهادات ثم تبطلها لاحقاً:

أ) ربما يطلب منها أن تحتفظ بتسجيل للتدقيق في أحداث الإبطال التي قامت بها لجميع أنماط الشهادات التي أصدرتها هذه السلطة (مثل شهادات المفتاح العمومي وشهادات النعت الصادرة لكيانات نهائية أو الصادرة لسلطات أخرى)؛

ب) يتعين عليها أن تقدم معلومات الوضع القانوني للإبطال إلى الأطراف الواثقة التي تستخدم القوائم CRL، أو بروتوكول الوضع القانوني للشهادات على الخط، أو أي وسيلة أخرى لنشر معلومات الوضع القانوني للإبطال؛

ج) تحتفظ وتنشر القوائم CRL التي ربما تستخدمها، حتى وإن كانت القوائم فارغة؛

د) يتعين عليها أن تصدر قائمة كاملة بالقوائم CRL المجزأة، إن كانت لا تستخدم إلا قوائم CRL مجزأة، تغطي المجموعة الكاملة من الشهادات التي يشار إلى وضع إبطالها القانوني عن طريق آلية القوائم CRL. وهكذا تكون المجموعة الكاملة من القوائم CRL المجزأة مكافئة لقائمة CRL كاملة لنفس المجموعة من الشهادات، إن كان مُصْدر القوائم CRL لا يستخدم القوائم CRL المجزأة.

تستطيع الأطراف الواثقة أن تستخدم عدداً من السبل لتحديد موقع معلومات الوضع القانوني للإبطال التي تقدمها سلطة ما، فقد تستخدم مثلاً مؤشراً موجوداً في الشهادة نفسها يدل الطرف الواثق على الموضع الذي توجد فيه معلومات الإبطال، وقد يكون هناك مؤشر في قائمة الإبطال يحيل الطرف الواثق نحو موضع آخر. ويستطيع الطرف الواثق أن يحدد موقع معلومات الإبطال في مجمّع مرجعي (مثل الدليل) أو عبر وسائل أخرى لا تدخل في نطاق هذه المواصفة (بصورة محلية مثلاً).

ويقع الاحتفاظ بمداخل الدليل المتأخرة بقوائم الإبطال الصادرة عن السلطة، على مسؤولية الدليل ومستعمليه، الذين يجب أن يعملوا في إطار السياسة الأمنية. فيمكن للمستعمل مثلاً أن يعدّل مدخل موضوعه عن طريق الاستعاضة عن شهادته القديمة بشهادة جديدة. وعندها تستخدم هذه الشهادة الأخيرة لاستيقان هذا المستعمل حيال الدليل.

وعندما تنشر قوائم الإبطال في الدليل، فإنها ترد في المداخل بشكل نعوت للأنماط التالية:

- قائمة إبطال الشهادات؛
- قائمة إبطال السلطات؛
- قائمة الإبطال دلتا؛
- قائمة إبطال شهادات النعت؛
- قائمة إبطال سلطات النعت.

```
CertificateList          ::=    SIGNED { SEQUENCE {
    version                     Version OPTIONAL,
                                -- if present, version shall be v2
                                -- (إن وجدت، تكون الصغية هي v2)
    signature                   AlgorithmIdentifier,
    issuer                      Name,
    thisUpdate                  Time,
    nextUpdate                  Time OPTIONAL,
    revokedCertificates         SEQUENCE OF SEQUENCE {
        serialNumber                CertificateSerialNumber,
        revocationDate              Time,
        crlEntryExtensions      Extensions OPTIONAL } OPTIONAL,
    crlExtensions      [0]      Extensions OPTIONAL }}
```

المكوّنة **الصيغة (version)** تمثل صيغة قائمة الإبطال المشفرة. وإذا كانت مكوّنة **التوسّعات (extensions)** الواردة في قائمة الإبطال موسومة بأنها حرجة، تكون الصيغة هي v2. وإذا كانت لا توجد أي مكوّنة **توسّعات (extensions)** في قائمة الإبطال موسومة بأنها حرجة، تكون الصيغة هي الصيغة v2 أو تكون غائبة.

والمكوّنة **التوقيع (signature)** تحتوي على معرف هوية الخوارزمية المستخدمة من السلطة لتوقيع قائمة الإبطال.

والمكوّنة هذا **التحيين (thisUpdate)** تحتوي على تاريخ وساعة إصدار قائمة الإبطال هذه.

والمكوّنة **التحيين القادم (nextUpdate)** تدل، إن وجدت، على تاريخ وساعة إصدار قائمة الإبطال التالية. ويمكن أن تصدر قائمة الإبطال التالية قبل التاريخ المشار إليه، ولكن ليس بعد هذا التاريخ بأي حال.

والمكوّنة **الشهادات المبطَلة (revokedCertificates)** تعرّف هوية الشهادات التي تم إبطالها. وتعرف هوية الشهادات المبطلة بأرقام تسلسلها. وإذا كان لم يتم إبطال أي واحدة من الشهادات المقصودة بهذه القائمة CRL، يوصى بشدة بحذف المعلمة **الشهادات المبطلة** من القائمة CRL، بدلاً من الاحتفاظ بها مع **تتابع (SEQUENCE)** خالٍ.

المكوّنة **توسعات القائمة CRL (crlExtensions)** تحتوي، إن وجدت، على توسع واحد أو أكثر من توسع للقائمة CRL.

ملاحظة 1 – التحقق من قائمة الشهادات هو مسألة محلية. ويفترض في القائمة ألاّ تكون مرتّبة، ما لم تكن سلطة الإصدار قد حددت قواعد ترتيب خاصة، كأن تكون ضمن سياسة السلطة.

ملاحظة 2 – إذا كانت خدمة عدم رفض المعطيات تتوقف على المفاتيح التي تقدمها السلطة، ينبغي للخدمة أن تتأكد من أن جميع المفاتيح التابعة للسلطة (المبطلة أو المنتهية صلاحيتها)، وجميع قوائم الإبطال المختومة بالتاريخ قد جرى حفظها في المحفوظات، وصدّقت عليها سلطة حالية.

ملاحظة 3 – إذا كان أي توسع وارد في **قائمة الشهادات (CertificateList)** معرفاً باعتباره حرجاً، يجب أن يكون عنصر الصيغة في **قائمة الشهادات (CertificateList)** موجوداً. ويمكن أن يكون عنصر **الصيغة (version)** غائباً، إذا كان لا يوجد أي توسع حرج، مما يسمح لتطبيق ما لا يحتمل إلا أعباء الصيغة 1 من القائمة CRL أن يستمر في استخدامه هذه الأخيرة، إذا كان تفحصه لتتابع **الشهادات المبطلة (revokedCertificates)** في القائمة CRL لا يكشف عن أي توسع. أما إذا كان التطبيق يتحمل أعباء الصيغة 2 (أو أعلى) من القائمة CRL، يمكنه في غياب دلالة على الصيغة أن يتمثل معالجته، إن كان يستطيع أن يحدد في مرحلة مبكّرة من المعالجة عدم وجود توسعات حرجة في القائمة CRL.

ملاحظة 4 – إذا كان التطبيق الذي يعالج قائمة إبطال الشهادات لا يعترف بوجود توسع حرج في حقل **توسعات مدخل القائمة CRL (crlEntryExtensions)**، يفترض عندئذ على الأقل بأن الشهادة المعرفة هويتها كانت قد أبطلت، وأنها لم تعد صالحة، ويتخذ إجراءات أخرى بخصوص هذه الشهادة المبطلة، تفرضها السياسة المحلّية. وإذا كان أحد التطبيقات لا يعترف بتوسع حرج في حقل **توسّعات القائمة CRL (crlExtensions)**، يفترض عندئذ بأن الشهادة المعنية قد أبطلت ولم تعد صالحة. ومع ذلك لا يمكن في الحالة الأخيرة اعتبار الشهادات التي لم تتحدد باعتبارها مبطلة، بأنها شهادات صالحة، نظراً إلى أن القائمة قد لا تكون مكتملة. وفي هذه الحالة تفرض السياسة المحلية الإجراء الواجب اتخاذه. وفي كل الأحوال يمكن للسياسة المحلية أن تفرض إجراءات أخرى إضافة إلى الإجراءات المقررة في هذه المواصفة أو أشد منها.

ملاحظة 5 – إذا أثر توسّع في معالجة القائمة (يجب مثلاً تفحص القوائم CRL العديدة بكاملها، لتحديد الشهادات المبطلة، أو يمكن لمدخل واحد أن يمثل مدى من الشهادات)، يوسم هذا التوسع بأنه حرج في الحقل **توسّعات القائمة CRL (crlExtensions)**، أينما كان موضع التوسع في القائمة CRL. وأي توسع يُدَلّ عليه في الحقل **توسعات مدخل القائمة CRL (crlEntryExtensions)** من عنصر ما، يتم إدراجه في هذا العنصر، ولا يؤثر إلا في الشهادة أو الشهادات التي يحددها هذا العنصر.

ملاحظة 6 – يحدد البند 8 من مواصفة الدليل هذه التوسعات المقيّسة للقوائم CRL.

وإذا وردت عناصر مجهولة في التوسعات، وإذا لم يكن التوسع معتبراً حرجاً، يتم تجاهل هذه العناصر المجهولة طبقاً لقواعد قابلية التوسع المشروحة في الفقرة 2.2.12 من التوصية ITU-T X.519 | المعيار ISO/IEC 9594-5.

4.7 رفض توقيع رقمي

يمكن لأي مشترك في حدث ما أن يقرر لاحقاً رفض أي وثيقة كان هذا المشترك قد وقّعها رقمياً أثناء هذا الحدث. فمثلاً يستطيع أحدهم أن يعترض على اشتراكه في إعداد مفتاح أو على كونه مُصْدر رسالة بريد إلكتروني موقّع عليها، تماماً كما يعترض أحدهم على توقيعه وثيقةً كان في نيته التقيد بمحتواها. وقد لا يفضي الرفض إلى نتيجة. وتحدد التوصية ITU-T X.813 | المعيار ISO/IEC 10181-4 إجراءً لحل المنازعات هو التالي:

1) تقديم البراهين؛

2) نقل البراهين وتخزينها والرجوع إليها؛

3) التحقق من البراهين؛

4) حل المنازعات.

وقد تشمل البراهين المقدمة بصورة غير حصرية:

- تسجيلات تدقيق ذات صلة بالحدث وتأكيد النية؛
- شهادات مصدّقة من موثّقي العقود (الكتّاب بالعدل) للأطراف المتخاصمة؛
- إعلانات مبادئ وسياسة؛
- معلومات موقعة رقمياً تشمل تسجيلات التدقيق ومصدِّقات موثّقي العقود؛
- أختام التاريخ والوقت للمعلومات التي تحمل توقيعاً رقمياً؛
- الشهادات التي تؤيد التوقيع الرقمي؛
- معلومات الإبطال المناسبة المنشورة والمتيسرة وقت وقوع الحدث المتنازع فيه؛
- أي إبطال شهادات لاحقاً وقت وقوع الحدث، يدلّ على أن المفتاح قد تعرض لخطر قبل وقوع الحدث.

أما سلامة المعطيات المخزونة التي يمكن أن تقدم كبراهين فيمكن الحفاظ عليها بأساليب مختلفة: التحكم في النفاذ، وتخزين المفرومات عن طريق طرف ثالث موثوق، والتوقيع الرقمي. وقد يكون من اللازم العمل بشكل دوري على تشديد الحماية على المعطيات المخزونة للتغلب على التحسينات الحاسوبية و/أو على التحليل التجفيري.

ملاحظة – لا تحدد مواصفة الدليل هذه لا نمط البراهين ولا عددها ولا سوية سلامتها. ومع ذلك يتوقع أن تتناسب سوية الجهود المبذولة مع المخاطرة المتعرض لها.

وقد يتطلب التحقق من البراهين أن يعاد إقرار صلاحية التوقيعات الرقمية للمعطيات، أي الرسائل والوثائق والشهادات، والقوائم CRL وأختام التواريخ التي كانت قد استخدمت في عملية إقرار الصلاحية الأولى. وواقع أن تكون صلاحية إحدى الشهادات قد انتهت، يجب ألا يمنع استعمالها لإعادة إقرار صلاحية التوقيعات أثناء فترة صلاحية هذه الشهادة. كما يمكن استعمال شهادة جرى إبطالها، وإذا أمكن التحديد بأن الشهادة كانت صالحة وقت وقوع الحدث المتنازع فيه.

حتى لو اعتبرت جميع البراهين الرقمية الموصوفة أعلاه صالحة من الناحية التقنية، فهناك ظروف أخرى، مثل نيّة الموقّع أو تفسيره للوقائع أو أهليته القانونية، تتيح للموقّع أن ينجح في رفض توقيعه.

8 التوسعات في شهادة المفتاح العمومي وفي القائمة CRL

توسعات الشهادة المحددة في هذا البند يمكن استعمالها في شهادات المفتاح العمومي، ما لم ينص على غير ذلك. أما التوسعات التي يمكن استعمالها في شهادات النعت فهي محددة في البند 15. والتوسعات في القائمة CRL المحددة في هذا البند يمكن استعمالها في القوائم CRL والقوائم CARL وكذلك في القوائم ACRL وAARL المحددة في البند 17.

يحدد هذا البند التوسعات في الميادين التالية:

أ) *معلومات عن المفتاح والسياسة:* تمرر هذه التوسعات في الشهادة والقائمة CRL معلومات إضافية بشأن المفاتيح المبطلة، وتحتوي على معرفات هوية لصاحب المفتاح ومُصدره، وعلى مؤشرات بشأن الاستخدام المتوقع أو المقيّد للمفتاح. وكذلك على مؤشرات تخص سياسة الشهادة.

ب) *نعوت الصاحب والمُصْدر:* يمكن أن تتحمل هذه التوسعات في الشهادة والقائمة CRL أسماء بديلة بأشكال مختلفة من الأسماء لصاحب شهادة أو مُصْدر شهادة أو مُصْدر قائمة CRL. وتستطيع هذه التوسعات أن تنقل معلومات نعت إضافية عن صاحب الشهادة، لكي تساعد مستعمل الشهادة على الوثوق بأن صاحب الشهادة هو الشخص المعين أو الكيان المعيّن.

ج) *تقييدات مسيرة إصدار الشهادة:* تتيح هذه التوسعات في الشهادة مواصفة التقييدات المطلوب إدراجها في الشهادة CA، أي شهادات سلطات إصدار الشهادة الصادرة عن غيرها من سلطات إصدار الشهادة، بغية تسهيل المعالجة الأوتوماتية لمسيرات إصدار الشهادات عندما تتدخل سياسات متعددة للشهادات. وتظهر السياسات المتعددة للشهادات عندما تختلف السياسات مع اختلاف التطبيقات في بيئة معينة، أو عندما يحدث تشغيل بيني مع بيئات خارجية. وقد تقيّد التقييدات أنماط الشهادات التي تستطيع إصدارها سلطة إصدار الشهادة الصاحبة أو التي قد تظهر لاحقاً في مسيرة لإصدار الشهادات.

د) *التوسّعات في القائمة الأساسية CRL:* تتيح هذه التوسعات في القائمة الأساسية CRL لهذه القائمة أن تشتمل على مؤشرات دواعي الإبطال، وأن تعلّق شهادة تعليقاً مؤقتاً، وأن تدرج أرقام تتابع إصدار القوائم CRL، مما يسمح لمستعملي الشهادات بالكشف عن القوائم CRL القائمة في تتابع من القوائم صادرة عن مُصدر القائمة CRL.

ه) *نقاط توزيع القوائم CRL والقوائم CRL دلتا:* تتيح هذه التوسعات في الشهادة وفي قائمة CRL تجزئة المجموعة الكاملة من معلومات الإبطال الصادرة من سلطة واحدة CA، إلى قوائم CRL منفصلة، كما تتيح ضم معلومات الإبطال الصادرة عن سلطات CA متعددة، في قائمة CRL واحدة. وتتحمل هذه التوسعات استخدام قوائم CRL جزئية تدل فقط على التغييرات التي طرأت على قائمة CRL صادرة سابقاً.

وإدراج أي توسع في شهادة أو في قائمة CRL هو خيار قد تأخذ به السلطة المُصْدرة لهذه الشهادة أو هذه القائمة CRL.

ويوسم التوسع في شهادة ما أو في قائمة CRL بأنه حرج أو غير حرج. فإذا كان توسع ما موسوماً بأنه حرج، وكان نظام استعمال الشهادات لا يعترف بنمط حقل التوسع أو كان لا ينفّذ علم دلالات هذا التوسع، يكون على هذا النظام أن يعتبر التوسع غير صالح. أما إذا كان توسع ما موسوماً بأنه غير حرج، وكان نظام استعمال الشهادات لا يعترف بهذا النمط من التوسع أو لا ينفذ علم دلالاته، فيمكن لهذا النظام أن يعالج بقية الشهادة وأن يتجاهل التوسع. وإذا كان توسع ما موسوماً بأنه غير حرج، يكون على نظام استعمال الشهادات الذي لا يعترف بالتوسع، أن يعالج التوسع. وتعريفات نمط التوسع الواردة في مواصفة الدليل هذه تدل إن كان التوسع حرجاً دائماً، أو كان غير حرج دائماً، أو كانت صفته الحرجة يقررها مُصدر الشهادة القائمة CRL. والسبب الذي يدعو إلى اعتبار بعض التوسعات غير حرجة دائماً هو أن يتاح للتطبيقات التي تستعمل شهادات ولا تحتاج إلى استعمال مثل هذه التوسّعات، بأن تحذف كل دعم لها، من دون أن تضرّ بإمكانية اشتغالها البيني مع جميع سلطات إصدار الشهادة.

ملاحظة – قد يتطلب نظام استعمال الشهادات وجود بعض التوسعات غير الحرجة في شهادة ما، لكي تعتبر هذه الشهادة مقبولة. وقد تلزم بوجود مثل هذه التوسعات قواعد السياسة المحلية لمستعمل الشهادة أو قد تلزم بوجود هذه التوسعات قاعدة في سياسة سلطة إصدار الشهادة، يستدل عليها نظام استعمال الشهادات، عن طريق إدراج معرف هوية خاص بسياسة الشهادة في توسع سياسات الشهادة موسوم بأنه حرج.

ويجب ألا يوجد أكثر من مطابق واحد من كل نوع من التوسع في أي شهادة أو أي قائمة CRL أو أي مدخل قائمة CRL على التوالي في جميع توسعات الشهادات وتوسعات القوائم CRL وتوسعات مداخل القوائم CRL المعرفة في مواصفة الدليل هذه.

1.8 معالجة السياسة

1.1.8 سياسة الشهادة

يحتوي هذا الإطار على ثلاثة أنماط من الكيانات: مستعمل الشهادة وسلطة إصدار الشهادة وصاحب الشهادة (أو الكيان النهائي). ويعمل كل كيان بموجب الالتزامات نحو الكيانين الآخرين، ويتمتع بالمقابل بضمانات محدودة يقدمانها له. وتحدد سياسة الشهادة هذه الالتزامات والضمانات. وسياسة الشهادة هي وثيقة (مكتوبة بلغة واضحة عادة). ويمكن الإحالة إليها بمعرف هوية وحيد، قد يكون موجوداً في توسع سياسات الشهادة للشهادة الصادرة عن سلطة إصدار الشهادة إلى الكيان النهائي وعليها يعتمد مستعمل الشهادة. ويمكن أن تصدر الشهادة طبقاً لسياسة واحدة أو لعدة سياسات. وتقوم سلطة السياسة بتعريف السياسة وإسناد معرف الهوية. ومجموعة السياسات التي تديرها سلطة السياسة تسمى الميدان السياسي. وجميع الشهادات تصدر وفقاً لسياسة، حتى ولو كانت السياسة غير مسجلة في أي مكان، أو غير محال إليها في الشهادة. ولا تشرح مواصفة الدليل هذه أسلوب سياسة الشهادة أو محتواها.

ويمكن أن يكون مستعمل الشهادة مرتبطاً بالتزاماته الناتجة عن سياسة الشهادة بفعل استيراده مفتاحاً عمومياً للسلطة واستعماله كمرسخة ثقة، أو بفعل اعتماده على شهادة تحتوي على معرف هوية السياسة المصاحب. كما يمكن أن تكون سلطة إصدار الشهادة مرتبطة بالتزاماتها الناتجة عن السياسة بفعل إصدارها شهادة تحتوي على معرف هوية السياسة المصاحب. أما الكيان النهائي فيمكن أن يكون مرتبطاً بالتزاماته الناتجة عن السياسة بفعل طلبه وقبوله شهادة تحتوي على معرف هوية السياسة المصاحب وبفعل استعماله المفتاح الخاص المقابل. والتطبيقات التي لا تستعمل توسع سياسة الشهادة، ينبغي لها أن تؤمن الارتباط المطلوب بوسائل أخرى.

ومجرد إعلان أحد الكيانات عن التطابق مع سياسة ما، لا يستوفي بصورة عامة متطلبات الضمان لبقية الكيانات الموجودة في الإطار، فهذه الكيانات الأخيرة تحتاج إلى سبب يجعلها تقبل بأن الأطراف الأخرى تستعمل تطبيقاً موثوقاً للسياسة. ومع ذلك فقد يقبل مستعملو الشهادة، إن كان ذلك منصوصاً عليه صراحة في الشهادة، ضمانات سلطة إصدار الشهادة، بأن أطرافها النهائيين يوافقون على الارتباط بالتزاماتهم الواردة في السياسة، دون الحاجة إلى تأكيد ذلك مباشرة معهم. ويقع هذا الجانب من سياسة الشهادة خارج نطاق هذه المواصفة.

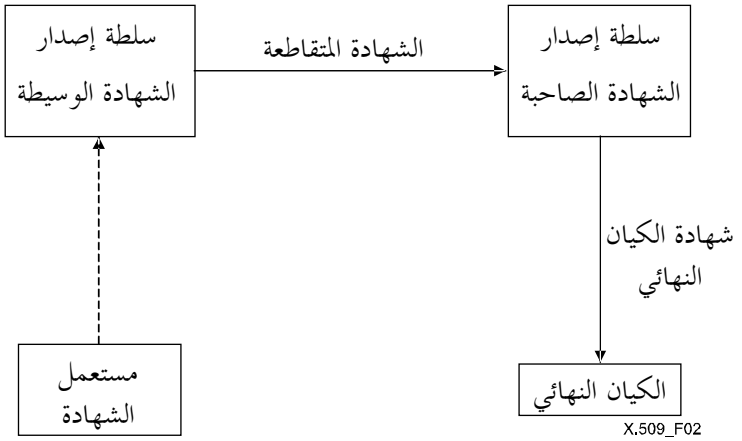
وقد تضع إحدى سلطات إصدار الشهادة حدوداً لاستعمال شهاداتها، بغية التحكم بالمخاطرة التي تتحملها نتيجة لإصدارها الشهادات. فهي مثلاً قد تحدّ من جماعة مستعملي الشهادة والأغراض التي يستعملون شهادتها لها و/أو نمط الأضرار ومداها التي هي مستعدة لتحملها في حالة فشل من ناحيتها أو من ناحية أطرافها النهائيين. يجب أن تكون هذه القضايا محددة في سياسة الشهادة.

وقد تكون معلومات إضافية موجودة في توسع سياسات الشهادة بشكل واصفات سياسة، بغية مساعدة الكيانات المتأثرة على فهم أحكام السياسة.

2.1.8 إصدار الشهادة المتقاطعة

يمكن أن تكون إحدى سلطات إصدار الشهادة صاحبة شهادة، تصدرها سلطة أخرى لإصدار الشهادة. وتدعى الشهادة في هذه الحالة شهادة متقاطعة، وتدعى سلطة إصدار الشهادة التي تكن صاحبة الشهادة بأنها سلطة الإصدار الصاحبة، كما تدعى سلطة إصدار الشهادة التي تُصدر الشهادة المتقاطعة بأنها سلطة الإصدار الوسيطة (انظر الشكل 2). ويمكن أن تحتوي كلتا الشهادتين: الشهادة المتقاطعة وشهادة الكيان النهائي، على توسّع في سياسات الشهادة.

والضمانات والالتزامات التي تقاسمها سلطة إصدار الشهادة الصاحبة وسلطة إصدار الشهادة الوسيطة ومستعمل الشهادة محددة في سياسة الشهادة المعرفة هويتها في الشهادة المتقاطعة، والتي تستطيع سلطة الإصدار الصاحبة أن تتصرف طبقاً لها بصفتها الكيان النهائي أو العاملة باسمه. كما أن الضمانات والالتزامات التي يتقاسمها صاحب الشهادة وسلطة إصدار الشهادة الصاحبة وسلطة إصدار الشهادة الوسيطة محددة في سياسة الشهادة المعرفة هويتها في شهادة الكيان النهائي، والتي تستطيع سلطة إصدار الشهادة الوسيطة أن تتصرف طبقاً لها بصفتها مستعمل الشهادة أو العاملة باسمه.



الشكل 2 – إصدار الشهادة المتقاطعة

تعتبر مسيرة إصدار الشهادة صالحة بموجب مجموعة السياسات المشتركة بين جميع الشهادات في المسيرة.

ويمكن اعتبار سلطة الإصدار الوسطية بدورها صاحبة شهادة تصدرها سلطة إصدار أخرى، مما يؤدي إلى إنشاء مسيرات إصدار تفوق أطوالها طول شهادتين. ونظراً إلى أن الثقة تعاني من ضياع مع ازدياد طول مسيرات إصدار الشهادة، يلزم اتخاذ تدابير مراقبة للتأكد من أن شهادات الكيان النهائي التي تكون سوية الثقة التي تصحبها منخفضة إلى حد غير مقبول، سوف يرفضها مستعمل الشهادة. وتشكل هذه الوظيفة جزءاً من إجراء معالجة مسيرة إصدار الشهادة.

وعلاوة على الحالة الموصوفة أعلاه، توجد حالتان خاصتان جديرتان بالاعتبار:

أ) لا تسعمل سلطة إصدار الشهادة توسّع سياسة الشهادة، لكي تنقل متطلبات سياستها إلى مستعملي الشهادات؛

ب) يفوّض مستعمل الشهادة أو سلطة إصدار الشهادة الوسيطة مهمة سياسة المراقبة إلى السلطة التالية في المسيرة.

وينبغي في الحالة الأولى ألا تحتوي الشهادة توسع سياسات الشهادة بتاتاً، وينتج عن ذلك أن تكون مجموعة السياسات التي تكون المسيرة بموجبها صالحة، مجموعة خالية، ومع ذلك تبقى المسرة صالحة. ويبقى مستعملو الشهادة يتأكدون من أنهم يستعملون الشهادة طبقاً لسياسات السلطات في المسيرة.

وينبغي لمستعمل الشهادة أو لسلطة إصدار الشهادة الوسيطة أن يضمّن القيمة الخاصة *أي سياسة (any-policy)* في *مجموعة السياسات الأولية (initial-policy-set)* أو في الشهادة المتقاطعة. وعندما تتضمن شهادة ما القيمة الخاصة *أي سياسة*، ينبغي لها ألا تتضمن أي معرفات أخرى بهوية سياسة الشهادة. وينبغي لمعرف هوية *أي سياسة* ألا تصحبه أي واصفات للسياسة.

ويستطيع مستعمل الشهادة التأكد من أن جميع التزاماته قد نقلت طبقاً للمعيار بوضع مؤشر *السياسة الصريحة الأولية (initial-explicit-policy)*. وبذلك لا تُقبل إلا السلطات التي تستعمل توسع سياسات الشهادة المعياري لتحقيق الارتباطات في المسيرة، ولا يترتب على مستعملي الشهادات أي التزامات إضافية. ولما كانت السلطات تفرض التزامات عندما تتصرف بصفتها مستعمل الشهادة أو العاملة باسمه، يمكنها أن تتأكد من أن جميع التزاماتها قد نقلت طبقاً للمعيار بوضع **مطلب السياسة الصريحة (requireExplicitPolicy)** في الشهادة المتقاطعة.

3.1.8 تقابل السياسات

يمكن لبعض مسيرات إصدار الشهادة أن تتجاوز الحدود الفاصلة بين ميادين السياسة. وقد تكون الضمانات والالتزامات التي صدرت بموجبها الشهادة المتقاطعة مكافئة مادياً لكل أو لبعض الضمانات والالتزامات التي تصدر بموجبها سلطة إصدار الشهادة الصاحبة الشهادات للكيانات النهائية، حتى ولو كانت سلطات السياسة التي تخضع لها سلطتا إصدار الشهادة في عملها، قد اختارت معرفات هوية وحيدة مختلفة لهاتين السياستين المتكافئتين. وفي هذه الحالة، يمكن أن تضمّن سلطة إصدار الشهادة الوسيطة توسعاً لتقابل السياسات في الشهادة المتقاطعة. وفي توسع تقابل السياسات، تؤكد سلطة إصدار الشهادة الوسيطة لمستعمل الشهادة أن بإمكانه أن يستمر في التمتع بالضمانات العادية، وأن عليه أن يستمر في التكفّل بالتزاماته العادية، حتى ولو كانت الكيانات اللاحقة في مسيرة إصدار الشهادة تعمل في ميدان سياسي مختلف. وينبغي لسلطة إصدار الشهادة الوسيطة أن تبيّن تقابلاً واحداً أو أكثر من واحد لكل واحدة من المجموعات الفرعية من السياسات التي تُصدر بموجبها الشهادة المتقاطعة، وينبغي لها ألا تبين أي تقابل لأي سياسة أخرى. وإذا كانت واحدة (أو أكثر من واحدة) من سياسات الشهادة التي تعمل بموجبها سلطة إصدار الشهادة الوسيطة (أي كان لها نفس معرف الهوية الوحيد)، يجب استبعاد هذه المعرفات للهوية من توسع تقابل السياسات، وإيرادها في توسع سياسة الشهادة.

ويكون لتقابل السياسات تأثير في تحويل جميع معرفات هوية السياسة، للشهادات الواردة لاحقاً في مسيرة إصدار الشهادة، إلى معرف هوية السياسة المكافئة، الذي يعترف به مستعمل الشهادة.

ولا يجري تقابل السياسات مع القيمة الخاصة *أي سياسة*، لا منها ولا إليها.

يمكن لمستعملي الشهادات أن يقرروا بأن الشهادات التي تصدر في ميدان سياسي غير الميدان الخاص بهم، ينبغي ألا يعتمد عليها، حتى ولو كانت سلطة وسيطة موثوقة لإصدار الشهادة راحت تقرر بأن سياستها تكافئ مادياً سياستهم. يمكن فعل ذلك إذا وضعت القيمة الخاصة *حظر تقابل السياسات الأولي (initial-policy-mapping-inhibit input)* في إجراء إقرار صلاحية المسيرة. وفوق ذلك تستطيع سلطة إصدار الشهادة الوسيطة أن تقوم بعمل مماثل باسم مستعملي شهاداتها. ولكي تتأكد السلطة من أن مستعملي الشهادات ينفّذون بالضبط هذا المطلب، فإنها تستطيع وضع المكوّنة **حظر تقابل السياسات (inhibitPolicyMapping)** في توسع لتقييدات السياسة.

4.1.8 معالجة مسيرة إصدار الشهادة

يواجه مستعمل الشهادة خياراً ما بين استراتيجيتين:

أ) يمكنه أن يطالب بأن تكون مسيرة إصدار الشهادة صالحة بموجب واحدة على الأقل من مجموعة السياسات التي حددها المستعمل مسبقاً؛ أو

ب) يمكنه أن يطلب من وحدة إقرار المسيرة أن تبلغه مجموعة السياسات التي تكون معها مسيرة إصدار الشهادة صالحة.

وتكون الاستراتيجية الأولى مناسبة أكثر، عندما يكون مستعمل الشهادة يعرف، *سلفاً*، مجموعة السياسات المقبولة لاستخدامه المزمع.

وتكون الاستراتيجية الثانية مناسبة أكثر، عندما يكون مستعمل الشهادة لا يعرف، *سلفاً*، مجموعة السياسات المقبولة لاستخدامه المزمع.

وفي الحالة الأولى، يبين إجراء إقرار الصلاحية لمسيرة إصدار الشهادة أن المسيرة صالحة فقط، إن كانت صالحة بموجب واحدة أو عدة من السياسات المحددة في *مجموعة السياسات الأولية (initial-policy-set)*، ويعيد المجموعة الفرعية من *مجموعة السياسات الأولية* التي تكون المسيرة صالحة بموجبها. وفي الحالة الثانية، يمكن لإجراء إقرار الصلاحية لمسيرة إصدار الشهادة أن يبين أن المسيرة ليست صالحة بموجب *مجموعة السياسات الأولية*، ولكنها صالحة بموجب مجموعة منفصلة هي *مجموعة السياسات التي تفرضها السلطات (authorities-constrained-policy-set)*. وبعد ذلك يقرر مستعمل الشهادة إن كان

استخدامه المزمع للشهادة يتسق مع واحدة أو عدة سياسات الشهادة التي تكون المسيرة صالحة بموجبها، وعندما يضع مستعمل الشهادة *مجموعة السياسات الأولية (initial-policy-set)* على *أي سياسة (any-policy)*، يستطيع أن يفرض على الإجراء أن يعيد نتيجة صالحة، إن كانت المسيرة صالحة بموجب أي سياسة (غير محددة).

5.1.8 الشهادات الصادرة لذاتها

تستطيع سلطة إصدار الشهادة إصدار شهادة لذاتها في الحالات الثلاث التالية:

أ) كوسيلة مناسبة لتشفير المفتاح العمومي المصاحب للمفتاح الخاص المستعمل لتوقيع الشهادة، وهكذا يمكن توصيله إلى أنظمة استعمال الشهادات لديها، حتى تختزنه هذه الأنظمة بصفة مرسّخات للثقة؛

ب) للتصديق على مفاتيح عمومية إضافة لسلطة إصدار الشهادة، لأغراض غير الأغراض المقصودة في الفقرة أ) (مثل البروتوكول OCSP وتوقيع القائمة CRL عند اللزوم)؛

ج) للاستعاضة عن شهاداتها الخاصة المنتهية صلاحيتها.

ويسمى هذا النمط من الشهادات شهادات صادرة لذاتها، ويمكن معرفتها من كون اسمي المُصْدر والصاحب متطابقين. ولأغراض إقرار صلاحية المسيرة، تكون الشهادات الصادرة لذاتها من فئة الحالة أ) هي شهادات موقعة من ذاتها، ولذلك يتم التحقق منها في إطار إقرار صلاحية المسيرة عن طريق المفتاح العمومي الموجود فيها، وإذا صودفت في المسيرة يجب تجاهلها.

أما الشهادات الصادرة لذاتها من فئة الحالة ب)، فهي لا تظهر إلا كشهادات في نهاية المسيرة، ويجب معالجتها على هذا الأساس.

والشهادات الصادرة لذاتها من فئة الحالة ج) (وتعرف أيضاً باسم شهادات صادرة لذاتها وسيطة) يمكن أن تظهر كشهادات وسيطة في مسيرة. ومن الممارسات الجيدة التي ينبغي لسلطة إصدار الشهادة أن تمارسها، عند تبديلها مفتاحاً على وشك انتهاء صلاحيته، هي أن تطلب إصدار أي شهادات متقاطعة ذات صلة وتحتاج إليها، لكي تستعيض عن مفتاحها العمومي، قبل استعمال المفتاح الجديد. وعلى أي حال، عندما تصادف في المسيرة شهادات صادرة لذاتها من هذه الفئة، يجب معالجتها على أنها شهادات وسيطة، مع الاستثناء التالي: إنها لا تساهم في حساب طول المسيرة، لأغراض معالجة المكوّنة **تقييد طول المسيرة (pathLenConstraint)** من التوسّع **تقييدات أساسية (basicConstraints)**، ومعالجة قيم *الشهادات المفوّتة (المتجاهلة) (skip-certificates)* المصاحبة للمؤشرين في انتظار حظر تقابل السياسات *(policy-mapping-inhibitpending) في انتظار سياسة صريحة (explicit-policy-pending indicators)*.

وإذا استخدمت سلطة ما نفس المفتاح لتوقيع الشهادات والقوائم CRL، يجب استعمال شهادة واحدة صادرة لذاتها من فئة الحالة أ). أما إذا استخدمت سلطة مفتاحاً لتوقيع القوائم CRL مختلفاً عن المفتاح المستخدم لتوقيع الشهادات، يكون للسلطة أن تختار بين إصدار شهادتين صادرتين لذاتيهما من فئة الحالة أ)، واحدة منهما لكل واحد من المفتاحين. وفي هذه الحالة، قد يحتاج مستعملا الشهادتين إلى النفاذ إلى كلتا الشهادتين الصادرتين لذاتيهما، حتى يقيما مرسّختي ثقة منفصلتين للشهادات وللقوائم CRL. وفي هذه الحالة، يستعمل مستعملا الشهادتين المفتاح المصدّق عليه في شهادة الفئة ب) باعتباره مرسّخة الثقة الوحيدة للشهادات وللقوائم CRL التي توقعها هذه السلطة. وفي هذه الحالة، إذا كانت الشهادة الصادرة لذاتها من فئة الحالة ب) هي المطلوب استعمالها للتحقق من التوقيعات على القوائم CRL، لا يعود يوجد في هذا المعيار أي وسيلة للتحقق من صلاحية هذه الشهادة.

وإذا صودفت في المسيرة شهادات صادرة لذاتها من فئة الحالة ب)، يجب تجاهلها (تفويتها).

ملاحظة – إن الآليات الأخرى المستخدمة لتوزيع المفاتيح العمومية التي تصدرها سلطات إصدار الشهادة، تقع خارج نطاق مواصفة الدليل هذه.

2.8 توسّعات في معلومات المفتاح والسياسة

1.2.8 المتطلبات

تتعلق المتطلبات التالية بمعلومات المفتاح والسياسة:

أ) يمكن أن يحيّن زوج المفاتيح لسلطة إصدار الشهادة، في فواصل زمنية متساوية أو في ظروف خاصة. فهناك إذن حاجة إلى حقل في شهادة معدّ لينقل معرف هوية المفتاح العمومي المستخدم للتحقق من توقيع الشهادة. ويستطيع نظام استعمال الشهادات أن يستعمل مثل هذه المعرفات للهوية لكي يفتش عن الشهادة الصحيحة لسلطة إصدار الشهادة من أجل إقرار صلاحية المفتاح العمومي لمُصْدر الشهادة.

ب) ويكون لصاحب الشهادة مفاتيح عمومية مختلفة، وبالتالي شهادات مختلفة لأغراض مختلفة، مثل التوقيع الرقمي وتجفير اتفاق المفتاح. فهناك إذن حاجة إلى حقل في شهادة لكي يساعد مستعمل الشهادة على انتقاء الشهادة الصحيحة لصاحب معين من أجل غرض خاص، أو لكي يتيح لسلطة إصدار الشهادة أن تشترط أن مفتاحاً مصدّقاً هو وحده الذي يمكن استعماله لغرض معين.

ج) يمكن أن يحيّن زوج مفاتيح الصاحب في فواصل زمنية متساوية أو في ظروف خاصة. فهناك إذن حاجة إلى حقل في شهادة معدّ لينقل معرف الهوية للمفتاح العمومي حتى يقوم بالتمييز بين المفاتيح العمومة المختلفة التابعة للصاحب نفسه والتي تستعمل في أوقات مختلفة. ويستطيع نظام استعمال الشهادات أن يستعمل مثل هذه المعرفات للهوية لكي يفتش عن الشهادة الصحيحة.

د) يستخدم المفتاح الخاص المقابل لمفتاح عمومي مصدّق عليه في فترة زمنية تختلف عموماً عن مدة صلاحية المفتاح العمومي. وفي حالة مفاتيح التوقيع الرقمي، تكون فترة استخدام المفتاح الخاص للتوقيع أقصر عموماً من فترة المفتاح العمومي للتحقق. وتبين فترة صلاحية الشهادة فترة يمكن استعمال المفتاح العمومي أثناءها، وهي فترة، لا تكون بالضرورة هي فترة استعمال المفتاح الخاص. وإذا ما تعرض المفتاح الخاص للخطر، يمكن الحدّ من فترة تعرّضه، إن كان المتحقق من التوقيع يعرف فترة الاستعمال القانونية للمفتاح الخاص. فهناك إذن حاجة إلى دلالة تبين في الشهادة فترة استعمال المفتاح الخاص.

هـ) لما كانت الشهادات قد تستعمل في بيئات تنطبق فيها عدة سياسات للشهادة، فهناك إذن حاجة إلى وضع حكم في الشهادة يبين معلومات عن سياسة الشهادة.

و) في حالة شهادة متقاطعة صادرة من هيئة إلى أخرى، يمكن القبول أحياناً باعتبار بعض من سياسات الهيئتين متكافئة. إذن تحتاج شهادة صادرة عن سلطة إصدار الشهادة إلى أن تسمح لمُصدر الشهادة بأن يبين أن واحدة من سياسات الشهادة الخاصة به مكافئة لسياسة شهادة أخرى في ميدان سلطة إصدار الشهادة الصاحبة. وتسمى هذه العملية تقابل السياسات.

ز) مستعمل نظام التجفير أو التوقيع الرقمي الذي يستخدم شهادات محددة في مواصفة الدليل هذه، يحتاج أن يكون قادراً على أن يحدد مسبقاً الخوارزميات التي يؤيدها المستعملون الآخرون.

2.2.8 حقول التوسع في شهادة المفتاح العمومي وفي القائمة CRL

تتحدد حقول التوسع التالية:

أ) *معرف هوية مفتاح السلطة؛*

ب) *معرف هوية مفتاح الصاحب؛*

ج) *استعمال المفتاح؛*

د) *استعمال المفتاح الموسّع؛*

ه) *فترة استعمال المفتاح الخاص؛*

و) *سياسات الشهادة؛*

ز) *تقابلات السياسات.*

ويجب أن تستعمل هذه التوسعات باعتبارها توسعات شهادات، ما عدا معرف هوية مفتاح السلطة الذي يمكن استعماله أيضاً باعتباره توسعاً في القائمة CRL. ويمكن استعمال هذه التوسعات في كلا نوعي الشهادات: شهادات سلطة إصدار الشهادة وشهادات الكيان النهائي، ما لم ينص على خلاف ذلك.

1.2.2.8 توسع معرف هوية مفتاح السلطة

يعرِّف هذا الحقل الذي يمكن استعماله بصفة توسع شهادة أو توسع قائمة CRL، بهوية المفتاح العمومي المطلوب استخدامه للتحقق من التوقيع على هذه الشهادة أو هذه القائمة CRL. وهو يمكّن من تمييز المفاتيح التي تستعملها نفس سلطة إصدار الشهادة (عند تحيين المفاتيح مثلاً). ويعرَّف هذا الحقل كما يلي:

```
authorityKeyIdentifier EXTENSION ::= {
    SYNTAX              AuthorityKeyIdentifier
    IDENTIFIED BY       id-ce-authorityKeyIdentifier }

AuthorityKeyIdentifier ::= SEQUENCE {
    keyIdentifier                [0] KeyIdentifier                OPTIONAL,
    authorityCertIssuer          [1] GeneralNames                 OPTIONAL,
    authorityCertSerialNumber    [2] CertificateSerialNumber      OPTIONAL }
    ( WITH COMPONENTS            {..., authorityCertIssuer PRESENT,
                                 authorityCertSerialNumber PRESENT} |
     WITH COMPONENTS             {..., authorityCertIssuer ABSENT,
                                 authorityCertSerialNumber ABSENT} )

KeyIdentifier ::= OCTET STRING
```

ويمكن تحديد المفتاح بمعرف هوية صريح للمفتاح في المكوّنة **معرف هوية المفتاح (keyIdentifier)**، أو بتعريف هوية شهادة للمفتاح (تبيّن مُصدر الشهادة في المكوّنة **السلطة المصدرة للشهادة (authorityCertIssuer)** ورقم تسلسل الشهادة في المكونة **رقم تسلسل سلطة الشهادة (authorityCertSerialNumber)**، أو بمعرف الهوية الصريح للمفتاح وبتعريف هوية شهادة للمفتاح معاً. وإذا استخدم شكلا تعريف الهوية، يجب على مُصدر الشهادة أو القائمة CRL أن يتأكد من أنهما متّسقان. ويجب أن يكون معرف هوية المفتاح وحيداً بين جميع معرفات هوية مفاتيح سلطة إصدار الشهادة أو القائمة CRL الحاوية على التوسع. ولا يطلب من التنفيذ الذي يعتمد هذا التوسع أن يكون قادراً على معالجة جميع أشكال الأسماء الموجودة في المكوّنة **مُصْدر شهادة السلطة (authorityCertIssuer)**. (انظر الفقرة 1.2.3.8 للتفصيلات بشأن نمط **الأسماء العامة (GeneralNames)**).

تقوم سلطات إصدار الشهادة بإسناد أرقام التسلسل للشهادات، بحيث يعرّف كل زوج (المُصدر ورقم تسلسل الشهادة) هوية شهادة وحيدة لا غير. ويمكن استخدام الشكل **معرف هوية المفتاح (keyIdentifier)** لانتقاء شهادات سلطة إصدار الشهادة أثناء إنشاء المسيرة. ولا يمكن استخدام الزوج **السلطة المصدرة للشهادة ورقم تسلسل السلطة** إلا لبيان تفضيل إحدى الشهادات على غيرها أثناء إنشاء المسيرة.

ويكون هذا التوسع غير حرج دائماً.

2.2.2.8 توسع معرف هوية مفتاح الصاحب

يحدد هذا الحقل المفتاح العمومي المصدق عليه. وهو يمكّن من تمييز المفاتيح التي يستعملها نفس الصاحب (عند تحيين المفاتيح مثلاً). ويعرّف هذا الحقل كما يلي:

```
subjectKeyIdentifier EXTENSION ::= {
    SYNTAX              SubjectKeyIdentifier
    IDENTIFIED BY       id-ce-subjectKeyIdentifier }

SubjectKeyIdentifier ::= KeyIdentifier
```

ويجب أن يكون معرف هوية المفتاح وحيداً بين جميع معرفات هوية مفاتيح الصاحب الذي يستعمل له. ويكون هذا التوسع غير حرج دائماً.

3.2.2.8 توسع استعمال المفتاح

يعرف هذا الحقل بهوية الاستعمال المزمع الذي أُصدرت الشهادة له. وقد يحدث تقييد لاحق للاستعمال المزمع بسبب السياسة المعتمدة. وقد ينص على هذه السياسة في تعريف سياسة الشهادة أو في عقد أو في مواصفة أخرى. ومع ذلك يجب ألا تلغي سياسة ما التقييد الذي تبيّنه بتة في مجال **استعمال المفتاح (KeyUsage)**، أي لا يمكن لسياسة شهادة ما أن تسمح باستخدام شهادة كتوقيع رقمي، إن كان **استعمال المفتاح** يبين أنها ينبغي ألا تستعمل إلا كاتفاق مفتاح.

وانتقاء قيمة معينة **لاستعمال المفتاح** في شهادة ما لا يشكل بحد ذاته دلالة، في إحدى مراحل الاتصال، على أن الأطراف المتواصلة تعمل طبقاً لهذا الانتقاء، أي عند توقيع إحدى الوثائق مثلاً. والتعريف بالطرائق التي تستطيع الأطراف المشاركة استعمالها للتعبير عن نيتها بشأن مرحلة معينة من الاتصال (أي الالتزام بمحتوى هذه المرحلة الخاصة)، يقع خارج نطاق مواصفة الدليل هذه، ولكن من المتوقع أن تكون هناك طرائق متعددة. ومن الممكن استعمال محتوى إحدى الشهادات، وإن كان لا يوصى بذلك، مثل سياسة الشهادة، للإشارة إلى الغاية من التوقيع. ومع ذلك لما كانت الإشارة حاصلة عند إصدار الشهادة من سلطة إصدار الشهادة، فإن مثل هذا الاستعمال لمحتوى الشهادة قد لا يلبي المتطلب القائل بأن التصريح عن النية، قد جرى في الوقت الذي قام فيه الموقّع بالتوقيع.

ويمكن أن يحدث انتقاء عدة بتات في مرحلة من التوسع **استعمال المفتاح**. وانتقاء عدة بتات يجب ألا يغير في معنى كل بتة لوحدها، ولكنه يجب أن يدل على أن الشهادة يمكن استعمالها لجميع الأغراض التي تبينها مجموعة البتات. وانتقاء عدة بتات قد ينطوي على مخاطرات. ويوثّق الملحق I استعراضاً لهذه المخاطرات، ويعرف هذا الحقل كما يلي:

```
keyUsage EXTENSION ::= {
    SYNTAX              KeyUsage
    IDENTIFIED BY       id-ce-keyUsage }

KeyUsage ::= BIT STRING {
    digitalSignature        (0),
    contentCommitment       (1),
    keyEncipherment         (2),
    dataEncipherment        (3),
    keyAgreement            (4),
    keyCertSign             (5),
    cRLSign                 (6),
    encipherOnly            (7),
    decipherOnly            (8) }
```

واستعمال بتات النمط **استعمال المفتاح (KeyUsage)** هو كما يلي:

أ) **التوقيع الرقمي (digitalSignature)**: للتحقق من التوقيعات الرقمية المستعملة في خدمة استيقان الكيان أو في خدمة استيقان المُصْدر و/أو في خدمة التكاملية؛

ب) **الالتزام بالمحتوى (contentCommitment)**: للتحقق من التوقيعات الرقمية التي ترمي إلى الإعراب عن أن الموقّع ملتزم بقبول المحتوى الذي يوقعه. ونمط الالتزام الذي تستعمل الشهادة لاعتماده، يمكن أن يخضع في المستقبل لتقييدات تفرضها سلطة إصدار الشهادة، عبر سياسة الشهادة مثلاً. ويمكن تبيان نمط التزام الموقّع بالضبط – "روجع وصدّق عليه" أو "مع نيّة الارتباط" – في المحتوى الجاري توقيعه، أي في الوثيقة الموقعة بذاتها أو في بعض المعلومات الإضافية الموقّعة.

ولما كان توقيع الالتزام بقبول المحتوى يعتبر معاملة موقّعة رقمياً، يجب ألا ترد بالضرورة بتة **التوقيع الرقمي** في الشهادة. وإذا وردت، فإنها لا تؤثر في سوية الالتزام الذي تعهد به الموقّع في المحتوى الموقَّع عليه.

ويلاحظ أنه ليس من الخطأ أن يحال إلى بتة **استعمال المفتاح** باستخدام معرف هوية **عدم الرفض (nonRepudiation)**. ومع ذلك فإن استخدام هذا المعرّف للهوية متروك. وبصرف النظر عن معرف الهوية المستخدم، فإن دلالات هذه البتة تبقى كما هي محددة في مواصفة الدليل هذه؛

ج) **تجفير المفتاح (keyEncipherment)**: تجفير المفاتيح أو غيرها من المعلومات الأمنية، لنقل المفاتيح مثلاً؛

د) **تجفير المعطيات (dataEncipherment)**: تجفير معطيات المستعمل، ولكن غير المفاتيح أو سواها من المعلومات الأمنية، كما هو مذكور في الفقرة ج) أعلاه؛

هـ) **اتفاق المفتاح (keyAgreement)**: يستعمل كاتفاق مفتاح بشأن مفتاح عمومي؛

و) **توقيع شهادة المفتاح (keyCertSign)**: للتحقق من توقيع سلطة إصدار الشهادة على الشهادة.

ولما كان توقيع الشهادة يعتبر التزاماً بمحتواها من سلطة إصدار الشهادة، فلا حاجة لإدراج بتة **التوقيع الرقمي** ولا بتة **الالتزام بالمحتوى** في الشهادة. وإذا أدرجت أي منها أو كلتاهما، فإن ذلك لا يؤثر في سوية الالتزام الذي تعهد به الموّقع على الشهادة؛

ز) **توقيع القائمة cRL (cRLSign)**: للتحقق من توقيع السلطة على القوائم CRL.

ولما كان توقيع القائمة CRL يعتبر التزاماً بمحتواها من مُصدر القائمة CRL، فلا حاجة لإدراج بتة **التوقيع الرقمي** ولا بتة **الالتزام بالمحتوى** في الشهادة. وإذا أدرجت أي منها أو كلتاهما، فإن ذلك لا يؤثر في سوية الالتزام الذي تعهد به الموّقع على القائمة CRL؛

ح) **تجفير فقط (encipherOnly)**: اتفاق المفتاح بشأن مفتاح عمومي يستعمل حصراً لتجفير المعطيات، عندما تكون بتة **اتفاق المفتاح** مدرجة أيضاً (لا يكون المعنى محدداً، عندما تدرج بتة استعمال المفتاح الأخرى)؛

ط) **فك التجفير فقط (decipherOnly)**: اتفاق المفتاح بشأن مفتاح عمومي يستعمل حصراً لفك تجفير المعطيات، عندما تكون بتة **اتفاق المفتاح** مدرجة أيضاً (لا يكون المعنى محدداً، عندما تدرج بتة استعمال المفتاح الأخرى).

وينبغي لمواصفات التطبيق أن تبين أيّ البتتين يناسب استعمالا في التطبيق: بتة **التوقيع الرقمي** أم بتة **الالتزام بالمحتوى**. وإذا كان تطبيق التوقيع لا يعرف نية الموقّع بشأن الالتزام بالمحتوى، يجب على التطبيق أن يوقّع وأن يدعم توقيعه بشهادة أدرجت فيها بتة **التوقيع الرقمي** في التوسع **استعمال المفتاح** لهذه الشهادة.

حتى ولو جرى التحقق من التوقيع الرقمي باستخدام شهادة أدرجت فيها فقط بتة **التوقيع الرقمي**، فقد تلعب عوامل أخرى خارجة عن التحقق من التوقيع الرقمي باستخدام شهادة أدرجت فيها فقط بتة **الالتزام بالمحتوى**. فقد يستعمل الموقّع عوامل خارجية لكي يتراجع عن التزامه بالمحتوى الذي وقّعه.

وتستعمل البتة **توقيع شهادة المفتاح** فقط في شهادات سلطة إصدار الشهادة. وإذا كان **استعمال المفتاح** موضوعاً على **توقيع شهادة المفتاح**، فإن قيمة المكوّنة cA (سلطة إصدار الشهادة) من التوسّع **التقييدات الأساسية (basicConstraints)** يجب أن توضع على "صائبة". وتستطيع سلطة إصدار الشهادة أن تستعمل أيضاً بتات أخرى معرّفة في **استعمال المفتاح (KeyUsage)**، مثل **التوقيع الرقمي** لتقديم الاستيقان والتكاملية للمعاملات الإدارية على الخط.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصْدر الشهادة.

وإذا كان التوسع موسوماً بأنه حرج، أو إذا كان التوسع موسوماً غير حرج ولكن نظام استمال الشهادات يعترف به، تستعمل الشهادة فقط للغرض الذي أدرجت من أجله بتة استعمال المفتاح المقابلة. أما إذا كان التوسع موسوماً بأنه غير حرج، ونظام استعمال الشهادات لا يعترف به، يجب عندئذ تجاهل هذا التوسّع. والبتة الموضوعة على الصفر تدل على أن

المفتاح غير معدّ لهذا الغرض. وإذا كان هذا التوسع موجوداً وجميع البتات الأخرى موضوعة على الصفر، يكون المفتاح معدّاً لبعض الأغراض الأخرى غير الأغراض المعددة أعلاه.

4.2.2.8 توسّع استعمال المفتاح الموسّع

يبين هذا الحقل الغرض أو الأغراض التي يمكن أن يستعمل لها المفتاح العمومي المصدّق عليه، إضافة إلى الأغراض الأساسية المبينة في مجال توسّع استعمال المفتاح، أو بدلاً من هذه الأغراض. ويعرف هذا الحق كما يلي:

```
extKeyUsage EXTENSION ::= {
    SYNTAX              SEQUENCE SIZE (1..MAX) OF KeyPurposeId
    IDENTIFIED BY       id-ce-extKeyUsage }

KeyPurposeId ::= OBJECT IDENTIFIER
```

تستطيع سلطة إصدار الشهادة الإعلان عن أي استعمال مفتاح موسّع باستخدامها معرف الهوية **توسّع استعمال المفتاح الموسّع (anyExtendedKeyUsage)**، مما يمكّن سلطة إصدار الشهادة من إصدار شهادة تحتوي على معرفات هوية الموضوع (OID) لاستعمالات المفتاح هذه. وإذا كان استعمال المفتاح الموسع يرمي إلى تقييد استعمال المفتاح، فإن إدراج هذا المعرّف بهوية الموضوع يزيل هذا التقييد.

```
anyExtendedKeyUsage  OBJECT IDENTIFIER  ::= { 2 5 29 37 0 }[S9]
```

يمكن لأي هيئة أن تحدد أغراضاً لاستعمال المفتاح، هي تحتاجها. ومعرفات هوية الموضوع المستعملة للتعريف بهذه الأغراض يتم إسنادها وفقاً للتوصية ITU-T X.660 | المعيار ISO/IEC 9834-1.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصدر الشهادة.

إذا كان التوسع موسوماً بأنه حرج، تستعمل الشهادة فقط لواحد من الأغراض المبيّنة.

وإذا كان التوسع موسوماً بأنه غير حرج، فهو يدل عندئذ على الغرض أو الأغراض المتوقعة لاستعمال المفتاح، ويمكن استعماله لإيجاد المفتاح الصحيح أو الشهادة الصحيحة من بين المفاتيح أو الشهادات التي يمتلكها كيان ما. وإذا كان هذا التوسع موجوداً، واعترف نظام استعمال الشهادات بنمط التوسّع، **استعمال المفتاح الموسّع** وعالجه، يجب على نظام استعمال الشهادات أن يؤكد على أن تستعمل الشهادة فقط لواحد من الأغراض المبيّنة (يمكن للتطبيقات المستعملة للشهادات أن تطلب تعيين غرض معيّن لكي يستطيع التطبيق قبول الشهادة).

وإذا كانت إحدى الشهادات تحتوي على حقلين معاً؛ حقل استعمال المفتاح الحرج وحقل استعمال المفتاح الموسّع الحرج، يعالج كلا المجالين، كل على حدة، ولا تستعمل الشهادة إلا لغرض متّسق مع المجالين كليهما. وإذا لم يكن هناك عرض متسق مع المجالين كليهما، لا تستعمل الشهادة لأي غرض.

وتحدد هذه المواصفة أغراض المفتاح التالية التي يمكن أن يشتمل عليها توسّع استعمال المفتاح الموسّع. وهناك أغراض أخرى يمكن أن يشتمل عليها هذا التوسع، هي معرفة في مواصفات أخرى، مثل IETF RFC 3280.

```
keyPurposes             OBJECT IDENTIFIER  ::=  {ds 38 1}
```

5.2.2.8 توسّع فترة استعمال المفتاح الخاص

يبين هذا الحقل فترة استعمال المفتاح الخاص المقابل للمفتاح العمومي المصدّق عليه. ولا ينطبق إلا على مفاتيح التوقيع الرقمي. ويتحدد هذا الحقل كما يلي:

```
privateKeyUsagePeriod EXTENSION ::= {
    SYNTAX              PrivateKeyUsagePeriod
    IDENTIFIED BY       id-ce-privateKeyUsagePeriod }

PrivateKeyUsagePeriod ::= SEQUENCE {
    notBefore   [0]   GeneralizedTime OPTIONAL,
    notAfter    [1]   GeneralizedTime OPTIONAL }
    ( WITH COMPONENTS {..., notBefore PRESENT} |
    WITH COMPONENTS       {..., notAfter PRESENT} )
```

تدل المكوّنة **ليس قبل (notBefore)** على أبكر تاريخ ووقت يمكن فيهما استعمال مفتاح خاص للتوقيع. وإذا كانت المكوّنة **ليس قبل** غير موجودة، لا تكون هناك أي معلومة تدل على متى تبدأ فترة صلاحية استعمال المفتاح الخاص. وتدل المكوّنة **ليس بعد (notAfter)** على آخر تاريخ ووقت يمكن فيهما استعمال مفتاح خاص للتوقيع. وإذا كانت المكوّنة **ليس بعد** غير موجودة، لا تكون هناك أي معلومة تدل على متى تنتهي فترة صلاحية استعمال المفتاح الخاص.

ويكون هذا التوسع غير حرج دائماً.

ملاحظة 1 – يمكن أن تكون فترة صلاحية استعمال المفتاح الخاص مختلفة عن فترة الصلاحية المصدق عليها للمفتاح العمومي التي تبيّنها فترة صلاحية الشهادة. وفي مفاتيح التوقيع الرقمي، تكون فترة استعمال المفتاح الخاص للتوقيع أقصر عامة من فترة استعمال المفتاح العمومي للتحقق.

ملاحظة 2 – إذا أراد المتحقق من توقيع رقمي، أن يتحقق من أن الشهادة لم يجر إبطالها حتى وقت إجراء التحقق، بسبب تعرض المفتاح للخطر، يجب أن تكون الشهادة الصالحة ما زالت قائمة للمفتاح العمومي حتى وقت التحقق. وبعد أن تنتهي صلاحية الشهادة (أو الشهادات) لمفتاح عمومي، لا يستطيع المتحقق من التوقيع، أن يعتمد القوائم CRL التي تبلّغ عن تعرض للخطر.

6.2.2.8 توسّع سياسات الشهادة

يعدّد هذا الحقل سياسات الشهادة التي تعرف بها سلطة إصدار الشهادة المُصدرة والتي تنطبق على الشهادة، ويعدّد معها المعلومات عن الواصف الاختياري المتصلة بسياسات الشهادة. وتستعمل قائمة سياسات الشهادة في تحديد صلاحية مسيرة لإصدار الشهادات، كما هو مشروح في البند 10. والواصفات الاختيارية لا تُستعمل في الإجراء الذي يعالج مسيرة إصدار الشهادة، بل إن الواصفات المعنيّة هي من نتاج هذه العملية، وتقدم للتطبيق الذي يستعمل الشهادة، وذلك للمساعدة على تقرير ما إذا كانت مسيرة صالحة هي مناسبة لهذه المعاملة الخاصة والسياسات المختلفة للشهادة تتعلق بتطبيقات مختلفة تستعمل المفتاح المصدّق عليه. ويدل وجود هذا التوسع في شهادة كيان نهائي على سياسات الشهادة التي تكون هذه الشهادة صالحة لها. ويدل وجود هذا التوسع في شهادة تصدرها سلطة إصدار شهادة إلى سلطة إصدار شهادة أخرى على سياسات الشهادة التي يمكن لمسيرات إصدار الشهادة الحاوية على هذه الشهادة أن تكون صالحة لها. ويعرّف هذا الحقل كما يلي:

```
certificatePolicies EXTENSION ::= {
    SYNTAX              CertificatePoliciesSyntax
    IDENTIFIED BY       id-ce-certificatePolicies }

CertificatePoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
    policyIdentifier    CertPolicyId,
    policyQualifiers    SEQUENCE SIZE (1..MAX) OF
                            PolicyQualifierInfo OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId   CERT-POLICY-QUALIFIER.&id
                        ({SupportedPolicyQualifiers}),
    qualifier           CERT-POLICY-QUALIFIER.&Qualifier
                        ({SupportedPolicyQualifiers}{@policyQualifierId})
                        OPTIONAL }

SupportedPolicyQualifiers CERT-POLICY-QUALIFIER ::= { ... }
```

وقيمة من النمط **معلومات السياسة (PolicyInformation)** تعرّف هوية معلومات الواصف وتنقلها بشأن سياسة شهادة واحدة. وتحتوي المكوّنة **معرف هوية السياسة (policyIdentifier)** على معرف الهوية لسياسية شهادة، بينما تحتوي المكوّنة **واصفات السياسة (policyQualifiers)** على قيم واصفات السياسة لهذا العنصر.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصْدر الشهادة.

إذا كان التوسع موسوماً بأنه حرج، فهو يدل على أن الشهادة يجب ألاّ تستعمل إلا للأغراض وطبقاً للقواعد التي تفرضها واحدة من سياسات الشهادة المبينة. وقد تتطلب قواعد إحدى السياسات الخاصة من نظام استعمال الشهادات أن يعالج قيمة الواصف بأسلوب خاص.

وإذا كان التوسع موسوماً بأنه غير حرج، فإن استعمال هذا التوسع لا يقيّد استعمال الشهادة بالضرورة بالسياسات المعدّدة. ومع ذلك يستطيع مستعمل الشهادة أن يطلب وجود سياسة معينة لكي يستعمل الشهادة (انظر البند 10). ويمكن حسب تقدير مستعمل الشهادة، معالجة واصفات السياسة أو تجاهلها.

ويمكن لأي هيئة أن تحدد أنماطاً، هي تحتاجها، من سياسات الشهادة أو من واصفات سياسات الشهادة. ومعرفات هوية الموضوع المستعملة للتعريف بهذه الأنماط من سياسات الشهادة وواصفات سياسات الشهادة يتم إسنادها وفقاً للتوصية ITU-T X.660 | المعيار ISO/IEC 9834-1. ويمكن لسلطة إصدار الشهادة أن تؤكد على معرف الهوية **أي سياسة (anyPolicy)**، لكي تضع ثقتها في شهادة لجميع السياسات المحتملة. ونظراً إلى الحاجة إلى تطبيق تعريف الهوية على هذه القيمة الخاصة، بصرف النظر عن التطبيق أو البيئة، فإن إسناد هذا المعرّف بهوية الموضوع، وارد في هذه المواصفة ولا يسند في هذه المواصفة أي معرف بهوية الموضوع من أجل سياسات خاصة للشهادة. وهذا الإسناد يقع على مسؤولية الكيان الذي يحدد سياسة الشهادة.

```
anyPolicy       OBJECT IDENTIFIER  ::=          { 2 5 29 32 0 }
```

وينبغي ألا يصحب أي واصف للسياسة المعرف بهوية **أي سياسة (anyPolicy)**.

ويستخدم صنف الموضوع التالي من الترميز ASN.1 في تعريف أنماط واصفات سياسات الشهادة:

```
CERT-POLICY-QUALIFIER ::= CLASS {
    &id                 OBJECT IDENTIFIER UNIQUE,
    &Qualifier          OPTIONAL }
WITH SYNTAX {
    POLICY-QUALIFIER-ID     &id
    [QUALIFIER-TYPE     &Qualifier] }
```

ويجب أن يشتمل تعريف نمط واصف السياسة على:

- إعلان عن المحتوى الدلالي للقيم المحتملة؛
- دلالة عما إذا كان معرّف هوية الواصف يمكن أن يظهر في توسع سياسات الشهادة من دون أن تصحبه قيمة، وأن يظهر معه عندئذ المحتوى الدلالي المتعلق بمثل هذه الحالة.

ملاحظة – يمكن تحديد واصف ما باعتباره نمطاً ما من الترميز ASN.1. يوصى بتوصيف النمط **سلسلة الأثمونات (OCTET STRING)**، عندما يتوقع أن الواصف سيستعمل بصورة أساسية مع تطبيقات ليس لها وظائف فك تشفير في الترميز ASN.1. وترسل عندئذ قيمة سلسلة الإثمونات **(OCTET STRING)** في الترميز ASN.1، قيمةً لواصف مشفرة وفقاً لأي اصطلاح تحدده الهيئة التي تعرّف عنصر السياسة.

7.2.2.8 توسّع تقابلات السياسات

هذا الحقل الذي لا يستعمل إلا لشهادات سلطة إصدار الشهادة، يتيح لمُصْدر الشهادة أن يبيّن أن واحدة من سياسات شهادة المُصْدر يمكن اعتبارها، لأغراض مستعمل مسيرة إصدار شهادة تحتوي على هذه الشهادة، مكافئة لسياسة شهادة أخرى مستعملة في ميدان سلطة الإصدار الصاحبة. ويعرف هذا الحقل كما يلي:

```
policyMappings EXTENSION ::= {
    SYNTAX              PolicyMappingsSyntax
    IDENTIFIED BY       id-ce-policyMappings }

PolicyMappingsSyntax ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
    issuerDomainPolicy      CertPolicyId,
    subjectDomainPolicy     CertPolicyId }
```

تدل المكوّنة **سياسة ميدان المُصْدر (issuerDomainPolicy)** على سياسة شهادة يعترف بها في ميدان سلطة إصدار الشهادة المُصْدرة، ويمكن اعتبارها مكافئة لسياسة الشهادة المبيّنة في المكوّنة **سياسة ميدان الصاحب (subjectDomainPolicy)** التي يعترف بها في ميدان سلطة إصدار الشهادة الصاحبة.

ولا يجري تقابل السياسات مع القيمة الخاصة **لأي سياسة (anyPolicy)**، لا منها ولا إليها.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرجٍ، حسب تقدير مُصْدر الشهادة. ويوصى بأن يكون حرجاً، لأنه في غير ذلك قد لا يستطيع مستعمل الشهادة أن يفسر تفسيراً صحيحاً اشتراط سلطة الإصدار المُصْدرة.

ملاحظة 1 – من أمثلة تقابل السياسات ما يلي. قد يكون لحكومة الولايات المتحدة سياسة تدعى "التجارة مع كندا"، كما قد يكون للحكومة الكندية سياسة تدعى "التجارة مع الولايات المتحدة". وهاتان السياستان محددتان، وهويتاهما معرفتّان بصورة منفصلة، ولكن يمكن أن يحصل اتفاق بين الحكومتين لقبول توسيع مسيرتي إصدار الشهادة إلى ما بعد الحدود، ضمن قواعد تفرضها هاتان السياستان لأغراض معينة.

ملاحظة 2 – يستدعي تقابل السياسات نفقات عامة إدارية مهمة، واشتراك موظفين نشيطين ومخوّلين باتخاذ القرارات المناسبة. ويفضل عامةً الاتفاق على سياسات مشتركة تستخدم على نطاق أوسع، بدلاً من تطبيق تقابل السياسات. ففي المثال السابق، ربما يكون من الأفضل للولايات المتحدة وكندا والبرازيل الاتفاق على سياسة مشتركة للتجارة في أمريكا الشمالية.

ملاحظة 3 – من المتوقع أن يقتصر استعمال تقابل السياسات عملياً، على البيئات المحددة التي تكون إعلانات سياساتها بسيطة جداً.

3.8 توسّعات في معلومات المُصْدر والصاحب

1.3.8 المتطلبات

تتعلق المتطلبات التالية بنعوت مُصْدر الشهادة وصاحبها:

أ) تحتاج الشهادة أن تكون قابلة للاستعمال في تطبيقات، تحمل أشكالاً متنوعة من الأسماء، منها أسماء البريد الإلكتروني على الإنترنت، وأسماء الميادين في الإنترنت، وعناوين المرسل والمستلم X.400، وأسماء الأطراف المشتركة في تبادل المعطيات الإلكتروني (EDI). لذلك يبدو من الضروري أن ترتبط بطريقة مأمونة أسماء متعددة، أشكالها متنوعة، بصاحب شهادة أو بمُصْدر شهادة أو قائمة CRL.

ب) ربما يحتاج مستعمل شهادة أن يعرف بطريقة مأمونة بعض معلومات تعرف الهوية عن صاحب، حتى تتوفر لديه الثقة بأن الصاحب هو الشخص أو الشيء المقصود. فقد تُطْلب مثلاً معلومات مثل العنوان البريدي أو الوظيفة في شركة أو صورة فوتوغرافية. يمكن تمثيل هذه المعلومات بطريقة مناسبة بصفتها نعوتاً في دليل، ولكن هذه النعوت لا تشكّل بالضرورة جزءاً من الاسم المميّز. وعليه يحتاج الأمر إلى وضع حقل في شهادة ينقل نعوت دليل غير النعوت الواردة في الاسم المميّز.

2.3.8 حقول توسع الشهادة والقائمة CRL

تعرّف فيما يلي حقوق التوسع التالية:

أ) *اسم بديل للصاحب؛*

ب) *اسم بديل للمُصْدر؛*

ج) *نعوت الدليل للصاحب.*

لا تستعمل هذه الحقول إلا كتوسّعات للشهادة، ما عدا الاسم البديل للمُصدر الذي يمكن استعماله أيضاً كتوسّع للقائمة CRL. وبصفتها توسعات للشهادة، يمكنها أن توجد في شهادات سلطة إصدار الشهادة وفي شهادات الكيان النهائي.

1.2.3.8 توسع الاسم البديل للصاحب

يحتوي هذا الحقل على اسم بديل واحد أو على أسماء، تستخدم أي شكل من أشكال الأسماء المتنوعة، التي تعود إلى كيان، تربطه سلطة إصدار الشهادة بمفتاح عمومي مصدّق. ويعرّف هذا الحقل كما يلي:

```
subjectAltName EXTENSION ::= {
    SYNTAX              GeneralNames
    IDENTIFIED BY       id-ce-subjectAltName }

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
    otherName                   [0]     INSTANCE OF OTHER-NAME,
    rfc822Name                  [1]     IA5String,
    dNSName                     [2]     IA5String,
    x400Address                 [3]     ORAddress,
    directoryName               [4]     Name,
    ediPartyName                [5]     EDIPartyName,
    uniformResourceIdentifier   [6]     IA5String,
    iPAddress                   [7]     OCTET STRING,
    registeredID                [8]     OBJECT IDENTIFIER }

OTHER-NAME ::= TYPE-IDENTIFIER

EDIPartyName ::= SEQUENCE {
    nameAssigner        [0]     DirectoryString {ub-name} OPTIONAL,
    partyName           [1]     DirectoryString {ub-name} }
```

قيم البدائل في النمط **الاسم العام (GeneralName)** هي أسماء لها الأشكال المتنوعة التالية:

- **الاسم الآخر (otherName)** هو اسم من أي شكل كان، معرّف كمطابق لصنف موضوعات المعلومات **(OTHER-NAME)**؛
- **rfc822Name** هو عنوان بريد إلكتروني على الإنترنت، معرّف طبقاً للطلب RFC 822 في الإنترنت؛
- **dNSName** هو اسم ميدان في الإنترنت، معرّف طبقاً للطلب RFC 1035 في الإنترنت؛
- **x400Address** هو عنوان إرسال/استلام، معرّف طبقاً للتوصية ITU-T X.411 | المعيار ISO/IEC 10021-4؛
- **اسم في الدليل (directoryName)** هو اسم في الدليل، معرّف طبقاً للتوصية ITU-T X.501 | المعيار ISO/IEC 9594-2؛
- **اسم الطرف المشترك في تبادل المعطيات الإلكتروني** (ediPartyName) هو اسم متفق على شكله بين الأطراف المشتركة في *تبادل المعطيات الإلكتروني* (EDI) والراغبة في الاتصال. وتعّرف المكوّنة **مُسْنِد الاسم (nameAssigner)** هوية السلطة التي تسند قيماً وحيدة للأسماء الموجودة في المكوّنة **اسم الطرفَ المشترك (partyName)**؛
- **uniformResourceIdentifier** هو *معرّف هوية المورد المنتظم* لشبكة الويب العالمية (www)، وهو معرّف طبقاً للطلب RFC 1630 في الإنترنت؛
- **iPAddress** هو عنوان في بروتوكول الإنترنت، معرّف طبقاً للطلب RFC 791 في الإنترنت، ويمثل باعتباره سلسلة اثنينية؛
- **registeredID** هو معرّف هوية لأي موضوع مسجّل طبقاً للتوصية ITU-T X.660 | المعيار ISO/IEC 9834-1.

سيكون هناك، لكل شكل اسم مستعمل في نمط **الاسم العام (GeneralName)**، نظام لتسجيل الأسماء، يضمن أن يُعرّف الاسم المستعمل دون لبس هويةَ كيانٍ واحد لمُصْدر الشهادة ولمستعمل الشهادة كليهما.

يمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصْدر الرسالة. ولا يطلب من التنفيذ الذي يعتمد هذا التوسع أن يكون قادراً على معالجة جميع أشكال الأسماء. فإذا كان التوسع موسوماً بأنه حرج، يجب أن يُعترف بواحد على الأقل من أشكال الأسماء الموجودة وأن يُعالج، وإلا يجب أن تعتبر الشهادة غير صالحة. وإلى جانب هذا التقييد السابق، يسمح لنظام استعمال الشهادات أن يتجاهل أي اسم، شكله غير معترف به أو غير معتمد. كما يوصى، نظراً إلى أن حقل الصاحب في الشهادة يحتوي على اسم وارد في الدليل يعرّف الصاحب دون لبس، أن يعتبر هذا الحقل غير حرج.

ملاحظة 1 – يشرح الملحقان A وC بالتوصية ITU-T X.681 | المعيار ISO/IEC 8824-1 استعمال الصنف **معرف هوية النمط (TYPE-IDENTIFIER)**.

ملاحظة 2 – إذا كان حقل هذا التوسع موجوداً، وكان موسوماً بأنه حرج، يمكن أن يحتوي حقل **الصاحب (subject)** في الشهادة اسماً خالياً (أي تتابع طوله صفر من الأسماء المميزة النسبية)، وفي هذه الحالة لا تعرّف هوية الصاحب إلا بالاسم أو بالأسماء الواردة في هذا التوسع.

2.2.3.8 توسّع الاسم البديل للمُصْدر

يحتوي هذا الحقل على اسم بديل واحد أو أكثر لمُصْدر الشهادة أو مُصْدر القائمة CRL، باستخدام أي من أشكال الاسم المختلفة. ويعرّف هذا الحقل كما يلي:

```
issuerAltName EXTENSION ::= {
    SYNTAX              GeneralNames
    IDENTIFIED BY       id-ce-issuerAltName }
```

يمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصْدر الشهادة أو مُصْدر القائمة CRL. ولا يطلب من التنفيذ الذي يعتمد هذا التوسع أن يكون قادراً على معالجة جميع أشكال الأسماء. فإذا كان التوسع موسوماً بأنه حرج، يجب أن يُعترف بواحد على الأقل من أشكال الأسماء الموجودة وأن يُعالج، وإلا يجب أن تعتبر الشهادة أو القائمة CRL غير صالحة. وإلى جانب هذا التقييد السابق، يسمح لنظام استعمال الشهادة أن يتجاهل أي اسم شكله غير معترف به أو غير معتمد. كما يوصى، نظراً إلى أن حقل الصاحب في الشهادة أو في القائمة CRL يحتوي على اسم وارد في الدليل يعرّف سلطة الإصدار دون لبس، أن يعتبر هذا الحقل غير حرج.

ملاحظة – إذا كان حقل هذا التوسع موجوداً، وكان موسوماً بأنه حرج، يمكن أن يحتوي حقل **المُصْدر (issuer)** في الشهادة أو في القائمة CRL اسماً خالياً (أي تتابع طوله صفر من الأسماء المميزة النسبية)، وفي هذه الحالة لا تعرّف هوية المُصْدر إلا بالاسم أو بالأسماء الواردة في هذا التوسع.

3.2.3.8 توسع نعوت الدليل للصاحب

ينقل هذا الحقل أي قيمة نعت في الدليل مرغوبة لصاحب الشهادة. ويُعرَّف هذا الحقل كما يلي:

```
subjectDirectoryAttributes EXTENSION ::= {
    SYNTAX              AttributesSyntax
    IDENTIFIED BY       id-ce-subjectDirectoryAttributes }

AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute
```

يمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصْدر الشهادة. ولا يطلب من نظام استعمال الشهادات الذي يعالج هذا التوسع أن يفهم جميع أنماط النعوت الموجودة في هذا التوسع. وإذا كان التوسع موسوماً بأنه حرج، يجب أن يكون واحد على الأقل من أنماط النعوت التي يحتوي عليها هذا التوسع مفهوماً من الشهادة، حتى تتقبّله. وإذا كان التوسع موسوماً بأنه حرج، ولم يُفهم أي واحد من أنماط النعت المحتواة، تُرفض الشهادة.

وإذا كان التوسع موجوداً في شهادة مفتاح عمومي، فقد تكون بعض التوسعات المعرّفة في البند 15، موجودة أيضاً.

4.8 التوسعات في تقييدات مسيرة إصدار الشهادة

1.4.8 المتطلبات

من أجل معالجة مسيرة إصدار الشهادة:

أ) يتعين أن تكون شهادات الكيان النهائي متمايزة عن شهادات سلطة إصدار الشهادة، لكي تُمْنع بعض الكيانات النهائية من أن تجعل من نفسها سلطات إصدار، من دون ترخيص لها بذلك. ويجب أن يكون لسلطة إصدار الشهادة القدرة على الحدّ من طول السلسلة اللاحقة الناتجة عن سلطة إصدار صاحبة مصدّق عليها، أي الاقتصار على شهادة واحدة تالية فقط أو على شهادتين تاليتين فقط.

ب) يتعين أن تكون سلطة إصدار الشهادة قادرة على فرض قيود تتيح لمستعمل الشهادة أن يتحقق من أن سلطات إصدار الشهادة، غير الموثوق بها كثيراً، الموجودة في مسيرة إصدار الشهادة (أي سلطات الإصدار الواقعة في مسيرة الإصدار بعد سلطة إصدار الشهادة التي يبدأ منها المفتاح العمومي لمستعمل الشهادة)، لا تنتهك الثقة بها بإصدارها شهادات إلى أصحاب ينتمون إلى مكان أسماء غير مناسب. ويجب أن يكون مستعمل الشهادة قادراً على التحقق أوتوماتياً من التقيد بهذه القيود.

ج) يجب أن تنفّذ معالجة مسيرة إصدار الشهادة في وحدة مؤتمتة مستقلة ذاتياً، وهذا ضروري لكي يتيح تنفيذ وحدات برمجية أو عتادية موثوقة تؤدي وظائف معالجة مسيرة إصدار الشهادة.

د) ينبغي أن يكون من الممكن تنفيذ معالجة مسيرة الإصدار، بصورة مستقلة عن أي تدخل من المستعمل المحلي في الوقت الفعلي.

هـ) ينبغي أن يكون من الممكن تنفيذ معالجة مسيرة الإصدار، من دون الاعتماد على استعمال قواعد معطيات محلية موثوقة بشأن معلومات وصف السياسة. (بعض المعلومات المحلية الموثوقة – مثل المفتاح العمومي الأولي – لازمة لمعالجة مسيرة إصدار الشهادة، ولكن مقدار مثل هذه المعلومات ينبغي أن يبقى في حدوده الدنيا).

و) يجب أن تكون مسيرات إصدار الشهادة قادرة على العمل في بيئات معترف فيها بسياسات شهادة متعددة. يجب أن تكون سلطة إصدار الشهادة قادرة على أن تشترط، ما هي سلطات إصدار الشهادة الواقعة في ميادين أخرى والتي تثق بها ولأي أغراض. ويجب اعتماد التسلسل في ميادين السياسة المتعددة.

ز) المرونة الكاملة مطلوبة في النموذجات الثقات. والنموذج التراتبي الصارم الوافي في حالة هيئة معينة، لا يكون وافياً في حالة مشروعات متعددة مترابطة ببعضها. والمرونة ضرورية أيضاً عند اختيار سلطة الإصدار الأولى الموثوقة في مسيرة إصدار الشهادة. يجب أن يكون من الممكن بشكل خاص النص على أن تنطلق مسيرة الإصدار من الميدان الأمني المحلي للنظام المستعمل للمفتاح العمومي.

ح) يجب ألا تكون بنى التسميات خاضعة لقيود استعمال الأسماء في الشهادات. وبعبارة أخرى يجب ألا تكون بنى الأسماء في الدليل، التي تعتبر طبيعية بالنسبة إلى بعض المنظمات أو المناطق الجغرافية، مضطرة للتكيف حتى تلبي اشتراطات سلطة الإصدار.

ط) يجب أن تكون مجالات وسّع الشهادات متوائمة إلى الخلف مع نظام مقاربة مسيرة الإصدار غير المقيّد، كما هو محدد في طبعات سابقة للتوصية بالتوصية ITU-T X.509 | المعيار ISO/IEC 9594-8.

ي) يتعين أن تكون سلطة إصدار الشهادة قادرة على حظر استخدام تقابل السياسات وعلى اشتراط وجود معرفات هوية صريحة لسياسة الشهادة في الشهادات اللاحقة من مسيرة إصدار الشهادة.

ملاحظة – تتطلب معالجة مسيرة إصدار الشهادة، في أي نظام لاستعمال الشهادات، سوية مناسبة من الضمان. وتحدد مواصفة الدليل هذه وظائف يمكن استعمالها في تطبيقات يطلب منها أن تكون مطابقة لإعلانات ضمان معينة. فقد

يتطلب اشتراط ضمان مثلاً، أن تكون معالجة مسيرة إصدار الشهادة محميّة من تلاعب في العملية (مثل تلاعب في البرمجيات أو تعديل في المعطيات). ويجب أن تكون سوية الضمان متناسبة مع المخاطرة التجارية. فمثلاً:

- من الممكن أن تطلب معالجة داخلية، تقوم بها وحدة تجفير مناسبة، من أجل المفاتيح العمومية المستعملة لإقرار صلاحية تحويل أموال مبالغها طائلة؛
- بينما قد تكون المعالجة البرمجية مناسبة، للطلبات التي تجري من المنزل عن حالة الحساب المصرفي.

وعليه، ينبغي أن تكون وظائف معالجة مسيرة إصدار الشهادة مناسبة للتنفيذ في وحدات عتادية مجفّرة أو في إذنات مجفّرة، هذا كمثال.

ك) يجب أن تكون سلطة إصدار الشهادة قادرة على أن تمنع من اعتبار القيمة الخاصة "أي سياسة" سياسةً صالحة في الشهادات اللاحقة في مسيرة إصدار الشهادة.

2.4.8 حقول توسّع الشهادة

تعرّف حقول التوسّع التالية:

أ) *التقييدات الأساسية؛*

ب) *تقييدات الأسماء؛*

ج) *تقييدات السياسة؛*

د) *حظر "أي سياسة".*

لا تستعمل حقول التوسع هذه إلا باعتبارها توسعات شهادة. ولا تستعمل تقييدات الأسماء وتقييدات السياسة إلا في شهادات سلطة إصدار الشهادة، بينما يمكن استعمال التقييدات السياسية في شهادات الكيان النهائي. ويعطي الملحق G أمثلة من استعمال هذه التوسعات.

1.2.4.8 توسع التقييدات الأساسية

يبين هذا الحقل إن كان يمكن للصاحب أن يتصرف وكأنه سلطة إصدار، مع كون المفتاح العمومي المصدّق عليه مستعملاً للتحقق من توقيعات الشهادة. وفي هذه الحالة يمكن أيضاً تعيين تقييد الطول لمسيرة إصدار الشهادة. ويعرّف هذا الحقل كما يلي:

```
basicConstraints EXTENSION ::= {
    SYNTAX              BasicConstraintsSyntax
    IDENTIFIED BY       id-ce-basicConstraints }

BasicConstraintsSyntax ::= SEQUENCE {
    cA                      BOOLEAN DEFAULT FALSE,
    pathLenConstraint       INTEGER (0..MAX) OPTIONAL }
```

وتبين المكونة **cA** إن كان المفتاح العمومي المصدّق يمكن استعماله للتحقق من توقيعات الشهادة.

ولا توجد المكوّنة **تقييد طول المسيرة (pathLenConstraint)** إلا إذا كانت المكونة **cA** موضوعة على "صائبة". وهي تعطي أقصى عدد من شهادات سلطة إصدار الشهادة التي يسمح لها بأن تلي هذه الشهادة في مسيرة إصدار الشهادة. والقيمة صفر تدل على أن لصاحب هذه الشهادة أن يصدر شهادات للكيانات النهائية فقط، وليس لسلطات إصدار الشهادة الأخرى. أما إذا لم يظهر الحقل **تقييد طول المسيرة** في أي شهادة في مسيرة إصدار الشهادات، فلا يعود يوجد حدّ للطول المسموح في مسيرة إصدار الشهادة. ويأخذ التقييد مفعوله بدءاً من الشهادة التالية في المسيرة. ويقيّد هذا التقييد طول المقطع من مسيرة إصدار الشهادة الواقع ما بين الشهادة التي تحتوي على هذا التوسع وشهادة الكيان النهائي. وليس له أي تأثير على عدد شهادات سلطة إصدار الشهادة الموجودة في مسيرة الإصدار ما بين مرسّخة الثقة والشهادة التي تحتوي على هذا التوسع. وبذلك يمكن لطول كامل مسيرة إصدار الشهادة أن يتجاوز الطول الأعظم للمقطع الذي يقيّده هذا التوسع. ويتحكم التقييد

في عدد شهادات سلطة إصدار الشهادة غير الصادرة لذاتها الواقعة ما بين شهادة سلطة إصدار الشهادة التي تحتوي على هذا التقييد وشهادة الكيان النهائي. وهكذا يمكن لكامل طول هذا المقطع من المسيرة، باستبعاد الشهادات الصادرة لذاتها، أن يتجاوز قيمة هذا التقييد بما يعادل شهادتين على الأكثر. (وهذا يشمل الشهادتين الموجودتين في النقطتين الطرفيتين للمقطع، مضافاً إليهما شهادات سلطة إصدار الشهادة الواقعة بين النقطتين الطرفيتين التي تكون مقيدة بقيمة هذا التوسع).

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصْدر الشهادة. ويوصى بأن يوسم بأنه حرج، وإلا فإن الكيان غير المرخص له بأن يكون سلطة إصدار الشهادة، يمكنه أن يصدر شهادات، يقوم نظام استعمال الشهادات باستعمالها سهواً وعن غير قصد.

إذا كان هذا التوسع موجوداً وموسوماً بأنه حرج، أو موسوماً بأنه غير حرج ولكن نظام استعمال الشهادة يعترف به، عندئذ:

- إذا كانت قيمة **cA** غير موضوعة على "صائبة"، يجب عدم استعمال المفتاح العمومي المصدّق للتحقق من توقيع الشهادة؛
- إذا كانت قيمة **cA** موضوعة على "صائبة"، وكان **تقييد طول المسيرة** موجوداً على نظام استعمال الشهادات أن يتحقق من كون مسيرة إصدار الشهادة الجارية معالجتها متّسقةً مع قيمة تقييد طول المسيرة.

ملاحظة 1 – إذا كان التوسع غير موجود، وكان موسوماً بأنه غير حرج، وكان نظام استعمال الشهادة لا يعترف به، يجب اعتبار الشهادة كأنها شهادة كيان نهائي، ولا يمكن استعمالها للتحقق من توقيعات الشهادات.

ملاحظة 2 – لتقييد صاحب شهادة بأن يكون فقط كياناً نهائياً، أي ليس سلطة إصدار الشهادة، يستطيع مُصْدر الشهادة أن يضمن حقل هذا التوسع قيمة **للتتابع (SEQUENCE)** تكون خالية.

2.2.4.8 توسّع تقييدات الأسماء

يدل هذا الحقل الذي يجب ألا يستعمل إلا في شهادة سلطة إصدار الشهادة، على مكان أسماء يجب أن تقع فيه جميع أسماء الصاحب الواردة في الشهادات اللاحقة في مسيرة إصدار الشهادة. ويعرّف هذا الحقل كما يلي:

```
nameConstraints EXTENSION ::= {
    SYNTAX          NameConstraintsSyntax
    IDENTIFIED BY       id-ce-nameConstraint }

NameConstraintsSyntax ::= SEQUENCE {
    permittedSubtrees       [0]   GeneralSubtrees OPTIONAL,
    excludedSubtrees        [1]   GeneralSubtrees OPTIONAL,
    requiredNameForms       [2]   NameForms OPTIONAL  }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
    base                    GeneralName,
    minimum  [0]   BaseDistance DEFAULT 0,
    maximum [1]   BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)
NameForms  ::= SEQUENCE {
    basicNameForms    [0]   BasicNameForms OPTIONAL,
    otherNameForms    [1]   SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER OPTIONAL }
(ALL EXCEPT ({ -- none; i.e., at least one component shall be present -- }))
                        -- لا شيء، يجب أن توجد مكوّنة واحدة على الأقل --
BasicNameForms  ::= BIT STRING {
    rfc822Name                  (0),
    dNSName                     (1),
    x400Address                 (2),
    directoryName               (3),
    ediPartyName                (4),
    uniformResourceIdentifier   (5),
    iPAddress                   (6),
    registeredID                (7) }  (SIZE (1..MAX))
```

وإذا كانت المكوّنتان **الأشجار الفرعية المسموحة (permittedSubtrees)** و**الأشجار الفرعية المستبعدة (excludedSubtrees)** موجودتين، تحدد كل منهما شجرة تسمية فرعية واحدة أو أكثر، يعرّف كلاً منها اسم جذر الشجرة الفرعية، واختيارياً منطقة داخل الشجرة الفرعية تحدَّها طبقتان فرعيتان علوية و/أو سفلية. وإذا كانت المكوّنة **الأشجار الفرعية المستبعدة** موجودة، لا تقبل أي شهادة صادرة عن سلطة إصدار الشهادة الصاحبية أو عن سلطات الإصدار اللاحقة في مسيرة إصدار الشهادة التي يكون لها اسم صاحب وارد في هذه الأشجار الفرعية. وإذا كانت أمكنة الأسماء تتشابك، تكون الأولوية لإعلان استبعاد الأسماء الموجودة داخل التشابك. وإذا كانت مكوّنتا الأشجار الفرعية المسموحة والمستبعدة محددتين لشكل معين من السماء، يُقبل أي اسم واقع داخل هذا الشكل المعيّن من الأسماء. وإذا كانت المكوّنة **أشكال الأسماء المطلوبة (requiredNameForms)** موجودة، يجب أن تحتوي جميع الشهادات اللاحقة في مسيرة إصدار الشهادة على اسم له واحد على الأقل من أشكال الأسماء المطلوبة.

وإذا كانت المكوّنة **الأشجار الفرعية المسموحة (permittedSubtrees)** موجودة، يطبق التالي على جميع الشهادات اللاحقة في المسيرة. وإذا كانت أي واحدة من الشهادات تحتوي على اسم صاحب (في حقل **الصاحب (subject)**) أو في توسيع **الأسماء البديلة للصاحب (subjectAltNames)**، له شكل اسم محددةٍ له الأشجار الفرعية المسموحة، يجب أن يقع الاسم داخل واحدة على الأقل من الأشجار الفرعية المحددة. وإذا كانت أي واحدة من الشهادات تحتوي على أسماء صاحب، لها أشكال أسماء غير الأشكال المحددة لها الأشجار الفرعية المسموحة، لا يطلب من أسماء الصاحب أن تقع داخل أي واحدة من الأشجار الفرعية المحددة. لنفرض مثلاً أن شجرتين فرعيتين مسموحتين هما محددتان، إحداهما لشكل الاسم في الدليل (DN)، والأخرى لشكل الاسم في الطلب rfc822، لا يتم تحديد أشجار فرعية مستبعدة، ولكن المكوّنة **أشكال الأسماء المطلوبة (requiredNameForms)** تُحدّد مع وجود البتة **الاسم في الدليل (directoryName)** والبتة في الطلب rfc822Name. وكل شهادة لا تحتوي إلا أسماء هي غير الاسم في الدليل أو الاسم في الطلب rfc822، تكون غير مقبولة. وإذا كانت المكوّنة **أشكال الأسماء المطلوبة** غير محددة، تقبل مع ذلك مثل هذه الشهادة. ولنفرض مثلاً أن شجرتين فرعيتين مسموحتين هما محددتان، إحداهما لشكل الاسم في الدليل (DN) والأخرى لشكل الاسم في الطلب rfc822، لا يتم تحديد أشجار فرعية مستبعدة، ولا تكون مكوّنة **أشكال الأسماء المطلوبة** موجودة. والشهادة التي تحتوي فقط على اسم DN، ويكون هذا الاسم DN واقعاً في شجرة فرعية مسموحة محددة، تكون شهادة مقبولة. والشهادة التي تحتوي على كلا الاسمين، الاسم في الدليل (DN) والاسم في الطلب rfc822، ويكون واحد منهما فقط واقعاً في الشجرة الفرعية المسموحة المحددة التي تخصه، تكون شهادة مقبولة. والشهادة التي تحتوي فقط على أسماء هي غير الاسم DN أو الاسم rfc822 تكون أيضاً مقبولة.

ملاحظة – هذا المثال معروض لأغراض التوضيح فقط. ولا تدخل في نطاق هذه التوصية|هذا المعيار الدولي، معالجة الأسماء الواردة في أشكال أسماء النمط **الاسم العام (GeneralName)**، باستثناء شكل **الاسم في الدليل (directoryName)**، في بنيتها التراتبية.

وإذا كانت المكوّنة **الأشجار الفرعية المستبعدة (excludedSubtrees)** موجودة، فأي شهادة صادرة عن سلطة إصدار الشهادة الصاحبة أو عن سلطات الإصدار اللاحقة في مسيرة إصدار الشهادة، وتحتوي على اسم صاحب (في حقل **الصاحب (subject)** أو في توسع **الأسماء البديلة للصاحب (subjectAltNames)**)، واقع داخل هذه الأشجار الفرعية، تكون شهادة غير مقبولة. لنفرض مثلاً أن شجرتين فرعيتين مستبعدتين هما محددتان، إحداهما لشكل الاسم DN والأخرى لشكل الاسم rfc822. فالشهادة التي تحتوي فقط على اسم DN واقع داخل شجرة فرعية مستبعدة محددة، تكون غير مقبولة. والشهادة التي تحتوي على كلا شكلي الاسمين DN وrfc822، ويكون واحد منهما على الأقل واقعاً داخل الشجرة الفرعية المستبعدة المحددة الخاصة به، تكون غير مقبولة.

وعندما يكون لصاحب شهادة أسماء عديدة من نفس شكل الاسم (بما في ذلك، في حالة شكل الاسم **الاسم في الدليل (directoryName)**، الاسم في حقل الصاحب من الشهادة، إن كان خالياً)، يجب عندئذ اختيار جميع هذه الأسماء لمعرفة ما إذا كانت متسقة مع تقييد الاسم لهذا الشكل من الأسماء.

وإذا كانت المكوّنة **أشكال الأسماء المطلوبة (requiredNameForms)** موجودة، يجب أن تحتوي جميع الشهادات اللاحقة في مسيرة إصدار الشهادات على اسم صاحب يكون واحداً على الأقل من أشكال الأسماء المطلوبة.

لا يمكن أن يستعمل من أشكال الأسماء المتيسرة في نمط **الاسم العام (GeneralName)**، إلا أشكال الأسماء التي لها بنية تراتبية معرفة تماماً في مجالي **الأشجار الفرعية المسموحة (permittedSubtrees)** و**الأشجار الفرعية المستبعدة (excludedSubtrees)**. ويلبي هذا المطلب شكل **الاسم في الدليل (directoryName)**. وعندما يستعمل شكل الاسم هذا، تكون هناك شجرة تسمية فرعية تقابل شجرة فرعية في شجرة معلومات الدليل (DIT).

والحقل الأصغر يعيّن الحدّ العلوي للمنطقة الواقعة داخل الشجرة الفرعية. وجميع الأسماء التي تقع مكوّنة الاسم النهائية فيها فوق هذه السوية المحددة، تكون غير محتواة في هذه المنطقة. وقيمة الصفر (القيمة بالتغيب) **للحقل الأصغر** هي التي تُقابل القاعدة، أي تُقابل العقدة الذروية للشجرة الفرعية، فإذا كان قيمة **الحق الأصغر** تساوي الواحد مثلاً، تكون شجرة التسمية الفرعية تستبعد عقدة القاعدة، ولكنها تضم العقد التابعة لها.

والحقل الأعظم يعيّن الحدّ السفلي للمنطقة الواقعة داخل الشجرة الفرعية. وجميع الأسماء التي تقع مكونتها الأخيرة تحت السوية المحددة، تكون غير محتواة في هذه المنطقة. وقيمة الصفر **للحقل الأعظم** هي حتى تقابل القاعدة، أي تقابل ذروة الشجرة الفرعية. وغياب مكوّنة **الحقل الأعظم** يدل على انه ينبغي ألا يفرض حدّ سفلي للمنطقة الواقعة داخل الشجرة الفرعية. فإذا كانت قيمة **الحقل الأعظم** تساوي الواحد مثلاً، تكون شجرة التسمية الفرعية تستبعد جميع العقد، ما عدا قاعدة الشجرة الفرعية والعقد التابعة لها مباشرة.

فيما يخص شكل **الاسم في الدليل (directoryName)**، تعتبر **الشهادة (certificate)** تابعة **للقاعدة (base)** (وبالتالي فهي مرشحة لتكون داخل الشجرة الفرعية)، إن كان **تتابع (SEQUENCE)** الأسماء المميّزة النسبية (RDN) الذي يشكل الاسم المميز (DN) الكامل في القاعدة، مطابقاً **للتتابع (SEQUENCE)** الأولي لنفس العدد من الأسماء RDN التي تشكل الجزء الأول من الاسم المميز (DN) في حقل **الصاحب (subject)** من **الشهادة (certificate)**. وقد يكون للاسم المميز الموجود في حقل **الصاحب** من **الشهادة**، ذَيْلِيَّة إضافية من الأسماء RDN في تتابعه لا تظهر في الاسم المميز في **القاعدة**. وتُستعمل قاعدة المواءمة **مواءمة الاسم المميز (distinguishedNameMatch)** لمقارنة قيمة **القاعدة** بالتتابع الأولي من الأسماء RDN في **الاسم المميز** الموجود في حقل **الصاحب** من الشهادة.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرجن حسب تقدير مُصْدر الشهادة. ويوصى بأن يوسم حرجاً، وإلا فإن مستعمل الشهادة قد لا يتحقق من أن الشهادات اللاحقة في مسيرة إصدار الشهادة، واقعة في مكان الأسماء الذي تقصده سلطة إصدار الشهادة المُصْدرة.

ولا يطلب من التطبيقات المطابقة أن تعترف بالضرورة بجميع أشكال الأسماء الممكنة.

إذا كان التوسع موجوداً، وكان موسوماً بأنه حرج، يجب على التنفيذ الذي يستعمل الشهادة أن يعترف ويعالج جميع أشكال الأسماء التي يكون لها بنفس الوقت مواصفة شجرة فرعية (مسموحة أو مستبعدة) في التوسع، وقيمة مقابلة في حقل **الصاحب** أو في التوسع **الأسماء البديلة للصاحب (subjectAltNames)** لأي شهادة لاحقة في مسيرة إصدار الشهادة. وإذا ظهر في شكل اسم غير معترف به في نفس الوقت في مواصفة شجرة فرعية وفي شهادة لاحقة، تعالج هذه الشهادة، كما لو صودف توسع حرج غير معترف به. وإذا وقع أي اسم صاحب شهادة داخل شجرة فرعية مستبعدة، تكون الشهادة غير مقبولة. وإذا كانت شجرة فرعية معيّنة لشكل اسم غير محتوى في شهادة لاحقة، يمكن تجاهل هذه الشجرة الفرعية. وإذا كانت المكوّنة **أشكال الأسماء المطلوبة (requiredNameForms)** تعيّن فقط أشكال أسماء غير معترف بها، يجب أن تعالج هذه الشهادة كما لو صودف توسع حرج غير معترف به. وفي الحالات الأخرى، يجب أن يظهر واحد على الأقل من أشكال الأسماء المعترف بها، في جميع الشهادات اللاحقة الموجودة في المسيرة.

وإذا كان التوسع موجوداً، وكان موسوماً بأنه غير حرج، وكان التنفيذ الذي يستعمل الشهادة لا يعترف بشكل الاسم المستعمل في مكوّنة **القاعدة (base)**، يمكن عندئذ تجاهل مواصفة هذه الشجرة الفرعية. وإذا كان التوسع موسوماً بأنه غير حرج، وكان التنفيذ الذي يستعمل الشهادة لا يعترف بأي واحد من أشكال الأسماء المحددة في المكوّنة **أشكال الأسماء المطلوبة (requiredNameForms)**، تعامل الشهادة عندئذ وكأن مكوّنة **أشكال الأسماء المطلوبة كانت غائبة**.

يلاحظ في بعض الحالات أن النتائج المطلوب إنجازها تتطلب من سلطة إصدار الشهادة أن تصدر أكثر من شهادة واحدة إلى سلطة أخرى لإصدار الشهادة، بسبب تعارض المتطلبات الناجمة عن تقييد الأسماء. ولنفرض مثلاً أن للشركة Acme، عشرين فرعاً في الولايات المتحدة.

وأن الشركة Widget ترغب في إصدار شهادة متقاطعة مع سلطة إصدار الشهادة المركزية في شركة Acme، ولكنها تريد من جماعة Widget أن تستعمل شهادات Acme للأصحاب الذين ينطبق عليهم المعياران التاليان:

- من الفرع 1 إلى الفرع 19 من الشركة Acme، تُقبل جميع الأقسام كأصحاب؛
- في الفرع 20 من الشركة Acme، تكون جميع الأقسام غير مقبولة كأصحاب، ما عدا قسم المشتريات.

يمكن تحقيق ذلك بإصدار شهادتين كالتالي: يكون في الشهادة الأولى مجال **للأشجار الفرعية المسموحة (permittedSubtrees)** فيه {القاعدة: C=US، وO=Acme}، ومجال **للأشجار الفرعية المستبعدة (excludedSubtrees)** فيه {القاعدة: C=US، وO=Acme، والفرع OU=20}. ويكون في الشهادة الثانية مجال **للأشجار الفرعية المسموحة (permittedSubtrees)** فيه {القاعدة: C=US، O=Acme، الفرع OU=20 والمشتريات =OU}.

ويحتوي الملحق G على أمثلة من استعمال توسع تقييدات الأسماء.

3.2.4.8 توسّع تقييدات السياسة

يحدد هذا الحقل التقييدات التي ربما تتطلب تعريفاً صريحاً بهوية سياسة الشهادة، أو ربما تحظر تقابل السياسات لما تبقّى من مسيرة إصدار الشهادة. ويعرّف هذا الحقل كما يلي:

```
policyConstraints EXTENSION ::= {
    SYNTAX              PolicyConstraintsSyntax
    IDENTIFIED BY       id-ce-policyConstraints }

PolicyConstraintsSyntax ::= SEQUENCE {
    requireExplicitPolicy       [0]   SkipCerts OPTIONAL,
    inhibitPolicyMapping        [1]   SkipCerts OPTIONAL }

SkipCerts ::= INTEGER (0..MAX)
```

إذا كانت المكوّنة **طلب سياسة صريحة (requireExplicitPolicy)** موجودة، وكانت مسيرة إصدار الشهادة تشمل شهادة صادرة عن سلطة إصدار للشهادة مسمّاة، يجب على جميع الشهادات الموجودة في المسيرة أن تحتوي على معرف هوية للسياسة مقبول، في توسّع سياسات الشهادة. ومعرف هوية السياسة المقبول هو معرف هوية لسياسة شهادة يتطلبه مستعمل مسيرة إصدار الشهادة، أو هو معرف هوية سياسة، كان قد أُعلن عنها مكافئةً لواحدة من تلك السياسات عبر تقابل السياسات، أو هو القيمة الخاصة *أي سياسة (any-policy)*. وسلطة إصدار الشهادة المسمّاة هي إما سلطة إصدار الشهادة المُصْدرة للشهادة الحاوية على هذا التوسع (إن كانت قيمة المكوّنة **طلب سياسة صريحة** تساوي الصفر)، وإما سلطة إصدار الشهادة المُصْدرة للشهادة التالية في مسيرة إصدار الشهادة (المبينة بقيمة لا تساوي الصفر).

وإذا كانت المكوّنة **حظر تقابل السياسات (inhibitPolicyMapping)** موجودة، فهي تدل على أن تقابل السياسات ممنوع في جميع الشهادات التي تبدأ من سلطة إصدار الشهادة المسمّاة في مسيرة إصدار الشهادة وتنتهي بنهاية هذه المسيرة. وسلطة إصدار الشهادة المسمّاة هي إما سلطة إصدار الشهادة الصاحبة للشهادة الحاوية على هذا التوسع (إن كانت قيمة المكوّنة **حظر تقابل السياسات** تساوي الصفر)، وإما سلطة إصدار الشهادة الصاحبة للشهادة التالية في مسيرة إصدار الشهادة (المبينة بقيمة لا تساوي الصفر).

وقيمة النمط **الشهادات المفوَّتة (المتجاهلة) (SkipCerts)** تدل على عدد الشهادات الموجودة في مسيرة إصدار الشهادة والمطلوب تفويتها (تجاهلها) قبل أن يبدأ مفعول تقييدٍ ما.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصدر الشهادة. ويوصى بأن يوسم حرجاً، وإلا فإن مستعمل الشهادة قد لا يفسر تفسيراً صحيحاً اشتراط سلطة إصدار الشهادة المُصدرة.

4.2.4.8 توسّع حظر "أي سياسة"

يحدد هذا الحقل تقييداً يدل على أن القيمة الخاصة "أي سياسة" لا تعتبر تقابلاً صريحاً مع سياسات أخرى للشهادة، فيما يخص جميع الشهادات الصادرة لغير ذاتها في مسيرة إصدار الشهادة بدءاً من سلطة إصدار مسماة. وسلطة إصدار الشهادة المسمّاة هي إما سلطة إصدار الشهادة الصاحبة للشهادة الحاوية على هذا التوسع (إن كانت قيمة المكونة **حظر "أي سياسة"** تساوي الصفر)، وإما سلطة إصدار الشهادة الصاحبة للشهادة التالية في مسيرة إصدار الشهادة (المبينة بقيمة لا تساوي الصفر).

```
inhibitAnyPolicy        EXTENSION   ::= {
    SYNTAX              SkipCerts
IDENTIFIED BY           id-ce-inhibitAnyPolicy }
```

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصدر الشهادة. ويوصى بأن يوسم حرجاً، وإلا فإن مستعمل الشهادة قد لا يفسر تفسيراً صحيحاً اشتراط سلطة إصدار الشهادة المُصْدرة.

5.8 التوسعات في القائمة الأساسية لإبطال الشهادة (CRL)

1.5.8 المتطلبات

ترتبط المتطلبات التالية بالقوائم CRL:

أ) يحتاج مستعملو الشهادات أن يكونوا قادرين على تتبّع جميع قوائم الإبطال CRL الصادرة عن مُصْدر القوائم CRL أو عن نقاط توزيع القوائم CRL (انظر الفقرة 6.8)، وعلى كشف غياب قائمة ما CRL من التتابع، لذلك لا بد من وجود أرقام تتابع للقوائم CRL.

ب) قد يرغب بعض مستعملي القوائم CRL في أن يستجيبوا استجابة مختلفة للإبطال، تبعاً لدواعي الإبطال، لذلك لا بد من وجود حقل في القائمة CRL يبين داعي الإبطال.

ج) يحتاج الأمر إلى سلطة قادرة على أن تعلّق صلاحية شهادة تعليقاً مؤقتاً، وفيما بعد تبطلها لاحقاً أو تعيد صلاحيتها إليها، ومن الأسباب التي تدعو إلى مثل هذا الإجراء:

- الرغبة في الحدّ من المسؤوليات في حالة إبطال خاطئ غير مستيقن، لا توجد معلومات وافية للتأكد من كونه صالحاً؛
- حاجات أعمال أخرى، مثل الإيقاف المؤقت لنشاط شهادة كيان ما، بانتظار تدقيق أو تحقيق جاريين.

د) تحتوي قائمة الإبطال CRL التاريخ الذي أرسلت السلطة فيه إبطال كل شهادة لوحدها. وكذلك بعض المعلومات التي ربما تكون معروفة، مثل متى حدث تعرّض المفتاح للخطر الفعلي أو المتوقع، والتي قد يعتبرها مستعمل الشهادة ذات أهمية خاصة. لا يكفي تاريخ الإبطال لحل بعض المنازعات لأنه يجب، في أسوأ الحالات، اعتبار جميع التوقيعات الصادرة أثناء فترة الصلاحية توقيعات غير صالحة. ومع ذلك يمكن أن يعتبر احد المستعملين أن من المهم الاعتراف بصلاحية وثيقة موقعة، وإن كان المفتاح الذي استعمل لتوقيعها قد تعرض للخطر بعد حصول التوقيع. وللمساعدة على حلّ هذا الإشكال، يمكن لقائمة الإبطال CRL أن تتضمن حقلاً يحتوي على تاريخ ثانٍ، يبين متى ثبت تعرّض المتاح الخاص للخطر أو متى اشتبه في ذلك.

هـ) يحتاج مستعملو الشهادات أن يستطيعوا جمع معلومات إضافية من القائمة CRL بالذات، بشأن مجال تطبيق الشهادات الواردة في هذه القائمة، وترتيب التبليغات عن الإبطال، وتقاطر القوائم CRL الذي يكون فيه رقم القائمة CRL وحيداً.

و) يحتاج المُصْدرون أن يكونوا قادرين على تغيير تجزئة القوائم CRL بصورة مستمرة، وإحالة مستعملي الشهادات على المواقع الجديدة للقوائم CRL المعنية عند كل تغيير في التجزئة.

ز) يمكن توفير قوائم دلتا CRL من أجل تحيين قاعدة أساسية معنية للإبطال CRL. ويجب أن يكون مستعملو الشهادات في وضع يمكّنهم من أن يعيّنوا، انطلاقاً من قائمة CRL معينة، إن كانت القوائم دلتا CRL متوفرة، وأين يجدونها، ومتى ستصدر القوائم دلتا CRL القادمة.

ح) إضافة إلى نشر القوائم CRL تبليغات بالشهادات التي جرى إبطالها، يطلب أيضاً نشر تبليغات بالشهادات التي سيجري إبطالها في المستقبل اعتباراً من تاريخ ووقت معيّنين.

ط) يطلب إيجاد وسائل أكثر فعالية، تبيّن في قائمة CRL مجموعة الشهادات التي جرى إبطالها.

2.5.8 حقول التوسع في القائمة CRL وفي مداخل القائمة CRL

تحدّد حقول التوسع التالية:

أ) *رقم القائمة CRL؛*

ب) *شفرة الداعي؛*

ج) *شفرة تعليمات الوضع في الانتظار؛*

د) *تاريخ عدم الصلاحية؛*

ه) *مجال تطبيق القائمة CRL؛*

و) *مرجع الوضع القانوني؛*

ز) *معرف هوية تقاطر القوائم CRL؛*

ح) *قائمة مرتّبة؛*

ط) *معلومات دلتا.*

ويجب ألا تستعمل الحقول التالية: رقم القائمة CRL، ومجال تطبيق القائمة CRL، ومرجع الوضع القانوني، ومعرف هوية تقاطر القوائم CRL، والقائمة المرتّبة، ومعلومات دلتا إلا كحقول توسع في القائمة CRL، بينما يجب ألا تستعمل الحقول الأخرى إلا كحقول توسع في مداخل القائمة CRL.

1.2.5.8 توسع رقم القائمة CRL

ينقل حقل التوسع هذا في القائمة CRL رقم تتابع متزايداً بانتظام إلى كل قائمة CRL صادرة عن مُصدر قائمة CRL معين عن طريق نعت سلطة معينة في الدليل أو نقطة توزيع القوائم CRL. وهو يسمح لمستعمل القائمة CRL أن يكتشف إن كان قد جرى أيضاً استلام ومعالجة قوائم CRL صادرة قبل القائمة CRL الجارية معالجتها. ويعرّف هذا الحقل كما يلي:

```
cRLNumber EXTENSION ::= {
    SYNTAX              CRLNumber
    IDENTIFIED BY       id-ce-cRLNumber }

CRLNumber ::= INTEGER (0..MAX)
```

ويكون هذا التوسع غير حرج دائماً.

2.2.5.8 توسع شفرة الداعي

يعرّف حقل التوسع هذا في مدخل القائمة CRL بهوية الداعي إلى إبطال الشهادة. ويمكن للتطبيقات أن تستعمل شفرة الداعي لكي تقرر كيف سترد على الإبطالات المرسلة، استناداً إلى سياساتها المحلية. ويعرف هذا الحقل كما يلي:

```
reasonCode EXTENSION ::= {
    SYNTAX              CRLReason
    IDENTIFIED BY       id-ce-reasonCode }
```

```
CRLReason ::= ENUMERATED {
    unspecified             (0),
    keyCompromise           (1),
    cACompromise            (2),
    affiliationChanged      (3),
    superseded              (4),
    cessationOfOperation    (5),
    certificateHold         (6),
    removeFromCRL           (8),
    privilegeWithdrawn      (9),
    aaCompromise            (10) }
```

وقيم شفرة الداعي التالية تبين لماذا يجري إبطال الشهادة:

- شفرة **غير محدد (unspecified)** يمكن استعمالها لإبطال شهادات لدواعٍ أخرى غير دواعي الشفرات المحددة؛
- شفرة **تعرّض المفتاح للخطر (keyCompromise)** تستعمل لإبطال شهادة كيان نهائي، وهي تدل على أن من المعروف أو من المعتقد أن المفتاح الخاص للصاحب، أو غيره من خصائص الصاحب الصالحة في الشهادة، قد تعرّض للخطر؛
- شفرة **تعرّض سلطة إصدار الشهادة للخطر (cACompromise)** تستعمل لإبطال شهادة سلطة إصدار الشهادة، وهي تدل على أن من المعروف أو من المعتقد أن المفتاح الخاص للصاحب، أو غيره من خصائص الصاحب الصالحة في الشهادة، قد تعرّض للخطر؛
- شفرة **تغيير النسب (affiliationChanged)** تدل على أن اسم الصاحب، أو غيره من المعلومات الواردة في الشهادة قد تعدّل، ولكن لا يوجد أي سبب للاعتقاد بأن المفتاح الخاص قد تعرّض للخطر؛
- شفرة **المستبدلة (superseded)** تدل على أن الشهادة قد استعيض عنها، ولكن لا يوجد أي سبب للاعتقاد بأن المفتاح الخاص قد تعرّض للخطر؛
- شفرة **إيقاف التشغيل (cessationOfOperation)** تدل على أن الشهادة لم تعد لازمة للغرض الذي أصدرت له، ولكن لا يوجد أي سبب للاعتقاد بأن المفتاح الخاص قد تعرّض للخطر؛
- شفرة **سحب الامتياز (privilegeWithdrawn)** تدل على أن شهادة المفتاح العمومي أو النعت قد جرى إبطالها، لأن الامتياز الممنوح فيها قد جرى سحبه؛
- شفرة **تعرض سلطة النعت للخطر (aACompromise)** تدل على أن من المعروف أو من المعتقد أن بعض خصائص سلطة النعت (AA) الصالحة في شهادة النعت، قد تعرّضت للخطر.

يمكن وضع شهادة ما في حالة الانتظار، بإصدار مدخل في قائمة إبطال CRL يحتوي على شفرة الداعي **الشهادة في الانتظار (certificateHold)**. والتبليغ عن وضع شهادة في الانتظار ربما يشتمل على شفرة تعليمات الوضع في الانتظار، لنقل معلومات إضافية إلى مستعملي الشهادات (انظر الفقرة 3.2.5.8). وبعد أن يصدر وضع الشهادة في الانتظار، يمكن معالجة الشهادة بواحد من الأساليب الثلاثة التالية:

أ) يمكن إبقاؤها في قائمة الإبطال CRL دون أي إجراء إضافي، مما يجعل مستعمليها يرفضون المعاملات الصادرة أثناء فترة الوضع في الانتظار؛ أو

ب) يمكن الاستعاضة عن الوضع في الانتظار بإبطال (نهائي) لنفس الشهادة، وفي هذه الحالة يجب أن يكون الداعي هو أحد دواعي الإبطال المعيارية، ويكون تاريخ الإبطال هو التاريخ الذي وضعت فيه الشهادة في الانتظار، ولا يعود يظهر حقل توسع شفرة التعليمات الاختياري؛ أو

ج) يمكن إلغاؤها صراحة وإزالة المدخل من قائمة الإبطال CRL.

وشفرة الداعي **السحب من القائمة CRL (removeFromCRL)** تستعمل فقط مع القائمة دلتا للإبطال delta-CRL (انظر الفقرة 6.8)، وتدل على وجوب إلغاء مدخل موجود في القائمة CRL، بسبب انتهاء صلاحية الشهادة أو إلغاء وضعها في الانتظار. والمدخل الذي يحمل شفرة الداعي هذه يستعمل في القوائم delta-CRL التي تكون القائمة الأساسية للإبطال CRL المقابلة لها، وكل قائمة CRL لاحقة (دلتا أو كاملة لمجال التطبيق)، تحتوي على مدخل لنفس الشهادة مع شفرة الداعي **الشهادة في الانتظار (certificateHold)**.

ويكون هذا التوسع غير حرج دائماً.

3.2.5.8 توسّع شفرة تعليمات الوضع في الانتظار

يقدم هذا الحقل من التوسع في مدخل القائمة CRL، معرف هوية مسجّلاً للتعليمات، لكي يدل أثناء وجوده على التدبير الواجب اتخاذه عند وجود شهادة موضوعة في الانتظار. ولا ينطبق إلا على مدخلٍ تكون شفرة الداعي فيه هي **الشهادة في الانتظار (certificateHold)**. ويعرّف هذا الحقل كما يلي:

```
holdInstructionCode EXTENSION ::= {
    SYNTAX              HoldInstruction
    IDENTIFIED BY       id-ce-instructionCode }

HoldInstruction ::= OBJECT IDENTIFIER
```

ويكون هذا التوسع غير حرج دائماً. ولا تعرّف مواصفة الدليل هذه أي شفرات مقيّسة لتعليمات الوضع في الانتظار.

ملاحظة – أمثلة من تعليمات الوضع في الانتظار يمكن أن تكون "يرجى الاتصال بالسلطة CA" أو "استرجع إذنة المستعمل".

4.2.5.8 توسع تاريخ عدم الصلاحية

يدل هذا الحقل من التوسع في مدخل القائمة CRL على التاريخ الذي يكون من المعروف فيه أو من المتوقع أن يكون المفتاح الخاص قد تعرّض للخطر، أو على التاريخ الذي ينبغي اعتبار الشهادة فيه غير صالحة لأسباب أخرى. وقد يكون هذا التاريخ أبكر من تاريخ الإبطال الوارد في مدخل القائمة CRL، الذي هو التاريخ الذي عالجت السلطة فيه عملية الإبطال. ويعرّف هذا الحقل كما يلي:

```
invalidityDate EXTENSION ::= {
    SYNTAX              GeneralizedTime
    IDENTIFIED BY       id-ce-invalidityDate }
```

ويكون هذا التوسع غير حرج دائماً.

ملاحظة 1 – التاريخ الموجود في هذا التوسع ليس كافياً بحد ذاته لأغراض عدم الرفض. فقد يكون هذا التاريخ مثلاً قد أشار به حامل المفتاح الخاص، ويحتمل أن يطالب هذا الشخص بالباطل بأن المفتاح كان قد تعرّض للخطر في وقت ما في الماضي، بحيث يتمكن من رفض توقيع جرى بطريقة صالحة.

ملاحظة 2 – عندما تنشر سلطة في قائمة CRL رفضاً لأول مرة، قد يحدث أن يكون تاريخ عدم الصلاحية سابقاً لتاريخ إصدار قوائم CRL سابقة. ويجب ألا يكون تاريخ الإبطال سابقاً لتاريخ إصدار القوائم CRL السابقة.

5.2.5.8 توسع مجال تطبيق القائمة CRL

ملاحظة – استعمال المصطلح "توسع مجال تطبيق القائمة CRL" متروك.

مجال تطبيق قائمة CRL يكون مبيّناً داخل هذه القائمة التي تستخدم التوسع التالي في القائمة CRL. ولاتّقاء حصول تهجم يستعيض عن القائمة CRL بتطبيق لا يعتمد توسع مجال التطبيق، فإن مجال التطبيق يوسم بأنه حرج، إن كان موجوداً.

يمكن استعمال هذا التوسع لتقديم إعلانات عن مجال التطبيق لمختلف أنماط القائم CRL التالية:

– قوائم CRL بسيطة تقدم معلومات الإبطال الخاصة بشهادات صادرة عن سلطة وحيدة؛

- قوائم CRL غير مباشرة تقدم معلومات الإبطال الخاصة بشهادات صادرة عن سلطات عديدة؛
- قوائم دلتا CRL (delta-CRL) تحيّن معلومات الإبطال الصادرة سابقاً؛
- قوائم دلتا CRL غير مباشرة تقدم معلومات إبطال تحيّن عدة قوائم أساسية CRL، صادرة عن سلطة وحيدة أو عن سلطات عديدة.

```
crlScope EXTENSION ::= {
    SYNTAX                  CRLScopeSyntax
    IDENTIFIED BY           id-ce-cRLScope }

CRLScopeSyntax ::=          SEQUENCE SIZE (1..MAX) OF PerAuthorityScope

PerAuthorityScope ::= SEQUENCE {
    authorityName               [0]     GeneralName OPTIONAL,
    distributionPoint           [1]     DistributionPointName OPTIONAL,
    onlyContains                [2]     OnlyCertificateTypes OPTIONAL,
    onlySomeReasons             [4]     ReasonFlags OPTIONAL,
    serialNumberRange           [5]     NumberRange OPTIONAL,
    subjectKeyIdRange           [6]     NumberRange OPTIONAL,
    nameSubtrees                [7]     GeneralNames OPTIONAL,
    baseRevocationInfo          [9]     BaseRevocationInfo OPTIONAL
    }

OnlyCertificateTypes ::= BIT STRING {
    user            (0),
    authority       (1),
    attribute       (2) }

NumberRange ::= SEQUENCE {
    startingNumber      [0]     INTEGER OPTIONAL,
    endingNumber        [1]     INTEGER OPTIONAL,
    modulus                     INTEGER OPTIONAL }

BaseRevocationInfo ::= SEQUENCE {
    cRLStreamIdentifier     [0]     CRLStreamIdentifier     OPTIONAL,
    cRLNumber               [1]     CRLNumber,
    baseThisUpdate          [2]     GeneralizedTime }
```

إذا كانت القائمة CRL هي القائمة CRL غير المباشرة التي تقدم معلومات وضع الإبطال القانوني الخاصة بسلطات عديدة، فإن التوسع يحتوي على عدة بنى من **مجال التطبيق لكل سلطة (PerAuthorityScope)**، تخص واحدة أو عدة منها، كل واحدة من السلطات الواردة معلوماتُ الإبطال بشأنها. وكل واحدة من مطابقات **مجال التطبيق لكل سلطة** تتعلق بسلطة هي غير السلطة المُصْدرة لهذه القائمة CRL هي القائمة دلتا CRL التي تقدم المعلومات دلتا عن وضع الإبطال القانوني الخاصة بقوائم CRL أساسية وعديدة صادرة عن سلطة وحيدة، فإن التوسع يحتوي على عدة بنى من **مجال التطبيق لكل سلطة**، تخص كل واحدة منها واحدةً من القوائم CRL الأساسية التي تقدم هذه القائمة دلتا CRL تحييناً لها. وحتى إذا وجدت عدة مطابقات من البنى **في مجال التطبيق لكل سلطة**، فإن قيمة المكوّنة **اسم السلطة**، إن وجدت، تكون هي نفسها لجميع المطابقات.

وإذا كانت القائمة CRL هي قائمة دلتا CRL غير مباشرة تقدم معلومات دلتا عن وضع الإبطال القانوني الخاصة بقوائم CRL أساسية وعديدة صادرة عن سلطات عديدة، فإن التوسع يحتوي على عدة بنى من **مجال التطبيق لكل سلطة**، تخص كل واحدة منها واحدةً من القوائم CRL الأساسية التي تقدم هذه القائمة دلتا CRL تحييناً لها. وكل مطابق من **مجال التطبيق لكل سلطة** يتعلق بسلطة غير السلطة التي أصدرت القائمة دلتا CRL غير المباشرة يجب أن يحتوي على المكوّنة **اسم السلطة**.

وتستعمل الحقول كما يلي بشأن كل مطابق **لمجال التطبيق لكل سلطة** موجود في التوسع. ويلاحظ أنه في حالة القوائم CRL غير المباشرة والقوائم دلتا CRL غير المباشرة، يمكن لكل مطابق **مجال التطبيق لكل سلطة** أن يحتوي على تركيبات مختلفة من هذه المجالات وهذه القيم المختلفة.

يحدد الحقل **اسم السلطة**، إن وجد، السلطة التي أصدرت الشهادات التي تقدم بشأنها معلومات الإبطال. وإذا كان الحقل **اسم السلطة** غالباً، تكون قيمته بالتغيب هي اسم مُصدر القائمة CRL.

ويستعمل الحقل **نقطة التوزيع (distributionPoint)**، إن وجدَ، كما هو موضع في التوسع **نقطة التوزيع المُصْدر (issuingDistributionPoint)**.

ويدل الحقل **يحتوي فقط (onlyContains)**، إن وجد، على نمط أو أنماط الشهادات التي تحتوي القائمة CRL معلومات عن وضع إبطالها القانوني. وإذا كان هذا الحقل غائباً، فإن القائمة CRL تحتوي معلومات عن جميع أنماط الشهادات.

يستعمل الحقل **بعض الدواعي فقط (onlySomeReasons)**، إن وجد، كما هو موضح في التوسع **نقطة التوزيع المُصدرة**.

يستعمل العنصر **مدى رقم التسلسل (serialNumberRange)** كالتالي، إن وجد. عندما تكون قيمة مقاس (modulus) موجودة، يخفض رقم التسلسل بأخذ الباقي من تقسيم القيمة المدروسة على قيمة المقاس قبل التحقق من الانتماء إلى المدى. ثم تعتبر الشهادة التي تحمل رقم التسلسل (المخفّض) واقعة في مجال تطبيق القائمة CRL، إن كان رقم تسلسلها:

- يساوي أو أكبر من رقم البداية (**startingNumber**)، وأصغر من رقم النهاية (**endingNumber**)، عندما يكونان كلاهما موجودين؛ أو
- يساوي أو أكبر من رقم البداية، إن كان رقم النهاية غائباً؛ أو
- أصغر من رقم النهائية، إن كان رقم البداية غائباً.

يفسَّر العنصر **مدى معرف هوية مفتاح الصاحب (subjectKeyIdRange)**، إن وجد، على أنه **مدى رقم التسلسل**، باستثناء كون الرقم المستعمل هو القيمة الموجودة في توسع الشهادة **معرف هوية مفتاح الصاحب (subjectKeyIdentifier)**. وتشفير **سلسلة البتات (BIT STRING)** بقواعد التشفير المميزة (DER) (بعد حذف الوسم والطول وأثمون البتات غير المستعملة) يجب أن ينظر إليه على أنه قيمة التشفير بقواعد التشفير المميزة (DER) **لعدد صحيح (INTEGER)**. وإذا كانت البتة صفر من **سلسلة البتات** موضوعة، ينبغي إضافة أثمون صفري، من أجل ضمان أن يكون التشفير الناتج يمثل **عدداً صحيحاً** موجباً **(INTEGER)**، فمثلاً:

f7 01 02 03 (يمثل عنصر البتات 6-0 المحدد)

وهو يقابل

f7 00 02 02 (أي 247 في النظام العشري)

ويستعمل الحقل **الأشجار الفرعية للاسم (nameSubtrees)**، إن وجد، نفس الاصطلاحات المستعملة لأشكال الاسم، كما هي محددة في توسّع **تقييدات الاسم (nameConstraints)**.

ويدل الحقل **معلومات إبطال أساسية (baseRevocationInfo)**، إن وجد، على أن القائمة CRL هي قائمة دلتا CRL، فيما يخص الشهادات التي تغطيها بنية **مجال التطبيق لكل سلطة (PerAuthorityScope)**. واستعمال التوسع **مجال تطبيق القائمة CRL (crlScope)** للتعريف بقائمة CRL على أنها قائمة دلتا CRL، يختلف عن استعمال التوسع **معرف هوية القائمة دلتا CRL (deltaCRLIdentifier)** بما يلي. ففي حالة **مجال تطبيق القائمة CRL**، تدل المكوّنة **معلومات إبطال أساسية** على اللحظة التي تبدأ فيها القائمة CRL الحاوية على هذا التوسع بتقديم تحيينات. وعلى الرغم من أن هذا يحيل إلى قائمة CRL، فإن القائمة CRL المحال إليها يمكنها أن تكون أو لا تكون قائمة كاملة لمجال التطبيق كله، بينما يحيل التوسع **معرف هوية القائمة دلتا CRL** على قائمة دلتا CRL صادرة لتكون كاملة لمجال التطبيق كله. وفي كل الأحوال، فإن المعلومات المحيّنة التي تقدمها قائمة دلتا CRL وتحتوي على التوسع **مجال تطبيق القائمة CRL** هي تحيينات لمعلومات الإبطال الكاملة الخاصة بمجال التطبيق، بصرف النظر عما إذا كانت القائمة CRL المحال إليها في المكوّنة **معلومات إبطال أساسية** أو لم تكن صادرة فعلاً كقائمة كاملة لنفس مجال التطبيق. وتوفر هذه الطريقة مرونة أكبر مما يوفره التوسع **مبيّن القائمة دلتا**

deltaCRLIdentifier) CRL)، لأن المستعملين يمكنهم إنشاء قوائم CRL كاملة محلياً، وإنشاؤها استناداً إلى التاريخ والوقت بدلاً من إصدار قوائم CRL أساسية وكاملة لمجال التطبيق كله. وفي كلتا الحالتين، تقدم القوائم دلتا CRL دائماً تحيينات لوضع الإبطال القانوني الخاص بشهادات صالحة في مجال تطبيق معيّن، وبدءاً من لحظة زمنية معينة. وفي حالة **مبيّن القائمة دلتا CRL**، تكون هذه اللحظة هي اللحظة التي يتم فيها إصدار قائمة CRL كاملة لمجال التطبيق هذا، وليصار إلى الإحالة إليها. أما في حالة **مجال تطبيق القائمة CRL**، فتكون هذه اللحظة هي لحظة إصدار القائمة CRL المحال إليها التي يمكن أن تكون أو لا تكون هي القائمة الكاملة لمجال التطبيق هذا.

وتبعاً لسياسة السلطة المسؤولة، يمكن نشر عدة قوائم دلتا CRL، قبل نشر القائمة الأساسية CRL الجديدة. إن القوائم دلتا CRL التي تحتوي على التوسع **مجال تطبيق القائمة CRL** للإحالة إلى لحظة إحداثها، لا تحتاج بالضرورة إلى الإحالة إلى **رقم القائمة CRL (cRLNumber)** لأحدث قائمة CRL أساسية صادرة في المجال **معلومات إبطال أساسية**. ويكون رقم القائمة CRL المحال إليه في المجال **معلومات إبطال أساسية** في قائمة دلتا CRL، يساوي أو أصغر من **رقم القائمة CRL** لأحدث قائمة CRL صادرة كاملة لمجال التطبيق كله.

يلاحظ أن التوسع **نقطة التوزيع المُصْدرة (issuingDistributionPoint)** والتوسع **مجال تطبيق القائمة CRL (crlScope)** قد يتنازعان فيما بينهما، وليسا مهيأين ليستعملا معاً. فإذا كانت قائمة CRL تحتوي في ظرف ما على التوسعين **نقطة التوزيع المُصْدر ومجال تطبيق القائمة CRL**، تقع عندئذ شهادة المفتاح العمومي في مجال تطبيق القائمة CRL إذا، وفقط إذا، كانت تطابق معايير التوسعين معاً. وإذا كانت القائمة CRL تحتوي على التوسع **نقطة التوزيع المُصْدرة لسلطة النعت (issuingDistributionPoint)**، ولكنها لا تحتوي على أي من التوسعين **نقطة التوزيع المُصْدرة أو مجال تطبيق القائمة CRL**، لا يكون مجال التطبيق حاوياً عندئذ على شهادات مفتاح عمومي. وإذا كانت القائمة CRL لا تحتوي على أي من التوسعات **نقطة التوزيع المُصْدرة** أو **نقطة التوزيع المُصْدرة لسلطة النعت أو مجال تطبيق القائمة CRL**، يكون مجال التطبيق عندئذ هو كامل مجال التطبيق للسلطة، ويمكن استعمال القائمة CRL لأي شهادة صادرة عن السلطة. وكذلك الأمر فإن التوسع **نقطة التوزيع المُصْدرة لسلطة النعت** والتوسع **مجال تطبيق القائمة CRL** قد يتنازعان فيما بينهما، وليسا مهيأين ليستعملا معاً. فإذا كانت قائمة CRL تحتوي في ظرف ما على التوسعين **نقطة التوزيع المُصْدرة لسلطة النعت ومجال تطبيق القائمة CRL**، تقع عندئذ شهادة النعت في مجال تطبيق القائمة CRL إذا، وفقط إذا، كانت تطابق معايير التوسعين معاً. وإذا كانت القائمة CRL تحتوي على التوسع **نقطة التوزيع المُصْدرة**، ولكنها لا تحتوي على أي من التوسعين **نقطة التوزيع المصدرة لسلطة النعت** أو **مجال تطبيق القائمة CRL**، لا يكون مجال التطبيق حاوياً على شهادات نعت. أما إذا كانت القائمة CRL لا تحتوي على أي من التوسعات **نقطة التوزيع المَصْدرة** و**نقطة التوزيع المُصْدرة لسلطة النعت** و**مجال تطبيق القائمة CRL**، يكون مجال التطبيق عندئذ هو كامل مجال التطبيق للسلطة، ويمكن استعمال القائمة CRL لأي شهادة صادرة عن السلطة.

عندما يستعمل نظام استعمال الشهادات قائمة CRL تحتوي على التوسع **مجال تطبيق القائمة CRL (crlScope)** للتحقق من الوضع القانوني لشهادة، ينبغي له أن يتحقق من أن الشهادة وشفرات الدواعي المرعيّة تقع داخل مجال تطبيق القائمة CRL، كما يعرفه التوسع **مجال تطبيق القائمة CRL**، وذلك على النحو التالي:

أ) يجب أن يتحقق نظام استعمال الشهادات من أن الشهادة تقع داخل مجال التطبيق الذي يبيّنه تقاطع مجالات التطبيق **لمدى رقم التسلسل، ولمدى معرّف هوية مفتاح الصاحب، وللأشجار الفرعية للاسم**، وأنها متسقة مع الحقل **نقطة التوزيع**، ومع الحقل **يحتوي فقط** في حال وجوده، بشأن البنية المعنيّة **مجال التطبيق لكل سلطة**.

ب) إذا كانت القائمة CRL تحتوي على المكوّنة **بعض الدواعي فقط** في التوسع **مجال تطبيق القائمة CRL**، يجب عندئذ على نظام استعمال الشهادات أن يتحقق من أن شفرات الدواعي التي تغطيها هذه القائمة CRL وافية بأغراض التطبيق. وإذا لم تكن الشفرات كذلك، يمكن تَطَلّب قوائم CRL إضافية. ويلاحظ أنه إذا احتوت قائمة CRL على التوسعين **مجال تطبيق القائمة CRL (crlScope)** و**نقطة التوزيع المُصْدرة (issuingDistributionPoint)**، وكان كلاهما يحتوي على المكوّنة **بعض الدواعي فقط (onlySomeReasons)**، لا تكون إلا شفرات الدواعي المتضمنة في المكوّنتين **بعض الدواعي فقط** في التوسعين معاً، هي الشفرات التي تغطيها القائمة CRL.

6.2.5.8 توسع مرجع الوضع القانوني

يستعمل هذا التوسع في القائمة CRL داخل بنية القائمة CRL كوسيلة لنقل المعلومات الخاصة بتبليغات الإبطال إلى مستعملي الشهادات. وبصفته هذه، يوجد في بنية قائمة CRL لا تحتوي هي ذاتها على تبليغات عن إبطال الشهادات. ويجب ألا يستعمل بنية القائمة CRL التي تحتوي على هذا التوسع مستعملو الشهادات أو الأطراف الواثقة، كمَصْدر لتبليغات الإبطال، بل كأداة تؤكد على أن معلومات الإبطال المناسبة مستعملة. ويجب ألا يستعمل الطرف الواثق أي قائمة CRL تحتوي على هذا التوسع باعتبارها مَصْدراً يتحقق به من وضع الإبطال القانوني لأي شهادة، ولكن الطرف الواثق يستطيع استعمال القائمة CRL الحاوية على هذا التوسع كأداة إضافية لتحديد مواقع القوائم CRL المناسبة للتحقق من وضع الإبطال القانوني.

ويتعلق هذا التوسع بالوظيفتين الأوليتين التاليتين:

- يقدم هذا التوسع آلية لنشر "قائمة من القوائم CRL"، تكون موثوقة وتشمل كل المعلومات ذات الصلة التي تساعد الأطراف الواثقة على تحديد ما إذا كانت تتوفر لديهم أم لا المعلومات الكافية التي يحتاجونها عن الإبطال. فيمكن مثلاً لأي سلطة أن تصدر دورياً قائمة CRL جديدة مستيقنة، على أن يكون تواتر إعادة إصدارها عالياً (بالنسبة إلى تواتر إعادة إصدار غيرها من القوائم CRL). ويمكن للقائمة أن تضم تاريخ ووقت آخر تحيين لكل قائمة CRL أحيل إليها. وعندما يستلم مستعمل الشهادة هذه القائمة، يستطيع أن يعيّن بسرعة إن كانت القوائم CRL الموجودة في المخبأ عنده ما زالت محيّنة. وقد يزيل هذا الأمر جزءاً كبيراً من الاستخراجات غير الضرورية للقوائم CRL. واستعمال هذه الآلية يفيد فوق ذلك مستعملي الشهادات ليكونوا على اطّلاع على القوائم CRL الصادرة عن السلطة خارج أوقات دورة تحيينها العادية، وبذلك يتحسن وثاق الصلة بنظام القائمة CRL.
- ويقدم هذا التوسع آلية لإعادة توجيه الطرف الواثق من موقع تمهيدي (أي الموقع المشار إليه في توسع نقطة توزيع القوائم CRL أو في مدخل الدليل لسلطة الإصدار) إلى موقع آخر لمعلومات الإبطال. وتمكّن هذه الميزة السلطات من تعديل خطة تجزئة القائمة CRL التي يستخدمونها، دون التأثير في الشهادات الحالية أو في مستعملي الشهادات. وتقوم السلطة في سبيل إنجاز ذلك بتبيان كل موقع جديد وكل مجال تطبيق للقائمة CRL يمكن أن يعثر عليه في ذلك الموقع. ويقوم الطرف الواثق بمقارنة الشهادة التي تهمه بالإعلانات عن مجال التطبيق، ويتبع المؤشر الذي يدل على الموقع الجديد المناسب للحصول على معلومات الإبطال الخاصة بالشهادة، والتي تقرّ بالصلاحية لهذه الشهادة.

والتوسع هو نفسه قابل للتوسع، ويمكن أن تستعمله في المستقبل أنظمة إبطال أخرى لا تستند إلى القوائم CRL.

```
statusReferrals EXTENSION ::= {
    SYNTAX              StatusReferrals
    IDENTIFIED BY       id-ce-statusReferrals }

StatusReferrals ::= SEQUENCE SIZE (1..MAX) OF StatusReferral

StatusReferral ::= CHOICE {
    cRLReferral         [0]     CRLReferral,
    otherReferral       [1]     INSTANCE OF OTHER-REFERRAL}


CRLReferral ::= SEQUENCE {
    issuer              [0]     GeneralName OPTIONAL,
    location            [1]     GeneralName OPTIONAL,
    deltaRefInfo        [2]     DeltaRefInfo OPTIONAL,
    cRLScope                    CRLScopeSyntax,
    lastUpdate          [3]     GeneralizedTime OPTIONAL,
    lastChangedCRL      [4]     GeneralizedTime OPTIONAL}

DeltaRefInfo ::= SEQUENCE {
    deltaLocation       GeneralName,
    lastDelta           GeneralizedTime OPTIONAL }

OTHER-REFERRAL ::= TYPE-IDENTIFIER
```

يبين حقل **المُصْدر (issuer)** الكيان الذي يوقّع القائمة CRL، وقيمة التغيب فيه تشير إلى اسم مُصدر القائمة CRL الذي يظهر فيها.

ويقدم حقل **المَوْقع (location)** الموقع الذي يجب أن يوجه إليه طالب المرجع، وقيمته بالتغيب هي نفس قيمة اسم **المُصْدر**.

ويقدم حقل **المعلومات المرجعية عن دلتا (deltaRefInfo)** موقعاً بديلاً خيارياً، يمكن الحصول فيه على القائمة dCRL، وعلى تاريخ خياري للقائمة دلتا السابقة.

ويقدم حقل **مجال تطبيق القائمة CRL (cRLScope)** مجال تطبيق القائمة CRL التي سيعثر عليها في الموقع المرجعي المحال إليه.

والحقل **آخر تحيين (lastUpdate)** هو قيمة حقل **هذا التحيين (thisUpdate)** للقائمة CRL التي تمت أحدث إحالة إليها.

والحقل **آخر قيمة CRL معدلة (lastChangedCRL)** هو قيمة حقل **هذا التحيين (thisUpdate)** للقائمة CRL المعدل محتواها وتمت أحدث إحالة إليها.

ومعرّف الهوية **مرجع آخر (OTHER-REFERRAL)** يقدم قابلية التوسع التي تسمح في المستقبل باستعمال أنظمة إبطال أخرى لا تستند إلى القوائم CRL.

ويوسم هذا التوسع بأنه حرج دائماً، للتأكد من أن القائمة CRL التي تحتوي على هذا التوسع لم تستعملها سهواً أنظمة استعمال الشهادات، باعتبارها مَصْدر المعلومات عن الشهادات بخصوص وضع إبطالها القانوني.

إذا كان هذا التوسع موجوداً ويعترف به نظام استعمال الشهادات، فإن هذا النظام لن يستعمل القائمة CRL كمَصْدر للمعلومات عن وضع الإبطال القانوني. وينبغي للنظام أن يستعمل إما المعلومات الموجودة في هذا التوسع، وإما غيرها من الوسائل التي تقع خارج نطاق هذه المواصفة، لكي يحدد الموقع المناسب لمعلومات وضع الإبطال القانوني.

وإذا كان هذا التوسع موجوداً ولكن نظام استعمال الشهادات لا يعترف به، فإن هذا النظام لن يستعمل القائمة CRL كمَصْدر للمعلومات عن وضع الإبطال القانوني. وينبغي للنظام أن يستعمل وسائل أخرى تقع خارج نطاق هذه التوصية، لكي يحدد الموقع المناسب لمعلومات وضع الإبطال القانوني.

7.2.5.8 توسع معرف هوية تقاطر القوائم CRL

يستعمل حقل معرف هوية تقاطر القوائم CRL لكي يبين السياق الذي يكون فيه رقم القائمة CRL وحيداً.

```
cRLStreamIdentifier EXTENSION      ::= {
    SYNTAX              CRLStreamIdentifier
    IDENTIFIED BY       id-ce-cRLStreamIdentifier }

CRLStreamIdentifier ::= INTEGER (0..MAX)
```

ويكون هذا التوسع غير حرج دائماً.

وتكون كل قيمة في هذا التوسع وحيدة لكل سلطة. ومعرف هوية تقاطر القوائم CRL، المتصاحب مع رقم القائمة CRL، يسمح بتحديد معرف هوية وحد لكل قائمة CRL صادرة عن أي سلطة معنية، بصرف النظر عن نمط القائمة CRL.

8.2.5.8 توسّع القائمة المرتبة

يدل توسع القائمة المرتبة على أن تتابع الشهادات المبطَلة في حقل **الشهادات المبطلة (revokedCertificates)** من قائمة CRL هو تتابع مصنف وفق الترتيب التصاعدي إما لأرقام تسلسل الشهادات وإما لتواريخ الإبطال. ويعرف هذا الحقل كما يلي:

```
orderedList EXTENSION      ::= {
    SYNTAX              OrderedListSyntax
    IDENTIFIED BY       id-ce-orderedList }

OrderedListSyntax ::= ENUMERATED {
ascSerialNum        (0),
ascRevDate          (1) }
```

ويكون هذا التوسع غير حرج دائماً.

- يدل **رقم التسلسل التصاعدي (ascSerialNum)** على أن تتابع الشهادات المبطَلة في قائمة CRL هو مرتّب وفق الترتيب التصاعدي لأرقام تسلسل الشهادات، استناداً إلى قيمة المكوّنة **رقم التسلسل (serialNumber)** لكل مدخل في القائمة؛
- يدل **تاريخ الإبطال التصاعدي (ascRevDate)** على أن تتابع الشهادات المبطَلة في قائمة CRL هو مرتّب وفق الترتيب التصاعدي لتواريخ الإبطال، استناداً إلى قيمة المكوّنة **تاريخ الإبطال (revocationDate)** لكل مدخل في القائمة.

وإذا كانت المكوّنة **القائمة المرتبة (orderedList)** غير موجودة، لا تكون توجد أي معلومات بشأن ترتيب الشهادات المبطلة في القائمة CRL.

9.2.5.8 توسّع المعلومات دلتا

يستعمل هذا التوسع في القائمة CRL، من أجل القوائم CRL التي لا تكون dCRL، وهو يبين للأطراف الواثقة أن القوائم دلتا CRL (dCRL) تكون متيسرة أيضاً في القائمة CRL التي تحتوي على هذا التوسع. ويقدم التوسع الموقع الذي يمكن العثور فيه على القوائم dCRL ذات الصلة، كما تقدم اختيارياً الموعد الذي ستصدر فيه القائمة dCRL التالية.

```
deltaInfo EXTENSION       ::=  {
    SYNTAX                DeltaInformation
    IDENTIFIED BY         id-ce-deltaInfo }

DeltaInformation          ::=       SEQUENCE {
        deltaLocation     GeneralName,
        nextDelta              GeneralizedTime OPTIONAL }
```

ويكون هذا التوسّع غير حرج دائماً.

10.2.5.8 توسع الشهادات الواجب إبطالها

يتيح هذا التوسع في القائمة CRL التبليغ عن الشهادات التي سيجري إبطالها في المستقبل بتاريخ ووقت معينين. ويستعمل التوسع **الواجب الإبطال (toBeRevoked)** لتحديد داعي إبطال الشهادة، وتاريخ ووقت إبطال الشهادة، ومجموعة الشهادات الواجب إبطالها. وتستطيع كل قائمة أن تحتوي على رقم تسلسل وحيد لشهادة، أو على مجموعة من أرقام تسلسل شهادات، أو على مكوّنة معيّنة في **شجرة فرعية (subtree)**. وقد تكون الشهادات شهادات مفتاح عمومي أو شهادات نعت.

```
toBeRevoked  EXTENSION  ::= {
  SYNTAX              ToBeRevokedSyntax
  IDENTIFIED BY       id-ce-toBeRevoked }

ToBeRevokedSyntax::=      SEQUENCE SIZE(1..MAX) OF ToBeRevokedGroup

ToBeRevokedGroup ::=      SEQUENCE {
  certificateIssuer   [0] GeneralName OPTIONAL,
  reasonInfo          [1] ReasonInfo     OPTIONAL,
  revocationTime          GeneralizedTime,
  certificateGroup        CertificateGroup }

ReasonInfo                ::=     SEQUENCE {
  reasonCode              CRLReason,
  holdInstructionCode     HoldInstruction OPTIONAL }

CertificateGroup     ::=  CHOICE {
  serialNumbers           [0]     CertificateSerialNumbers,
  serialNumberRange       [1]     CertificateGroupNumberRange,
  nameSubtree             [2]     GeneralName }

CertificateGroupNumberRange ::= SEQUENCE {
  startingNumber    [0]     INTEGER,
  endingNumber      [1]     INTEGER }

CertificateSerialNumbers ::= SEQUENCE SIZE(1..MAX) OF CertificateSerialNumber
```

ويحدد الحقل **مُصْدر الشهادة (certificateIssuer)**، إن وجد، هوية السلطة (سلطة إصدار الشهادة أم سلطة النعت) التي أصدرت جميع الشهادات المعدّدة في **المجموعة الواجب إبطالها (ToBeRevokedGroup)**. وإذا كان **مُصْدر الشهادة** محذوفاً، تكون قيمته بالتغيب هي اسم مصدر القائمة CRL.

وإذا كان حقل **معلومات الداعي (reasonInfo)** موجوداً، فهو يعرف هوية دواعي إبطال الشهادات. وعندما يكون هذا المجال موجوداً، فهو يدل على أن جميع الشهادات المعرّفة هويتها في **المجموعة الواجب إبطالها**، سيجري إبطالها للداعي المذكور في هذا المجال. وإذا كانت **شفرة الداعي (ToBeRevokedGroup)** تحتوي على قيمة **الشهادة في الانتظار (reasonCode)**، يمكن أن تكون **شفرة تعليمات الوضع في الانتظار (certificateHold)** موجودة أيضاً. وإذا كانت **شفرة تعليمات الوضع في الانتظار (holdInstructionCode)** موجودة، فهي تدل على الإجراء الواجب اتخاذه عند مصادفة أي واحدة من الشهادات المحددة في **المجموعة المطلوب إبطالها**. وينبغي ألا يتخذ هذا الإجراء، إلا بعد انقضاء الوقت المحدد للإبطال في حقل **موعد الإبطال (revocationTime)**.

ويدل حقل **موعد الإبطال (revocationTime)** على التاريخ والوقت اللذين سيجري فيهما إبطال هذه المجموعة من الشهادات، وعندئذ تعتبر غير صالحة. ويكون هذا الموعد متأخراً عن موعد **هذا التحيين (thisUpdate)** الموجود في القائمة CRL الحاوية على هذا التوسع. وإذا كان **موعد الإبطال** سابقاً لموعد **التحيين القادم (nextUpdate)** الموجود في القائمة CRL الحاوية على هذا التوسع، يجب أن تعتبر الشهادة مبطلة ما بين **موعد الإبطال** وموعد **التحيين القادم** من قبل طرف واثق يستعمل قائمة CRL تحتوي على هذا التوسع. وإلا فإن هذا يعتبر تبليغاً عن أن هذه الشهادات سيجري إبطالها في موعد معين في المستقبل. وعند انقضاء موعد الإبطال، إما أن تكون سلطة إصدار الشهادة قد أبطلتها أو لا تكون. فإن كانت قد أبطلتها، تصبح القوائم CRL المستقبلية تحتوي هذه الشهادة في قوائم الشهادات المبطلة، إلى حين انتهاء صلاحية الشهادة على الأقل. أما إذا كانت سلطة إصدار الشهادة لم تبطلها، ولكنها ما زالت تنوي إبطالها في المستقبل، يمكنها أن تتضمن الشهادة في هذا التوسع من الشهادات CRL اللاحقة، ولكن مع **موعد إبطال** مراجَع. أما إذا كانت سلطة إصدار الشهادة لم تعد تنوي إبطال الشهادة، فيمكن استبعاد الشهادة من جميع القوائم CRL اللاحقة، ويجب ألا تعتبر الشهادة مبطلة.

يعدّد الحقل **مجموعة الشهادات (certificateGroup)** مجموعة الشهادات الواجب إبطالها. يحدد هذا المجال الشهادات التي أصدرتها السلطة المعرفة هويتها في **مُصْدر الشهادة** والواجب إبطالها في التاريخ والوقت المحددين في **موعد الإبطال**. ولا يعود يجري على هذه المجموعة من الشهادات أي تعديل جديد تدخله تحكمات خارجية (مثل **نقطة التوزيع المُصْدرة**).

وإذا وجدت المكونة **أرقام التسلسل**، ينبغي للشهادة أو للشهادات التي تحمل هذه الأرقام الواردة في هذا الحقل والصادرة عن مُصْدر الشهادة المحدد، أن يجري إبطالها في الموعد المحدد.

إذا وجدت المكوّنة **مدى أرقام التسلسل**، ينبغي لجميع الشهادات التي تقع أرقامها في هذا المدى، بدءاً من رقم تسلسل بداية المدى وانتهاءً برقم تسلسل نهايته، أن يجري إبطالها في الموعد المحدد.

إذا وجدت المكوّنة **الشجرة الفرعية للاسم**، ينبغي لجميع الشهادات التي يكون اسم صاحبها أو حاملها تابعاً للاسم المحدد والصادر عن مُصْدر الشهادة المحدد، أن يجري إبطالها في الموعد المحدد. وإذا كانت **الشجرة الفرعية للاسم** تحتوي على اسم مميز (DN)، يجب ألا تؤخذ بالاعتبار جميع الأسماء المميزة المتصاحبة مع صاحب شهادة المفتاح العمومي (أي حقل **الصاحب (subject)** وتوسع **الأسماء البديلة للصاحب (subjectAltNames)**) أو مع حقل **حامل (holder)** شهادة النعت. أما بالنسبة إلى جميع أشكال الأسماء الأخرى، فيجب أن يؤخذ بالاعتبار توسع **الأسماء البديلة للصاحب** لشهادات المفتاح العمومي، وحقل **الحامل** لشهادات النعت. وإذا كان واحد على الأقل من السماء المصاحبة للصاحب أو الحامل، موجوداً في الشهادة وواقعاً داخل الشجرة الفرعية التي تحددها المكوّنة **الشجرة الفرعية للاسم**، يجب إبطال هذه الشهادة في الموعد المحدد. وكما في حالة توسع **تقييدات الأسماء (nameConstraints)**، لا تكون جميع أشكال السماء مناسبة لمواصفة **الشجرة الفرعية**. ويجب ألا تستعمل في هذا التوسع إلا الأسماء الخاضعة لقواعد تَبَعية معترف بها.

يمكن لهذا التوسع أن يكون حرجاً أو غاير حرج، حسب تقدير مُصْدر القائمة CRL. ويوصى بأن يوسم هذا التوسع بغير الحرج، نظراً إلى أن المعلومات الواردة في هذا التوسع تخص الإبطالات، وبذلك ينخفض خطر ظهور مشاكل في التشغيل البيني والمواءمة الراجعة.

11.2.5.8 توسع مجموعة الشهادة المبطلة

يمكن أن تنشر الشهادات التي جرى إبطالها، باستخدام التوسع التالي في القائمة CRL. وترافق كل قائمة من الشهادات الواجب إبطالها بمُصدر الشهادة المحدد وبموعد الإبطال. ويمكن لكل قائمة أن تضم مدى من أرقام تسلسل الشهادات أو شجرة فرعية مسماة. ويمكن أن تكون هذه الشهادات شهادات مفتاح عمومي أو شهادات نعت.

```
revokedGroups  EXTENSION  ::= {
  SYNTAX            RevokedGroupsSyntax
  IDENTIFIED BY     id-ce-RevokedGroups }

RevokedGroupsSyntax ::=   SEQUENCE SIZE (1..MAX) OF RevokedGroup

RevokedGroup ::=   SEQUENCE {
  certificateIssuer           [0]   GeneralName OPTIONAL,
  reasonInfo                  [1]   ReasonInfo OPTIONAL,
  invalidityDate              [2]   GeneralizedTime OPTIONAL,
  revokedcertificateGroup     [3]   RevokedCertificateGroup }

RevokedCertificateGroup ::= CHOICE {
  serialNumberRange           NumberRange,
  nameSubtree                 GeneralName }
```

ويحدد الحقل **مُصْدر الشهادة (certificateIssuer)**، إن وجد، هوية السلطة (سلطة إصدار الشهادة أم سلطة نعت) التي أصدرت جميع الشهادات المعددة في **هذه المُبْطلة (RevokedGroup)**. وإذا كان مُصْدر الشهادة محذوفاً، تكون قيمته بالتغيب هي اسم مصدر القائمة CRL.

وإذا كان حقل **معلومات الداعي (reasonInfo)** موجوداً، فهو يعرف هوية دواعي إبطال الشهادات. وعندما يكون هذا الحقل موجوداً، فهو يدل على أن جميع الشهادات المعرفة هويتها في **المجموعة المبطَلة**، كانت قد أبطلت للداعي المذكور في هذا الحقل. وإذا كانت **شفرة الداعي (reasonCode)** تحتوي على قيمة **الشهادة في الانتظار (certificateHold)**، يمكن أن تكون **شفرة تعليمات الوضع في الانتظار (holdInstructionCode)** موجودة أيضاً. وإذا كانت **شفرة تعليمات الوضع في الانتظار** موجودة، فهي تدل على الإجراء الواجب اتخاذه عند مصادفة أي واحدة من الشهادات المحددة في **المجموعة المبطَلة**.

ويدل الحقل **تاريخ عدم الصلاحية (invalidityDate)**، إن وجد، على الموعد الذي تعتبر بدءاً منه جميع الشهادات المحددة في **المجموعة المبطَلة** غير صالحة. ويكون هذا التاريخ أبكر من التاريخ الموجود في حقل **هذا التحيين (thisUpdate)** الموجود في القائمة CRL. وإذا كان هذا التاريخ محذوفاً، ينبغي أن تعتبر جميع الشهادات المحددة في **المجموعة المبطَلة** غير صالحة، على الأقل اعتباراً من التاريخ المبين في **هذا التحيين** الموجود في القائمة CRL. وإذا كان الوضع القانوني للشهادة قبل موعد **هذا التاريخ** حرجاً بالنسبة إلى نظام استعمال الشهادات (أي لتحديد ما إذا كان التوقيع الرقمي الذي كان قد أحدث قبل إصدار هذه القائمة CRL، قد جرى حين كانت الشهادة ما تزال صالحة أو بعد أن جرى إبطالها)، فإن الأمر يتطلب تقنيات إضافية للتحقق من الوضع القانوني للإبطال وتحديد التاريخ الفعلي الذي تعتبر فيه إحدى الشهادات غير صالحة.

ويعدّد الحقل **مجموعة الشهادات المبطلة (revokedCertificateGroup)** مجموعة الشهادات التي كان قد جرى إبطالها. ويحدد هذا الحقل الشهادات التي أصدرتها السلطة المحددة في **مُصْدر الشهادة**، وأُبطلت في ظروف محددة. ولا تعود هذه المجموعة من الشهادات تخضع لأي تعديل يصدر عن تحكم خارجي (مثل **نقطة التوزيع المُصْدرة (issuingDistributionPoint)**).

وإذا كان الحقل **مدى أرقام التسلسل (serialNumberRange)** موجوداً، فإن جميع الشهادات التي تحمل أرقاماً لتسلسل الشهادات واقعة داخل المدى المحدد وصادرة عن مُصْدر الشهادة المحدّد، تعتبر قابلة للتطبيق.

إذا وجدت المكوّنة **الشجرة الفرعية للاسم (nameSubtree)**، ينبغي لجميع الشهادات التي يكون اسم صاحبها أو حاملها تابعاً للاسم المحدد والصادر عن مُصْدر الشهادة المحدد، أن يجري إبطالها في الموعد المحدد. وإذا كانت **الشجرة الفرعية للاسم** تحتوي على اسم مميز (DN)، يجب ألا تؤخذ بالاعتبار جميع الأسماء المميزة المتصاحبة مع شهادة المفتاح العمومي (أي حقل **الصاحب (subject)** وتوسع **الأسماء البديلة للصاحب (subjectAltNames)**) أو مع حقل **حامل (holder)** شهادة النعت. أما بالنسبة إلى جميع أشكال الأسماء الأخرى، فيجب أن يؤخذ بالاعتبار توسع **الأسماء البديلة للصاحب** لشهادات المفتاح العمومي، وحقل **الحامل** لشهادات النعت. وإذا كان واحد على الأقل من السماء المصاحبة للصاحب أو الحامل، موجوداً في الشهادة وواقعاً داخل الشجرة الفرعية التي تحدده المكوّنة **الشجرة الفرعية للاسم**، تكون هذه الشهادة قد أبطلت. وكما في حالة توسع **تقييدات الأسماء (nameConstraints)**، لا تكون جميع أشكال الأسماء مناسبة لمواصفة الشجرة الفرعية. ويجب ألا تستعمل في هذا التوسع إلا الأسماء الخاضعة لقواعد تَبَعية معترف بها.

يكون هذا التوسع حرجاً دائماً، وإلا يحتمل لنظام استعمال الشهادة أن يفترض، وهو على خطأ، بأن هذه الشهادات غير مبطلة، وهي مبطلة في هذا التوسع. وعندما يكون هذا التوسع موجوداً، فقد يكون هو الدلالة الوحيدة على الشهادات المبطلة في قائمة CRL (أي إن الحقل **الشهادات المبطلة** يكون خالياً)، أو إنه قد يعدّد شهادات مبطلة إضافية فوق تلك الشهادات المبينة في حقل **الشهادات المبطلة**). ولا ترد شهادة مبطلة مرتين في حقل **الشهادات المبطلة** وفي هذا التوسع.

12.2.5.8 توسع الشهادات المنتهية صلاحيتها في القائمة CRL

يدل حقل هذا التوسع في القائمة CRL على أن القائمة CRL تشتمل على تبليغات إبطال تخص شهادات منتهية الصلاحية.

```
expiredCertsOnCRL EXTENSION  ::= {
  SYNTAX      ExpiredCertsOnCRL
  IDENTIFIED BY      id-ce-expiredCertsOnCRL }

ExpiredCertsOnCRL  ::= GeneralizedTime
```

ويكون هذا التوسع غير حرج دائماً.

إن مجال تطبيق قائمة CRL حاوية على هذا التوسع هو موسّع ليشتمل على الوضع القانوني لإبطال شهادات انتهت صلاحيتها تماماً في الموعد المحدد في التوسع أو بعد هذا الموعد. وإذا تم تحديد بعض الحدود لمجال تطبيق القائمة CRL (إما بشفرات الدواعي أو بنقاط التوزيع)، فإن ذلك ينطبق أيضاً على الشهادات المنتهية صلاحيتها. ولا يجري تحيين الوضع القانوني لإبطال شهادة، بمجرد أن تنتهي صلاحية هذه الشهادة.

6.8 نقاط توزيع القوائم CRL والتوسعات في القوائم دلتا CRL (dCRL)

1.6.8 المتطلبات

يمكن أن تصبح قوائم الإبطال طويلة وضخمة، حتى لَيُطْلب تقديم قوائم جزئية. وتوجد حلول عديدة لاستخدامها في نمطي التنفيذ التاليين اللذين يعالجان القوائم CRL.

يتكون نمط التنفيذ الأول من محطات عمل شخصية، ربما تستخدم إذْنَة مجفرّة مرفقة. ويحتمل أن تتوفر لهذا النمط من التنفيذ مقدرة محدودة على التخزين المأمون. ولذلك فإن القائمة CRL بكاملها تحتاج إلى التفحص للتحقق من صلاحيتها، ثم التحقق من صلاحية الشهادة. وقد تستغرق هذه المعالجة وقتاً طويلاً إذا كانت القائمة CRL طويلة. إذاً لا بدّ من تجزئة القوائم CRL للتغلب على هذه المشكلة في هذا النمط.

ويعتمد نمط التنفيذ الثاني على مخدّمات عالية الأداء، يعالج فيها حجم كبير من الرسائل، أي مخدّم معالجات المعاملات. وفي هذه البيئة، تعالج القوائم CRL عادة كمهمة خلفية، حيث يختزن محتوى القائمة CRL عادة كمهمة خلفية، حيث يختزن محتوى القائمة CRL محلياً، بعد إقرار صلاحيتها، بطريقة عَرْض تسرّع تفحصها، أي ببتة واحدة لكل شهادة لتبيّن إن كانت قد أبطلت. ويختزن هذا الغرض في ذاكرة مأمونة. ويتطلب هذا النمط من المخدمات عادة قوائم CRL محيّنة بالنسبة إلى عدد كبير من السلطات. ولما كان يمتلك بالفعل قائمة بالشهادات المبطلة سابقاً، فإنه لا يحتاج إلا إلى استخراج قائمة بالشهادات المبطلة حديثاً. وهذه القائمة التي تدعى القائمة دلتا CRL (dCRL) تكون أصغر قدّاً من قائمة CRL كاملة، وتتطلب موارد أقل منها للاستخراج والمعالجة.

ولذلك فالمتطلبات التالية ذات صلة بنقاط توزيع القوائم CRL وبالقوائم دلتا CRL.

أ) لكي يمكن التحكم في قدود القوائم CRL، يجب أن تتوفر إمكانية إسناد مجموعات فرعية من مجموعة جميع الشهادات الصادرة عن سلطة واحدة، إلى قوائم CRL مختلفة. ولكي ينفذ ذلك يجب إرفاق كل شهادة بنقطة توزيع القائمة CRL التي تكون:

- إما مدخلاً في الدليل يحتوي نعت القائمة CRL فيه على مدخل إبطال لهذه الشهادة، إن كانت قد أبطلت؛
- وإما موقعاً، مثل عنوان بريد إلكتروني أو معرف هوية منتظم لمورد في الإنترنت، يمكن الحصول منه على القائمة CRL ذات الصلة.

ب) من المستحسن، لدواعٍ تتعلق بالأداء، خفض عدد القوائم التي تحتاج إلى تحقق، عند إقرار صلاحية شهادات عديدة، مثل مسيرة إصدار الشهادة. ويمكن إنجاز ذلك بتوفير مُصْدر قوائم CRL واحد يوقّع ويصدر قوائم CRL تحتوي على إبطالات قادمة من سلطات متعددة.

ج) هناك مطلب يدعو إلى قوائم CRL منفصلة تغطي إبطالات لشهادات سلطات وإبطالات لشهادات كيانات نهائية، مما يسهل معالجة مسيرات إصدار الشهادات، نظراً إلى أن من المتوقع أن القائمة CRL الخاصة بشهادات السلطة المبطلة ستكون قصيرة جداً (خالية عادة). وقد حددت لهذا الغرض نعوت **قائمة إبطالات السلطة (authorityRevocationList) وقائمة إبطالات الشهادة (certificateRevocationList)**. ولكي يضمن أمن عملية الفصل هذه، يلزم مؤشر يوضع في القائمة CRL، ليحدد أي قائمة CRL هي هذه القائمة. وإلا لا يعود يمكن كشف أي تبديل غير شرعي يحدث بين قائمة وأخرى.

د) يلزم تأمين قائمة CRL من أجل الحالات الخطرة المحتملة (عندما تكون هناك مخاطرة كبيرة من سوء استعمال مفتاح خاص)، بدلاً من القائمة التي تحتوي على جميع انتهائيات الربط العادية (عندما لا تكون هناك مخاطرة كبيرة من سوء استعمال مفتاح خاص).

هـ) كما يلزم أيضاً تأمين قائمة CRL جزئية (معروفة باسم dCRL) لا تحتوي إلا على المداخل إلى الشهادات التي كان قد جرى إبطالها منذ إصدار قائمة أساسية CRL.

و) يلزم أيضاً في حالة القوائم دلتا CRL أن يبيّن التاريخ والوقت التي ستحتوي هذه القائمة بعدهما على تحيينات.

ز) يوجد مطلب لكي يبيّن داخل الشهادة أين يمكن العثور على أحدث قائمة CRL (مثلاً أحدث قائمة dCRL).

2.6.8 مجالات التوسع في نقطة توزيع القائمة CRL وفي الشهادة دلتا CRL

تعرّف فيما يلي مجالات التوسع التالية:

أ) *نقاط توزيع القوائم CRL؛*

ب) *نقطة التوزيع المُصْدرة؛*

ج) *نقطة التوزيع المُصْدرة لسلطة النعت (AA)؛*

د) *مُصْدر الشهادة؛*

هـ) *مبين القائمة دلتا CRL؛*

و) *التحيين الأساسي؛*

ز) *أحدث قائمة CRL.*

ويجب ألا يستعمل التوسعان، نقاط توزيع القوائم CRL، وأحدث قائمة CRL، إلا كتوسعين في شهادة. ويجب ألا تستعمل التوسعات، نقطة التوزيع المُصْدرة، ونقطة التوزيع المُصْدرة لسلطة النعت، ومبين القائمة دلتا CRL، والتحيين الأساسي في قائمة CRL. ولا يستعمل التوسع، مُصْدر الشهادة، إلا كتوسع في مدخل القائمة CRL.

وإن كان توسع نقطة التوزيع المصدرة وتوسع نقطة التوزيع المصدرة لسلطة النعت يخدمان أغراضاً متشابهة، إلا أنهما يطبقان على شهادات مختلفة. فتوسع نقطة التوزيع المصدرة لا تنطبق إلا على شهادات المفتاح العمومي الصادرة إلى مستعملين و/أو إلى سلطات إصدار الشهادة. بينما لا ينطبق توسع نقطة التوزيع المصدرة لسلطة النعت على شهادات النعت الصادرة لمستعملين ولسلطات النعت، وكذلك على شهادات المفتاح العمومي الصادرة لَمصْدر السلطة. وإذا كانت إحدى القوائم CRL تضم شهادات تغطي كلا هذين النوعين من التوسع، يتعين عليها أن تضم هذين التوسعين.

1.2.6.8 توسع نقاط توزيع القوائم CRL

يجب ألا يستعمل توسع نقاط توزيع القوائم CRL إلا كتوسع في شهادة، ويمكن استعماله في شهادات السلطة، وفي شهادات المفتاح العمومي لكيان نهائي تصدرها السلطة وفي شهادات النعت. ويعرّف هذا المجال نقطة أو نقاط توزيع القوائم CRL التي ينبغي لمستعمل شهادة أن يتوجه إليها ليتأكد مما إذا كانت الشهادة قد أبطلت. يستطيع مستعمل الشهادة الحصول على قائمة CRL من نقطة توزيع ذات صلة، أو يمكنه الحصول على قائمة CRL حالية من مدخل الدليل للسلطة.

ويعرّف هذا الحقل كما يلي:

```
cRLDistributionPoints EXTENSION ::= {
    SYNTAX              CRLDistPointsSyntax
    IDENTIFIED BY       id-ce-cRLDistributionPoints }

CRLDistPointsSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
    distributionPoint   [0]     DistributionPointName OPTIONAL,
    reasons             [1]     ReasonFlags OPTIONAL,
    cRLIssuer           [2]     GeneralNames OPTIONAL }

DistributionPointName ::= CHOICE {
    fullName                        [0]     GeneralNames,
    nameRelativeToCRLIssuer         [1]     RelativeDistinguishedName }

ReasonFlags ::= BIT STRING {
    unused                  (0),
    keyCompromise           (1),
    cACompromise            (2),
    affiliationChanged      (3),
    superseded              (4),
    cessationOfOperation    (5),
    certificateHold         (6),
    privilegeWithdrawn      (7),
    aACompromise            (8) }
```

تحدّد المكوّنة **نقطة التوزيع (distributionPoint)** الموقع الذي يمكن الحصول فيه على القائمة CRL. وإذا كانت هذه المكونة غائبة، يكون اسم نقطة التوزيع بالتغيب هو اسم مُصْدر القائمة CRL.

وعند استعمال **الاسم الكامل (fullName)** البديل أو عندما ينطبق خيار التغيب، يمكن أن يأخذ اسم نقطة التوزيع أشكال اسم متعددة. ويجب أن يظهر نفس الاسم، على الأقل بواحد من أشكال اسمه، في مجال **نقطة التوزيع (distributionPoint)** من توسع نقطة التوزيع المُصْدرة للقائمة CRL. ولا يطلب من نظام استخدام الشهادات أن يكون على الأقل شكل واحد للاسم قابلاً للمعالجة. وإذا لم يوجد أي شكل من أشكال الاسم قابلاً للمعالجة، يستطيع نظام استعمال الشهادات أن يبقى يستعمل الشهادة، شريطة توفر إمكانية الحصول على معلومات الإبطال من مَصْدر آخر، مثل نقطة توزيع أخرى أو مدخل الدليل للسلطة.

ولا يمكن استعمال المكوّنة **الاسم النسبي بالنسبة إلى مُصْدر القائمة CRL (nameRelativeToCRLIssuer)** إلا إذا كانت نقطة توزيع القائمة CRL قد أسند إليها اسم في الدليل تابع مباشرة لاسم مُصْدر القائمة CRL قد أسند إليها اسم في الدليل

تابع مباشرة لاسم مُصْدر القائمة CRL في الدليل. وفي هذه الحالة، تنقل المكوّنة **الاسم النسبي بالنسبة إلى مُصْدر القائمة CRL** الاسم المميّز النسبي بالنسبة إلى اسم مُصْدر القائمة CRL في الدليل.

وتدل مكوّنة **الدواعي (reasons)** على دواعي الإبطال التي تغطيها هذه القائمة CRL. وإذا كانت مكوّنة **الدواعي** غائبة، تقوم نقطة توزيع القائمة CRL المقابلة بتوزيع قائمة CRL، تحتوي على مدخل إلى هذه الشهادة، إن كانت هذه الشهادة قد جرى إبطالها، بصرف النظر عن داعي الإبطال. وإلا فإن قيمة المكونة **الدواعي** تدل على دواعي الإبطال التي تغطيها نقطة توزيع القائمة CRL المقابلة.

وتحدد المكوّنة **مُصدر القائمة CRL (cRLIssuer)** السلطة التي تُصْدر وتوقّع القائمة CRL. وإذا كانت هذه المكوّنة غائبة، يكون اسم مُصْدر القائمة CRL بالتغيب هو اسم مُصْدر الشهادة.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصْدر الشهادة، ويوصى بأن يوسم بغير الحرج لصالح التشغيل البيني.

أما إذا كان هذا التوسع موسوماً بأنه حرج، فيكون على نظام استعمال الشهادات ألا يستعمل الشهادة، قبل أن يسحب أولاً قائمة CRL من إحدى نقاط التوزيع المسمّاة، ويتحقق من أنها تغطي شفرات الدواعي المعنية. وحيثما تستعمل نقاط التوزيع لتوزيع معلومات القائمة CRL عن جميع شفرات دواعي الإبطال، وتكون جميع الشهادات الصادرة عن سلطة إصدار الشهادة (CA) تحتوي على المكوّنة **نقاط توزيع القوائم CRL (cRLDistributionPoints)** كتوسع حرج، لا يطلب من سلطة إصدار الشهادة أن تنشر أيضاً قائمة CRL كاملة عند مدخل سلطة إصدار الشهادة.

وأما إذا كان هذا التوسع موسوماً بأنه غير حرج، وكان نظام استعمال الشهادات لا يعترف بنمط حقل التوسع، ينبغي لهذا النظام ألا يستعمل الشهادة إلا إذا كان:

- يستطيع أن يحصل على قائمة CRL كاملة من السلطة وأن يتحقق منها (تتم الدلالة على أن هذه القائمة CRL الأخيرة هي كاملة من غياب مجال التوسع نقطة التوزيع المُصْدرة من القائمة CRL)؛ أو
- التحقق من أن الإبطال ليس مطلوباً بموجب السياسة المحلية؛ أو
- التحقق من أن الإبطال يتم بوسائل أخرى.

ملاحظة 1 – يحتمل الحصول على قوائم CRL صادرة عن أكثر من مُصْدر واحد للقوائم CRL من أجل شهادة واحدة. والتنسيق بين مُصْدري هذه القوائم CRL وسلطة الإصدار يقع على مسؤولية سياسة السلطة.

ملاحظة 2 – يكون معنى كل شفرة داعٍ هو المعنى المحدد في حقل شفرة الداعي الوارد في الفقرة 2.2.5.8 من هذه المواصفة.

2.2.6.8 توسع نقطة التوزيع المُصْدرة

يحدد هذا الحقل لتوسع القائمة CRL نقطة توزيع القائمة CRL لشهادات المفتاح العمومي لهذه القائمة CRL الخاصة، ويبين إن كانت هذه القائمة الأخيرة CRL غير مباشَرة أو إن تطبيقها مقتصر على مجموعة فرعية من معلومات الإبطال. وإذا كان لا يُستعمل إلا قوائم CRL مجزأة، فإن المجموعة الكاملة من القوائم CRL المجزأة تغطي المجموعة الكاملة من الشهادات التي يشار إلى وضع إبطالها القانوني باستخدام آلية القائمة CRL. وهكذا تكون المجموعة الكاملة من القوائم CRL المجزأة مكافئة لقائمة CRL كاملة بشأن نفس المجموعة من الشهادات، إذا كان مُصْدر القائمة CRL لا يستخدم القوائم CRL المجزأة. ويمكن أن يكون الاقتصار مبنياً على مجموعة فرعية من كامل الشهادات أو على مجموعة فرعية من دواعي الإبطال. ويجري التوقيع على القائمة CRL بالمفتاح الخاص لمُصْدر القائمة CRL، لأن نقاط توزيع القائمة CRL لا تمتلك أزواج المفاتيح الخاصة بها. ومع ذلك فيما يخص قائمة CRL موزعة عبر الدليل، فإن القائمة CRL تختزن في مدخل نقطة توزيع القائمة CRL الذي قد لا يكون هو نفسه مدخل الدليل لمُصْدر القائمة CRL. وإذا كان حقل نقطة التوزيع المُصدرة، وحقل نقطة التوزيع المصدرة لسلطة النعت، وحقل تطبيق القائمة CRL، كلها غائبة، يجب أن تحتوي القائمة CRL على مداخل لجميع شهادات المفتاح العمومي المبطلة وغير المنتهية صلاحيتها والصادرة عن مصدر القائمة CRL. أما إذا كان حقل نقطة التوزيع المُصدرة

وحقل تطبيق القائمة CRL كلاهما غائبين، ولكن حقل نقطة التوزيع المُصدرة لسلطة النعت موجوداً، لا يكون حقل تطبيق القائمة CRL يشتمل على شهادات المفتاح العمومي.

بعد أن تظهر إحدى الشهادات في قائمة CRL، لا تعود تظهر في قائمة CRL لاحقة بعد انتهاء صلاحية الشهادة.

ويعرف هذا الحقل كما يلي:

```
issuingDistributionPoint EXTENSION  ::= {
    SYNTAX IssuingDistPointSyntax
    IDENTIFIED BY id-ce-issuingDistributionPoint }

IssuingDistPointSyntax ::= SEQUENCE {
    -- If onlyContainsUserPublicKeyCerts and onlyContainsCACerts are both FALSE,
    -- the CRL covers both certificate types
    -- إذا كانت المكوّنتان يحتوي فقط على شهادات مفتاح عمومي للمستعمل ويحتوي فقط على شهادات سلطة
    -- إصدار الشهادة موضوعين كلتيهما على "خاطئة" (FALSE)، فإن القائمة CRL تغطي نمطي الشهادة كليهما
    distributionPoint          [0] DistributionPointName OPTIONAL,
    onlyContainsUserPublicKeyCerts  [1] BOOLEAN DEFAULT FALSE,
    onlyContainsCACerts        [2] BOOLEAN DEFAULT FALSE,
    onlySomeReasons            [3] ReasonFlags OPTIONAL,
    indirectCRL                [4] BOOLEAN DEFAULT FALSE }
```

تحتوي المكوّنة **نقطة التوزيع (distributionPoint)** على اسم نقطة التوزيع بواحد من أشكال الاسم أو أكثر. وإذا كانت المكوّنة **يحتوي فقط على شهادات مفتاح عمومي للمستعمل (onlyContainsUserPublicKeyCerts)** موضوعة على "صائبة"، تكون القائمة CRL تحتوي على إبطالات لشهادات المفتاح العمومي للكيان النهائي. وإذا كانت المكوّنة **يحتوي فقط على شهادة إصدار الشهادة (onlyContainsCACerts)** موضوعة على "صائبة"، تكون القائمة CRL تحتوي على إبطالات لشهادات سلطة إصدار الشهادة. وإذا كانت المكونتان **يحتوي فقط على شهادة مفتاح عمومي للمستعمل ويحتوي فقط على شهادات سلطة إصدار الشهادة** موضوعتين كلتيهما على "خاطئة"، تكون القائمة CRL تحتوي على إبطالات لكلا نمطي الشهادات: شهادات المفتاح العمومي للكيان النهائي وشهادات سلطة إصدار الشهادة. وإذا كانت المكوّنة **بعض الدواعي فقط (onlySomeReasons)** موجودة، تكون القائمة CRL تحتوي فقط على إبطالات لشهادات المفتاح العمومي للداعي أو الدواعي المحدّدة، وإلا فإن القائمة CRL تحتوي على إبطالات لجميع الدواعي. وإذا كانت المكوَّنة **القائمة CRL غير المباشرة (indirectCRL)** موضوعة على "صائبة"، يمكن للقائمة CRL أن تحتوي على تبليغات لشهادات مفتاح عمومي صادرة عن سلطات غير مُصْدر القائمة CRL. أما السلطة الخاصة المسؤولة عن كل مدخل فيبينها التوسع في مدخل مُصْدر القائمة CRL للشهادة في هذا المدخل أو تكون متوافقة مع قواعد التغيب المشروحة في الفقرة 3.2.6.8. وفي مثل هذه القائمة CRL، يكون من مسؤولية مُصْدر القائمة CRL أن يضمن كون القائمة CRL كاملة، من حيث إنها تحتوي على جمع مداخل الإبطالات بطريقة منسجمة مع المؤشرات يحتوي فقط على شهادات مفتاح عمومي للمستعمل، **ويحتوي فقط على شهادات سلطة إصدار الشهادة**، وبعض الدواعي فقط، الصادرة عن جميع السلطات التي تبين هذا المُصدر للقائمة CRL في شهادات المفتاح العمومي الخاصة بها.

إذا كانت القوائم CRL مجزأة بشفرة الداعي، وكانت شفرة الداعي تتغير مع شهادة مبطلة (مسببة انتقال الشهادة من تقاطر قوائم CRL إلى تقاطر آخر)، يكون من الضروري الاستمرار في إبقاء الشهادة في تقاطر القوائم CRL المقابل لداعي الإبطال القديم، إلى أن تحيّن مواعيد **التحيين القادم** لجميع القوائم CRL التي لا ترد فيها الشهادة والموجودة في تقاطر القوائم CRL المقابل لشفرة الداعي الجديدة.

وإذا كانت القائمة CRL تحتوي على التوسع **نقطة التوزيع المُصْدرة** مع وجود الحقل **نقطة التوزيع**، فإن اسماً واحداً على الأقل لنقطة التوزيع وارداً في الشهادة (مثل **نقاط توزيع القوائم CRL**، **وأحدث قائمة CRL**، **والمُصْدر**)، **يقابل اسماً لنقطة التوزيع وارداً في القائمة** CRL. وفوق ذلك يمكن ألا يكون موجوداً إلا في الحقل **الاسم النسبي بالنسبة إلى مُصْدر القائمة CRL**. وفي هذه الحالة يجب إجراء مقارنة بين الأسماء على كامل الاسم المميز (DN)، المنشأ بإضافة قيمة الحقل **الاسم النسبي بالنسبة إلى مُصْدر القائمة CRL** إلى الاسم المميز الموجود في حقل **المُصْدر** من القائمة CRL. وإذا كانت الأسماء

المقارنة هي أسماء مميزة (بعكس أسماء الأشكال الأخرى داخل الإنشاء **الأسماء العامة**)، تستعمل قاعدة **مواءمة الأسماء المميزة** لمقارنة الاسمين المميزين والتحقق من تطابقهما.

وتطبق القواعد التالية على القوائم CRL الموزعة من خلال الدليل. فإذا كانت القائمة CRL هي قائمة دلتا CRL (dCRL)، يجب أن توزع من خلال النعت **قائمة إبطال دلتا (deltaRevocationList)** لنقطة التوزيع المصاحبة، أو من خلال النعت **قائمة إبطال دلتا** لمدخل مُصدر القائمة CRL، إن كانت لا توجد أي نقطة توزيع محددة، مهما تكن حالات الشهادات التي تغطيها القائمة. وفيما عدا الحالة التي تكون فيها القائمة CRL هي قائمة دلتا CRL:

- يتعين على القائمة CRL، المنشطة فيها المكوّنة **يحتوي فقط على شهادات سلطة إصدار الشهادة**، ولا تحتوي على التوسع **نقطة التوزيع المُصْدرة لسلطة النعت**، أن توزع عبر النعت **قائمة إبطال السلطة** لنقطة التوزيع المصاحبة، أو عبر النعت **قائمة إبطال السلطة** لمدخل مُصْدر القائمة CRL، إن كانت لا توجد أي نقطة توزيع محدد؛
- يتعين على القائمة CRL، المنشطة فيها المكوّنة **يحتوي فقط على شهادات سلطة إصدار الشهادة**، وتحتوي على التوسع **نقطة التوزيع المُصْدرة لسلطة النعت**، الذي تكون فيه المكوّنة **يحتوي على شهادات النعت للمستعمل موضوعة على "خاطئة"**، أو عبر النعت **قائمة إبطال السلطة** لنقطة التوزيع المصاحبة، أو عبر النعت **قائمة إبطال السلطة** لمدخل مُصْدر القائمة CRL، إن كانت لا توجد أي نقطة توزيع محددة؛
- يتعين على القائمة CRL، التي فيها فقط المكوّنة **يحتوي فقط على شهادة سلطة إصدار الشهادة** موضوعة على "خاطئة"، أن توزع عبر النعت **قائمة إبطال الشهادة** لنقطة التوزيع المصاحبة، أو عبر النعت **قائمة إبطال الشهادة** لمدخل مُصْدر القائمة CRL، إن كانت لا توجد أي نقطة توزيع محددة.
- يتعين على الشهادة CRL، التي فيها فقط المكوّنة **يحتوي فقط على شهادات سلطة إصدار الشهادة** موضوعة على "خاطئة" أن توزع عبر النعت **قائمة إبطال الشهادة** لنقطة التوزيع المصاحبة، أو عبر النعت **قائمة إبطال الشهادة** لمدخل مُصْدر القائمة CRL، إن كانت لا توجد أي نقطة توزيع محددة.

يكون هذا التوسع حرجاً دائماً. ومستعمل الشهادة الذي لا يفهم هذا التوسع لا يستطيع أن يفترض أن القائمة CRL تحتوي على قائمة كاملة بالشهادات المبطلة من السلطة المعنية. والشهادة CRL التي لا تحتوي على توسعات حرجة يجب أن تحتوي على جميع المداخل الحالية للقائمة CRL التابعة للسلطة المُصْدرة، بما فيها المداخل إلى جميع الشهادات المبطلة: شهادات المستعمل وشهادات السلطة.

ملاحظة 1 – تقع الوسائل التي تستعملها السلطات لتبليغ معلومات الإبطال إلى مُصْدري القوائم CRL خارج نطاق مواصفة الدليل هذه.

ملاحظة 2 – إذا نشرت إحدى السلطات قائمة CRL وفيها المكونة **يحتوي فقط على شهادات المفتاح العمومي للمستعمل** أو المكوّنة **يحتوي فقط على شهادات سلطة إصدار الشهادة**، موضوعة على "صائبة"، يجب على السلطة أن تتأكد من أن جميع شهادات سلطة إصدار الشهادة التي تغطيها هذه القائمة CRL تحتوي على التوسع **التقييدات الأساسية**.

3.2.6.8 توسّع مُصْدر الشهادة

يحدد هذا التوسع في مدخل القائمة CRL، مُصْدر الشهادة المصاحب لمدخل في قائمة CRL غير مباشرة، أي في قائمة CRL يكون فيها المبيّن **القائمة CRL غير المباشرة** موضوعاً في توسع نقطة التوزيع المُصْدرة. وإذا كان هذا التوسع غير موجود في أول مدخل من قائمة CRL غير مباشرة، يكون مُصْدر الشهادة بالتغيب هو مُصْدر القائمة CRL. وإذا كان هذا التوسع غير موجود في مداخل تالية من القائمة CRL غير المباشرة، يكون مصدر الشهادة للمدخل هو نفس المُصْدر في المدخل السابق. ويَعرف هذا الحقل كما يلي:

```
certificateIssuer EXTENSION ::= {
    SYNTAX              GeneralNames
    IDENTIFIED BY       id-ce-certificateIssuer }
```

يكون هذا التوسع حرجاً دائماً. وإذا كان تنفيذ ما يجهل هذا التوسع، لن يستطيع أن يسند المداخل في القائمة CRL بشكل صحيح إلى الشهادات.

4.2.6.8 توسّع مبين القائمة دلتا CRL

يعرّف حقل مبين القائمة دلتا CRL، بقائمة CRL على أنها قائمة دلتا CRL (dCRL) تقدم تحيينات لقائمة أساسية CRL، تعتبر مرجعية. والقائمة الأساسية CRL المرجعية هي قائمة CRL كانت قد صدرت صراحة على أنها قائمة CRL كاملة في مجال تطبيق معين. والقائمة CRL التي تحتوي على التوسع مبين القائمة دلتا CRL تحتوي على تحيينات لوضع الإبطال القانوني لشهادة في نفس هذا المجال التطبيقي. ولا يشتمل مجال التطبيق هذا بالضرورة على جميع دواعي الإبطال أو على جميع الشهادات الصادرة عن سلطة إصدار الشهادة، لا سيما في حالة كون القائمة CRL هي نقطة توزيع القائمة CRL. ومع ذلك فإن تجميعه قائمة CRL تحتوي على التوسع مبيّن القائمة دلتا CRL مع القائمة CRL المرجعية في المكوّنة **رقم القائمة الأساسية CRL (BaseCRLNumber)** من هذا التوسع، تكافئ قائمة CRL كاملة لمجال التطبيق في وقت نشر القائمة dCRL.

ويعرّف هذا الحقل كما يلي:

```
deltaCRLIndicator EXTENSION ::= {
    SYNTAX              BaseCRLNumber
    IDENTIFIED BY       id-ce-deltaCRLIndicator }

BaseCRLNumber ::= CRLNumber
```

وتبين قيمة النمط رقم **القائمة الأساسية CRL** رقم القائمة الأساسية CRL التي اعتمدت كأساس لتوليد هذه القائمة دلتا CRL (dCRL). وتكون القائمة CRL المرجعية هي قائمة CRL كاملة لمجال التطبيق المعني.

ويكون هذا التوسع حرجاً دائماً. ويجب على مستعمل الشهادة الذي لا يفهم استعمال القوائم dCRL، ألا يستعمل قائمة CRL تحتوي على هذا التوسع، نظراً إلى أن القائمة CRL قد لا تكون كاملة، كما يتوقع لها المستعمل.

5.2.6.8 توسع التحيين الأساسي

يستعمل توسع التحيين الأساسي في القوائم dCRL، لكي يحدد التاريخ والوقت اللذين تقدم بعدهما هذه القائمة دلتا تحيينات لوضع الإبطال القانوني. وينبغي ألا يستعمل هذا التوسع إلا في القوائم dCRL التي تحتوي على التوسع **مبين في القائمة دلتا CRL (deltaCRLIndicator)**. والقائمة dCRL التي تحتوي بالعكس على التوسع **مجال تطبيق القائمة CRL**، لا تحتاج إلى هذا التوسع، نظراً إلى أن الحقل **أساس هذا التحيين (baseThisUpdate)** من التوسع **مجال تطبيق القائمة CRL** يمكن استعماله للغرض نفسه.

```
baseUpdateTime EXTENSION        ::= {
    SYNTAX              GeneralizedTime
    IDENTIFIED BY       id-ce-baseUpdateTime }
```

ويكون هذا التوسع غير حرج دائماً.

6.2.6.8 توسع أحدث قائمة CRL

يمكن أن يستعمل توسع أحدث قائمة CRL كتوسع في شهادة أو في قائمة CRL. وفي حالة الشهادة، يمكن استعمال هذا التوسع في الشهادات الصادرة لسلطات وفي الشهادات الصادرة لمستعملين. ويحدد هذا الحقل القائمة CRL التي يجب على مستعمل الشهادة أن يعود إليها لكي يحصل على أحدث معلومات عن الإبطال (أي على آخر قائمة dCRL).

ويعرف هذا الحقل كما يلي:

```
freshestCRL EXTENSION     ::= {
    SYNTAX              CRLDistPointsSyntax
    IDENTIFIED BY       id-ce-freshestCRL }
```

وتكون قيمة النمط **قواعد تركيب نقاط توزيع القوائم CRL (CRLDistPointsSyntax)** كما هي معرفة في توسع نقاط توزيع القوائم CRL المشروح في الفقرة 1.2.6.8.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج، حسب تقدير مُصْدر الشهادة. فإذا وضع توسع أحدث قائمة CRL حرجاً، يجب على نظام استعمال الشهادات ألا يستعمل الشهادة قبل أن يسحب ويتحقق من أحدث قائمة CRL. أما إذا وسم التوسع بأنه غير حرج، فيمكن لنظام استعمال الشهادات أن يستعمل وسائل محلية، لكي يحدد ما إذا كانت أحدث قائمة CRL تحتاج إلى تحقق أم لا.

7.2.6.8 توسع نقطة التوزيع المصدرة لسلطة النعت

يحدد هذا المجال للتوسع في القائمة CRL نقطة توزيع القائمة CRL لشهادات النعت الموجودة في القائمة CRL المعتبرة، ويبين ما إذا كانت هذه الأخيرة غير مباشرة أو أن تطبيقها مقتصر على مجموعة فرعية فقط من معلومات الإبطال. وقد يكون الاقتصار على مجموعة فرعية من مجمل الشهادات أو على مجموعة فرعية من دواعي الإبطال. ويوقّع على القائمة CRL بواسطة المفتاح العمومي لمُصْدر القائمة CRL، نظراً إلى أن نقاط توزيع القوائم CRL بواسطة المفتاح العمومي لمُصْدر القائمة CRL، نظراً إلى أن نقاط توزيع القوائم CRL لا تمتلك أزواج المفاتيح الخاصة بها. وفيما يخص القائمة CRL، الموزعة عبر الدليل، تختزن القائمة CRL في مدخل نقطة توزيع القائمة CRL، الذي قد لا يكون هو مدخل الدليل لمُصْدر القائمة CRL. وإذا كان توسع نقطة التوزيع المُصدرة، وتوَسع نقطة التوزيع المُصْدرة لسلطة النعت، ومجال تطبيق القائمة CRL، كلها غائبة، عندئذ تحتوي القائمة CRL على مداخل لجميع شهادات النعت غير المنتهية صلاحيتها المبطلة والصادرة عن مُصْدر القائمة CRL غائبين كليهما، ولكن نقطة التوزيع لمصْدرة موجودة، لا يعود مجال تطبيق القائمة CRL يتضمن شهادات نعت.

وبعد أن تظهر شهادة في قائمة CRL، يمكن شطبها من قائمة CRL لاحقة، بعد انتهاء صلاحية الشهادة.

ويعرّف هذا الحقل كما يلي:

```
AAissuingDistributionPoint EXTENSION  ::= {
    SYNTAX AAIssuingDistPointSyntax
    IDENTIFIED BY id-ce-AAissuingDistributionPoint }

AAIssuingDistPointSyntax  ::= SEQUENCE {
    distributionPoint           [ 0 ] DistributionPointName OPTIONAL,
    onlySomeReasons             [ 1 ] ReasonFlags OPTIONAL,
    indirectCRL                 [ 2 ] BOOLEAN DEFAULT FALSE,
    containsUserAttributeCerts  [ 3 ] BOOLEAN DEFAULT TRUE,
    containsAACerts             [ 4 ] BOOLEAN DEFAULT TRUE,
    containsSOAPublicKeyCerts   [ 5 ] BOOLEAN DEFAULT TRUE }
```

تحتوي المكوّنة **نقطة التوزيع** اسم نقطة التوزيع بواحد من أشكال الاسم أو بأكثر من واحد. وإذا كانت المكوّنة **بعض الدواعي فقط** موجودة، فإن القائمة CRL تحتوي فقط على إبطالات شهادات النعت للداعي أو للدواعي المحددة، وإلا فإن القائمة CRL تحتوي فقط على إبطالات شهادات النعت للداعي أو للدواعي المحددة، وإلا فإن القائمة CRL تحتوي الإبطالات لجميع الدواعي.

وإذا كانت المكوّنة **القائمة CRL غير المباشرة (indirectCRL)** موضوعة على "صائبة"، يمكن عندئذ للقائمة CRL أن تحتوي على تبليغات بالإبطال لشهادات صادرة عن سلطات غير سلطة مُصْدر القائمة CRL. والسلطة الخاصة المسؤولة عن كل مدخل تكون مبينة في توسع مدخل مُصْدر القائمة CRL للشهادة الواردة في هذا المدخل أو طبقاً لقواعد التغيب المشروحة في الفقرة 3.2.6.8. وفي مثل هذه القائمة، يقع على مسؤولية مصدر القائمة CRL أن يتأكد من أن القائمة CRL كاملة، من حيث احتواؤها على جميع مداخل الإبطالات بطريقة منسجمة مع المبيّنات **يحتوي على شهادات النعت للمستعمل (containsUserAttributeCerts)**، **ويحتوي على شهادات سلطة النعت (containsAACerts)**، **ويحتوي على شهادات المفتاح العمومي لمَصْدر السلطة (containsSOAPublicKeyCerts)**، **وبعض الدواعي فقط (onlySomeReasons)**، القادمة من جميع السلطات التي تعرف هذا المُصدر للقائمة CRL في شهادات النعت الخاصة بها.

وإذا كانت المكوّنة **يحتوي على شهادات النعت للمستعمل** موضوعة على "صائبة"، تكون القائمة CRL تحتوي على إبطالات شهادات النعت الخاصة لكيانات نهائية، ليست هي بالذات سلطات نعت. وإذا كانت المكوّنة **يحتوي على شهادات سلطة النعت** موضوعة على "صائبة"، تكون القائمة CRL تحتوي على إبطالات شهادات النعت الصادرة لأصحاب، هم بالذات سلطات نعت.

وإذا كانت المكوّنة **يحتوي على شهادات المفتاح العمومي لَمصْدر السلطة** موضوعة على "صائبة"، تكون القائمة CRL تحتوي على إبطالات شهادات المفتاح العمومي الصادرة لكيان هو مَصْدر السلطة لأغراض إدارة الامتيازات (أي الشهادات التي تحتوي على التوسع **معرف هوية مَصْدر السلطة (SOAIdentifier)**). وفيما يخص القوائم CRL الموزعة عبر الدليل، تنطبق القواعد التالية. إذا كانت القائمة CRL هي قائمة دلتا CRL (dCRL) يجب توزيعها عبر النعت **قائمة إبطال القوائم دلتا (deltaRevocationList)** لنقطة التوزيع المصاحبة، أو عبر النعت قائمة إبطال القوائم دلتا لمدخل مُصْدر القائمة CRL، إن كانت لا توجد أي نقطة توزيع محددة، مهما تكن حالات الشهادات التي تغطيها القائمة CRL. وفي غير الحالة التي تكون فيها القائمة CRL هي قائمة دلتا CRL (dCRL)، يتحقق ما يلي:

- إن القائمة CRL، التي لا تحتوي على التوسع **نقطة التوزيع المُصْدرة** الذي تكون فيه المكوّنة **يحتوي على شهادات سلطة النعت** و/أو المكوّنة يحتوي على **شهادات المفتاح العمومي لَمصْدر السلطة** فقط هي المنشَّطة، يجب أن توزع عبر النعت **قائمة إبطال سلطات النعت (attributeAuthorityRevocationList)** لنقطة التوزيع المصاحبة، أو عبر النعت **قائمة إبطال سلطات النعت** لمدخل مُصْدر القائمة CRL، إن كانت لا توجد أي نقطة توزيع محددة.
- إن القائمة CRL، التي لا تحتوي على **التوسع نقطة التوزيع المُصْدرة** الذي تكون فيه المكوّنة **يحتوي على شهادات نعت المستعمل** منشَّطة (مع أو بدون المكوّنة **يحتوي على شهادات سلطة النعت** و/أو المكوّنة **يحتوي على شهادات المفتاح العمومي لَمصْدر السلطة** منشطتين أيضاً)، يجب أن توزع عبر النعت **قائمة إبطال شهادات النعت (attributeCertificateRevocationList)** لنقطة التوزيع المصاحبة، أو عبر النعت **قائمة إبطال شهادات النعت** لمدخل مُصْدر القائمة CRL، إن كانت لا توجد أي نقطة توزيع محددة.
- إن القائمة CRL، التي تحتوي على التوسع **نقطة التوزيع المُصْدرة**، يجب أن توزع كما هو محدد في الفقرة 8.2.2.6.

ويكون هذا التوسع حرجاً دائماً. ومستعمل الشهادة الذي لا يفهم هذا التوسع لا يستطيع أن يفترض أن القائمة CRL تحتوي على قائمة كاملة للشهادات المبطلة التابعة للسلطة المحددة. والقوائم CRL التي لا تحتوي على توسعات حرجة لن تحتوي على جميع المداخل الحالية للقوائم CRL التابعة لسلطة الإصدار، بما فيها جميع الشهادات المبطلة: شهادات المستعمل وشهادات السلطة.

ملاحظة 1 – تقع الوسائل التي تستعملها السلطات لتبليغ معلومات الإبطال إلى مُصْدري القوائم CRL خارج نطاق مواصفة الدليل هذه.

ملاحظة 2 – إذا نشرت إحدى السلطات قائمة CRL وفيها المكوّنة **يحتوي على شهادات سلطة النعت** موضوعة على "صائبة" والمكوّنة **يحتوي على شهادات النعت للمستعمل** غير موضوعة على "صائبة"، يجب على السلطة أن تتأكد من أن جميع شهادات سلطة النعت التي تغطيها هذه القائمة CRL تحتوي على التوسع **تقييدات النعت الأساسية (basicAttConstraints)**.

ملاحظة 3 – إذا نشرت إحدى السلطات قائمة CRL وفيها المكونة **يحتوي على شهادات المفتاح العمومي لَمصْدر السلطة** موضوعة على "صائبة"، يجب على السلطة أن تتأكد من أن جميع شهادات مَصْدر السلطة التي تغطيها القائمة CRL تحتوي على التوسع **معرف هوية مَصْدر السلطة (SOAIdentifier)**.

9 العلاقات بين القائمة دلتا CRL والقائمة الأساسية CRL

تحتوي القائمة دلتا CRL (dCRL) على التوسع **مبين القائمة دلتا CRL (deltaCRLIndicator)** أو على التوسع **مجال تطبيق القائمة CRL (crlScope)**، لكي تبين معلومات الإبطال الأساسية التي تحيّنها هذه القائمة dCRL.

فإذا كان التوسع **مبيّن القائمة دلتا CRL** موجوداً في قائمة dCRL، تكون معلومات الإبطال الأساسية التي يجري تحيينها هي القائمة الأساسية CRL المرجعية الموجودة في هذا التوسع. والقائمة الأساسية CRL التي يحيل إليها التوسع **مبيّن القائمة دلتا CRL** هي قائمة CRL صادرة باعتبارها كاملة في مجال تطبيقها (أي إنها ليست بحدّ ذاتها قائمة dCRL.

وإذا كان التوسع **مجال تطبيق القائمة CRL** موجوداً ويحتوي على المكوّنة **معلومات الإبطال الأساسية (baseRevocationInfo)** التي تحيل إلى معلومات الإبطال الأساسية التي يجري تحيينها، تكون هذه الإحالة عندئذ إلى وقت معين، تقدم هذه القائمة dCRL التحيينات اعتباراً منه. وتحيل المكوّنة **معلومات الإبطال الأساسية** إلى قائمة CRL يمكن أن تكون أو لا تكون قد أصدرت على أنها كاملة في مجال التطبيق هذا (أي قد تكون القائمة CRL المحال غليها قد أصدرت كقائمة دلتا CRL). في جميع الأحوال، فإن القائمة dCRL التي تحتوي على المكوّنة **معلومات الإبطال الأساسية** تحيّن معلومات الإبطال التي هي كاملة لمجال تطبيق القائمة CRL المرجعية. ويستطيع مستعمل الشهادة أن يطبق القائمة dCRL على قائمة CRL هي كاملة بالنسبة لمجال تطبيق معين وكانت قد صدرت في نفس وقت صدور القائمة CRL المحال إليها في القائمة dCRL الحاوية على المكوّنة **معلومات الإبطال الأساسية** أو بعد هذا الوقت.

وخشية احتمال وقوع معلومات متعارضة، يجب ألا تحتوي قائمة CRL معاً على التوسع **مبيّن القائمة دلتا CRL** وعلى التوسع **مجال تطبيق القائمة CRL** الذي يحتوي على المكوّنة **معلومات الإبطال الأساسية**. ولكن يمكن لقائمة CRL أن تحتوي معاً على التوسع **مبيّن القائمة دلتا CRL** وعلى التوسع **مجال تطبيق القائمة CRL**، شريطة ألا يحتوي التوسع الأخير على المكوّنة **معلومات الإبطال الأساسية**.

ويمكن لقائمة dCRL أن تكون قائمة CRL غير مباشرة، إن كان يمكن لها أن تحتوي على معلومات إبطال محيّنة خاصة بقوائم CRL أساسية صادرة عن سلطة واحدة أو عن عدة سلطات. ويجب استعمال التوسع **مجال تطبيق القائمة CRL** كوسيلة تبيّن كون قائمة CRL هي قائمة دلتا CRL غير مباشرة. ويجب أن يحتوي **مجال تطبيق القائمة CRL** مطابقاً واحداً من المكوّنة **مجال التطبيق لكل سلطة (PerAuthorityScope)** لكل واحدة من القوائم الأساسية CRL التي تقدم لها القائمة دلتا CRL غير المباشرة، معلومات محيّنة.

ويتعين على تطبيق قائمة dCRL على معلومات الإبطال الأساسية المرجعية أن يأخذ بالاعتبار بكل دقة الوضع القانوني الحالي للإبطال.

- قد يظهر التبليغ عن إبطال شهادة مع كون داعي الإبطال هو **الشهادة في الانتظار (certificateHold)**، إما في قائمة دلتا CRL وإما في قائمة CRL كاملة بخصوص مجال تطبيق معين. وشفرة الداعي هذه مهيأة لكي تدل على إبطال مؤقت للشهادة، بانتظار قرار لاحق يحدد إبطال الشهادة نهائيا أو إعادتها إلى حالتها السابقة، كما لو لم تكن قد أبطلت.

- إذا كانت شهادة قد أدرجت في قائمة CRL (إما قائمة dCRL وإما قائمة CRL كاملة بخصوص مجال تطبيق معين)، باعتبارها مبطلة بداعي الإبطال **الشهادة في الانتظار، ورقم القائمة CRL** هو *n*، ثم ألغي وضعها في الانتظار لاحقاً، يجب إدراج الشهادة في جميع القوائم dCRL الصادرة بعد إلغاء الوضع في الانتظار وحيث يكون **رقم القائمة CRL** للقائمة CRL الأساسية المرجعية يساوي أو يقل عن *n*. وحسب التوسع الذي يستعمل للدلالة على أن هذه القائمة CRL هي قائمة دلتا CRL، يكون رقم القائمة CRL لقائمة CRL أساسية مرجعية هو إما قيمة المكوّنة **رقم القائمة الأساسية CRL (BaseCRLNumber)** في التوسع **مبين القائمة دلتا CRL**، وإما قيمة العنصر **رقم القائمة CRL** في المكوّنة **معلومات الإبطال الأساسية** من التوسع **مجال تطبيق القائمة CRL**. وتدرج الشهادة في القائمة مع كون داعي الإبطال هو **السحب من القائمة CRL (removeFromCRL)**، ما لم تكن الشهادة قد أبطلت ثانية فيما بعد لأحد دواعي الإبطال التي تغطيها القائمة dCRL، وعندئذ يجب إدراج الشهادة مع داعي الإبطال الخاص بالإبطال اللاحق.

- وإذا لم تكن الشهادة قد سحبت من الوضع في الانتظار، بل تم إبطالها نهائياً، يجب إدراجها عندئذ في جميع القوائم dCRL التي يكون فيها **رقم القائمة CRL** الأساسية المرجعية أقل من **رقم القائمة CRL** للقائمة CRL (إما قائمة dCRL وإما قائمة CRL كاملة في مجال تطبيق معين) التي ظهر فيها لأول مرة تبليغ الإبطال النهائي. وحسب التوسع الذي يستعمل للدلالة على أن هذه القائمة CRL هي قائمة دلتا CRL، يكون رقم القائمة CRL لقائمة CRL أساسية مرجعية هو إما قيمة المكوّنة **رقم القائمة الأساسية CRL** في التوسع **مبيّن القائمة دلتا CRL**، وإما قيمة العنصر **رقم القائمة CRL** في المكونة **معلومات الإبطال الأساسية** من التوسع **مجال تطبيق القائمة CRL**.

- وقد يظهر التبليغ عن إبطال شهادة لأول مرة في قائمة دلتا CRL، ويحتمل أن تنتهي مدة صلاحية الشهادة قبل صدور القائمة CRL التالية التي هي كاملة بخصوص مجال التطبيق المعني. وفي مثل هذه الحالة، يجب أن يرد التبليغ عن الإبطال في جميع القوائم dCRL اللاحقة، إلى أن يظهر التبليغ عن الإبطال على الأقل في قائمة CRL صادرة وهي كاملة بخصوص مجال تطبيق الشهادة.

يمكن إنشاء قائمة CRL تكون كاملة في الوقت الحالي بخصوص مجال تطبيق معين إنشاءً محلياً بواحدة من الطريقتين التاليتين:

- تستخرج القائمة dCRL الحالية بخصوص مجال التطبيق هذا، وتدمج مع قائمة CRL كاملة صادرة بخصوص هذا المجال من التطبيق، يكون **رقم القائمة CRL** فيها يساوي أو أكبر من الرقم الوارد في القائمة CRL الأساسية التي تحيل إليها القائمة dCRL؛

- تستخرج القائمة dCRL الحالية بخصوص مجال التطبيق هذا، وتدمج مع قائمة CRL كاملة بخصوص هذا المجال من التطبيق، كانت قد أنشئت محلياً من قائمة dCRL، يكون **رقم القائمة CRL** فيها يساوي أو أكبر من الرقم الوارد في القائمة CRL الأساسية التي تحيل إليها القائمة dCRL الحالية.

10 إجراءات معالجة مسيرة إصدار الشهادة

تجري معالجة مسيرة إصدار الشهادة في نظام يحتاج إلى استخدام المفتاح العمومي لكيان نهائي بعيد، للتحقق مثلاً من توقيع رقمي ولّده مثل هذا الكيان البعيد. لقد صممت التوسعات: سياسات الشهادة، والتقييدات الأساسية، وتقييدات الأسماء، وتقييدات السياسة لكي تسهل التنفيذ الأوتوماتي والمستقل ذاتياً لمنطق معالجة مسيرة إصدار الشهادة.

والعرض الموجز التالي هو الخطوط العريضة لإجراء الإقرار بصلاحية مسيرات إصدار الشهادة. ويجب أن يكون التنفيذ مكافئاً من حيث الوظيفة لسلوك خارجي ناتج عن هذا الإجراء. ولم يتم تقييس الخوارزمية التي يستعملها تنفيذ معين لاشتقاق المُخْرَج أو المُخْرجَات الصحيحة انطلاقاً من مُدْخَلات معينة.

1.10 مُدْخَلات معالجة المسيرة

مُدْخَلات الإجراءات لمعالجة مسيرة إصدار الشهادة هي:

أ) مجموعة الشهادات التي تشكل مسيرة إصدار الشهادة؛

ملاحظة – تكون كل شهادة موجودة في مسيرة إصدار الشهادة، وحيدة. وكل مسيرة تحتوي على نفس الشهادة مرتين أو أكثر، لا تكون مسيرة إصدار شهادة صالحة.

ب) قيمة موثوقة لمفتاح عمومي أو لمعرّف بهوية مفتاح (إن كان المفتاح مختزناً داخلياً من وحدة معالجة مسيرة إصدار الشهادة)، لكي تستعمل في التحقق من أول شهادة واقعة في مسيرة إصدار الشهادة؛

ج) *مجموعة سياسات أولية (initial-policy-set)* تتكون من محدّد واحد أو أكثر لسياسة الشهادة، لتبين أن أي واحدة من هذه السياسات يمكن أن تكون مقبولة من مستعمل الشهادة لأغراض معالجة مسيرة إصدار الشهادة. ويمكن لهذا المُدْخل أن يأخذ القيمة الخاصة *أي سياسة (any-policy)*، ولكنه لا يمكن أن يكون معدوماً؛

د) قيمة لمبيّن *سياسة صريحة أولية (initial-explicit-policy)*، تدل إن كان محدّد سياسة مقبولة يجب أن يظهر صراحة في حقل توسع سياسات الشهادة في جميع شهادات المسيرة؛

هـ) قيمة لمبيّن *حظر أولي التقابل السياسات (initial-policy-mapping-inhibit)*، تدل إن كان تقابل السياسات محظوراً في مسيرة إصدار الشهادة؛

و) قيمة لمبيّن *سياسة حظر أولي (initial-inhibit-policy)*، تدل عما إذا كانت القيمة الخاصة **لأي سياسة (anyPolicy)**، حين تكون موجودة في توسع سياسات الشهادة، تعتبر موائمة لأي قيمة خاصة من سياسة الشهادة موجودة في مجموعة خاضعة لتقييدات؛

ز) التاريخ والوقت الحاليان (إن كانا غير متيسرين داخلياً في وحدة معالجة مسيرة إصدار الشهادة)؛

ح) *مجموعة أولية من الأشجار الفرعية المسموحة (initial-permitted-subtrees-set)* تحتوي على مجموعة أولية من مواصفات الشجرة الفرعية التي تعرّف الأشجار الفرعية التي تكون فيها أسماء الصاحب مسموحة (من شكل الأسماء المستعملة لتعيين الأشجار الفرعية). وفي الشهادات الموجودة داخل مسيرة إصدار الشهادة يتعين على جميع أسماء الصاحب التي لها شكل اسم معين والتي تكون أشجارها الفرعية الأولية معرّفة، أن تقع داخل مجموعة الأشجار الفرعية المسموحة لشكل الاسم المعين هذا. ويمكن لهذا المُدْخل أن يحتوي أيضاً على القيمة المعينة "غير المرتبطة" لكي تدل على جميع أسماء الصاحب المقبولة في البداية. وفي نظر البند 10، تكون أسماء الصاحب هي قيم الأسماء التي تظهر في حقل الصاحب أو في توسع الاسم البديل للصاحب؛

ط) *مجموعة أولية من الأشجار الفرعية المستبعدة (initial-excluded-subtrees-set)* تحتوي على مجموعة أولية من مواصفات الشجرة الفرعية التي تعرّف الأشجار الفرعية التي لا يمكن أن تقع فيها أسماء الصاحب الواردة في الشهادة الموجودة في مسيرة إصدار الشهادة. ويمكن لهذا المُدْخل أن يكون أيضاً مجموعة خالية لكي يدل على أنه لم يكن يوجد في البداية استبعاد ساري المفعول لأشجار فرعية؛

ي) *أشكال اسم مطلوبة أولية (initial-required-name-forms)* تحتوي على مجموعة أولية من أشكال الاسم تدل على أن جميع الشهادات الموجودة في المسيرة يجب أن تحتوي على الأقل اسم صاحب واحداً من أشكال الأسماء المعيّنة. ويمكن لهذا المُدْخل أن يكون أيضاً مجموعة خالية لكي يدل على أنه لا توجد أشكال أسماء معينة مطلوبة لأسماء الصاحب في الشهادات.

تتوقف القيم الواردة في الفقرات ج) ود) وهـ) وو) على المتطلبات السياسية التي يحتاجها الزوج المستعمل – التطبيق لاستعمال مفتاح عمومي مصدّق عليه للكيان النهائي.

وتجدر الملاحظة بأن هذه المدخلات هي إفرادية في عملية إقرار الصلاحية للمسيرة، لذلك فهي تفيد في جعل مستعمل شهادة يحدّ من ثقته التي يضعها في مفتاح عمومي موثوق للمجموعة المعينة من سياسات الشهادة. ويمكن تأمين ذلك بضمان كون مفتاح عمومي معين هو المُدْخل إلى العملية، فقط إذا كان مُدْخل مجموعة السياسات الأولية يشتمل على سياسات تجعل مستعمل الشهادة يثق بالمفتاح العمومي. ولما كانت مسيرة إصدار الشهادة هي نفسها تشكل مُدْخلاً آخر إلى العملية، يمكن إجراء هذا التحقق على أساس كل معاملة لوحدها.

2.10 مُخْرجات معالجة المسيرة

مُخْرجات الإجراءات هي:

أ) دلالة على نجاح أو فشل إقرار الصلاحية لمسيرة إصدار الشهادة؛

ب) في حالة فشل إقرار الصلاحية، شفرة تشخيصية تبيّن داعي الفشل؛

ج) مجموعة من السياسات تفرضها السلطة وواصفاتها المصاحبة التي تكون بموجبها مسيرة إصدار الشهادة صالحة، أو تكون القيمة الخاصة *أي سياسة*؛

د) مجموعة من السياسات يفرضها المستعمل، مشكَّلة من تقاطع *مجموعة السياسات التي تفرضها السلطة ومجموعة السياسات الأولية*؛

هـ) *مبيّن السياسة الصريحة* الذي يدل عما إذا كان مستعمل الشهادة أو سلطة موجودة داخل المسيرة، هو الذي يتطلب أن تتحدد سياسة مقبولة في كل شهادة موجودة في المسيرة؛

و) تفصيلات عن أي تقابل سياسات يحدث أثناء معالجة مسيرة إصدار الشهادة.

ملاحظة – في حالة نجاح إقرار الصلاحية، يحتمل أن يبقى نظام استعمال الشهادات يختار ألا يستعمل الشهادة، كنتيجة لقيم واصفات السياسة أو غيرها من المعلومات الموجودة في الشهادة.

3.10 متحولات معالجة المسيرة

تستعمل الإجراءات المجموعة التالية من متحولات الحالة:؛

أ) *مجموعة السياسات المفروضة من السلطة (authorities-constrained-policy-set)*: جدول بمعرّفات هوية السياسات وواصفاتها، مأخوذ من الشهادات الموجودة في مسيرة إصدار الشهادة (الصفوف فيه تمثل السياسات وواصفاتها وتاريخ التقابل، بينما الأعمدة تمثل الشهادات الموجودة في مسيرة إصدار الشهادة)؛

ب) *الأشجار الفرعية المسموحة (permitted-subtrees)*: مجموعة من مواصفات الأشجار الفرعية، تعرّف الأشجار الفرعية التي تقع فيها جميع أسماء الصاحب الموجودة في الشهادات اللاحقة في مسيرة إصدار الشهادة، أو القيمة الخاصة *غير المرتبطة (unbounded)*؛

ج) *الأشجار الفرعية المستبعدة (excluded-subtrees)*: مجموعة (ربما خالية) من مواصفات الأشجار الفرعية (تحتوي كل منها على اسم أساسي لشجرة فرعية ومبيّني سويتين عظمى وصغرى) تعرّف الأشجار الفرعية التي يمكن ألا يقع فيها أي اسم صاحب موجود في شهادة لاحقة في مسيرة إصدار الشهادة؛

د) *أشكال أسماء مطلوبة (required-name-forms)*: مجموعة (ربما خالية) من مجموعات أشكال الأسماء. وفي كل مجموعة من أشكال الأسماء، يجب أن تحتوي كل شهادة لاحقة اسماً من واحد من أشكال الأسماء الواردة في المجموعة؛

هـ) *مبيّن سياسة صريحة (explicit-policy-indicator)*: يبيّن إن كان يلزم أن تتحدد بصراحة سياسة مقبولة في كل شهادة موجودة في المسيرة؛

و) *عمق المسيرة (path depth)*: عدد صحيح يساوي عدد الشهادات الموجودة في مسيرة إصدار الشهادة، مضافاً إليه واحد، التي اكتملت معالجتها؛

ز) *مبيّن حظر تقابل السياسات (policy-mapping-inhibit-indicator)*: يبين إن كان تقابل السياسات محظوراً؛

ح) *مبيّن حظر أي سياسة (inhibit-any-policy-indicator)*: يبين إن كانت القيمة الخاصة **أي سياسة (anyPolicy)** تعتبر موائمة لأي سياسة خاصة بشهادة؛

ط) *تقييدات في الانتظار (pending-constraints)*: تفصيلات عن التقييدات: سياسة صريحة و/أو حظر تقابل السياسات و/أو حظر أي سياسة، التي هي مشترطة، ولكنها لم تصبح بَعْد سارية المفعول. وتوجد ثلاثة مبيّنات ذات بتة واحدة تسمى *سياسة صريحة في الانتظار (explicit-policy-pendin)*، *وحظر أي سياسة في الانتظار (inhibit-pending and inhibit-any-policy-pending)*، ومع كل واحد منها عدد صحيح يدعى *الشهادات المفوّتة (المتجاهلة) (skip-certificates)* الذي يعطي عدد الشهادات التي ينبغي تجاهلها قبل أن تصبح التقييدات سارية المفعول.

4.10 مرحلة التدميث

تتضمن الإجراءات مرحلة تدميث، تليها سلسلة من مراحل معالجة الشهادة. وتشتمل مرحلة التدميث على:

أ) كتابة القيمة *أي سياسة* في العمودين صفر وواحد من الصف صفر في جدول *مجموعة أولية من الأشجار الفرعية المسموحة*؛

ب) تدميث المتحول *الأشجار الفرعية المسموحة* بالقيمة *مجموعة أولية من الأشجار الفرعية المسموحة*؛

ج) تدميث المتحول *الأشجار الفرعية المستبعدة* بالقيمة *مجموعة أولية من الأشجار الفرعية المستبعدة*؛

د) تدميث المتحول *أشكال الاسم المطلوبة* بالقيمة *أشكال الاسم الأولية المطلوبة*؛

هـ) تدميث *مبين سياسة صريحة* بالقيمة *سياسة صريحة أولية*؛

و) تدميث *عمق المسيرة* بالقيمة واحد؛

ز) تدميث *مبين حظر تقابل السياسات* بالقيمة *حظر أولي لتقابل السياسات*؛

ح) تدميث *مبين حظر أي سياسة* بالقيمة *سياسة حظر أولي*؛

ط) تدميث ثلاثة *تقييدات في الانتظار* بالقيمة "غير موضوعة".

5.10 معالجة الشهادة

ثم تعالج كل شهادة بدورها، بدءاً بالشهادة الموقعة باستعمال المفتاح العمومي الموثوق كَمُدْخل، وتعتبر آخر شهادة هي الشهادة النهائية. وتعتبر بقية الشهادات الأخرى شهادات وسيطة.

1.5.10 التحقق الأساسي من الشهادات

تطبق التحققات التالية على الشهادة. ويتم تجاهل الشهادات الموقعة من ذاتها، عندما تصادف في المسيرة.

أ) التحقق من أن التوقيع صحيح، وأن التواريخ صالحة، وأن اسم مُصْدر الشهادة واسم صاحب الشهادة واردان بتسلسل صحيح، وأن الشهادة لم يجر إبطالها.

ب) في حالة شهادة وسيطة بالصيغة 3، التحقق من وجود التوسع **التقييدات الأساسية (basicConstraints)**، ومن أن المكوّنة **سلطة إصدار الشهادة (cA)** الموجودة في توسع التقييدات الأساسية موضوعة على **"صائبة"**. وإذا كانت المكوّنة **تقييد طول المسيرة (pathLenConstraint)** موجودة، التحقق من أن **مسيرة إصدار الشهادة** الحالية لا تنتهك هذا التقييد (مع تجال الشهادات الوسيطة الصادرة لذاتها).

ج) إذا كان التوسع سياسات الشهادة غير موجود، توضع **مجموعة السياسات المفروضة من السلطة** على الصفر (مجموعة خالية)، بشطب جميع الصفوف الموجودة في الجدول *مجموعة السياسات المفروضة من السلطة*.

د) إذا كان توسع سياسات الشهادة موجوداً، يرفق بكل سياسة P موجودة في التوسع غير **أي سياسة**، واصفات السياسة المصاحبة للسياسة P، في كل صف من الجدول *مجموعة السياسات المفروضة من السلطة* يحتوي على القيمة P. وإذا كان لا يوجد أي صف في الجدول *مجموعة السياسات المفروضة من السلطة* يحتوي على القيمة P في مدخل عموده [*عمق المسيرة*]، غير أن القيمة هي *أي سياسة* في *مجموعة السياسات المفروضة من السلطة* [0، *عمق المسيرة*]، عندئذ يضاف صف جديد إلى الجدول بنسخ الصف صفر وكتابة معرف هوية السياسة P مع واصفاته في مدخل العمود [*عمق المسيرة*] من الصف الجديد.

هـ) إذا كان توسع سياسات الشهادة موجوداً، ولا يحتوي على القيمة **أي سياسة**، أو إذا كان *مبّين حظر أي سياسة* موضوعاً، وكانت الشهادة ليست شهادة وسيطة صادرة لذاتها، عندئذ يشطب أي صف يكون فيه مدخل العمود [*عمق المسيرة*] يحتوي على القيمة *أي سياسة*، ومعه كل صف لا يحتوي فيه مدخل العمود [*عمق المسيرة*] على واحدة من القيم الموجودة في توسع سياسات الشهادة.

و) إذا كان توسع سياسات الشهادة موجوداً، ويحتوي على القيمة **أي سياسة**، وكان *مبيّن حظر أي سياسة* غير موضوع، عندئذ ترفق واصفات السياسة المتصاحبة مع **أي سياسة** في كل صف من الجدول *مجموعة السياسات المفروضة من السلطة* يكون فيه مدخل العمود [*عمق المسيرة*] يحتوي على القيمة *أي سياسة* أو يحتوي على قيمة لا تظهر في توسع سياسات الشهادة.

ز) إذا كانت الشهادة ليست شهادة وسيطة صادرة لذاتها، التحقق من أن اسم الصاحب وارد في مكان الاسم الذي تعطيه قيمة *الأشجار الفرعية المسموحة*، وليس في مكان الاسم الذي تعطيه قيمة الأشجار الفرعية المستبعدة.

ح) إذا كانت الشهادة ليست شهادة وسيطة صادرة لذاتها، وكانت المجموعة *أشكال الأسماء المطلوبة* ليست مجموعة خالية، التحقق في كل مجموعة من أشكال الاسم الموجودة في *أشكال الأسماء المطلوبة*، من وجود اسم صاحب في الشهادة هو واحد من أشكال الاسم الوارد في المجموعة.

2.5.10 معالجة الشهادات الوسيطة

في حالة شهادة وسيطة، تؤدى الأعمال التالية لتسجيل التقييد، بغية الموضعة الصحيحة لمتحولات الحالة من أجل معالجة الشهادة التالية. ويتم تجاهل الشهادات الموقعة من ذاتها، عندما تصادف في المسيرة.

أ) إذا كان التوسع **تقييدات الأسماء (nameConstraints)** والمكوّنة **الأشجار الفرعية المسموحة (permittedSubtrees)** موجودين في الشهادة، يستعاض عن قيمة متحول الحالة *الأشجار الفرعية المسموحة* بتقاطع قيمته السابقة مع القيمة المبينة في توسع الشهادة.

ب) إذا كان التوسع **تقييدات الأسماء (nameConstraints)** موجوداً في الشهادة مع لمكوّنة **الأشجار الفرعية المستبعدة (excludedSubtrees)**، يستعاض عن قيمة متحول الحالة *الأشجار الفرعية المستبعدة* باجتماع قيمته السابقة مع القيمة المبينة في توسع الشهادة.

ج) إذا كان التوسع **تقييدات الأسماء (nameConstraints)** **والمكوّنة أشكال الأسماء المطلوبة (requiredNameForms)** موجودين في الشهادة، يعطى المتحول أشكال الأسماء المطلوبة قيمة اجتماع قيمته السابقة مع المجموعة المكوّنة من مجموعة أشكال الأسماء المحددة في توسع الشهادة. وإذا كانت المكوّنة **أشكال الأسماء المطلوبة** تحتوي على أكثر من شكل واحد للاسم، فإن المتحول *أشكال الأسماء المطلوبة* يشير إلى أن اسماً لواحد على الأقل من أشكال الاسم المبينة في هذا التوسع، يجب أن يكون موجوداً في جميع الشهادات اللاحقة. ويكون اجتماع قيمة المتحول أشكال الأسماء المطلوبة مع قيمة من توسع الشهادة الحالية هو مجموعة مجموعات تشير إلى المتطلبات الواجب تحققها لجميع الشهادات اللاحقة. فإذا وضع مثلاً المتحول *أشكال الأسماء المطلوبة* الحالي على قيمة تتطلب وجود اسم مميز (DN) أو اسم طلب rfc822 في الشهادات، وكان التوسع الحالي للشهادة الموجودة قيد المعالجة يدل على تطلّب أسماء rfc822 أو أسماء من مكان اسم الميدان (DNS)، فإن الاجتماع الناتج، أي المتحول الجديد *أشكال الأسماء المطلوبة*، يدل على أن كل شهادة لاحقة يجب أن يكون لها اسم rfc822 أو أن يكون لها بنفس الوقت اسم مميز (DN) مع اسم من مكان اسم الميدان (DNS).

د) إذا كان *مبين حظر تقابل السياسات* موضوعاً:

- يعالج كل توسع لتقابل السياسات، من أجل كل تقابل محدّد في التوسع، بتحديد مواقع جميع الصفوف الموجودة في جدول *مجموعة السياسات المفروضة من السلطة* التي يكون فيها مدخل العمود [*عمق المسيرة*] مساوياً قيمة سياسة الميدان للمُصْدر في التوسع، ويشطب الصف.

هـ) إذا كان *مبين حظر تقابل السياسات* غير موضوع:

- يعالج كل توسع لتقابل السياسات، من أجل كل تقابل محدّد في التوسع، بتحديد مواقع جميع الصفوف الموجودة في جدول *مجموعة السياسات المفروضة من السلطة* التي يكون فيها مدخل العمود [*عمق*

المسيرة] مساوياً قيمة سياسة الميدان للمُصْدر في التوسع، وبكتابة قيمة سياسة الميدان للصاحب الوارد في التوسع في مدخل [*عمق المسيرة*+1] من نفس الصف. وإذا كان التوسع يقابل سياسة ميدان المُصْدر بأكثر من سياسة ميدان واحدة لصاحب، ينسخ عندئذ الصف المتأثر، ويضاف المدخل الجديد إلى كل صف. وإذا كانت قيمة العنصر *مجموعة السياسات المفروضة من السلطة* [0، *عمق المسيرة*] هي *أي سياسة*، يكتب عندئذ معرف هوية كل سياسة ميدان لمُصْدر، من توسع تقابل السياسات في عمود [*عمق المسيرة*] وتضاعف الصفوف بالقدر اللازم، ويحتفظ بالمواصفات إن كانت موجودة، وتكتب قيمة سياسة الميدان للصاحب، من التوسع في مدخل العمود [*عمق المسيرة*+1] من نفس الصف؛

- إذا كان المبين *في انتظار حظر تقابل السياسات* موضوعاً، وكانت الشهادة ليست شهادة صادرة لذاتها، يجري إنقاص قفزي لقيمة *الشهادات المفوّتة* المقابلة، وإذا أصبحت هذه القيمة مساوية للصفر، يوضع *مبّين حظر تقابل الشهادات*؛

- إذا كان التقيد **حظر تقابل السياسات (inhibitPolicyMapping)** موجوداً في الشهادة، ينفذ التالي. إذا كانت قيمة المكوّنة **الشهادة المفوّتة (SkipCerts)** تساوي الصفر، يوضع *مبّين حظر تقابل الشهادات*. ومن أجل أي قيمة أخرى للمكوّنة **الشهادات المفوّتة** يوضع المبين *في انتظار حظر تقابل الشهادات*، وتوضع قيمة *الشهادات المفوّتة* المقابلة على أصغر قيمة للمكوّنة **الشهادات المفوّتة** وللقيمة السابقة للمتحول *الشهادات المفوّتة* (إن كان المبين *في انتظار حظر تقابل الشهادات* موضوعاً سلفاً).

و) فيما يخص كل صف غير معدل في المرحلة ج) أو د) أعلاه (وما يخص كل صف عندما لا يوجد أي توسع تقابل في الشهادة)، تنسخ قيمة معرف هوية السياسة من العمود [*عمق المسيرة*] إلى العمود [*عمق المسيرة*+1] في الصف.

ز) إذا كان *مبين حظر أي سياسة غير موضوع:*

- إذا كان المبين في *انتظار حظر أي سياسة* موضوعاً، وكانت الشهادة ليست صادرة لذاتها، تنقص قفزياً قيمة *الشهادات المفوّتة* المقابلة، وعندما تصبح هذه القيمة مساوية صفراً، يوضع *مبين حظر أي سياسة*؛

- إذا كان التقيد **حظر أي سياسة (inhibitAnyPolicy)** موجوداً في الشهادة، ينفذ التالي. إذا كانت المكوّنة **الشهادة المفوّتة (SkipCerts)** ذات قيمة صفر، يوضع *مبّين حظر أي سياسة*. ومن أجل أي قيمة أخرى للمكوّنة **الشهادات المفوّتة** يوضع المبين *في انتظار حظر أي سياسة*، وتوضع قيمة *الشهادات المفوّتة* المقابلة على أصغر القيمتين للمكوّنة **الشهادات المفوّتة** وللقيمة السابقة للمتحول *الشهادات المفوّتة* (إن كان المبين *في انتظار حظر أي سياسة* موضوعاً سلفاً).

ح) يزاد قفزياً المتحول [*عمق المسيرة*].

3.5.10 معالجة مبين سياسة صريحة

تطبق بعدئذ الإجراءات التالية بشأن جميع الشهادات:

أ) إذا كان *مبين سياسة صريحة* غير موضوع:

- إذا كان *مبين سياسة صريحة في الانتظار* موضوعاً، وكانت الشهادة ليست شهادة وسيطة صادرة لذاتها، تنقص قفزياً قيمة *الشهادات المفوّتة* المقابلة، وعندما تصبح هذه القيمة مساوية صفراً، يوضع *مبين سياسة صريحة*.

- وإذا كان التقييد **سياسة صريحة مطلوبة (requireExplicitPolicy)** موجوداً في الشهادة، ينفذ التالي. إذا كانت قيمة المكوّنة **الشهادة المفوّتة (SkipCerts)** تساوي الصفر، يوضع *مبين سياسة صريحة*. ومن أجل أي قيمة أخرى للمكونة **الشهادات المفوّتة**، يوضع المبين **سياسة صريحة في الانتظار**، وتوضع قيمة

الشهادات المفوتة المقابلة على أصغر القيمتين للمكونة **الشهادات المفوتة** وللقيمة السابقة للمتحول *الشهادات المفوتة* (إن كان المبين *سياسة صريحة في الانتظار* موضوعاً سلفاً).

- وإذا كانت المكوّنة **سياسة صريحة مطلوبة (requireExplicitPolicy)** موجودة، وكانت مسيرة إصدار الشهادة تشتمل على شهادة صادرة عن سلطة مسمّاة لإصدار الشهادة، يلزم على جميع الشهادات الموجودة في المسيرة أن تحتوي في توسع سياسات الشهادة على معرف هوية مقبول للسياسة. ومعرف الهوية المقبول للسياسة هو معرف الهوية لسياسة الشهادة الذي يتطلبه مستعمل مسيرة إصدار الشهادة، أو هو معرف الهوية لسياسة كان قد صُرّح بشأنها أنها مكافئة للأولى عبر تقابل السياسات، أو القيمة الخاصة *"أي سياسة"*. ويمكن لسلطة إصدار الشهادة المسمّاة أن تكون إما السلطة المُصْدرة للشهادة الحاوية على هذا التوسع (إن كانت قيمة المكوّنة **سياسة صريحة مطلوبة** تساوي الصفر)، وإما سلطة إصدار الشهادة التي هي صاحبة الشهادة اللاحقة في مسيرة إصدار الشهادة (كما تبين ذلك قيمة لا تساوي الصفر).

4.5.10 المعالجة النهائية

بعد أن تكون قد تمت معالجة جميع الشهادات الموجودة في المسيرة، تنفذ الإجراءات التالية:

أ) تحدد *مجموعة السياسات المفروضة من السلطة* من جدول *مجموعة السياسات المفروضة من السلطة*. فإذا كان الجدول خالياً، تكون عندئذ *مجموعة السياسات المفروضة من السلطة* مجموعة خالية أو صفرية. وإذا كانت *مجموعة السياسات المفروضة من السلطة* [0، *عمق المسيرة*] هي *أي سياسة*، تكون عندئذ *مجموعة السياسات المفروضة من السلطة* هي *أي سياسة*. وإلا فإن *مجموعة السياسات المفروضة من السلطة* تكون لكل صف في الجدول هي القيمة الموجودة في خلية أقصى اليسار التي لا تحتوي على معرف الهوية *أي سياسة*.

ب) تحسب *مجموعة السياسات المفروضة من المستعمل* بتشكيل تقاطع المجموعتين: *مجموعة السياسات المفروضة من السلطة* و*مجموعة السياسات الأولية*.

ج) إذا كان *مبين سياسة صريحة* موجوداً، يتم التحقق من أن أي واحدة من المجموعتين التاليتين ليست خالية: *مجموعة السياسات المفروضة من السلطة*، و*مجموعة السياسات المفروضة من المستعمل*.

إذا وقع لأي واحد من التحققات السابقة أن فشل، يجب أن ينهى الإجراء، بترجيع دلالة فشل، مع شفرة داعٍ وافٍ، *ومبين سياسة صريحة*، و*مجموعة السياسات المفروضة من السلطة*، و*مجموعة السياسات المفروضة من المستعمل*. وإذا كان الفشل ناجماً عن كون *مجموعة السياسات المفروضة من المستعمل* خالية، تكون المسيرة صالحة في إطار السياسة أو السياسات المفروضة من السلطة، ولكن لا تكون أي واحدة من السياسة مقبولة من المستعمل.

وإذا لم يقع لأي واحد من التحققات السابقة أن فشل بالنسبة إلى الشهادة النهائية، ينهى الإجراء عندئذ بترجيع دلالة نجاح، ومعها *مبين سياسة صريحة*، و*مجموعة السياسات المفروضة من السلطة*، و*مجموعة السياسات المفروضة من المستعمل*.

11 تخطيطة الدليل للبنية التحتية للمفتاح العمومي (PKI)

يحدد هذا البند عناصر تخطيطة الدليل التي تستعمل التمثيل معلومات البنية PKI في الدليل. وهو يشتمل على مواصفة أصناف الموضوعات والنعوت وقواعد مواءمة قيم النعوت ذات الصلة.

1.11 أصناف الموضوعات وأشكال السماء في الدليل للبنية PKI

يتضمن هذا البند الفرعي تعريف أصناف الموضوعات المستعملة لتمثيل موضوعات البنية PKI في الدليل.

1.1.11 صنف الموضوعات "مستعمل البنية التحتية PKI"

صنف الموضوعات "مستعمل البنية التحتية PKI" يعرّف المداخل لموضوعات يمكن أن تكون أصحاب شهادات مفتاح عمومي.

```
pkiUser    OBJECT-CLASS   ::= {
   SUBCLASS OF        {top}
   KIND               auxiliary
   MAY CONTAIN        {userCertificate}
   ID                 id-oc-pkiUser }
```

2.1.11 صنف الموضوعات "سلطة إصدار الشهادة في البنية PKI"

صنف الموضوعات "سلطة إصدار الشهادة في البنية PKI" يستعمل في تعرّيف المداخل للموضوعات التي تعمل كسلطات إصدار الشهادة.

```
pkiCA      OBJECT-CLASS   ::= {
   SUBCLASS OF        {top}
   KIND               auxiliary
   MAY CONTAIN        {cACertificate |
                      certificateRevocationList |
                      authorityRevocationList |
                      crossCertificatePair }
ID                    id-oc-pkiCA }
```

3.1.11 صنف الموضوعات وشكل الاسم لنقاط توزيع القائمة CRL

صنف الموضوعات "نقطة توزيع القائمة CRL" يفيد في تعريف المداخل للموضوعات التي يمكنها أن تعلب دور نقاط توزيع القائمة CRL.

```
cRLDistributionPoint        OBJECT-CLASS        ::= {
   SUBCLASS OF              { top }
   KIND                     structural
   MUST CONTAIN             { commonName }
   MAY CONTAIN              { certificateRevocationList |
                            authorityRevocationList |
                            deltaRevocationList }
   ID                       id-oc-cRLDistributionPoint }
```

وشكل الاسم "نقطة توزيع القائمة CRL" يحدد الطريقة التي يمكن بها تسمية المداخل الخاصة بصنف الموضوعات **نقطة توزيع القائمة CRL (cRLDistributionPoint)**

```
cRLDistPtNameForm           NAME-FORM ::= {
   NAMES                    cRLDistributionPoint
   WITH ATTRIBUTES          { commonName}
   ID                       id-nf-cRLDistPtNameForm }
```

4.1.11 صنف الموضوعات "القائمة دلتا CRL"

صنف الموضوعات "القائمة دلتا CRL" يفيد في تعريف المداخل للموضوعات التي تتضمن قوائم الإبطال دلتا (أي سلطات إصدار الشهادة (CA) وسلطات النعت (AA) وغيرها.

```
deltaCRL                    OBJECT-CLASS   ::= {
   SUBCLASS OF              {top}
   KIND                     auxiliary
   MAY CONTAIN              {deltaRevocationList}
   ID                       id-oc-deltaCRL }
```

5.1.11 صنف الموضوعات "سياسة الشهادة وإعلان الممارسات في إصدار الشهادة" (CP/CPS)

صنف الموضوعات "سياسة الشهادة (CP) وإعلان الممارسات في إصدار الشهادة (CPS) يستعمل في تعريف المداخل للموضوعات التي تحتوي على سياسة الشهادة و/أو على معلومات عن الممارسات في إصدار الشهادة.

```
cpCps                OBJECT-CLASS  ::= {
   SUBCLASS OF       {top}
   KIND              auxiliary
   MAY CONTAIN       {certificatePolicy |
                     certificationPracticeStmt}
   ID                id-oc-cpCps }
```

6.1.11 صنف الموضوعات "مسيرة الشهادة في البنية PKI"

صنف الموضوعات "مسيرة الشهادة في البنية PKI" يستعمل في تعريف المداخل للموضوعات التي تحتوي على مسيرات في البنية PKI. وتستعمل عادة بالاشتراك مع المداخل إلى بنية المسيرين: **البنية التحتية PKI لسلطة إصدار الشهادة (pkiCA)** و**البنية التحتية PKI للمستعمل (pkiUser)**.

```
pkiCertPath          OBJECT-CLASS  ::= {
   SUBCLASS OF       {top}
   KIND              auxiliary
   MAY CONTAIN       { pkiPath }
   ID                id-oc-pkiCertPath }
```

2.11 النعوت الدليلية للبنية التحتية PKI

يتضمن هذا البند الفرعي تعريف النعوت الدليلية التي تتيح تخزين معلومات البنية PKI في الدليل.

1.2.11 نعت "شهادة المستعمل"

يستطيع المستعمل أن يحصل على شهادة مفتاح عمومي أو على أكثر من شهادة، صادرة عن سلطة إصدار شهادة واحدة أو عن أكثر من سلطة. ويحتوي نمط النعت **"شهادة المستعمل" (userCertificate)** على شهادات المفتاح العمومي التي حصل عليها مستعمل من سلطة واحدة لإصدار الشهادة أو من أكثر من سلطة.

```
userCertificate                  ATTRIBUTE  ::=  {
   WITH SYNTAX                   Certificate
   EQUALITY MATCHING RULE        certificateExactMatch
   ID                            id-at-userCertificate}
```

2.2.11 نعت "شهادة سلطة إصدار الشهادة"

نعت **"شهادة سلطة إصدار الشهادة" (cACertificate)** لمدخل في الدليل لسلطة إصدار شهادة، يستعمل لتخزين الشهادات الصادرة لذاتها (إن وجدت) والشهادات الصادرة لهذه السلطة لإصدار الشهادة، من سلطات أخرى لإصدار الشهادة موجودة في نفس ميدانها. وفي حالة الشهادات من الصيغة 3، يجب أن تشتمل هذه الشهادات على توسع **التقييدات الأساسية (basicConstraints)** وعلى قيمة السلطة cA موضوعة على "صائبة". ويكون تعريف الميدان مسألة سياسية محلية صرف.

```
cACertificate                    ATTRIBUTE  ::=  {
   WITH SYNTAX                   Certificate
   EQUALITY MATCHING RULE        certificateExactMatch
   ID                            id-at-cAcertificate }
```

3.2.11 نعت "زوج الشهادات المتقاطعة"

العناصر **الصادرة لهذه السلطة لإصدار الشهادة (issuedToThisCA)** من النعت **"زوج الشهادات المتقاطعة" (crossCertificatePair)** لمدخل سلطة إصدار الشهادة في الدليل، تستعمل من أجل تخزين جميع الشهادات الصادرة عن سلطة CA، ما عدا الشهادات الصادرة لذاتها. ويمكن للعناصر **الصادرة عن هذه السلطة لإصدار الشهادة (CA) (issuedByThisCA)** من النعت **"زوج الشهادات المتقاطعة"** لمدخل سلطة CA في الدليل أن تحتوي بصورة اختيارية على مجموعة فرعية من الشهادات الصادرة عن هذه السلطة CA إلى غيرها من السلطات CA. فإذا أصدرت سلطة CA شهادة إلى سلطة CA أخرى، وكانت السلطة CA الصاحبة ليست أدنى تراتبياً من السلطة CA المُصْدرة، يكون على السلطة CA المصدرة أن تضع الشهادة في العنصر **صادرة عن هذه السلطة CA** من النعت **زوج الشهادات المتقاطعة** في مدخلها الخاص في الدليل. وإذا تواجد العنصران **صادرة لهذه السلطة CA وصادرة عن هذه السلطة CA** معاً في نفس قيمة النعت، يكون اسم المُصْدر في إحدى الشهادتين منطبقاً على اسم الصاحب في الشهادة الأخرى، والعكس بالعكس، ويكون المفتاح العمومي للصاحب في إحدى الشهادتين قادراً على التحقق من التوقيع الرقمي في الشهادة الأخرى، والعكس بالعكس. والمصطلح **ذاهبة (forward)** كان قد استعمل في الطبعات السابقة ليدل على **صادرة لهذه السلطة CA**، كما كان قد استعمل المصطلح **عائدة (reverse)** في الطبعات السابقة ليدل على **صادرة عن هذه السلطة CA**.

عندما يكون العنصر **صادرة عن هذه السلطة CA (issuedByThisCA)** موجوداً، لا يلزم تخزين قيمة العنصر **صادرة لهذه السلطة CA (issuedToThisCA)** وقيمة **العنصر صادرة عن هذه السلطة CA** في قيمة النعت ذاتها، أو بعبارة أخرى يمكن تخزينها إما في قيمة نعت وحيدة وإما في قيمتي نعت مختلفتين.

إذا كانت الشهادة من الصيغة 3، يجب على هذه الشهادات أن تحتوي على التوسع **تقييدات أساسية (basicConstraints)** مع وجود قيمة CA موضوعة على "صائبة".

```
crossCertificatePair                ATTRIBUTE  ::=  {
    WITH SYNTAX                     CertificatePair
    EQUALITY MATCHING RULE          certificatePairExactMatch
    ID                              id-at-crossCertificatePair }

CertificatePair         ::=     SEQUENCE {
issuedToThisCA          [0]     Certificate OPTIONAL,
issuedByThisCA          [1]     Certificate OPTIONAL
                                -- at least one of the pair shall be present -- }
                                -- يجب أن يوجد واحد من فردي الزوج على الأقل --
(WITH COMPONENTS { ..., issuedToThisCA PRESENT} |
WITH COMPONENTS { ..., issuedByThisCA PRESENT})
```

4.2.11 نعت "قائمة إبطال الشهادات"

يحتوي النعت التالي على قائمة من الشهادات المبطلة:

```
certificateRevocationList           ATTRIBUTE  ::=  {
    WITH SYNTAX                     CertificateList
    EQUALITY MATCHING RULE          certificateListExactMatch
    ID                              id-at-certificateRevocationList }
```

5.2.11 نعت "قائمة إبطال السلطات"

يحتوي النعت التالي على قائمة من شهادات **سلطات** مبطلة:

```
authorityRevocationList             ATTRIBUTE  ::=  {
    WITH SYNTAX                     CertificateList
    EQUALITY MATCHING RULE          certificateListExactMatch
    ID                              id-at-authorityRevocationList }
```

6.2.11 نعت "قائمة إبطال دلتا"

هذا النمط من النعت التالي معرّف على قائمة dCRL في مدخل الدليل:

```
deltaRevocationList                ATTRIBUTE ::= {
    WITH SYNTAX                    CertificateList
    EQUALITY MATCHING RULE         certificateListExactMatch
    ID                             id-at-deltaRevocationList }
```

7.2.11 نعت "الخوارزميات المدعومة"

يعرّف نعت الدليل ليدعم انتقاء خوارزمية يمكن استعمالها للاتصال مع كيان نهائي بعيد، يستعمل شهادات كما هي محددة في مواصفة الدليل هذه. والترميز ASN.1 التالي يحدد هذا النعت (متعدد القيم):

```
supportedAlgorithms ATTRIBUTE ::= {
    WITH SYNTAX                    SupportedAlgorithm
    EQUALITY MATCHING RULE         algorithmIdentifierMatch
    ID                             id-at-supportedAlgorithms }

SupportedAlgorithm ::= SEQUENCE {
    algorithmIdentifier                    AlgorithmIdentifier,
    intendedUsage                  [0]     KeyUsage OPTIONAL,
    intendedCertificatePolicies    [1]     CertificatePoliciesSyntax OPTIONAL }
```

وكل قيمة من قيم النعت (متعدد القيم)، تكون لها قيمة متميزة **لمعرف هوية الخوارزمية (algorithmIdentifier)**. وتوفر قيمة **الاستعمال المزمع (intendedUsage)** دلالة على الاستعمال المزمع للخوارزمية (انظر الفقرة 3.2.2.8 لمعرفة الاستعمالات المعترف بها). وتحدد قيمة المكوّنة **سياسات الشهادة المزمعة** سياسات الشهادة ومعها، اختيارياً، واصفات سياسات الشهادة التي يمكن استعمال الخوارزمية المحددة معها.

8.2.11 نعت "إعلان الممارسات في إصدار الشهادة"

يستعمل نعت **"إعلان الممارسات في إصدار الشهادة" (certificationPracticeStmt)** لتخزين المعلومات الخاصة بإعلان سلطة عن الممارسات في إصدار الشهادة.

```
certificationPracticeStmt     ATTRIBUTE  ::=  {
    WITH SYNTAX         InfoSyntax
    ID                  id-at-certificationPracticeStmt }

InfoSyntax          ::=         CHOICE {
    content         DirectoryString {ub-content},
    pointer         SEQUENCE {
        name                        GeneralNames,
        hash                        HASH { HashedPolicyInfo } OPTIONAL } }

    POLICY    ::=   TYPE-IDENTIFIER

HashedPolicyInfo        ::=    POLICY.&Type( {Policies} )

Policies POLICY ::= {...} -- Defined by implementors --
                                        -- يعرفه المنفذون --
```

إذا كانت المكوّنة **محتوى (content)** موجودة، فهي تحتوي على النص الكامل لإعلان السلطة عن الممارسات في إصدار الشهادة.

وإذا كانت المكوّنة **مؤشر (pointer)** موجودة، فإن المكوّنة **اسم (name)** تحيل عندئذ إلى موقع أو إلى مواقع يمكن الحصول فيها على نسخة من إعلان السلطة عن الممارسات في إصدار الشهادة. وإذا كانت المكوّنة **فَرْم (hash)** موجودة، فهي تحتوي على فرم لمحتوى إعلان الممارسات في إصدار الشهادة الذي ينبغي أن يوجد في الموقع المرجعي. ويمكن استخدام هذا الفرم للقيام بالتحقق من تكاملية الوثيقة المرجعية.

9.2.11 نعت "سياسة الشهادة"

يستعمل نعت "**سياسة الشهادة**" (certificatePolicy) لتخزين معلومات عن سياسة شهادة.

```
certificatePolicy       ATTRIBUTE  ::=  {
   WITH SYNTAX          PolicySyntax
   ID                   id-at-certificatePolicy }

PolicySyntax  ::=       SEQUENCE {
   policyIdentifier     PolicyID,
   policySyntax         InfoSyntax
}

PolicyID  ::=  CertPolicyId
```

تشتمل المكوّنة معرف **هوية السياسة (policyIdentifier)** على معرف هوية الموضوع المسجل لهذه السياسة الخاصة بالشهادة.

إذا كانت المكوّنة **محتوى (content)** موجودة، فهي تحتوي على النص الكامل لسياسة الشهادة.

إذا كانت المكوّنة **مؤشر (pointer)** موجودة، فإن المكوّنة **اسم (name)** تحيل عندئذ إلى موقع أو إلى مواقع يمكن الحصول فيها على نسخة من سياسة الشهادة. وإذا كانت المكوّنة **فَرْم (hash)** موجودة، فهي تحتوي على فَرْم لمحتوى سياسة الشهادة الذي ينبغي أن يوجد في الموقع المرجعي. ويمكن استخدام هذا الفَرْم للقيام بالتحقق من تكاملية الوثيقة المرجعية.

ملاحظة – إن خيار إدراج فرم في هذا النعت هو للقيام بكل بساطة بتحقق من التكاملية بالنسبة إلى معطيات موجودة في مَصْدر غير الدليل. ويجب حماية **الفرم** المخزون في الدليل. ويمكن استخدام خدمات الدليل الأمنية لهذا الغرض، بما فيها من استيقان معمق و/أو تحكّم في النفاذ و/أو نعوت موقّعة. وفوق ذلك، حتى لو كان **الفرم** يتواءم مع الوثيقة سياسة الشهادة/إعلان الممارسات في إصدار الشهادة (CP/CPS) الأصلية، إلا أن هناك متطلبات أمنية إضافية لكي تضمن كون المواصفة الأصلية ذاتها هي الوثيقة الصحيحة (كأن تكون الوثيقة موقّعة من سلطة مختصة).

10.2.11 نعت "مسيرة البنية التحتية PKI"

يستعمل نعت مسيرة البنية التحتية PKI لتخزين مسيرات إصدار الشهادة، التي تتكون كل منها من تتابع شهادات.

```
pkiPath    ATTRIBUTE  ::= {
   WITH SYNTAX        PkiPath
   ID                 id-at-pkiPath }
```

يمكن تخزين هذا النعت في مدخل دليل لصنف الموضوع **pkiCA** أو **pkiUser** (سلطة إصدار الشهادة في البنية PKI أو مستعمل البنية PKI).

عندما تختزن قيم هذا النعت في مداخل **pkiCA**، فإنها تحتوي على مسيرات إصدار الشهادة التي تستبعد شهادات الكيان النهائي. ولذلك يستعمل هذا النعت لتخزين مسيرات إصدار الشهادة التي يتواتر استعمالها من الأطراف الواثقة التي تصاحب هذه السلطة CA. ويمكن استعمال قيمة لهذا النعت بالاشتراك مع أي شهادة كيان نهائي صادرة عن صاحب آخر شهادة في قيمة النعت.

وعندما تختزن قيم هذا النعت في مداخل **pkiUser**، فإنها تحتوي على مسيرات إصدار الشهادة التي تستبعد شهادات الكيان النهائي. ويكون الكيان النهائي في هذه الحالة هو المستعمل الذي يحمل مدخله هذا النعت. وتمثل قيم هذا النعت كامل مسيرات إصدار الشهادة للشهادات الصادرة لهذا المستعمل.

3.11 قواعد المواءمة في الدليل للبنية التحتية للمفتاح العمومي (PKI)

تحدد مواصفة الدليل هذه قواعد المواءمة الواجب استعمالها مع النعوت التي أنماطها **شهادة (Certificate)**، **وزوج الشهادات (CertificatePair)**، **وقائمة شهادات (CertificateList)**، **وسياسة الشهادة (CertificatePolicy)**، **وخوارزمية مدعومة**

(SupportedAlgorithm)، على التوالي. ويحدد هذا البند أيضاً قواعد المواءمة لتسهيل انتقاء الشهادات أو القوائم CRL التي تمتلك خصائص خاصة، من بين الشهادات أو القوائم CRL التي تستخدم نعوتاً متعددة القيم. وتوفر القاعدة المحسّنة لمواءمة الشهادة، إمكانية إقامة مواءمة متقنة التعقيد ما بين الشهادات المخزونة في مداخل الدليل.

1.3.11 مواءمة مضبوطة للشهادة

تقارن قاعدة المواءمة المضبوطة للشهادة، قيمة معروضة بقيمة نعت من النمط **شهادة (certificate)**. وهي تنتقي بلا لبس شهادة وحيدة.

```
certificateExactMatch MATCHING-RULE ::= {
    SYNTAX      CertificateExactAssertion
    ID          id-mr-certificateExactMatch }

CertificateExactAssertion ::= SEQUENCE {
    serialNumber    CertificateSerialNumber,
    issuer          Name }
```

وترجع قاعدة المواءمة هذه، القيمة "**صائب**"، إن كانت مكوّنات قيمة النعت توائم مكوّنات القيمة المعروضة.

2.3.11 مواءمة الشهادة

تقارن قاعدة مواءمة الشهادة، قيمة معروضة بقيمة نعت من النمط **شهادة (certificate)**. وهي تنتقي شهادة واحدة أو أكثر استناداً إلى خصائص متنوعة.

```
certificateMatch MATCHING-RULE ::= {
    SYNTAX      CertificateAssertion
    ID          id-mr-certificateMatch }

CertificateAssertion ::= SEQUENCE {
    serialNumber            [0]     CertificateSerialNumber     OPTIONAL,
    issuer                  [1]     Name                        OPTIONAL,
    subjectKeyIdentifier    [2]     SubjectKeyIdentifier        OPTIONAL,
    authorityKeyIdentifier  [3]     AuthorityKeyIdentifier      OPTIONAL,
    certificateValid        [4]     Time                        OPTIONAL,
    privateKeyValid         [5]     GeneralizedTime             OPTIONAL,
    subjectPublicKeyAlgID   [6]     OBJECT IDENTIFIER           OPTIONAL,
    keyUsage                [7]     KeyUsage                    OPTIONAL,
    subjectAltName          [8]     AltNameType                 OPTIONAL,
    policy                  [9]     CertPolicySet               OPTIONAL,
    pathToName              [10]    Name                        OPTIONAL,
    subject                 [11]    Name                        OPTIONAL,
    nameConstraints         [12]    NameConstraintsSyntax       OPTIONAL
}

AltNameType ::= CHOICE {
    builtinNameForm     ENUMERATED {
                            rfc822Name              (1),
                            dNSName                 (2),
                            x400Address             (3),
                            directoryName           (4),
                            ediPartyName            (5),
                            uniformResourceIdentifier (6),
                            iPAddress               (7),
                            registeredId            (8) },
    otherNameForm       OBJECT IDENTIFIER }

CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId
```

وترجع قاعدة المواءمة هذه، القيمة "صائب"، إذا كانت جميع المكوّنات الموجودة في القيمة المعروضة، توائم المكوّنات المقابلة في قيمة النعت، على النحو التالي:

المكونة **رقم التسلسل (serialNumber)** موائمة، إذا كانت قيمة هذه المكوّنة في قيمة النعت تساوي قيمتها في القيمة المعروضة؛

المكونة **المُصْدر (issuer)** موائمة، إذا كانت قيمة هذه المكوّنة في قيمة النعت تساوي قيمتها في القيمة المعروضة؛

المكونة **معرف هوية مفتاح الصاحب (subjectKeyIdentifier)** موائمة، إذا كانت قيمة هذه المكوّنة في قيمة النعت المخزونة تساوي قيمتها في القيمة المعروضة. ولا تكون موائمة، إن كانت قيمة النعت المخزونة لا تحتوي على توسع معرف هوية مفتاح الصاحب؛

المكونة **معرف هوية مفتاح السلطة (authorityKeyIdentifier)** موائمة، إذا كانت قيمة هذه المكوّنة في قيمة النعت المخزونة تساوي قيمتها في القيمة المعروضة. ولا تكون موائمة، إن كانت قيمة النعت المخزونة لا تحتوي على توسع معرف هوية مفتاح السلطة أو إذا لم تكن جميع المكونات الواردة في القيمة المعروضة، موجودة في قيمة النعت المخزونة؛

المكونة **صلاحية الشهادة (certificateValid)** موائمة، إذا وقعت القيمة المعروضة داخل فترة الصلاحية لقيمة النعت المخزونة؛

المكونة **صلاحية المفتاح الخاص (privateKeyValid)** موائمة، إذا وقعت القيمة المعروضة داخل الفترة التي يبينها توسع فترة استعمال المفتاح الخاص في قيمة النعت المخزونة أو إذا كان لا يوجد توسع فترة استعمال المفتاح الخاص في قيمة النعت المخزونة؛

المكونة **معرف الهوية الخوارزمية المفتاح العمومي للصاحب (subjectPublicKeyAlgID)** موائمة، إذا كانت تساوي مكوّنة **الخوارزمية (algorithm)** في **معرف هوية الخوارزمية (algorithmIdentifier)** من المكونة **معلومات المفتاح العمومي للصاحب (subjectPublicKeyInformation)** لقيمة النعت المخزونة؛

المكونة **استعمال المفتاح (keyUsage)** موائمة، إذا كانت جميع البتات الموضوعة في القيمة المعروضة هي موضوعة أيضاً في توسع استعمال المفتاح لقيمة النعت المخزونة، أو إذا كان لا يوجد مثل هذا التوسع في قيمة النعت المخزونة؛

المكونة **اسم بديل للصاحب (subjectAltName)** موائمة، إذا كانت قيمة النعت المخزونة تحتوي على توسع الاسم البديل للصاحب مع مكوّنة **الأسماء البديلة (AltNames)** لنفس نمط الاسم المبين في القيمة المعروضة؛

المكونة **السياسية (policy)** موائمة، إذا كان واحد على الأقل من أفراد المجموعة **مجموعة سياسات الشهادات (CertPolicySet)** المقدمة، يظهر في توسع سياسات الشهادات في قيمة النعت المخزونة أو إذا كانت إما الشهادة المعروضة وإما الشهادة المخزونة تحتوي على القيمة الخاصة **أي سياسة** في مكوّنة **السياسة**. ولا تكون موائمة إذا كان توسع سياسات الشهادات غير موجود في قيمة النعت المخزونة؛

المكونة **مسيرة إلى الاسم (pathToName)** موائمة، إلا إذا كان للشهادة توسع تقييدات الأسماء الذي يحظر إنشاء مسيرة إصدار الشهادة إلى قيمة الاسم المعروضة؛

المكونة **الصاحب (subject)** موائمة، إذا كانت قيمة هذه المكونة في قيمة النعت تساوي قيمتها الواردة في القيمة المعروضة؛

المكونة **تقييدات الأسماء (nameConstraints)** موائمة، إذا كانت أسماء الصاحب في قيمة النعت المخزونة تقع في مكان الأسماء الذي تعطيه قيمة المكوّنة الأشجار الفرعية المسموحة في القيمة المعروضة، ولا تقع في مكان الأسماء الذي تعطيه قيمة المكوّنة الأشجار الفرعية المستبعدة في القيمة المعروضة.

3.3.11 مواءمة مضبوطة لزوج الشهادات

تقارن قاعدة المواءمة المضبوطة لزوج الشهادات، قيمة معروضة بقيمة نعت من النمط **زوج الشهادات (CertificatePair)**. وهي تنتقي بلا لبس زوجاً من الشهادات المتقاطعة.

```
certificatePairExactMatch MATCHING-RULE          ::=  {
    SYNTAX      CertificatePairExactAssertion
    ID          id-mr-certificatePairExactMatch }

CertificatePairExactAssertion ::= SEQUENCE {
    issuedToThisCAAssertion     [0] CertificateExactAssertion OPTIONAL,
    issuedByThisCAAssertion     [1] CertificateExactAssertion OPTIONAL }
    ( WITH COMPONENTS                {..., issuedToThisCAAssertion PRESENT} |
      WITH COMPONENTS                {..., issuedByThisCAAssertion PRESENT} )
```

وترجع قاعدة المواءمة هذه، القيمة "صائب"، إذا كانت المكوّنات الموجودة في المكوّنتين: **صادرة لتأكيد هذه السلطة CA (issuedToThisCAAssertion)** و**صادرة عن تأكيد هذه السلطة CA (issuedToThisCAAssertion)** الموجودتين في القيمة المعروضة، توائم المكوّنات المقابلة في المكونتين: **صادرة لهذه السلطة CA (issuedToThisCA)** و**صادرة عن هذه السلطة CA (issuedByThisCA)**، على التوالي، في قيمة النعت المخزونة.

4.3.11 مواءمة زوج الشهادات

تقارن قاعدة مواءمة زوج الشهادات، قيمة معروضة بقيمة نعت من النمط **زوج الشهادات (CertificatePair)**. وهي تنتقي زوجاً أو أزواجاً من الشهادات المتقاطعة استناداً إلى خصائص متنوعة للشهادة **صادرة لهذه السلطة** أو للشهادة **صادرة عن هذه السلطة CA** من زوج الشهادات.

```
certificatePairMatch MATCHING-RULE ::=  {
    SYNTAX      CertificatePairAssertion
    ID          id-mr-certificatePairMatch }

CertificatePairAssertion ::= SEQUENCE {
    issuedToThisCAAssertion     [0] CertificateAssertion OPTIONAL,
    issuedByThisCAAssertion     [1] CertificateAssertion OPTIONAL }
    ( WITH COMPONENTS                {..., issuedToThisCAAssertion PRESENT} |
    WITH COMPONENTS                  {..., issuedByThisCAAssertion PRESENT} )
```

وترجع قاعدة المواءمة هذه، قيمة "صائب"، إذا كانت جميع المكونات الموجودة في المكونتين: **صادرة لتأكيد هذه السلطة CA وصادرة عن تأكيد هذه السلطة CA**، في القيمة المعروضة، توائم المكوّنات المقابلة الموجودة في المكوّنتين: **صادرة لهذه السلطة CA وصادرة عن هذه السلطة CA**، على التوالي، في قيمة النعت المخزونة.

5.3.11 مواءمة مضبوطة لقائمة الشهادات

تقارن قاعدة المواءمة المضبوطة لقائمة الشهادات، قيمة معروضة بقيمة نعت من النمط **قائمة الشهادات**. وهي تنتقي بلا لبس قائمة CRL وحيدة.

```
certificateListExactMatch MATCHING-RULE ::=      {
    SYNTAX      CertificateListExactAssertion
    ID          id-mr-certificateListExactMatch }

CertificateListExactAssertion ::= SEQUENCE {
    issuer              Name,
    thisUpdate          Time,
    distributionPoint   DistributionPointName OPTIONAL }
```

وترجع قاعدة المواءمة هذه، قيمة "صائب"، إذا كانت المكونات الموجودة في قيمة النعت المخزونة توائم المكونات الموجودة في القيمة المعروضة. وإذا كانت المكونة **نقطة التوزيع (distributionPoint)** موجودة، يجب أن توائم شكلَ اسمٍ واحداً على الأقل.

6.3.11 مواءمة قائمة الشهادات

تقارن قاعدة المواءمة لقائمة الشهادات، قيمة معروضة بقيمة نعت من النمط **قائمة الشهادات**. وهي تنتقي قائمة أو قوائم CRL استناداً إلى خصائص متنوعة.

```
certificateListMatch MATCHING-RULE ::= {
    SYNTAX    CertificateListAssertion
    ID        id-mr-certificateListMatch }

CertificateListAssertion ::= SEQUENCE {
    issuer                  Name                    OPTIONAL,
    minCRLNumber      [0]   CRLNumber               OPTIONAL,
    maxCRLNumber      [1]   CRLNumber               OPTIONAL,
    reasonFlags             ReasonFlags             OPTIONAL,
    dateAndTime             Time                    OPTIONAL,
    distributionPoint [2]   DistributionPointName   OPTIONAL,
    authorityKeyIdentifier [3] AuthorityKeyIdentifier OPTIONAL }
```

وترجع قاعدة المواءمة هذه، قيمة "صائب"، إذا كانت جميع المكوّنات الموجودة في القيمة المعروضة، توائم المكوّنات المقابلة في قيمة النعت المخزونة، على النحو التالي:

المكونة **المُصْدر (issuer)** موائمة، إذا كانت قيمة هذه المكوّنة في قيمة النعت تساوي قيمتها في القيمة المعروضة؛

المكونة **اصغر رقم للقائمة (minCRLNumber)** موائمة، إذا كانت قيمته تساوي أو أصغر من القيمة الواردة في توسع القائمة CRL في قيمة النعت المخزونة. ولا تكون موائمة إذا كانت قيمة النعت المخزونة لا تحتوي على توسع رقم القائمة CRL؛

المكونة **أكبر رقم للقائمة (maxCRLNumber)** موائمة، إذا كانت قيمته تساوي أو أكبر من القيمة الواردة في توسع القائمة CRL في قيمة النعت المخزونة. ولا تكون موائمة إذا كانت قيمة النعت المخزونة لا تحتوي على توسع رقم القائمة CRL؛

المكونة **رايات الدواعي (reasonFlags)** موائمة، إذا كانت كل واحدة من البتات الموضوعة في القيمة المعروضة هي أيضاً موضوعة في المكونات **فقط بعض الدواعي (onlySomeReasons)** من توسع نقطة التوزيع المُصْدرة في قيمة النعت المخزونة. وتكون موائمة أيضاً إذا كانت قيمة النعت المخزونة لا تحتوي على المكونة **رايات الدواعي** في توسع نقطة التوزيع المُصْدرة، أو إذا كانت قيمة النعت المخزونة لا تحتوي على توسع نقطة التوزيع المُصْدرة؛

ملاحظة – على الرغم من كون قائمة CRL قد توائم قيمة خاصة من **رايات الدواعي**، إلا أنه يحتمل ألا تحتوي القائمة CRL على أي تبليغات عن إبطال مع شفرة الداعي هذه.

المكونة **التاريخ والوقت (dateAndTime)** موائمة، إذا كانت قيمته تساوي أو تتأخر عن القيمة الموجودة في المكونة **هذا التحيين (thisUpdate)** من قيمة النعت المخزونة، أو إنها تبكّر عن القيمة الموجودة في المكونة **التحيين القادم (nextUpdate)** من قيمة النعت المخزونة. ولا تكون موائمة إذا كانت قيمة النعت المخزونة لا تحتوي على المكوّنة **التحيين القادم**؛

المكونة **نقطة التوزيع (distributionPoint)** موائمة، إذا كانت قيمة النعت المخزونة تحتوي على المكونة نقطة التوزيع المُصْدرة، وكانت قيمة هذه المكونة في القيمة المعروضة تساوي القيمة المقابلة في هذا التوسع، بواحد من أشكال الاسم على الأقل؛

المكونة **معرف هوية مفتاح السلطة (authorityKeyIdentifier)** موائمة، إذا كانت قيمة هذه المكونة في قيمة النعت المخزونة تساوي قيمتها في القيمة المعروضة. ولا تكون موائمة إذا كانت قيمة النعت المخزونة لا تحتوي على توسع معرف هوية مفتاح السلطة، أو إذا لم تكن جميع مكونات القيمة المعروضة موجودة في قيمة النعت المخزونة.

7.3.11 مواءمة معرف هوية الخوارزمية

تقارن قاعدة المواءمة لمعرف هوية الخوارزمية، قيمة معروضة بقيمة نعت من النمط **خوارزميات مدعومة (SupportedAlgorithms)**.

```
algorithmIdentifierMatch MATCHING-RULE::= {
    SYNTAX    AlgorithmIdentifier
    ID        id-mr-algorithmIdentifierMatch }
```

وترجع هذه القاعدة القيمة "صائب"، إذا كانت القيمة المعروضة تساوي المكوّنة **معرف هوية الخوارزمية (algorithmIdentifier)** في قيمة النعت المخزونة.

8.3.11 مواءمة السياسة

تقارن قاعدة المواءمة السياسة، قيمة معروضة بقيمة نعت من النمط **سياسة الشهادة (CertificatePolicy)**، أو بقيمة نعت من النمط **سياسة خاصة (privPolicy)**.

```
policyMatch MATCHING-RULE    ::= {
   SYNTAX     PolicyID
   ID         id-mr-policyMatch }
```

وترجع هذه القاعدة القيمة "صائب"، إذا كانت القيمة المعروضة تساوي المكوّنة **معرف هوية السياسة (policyIdentifier)** في قيمة النعت المخزونة.

9.3.11 مواءمة مسيرة البنية التحتية PKI

تقارن قاعدة المواءمة **لمواءمة مسيرة البنية PKI (pkiPathMatch)**، قيمة معروضة بقيمة نعت من النمط **مسيرة البنية PKI (pkiPath)**. ويمكن لنظام استعمال الشهادات أن يستعمل هذه القاعدة للمواءمة من أجل انتقاء مسيرة تبدأ بشهادة تصدرها سلطة CA يثق هو بها، وتنتهي بشهادة صادرة للصاحب المعين.

```
pkiPathMatch MATCHING-RULE  ::= {
   SYNTAX     PkiPathMatchSyntax
   ID         id-mr-pkiPathMatch }

PkiPathMatchSyntax     ::=  SEQUENCE {
   firstIssuer         Name,
   lastSubject         Name }
```

وترجع قاعدة المواءمة هذه، القيمة "صائب"، إذا كانت القيمة المعروضة في المكوّنة **المُصْدر الأول (firstIssuer)** تتوافق مع العناصر المقابلة في مجال **المُصْدر (issuer)** لأول شهادة في التتابع **(SEQUENCE)** في القيمة المخزونة، وإذا كانت القيمة المعروضة في المكوّنة **الصاحب الأخير (lastSubject)** تتوافق مع العناصر المقابلة في مجال الصاحب لآخر شهادة في التتابع **(SEQUENCE)** في القيمة المخزونة. وترجع قاعدة المواءمة هذه، القيمة "خاطئ"، إذا فشلت أي واحدة من هاتين المقارنتين.

10.3.11 قاعدة محسّنة لمواءمة الشهادة

تقارن القاعدة المحسّنة لمواءمة الشهادة، قيمة معروضة بقيمة نعت من النمط **شهادة (Certificate)**. وهي تنتقي شهادة واحدة أو عدة شهادات استناداً إلى خصائص متنوعة.

```
enhancedCertificateMatch MATCHING-RULE  ::= {
   SYNTAX     EnhancedCertificateAssertion
   ID         id-mr-enhancedCertificateMatch }

EnhancedCertificateAssertion  ::= SEQUENCE {
   serialNumber              [0]  CertificateSerialNumber     OPTIONAL,
   issuer                    [1]  Name                        OPTIONAL,
   subjectKeyIdentifier      [2]  SubjectKeyIdentifier        OPTIONAL,
   authorityKeyIdentifier    [3]  AuthorityKeyIdentifier      OPTIONAL,
   certificateValid          [4]  Time                        OPTIONAL,
   privateKeyValid           [5]  GeneralizedTime             OPTIONAL,
   subjectPublicKeyAlgID     [6]  OBJECT IDENTIFIER           OPTIONAL,
   keyUsage                  [7]  KeyUsage                    OPTIONAL,
   subjectAltName            [8]  AltName                     OPTIONAL,
   policy                    [9]  CertPolicySet               OPTIONAL,
   pathToName                [10] GeneralNames                OPTIONAL,
   subject                   [11] Name                        OPTIONAL,
   nameConstraints           [12] NameConstraintsSyntax       OPTIONAL
}
        -- لا شيء، يجب أن تكون مكونة واحدة موجودة على الأقل --
(ALL EXCEPT ({ -- none; at least one component shall be present -- }))
```

```
AltName ::= SEQUENCE {
  altnameType AltNameType,
  altNameValue      GeneralName OPTIONAL }
```

تتيح عملية التفتيش في الدليل دمج عدة قيم **لتأكيد الشهادة المحسّنة (EnhancedCertificateAssertion)** في مواصفات الترشيح، بما في ذلك و/أو المنطقية. وترجع قاعدة المواءمة هذه، القيمة "صائب"، إذا كانت جميع المكوّنات الموجودة في القيمة المعروضة تتوافق مع المكوّنات المقابلة في قيمة النعت، على النحو التالي:

مواءمة المكوّنات التالية: **رقم التسلسل (serialNumber)**، **والمُصْدر (issuer)**، **ومعرف هوية مفتاح الصاحب (subjectKeyIdentifier)**، **ومعرف هوية مفتاح السلطة (authorityKeyIdentifier)**، **وصلاحية الشهادة (certificateValid)**، **وصلاحية المفتاح الخاص (privateKeyValid)**، **والسياسة (policy)**، **والصاحب (subject)**، **وتقييدات الأسماء (nameConstraints)**، تجري كما هي معرفة للمكوّنات نفسها في قاعدة المواءمة **مواءمة الشهادة (certificateMatch)**.

المكوّنة **الاسم البديل للصاحب (subjectAltName)** تحتوي على الحقل تحتوي على الحقل **نمط الاسم البديل (altNameType)** واختيارياً على الحقل **قيمة الاسم البديل (altNameValue)**. وعندما يكون الحقل **قيمة الاسم البديل** موجوداً، تكون قيمته هي نفس شكل الاسم المبين في **نمط الاسم البديل**.

المكوّنة **الاسم البديل للصاحب** موائمة، إذا كان احد الشرطين التاليين على الأقل "صائباً":

- لا تحتوي القيمة المعروضة إلا على المكوّنة **نمط الاسم البديل**، وتحتوي قيمة النعت المخزونة على توسع الاسم البديل للصاحب، مع المكوّنة **الأسماء البديلة (AltNames)** لنفس النمط كما هو مبين في القيمة المعروضة؛
- تحتوي القيمة المعروضة إلا على المكوّنتين **نمط الاسم البديل وقيمة الاسم البديل** كلتيهما، وتحتوي قيمة النعت المخزونة على توسع الاسم البديل للصاحب، مع المكوّنة **الأسماء البديلة** لنفس النمط والقيمة المبينة في القيمة المعروضة.

والمكوّنة **الاسم البديل للصاحب** ليست موائمة، إذا كان واحد من الشروط التالية على الأقل "صائباً":

- لا تحتوي قيمة النعت المخزونة على توسع الاسم البديل للصاحب؛
- تحتوي قيمة النعت المخزونة على توسع الاسم البديل للصاحب، ولكن المكوّنة **الأسماء البديلة** لا تتضمن نفس النمط المعرفة هويته في القيمة المعروضة؛
- تحتوي القيمة المعروضة على المكوّنتين **نمط الاسم البديل وقيمة الاسم** كلتيهما، وتحتوي قيمة النعت المخزونة على توسع الاسم البديل للصاحب، مع المكوّنة **الأسماء البديلة** لنفس النمط المبين في القيمة المعروضة، غير أن القيمة المخزونة لا تحتوي على نفس قيمة النمط الموجودة في القيمة المعروضة.

ولا تكون مواءمة المكوّنة **الاسم البديل للصاحب**، معيّنة، إذا كانت القيمة المعروضة تحتوي على المكوّنتين **نمط الاسم البديل وقيمة الاسم البديل** كلتيهما، وكانت قيمة النعت المخزونة تحتوي على توسع **الاسم البديل للصاحب**، مع المكوّنة **الأسماء البديلة** لنفس النمط المبين في القيمة المعروضة، غير أن النمط هو نمط لا يستطيع الدليل أن يقارن قيماً له بغية تحديد المواءمة. وقد يكون ذلك الآن شكل الاسم لا يناسب المواءمة أو لأن الدليل غير قادر على القيام بالمقارنات المطلوبة.

والمكوّنة **مسيرة إلى الاسم (pathToName)** موائمة، ما لم يكن في الشهادة توسع تقييدات الأسماء الذي يحظر إنشاء مسيرة إصدار الشهادة إلى أي واحدة من قيم الأسماء المعروضة. فمثلاً عند محاولة استخراج شهادات من الشهادات التي تشكل المسيرة، نحو شهادة مستعمل قيمة صاحبها هي "dc=com; dc=corporate; cn=john.smith"، قد يكون من المفيد إدراج تأكيد في عملية التفتيش التي تحتوي على هذا الاسم المميز (DN) في المكوّنة **مسيرة إلى الاسم**. والشهادة المخزونة التي تحتوي على توسع تقييدات الأسماء الذي يستبعد كامل الشجرة الفرعية الموجودة تحت قيمة القاعدة "dc=com; dc=company A" يحتمل أن تفشل في عملية إقرار صلاحية مسيرة إصدار الشهادة بالنسبة إلى شهادة المستعمل هذه، وبالتالي يحتمل أن تكون قيمة غير موائمة لهذا المثال من التأكيد.

القسم الثالث – إطار شهادة النعت

يقدم إطار شهادة النعت المعرف هنا أساساً يمكن أن تقام عليه البنية التحية لإدارة امتياز (PMI) ويمكن لهذه البنى التحتية أن تتحمل تطبيقات مثل التحكم في النفاذ.

وربط امتياز معين بكيان ما توفره سلطة عبر بنية من المعطيات موقّعة رقمياً تدعى شهادة النعت، أو عبر شهادة مفتاح عمومي تحتوي على توسع معرّف صراحة لهذا الغرض. ونسق شهادات النعت معرف في مواصفة الدليل هذه، ويتضمن آلية قابلية التوسع مع مجموعة معينة من توسعات الشهادة. وقد تحتاج شهادات النعت إلى إبطال وقد لا تحتاج إليه. فقد تكون في بعض الحالات فترات صلاحية شهادة النعت قصيرة جداً (دقائق مثلاً)، مما ينفي الحاجة إلى تخطيطة إبطال. وإذا لجأت إحدى السلطات، لأي داعٍ كان، إلى إبطال شهادة نعت صادرة سابقاً، يصبح المستعملون في حاجة إلى معرفة حدوث الإبطال، لكيلا يستعملوا شهادة لم تعد أهلاً للثقة. وقوائم الإبطال هي واحد من الإجراءات التي يمكن استخدامها لتبليغ المستعملين بالإبطالات. ونسق قوائم الإبطال محدد في القسم الثاني من هذه المواصفة، وهو يشتمل على آلية لقابلية التوسع وعلى مجموعة من توسعات قوائم الإبطال. وهناك توسعات إضافية محددة في هذه المواصفة. وفي كلتا حالتي الشهادة وقائمة الإبطال، يمكن لهيئات أخرى أن تحدد توسعات إضافية مفيدة لها في بيئاتها الخاصة.

ويحتاج نظام استعمال شهادات النعت أن يقرّ صلاحية شهادة ما قبل استعماله هذه الشهادة لتطبيق ما. وإجراءات القيام بهذا الإقرار للصلاحية محددة هي الأخرى في هذه المواصفة، وهي تشتمل على التحقق من تكاملية الشهادة بحد ذاتها، ووضع إبطالها القانوني، وصلاحيتها بالنسبة إلى الاستعمال المزمع لها.

ويتضمن هذا الإطار عدداً من العناصر الاختيارية التي لا تناسب إلا بعض البيئات. وعلى الرغم من تعريف النموذجات على أنها مكتملة، إلا أن هذا الإطار يمكن استخدامه حيث لا تكون جميع مكوّنات النموذجات المحددة مستعملة. فهناك بيئات مثلاً لا يكون مطلوباً فيها إبطال شهادات النعت. وتفويض الامتياز واستخدام الأدوار هما مظهران لهذا الإطار، لا ينطبقان في جميع الحالات. وهما واردان في هذه المواصفة بحيث يتاح للبيئات التي تحتاج إليهما أن تأخذهما على عاتقها.

ويستعمل الدليل شهادات النعت، لكي يقدم بشأن معلومات الدليل تحكماً في النفاذ مبنياً على قواعد.

12 شهادات النعت

شهادات المفتاح العمومي مصممة من حيث الأساس لكي تقدم خدمات تعريف بالهوية، يمكن أن تبنى عليها خدمات أمنية أخرى، مثل تكاملية المعطيات (سلامتها)، واستيقان الكيان، والسرية، والترخيص. وتوجد في هذه المواصفة آليتان متمايزتان لربط إسناد امتياز إلى حامل.

يمكن لشهادات المفتاح العمومي المستعملة مع خدمة استيقان الكيان، أن تقدم مباشرة خدمة ترخيص، إن كانت الامتيازات تتصاحب مع الصاحب عبر ممارسات السلطة CA المُصْدرة. ويمكن لشهادات المفتاح العمومي أن تحتوي على توسع **نعوت الدليل للصاحب (subjectDirectoryAttributes)** الذي يتضمن الامتيازات المصاحبة لصاحب شهادة المفتاح العمومي. وتكون هذه الآلية مناسبة في الحالات التي تكون فيها سلطة إصدار شهادة المفتاح العمومي (CA) هي بنفس الوقت سلطة تفويض الامتياز (AA)، وتكون فترة صلاحية الامتياز تقابل فترة صلاحية شهادة المفتاح العمومي. لا تستطيع الكيانات النهائية أن تعمل كسلطات نعت (AA). وإذا كان أي واحد من التوسعات المعرفة في البند 15 وارداً في شهادة مفتاح عمومي، تكون هذه الامتيازات تنطبق أيضاً على جميع الامتيازات المسندة في توسع شهادة المفتاح العمومي الذي هو **نعوت الدليل للصاحب**.

وفي معظم الحالات، يكون لامتيازات الكيان أعمار نافعة لا تتواءم مع فترة الصلاحية لشهادة المفتاح العمومي. وكثيراً ما تكون الأعمار النافعة للامتيازات أقصر بكثير. وكثيراً ما تكون سلطة إسناد الامتياز هي غير السلطة التي تصدر شهادة المفتاح العمومي لنفس الكيان، كما تكون غالباً سلطات نعت مختلفة هي التي تقوم بإسناد الامتيازات المختلفة. ويمكن أن يكون إسناد الامتيازات قائماً على سياق زمني، كما يمكن ألا تكون جوانب "وضع الامتيازات في الخدمة أو سحبها منها"

متزامنة مع العمر النافع لشهادة المفتاح العمومي و/أو متزامنة مع امتيازات الكيان الصادرة عن سلطات نعت مختلفة. ويوفر استعمال شهادات نعت صادرة عن سلطات نعت، بنية تحتية لإدارة الامتياز (PMI) مرنة، يمكن إنشاؤها وإدارتها بصورة مستقلة عن البنية التحتية للمفتاح العمومي (PKI). وتوجد بنفس الوقت علاقة بين البنيتين، حيث تكون البنية (PKI) مستعملة لاستيقان هويات المُصْدرين والحاملين الواردة في شهادات النعت.

1.12 بنية شهادة النعت

تختلف بنية شهادة النعت عن بنية شهادة المفتاح العموم. وقد يكون للصاحب شهادات نعت متعددة تصاحب كل واحدة من شهادات مفاتيحه العمومية. ولا يتوجب أن تكون نفس السلطة هي التي تنشئ شهادة المفتاح العمومي وشهادة (شهادات) النعت للمستعمل، وبالفعل كثيراً ما يفرض فصل الواجبات غير هذا الأمر. وفي الحالات التي تتحمل فيها سلطات مختلفة مسؤولية إصدار شهادات المفتاح العمومي وشهادات النعت، ينبغي لشهادة (شهادات) المفتاح العمومي التي تصدرها سلطة إصدار الشهادة (CA)، ولشهادة (شهادات) النعت التي تصدرها سلطة النعت (AA) أن يتم توقيعها باستخدام مفاتيح توقيع خاصة مختلفة. أما في الحالات التي يكون فيها الكيان نفسه هو سلطة CA تصدر شهادات المفتاح العمومي، وسلطة AA تصدر شهادة النعت، فيوصى بشدة أن يكون المفتاح الذي يستعمل لتوقيع شهادات النعت مختلفاً عن المفتاح الذي يستعمل لتوقيع شهادات المفتاح العمومي. وتقع المبادات التي تحصل بين سلطة إصدار شهادة والكيان الذي يستلم الشهادة خارج نطاق هذه المواصفة.

تعرّف شهادة النعت كما يلي:

```
AttributeCertificate ::= SIGNED {AttributeCertificateInfo}

AttributeCertificateInfo ::= SEQUENCE
   {
                                        -- الصيغة هي v2
   version                  AttCertVersion, -- version is v2
   holder                   Holder,
   issuer                   AttCertIssuer,
   signature                AlgorithmIdentifier,
   serialNumber             CertificateSerialNumber,
   attrCertValidityPeriod   AttCertValidityPeriod,
   attributes               SEQUENCE OF Attribute,
   issuerUniqueID           UniqueIdentifier OPTIONAL,
   extensions               Extensions    OPTIONAL
   }
   AttCertVersion      ::= INTEGER { v2(1) }

Holder     ::=   SEQUENCE
          {
          baseCertificateID      [0] IssuerSerial          OPTIONAL,
                                        -- المُصْدر ورقم التسلسل لشهادة المفتاح العمومي للحامل
               -- the issuer and serial number of the holder's Public Key Certificate
          entityName             [1] GeneralNames          OPTIONAL,
                                                  -- اسم الكيان أو دوره
               -- the name of the entity or role
     objectDigestInfo       [2] ObjectDigestInfo     OPTIONAL
               -- used to directly authenticate the holder, e.g., an executable
               -- at least one of baseCertificateID, entityName or objectDigestInfo shall be present --}
                    -- يستعمل لاستيقان الحامل مباشرة، أي واحد على الأقل قابل للتنفيذ من المكونات: معرف
          -- هوية أساسي للشهادة، أو اسم الكيان، أو معلومات موجزة عن الموضوع، يجب أن يكون موجوداً--

ObjectDigestInfo   ::= SEQUENCE {
   digestedObjectType  ENUMERATED {
      publicKey            (0),
      publicKeyCert        (1),
      otherObjectTypes     (2) },
   otherObjectTypeID       OBJECT IDENTIFIER  OPTIONAL,
   digestAlgorithm         AlgorithmIdentifier,
   objectDigest            BIT STRING }
```

```
AttCertIssuer ::=    [0]  SEQUENCE {
issuerName                    GeneralNames OPTIONAL,
baseCertificateID        [0]  IssuerSerial OPTIONAL,
objectDigestInfo         [1]  ObjectDigestInfo OPTIONAL }
                                -- مكوّنة واحدة على الأقل يجب أن تكون موجودة

-- At least one component shall be present
   ( WITH COMPONENTS { ..., issuerName PRESENT } |
   WITH COMPONENTS { ..., baseCertificateID PRESENT } |
   WITH COMPONENTS { ..., objectDigestInfo PRESENT } )

IssuerSerial  ::=  SEQUENCE {
   issuer        GeneralNames,
   serial        CertificateSerialNumber,
   issuerUID     UniqueIdentifier OPTIONAL }

AttCertValidityPeriod  ::= SEQUENCE {
   notBeforeTime       GeneralizedTime,
   notAfterTime        GeneralizedTime }
```

تختلف **الصيغة (version)** من صيغة إلى أخرى من صيغ شهادة النعت. وتكون صيغ شهادات النعت الصادرة وفقاً لقواعد تركيب (نحو) هذه المواصفة هي **الصيغة v2**.

وحقل **الحامل (holder)** يحمل هوية حامل شهادة النعت.

والمكوّنة **معرف هوية الشهادة الأساسية (baseCertificateID)** تدل، إن وجدت، على هوية شهادة مفتاح عمومي خاصة، يطلب استعمالها لاستيقان هوية هذا الحامل، عندما يجري التأكيد على الامتيازات بشهادة النعت هذه.

والمكوّنة **اسم الكيان (entityName)** تدل، إن وجدت، على اسم واحد للحامل أو على أكثر من اسم. وإذا كانت المكوّنة **اسم الكيان** هي المكوّنة الوحيدة الموجودة في حقل **الحامل**، يمكن لأي شهادة مفتاح عمومي تحمل واحداً من هذه الأسماء كصاحب لها، أن تستعمل لاستيقان هوية هذا الحامل عندما يجري التأكيد على الامتيازات بشهادة النعت هذه. وعندما تكون المكوّنتان **معرف هوية الشهادة الأساسية واسم الكيان** موجودتين كلتيهما، لا يمكن استعمال إلا الشهادة التي تحددها المكوّنة **معرف هوية الشهادة الأساسية**. وفي هذه الحالة، تدرج المكوّنة **اسم الكيان** فقط كأداة تساعد المتحقق من الامتياز على تحديد موقع شهادة المفتاح العمومي المعنية.

ملاحظة 1 – ينطوي استعمال المكوّنة **الأسماء العامة (GeneralNames)** وحدها لتحديد الحامل على مخاطرة، في كونها تسدد فقط نحو اسم واحد للحامل. وهذا لا يكفي عموماً للتمكن من استيقان هوية الحامل بغية إسناد امتيازات لهذا الحامل. واستعمال اسم مُصْدر شهادة مفتاح عمومي معينة ورقم تسلسلها يساعدان مع ذلك مُصْدر شهادة النعت على الاعتماد على عملية الاستيقان التي تقوم بها السلطة CA عند إصدارها هذه الشهادة الخاصة للمفتاح العمومي. وفوق ذلك فإن بعض الخيارات في **الأسماء العامة** (مثل **عناوين بروتوكول الإنترنت (IPAddress)**) غير مناسبة لاستعمالها في تسمية حامل لشهادة نعت، لا سيما عندما يكون الحامل دوراً وليس كياناً منفرداً. وهناك مشكلة أخرى مع **الأسماء العامة** لاستعمالها وحدها كمعرّف هوية لحامل ما، هي أن كثيراً من أشكال الأسماء الواردة في هذه البنية لا يكون لها سلطات أو عمليات تسجيل صارمة لإسناد الأسماء.

المكوّنة **معلومات موجزة عن الهدف (objectDigestInfo)** تستعمل مباشرة، إن وجدت، لاستيقان هوية الحامل، بما في ذلك حالة حامل قابل للتنفيذ (مثل البُرَيْمج applet). يتم استيقان الحامل بمقارنة محتوى **موجز الهدف (objectDigest)** بموجز عن المعلومات المقابلة التي يولدها المتحقق من الامتياز باستعمال نفس الخوارزمية المحددة في المكوّنة **معلومات موجزة عن الهدف**. وإذا وجد الموجزان متطابقين، يكون قد تم الاستيقان من الحامل لأغراض توكيد الامتيازات المعلن عنها في شهادة النعت هذه.

- يشار إلى مكوّنة **المفتاح العمومي (publicKey)**، عندما يوجد فَرْم للمفتاح العمومي لكيان ما. وقد لا يؤدي فرم المفتاح العمومي فقط إلى تحديد شهادة واحدة (أي يمكن أن تظهر قيمة مفتاح متطابقة في عدة شهادات). ولكي تربط شهادة نعت بمفتاح عمومي، يجب حساب الفرم على تمثيل هذا المفتاح العمومي الذي قد يكون موجوداً في شهادة مفتاح عمومي. ويجب بصورة خاصة أن يكون مُدْخَل خوارزمية الفَرْم هو التشفير بقواعد التشفير المميزة (DER) لتمثيل مفتاح وارد في **معلومات المفتاح العمومي للصاحب**

(SubjectPublicKeyInfo). ويلاحظ أن هذا يتضمن **معرف هوية الخوارزمية (AlgorithmIdentifier)** ومعه كذلك **سلسلة البتات (BIT STRING)**. ويلاحظ أيضاً أنه إذا كانت قيمة المفتاح العمومي المستعملة مُدْخَلاً لدالّة الفَرْم، قد استخرجت من شهادة مفتاح عمومي، يصبح من الممكن عندئذ (أي إذا كانت معلمات خوارزمية التوقيع الرقمي موروثة) أن يكون ذلك مُدخَلاً غير كافٍ للفَرْم. والمُدْخل الصحيح للفَرم في هذا السياق، يجب أن يشمل قيمة المعلمات الموروثة، وبذلك يمكن أن يختلف عن المكوّنة **معلومات المفتاح العمومي للصاحب** الموجودة في شهادة المفتاح العمومي.

- يشار إلى المكوّنة **شهادة المفتاح العمومي (publicKeyCert)**، عندما تُفْرم شهادة مفتاح عمومي، ويكون الفرم يشمل كامل التشفير بقواعد التشفير المميزة (DER) الواقع على شهادة مفتاح عمومي، بما في ذلك بتات التوقيع.
- يشار إلى المكوّنة **أنماط هدف أخرى (otherObjectTypes)**، عندما تُفْرم أهداف أخرى غير المفاتيح العمومية أو شهادات المفتاح العمومي (أي: أهداف البرمجيات). ويمكن، بصورة اختيارية، تقديم هوية نمط الهدف. ويمكن تحديد الجزء المطلوب فرمه من الهدف إما بمعرف هوية للهدف يعلن عنه صراحة، وإما، في حالة كون معرف الهوية غير مقدم، بالسياق الذي يستعمل فيه الهدف.

ويقدّم الحقل **المُصْدر (issuer)** هوية سلطة النعت (AA) التي تُصدر الشهادة.

- المكوّنة **اسم المُصْدر (issuerName)** تبيّن، إن وجدت، اسماً أو عدة أسماء للمُصْدر.
- المكوّنة **معرف هوية الشهادة الأساسية (baseCertificateID)** تبيّن المُصْدر، إن وجدت، بالإحالة إلى شهادة مفتاح عمومي خاصة، يكون هذا المُصْدر صاحبها.
- المكوّنة **معلومات موجزة عن الهدف (objectDigestInfo)** تبيّن المُصْدر، إن وجدت، بتقديم فَرْم لمعلومات التعريف بالهوية الخاصة بالمُصْدر.

المكوّنة **التوقيع (signature)** تبين الخوارزمية التجفيرية المستعملة للتوقيع رقمياً على شهادة النعت.

المكوّنة **رقم التسلسل (serialNumber)** تحتوي على الرقم المتسلسل الذي يحدّد دون لبس شهادة النعت في ميدان تطبيق مُصْدرها.

المكوّنة **فترة صلاحية شهادة النعت (attrCertValidityPeriod)** تحمل الفترة الزمنية التي تبقى أثناءها شهادة النعت معتبرة صالحة، معبراً عنها في نسق **التوقيع المعمّم (GeneralizedTime)**.

المكوّنة **النعوت (attributes)** تحتوي على النعوت المصاحبة للحامل والتي يجري التصديق عليها (مثل الامتيازات).

ملاحظة 2 – يمكن أن يكون هذا التتابع من النعوت خالياً، في حالة كون شهادات النعت واصفاتٍ للنعت.

المكوّنة **معرف هوية المُصْدر الوحيد (issuerUniqueID)** يمكن استعمالها للتعريف بهوية مُصْدر شهادة النعت، في الحالات التي تكون فيها مكوّنة المصدر غير كافية.

المكوّنة **توسّعات (extensions)** تتيح إضافة مجالات جديدة إلى شهادة النعت.

وإذا ظهرت عناصر مجهولة داخل التوسع، وكان التوسع موسوماً غير حرج، يجب تجاهل هذه العناصر وفقاً لقواعد قابلية التوسع الموثقة في الفقرة 2.2.12 من التوصية ITU-T X.519 | من المعيار ISO/IEC 9594-5.

يركز إطار شهادة النعت المشروح في هذا القسم تركيزاً رئيسياً على النموذج الموضوع فيه الامتياز داخل شهادات النعت. ومع ذلك نوّه بذلك سابقاً، يمكن أيضاً وضع توسعات الشهادات المحددة في هذا القسم داخل شهادة مفتاح عمومي تستخدم التوسع **نعوت الدليل للصاحب (subjectDirectoryAttributes)**.

2.12 مسيرات شهادة النعت

كما في حالة شهادات المفتاح العمومي بالضبط، قد تكون هناك ضرورة لنقل مسيرة شهادة نعت (مثلاً للإعلان عن امتيازات في بروتوكول أحد التطبيقات). ويمكن استعمال نمط المعطيات التالية من الترميز ASN.1 لتمثيل مسيرة شهادة نعت:

```
AttributeCertificationPath ::= SEQUENCE {
   attributeCertificate        AttributeCertificate,
   acPath                      SEQUENCE OF ACPathData OPTIONAL }

ACPathData ::= SEQUENCE {
   certificate           [0]   Certificate  OPTIONAL,
   attributeCertificate  [1]   AttributeCertificate  OPTIONAL }
```

13 العلاقة بين سلطة النعت (AA) ومَصْدر السلطة (SOA) وسلطة إصدار الشهادة (CA)

إن سلطة النعت (AA) وسلطة إصدار الشهادة (CA) هما منطقياً (وغالباً مادياً) مستقلتان بالكامل. إن إحداث "هوية" والاحتفاظ بها يمكن (وينبغي) أن يكونا منفصلين عن البنية التحتية لإدارة الامتياز (PMI). وهكذا يمكن أن توجد البنية التحتية للمفتاح العمومي (PKI)، بما فيها السلطات CA، وأن تصبح شغّالة بالكامل، قبل أن تقام البنية PMI. والسلطة CA، وإن كانت هي مصدر السلطة للهويات داخل ميدانها، إلا أنها ليست أوتوماتياً مصدر السلطة للامتيازات. ولذلك لا تكون السلطة CA بالضرورة هي سلطة AA، وبالاقتضاء المنطقي لن تكون بالضرورة مسؤولة عن القرار الذي يحدد أي الكيانات يمكن أن يعمل بصفة سلطة النعت (AA) (وذلك بتسميتها لهذه المهمة في شهادات هوياتها).

أما مَصْدر السلطة (SOA) فهو كيان يضع الثقة فيه متحقق من الامتياز، باعتباره كياناً تعود إليه المسؤولية النهائية عن إسناد مجموعة من الامتيازات. وقد يقوم أحد الموارد بالحدّ من سلطة مُصْدر السلطة، عن طريق وضعه الثقة في بعض مصادر السلطة لوظائف معينة (كأن يعتمد سلطة لامتيازات القراءة، ويعتمد سلطة أخرى لامتيازات الكتابة). ومصدر السلطة (SOA) هو بحد ذاته سلطة نعت (AA)، لأنه يصدر شهادات إلى كيانات أخرى، تسند فيها امتيازات إلى هذه الكيانات. ومصدر السلطة يعتبر مماثلاً "لسلطة جذرية في إصدار الشهادة" أو "لمرسّخة الثقة" في البنية PKI، من حيث إن متحققاً من الامتياز يضع ثقته في الشهادات التي يوقعها مصدر السلطة (SOA). وقد يلزم في بعض البيئات أن تراقب السلطات CA مراقبة صارمة الكيانات التي يمكنها أن تعمل كمُصْدر سلطة. ويقدم هذا الإطار آلية لدعم هذا المطلب. وقد لا تكون المراقبة لازمة في بعض البيئات الأخرى، والآليات التي تحدد الكيانات التي يمكنها أن تعمل كمَصْدر سلطة في مثل هذه البيئات قد تقع خارج نطاق هذه المواصفة.

هذا الإطار يتميز بالمرونة ويمكنه أن يفي بمتطلبات العديد من أنماط البيئات.

أ) يمكن في كثير من البيئات إسناد جميع الامتيازات مباشرة إلى كيانات فردية عن طريق سلطة نعت واحدة، هي مَصْدر السلطة.

ب) وقد تتطلب بيئات أخرى أن تكون ميزة الأدوار الخيارية مدعومة، حيث يقوم أفراد بإصدار شهادات تسند أدواراً إليهم بالذات. والامتيازات التي تصحب دوراً معنياً هي مسندة ضمناً لهؤلاء الأفراد. ويمكن أن يتم إسناد امتيازات الدور في شهادات نعت صادرة للدور بالذات أو عبر وسائل أخرى (تشكيلات محلية مثلاً).

ج) ولهذا الإطار ميزة اختيارية أخرى هي تحمّل تفويض الامتياز. وعند القيام بالتفويض، يسند مصدر السلطة امتيازاً إلى كيان مسموح له هو الآخر أن يعمل كسلطة نعت، فيقوم هو بدوره بتفويض الامتياز. ويمكن أن يستمر التفويض عبر عدة سلطات نعت وسيطة إلى أن يسند الامتياز أخيراً إلى كيان نهائي، لا يعود بمقدوره أن يفوّض الامتياز بعد ذلك. وقد تكون سلطات النعت الوسيطة قادرة أيضاً أو قد لا تكون قادرة على العمل بصفة مؤكد امتياز بخصوص الامتيازات التي تفوّضها إلى غيرها.

د) ويمكن في بعض البيئات لنفس الكيان المادي أن يعمل بنفس الوقت كسلطة نعت وكسلطة إصدار الشهادة. وتقع حالة هذا الدور المنطقي المزدوج مع الكيان المادي نفسه، عندما يكون الامتياز محمولاً في توسع **نعوت الدليل للصاحب (subjectDirectoryAttributes)** من شهادة مفتاح عمومي. بينما تعمل كيانات مادية

منفصلة في بيئات أخرى كسلطات نعت وسلطات إصدار شهادة. وفي حالة سلطة النعت، يسند الامتياز باستخدام شهادات النعت بدلاً من شهادات المفتاح العمومي.

وعندما تكون شهادات النعت تشير إلى شهادات المفتاح العمومي من حيث مُصْدروها وحاملوها، تستعمل البينة PKI لاستيقان الحاملين (مؤكدي الامتياز)، وللتحقق من توقيعات المُصْدرين الرقمية.

وتشرح هذه المواصفة نموذجين للتفويض. وفي أول نموذجي التفويض يكون مفوِّض الامتياز هو سلطة نعت قادرة على إصدار شهادات لتفويض هذا الامتياز إلى الآخرين. والنموذج الثاني للتفويض ينص على خدمة تفويض (DS) مستقلة، يكون الكيان فيها يصدر شهادات باسم سلطة نعت أخرى (قد تكون قادرة أو غير قادرة على إصدار شهادة نعت بالذات). ولا تستطيع خدمة التفويض هذه أن تعمل كمؤكد بذاتها على هذا الامتياز. وتتبع خدمة التفويض بصورة خاصة للظروف التي ترغب في الاحتفاظ ببعض الإدارة المركزية على مجموعة الامتيازات التي يجري تفويضها داخل ميدانها. كأن تسمح مثلاً مجموعة من مخدّم واحد أو من عدة مخدّمين تابعين لخدمة التفويض يقومون بالتفويض، بدلاً من حاملي امتيازات أفراد، بأن يتم تحديد المجموعة الكاملة من الامتيازات المفوّض بها في بيئة معينة، انطلاقاً من بنية تحتية مركزية، وأن يتم تبعاً لذلك تعديل قرارات السياسة والإدارة. ويمكن أن يتم نشر المخدّمين في خدمة التفويض وفقاً لنموذجين متمايزين. فيسند مَصْدر السلطة الامتياز، في أحد النموذجين، إلى حاملي امتيازات، ويرخص لهؤلاء الحاملين أن يفوضوا الامتياز إلى غيرهم. ومع ذلك يطلب حاملو الامتيازات من خدمة التفويض أن تفوض الامتياز باسمهم، بدلاً من أن يصدروا هم بأنفسهم شهادات نعت تقوم هي بتفويض الامتياز. ولا تحمل خدمة التفويض هذا الامتياز لذاتها، ولذلك فهي لا تستطيع أن تعمل كمؤكد على هذا الامتياز، ومع ذلك، يرخص مَصْدر السلطة لخدمة التفويض بأن تصدر شهادات نعت باسم حاملي امتيازات آخرين. أما نموذج الانتشار الآخر فهو شبيه بالنموذج الأول مع الاستثناء التالي، فخدمة التفويض هي حامل بالفعل، مسند إليه الامتياز المطلوب تفويضه، غير أن خدمة التفويض لا يرخص لها بأن تعمل مؤكداً للامتياز، ولكنها مخوّلة بتفويضه فقط. وفي هذه الحالة يجب إدراج التوسع **لا تأكيد (noAssertion)** في شهادة النعت الصادرة من مَصْدر السلطة إلى خدمة التفويض. وتدعى خدمة التفويض مُصْدراً غير مباشر.

وفي كلا نموذجي النشر، يصدر مَصْدر السلطة نعوتاً أو امتيازات إلى سلطات نعت تابعة. فتطلب سلطات النعت بعدئذ من خدمة التفويض أن تصدر مجموعات فرعية من نعوت هذه الامتيازات إلى حاملين آخرين. وفي نموذج النشر الثاني، تستطيع خدمة التفويض أن تتحقق، ويكون على الطرف الواثق أن يتحقق من كون التفويض يجري بطريقة صحيحة.

1.13 الامتياز في شهادة النعت

تستطيع الكيانات أن تحصل على الامتياز بطريقتين:

- يمكن لسلطة النعت أن تسند من جانب واحد امتيازاً إلى كيان ما، عبر إحداث شهادة نعت (قد تكون بمبادرة خالصة منها، أو بناء على طلب من طرف ثالث). ويمكن تخزين هذه الشهادة في فهرس مفتوح للعموم، وبالتالي يمكن لمتحقق من الامتياز أو لمتحققين أن يعالجوها لاحقاً، لاتخاذ قرار بالترخيص. وقد يتم كل ذلك دون مفرمة الكيان أو دون إجراء صريح من جانبه.
- كما يمكن لكيان ما أن يطلب امتيازاً من سلطة نعت معينة. وبمجرد إحداث هذه الشهادة، يمكن إرجاعها (حصراً) إلى الكيان الطالب، الذي يقدمها صراحة عندما يطلب النفاذ إلى مورد محمّي.

ويلاحظ أن سلطة النعت تحتاج في الطريقتين إلى أن تقوم بالأعمال الواجبة لتتأكد من أن الامتياز قد أسند فعلاً إلى الكيان. وقد ينطوي ذلك على آليات تقع خارج النطاق، شبيهة بتصديق سلطة CA على ارتباط زوج مؤلف من هوية ومفتاح.

وتصلح البنية التحتية لإدارة الامتياز (PMI) القائمة على شهادات النعت في البيئات التي يكون فيها أي واحد من الشروط التالية متوفراً:

- الكيان المسؤول عن إسناد امتياز خاص إلى حامل يكون مختلفاً عن الكيان المسؤول عن إصدار شهادات المفتاح العمومي لنفس الصاحب؛ أو

- يوجد عدد من نعوت الامتياز المطلوب إسنادها إلى حامل، من عدد من السلطات؛ أو
- يختلف العمر المفيد لامتياز ما عن فترة الصلاحية لشهادة المفتاح العمومي للحامل (يكون العمر المفيد للامتياز أصغر بكثير من فترة الصلاحية بصورة عامة)؛ أو
- يكون الامتياز صالحاً فقط أثناء بعض الفواصل الزمنية التي تكون متزامنة مع صلاحية المفتاح العمومي للمستعمل أو مع صلاحية امتيازات أخرى.

2.13 الامتياز في شهادة المفتاح العمومي

في بعض الحالات، تتم مصاحبة الامتيازات للصاحب عبر ممارسات سلطة CA. وقد توضع مثل هذه الامتيازات مباشرة في شهادات المفتاح العمومي (وبذلك يعاد استعمال قسم كبير من بنية تحتية مقامة فعلاً)، بدلاً من إصدار شهادات نعت. ويكون الامتياز في هذه الحالات مدرجاً في التوسع **نعوت الدليل للصاحب (subjectDirectoryAttributes)** من شهادة المفتاح العمومي.

وتصلح هذه الآلية في البيئات التي يكون واحد أو أكثر من الشروط التالية متوفراً:

- نفس الكيان المادي يعمل بنفس الوقت كسلطة إصدار الشهادة (CA) وسلطة النعت (AA)؛ أو
- العمر المفيد للامتياز متراصف مع عمر المفتاح العمومي الوارد في الشهادة؛ أو
- تفويض الامتياز غير مسموح به؛ أو
- التفويض مسموح به، ولكن في كل عملية تفويض، تكون جميع الامتيازات الواردة في الشهادة (في التوسع **نعوت الدليل للصاحب**) تمتلك نفس معلمات التفويض، وتنطبق جميع التوسعات المتصلة بالتفويض بصورة متساوية على جميع الامتيازات الواردة في الشهادة.

14 نموذجات البنية التحتية لإدارة الامتياز (PMI)

1.14 النموذج العام

يتكون النموذج العام لإدارة الامتياز من ثلاثة كيانات: الهدف ومؤكد الامتياز والمتحقق من الامتياز.

ويمكن أن يكون الهدف مورداً محمياً، كما في حالة تطبيق التحكم في النفاذ. والمورد المحميّ هو هدف، ويكون لهذا النمط من الأهداف طرائق قد تكون منفذة (كأن يكون الهدف هو الجدار الواقي الذي تتوفر له الطريقة الهدف "السماح بالدخول"، أو يمكن أن يكون الهدف ملفاً في نظام محفوظات تتوفر له الطرائق الأهداف: القراءة والكتابة والتنفيذ). ومن أنماط الأهداف الأخرى في هذا النموذج يمكن أن يكون هدفاً موقّعاً في تطبيق بغير رفض.

ومؤكد الامتياز هو كيان يحمل امتيازاً خاصاً، ويؤكد على امتيازاته في سياق استعمال خاص.

والمتحقق من الامتياز هو كيان يحدد إن كانت الامتيازات المؤكد عليها تكفي أو لا تكفي لسياق الاستعمال المعيّن.

ويقرر المتحقق من الامتياز تحديد النجاح أو الفشل، وفقاً للعوامل الأربعة التالية:

- امتياز المؤكِّد على الامتياز؛
- سياسة الامتياز النافذة؛
- المتحولات البيئية الفعلية، إن كانت ذات صلة؛
- حساسية الطريقة الهدف، إن كانت ذات صلة.

ويبين امتياز حامل الامتياز درجة الثقة التي يضعها مُصْدر الشهادة في هذا الحامل، من حيث كون هذا الحامل يتقيد بخصائص السياسة غير المنفذة بوسائل تقنية. ويكون هذا الامتياز مغلفاً في شهادة أو شهادات نعت حامل الامتياز (أو في توسع **نعوت الدليل للصاحب** لشهادة المفتاح العمومي الخاصة به)، التي يمكن أن تقدم إلى المتحقق من الامتياز في طلب الإبطال، أو

الموزعة بوسيلة أخرى، كالدليل مثلاً. ويتم تبويب الامتياز عبر استخدام بنية **النعت** التي تحتوي **نمط النعت (AttributeType)** وعلى **مجموعة من قيم النعت (SET OF AttributeValue)**. وقد يكون لبعض أنماط النعت المستعملة لتحديد امتياز قواعد تركيب (نَحْوٌ) بسيطة جداً، كأن تكون **عدداً صحيحاً (INTEGER)** واحداً أو **سلسلة أثمونات (OCTET STRING)**. وقد يكون لبعضها الآخر قواعد تركيب أكثر تعقيداً، ويورد الملحق D مثالاً منها.

وتحدد سياسة الامتياز الدرجة التي يجب أن يكون عليها الامتياز لكي يعتبر كافياً، من أجل حساسية طريقة هدفٍ معينة أو سياق استعمال معين. وتحتاج سياسة الامتياز إلى حماية من أجل تكاملية المعطيات وأصالتها. وتوجد عدة إمكانيات لنقل السياسة. والإمكانية الطرفية الأولى هي فكرة اعتبار السياسة لم يجر نقلها إطلاقاً في الواقع، بل إنه جرى تعريفها بكل بساطة، واحتفظ بها محلياً في بيئة المتحقق من الامتياز. والإمكانية الطرفية الأخرى هي فكرة اعتبار بعض السياسات "عامة" وينبغي نقلها نحو كل كيان في النظام، أو ينبغي أن تكون معروفة منه. وتوجد بدائل عديدة ما بين هاتين الإمكانيتين الطرفيتين. وتشرح هذه المواصفة مكوّنات تخطيطية، لتخزين معلومات سياسة الامتياز في الدليل.

تحدّد سياسة الامتياز عتبة القبول لمجموعة معينة من الامتيازات. وهذا يعني أنها تحدد بدقة متى ينبغي لمتحقق من الامتياز أن يستنتج أن مجموعة من الامتيازات تكون "كافية" لكي تضمن النفاذ لمؤكد الامتياز (بشأن طلبه الهدف أو المورد أو التطبيق وغيرها).

لا تقيّس هذه المواصفة قواعد التركيب (النحو) من أجل تعريف سياسة الامتياز. ويحتوي الملحق D على زوج من أمثلة النحو التي يمكن استعمالها لهذا الغرض. ومع ذلك فإنها ليست سوى أمثلة فقط. ويمكن استمال أي قواعد تركيب لهذا الغرض، بما في ذلك النص الواضح. وبصرف النظر عن قواعد التركيب المستعملة لتعريف سياسة الامتياز، يجب أن يُعرَّف بكل مرحلة من سياسة الامتياز تعريفاً لا لبس فيه. وتستعمل معرفات هوية الهدف لهذا الغرض.

```
PrivilegePolicy ::= OBJECT IDENTIFIER
```

وتبيّن المتحولات البيئية، إن كانت ذات صلة، تلك الجوانب المطلوبة من السياسة لتحديد النجاح أو الفشل (مثل الوقت من اليوم أو الرصيد الحالي للحساب) التي يستطيع المتحقق من الامتياز النفاذ إليها بالوسائل المحلية. وتمثيل المتحولات البيئية هي مسألة محلية بالكامل.

كما تبيّن حساسية الطريقة الهدف، إن كانت ذات صلة، نعوت الوثيقة أو الطلب المطلوبة معالجتهما، مثل القيمة النقدية لنقل الأموال المقترح تنفيذه، أو سرية محتوى الوثيقة. ويمكن تشفير حساسية الطريقة الهدف تشفيراً صريحاً في واسم أمني مصاحب أو في شهادة نعت تحملها الطريقة الهدف، أو يمكن تغليفها ضمناً في بنية ومحتويات هدف المعطيات المصاحب. ويمكن تشفيرها بواحد من عدة أساليب مختلفة. فيمكن تشفيرها مثلاً خارج ميدان تطبيق البنية التحتية PMI، داخل الواسم X.411 المصاحب للوثيقة أو داخل حقل تبادل المعطيات EDIFACT، كما يمكن تشفيرها تشفيراً صلباً في تطبيق المتحقق من الامتياز. ويمكن كبديل أيضاً إجراء التشفير داخل البنية التحتية PMI، في شهادة نعت مصاحبة للطريقة الهدف. ولا تستعمل حساسية الطريقة الهدف، في بعض سياقات الاستعمال.

لا توجد بالضرورة أي علاقة ربط بين متحقق من امتياز وأي سلطة نعت خاصة. وكما أن لحاملي الامتيازات شهادات نعت صادرة لهم من سلطات نعت مختلفة عديدة، كذلك يمكن للمتحققين من الامتيازات أن يقبلوا شهادات صادرة عن سلطات نعت عديدة، ليست بالضرورة مترابطة ترابطاً تراتبياً فيما بينها، لكي يؤمنوا النفاذ إلى مورد خاص.

ويمكن أن يستعمل إطار شهادة النعت لإدارة امتيازات من أنماط مختلفة ولأغراض متعددة. والمصطلحات المستعملة في هذه المواصفة، مثل مؤكد الامتياز والمتحقق من الامتياز وغير ذلك، هي مستقلة عن أي تطبيق أو استعمال خاص.

1.1.14 البنية PMI في سياق التحكم في النفاذ

يوجد إطار معياري للتحكم في النفاذ (الوصية ITU-T X.812 | المعيار ISO/IEC 10181-3) يحدد مجموعة مقابلة من المصطلحات خاصة بتطبيق التحكم في النفاذ. وتجد هنا تقابلاً بين المصطلحات العامة المستعملة في هذه المواصفة والمصطلحات المستعملة في إطار التحكم في النفاذ، بغية توضيح العلاقة القائمة بين هذا النموذج وهذه المواصفة.

فمؤكد الامتياز في هذه المواصفة يقوم بدور "المبادر" في إطار التحكم في النفاذ.

والمتحقق من الامتياز في هذه المواصفة يقوم بدور "وظيفة القرار في التحكم في النفاذ (ADF)" في إطار التحكم في النفاذ.

والطريقة الهدف التي يعلن عن امتياز لها في هذه المواصفة تقابل "الدريئة المستهدفة" المحددة في إطار التحكم في النفاذ.

والمتحولات البيئية في هذه المواصفة تقابل "معلومات السياق" في إطار التحكم في النفاذ.

وسياسة الامتياز المدروسة في هذه المواصفة يمكن أن تتضمن "سياسة التحكم في النفاذ" و"قواعد سياسة التحكم في النفاذ" كما هي محددة في إطار التحكم في النفاذ.

يتيح هذا النموذج تغطية شبكة قائمة من الموارد المطلوبة حمايتها، تغطية متجانسة سَلِسة ببنية تحتية لإدارة الامتياز (PMI). وكون المتحقق من الامتياز يعمل كبوّابة إلى طريقة هدف حساسة، فيقبل أو يرفض طلبات لإبطال هذه الطريقة الهدف، يتيح حماية الهدف دون أن يتأثر الهدف نفسه أو إنه يتأثر قليلاً. فالمتحقق من الامتياز يرشح جميع الطلبات المتعلقة بالطرائق الأهداف، ولا يسمح إلا بمرور الطلبات المرخّصة أصولاً إلى الطرائق الأهداف المناسبة.

2.1.14 البنية PMI في سياق عدم الرفض

يوجد إطار معياري للتحكم في النفاذ (الوصية ITU-T X.813 | المعيار ISO/IEC 10181-4) يحدد مجموعة مقابلة من المصطلحات خاصة بعدم الرفض. وتجد هنا تقابلاً بين المصطلحات العامة المستعملة في هذه المواصفة والمصطلحات المستعملة في إطار عدم الرفض، بغية توضيح العلاقة بين هذا النموذج وهذه المواصفة.

فمؤكد الامتياز في هذه المواصفة يقوم بدور "صاحب البرهان" أو "المَصْدر" في إطار عدم الرفض.

والمتحقق من الامتياز في هذه المواصفة يقوم بدور "مستعمل البرهان" أو "المستلم" في إطار عدم الرفض.

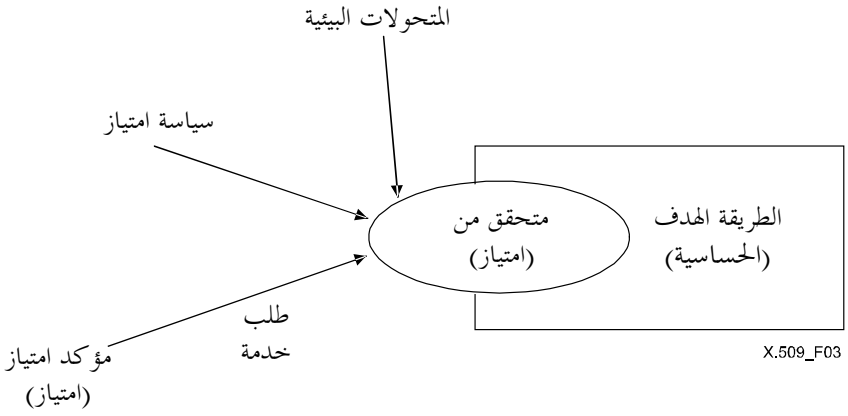
والطريقة الهدف التي يعلن عن امتياز لها في هذه المواصفة تقابل "الدريئة المستهدفة" المحددة في إطار عدم الرفض.

والمتحولات البيئية في هذه المواصفة تقابل "التاريخ والوقت الذي يقدّم فيه البرهان أو يتم التحقق منه" في إطار عدم الرفض.

وسياسة الامتياز المدروسة في هذه المواصفة يمكن أن تتضمن "سياسة أمن عدم الرفض" في إطار عدم الرفض.

2.14 نموذج التحكم في النفاذ

يبين نموذج التحكم كيف يمارس التحكم في النفاذ إلى الطريقة الهدف الحساسة. ولهذا النموذج خمس مكوّنات هي: مؤكد الامتياز، والمتحقق من الامتياز، والطريقة الهدف، وسياسة الامتياز، والمتحولات البيئية (انظر الشكر 3). ومؤكد الامتياز هو الذي يمتلك الامتياز، والطريقة الهدف تمتلك الحساسية. والتقنيات المشروحة هنا تمكن المتحقق من الامتياز من التحكم في النفاذ إلى الطريقة الهدف بواسطة مؤكد الامتياز، وفقاً لسياسة الامتياز. ويمكن أن يكون الامتياز والحساسية كلاهما مَعْلَمتين متعددتي القيم.

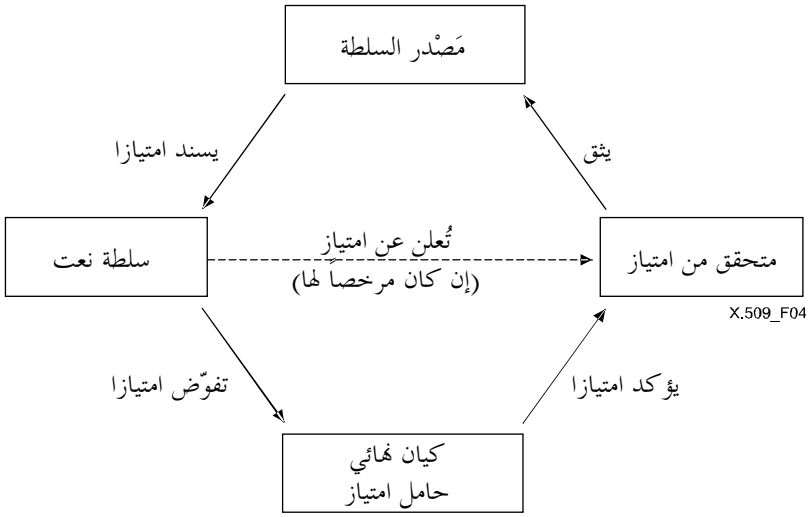


الشكل 3 – نموذج التحكم

ويمكن أن يكون مؤكد الامتياز كياناً تعرف هويته شهادة مفتاح عمومي، أو أن يكون هدفاً قابلاً للتنفيذ، يعرف هويته موجز لصورته على قرص، وغير ذلك.

3.14 نموذج التفويض

قد يحتاج الأمر أحياناً إلى تفويض الامتياز في بعض البيئات، وهذا هو أحد وجوه الإطار الاختيارية، وهو غير مطلوب في جميع البيئات. ولنموذج التفويض أربع مكوّنات هي: المتحقق من الامتياز، ومَصْدر السلطة (SOA)، وسلطات النعت الأخرى، ومؤكد الامتياز (انظر الشكل 4).



الشكل 4 – نموذج التفويض

لما كانت بعض البيئات لا تستخدم التفويض، فإن مَصْدر السلطة يكون هو المُصْدر الأولي للشهادات التي تسند امتيازات على حاملي امتيازات. وفي هذه الحالة يرخص مَصْدر السلطة لحامل الامتياز أن يعمل كسلطة نعت، وأن يفوض بدوره هذا الامتياز إلى كيانات أخرى بإصداره شهادات تحتوي على نفس الامتياز (أو على مجموعة فرعية منه). ويمكن لمَصْدر السلطة أن يفرض تقييدات على هذا التفويض (كأن يحدّ من طول المسيرة أو يحد من مكان الأسماء في التفويض المسموح به). وجميع سلطات النعت الوسيطة هذه تستطيع، عن طريق شهادات تصدرها إلى حاملي امتيازات آخرين، أن ترخص لهؤلاء الحاملين بأن يعملوا كسلطات نعت وأن يقوموا بدورهم بالتفويض. وأحد التقييدات العامة المفروضة على التفويض هو أن أي سلطة نعت لا تستطيع التفويض بامتيازات أكثر مما تحمل هي منها. وأي كيان يقوم بالتفويض يمكنه فرض تقييدات أخرى على مَقْدرات سلطات النعت الواقعة بعده.

وعند استعمال التفويض، يضع المتحقق من الامتياز ثقته في مَصْدر السلطة، لكي يفوّض بكل هذه الامتيازات أو ببعضها إلى حاملين، يمكن أن يقوم بعضهم بدوره بتفويض كل هذه الامتيازات أو بعضها إلى حاملين آخرين.

يضع المتحقق من الامتياز ثقته في مَصْدر السلطة (SOA) كسلطة تهتم بمجموعة معينة من الامتيازات الخاصة بالمورد. وإذا كانت شهادة مؤكد الامتياز ليست صادرة عن هذا المُصْدر للسلطة، يجب على المتحقق من الامتياز أن يوجد مسيرة تفويض للشهادات، تذهب من هذا المؤكد للامتياز إلى شهادة صادرة عن مَصْدر السلطة. وإقرار صلاحية مسيرة التفويض هذه يجب أن يتضمن التحقق من كل سلطة نعت عندها ما يكفي من الامتيازات، وأنها كانت مرخصاً لها حسب الأصول بتفويض هذه الامتيازات.

وفي الحالة التي تنقل الامتيازات فيها عن طريق شهادات النعت، تكون مسيرة التفويض متمايزة عن مسرية إقرار صلاحية الشهادة التي تستعمل لإقرار صلاحية شهادات المفتاح العمومي للكيانات المشتركة في عملية التفويض. ومع ذلك فإن نوعية الأصالة التي تعطى لعملية إقرار الصلاحية لشهادة مفتاح عمومي تكون متناسبة مع قياس الهدف الجارية حمايته.

ويمكن لمسيرة التفويض أن تكون مؤلفة بكاملها من شهادات نعت أو بكاملها من شهادات مفتاح عمومي. وكيان التفويض الذي يحصل على امتيازه في شهادة نعت لا يمكنه القيام بالتفويض، إن كان مرخصاً له، إلا بإصداره لاحقاً شهادات نعت. وبالمثل كيان

التفويض الذي يحصل على امتيازه في شهادة مفتاح عمومي، لا يمكنه القيام بالتفويض، إن كان مرخصاً له، إلا بإصداره لاحقاً شهادات مفتاح عمومي. ولا تستطيع تفويض الامتياز إلا سلطات النعت فقط، أما الكيانات النهائية فلا تستطيع.

4.14 نموذج الأدوار

تتيح الأدوار إسناد امتيازات إلى أفراد بصورة غير مباشرة. وشهادات إسناد الأدوار إلى الأفراد، التي تسند دوراً واحداً لهم أو أكثر من دور، تصدر عبر نعت للدور، تحتوي الشهادة عليه. وتسند امتيازات خاصة إلى اسم دور عبر شهادات مواصفة الدور، بدلاً من أن تسند إلى حاملي امتيازات أفراد عبر شهادات نعت. هذه السوية غير المباشرة تسمح مثلاً بتحيين الامتيازات المسندة إلى دور ما، من دون أن تتأثر الشهادات التي تسند الأدوار إلى أفراد. وشهادات إسناد الأدوار يمكن أن تكون شهادات نعت أو شهادات مفتاح عمومي. أما شهادات مواصفة الأدوار فيمكن أن تكون شهادات نعت، ولكن ليس شهادات مفتاح عمومي. وإذا كانت شهادات مواصفة الأدوار غير مستعملة، يمكن إجراء إسناد الامتيازات إلى الأدوار عبر وسائل أخرى (بتشكيلة محلية لمتحقق من امتياز مثلاً).

ويمكن أن تحدث الإجراءات التالية:

- يمكن لأي سلطة نعت أن تحدد أي عدد من الأدوار؛
- يمكن لسلطات نعت مختلفة أن تحدد الدور نفسه وتديره، وأن تحدد أعضاء الدور وتديرهم بصورة منفصلة؛
- يمكن تفويض عضوية الدور، تماماً كأي امتياز آخر.
- يمكن إعطاء الدوار والعضوية فيها أي عمر نافع مناسب.

وإذا كانت شهادة إسناد الدور هي شهادة نعت، يكون نعت **الدور (role)** موجوداً في مكوّنة النعوت من شهادة النعت. وإذا كانت شهادة إسناد الدور هي شهادة مفتاح عمومي، يكون نعت **الدور** موجوداً في توسع **نعوت الدليل للصاحب (subjectDirectoryAttributes)**. وفي هذه الحالة الأخيرة، تكون كل الامتيازات الإضافية الموجودة في شهادة المفتاح العمومي، امتيازات مسندة مباشرة إلى صاحب الشهادة، وليست امتيازات مسندة إلى الدور.

وهكذا يستطيع مؤكد الامتياز أن يقدم شهادة إسناد دور إلى المتحقق من الامتياز، يبيّن فقط أن مؤكد الامتياز يمتلك دوراً خاصاً (مثل "المدير" أو "المشتري"). ويستطيع المتحقق من الامتياز أن يعرف مسبقاً الامتيازات المصاحبة للدور المؤكد، أو قد يكون مضطراً لاكتشافها بوسائل أخرى، حتى يتخذ قرار بنجاح الترخيص أو فشله. ويمكن استخدام شهادة مواصفة الدور لهذا الغرض.

ويجب على المتحقق من الامتياز أن يكون على مستوى من الفهم لكي يستوعب الامتيازات المحددة في الدور. ويمكن أن يجري إسناد هذه الامتيازات إلى الدور داخل البنية التحتية PMI ضمن شهادة مواصفة الدور أو خارج البنية PMI (بتشكيلة محلية مثلاً). وإذا كانت امتيازات الدور مؤكدة في شهادة مواصفة الدور، فإن هذه المواصفة تقدم الآليات التي يمكن بها ربط هذه الشهادة بشهادة إسناد الدور ذات الصلة. ولا يمكن تفويض شهادة مواصفة الدور إلى أي كيان آخر. ويمكن أن يكون مُصْدر شهادة إسناد الدور مستقلاً عن مُصْدر شهادة مواصفة الدور، ويمكن إدارتهما بصورة مستقلة عن بعضهما (من حيث انقضاء الصلاحية أو الإبطال أو ما إلى ذلك). ويمكن للشهادة نفسها (شهادة النعت أو شهادة المفتاح العمومي) أن تكون شهادة إسناد دور وأن تحتوي في الوقت نفسه على إسناد امتيازات أخرى مباشرة إلى الفرد نفسه. وفي كل الأحوال يجب أن تكون شهادة مواصفة الدور شهادة منفصلة متمايزة.

ملاحظة – استعمال الأدوار في إطار ترخيص واحد يمكن أن يزيد التعقيد في معالجة المسيرة، لأن مثل هذه الوظائفية تحدد مسيرة تفويض أخرى تحتاج إلى متابعة. ويمكن لمسيرة التفويض الخاصة بشهادة تخصيص الدور أن تشرك سلطات نعت مختلفة، ويمكنها أن تكون مستقلة عن سلطة النعت التي أصدرت شهادة مواصفة الدور.

1.4.14 نعت الدور

إن مواصفة أنماط نعت الامتياز هي بصورة عامة مسألة خاصة بكل تطبيق، وتخرج عن نطاق هذه المواصفة. والشذوذ الوحيد في هذا المضمار هو نعت محدد فيما يلي بشأن إسناد حامل إلى دور. وتقع مواصفة قيم نعت الدور خارج نطاق هذه المواصفة.

```
role  ATTRIBUTE  ::= {
      WITH SYNTAX          RoleSyntax
      ID                   id-at-role }

RoleSyntax ::= SEQUENCE {
roleAuthority      [0]     GeneralNames     OPTIONAL,
roleName           [1]     GeneralName }
```

يستعمل نعت الامتياز هذا لملء حقل **النعوت** في شهادة إسناد الدور. فإذا كانت شهادة إسناد الدور هي شهادة مفتاح عمومي، يمكن استعمال هذا النعت لملء التوسع **نعوت الدليل للصاحب** في هذه الشهادة.

والمكوّنة **سلطة الدور (roleAuthority)**، إن وجدت، تحدد السلطة المعترف بها لكي تكون مسؤولة عن إصدار شهادة مواصفة الدور.

وإذا كانت **سلطة الدور** موجودة، وكان متحقق من الامتياز يستخدم شهادة مواصفة دور لكي يحدد الامتيازات المسندة إلى الدور، يجب أن يكون واحد على الأقل من الأسماء الواردة في **سلطة الدور** موجوداً في مجال **المُصْدر (issuer)** لشهادة مواصفة هذا الدور. وإذا كان المتحقق من الامتياز يستخدم وسائل أخرى غير شهادة مواصفة الدور لكي يجدد الامتيازات المسندة إلى الدور، فإن الآليات المطلوبة لضمان كون هذه الامتيازات مسندة من قبل سلطة مسمّاة في هذه المكوّنة، تكون واقعة خارج نطاق هذه المواصفة.

أما إذا كانت **سلطة الدور** غائبة، فتتحدد هوية السلطة المسؤولة عبر وسائل أخرى. ويكون التوسّع **معرف هوية شهادة مواصفة الدور (roleSpecCertIdentifier)** في شهادة إسناد الدور هو إحدى الوسائل لإنجاز هذا الربط، وذلك في الحالة التي تكون فيها شهادة مواصفة الدور مستعملة لإسناد امتيازات إلى الدور.

والمكوّنة **اسم الدور (roleName)** تعرّف بالدور الذي يكون مسنداً إليه حامل شهادة إسناد الدور التي تحتوي على هذا النعت. وإذا استعمل متحقق من امتياز شهادة مواصفة دور لتحديد الامتيازات المسندة إلى هذا الدور، يجب أن يظهر اسم هذا الدور في حقل **الحامل (holder)** من شهادة مواصفة الدور.

5.14 نعت معلومات عن الامتياز في اللغة XML (اللغة التأشيرية التوسعية)

إن مواصفة الامتيازات هي بصورة عامة مسألة خاصة بكل تطبيق، وتخرج عن نطاق هذه المواصفة. وبينما لا يعرّف هذا النعت أي معلومات خاصة بالامتياز، إلا أنه يشكل نعت احتواء، يمكن بواسطته نقل امتيازات مشفرة باللغة XML (اللغة التأشيرية التوسّعية) في شهادات النعت.

```
xmlPrivilegeInfo   ATTRIBUTE  ::= {
  WITH SYNTAX      UTF8String -- contains XML-encoded privilege information
  ID               id-at-xMLPrivilegeInfo }
```

ويمكن تعريف تخطيطة اللغة XML بشأن نمط نعت الدور إما بالترميز ASN.1 (ترميز علم النحو المجرد 1) وإما بالتخطيطة XSD (تخطيطة اللغة XML في تجمّع شبكة العنكبوت العالمية (W3C)).

أما اللغة XML الموجودة في **UTF8String** فيجب أن تعرّف هويتها ذاتياً.

وفيما يلي تخطيطة في الترميز ASN.1 تعرف نمط النعت "دور" في اللغة XML. وتتبعه مواصفة XDS لنفس نمط النعت، مع مثال عن مطابق XML. وهذا المثال صالح لمطابقي التخطيطتين ASN.1 وXDS، ويمكن إقرار صلاحيته للأداتين ASN.1 أو XDS كلتيهما.

ومثال التخطيطة يعرّف نعتاً "للدور" مع معرف هوية، وسلطة إصدار، واسم للدور.

```
CERTIFICATE-ATTRIBUTE DEFINITIONS ::=
BEGIN
  Role ::= [UNCAPITALIZED] SEQUENCE {
     id            [ATTRIBUTE] XML-ID,
     authorities   SEQUENCE (1..MAX) OF
```

```
                authority UTF8String,
    name        UTF8String }

  XML-ID  ::= UTF8String

END
```

تقدم التخطيطة XSD التالية تعريفاً بذيلاً (مكافئاً بكل صرامة):

```
<schema xmlns="http://www.w3.org/2000/08/XMLSchema">
 <element name="role">
  <attribute name="id" type="ID"/>
  <complexType>
   <sequence>
    <element name="authorities">
     <complexType>
      <sequence>
       <element name="authority" type="string" minOccurs="1" maxOccurs="*"/>
      </sequence>
     </complexType>
    </element>
    <element name="name" type="string"/>
   </sequence>
  </complexType>
 </element>
</schema>
```

مثال من مطابق لتعريفات التخطيطة أعلاه، التي يمكنها أن تعطي قيمة لنمط النعت **معلومات عن الامتياز في اللغة** XML (xMLPrivilegeInfo) الذي قد يكون التالي:

```
<role id="123" xmlns="http://www.example.org/certificates/attribute">
<authorities>
<authority>Fictitious Organization</authority>
</authorities>
<name>manager</name>
</role>
```

15 توسعات شهادة إدارة الامتياز

يمكن أن تدمج التوسعات التالية في شهادات الأغراض إدارة الامتياز. ومع إيراد تعريفات التوسعات بحد ذاتها، ترد أيضاً قواعد خاصة بأنماط الشهادات التي يمكن أن توجد فيها توسعات.

وباستثناء توسع معرف الهوية لمَصْدر السلطة، لا يمكن لأي واحد ن التوسعات التي يمكن أن تدمج في شهادة مفتاح عمومي، أن يدمج في مثل هذه الشهادة إلا إذا كانت هذه الشهادة تسند امتيازاً لصاحبها (مما يقتضي وجود التوسع **نعوت الدليل للصاحب (subjectDirectoryAttributes)**). وينطبق هذا التوسع على **جميع** الامتيازات الموجودة في توسع **نعوت الدليل للصاحب**، إذا كان أي واحد من هذه التوسعات موجوداً في شهادة مفتاح عمومي.

وقوائم الإبطال التي تستخدم لإصدار تبليغات الإبطال بخصوص شهادات النعت (القوائم ACRL والقوائم AARL) يمكنها أن تحتوي على أي توسع في القائمة CRL أو في مدخل CRL، كما هو معرّف في القسم الثاني من هذه المواصفة لاستعماله في القوائم CRL أو في القوائم CARL.

ويحدد هذا البند التوسعات في الميادين التالية:

أ) *إدارة امتياز أساسي:* تحمل هذه التوسعات في الشهادات معلومات تتعلق بتأكيد امتياز.

ب) *إبطال امتياز:* تحمل هذه التوسعات في الشهادات معلومات تخص الموقع الذي توجد فيه معلومات الوضع القانوني للإبطال.

ج) *مَصْدر السلطة:* تتعلق هذه التوسعات في الشهادات بمَصْدر إسناد الامتياز الذي توجد فيه معلومات الوضع القانوني للإبطال.

د) *الأدوار:* تحمل هذه التوسعات في الشهادات معلومات تخص الموقع الذي توجد فيه شهادات توصيف (مواصفة) الدور ذات الصلة.

هـ) *التفويض:* تسمح هذه التوسعات في الشهادات بفرض تقييدات على التفويض لاحقاً للامتيازات المسندة.

1.15 توسعات إدارة الامتياز الأساسي

1.1.15 المتطلبات

ترتبط المتطلبات التالية بإدارة الامتياز الأساسي.

أ) يجب أن يكون المُصْدرون قادرين على وضع تقييدات على المدة التي يمكن أن يبقى الامتياز فيها قابلاً للتأكيد؛

ب) يجب أن يكون المُصْدرون قادرين على تحديد شهادات نعت مستهدفة من مخدّمين أو خدمات معينة؛

ج) قد يحتاج المُصْدرون إلى نقل معلومات مهيأة لعرضها على مؤكدي الامتياز و/أو على المتحققين من الامتياز الذين يستعملون هذه الشهادة؛

د) يمكن أن يكون المُصْدرون قادرين على وضع تقييدات على سياسات الامتياز، يمكن معها استعمال الامتياز المسند.

2.1.15 حقول توسع إدارة الامتياز الأساسي:

تعرّف حقول التوسع التالية:

أ) توصيف المدة؛

ب) المعلومات المستهدفة؛

ج) تبليغ المستعمل؛

د) سياسات الامتياز المقبولة؛

هـ) المُصْدر غير المباشر؛

و) غياب التأكيد.

1.2.1.15 توسّع توصيف المدة

يمكن لسلطة نعت (AA) أن تستعمل توسع توصيف المدة لكي تحدّ من الفترة الزمنية التي يمكن خلالها لحامل الامتياز، المسند في الشهادة التي تحتوي على هذا التوسع، أن يؤكد عليه. فيمكن لسلطة نعت مثلاً أن تصدر شهادة تسند امتيازات لا يمكن التأكيد عليها إلا من يوم الاثنين إلى يوم الجمعة ومن الساعة 9:00 صباحاً إلى الساعة 5:00 بعد الظهر. وإليك مثالاً آخر، ينطبق على حالة التفويض التي يفوض فيها أحد المديرين سلطة التوقيع في فترة غيابه في الإجازة إلى أحد مرؤوسيه.

ويعرف هذا الحقل كما يلي:

```
timeSpecification EXTENSION ::= {
    SYNTAX              TimeSpecification
    IDENTIFIED BY       id-ce-timeSpecification }
```

قد يوجد هذا التوسع في شهادات النعت أو شهادات المفتاح العمومي التي تصدرها سلطات النعت، بما فيها مصادر السلطة، إلى كيانات قد تعمل كمؤكدات امتياز، يمكنها أن تشمل سلطات نعت أخرى أو كيانات نهائية. ولا يمكن أن يوجد هذا التوسع في شهادات تحتوي على توسع معرف الهوية لمَصْدر السلطة أو في شهادات صادرة لسلطات نعت لا يمكنها أن تعمل أيضاً كمؤكدات امتياز.

إذا كان هذا التوسع موجوداً في شهادة صادرة إلى كيان هو سلطة نعت، فهو لا ينطبق إلا على تأكيد هذا الكيان بشأن الامتيازات الواردة في الشهادة. وهو لا يؤثر على الفترة الزمنية التي تكون أثناءها سلطة النعت قادرة على إصدار الشهادات.

ولما كان هذا التوسع يعيّن بالفعل تخفيضاً لفترة صلاحية الشهادة التي تحتوي عليه، يجب أن يوسم هذا التوسع بأنه حرج (أي إن المُصْدر بإدماجه هذا التوسع، يحدد بصراحة بأن إسناد الامتياز لا يعود صالحاً خارج الوقت المحدد).

وإذا كان هذا التوسع موجوداً ولكن المتحقق من الامتياز لا يفهمه، يجب أن ترفض الشهادة.

1.1.2.1.15 مواءمة توصيف المدة

تقارن قاعدة مواءمة توصيف المدة من حيث التساوي قيمة معروضة بقيمة نعت من نمط **شهادة النعت (AttributeCertificate)**.

```
timeSpecificationMatch MATCHING-RULE ::= {
    SYNTAX          TimeSpecification
    ID              id-mr-timeSpecMatch }
```

2.2.1.15 توسع المعلومات المستهدفة

يتيح توسع المعلومات المستهدفة لشهادة نعت أن تستهدف مجموعة معينة من المخدّمين أو الخدمات. وينبغي ألا تستعمل شهادة النعت التي تحتوي على هذا التوسع إلا للمخدّمين المحددة ويعرّف هذا الحقل كما يلي:

```
targetingInformation EXTENSION ::= {
    SYNTAX              SEQUENCE SIZE (1..MAX) OF Targets
    IDENTIFIED BY       id-ce-targetInformation }

Targets ::=         SEQUENCE SIZE (1..MAX) OF Target

Target : :=         CHOICE {
    targetName          [0]     GeneralName,
    targetGroup         [1]     GeneralName,
    targetCert          [2]     TargetCert }

TargetCert ::=      SEQUENCE {
    targetCertificate   IssuerSerial,
    targetName          GeneralName OPTIONAL,
    certDigestInfo      ObjectDigestInfo OPTIONAL }
```

إذا كانت المكوّنة **الاسم المستهدف (targetName)** موجودة، فإنها تقدم أسماء المخدّمين أو الخدمات المستهدفة التي تستهدفها شهادة النعت الحاوية.

وإذا كانت المكوّنة **المجموعة المستهدفة (targetGroup)** موجودة، فإنها تقدم اسم مجموعة مستهدفة تستهدفها شهادة النعت الحاوية. وكيف تتحدد عضوية هدف في مجموعة مستهدفة هو أمر يقع خارج هذه المواصفة.

وإذا كانت المكوّنة **الشهادة المستهدفة (targetCert)** موجودة، فإنها تحدد هويات المخدّمين أو الخدمات بالإحالة إلى شهادتها.

ويمكن أن يوجد هذا التوسع في شهادات نعت صادرة عن سلطات نعت، بما فيها مصادر السلطة، إلى كيانات يمكنها أن تعمل كمؤكدات امتياز، بما فيها سلطات النعت والكيانات النهائية. ولا يمكن أن يوجد هذا التوسع في شهادات مفتاح عمومي أو في شهادات نعت صادرة إلى سلطات نعت لا يمكنها أن تعمل أيضاً كمؤكدات امتياز.

وإذا كان هذا التوسع موجوداً في شهادة نعت صادرة إلى كيان هو سلطة نعت، فإنه لا ينطبق إلا على تأكيد هذا الكيان للامتيازات الموجودة في الشهادة. وهو لا يؤثر على مقدرة سلطة النعت على إصدار الشهادات.

ويكون هذا التوسع حرجاً دائماً.

وإذا كان هذا التوسع موجوداً، ولكن المتحقق من الامتياز ليس من بين المتحققين المحددين من الامتياز، ينبغي أن ترفض شهادة النعت.

وإذا كان هذا التوسع موجوداً، لا تكون شهادة النعت مستهدفة، ويمكن أن يقبلها أي مخدّم.

3.2.1.15 توسّع تبليغ المستعمل

يتيح توسع تبليغ المستعمل لسلطة نعت أن تدرج تبليغاً ينبغي عرضه على الشاشة لحامل الامتياز عندما يؤكدا امتيازه و/أو للمتحقق من الامتياز عندما يستعمل شهادة النعت التي تحتوي على هذا الامتياز.

ويعرّف هذا الحقل كما يلي:

```
userNotice  EXTENSION  ::= {
    SYNTAX              SEQUENCE SIZE (1..MAX) OF UserNotice
    IDENTIFIED BY       id-ce-userNotice }
```

يمكن أن يوجد هذا التوسع في شهادات نعت أو في شهادات مفتاح عمومي صادرة عن سلطات نعت، بما فيها مصادر السلطة، إلى كيانات يمكنها أن تعمل كمؤكدات امتياز، بما فيها سلطات نعت أخرى، وكيانات نهائية. ولا يمكن أن يوجد هذا التوسع في الشهادات التي تحتوي على توسع معرف الهوية لمَصْدر السلطة أو في شهادات النعت الصادرة عن سلطات نعت لا يمكنها أن تعمل أيضاً كمؤكدات امتياز.

وإذا كان هذا التوسع موجوداً في شهادة صادرة عن كيان هو سلطة نعت، فإنه لا ينطبق إلا على تأكيد هذا الكيان للامتيازات الموجودة في الشهادة. وهو لا يؤثر على مقدرة سلطة النعت على إصدار الشهادات.

ويمكن أن يكون هذا الوسع حرجاً أو غير حرج، حسب تقدير مصدر الشهادة.

فإذا كان هذا التوسع موسوماً بأنه حرج، يجب أن تعرض تبليغات المستعمل على الشاشة للمتحقق من الامتياز في كل مرة يؤكد فيها على امتياز. وإذا كان مؤكد الامتياز يقدم شهادة النعت إلى المتحقق من الامتياز (أي كان المتحقق من الامتياز لا يستخرج الشهادة من مستودع)، يجب أن تعرض تبليغات المستعمل على الشاشة لمؤكّد الامتياز أيضاً.

وإذا كان هذا التوسع موسوماً بأنه غير حرج، يمكن لمتحقق من الامتياز أن يمنحه إلى مؤكد الامتياز بصرف النظر عما إذا كانت تبليغات المستعمل معروضة أم لا على الشاشة لمؤكد الامتياز و/أو للمتحقق من الامتياز.

4.2.1.15 توسّع سياسات الامتياز المقبولة

يستعمل حقل سياسات الامتياز المقبولة لكي يقيّد تأكيد الامتيازات المسندة أثناء الاستعمال مع مجموعة محددة من سياسات الامتياز.

ويعرف هذا الحقل كما يلي:

```
acceptablePrivilegePolicies EXTENSION ::= {
    SYNTAX              AcceptablePrivilegePoliciesSyntax
    IDENTIFIED BY       id-ce-acceptablePrivilegePolicies }

AcceptablePrivilegePoliciesSyntax       ::=     SEQUENCE SIZE (1..MAX) OF PrivilegePolicy
```

يمكن أن يوجد هذا التوسع في شهادات نعت أو في شهادات مفتاح عمومي صادرة عن سلطات نعت، بما فيها مصادر السلطة، إلى سلطات نعت أخرى أو إلى كيانات نهائية. وعندما يكون هذا التوسع موجوداً في شهادة مفتاح عمومي، فهو لا يعني إلا مقدرة الصاحب على العمل كمؤكد امتياز فيما يخص الامتيازات الموجودة في التوسع **نعوت الدليل للصاحب**.

وعندما يكون هذا التوسع موجوداً، يوسم بأنه حرج.

وإذا كان هذا التوسع موجوداً، وكان المتحقق من الامتياز يفهمه، يجب على المتحقق أن يتأكد من أن سياسة الامتياز التي هي موضوع المقارنة مع هذه الامتيازات هي واحدة من السياسات المحددة في هذا التوسع.

وإذا كان هذا التوسع موجوداً، وكان المتحقق من الامتياز لا يفهمه، يجب رفض الشهادة.

5.2.1.15 توسّع المُصْدر غير المباشر

يمكن في بعض البيئات أن يجري تفويض الامتياز بصورة غير مباشرة. فيطلب مانح التفويض في مثل الحالات أن تصدر سلطة نعت شهادة تفوّض فيها الامتياز باسمه إلى كيان آخر. ويستعمل حقل المُصْدر غير المباشر في شهادة نعت أو في شهادة مفتاح عمومي صادرة عن مَصْدر سلطة إلى سلطة نعت. ووجود هذا التوسع يعني أن سلطة النعت الصاحبة مخوّلة من مَصْدر السلطة هذا أن تعمل كمكتب وسيط وتصدر شهادات تفوض الامتياز باسم مانحي تفويض آخرين.

```
indirectIssuer EXTENSION ::= {
  SYNTAX              BOOLEAN
  IDENTIFIED BY     id-ce-indirectIssuer }
```

ويكون هذا التوسع غير حرج دائماً.

وتقارن قاعدة مواءمة المُصْدر غير المباشر قيمة معروضة من حيث التساوي بقيمة نعت من النمط **شهادة النعت**.

```
indirectIssuerMatch MATCHING-RULE  ::= {
SYNTAX  BOOLEAN
IDid-mr-indirectIssuerMatch }
```

وترجع هذه القاعدة القيمة "**صائب**" إذا كانت القيمة المخزونة تحتوي على التوسع **المُصْدر غير المباشر (indirectIssuer)**، وكانت القيمة الموجودة في القيمة المعروضة تتوافق مع القيمة المخزونة.

6.2.1.15 توسع غياب التأكيد

عندما يكون هذا التوسع موجوداً، فهو يدل على أن حامل شهادة النعت لا يستطيع التأكيد على الامتيازات المبيّنة في نعوت شهادة النعت. ولا يمكن إدراج هذا الحقل إلا في شهادات النعت لسلطة النعت، وليس في شهادات النعت للكيان النهائي. وعندما يوجد هذا التوسع يكون موسوماً بأنه حرج دائماً.

```
noAssertion EXTENSION ::= {
SYNTAX NULL
IDENTIFIED BY  id-ce-noAssertion }
```

2.15 توسعات إبطال الامتياز

1.2.15 المتطلبات

يتعلق المتطلبان التاليان بإبطال شهادات النعت:

أ) لكي يتم التحكم في قدود القوائم CRL، قد يكون من اللازم أن تخصص مجموعات فرعية من مجموعة جميع الشهادات التي تصدرها سلطة نعت واحدة، إلى قوائم CRL مختلفة؛

ب) يجب أن يكون مصدرو شهادات النعت قادرين على أن يبينوا في إحدى شهادات النعت، عدم وجود معلومات إبطال بشأن هذه الشهادة.

2.2.15 حقول توسع إبطال الامتياز

يعرّف حقلا التوسع التاليان:

أ) *نقاط توزيع القائمة CRL؛*

ب) *غياب معلومات الإبطال.*

1.2.2.15 توسع نقاط توزيع القائمة CRL

يعرف القسم الثاني من هذه المواصفة توسع نقاط توزيع القائمة CRL، لكي يستعمل في شهادات المفتاح العمومي. ويمكن أن يدرج هذا الحقل أيضاً في شهادات النعت. وقد يوجد في شهادات صادرة إلى سلطات نعت، بما فيها مصادر السلطة، كما قد يوجد في شهادات صادرة إلى كيانات نهائية.

وعندما يوجد متحقق من الامتياز في إحدى الشهادات، يجب عليه أن يعالج هذا التوسع تماماً بنفس الطريقة المشروحة في القسم الثاني بشأن شهادات المفتاح العمومي.

2.2.2.15 توسع غياب معلومات الإبطال

في بعض البيئات التي تصدر فيها شهادات النعت بفترات صلاحية قصيرة جداً، قد لا تكون هناك حاجة إلى إبطال الشهادات. وتستطيع سلطة النعت أن تستعمل هذا التوسع لكي تبين عن عدم وجود معلومات عن الوضع القانوني لإبطال شهادة النعت هذه. ويعرف هذا الحقل كما يلي:

```
noRevAvail EXTENSION ::= {
    SYNTAX                  NULL
    IDENTIFIED BY           id-ce-noRevAvail }
```

ويمكن أن يوجد هذا التوسع في شهادات النعت الصادرة إلى كيانات نهائية عن سلطات نعت، بما فيها مصادر السلطة. ويجب ألا يوجد هذا التوسع في شهادات مفتاح عمومي أو في شهادات نعت صادرة إلى سلطات النعت.

يكون هذا التوسع غير حرج دائماً.

وإذا كان هذا التوسع موجوداً في شهادة نعت، يكون على متحقق من الامتياز أن يبحث عن معلومات الوضع القانوني للإبطال.

3.15 توسعات مَصْدر السلطة

1.3.15 المتطلبات

يتعلق المتطلبان التاليان بمصادر السلطة:

أ) إن من الضروري أن تقوم سلطة إصدار الشهادة في بعض البيئات بمراقبة صارمة للكيانات التي يمكن أن تعمل كمصادر سلطة؛

ب) إن من الضروري وضع تعريفات نحوية وقواعد تراتبية تكون صالحة لنعوت الامتياز التي توفرها مصادر السلطة المسؤولة.

2.3.15 حقول توسع مَصْدر السلطة

يعرّف حقلا التوسع التاليان:

أ) *معرف هوية مَصْدر السلطة؛*

ب) *واصف النعت.*

1.2.3.15 توسع معرف الهوية لمَصْدر السلطة (SOA)

يبين توسع معرف الهوية لمصدر السلطة أن صاحب الشهادة يمكنه أن يعمل كمَصْدر سلطة لأغراض إدارة الامتياز. وبهذه الصفة يستطيع صاحب الشهادة أن يحدد نعوتاً تسند امتيازاً، وأن يصدر شهادة واصف النعت لهذه النعوت وأن يستعمل المفتاح الخاص المقابل للمفتاح العمومي المصدّق عليه لكي يصدر شهادات تسند الامتيازات إلى حاملين. ويمكن أن تكون هذه الشهادات الأخيرة شهادات نعت أو شهادات مفتاح عمومي مع توسع **نعوت الدليل للصاحب** الذي يضم هذه الامتيازات.

ولا يكون هذا التوسع مطلوباً في بعض البيئات، وتحل محله آليات أخرى لاستعمالها في تحديد الكيانات التي يمكنها أن تعمل كمصادر سلطة. ولا يكون هذا التوسع مطلوباً إلا في البيئات التي يحتاج الأمر فيها إلى مراقبة مركزية صارمة تقوم بها سلطة إصدار الشهادة لكي تدير الكيانات التي تعمل كمصادر سلطة.

ويعرّف هذا الحقل كما يلي:

```
sOAIdentifier EXTENSION  ::= {
   SYNTAX              NULL
   IDENTIFIED BY       id-ce-sOAIdentifier }
```

وعندما يكون هذا التوسع غير موجود في إحدى الشهادات، تتحدد بوسائل أخرى مقدرة الصاحب أو الحامل على العمل كمصدر سلطة.

ولا يمكن أن يوجد هذا الحقل إلا في شهادة مفتاح عمومي صادرة لَمصْدر سلطة. ويجب ألا يوجد في شهادات النعت أو في شهادات المفتاح العمومي التي تكون صادرة إلى سلطات نعت أخرى أو إلى كيانات نهائية صاحبة امتيازات.

وتنطبق الشهادات المتقاطعة على شهادات المفتاح العمومي فقط، ولا تنطبق على شهادات النعت، وعليه فإن الشهادة المتقاطعة الصادرة إلى سلطة إصدار الشهادة التي هي مُصْدرة شهادة تحتوي على توسع معرف الهوية لَمصْدر السلطة، لا يمكنها أن توفر نقل الثقة إلى مَصْدر السلطة المعرفة هويته في هذا التوسع.

ويكون هذا التوسع غير حرج دائماً.

1.1.2.3.15 مواءمة معرف هوية مَصْدر السلطة

تقارن قاعدة مواءمة معرف الهوية لَمصْدر السلطة، قيمة معروضة بقيمة نعت من النمط **شهادة**.

```
sOAIdentifierMatch MATCHING-RULE ::= {
  SYNTAX     NULL
  ID         id-mr-sOAIdentifierMatch }
```

وترجع هذه القاعدة القيمة "**صائب**" إذا كانت القيمة المخزونة تحتوي على توسع معرف الهوية لمصدر السلطة.

2.2.3.15 توسع واصف النعت

يحتاج المتحققون من الامتياز إلى تعريف نعت الامتياز وإلى القواعد التراتبية التي تحكُم تفويض هذا الامتياز لاحقاً، لكي يتأكدوا من صحة الترخيص تماماً. ويمكن أن تقدم هذه التعريفات والقواعد إلى المتحققين من الامتياز بوسائل متنوعة تقع خارج نطاق هذه المواصفة (أي يمكن أن يقوم بتشكيلها محلياً المتحقق من الامتياز).

ويقدم هذا التوسع آلية يمكن أن يستعملها مَصْدر سلطة لكي يوفر للمتحققين من الامتياز تعريفات نعوت الامتياز وما يصاحبها من القواعد التراتبية. وشهادة النعت التي تحتوي على هذا التوسع تدعى شهادة واصف النعت، وهي نوع خاص من شهادات النعت. وعلى الرغم من كون شهادة واصف النعت تطابق **شهادة النعت** من حيث قواعد التركيب فهي:

- تحتوي على **تتابع (SEQUENCE)** خالٍ في حقل **نعوتها**؛
- شهادة صادرة لذاتها (أي المُصْدر والحامل فيها هما كيان واحد)؛
- تحتوي على توسع واصف النعت.

ويعرف هذا الحقل كما يلي:

```
attributeDescriptor EXTENSION  ::= {
   SYNTAX              AttributeDescriptorSyntax
   IDENTIFIED BY       {id-ce-attributeDescriptor } }
```

```
AttributeDescriptorSyntax ::= SEQUENCE {
    identifier                  AttributeIdentifier,
    attributeSyntax             OCTET STRING (SIZE(1..MAX)),
    name                [0]     AttributeName   OPTIONAL,
    description         [1]     AttributeDescription   OPTIONAL,
    dominationRule              PrivilegePolicyIdentifier}

AttributeIdentifier ::= ATTRIBUTE.&id({AttributeIDs})

AttributeIDs ATTRIBUTE ::= {...}

AttributeName ::= UTF8String(SIZE(1..MAX))

AttributeDescription ::= UTF8String(SIZE(1..MAX))

PrivilegePolicyIdentifier ::=  SEQUENCE {
    privilegePolicy             PrivilegePolicy,
    privPolSyntax               InfoSyntax }
```

وتكون المكوّنة **معرف الهوية (identifier)** التي قيمتها من التوسع **واصف النعت (attributeDescriptor)** هي معرف هوية الهدف الذي يعرف نمط النعت.

وتحتوي المكوّنة **قواعد تركيب النعت (attributeSyntax)** على تعريف الترميز ASN.1 لقواعد تركيب النعت ويعطى تعريف الترميز ASN.1 هذا كما هو محدد لمكوّنة **المعلومات في** *قواعد التوائم* للنعت الشغّال المعرفة في التوصية ITU-T X.501 | المعيار ISO/IEC 9594-2.

والمكوّنة **الاسم (name)** تحتوي بصورة اختيارية على اسم بلغة واضحة يمكن التعرف به إلى النعت.

والمكوّنة **الوصف (description)** تحتوي بصورة اختيارية على وصف للنعت بلغة واضحة.

وتحدد المكوّنة **قاعدة التراتب (dominationRule)** ماذا يعني قولنا عن نعت بشأن امتياز مفوض بأنه "أقل من" الامتياز المقابل الذي يحمله القائم بالتفويض. وتحدد المكوّنة **سياسة الامتياز (privilegePolicy)** المرحلة التي تحتوي على قواعد سياسة الامتياز بواسطة معرف هوية الهدف فيها. وتحتوي المكوّنة **قواعد تركيب السياسة الخاصة (privPolSyntax)** إما على سياسة الامتياز بذاتها وإما على مؤشر يدل على الموقع الذي تقع فيه سياسة الامتياز. وعندما يكون المؤشر مدرجاً، يكون مدرجاً أيضاً فَرْم اختياري لسياسة الامتياز، لكي يتيح التحقق من تكاملية معطيات سياسة الامتياز المحال إليها.

ولا يمكن أن يوجد هذا التوسع إلا في شهادات واصف النعت. ويجب ألا يوجد هذا التوسع في شهادات المفتاح العمومي أو في شهادات النعت، غير الشهادات الصادرة لذاتها عن مصادر السلطة.

ويكون هذا التوسع غير حرج دائماً.

وشهادة واصف النعت التي يحدثها مَصْدر السلطة عند إحداث أو تعريف نمط النعت المقابل هي وسيلة يمكن بها أن يفهم التقييد العام المتعلق بالتفويض "البَعْدي"، وأن ينفذ كذلك في البنية التحتية. وشهادات النعت التي تحتوي على هذا التوسع تُخْتزن في الدليل داخل النعت **شهادة واصف النعت (attributeDescriptorCertificate)** من مدل الدليل مَصْدر السلطة.

1.2.2.3.15 مواءمة واصف النعت

تقارن قاعدة مواءمة واصف النعت من حيث التساوي قيمة معروضة بقيمة نعت من النمط **شهادة النعت (AttributeCertificate)**.

```
attDescriptor MATCHING-RULE ::= {
    SYNTAX          AttributeDescriptorSyntax
    ID              id-mr-attDescriptorMatch }
```

وترجع هذه القاعدة القيمة **"صائب"**، إذا كانت القيمة المخزونة تحتوي على التوسع **واصف النعت (attributeDescriptor)** وكانت المكوّنات الموجودة في القيمة المعروضة تتوافق مع المكونات المقابلة الموجودة في القيمة المخزونة.

4.15 توسعات الأدوار

1.4.15 المتطلبات

يتعلق المتطلب التالي بالأدوار:

- إذا كانت إحدى الشهادات هي شهادة إسناد دور، يجب على المتحقق من الامتياز أن يكون قادراً على تحديد موقع شهادة توصيف الدور المقابلة التي تحتوي على الامتيازات المسندة إلى هذا الدور بالذات.

2.4.15 حقول توسع الدور

يعرّف حقل التوسع كما يلي:

- *معرف الهوية لشهادة توصيف الدور.*

1.2.4.15 توسع معرف الهوية لشهادة توصيف الدور

يمكن أن تستعمل هذا التوسع سلطة نعت، كمؤشر على شهادة توصيف الدور التي تحتوي على إسناد الامتيازات إلى الدور. كما يمكن أن يوجد في شهادة إسناد الدور (أي في شهادة تحتوي على نعت **الدور**).

ويجب على المتحقق من الامتياز الذي يتعامل مع شهادة إسناد الدور، أن يحصل على مجموعة الامتيازات الممنوحة لهذا الدور، لكي يحدد إمكانية نجاح التحقق أو فشله. فإذا كانت الامتيازات مسندة إلى الدور في شهادة توصيف الدور، يمكن استعمال هذا الحقل لتحديد موقع الشهادة.

ويعرّف هذا الحقل كما يلي:

```
roleSpecCertIdentifier EXTENSION ::=
    {
    SYNTAX              RoleSpecCertIdentifierSyntax
    IDENTIFIED BY       { id-ce-roleSpecCertIdentifier }
}

RoleSpecCertIdentifierSyntax  ::= SEQUENCE SIZE (1..MAX) OF RoleSpecCertIdentifier

RoleSpecCertIdentifier  ::= SEQUENCE {
    roleName                    [0]     GeneralName,
    roleCertIssuer              [1]     GeneralName,
    roleCertSerialNumber        [2]     CertificateSerialNumber     OPTIONAL,
    roleCertLocator             [3]     GeneralNames                OPTIONAL
    }
```

المكوّنة **اسم الدور (roleName)** تعرّف بالدور. وقد يكون هذا الاسم هو نفسه الاسم الوارد في مكوّنة **الحامل (holder)** من شهادة توصيف الدور التي يحيل إليها هذا التوسع.

والمكوّنة **مُصْدر شهادة الدور (roleCertIssuer)** تعرّف بهوية سلطة النعت التي تصدر شهادة توصيف الدور المحال إليها.

والمكوّنة **رقم تسلسل شهادة الدور (roleCertSerialNumber)** تحتوي، إن وجدت، على رقم التسلسل لشهادة توصيف الدور. ويلاحظ أنه إذا تغيرت الامتيازات المسندة إلى الدور بالذات، ينبغي إصدار شهادة توصيف جديدة للدور. ويتعين على أي شهادة تحتوي على هذا التوسع، بما فيه المكوّنة **رقم تسلسل شهادة الدور**، أن يستعاض عنها بشهادة تحيل إلى رقم التسلسل الجديد وإن كان هذا السلوك مطلوباً في بعض البيئات، إلا أنه غير مرغوب فيه في بيئات أخرى. وتكون هذه المكوّنة غائبة بصورة عامة، مما يتيح التحيين الأوتوماتي للامتيازات المسندة إلى الدور بالذات دون أن تتأثر شهادات إسناد الدور.

والمكوّنة **محدّد موقع شهادة الدور (roleCertLocator)** تحتوي، إن وجدت، على معلومات يمكن استعمالها لتحديد موقع شهادة توصيف الدور.

ويمكن أن يوجد هذا التوسع في شهادات إسناد الدور التي تكون شهادات نعت أو شهادات مفتاح عمومي صادرة عن سلطات نعت، بما فيها مصادر السلطة، إلى سلطات نعت أخرى أو إلى كيانات نهائية حاملة للامتياز. ويجب ألا يوجد هذا التوسع في شهادات تحتوي على توسع معرف الهوية لمَصْدر السلطة.

ويمكن لمتحقق من الامتياز أن يستعمل هذا التوسع، إن وجد، لكي يحدد موقع شهادة توصيف الدور.

وإذا لم يكن هذا التوسع موجوداً:

أ) فإما أن تستعمل وسائل أخرى لتحديد موقع شهادة توصيف الدور؛

ب) وإما أن تستعمل آليات لا تستند إلى شهادة توصيف الدور، في سبيل إسناد الامتيازات إلى الدور (أي يمكن أن يشكل المتحقق من الامتياز محلياً امتيازات الدور).

ويكون هذا التوسع غير حرج دائماً.

1.1.2.4.15 مواءمة معرف الهوية لشهادة توصيف الدور

تقارن قاعدة مواءمة معرف الهوية لشهادة توصيف الدور من حيث التساوي قيمة معروضة بقيمة نعت من النمط **شهادة النعت (AttributeCertificate)**.

```
roleSpecCertIdMatch MATCHING-RULE ::= {
    SYNTAX          RoleSpecCertIdentifierSyntax
    ID              id-mr-roleSpecCertIdMatch }
```

وترجع هذه القاعدة القيمة "**صائب**" إذا كانت القيمة المخزونة تحتوي على التوسع **معرف الهوية لشهادة توصيف الدور (roleSpecCertIdentifier)**، وكانت المكوّنات الموجودة في القيمة المعروضة تتوافق مع المكوّنات المقابلة في القيمة المخزونة.

5.15 توسعات التفويض

1.5.15 المتطلبات

تتعلق المتطلبات التالية بتفويض الامتيازات:

أ) يجب أن تكون شهادات امتياز الكيانات النهائية متمايزة عن شهادات سلطة النعت، منعاً للكيانات النهائية من أن تجعل أنفسها سلطات نعت من دون ترخيص. ويجب أيضاً أن تتمكن سلطة النعت من الحدّ من أن تجعل أنفسها سلطات نعت من دون ترخيص. ويجب أيضاً أن تتمكن سلطة النعت من الحدّ من طول مسيرة التفويض المتلاحق؛

ب) يجب أن تكون سلطة النعت قادرة على تعيين مكان الأسماء المناسب الذي يمكن أن يحدث فيه تفويض الامتياز. ويجب أن يكون المتحقق من الامتياز قادراً على التحقق من احترام هذه القيود؛

ج) يجب أن تكون سلطة النعت قادرة على تعيين سياسات الشهادة المقبولة التي يجب أن يستعملها مؤكدو الامتياز لاحقاً فيما بعد من مسيرة التفويض، لاستيقان أنفسهم عندما يؤكدون على تفويض امتياز لدى سلطة النعت هذه؛

د) يجب على المتحقق من امتياز أن يكون قادراً على تحديد موقع شهادة النعت المقابلة لمُصْدر للتأكد من أن هذا المُصْدر يتيسر له ما يكفي من الامتياز حتى يقوم بتفويض الامتياز الوارد في الشهادة الحالية؛

هـ) يحتاج الأمر إلى خدمة تفويض (DS) مستقلة، تصدر شهادات بتفويض الامتيازات، ولا يكون مخدّم هذه الخدمة DS قادراً على التصرف بصفة المؤكد على هذه الامتيازات.

2.5.15 حقول توسع التفويض

تعرّف حقول التوسع التالية:

أ) *تقييدات النعت الأساسية؛*

ب) *تقييدات الاسم المفوّض به؛*

ج) *سياسات الشهادات المقبولة؛*

د) *معرف هوية نعت السلطة؛*

هـ) *المُصدر غير المباشر؛*

و) *صادر نيابة عن (باسم ...).*

1.2.5.15 توسع تقييدات النعت الأساسية

يبين هذا الحقل إن كان التفويض اللاحق للامتيازات المسندة في الشهادة التي تحتوي على هذا التوسع هو تفويض مسموح. وإن كان كذلك يمكن أيضاً تحديد قيد على طول مسيرة التفويض.

ويعرّف هذا الحقل كما يلي:

```
basicAttConstraints EXTENSION ::=
{
    SYNTAX              BasicAttConstraintsSyntax
    IDENTIFIED BY       { id-ce-basicAttConstraints }
}

BasicAttConstraintsSyntax ::= SEQUENCE
  {
    authority           BOOLEAN DEFAULT FALSE,
    pathLenConstraint   INTEGER (0..MAX) OPTIONAL
  }
```

المكوّنة **السلطة (authority)** تبين إن كان الحامل مرخصاً له أم لا بتفويض الامتياز من جديد. وإذا كانت قيمة المكوّنة **السلطة** تساوي "**صائبة**"، يكون الحامل عندئذ سلطة نعت أيضاً، وهو مرخص له بالتفويض بدوره، مع مراعاة التقييدات ذات الصلة. وإذا كانت قيمة المكوّنة **السلطة** تساوي "**خاطئة**"، يكون الحامل عندئذ كياناً نهائياً، وليس مرخصاً له بتفويض الامتياز.

ولا يكون للمكوّنة **تقييد طول المسيرة (pathLenConstraint)** أي معنى إلا إذا كانت قيمة مكوّنة **السلطة** موضوعة على "**صائبة**". وهي تعطي العدد الأعظم من شهادات سلطة النعت التي يمكنها أن تتبع هذه الشهادة في مسيرة التفويض. وتدل القيمة صفر على أن صاحب هذه الشهادة يمكنه إصدار الشهادات فقط للكيانات النهائية وليس لسلطات النعت. وعندما لا يظهر حقل **تقييد طول المسيرة** في أي شهادة من سيرة التفويض، يكون ذلك دليلاً على عدم وجود حدّ لطول مسيرة التفويض. ويلاحظ أن مفعول التقييد يبدأ من الشهادة التي تليه في المسيرة. والتقييد يحدّد عدد شهادات سلطة النعت التي توجد بين شهادة سلطة النعت الوارد فيها التقييد وشهادة الكيان النهائي. والتقييد يحدّد أيضاً طول المقطع من مسيرة التفويض الموجود بين الشهادة الحاوية على هذا التوسع وشهادة الكيان النهائي. وليس له أي تأثير على عدد شهادات سلطة النعت الموجودة في مسيرة التفويض بين مرسّخة الثقة والشهادة التي تحتوي على هذا التوسع. وعليه فإن طول مسيرة التفويض الكاملة يمكن أن يكون أكبر من الطول الأعظم للمقطع الذي يقيّده هذا التوسع. ويتحكم التقييد في عدد شهادات سلطة النعت الموجودة بين شهادة سلطة النعت المحتوية على التقييد وشهادة الكيان النهائي. وعليه فإن الطول الكلي لهذا المقطع من المسيرة يمكن أن يكون أكبر من قيمة التقييد بشهادتين على الأكثر. (وهذا يشمل الشهادتين الموجودتين في النقطتين الطرفيتين من المقطع مع شهادات سلطة النعت الموجودة بين النقطتين الطرفيتين التي تقيد عددها قيمة هذا التوسع).

يمكن أن يوجد هذا التوسع في شهادات النعت أو في شهادات المفتاح العمومي الصادرة عن سلطات النعت، بما فيها مصادر السلطة، إلى سلطات نعت أخرى أو إلى كيانات نهائية. ويجب ألا يوجد هذا التوسع في شهادات تحتوي على توسع معرف هوية مَصْدر السلطة.

وإذا كان هذا التوسع موجوداً في شهادة نعت وكانت قيمة المكونة **السلطة** تساوي **"صائبة"**، يكون الحامل مرخصاً له بإصدار شهادات نعت بدوره تفوّض الامتيازات الموجودة فيها إلى كيانات أخرى، ولكن دون تفويض بإصدار شهادات مفتاح عمومي.

وإذا كان هذا التوسع موجوداً في شهادة مفتاح عمومي، وكان التوسع **تقييدات أساسية (basicConstraints)** يدل على أن الصاحب أيضاً هو سلطة إصدار الشهادة، يكون الصاحب مرخصاً له بإصدار شهادات مفتاح عمومي لاحقة تفوّض هذه الامتيازات إلى كيانات أخرى، ولكن لا يرخص له بإصدار شهادات نعت. وإذا كان تقييد طول المسيرة موجوداً، يفوض الصاحب فقط داخل تقاطع التقييد المحدد في هذا التوسع وأي تقييد موجود في التوسع **تقييدات أساسية**. وإذا كان هذا التوسع موجوداً في شهادة مفتاح عمومي ولكن التوسع **تقييدات أساسية** كان غائباً، أو كان يدل على أن الصاحب هو كيان نهائي، لا يسمح عندئذ لهذا الأخير بتفويض الامتيازات.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج حسب تقدير مُصدر الشهادة. ويوصى بأن يوسم حرجاً، وإلا فإن الحامل الذي لا يكون مرخصاً بأن يكون سلطة نعت، قد يقوم بإصدار الشهادات ويستعمل المتحقق من الامتياز مثل هذه الشهادات سهواً.

وإذا كان هذا التوسع موجوداً وكان موسوماً بأنه حرج، يحصل عندئذ ما يلي:

- إذا كانت قيمة المكوّنة **السلطة** غير موضوعة على **"صائبة"**، لا يعود النعت المفوّض به يستعمل لتفويضات جديدة؛
- وإذا كانت قيمة المكوّنة **السلطة** موضوعة على **"صائبة"**، وكانت المكوّنة **تقييد طول المسيرة (pathLenConstraint)** موجودة، يقوم المتحقق من الامتياز عندئذ بالتحقق مما إذا كانت مسيرة التفويض الجارية معالجتها تحترم التقييد **تقييد طول المسيرة**.

وإذا كان هذا التوسع موجوداً وموسوماً بأنه غير حرج، وكان المتحقق من الامتياز لا يعترف به يتعين على النظام عندئذ أن يستعمل وسائل أخرى ليحدد ما إذا كان النعت المفوض به يمكن استعماله لتفويض جديد.

وإذا كان هذا التوسع غير موجود، أو إذا كان موجوداً مع قيمة **للتتابع** خالية، يكون الحامل مقيّداً بأن يكون كياناً نهائياً فقط وليس سلطة نعت، ولا يسمح للحامل بأن يقوم بأي تفويض للامتيازات الموجودة في شهادة النعت.

1.1.2.5.15 مواءمة تقييدات النعت الأساسية

تقارن قاعدة مواءمة تقييدات النعت الأساسية من حيث التساوي قائمة معروضة بقائمة نعت من النمط **شهادة النعت (AttributeCertificate)**.

```
basicAttConstraintsMatch MATCHING-RULE  ::= {
    SYNTAX          BasicAttConstraintsSyntax
    ID              id-mr-basicAttConstraintsMatch }
```

وترجع هذه القاعدة القيمة **"صائب"**، وإذا كانت القيمة المخزونة تحتوي على التوسع **تقييدات النعت الأساسية (basicAttConstraints)**، وكانت المكونات الموجودة في القيمة المعروضة تتوافق مع المكونات المقابلة في القيمة المخزونة.

2.2.5.15 توسع تقييدات الاسم المفوّض به

يدل حقل تقييدات الاسم المفوّض به على مكان أسماء، يجب أن تتحدد فيه مواقع جميع أسماء الحاملين الموجودة في الشهادات التالية من مسيرة التفويض.

ويعرّف هذا الحقل كما يلي:

```
delegatedNameConstraints EXTENSION ::= {
    SYNTAX              NameConstraintsSyntax
    IDENTIFIED BY       id-ce-delegatedNameConstraints }
```

يعالج هذا التوسع بنفس الطريقة التي يعالج بها توسع **تقييدات الاسم (nameConstraints)** لشهادات المفتاح العمومي. وإذا كانت مكوّنة **الأشجار الفرعية المسموحة** موجودة، لا تقبل إلا شهادات النعت التي أسماء حامليها واردة في هذه الأشجار الفرعية، من أصل جميع شهادات النعت الصادرة عن سلطة النعت الحاملة وعن سلطات النعت التالية في مسيرة التفويض وأما إذا كانت مكوّنة **الأشجار الفرعية المستبعدة** موجودة، فلا تقبل أي شهادة نعت صادرة عن سلطة النعت الحاملة أو عن سلطات النعت التالية في مسيرة التفويض، ويقع اسم حاملها داخل هذه الأشجار الفرعية. وإذا كانت المكوّنتان **الأشجار الفرعية المسموحة والأشجار الفرعية المستبعدة** موجودتين كلتيهما، وكان مكانا الأسماء متشابكين، تعطى الأولوية لإعلان الاستبعاد.

ويمكن أن يوجد هذا التوسع في شهادات النعت أو في شهادات المفتاح العمومي الصادرة عن سلطات نعت، بما فيها مصادر السلطة، إلى سلطات نعت أخرى. ويجب ألا يوجد هذا التوسع في شهادات صادرة إلى كيانات نهائية أو في شهادات تحتوي على توسع معرّف هوية مَصْدر السلطة.

وإذا كان هذا التوسع موجوداً في شهادة مفتاح عمومي، وإذا كان التوسع **تقييدات الاسم** موجوداً كذلك، يمكن للصاحب أن يقوم بالتفويض فقط في تقاطع التقييد المحدد في هذا التوسع والتقييد المحدد في التوسع **تقييدات الاسم**.

ويمكن أن يوسم هذا التوسع بأنه حرج أو غير حرج حسب تقدير مُصْدر شهادة النعت. ويوصى بأن يوسم بالحرج، وإلا فإن المستعمل لشهادة نعت قد لا يتحقق من أن شهادات النعت التالية في مسيرة التفويض واقعة في مكان الأسماء الذي تتوقعه سلطة النعت المصدرة.

1.2.2.5.15 مواءمة تقييدات الاسم المفوّض به

تقارن قاعدة مواءمة تقييدات الاسم المفوّض به من حيث التساوي قيمة معروضة بقيمة نعت من النمط **شهادة النعت**.

```
delegatedNameConstraintsMatch MATCHING-RULE  ::= {
    SYNTAX          NameConstraintsSyntax
    ID              id-mr-delegatedNameConstraintsMatch}
```

وترجع هذه القاعدة القيمة "**صائب**"، إذا كانت القيمة المخزونة تحتوي على التوسع **تقييدات اسم النعت (attributeNameConstraints)**، وكانت المكونات الموجودة في القيمة المعروضة تتوافق مع المكونات الموجودة في القيمة المخزونة.

3.2.5.15 توسع سياسات الشهادة المقبولة

يستعمل حقل سياسات الشهادة المقبولة، في التفويض مع شهادات النعت، للتحكم في سياسات الشهادة المقبولة التي كان يجب أن تصدر بموجبها شهادات المفتاح العمومي للحاملين التالين في مسيرة تفويض. وتعداد سلطة النعت لمجموعة من السياسات في هذا الحقل، يساعدها على أن تتطلب من المصدرين التالين في مسيرة التفويض ألا يفوّضوا الامتيازات الموجودة إلا لحاملي شهادات مفتاح عمومي صادرة بموجب واحدة من سياسات الشهادة المعددة أو أكثر من واحد والسياسات المعدّدة ها هنا ليست السياسات التي صدرت بموجبها شهادة النعت، ولكنها السياسات التي كان يجب أن تصدر بموجبها شهادات المفتاح العمومي المقبولة للحاملين التالين.

ويعرّف هذا الحقل كما يلي:

```
acceptableCertPolicies EXTENSION ::= {
    SYNTAX              AcceptableCertPoliciesSyntax
    IDENTIFIED BY       id-ce-acceptableCertPolicies }

AcceptableCertPoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId

CertPolicyId ::= OBJECT IDENTIFIER
```

لا يمكن أن يوجد هذا التوسع إلا في شهادات نعت صادرة عن سلطات نعت، بما فيها مصادر السلطة إلى سلطات نعت أخرى. ويجب ألا يوجد هذا التوسع في شهادات نعت لكيانات نهائية أو في أي شهادة مفتاح عمومي. وفي حالة التفويض الذي يستخدم شهادات المفتاح العمومي، توفر المكوّنة **سياسات الشهادة (certificatePolicies)** وغيرها من التوسعات ذات الصلة، نفس الوظائفية.

ويجب أن يوسم هذا التوسع بالحرج، إذا وجد.

وإذا كان هذا التوسع موجوداً وكان المتحقق من الامتياز يفهمه، يجب على المتحقق أن يتأكد من أن جميع مؤكدي الامتيازات الواردين فيما بعد في مسيرة التفويض يتم استيقافهم بشهادة مفتاح عمومي بموجب واحدة من سياسات الشهادة المعددة أو أكثر من واحدة.

وعندما يكون هذا التوسع موجوداً، ولكن المتحقق من الامتياز لا يفهمه، يجب رفض الشهادة.

1.3.2.5.15 مواءمة سياسات الشهادة المقبولة

تقارن قاعدة مواءمة سياسات الشهادة المقبولة من حيث التساوي قيمة معروضة بقيمة نعت من النمط **شهادة النعت**.

```
acceptableCertPoliciesMatch MATCHING-RULE  ::= {
    SYNTAX          AcceptableCertPoliciesSyntax
    ID              id-mr-acceptableCertPoliciesMatch }
```

وترجع هذه القاعدة القيمة "**صائب**" إذا كانت القيمة المخزونة تحتوي على التوسع **سياسات الشهادة المقبولة**، وكانت المكوّنات الموجودة في القيمة المعروضة تتوافق مع المكوّنات المقابلة الموجودة في القيمة المخزونة.

4.2.5.15 توسع معرف الهوية لنعت السلطة

يجب أن يكون لدى سلطة النعت التي تفوّض الامتيازات في عملية تفويض الامتيازات، نفس الامتياز على الأقل، ومعه الترخيص بتفويض نفس الامتياز. يمكن لسلطة نعت تقوم بتفويض الامتياز إلى سلطة نعت أخرى أو إلى كيان نهائي، أن تضع هذا التوسع في شهادة سلطة النعت أو في شهادة كيان نهائي تصدرها هي. ويشكل التوسع مؤشراً إلى الخلف يدل على الشهادة التي كان مُصْدر الشهادة التي تحتوي على التوسع، قد أسند إليه فيها الامتياز المقابل. ويمكن لمتحقق من الامتياز أن يستعمل التوسع ليتأكد من أن سلطة النعت المُصْدرة، لديها ما يكفي من الامتياز لكي يكون تفويضه ممكناً إلى حامل الشهادة التي تحتوي على هذا التوسع.

ويعرف هذا الحقل كما يلي:

```
authorityAttributeIdentifier EXTENSION  ::=
    {
    SYNTAX              AuthorityAttributeIdentifierSyntax
    IDENTIFIED BY       { id-ce-authorityAttributeIdentifier }
    }
AuthorityAttributeIdentifierSyntax   ::=      SEQUENCE SIZE (1..MAX) OF AuthAttId
AuthAttId      ::=     IssuerSerial
```

والشهادة التي تحتوي على هذا التوسع يمكنها أن تتضمن تفويضاً بعدة امتيازات إلى حامل الشهادة. وإذا كان إسناد هذه الامتيازات إلى سلطة النعت التي أصدرت هذه الشهادة، كان قد جرى في أكثر من شهادة واحدة، يمكن لهذا التوسع أن يتضمن أكثر من مؤشر.

ويمكن أن يوجد هذا التوسع في شهادة نعت أو في شهادات مفتاح عمومي صادرة عن سلطة نعت إلى سلطات نعت غيرها أو على كيانات نهائية حاملة للامتيازات. ويجب ألا يوجد هذا التوسع في شهادات صادرة عن مَصْدر السلطة أو في شهادات مفتاح عمومي تحتوي على توسع معرف هوية مَصْدر السلطة .

ويكون هذا التوسع غير حرج دائماً.

1.4.2.5.15 مواءمة معرف هوية سلطة النعت

تقارن قاعدة مواءمة معرف هوية نعت السلطة من حيث التساوي قيمة معروضة بقيمة نعت من النمط **شهادة النعت**.

```
authAttIdMatch MATCHING-RULE ::= {
    SYNTAX          AuthorityAttirbuteIdentifierSyntax
    ID              id-mr-authAttIdMatch }
```

وترجع قاعدة المواءمة القيمة "**صائب**" إذا كانت القيمة المخزونة تحتوي على التوسع **معرف هوية نعت السلطة (authorityAttributeIdentifier)**، وكانت المكوّنات الموجودة في القيمة المعروضة تتوافق مع المكونات المقابلة الموجودة في القيمة المخزونة.

5.2.5.15 توسع المُصْدر غير المباشر

يمكن تفويض الامتياز في بعض البيئات بصورة غير مباشرة. وفي مثل هذه الحالة يطلب مانح التفويض أن يصدر المخدّم في خدمة التفويض (DS) شهادة تفوّض الامتياز نيابة عنه (باسمه) إلى كيان آخر ويستعمل حقل المُصْدر غير المباشر في شهادة نعت أو في شهادة مفتاح عمومي صادرة إلى المخدّم في خدمة التفويض من مَصْدر السلطة. ويعني وجود هذا التوسع أن سلطة النعت الصاحبة (المخدّم في خدمة التفويض) مرخص لها من مصدر السلطة هذا بأن تعمل كوسيط وتصدر شهادة تفوّض الامتياز نيابة عن مانحي تفويض آخرين.

```
indirectIssuer EXTENSION ::= {
    SYNTAX          NULL
    IDENTIFIED BY   id-ce-indirectIssuer }
```

ويكون هذا التوسع غير حرج دائماً.

وتقارن قاعدة مواءمة المصدر غير المباشر من حيث التساوي قيمة معروضة بقيمة نعت من النمط **شهادة النعت**.

```
indirectIssuerMatch MATCHING-RULE ::= {
    SYNTAX  NULL
    ID  id-mr-indirectIssuerMatch }
```

وترجع هذه القاعدة قيمة "**صائب**"، إذا كانت القيمة المخزونة تحتوي على التوسع **المصدر غير المباشر (indirectIssuer)** وإذا كانت القيمة الموجودة في القيمة المعروضة تتوافق مع القيمة المقابلة في القيمة المخزونة.

6.2.5.15 صادر نيابة عن (باسم ...)

يدرج المُصْدر غير المباشر (المخدّم في خدمة التفويض) هذا التوسع في شهادة نعت، وهذا التوسع يدل على سلطة النعت التي طلبت من المخدّم في خدمة التفويض أن يصدر شهادة النعت، ويسمح بإنشاء سلسلة التفويض وإقرار صلاحيتها.

```
issuedOnBehalfOf EXTENSION ::= {
    SYNTAX GeneralName
    ID id-ce-issuedOnBehalfOf }
```

والمكوّنة *الاسم العام (GeneralName)* هي اسم سلطة النعت التي طلبت من المصدر غير المباشر (المخدّم في خدمة التفويض) أن يصدر شهادة النعت هذه.

ويجب على مُصْدر شهادة النعت هذه، أن يكون قد منح من مَصْدر السلطة امتياز إصدار شهادات النعت نيابة عن سلطات نعت أخرى، عن طريق توسع المصدر غير المباشر في شهادة نعته.

ويمكن أن يكون هذا التوسع حرجاً أو غير حرج حسب اللزوم، من أجل ضمان إقرار الصلاحية لمسيرة التفويض.

16 إجراء معالجة مسيرة الامتياز

يقوم المتحقق من الامتياز بمعالجة مسيرة الامتياز. وتكون قواعد معالجة المسرة متماثلة نوعاً ما، من أجل شهادات النعت وشهادات المفتاح العمومي.

وبعض المكونات الأخرى لمعالجة المسيرة غير المتطرق إليها في هذا البند هي التحقق من توقيعات الشهادات وإقرار صلاحية فترات صلاحية الشهادات وغير ذلك.

والإجراء الأساسي المشروح في الفقرة 1.16 أدناه هو وحده المطلوب في مسيرات الامتياز التي تتألف من شهادة واحدة (أي أن الامتيازات قد أسندت مباشرة إلى مؤكد الامتياز من مَصْدر السلطة)، إلا إذا كان الامتياز مسنداً إلى دور. وفي هذه الحالة الأخيرة، ربما يكون على المتحقق من الامتياز أن يطلب الحصول على شهادة توصيف الدور التي أسندت الامتيازات المعيّنة إلى الدور كما هو مشروح في الفقرة 2.16 أدناه، إن كان المتحقق غير مشكّل مع الامتيازات المعيّنة للدور. وإذا قام مؤكد الامتياز بتفويض امتيازه بواسطة سلطة نعت وسيطة، يطلب أيضاً إجراء مسيرة التفويض الوارد في الفقرة 3.16. ولا يؤدى هذان الإجراءان بصورة متتابعة، فإجراء معالجة الدور وإجراء معالجة التفويض يؤديان، قبل أن يتحدد ما إذا كانت الامتيازات المؤكدة كافية أم لا، في سياق الاستعمال داخل الإجراء الأساسي.

1.16 إجراء المعالجة الأساسي

يجب التحقق من التوقيع الوارد في كل شهادة موجودة في المسيرة. والإجراءات المتعلقة بإقرار صلاحية التوقيعات وشهادات المفتاح العمومي غير مكررة في هذه الفقرة. ويجب على المتحقق من الامتياز أن يتحقق من هوية كل كيان موجود في المسيرة، مستخدماً إجراءات البند 10. ويلاحظ أن التحقق من التوقيع على شهادة نعت يستدعي بالضرورة التحقق من صلاحية شهادة المفتاح العمومي المحال إليها. وحيث تكون الامتيازات مسندة باستخدام شهادات النعت، يجب على إجراءات معالجة المسيرة أن تأخذ بالاعتبار، أثناء عملية تحديد الصلاحية النهائية لشهادة النعت لمؤكد الامتياز، بعض العناصر المنتمية إلى البنية التحتية PMI والبنية التحتية PKI. وبمجرد أن تتأكد الصلاحية، يمكن استعمال الامتيازات الواردة في هذه الشهادة، تبعاً لمقارنة تجري مع سياسة الامتياز ذات الصلة ومع غيرها من المعلومات المتصاحبة في السياق الذي تستعمل فيه الشهادة.

ويجب أن يحدد سياق الاستعمال إن كان حامل الامتياز ينوي فعلاً تأكيد الامتياز المحتوى، لاستعماله في السياق. ووجود سلسلة شهادات موثوقة نحو مَصْدر سلطة ليس كافياً بحد ذاته ليعتمد عليه في إجراء هذا التحديد. بل يجب أن تبين رغبة حامل الامتياز بكل وضوح في استعمال هذه الشهادة وأن يتم التحقق من ذلك. مع ذلك فإن آليات التأكد من أن مثل هذا التأكيد للامتياز قد أثبته حامل الامتياز إثباتاً وافياً، تقع خارج نطاق هذه المواصفة. ومثال على ذلك، يمكن التحقق من تأكيد الامتياز إذا قام حامل الامتياز بتوقيع إحالة إلى هذه الشهادة، يبين فيها رغبته في استعمال هذه الشهادة ضمن هذا السياق.

وفيما يخص كل شهادة نعت موجودة في المسيرة ولا تحتوي على التوسع **لا يوجد إبطال متيسر (noRevAvail)**، يجب على المتحقق من الامتياز أن يتأكد من أن هذه الشهادة لم يجر إبطالها.

ويجب على المتحقق من الامتياز أن يتأكد من أن الامتياز المؤكد هو صالح في الوقت المسمى "وقت التقييم"، الأمر الذي يمكن إجراؤه في *أي وقت*، أي في الوقت الحالي للتحقق أو في أي وقت سابق وفي سياق خدمة التحكم في النفاذ، يجري التحقق دائماً في الوقت الحاضر. ومع ذلك ففي سياق عدم الرفض يمكن أن يجري التحقق في وقت سابق أو في الوقت الحالي. وبعد إقرار صلاحية الشهادات، يجب على المتحقق من الامتياز أن يتأكد من أن وقت التقييم يقع داخل فترت الصلاحية لجميع

الشهادات المستعملة في المسيرة. ومع ذلك، إذا كانت أي واحدة من الشهادات الموجودة في المسيرة، تحتوي على التوسع **توصيف الوقت (timeSpecification)**، فإن التقييدات الموضوعة على أوقات تأكيد الامتياز يجب عليها أن تؤكد أيضاً أن تأكيد الامتياز صالح أيضاً في وقت التقييم.

إذا كان التوسع **المعلومات المستهدفة (targetingInformation)** موجوداً في شهادة تستعمل لتأكيد امتياز، يجب على المتحقق من الامتياز أن يتأكد من أن المخدّم أو الخدمة اللذين يتأكد منهما، واردان في قائمة المستهدفات.

وإذا كانت الشهادة هي شهادة إسناد دور، يكون إجراء المعالجة المشروح في الفقرة 2.16 لازماً للتأكد من أن الامتيازات المناسبة قد تم تعرّف هويتها. وإذا كان قد جرى تفويض الامتياز إلى كيان، بدلاً من أن يكون مسنداً مباشرة من مَصْدر السلطة الذي يثق به المتحقق من الامتياز، يكون إجراء المعالجة المشروح في الفقرة 3.16 لازماً للتأكد من أن التفويض قد جرى بطريقة سليمة.

ويجب على المتحقق من الامتياز أن يحدد أيضاً إن كانت الامتيازات الجارية تأكيدها هي كافية أم لا لسياق الاستعمال. وتضع سياسة الامتياز القواعد اللازمة للقيام بهذا التحديد، وتشمل توصيف أي متحولات بيئية ينبغي اعتبارها. وجميع الامتيازات المؤكدة، بما فيها الامتيازات الناتجة من إجراء الدور المشروح في الفقرة 2.16 ومن إجراء التفويض المشروح في الفقرة 3.16، وأي متحولات بيئية ذات صلة (أي الوقت من اليوم أو رصيد الحساب الجاري) تجري مقارنتها بسياسة الامتياز، لتحديد ما إذا كانت كافية أم لا لسياق الاستعمال. وإذا كان التوسع **سياسات الامتياز المقبولة (acceptablePrivilegePolicies)** موجوداً، لا يكون تأكيد الامتياز ناجحاً إلا إذا كانت سياسة الامتياز التي يستخدمها المتحقق من الامتياز للمقارنة هي واحدة من السياسات الموجودة في هذا التوسع.

وإذا نجح التحقق، تقدم إلى المتحقق من الامتياز جميع تبليغات المستعملين ذات الصلة.

2.16 إجراء معالجة الدور

إذا كانت الشهادة المؤكد عليها هي شهادة إسناد الدور، يجب على المتحقق من الامتياز أن يحصل على الامتيازات الخاصة المسندة إلى الدور. ويوجد اسم الدور المسند إلى مؤكد الامتياز في النعت **الدور (role)** من الشهادة. وإذا كانت تشكيلة المتحقق من الامتياز لا تحتوي فعلاً امتيازات الدور المسمّى، فقد يحتاج المتحقق أن يحدد موقع شهادة توصيف الدور التي تسند الامتيازات إلى هذا الدور. ويمكن استخدام المعلومات الواردة في نعت **الدور** وفي التوسع **معرف هوية شهادة توصيف الدور (roleSpecCertIdentifier)**.

وتكون الامتيازات المسندة إلى الدور مسندةً ضمناً إلى مؤكد الامتياز، وتكون بالتالي واردة بين الامتيازات المؤكدة التي تجري مقارنتها بسياسة الامتياز في الإجراء الأساسي الوارد في الفقرة 1.16 لتحديد ما إذا الامتيازات المؤكدة كافية أم لا لسياق الاستعمال.

3.16 إجراء معالجة التفويض

إذا كانت الامتيازات المؤكدة قد جرى تفويضها إلى مؤكد الامتياز عن طريق سلطة نعت وسيطة، يجب على المتحقق من الامتياز أن يتأكد من أن المسيرة هي مسيرة تفويض صالحة، عن طريق التأكد من:

- أن كل سلطة نعت تصدر شهادة في مسيرة التفويض هي سلطة مرخص لها بفعل ذلك؛
- أن كل شهادة موجودة في مسيرة التفويض هي شهادة صالحة بالنسبة إلى المسيرة وتقييدات الاسم المفروضة عليها؛
- أن كل كيان موجود في مسيرة التفويض هو كيان مُسْتيقن بشهادة مفتاح عمومي صالحة من حيث أي تقييدات مفروضة في السياسة؛
- أنه لا توجد أي سلطة نعت تفوض امتيازاً أكبر من الامتياز التي تحمله.

وقبل أن يبدأ المتحقق من الامتياز بإقرار صلاحية مسيرة التفويض، يكون عليه أن يحصل على التالي، وأي بند مما يلي يمكن تأمينه عن طريق مؤكد الامتياز، أو يمكن أن يحصل عليه المتحقق من الامتياز من أي مصدر آخر، كالدليل مثلاً. كما يمكن تأمين نعوت الخدمة إلى المتحقق من الامتياز في وثيقة مبوّبة أو بوسائل أخرى.

- إقامة الثقة في مفتاح التحقق العمومي المستعمل لإقرار صلاحية توقيع مَصْدر السلطة الموثوق. ويمكن إقامة هذه الثقة إما بوسائل تقع خارج النطاق وإما بشهادة مفتاح عمومي صادرة إلى مَصْدر سلطة عن سلطة إصدار الشهادة، يكون المتحقق من الامتياز قد وضع الثقة فيها سلفاً. وربما تحتوي مثل هذه الشهادة على التوسع **معرف هوية مَصْدر السلطة (sOAIdentifier)**.
- امتياز مؤكد الامتياز، المشفر في شهادة نعته أو في توسع نعوت الدليل للصاحب في شهادة المفتاح العمومي.
- مسيرة تفويض الشهادات من مؤكد الامتياز إلى مَصْدر السلطة الموثوق.
- القاعدة التراتبية للامتياز الجاري تأكيده. ويمكن الحصول عليها من واصف النعت الصادر عن مَصْدر السلطة المسؤول عن النعت المدروس، أو يمكن الحصول عليها عبر وسائل تقع خارج النطاق.
- سياسة الأمتياز، ويمكن الحصول عليها من الدليل أو من بعض الوسائل الواقعة خارج النطاق.
- المتحولات البيئية التي تَشمل التاريخ أو الوقت الحالي، ورصيد الحساب الجاري وغيرها.

يجب أن يكون هناك تنفيذ مكافئ وظيفياً للسلوك الخارجي الناتج عن هذا الإجراء، ومع ذلك لا يوجد تقييس للخوارزمية التي يستعملها تطبيق معين لاستنتاج المُخْرجات الصحيحة من مُدْخلات معّينة.

وفي الحالة التي يكون فيه شهادات النعت صادرة عن مُصْدر غير مباشرة (خدمة التفويض)، ينبغي للطرف الواثق أن يقرّ تماماً صلاحية سلسلة التفويض كما يلي:

i) يبدأ الطرف الواثق بشهادة النعت للكيان النهائي، ويستخرج اسم المُصْدر واسم *الصادر نيابة عن (issuedOnBehalfOf)*.

ii) يستخرج الطرف الواثق نعت المُصْدر، ويقرّ بأن المُصْدر هو مُصْدر غير مباشر لمُصْدر السلطة (أي فيه التوسع *المصدر غير المباشر*).

iii) يستخرج الطرف الواثق شهادة النعت لسلطة نعت *الصادرة نيابة عن*، ويقرّ بأن سلطة النعت عندها مجموعة فائقة من نعوت الامتياز صادرة للكيان النهائي.

ويعود الطرف الواثق إلى المرحلة ii) مستعملاً شهادة النعت لسلطة النعت، ويصعد السلسلة بعدئذ إلى أن يصل إلى شهادة النعت لسلطة النعت الصادرة عن مَصْدر السلطة.

1.3.16 التحقق من تكاملية معطيات القاعدة التراتبية

تتصاحب القاعدة التراتبية مع الامتياز الجاري تفويضه. ولا يوجد تقييس لا لقواعد التركيب ولا للطريقة اللازمة للحصول على القاعدة التراتبية. ومع ذلك يمكن التحقق من تكاملية القاعدة التراتبية المستخرجة. ويمكن لشهادة واصف النعت الصادرة عن مَصْدر السلطة المسؤول عن النعت الجاري تفويضه، أن تحتوي على **فرم** للقاعدة التراتبية. ويستطيع المتحقق من الامتياز أن ينسخ دالّة **الفرم** من نسخة القاعدة التراتبية المستخرجة، وأن يقارن بين عمليتي الفرم. فإذا كانتا متطابقتين، يكون المتحقق من الامتياز قد حصل على القاعدة التراتبية الصحيحة.

2.3.16 إقامة مسيرة تفويض صالحة

يجب على المتحقق من الامتياز أن يجد مسيرة التفويض، وأن يحصل على شهادات لكل كيان موجود في المسيرة. وتمتد مسيرة التفويض من مؤكد الامتياز المباشر إلى مَصْدر السلطة. ويجب أن تحتوي كل شهادة وسيطة موجودة في مسيرة التفويض على التوسع **تقييدات النعت الأساسية (basicAttConstraints)** مع مكوّنة السلطة موضوعة على "**صائب**". ويجب أن يكون مُصْدر كل شهادة هو نفس الحامل أو الصاحب لكل شهادة مجاورة في مسيرة التفويض. ويستعمل التوسع **معرف هوية نعت**

السلطة (authorityAttributeIdentifier) لتحديد موقع الشهادة المناسبة للكيان المجاور في مسيرة التفويض. ويكون عدد الشهادات في المسيرة، من كل كيان إلى مؤكد الامتياز المباشر (ضمناً)، لا يزيد بأكثر من 2 على قيمة المكوّنة **تقييد طول المسيرة** تحدّ من عدد الشهادات الوسطية الموجودة بين نقطتين طرفيتين (أي بين الشهادة التي تحتوي على التقييد وشهادة الكيان النهائية). بحيث يكون الطول الأعظم يساوي قيمة هذا التقييد مضافاً إليها الشهادتان الموجودتان في الطرفين.

وإذا كان التوسع **تقييدات الاسم المفوض به (delegatedNameConstraints)** موجوداً في أي واحدة من شهادات مسيرة التفويض، تعالج التقييدات بنفس الطريقة التي يعالج بها التوسع **تقييدات الاسم** في إجراء معالجة مسيرة إصدار الشهادة الواردة في البند 10.

وإذا كان التوسع **سياسات الشهادة المقبولة** موجوداً في أي واحدة من شهادات مسيرة التفويض يجب على المتحقق من الامتياز أن يتأكد من أن استيقان كل كيان تالٍ في مسيرة التفويض قد جرى بشهادة مفتاح عمومي تحتوي على الأقل على واحدة من السياسات المقبولة.

3.3.16 التحقق من تفويض الامتياز

لا يستطيع أي مانح تفويض أن يفوّض امتيازاً أكبر من الامتياز الذي يمتلكه هو. وتقدم القاعدة التراتبية الواردة في واصف النعت مجموعة القواعد التي تحدد متى تكون قيمة معينة "أقل من" قيمة أخرى هي قيمة النعت الجاري تفويضه.

يجب على المتحقق من الامتياز أن يتأكد، بخصوص كل شهادة في مسرة التفويض، بما فيها شهادة المتحقق المباشر من الامتياز، من أن مانح التفويض مرخص له بتفويض الامتياز الذي يمتلكه، وأن قيمة الامتياز الذي جرى تفويضه ليست أكبر من قيمة الامتياز الذي يمتلكه هذا المانح.

ويجب على المتحقق من الامتياز أن يقوم، بخصوص كل واحدة من هذه الشهادات، بمقارنة الامتياز الجاري تفويضه بالامتياز الذي يمتلكه مانح التفويض، طبقاً للقاعدة التراتبية الخاصة بالامتياز. ويمكن الحصول على الامتياز الذي يمتلكه مانح التفويض، من الشهادة المجاورة في مسيرة التفويض كما هو مشروح في الفقرة 2.16. وتتم مقارنة الامتيازين استناداً إلى القاعدة التراتبية المشروحة في الفقرة 1.3.16.

4.3.16 تحديد النجاح أو الفشل

بافتراض أن مسيرة تفويض صالحة قد أقيمت، فإن امتيازات مؤكد الامتياز المباشر تقدم باعتبارها مُدْخلات لمقارنتها بسياسة الامتياز كما هو مناقش في الفقرة 1.16، لتحديد ما إذا مؤكد الامتياز المباشر يمتلك امتيازاً كافياً أم لا لسياق الاستعمال.

17 تخطيط الدليل للبنية التحتية لإدارة الامتياز (PMI)

يحدد هذا البند عناصر تخطيطية الدليل التي تستعمل لتمثيل معلومات البنية PMI في الدليل. وهو يشتمل على توصيف أصناف الموضوعات والنعوت وقواعد مواءمة قيم النعوت ذات الصلة.

1.17 أصناف الموضوعات في الدليل للبنية PMI

يتضمن هذا البند الفرعي تعريف أصناف الموضوعات المستعملة لتمثيل موضوعات البنية PMI في الدليل.

1.1.17 صنف الموضوعات "مستعمل البنية التحتية PMI"

صنف الموضوعات "مستعمل البنية PMI" يعرّف مداخل موضوعات يمكن أن تكون حاملة شهادات نعت.

```
pmiUser OBJECT-CLASS ::= {
-- a PMI user (i.e., a "holder") -- مستعمل PMI (أي "حامل")
  SUBCLASS OF    {top}
  KIND           auxiliary
  MAY CONTAIN    {attributeCertificateAttribute}
  ID             id-oc-pmiUser }
```

2.1.17 صنف الموضوعات "سلطة النعت في البنية PMI"

صنف الموضوعات "سلطة النعت في البنية PMI" يستعمل في تعريف مداخل الموضوعات التي تعمل كسلطات نعت.

```
pmiAA OBJECT-CLASS ::= {
-- a PMI AA
  SUBCLASS OF    {top}
  KIND           auxiliary
  MAY CONTAIN    {aACertificate |
                 attributeCertificateRevocationList |
                 attributeAuthorityRevocationList}
  ID             id-oc-pmiAA }
```

3.1.17 صنف الموضوعات "مَصْدر السلطة في البنية PMI"

صنف الموضوعات "مَصْدر السلطة في البنية PMI" يستعمل في تعريف مداخل الموضوعات التي تعمل كمصادر سلطة. ويلاحظ أن الموضوع الذي يرخص له أن يعمل كمَصْدر سلطة بإصدار شهادة مفتاح عمومي تحتوي على التوسع **معرف هوية مَصْدر السلطة**، يكون هناك مدخل للدليل يمثل هذا الموضوع ويحتوي أيضاً على صنف الموضوعات **pkiCA**.

```
pmiSOA OBJECT-CLASS ::= { -- a PMI Source of Authority
  SUBCLASS OF    {top}          -- مَصْدر سلطة في البنية PMI
  KIND           auxiliary
  MAY CONTAIN    {attributeCertificateRevocationList |
                 attributeAuthorityRevocationList |
                 attributeDescriptorCertificate}
  ID             id-oc-pmiSOA }
```

4.1.17 صنف الموضوعات "شهادة نعت لنقطة توزيع القائمة CRL"

صنف الموضوعات "شهادة نعت لنقطة توزيع القائمة CRL" يستعمل في تعريف مداخل الموضوعات التي تحتوي على شهادة نعت و/أو مقاطع من قائمة إبطال سلطات نعت. ومن المزمع أن يستعمل هذا الصنف المساعد بالاشتراك مع صنف الموضوعات المبنين **نقطة توزيع القائمة CRL** عند المداخل البدائية. ولما كان النعتان **قائمة إبطال الشهادات** و**قائمة إبطال السلطات** اختياريين في هذا الصنف، يمكن إحداث مداخل تحتوي مثلاً فقط على قائمة إبطال سلطات النعت أو على مداخل تحتوي على قوائم إبطال من أنماط متعددة تتوقف على المتطلبات.

```
attCertCRLDistributionPt     OBJECT-CLASS ::= {
  SUBCLASS OF    {top}
  KIND           auxiliary
  MAY CONTAIN    { attributeCertificateRevocationList |
                 attributeAuthorityRevocationList }
  ID             id-oc-attCertCRLDistributionPts }
```

5.1.17 صنف الموضوعات "مسيرة التفويض في البنية PMI"

صنف الموضوعات "مسيرة التفويض في البنية PMI" يستعمل لتعريف مداخل الموضوعات التي يمكنها أن تحتوي على مسيرات تفويض. ويستعمل عادة بالاشتراك مع مداخل صنف الموضوعات المبنين **pmiAA**.

```
pmiDelegationPath      OBJECT-CLASS   ::= {
   SUBCLASS OF         {top}
   KIND                auxiliary
   MAY CONTAIN         { delegationPath }
   ID                  id-oc-pmiDelegationPath }
```

6.1.17 صنف الموضوعات "سياسة الامتياز"

صنف الموضوعات "سياسة الامتياز" يستعمل لتعريف مداخل الموضوعات التي تحتوي معلومات عن سياسة الامتياز.

```
privilegePolicy      OBJECT-CLASS   ::= {
   SUBCLASS OF       {top}
   KIND              auxiliary
   MAY CONTAIN       {privPolicy }
   ID                id-oc-privilegePolicy }
```

7.1.17 صنف الموضوعات "سياسة الامتياز المحميّة"

صنف الموضوعات "سياسة الامتياز المحميّة" يستعمل لتعريف مداخل الموضوعات التي تحتوي على سياسات امتياز محميّة داخل شهادات النعت.

```
protectedPrivilegePolicy          OBJECT-CLASS   ::= {
   SUBCLASS OF       {top}
   KIND              auxiliary
   MAY CONTAIN       {protPrivPolicy }
   ID                id-oc-protectedPrivilegePolicy }
```

2.17 النعوت الدليلية للبنية التحتية PMI

يتضمن هذا البند الفرعي تعريف النعوت الدليلية التي تستعمل لتخزين معطيات البنية PMI في الدليل.

1.2.17 نعت "شهادة النعت"

يحتوي النعت التالي على شهادات النعت الصادرة لحامل معين وهي مخزونة في مدخل الدليل الخاص بهذا الحامل.

```
attributeCertificateAttribute ATTRIBUTE  ::= {
   WITH SYNTAX                    AttributeCertificate
   EQUALITY MATCHING RULE         attributeCertificateExactMatch
   ID                             id-at-attributeCertificate }
```

2.2.17 نعت "شهادة سلطة النعت"

يحتوي النعت التالي على شهادات النعت الصادرة لسلطة نعت وهي مخزونة في مدخل الدليل الخاص بسلطة النعت الحامل.

```
aACertificate        ATTRIBUTE   ::=  {
   WITH SYNTAX                    AttributeCertificate
   EQUALITY MATCHING RULE         attributeCertificateExactMatch
   ID                             id-at-aACertificate }
```

3.2.17 نعت "شهادة واصف النعت"

يحتوي النعت التالي على شهادات النعت الصادرة عن مصدر السلطة التي تحتوي على التوسع **واصف النعت** وتحتوي شهادات النعت هذه على مواصفة قواعد التركيب الصالحة والقواعد التراتبية الخاصة بنعوت الامتياز وهي مخزونة في مدخل الدليل الخاص بمَصْدر السلطة المُصْدر.

```
attributeDescriptorCertificate      ATTRIBUTE  ::= {
   WITH SYNTAX                    AttributeCertificate
   EQUALITY MATCHING RULE         attributeCertificateExactMatch
   ID                             id-at-attributeDescriptorCertificate }
```

4.2.17 نعت "قائمة إبطال شهادات النعت"

يحتوي النعت التالي على قائمة من شهادات النعت المبطلة. ويمكن تخزين هذه القوائم في مدخل الدليل الخاص بسلطة الإصدار أو في مدخل آخر في الدليل (مثل نقطة التوزيع).

```
attributeCertificateRevocationList     ATTRIBUTE ::= {
   WITH SYNTAX                    CertificateList
   EQUALITY MATCHING RULE         certificateListExactMatch
   ID                             id-at-attributeCertificateRevocationList}
```

5.2.17 نعت "قائمة إبطال شهادات سلطة النعت"

يحتوي النعت التالي على قائمة من شهادات النعت المبطلة الصادرة إلى سلطات النعت. ويمكن تخزين هذه القائمة في مدخل الدليل الخاص بسلطة الإصدار أو في مدخل آخر في الدليل (مثل نقطة التوزيع).

```
attributeAuthorityRevocationList    ATTRIBUTE  ::= {
    WITH SYNTAX                     CertificateList
    EQUALITY MATCHING RULE          certificateListExactMatch
    ID                              id-at-attributeAuthorityRevocationList }
```

6.2.17 نعت "مسيرة التفويض"

يحتوي نعت مسيرة التفويض على مسيرات تفويض، تتكون كل منها من تتابع من شهادات النعت.

```
delegationPath      ATTRIBUTE  ::= {
    WITH SYNTAX                AttCertPath
    ID                         id-at-delegationPath }

AttCertPath     ::=  SEQUENCE OF AttributeCertificate
```

يمكن تخزين هذا النعت في مدخل الدليل الخاص بسلطة النعت، ويمكن أن يحتوي على مسيرات تفويض تمتد من سلطة النعت هذه إلى سلطات نعت أخرى. واستعمال هذا النعت يساعد على تسريع استخراج شهادات نعت مفوّض بها، تكوّن مسيرات التفويض الأكثر استعمالاً. وهكذا، لا توجد متطلبات خاصة لاستعمال هذا النعت، ومجموعة القيم التي تختزن في النعت قد لا تكون تمثل المجموعة الكاملة من مسيرات التفويض لأي سلطة نعت معنية.

7.2.17 نعت "سياسة الامتياز"

يحتوي نعت سياسة الامتياز على المعلومات الخاصة بسياسات الامتياز.

```
privPolicy ATTRIBUTE  ::= {
    WITH SYNTAX       PolicySyntax
    ID                id-at-privPolicy }
```

تحتوي المكوّنة **معرّف هوية السياسة** على معرّف هوية الهدف المسجل لسياسة امتياز معينة.

وتحتوي المكوّنة **المحتوى**، إن وجدت، على النص الكامل لسياسة الامتياز.

وإذا كانت المكوّنة **المؤشر** موجودة، فإن مكوّنة **الاسم** تحيل إلى موقع أو إلى أكثر من موقع، يمكن أن توجد فيه نسخة من سياسة الامتياز. وإذا كانت المكوّنة **الفَرْم** موجودة، فهي تحتوي على **فَرْم** لمحتوى سياسة الامتياز التي يجب العثور عليها في موقع محال إليه. ويستعمل هذا الفرم للقيام بتحقيق كامل من الوثيقة المحال إليها.

8.2.17 نعت "سياسة الامتياز المحميّة"

يحتوي نعت سياسة الامتياز المحميّة سياسات للامتياز تكون محميّة داخل شهادة النعت.

```
protPrivPolicy      ATTRIBUTE  ::= {
WITH SYNTAX                    AttributeCertificate
EQUALITY MATCHING RULE         attributeCertificateExactMatch
ID                             id-at-protPrivPolicy }
```

ويلاحظ أن شهادات النعت الموجودة في النعت **سياسة الامتياز المحمية (protPrivPolicy)** بخلاف شهادات النعت العادية، تحتوي على سياسات امتياز وليس على امتيازات. وتكون المكونتان المُصْدر والحامل في شهادات النعت هذه تعرفان بهوية نفس الكيان. والنعت الموجود في شهادة النعت الموجودة داخل النعت **سياسة الامتياز المحميّة** يكون إما نعت **سياسة الامتياز** وإما نعت **سياسة الامتياز في اللغة XML (اللغة التأشيرية التوسعية)**.

9.2.17 نعت "سياسة الامتياز المحميّة"

يحتوي نعت سياسة الامتياز المحميّة في اللغة XML على معلومات سياسة الامتياز المشفرة في اللغة XML.

```
xmlPrivPolicy      ATTRIBUTE   ::= {
WITH SYNTAX        UTF8String -- contains XML-encoded privilege policy information
ID                 id-at-xMLPprotPrivPolicy }
```

3.17 قواعد المواءمة في الدليل للبنية التحتية لإدارة الامتياز (PMI)

يعرف هذا البند الفرعي قواعد المواءمة لنعوت الدليل الخاصة بالبنية التحتية (PMI)

1.3.17 مواءمة مضبوطة لشهادة النعت

تقارن قاعدة المواءمة المضبوطة لشهادة النعت من حيث التساوي قيمة معروضة بقيمة نعت من النمط **شهادة النعت (AttributeCertificate)**.

```
attributeCertificateExactMatch MATCHING-RULE  ::= {
   SYNTAX          AttributeCertificateExactAssertion
   ID              id-mr-attributeCertificateExactMatch }

AttributeCertificateExactAssertion     ::=  SEQUENCE {
   serialNumber              CertificateSerialNumber,
   issuer                    AttCertIssuer }
```

وترجع هذه القاعدة القيمة "**صائب**"، إذا كانت المكوّنات الموجودة في قيمة النعت تتوافق مع المكوّنات الموجودة في القيمة المعروضة.

2.3.17 مواءمة شهادة النعت

تقارن قاعدة المواءمة شهادة النعت قيمة معروضة بقيمة نعت من النمط **شهادة النعت**، وتتيح قاعدة المواءمة هذه البحث عن مواءمة أكثر تعقيداً من قاعدة المواءمة المضبوطة للشهادة.

```
attributeCertificateMatch  MATCHING-RULE  ::= {
   SYNTAX          AttributeCertificateAssertion
   ID              id-mr-attributeCertificateMatch  }

AttributeCertificateAssertion  ::=  SEQUENCE  {
   holder          [0]  CHOICE {
                           baseCertificateID      [0]  IssuerSerial,
                           holdertName            [1]  GeneralNames} OPTIONAL,
   issuer          [1]  GeneralNames OPTIONAL,
   attCertValidity [2]  GeneralizedTime OPTIONAL,
   attType         [3]  SET OF AttributeType OPTIONAL}
-- At least one component of the sequence shall be present
                        -- يجب أن تكون مكونة واحدة على الأقل موجودة
```

وترجع هذه القاعدة القيمة "**صائب**" إذا كانت جميع المكوّنات الموجودة في القيمة المعروضة توائم المكوّنات المقابلة من قيمة النعت، على النحو التالي:

- المكوّنة **معرف هوية الشهادة الأساسي** (baseCertificateID) موائمة، إذا كانت قيمتها تساوي قيمة المكوّنة **تسلسل المُصْدر** (IssuerSerial) في قيمة النعت المخزونة؛
- المكوّنة **اسم الحامل (holderName)** موائمة، إذا كانت قيمة النعت المخزنة تحتوي على مكوّنة الاسم من نفس نمط الاسم المبين في القيمة المعروضة؛
- المكوّنة **المُصْدر (issuer)** موائمة، إذا كانت قيمة النعت المخزونة تحتوي على مكوّنة الاسم من نفس نمط الاسم المبين في القيمة المعروضة؛

- المكوّنة **صلاحية شهادة النعت (attCertValidity)** موائمة، إذا كانت قيمتها تقع ضمن فترة الصلاحية المحددة في قيمة النعت المخزونة؛
- يكون لكل مكوّنة **نمط النعت (attType)** موجودة في القيمة المعروضة، نعت لهذا النمط موجودة في مكوّنة **النعوت** من القيمة المخزونة.

3.3.17 مواءمة المُصْدر/الحامل

تقارن قاعدة مواءمة المُصْدر/الحامل من حيث التساوي قيمة معروضة لمكونتي الحامل و/أو المُصْدر بقيمة نعت من النمط **شهادة النعت**.

```
holderIssuerMatch MATCHING-RULE ::= {
    SYNTAX          HolderIssuerAssertion
    ID              id-mr-holderIssuerMatch }

HolderIssuerAssertion ::= SEQUENCE {
    holder          [0]     Holder          OPTIONAL,
    issuer          [1]     AttCertIssuer   OPTIONAL }
```

وترجع هذه القاعدة القيمة "صائب"، إذا كانت جميع المكوّنات الموجودة في القيمة المعروضة تتوافق مع المكوّنات المقابلة الموجودة في قيمة النعت.

4.3.17 مواءمة مسيرة التفويض

تقارن قاعدة **مواءمة مسيرة التفويض (delegationPathMatch)** من حيث التساوي قيمة معروضة بقيمة نعت من النمط **مسيرة التفويض (delegationPath)**. ويمكن للمتحقق من الامتياز أن يستعمل قاعدة المواءمة هذه، لكي ينتقي مسيرة تبدأ بشهادة صادرة عن مَصْدر سلطتها، وتنتهي بشهادة صادرة إلى سلطة النعت التي أصدرت شهادة الحامل للكيان النهائي الجاري إقرار صلاحيتها.

```
delegationPathMatch MATCHING-RULE ::= {
    SYNTAX          DelMatchSyntax
    ID              id-mr-delegationPathMatch }

DelMatchSyntax  ::= SEQUENCE {
    firstIssuer     AttCertIssuer,
    lastHolder      Holder }
```

وترجع هذه القاعدة **القيمة "صائب"**، إذا كانت القيمة المعروضة في المكوّنة **المُصْدر الأول (firstIssuer)** توائم العناصر المقابلة في حقل المُصْدر من أول شهادة واردة في **التتابع (SEQUENCE)** من القيمة المخزنة، وكانت القيمة المعروضة في المكوّنة **الحامل الأخير (lastHolder)** توائم العناصر المقابلة في حقل الحامل من آخر شهادة واردة في **التتابع** من القيمة المخزنة. وترجع هذه القاعدة القيمة **"خاطئ"** إذا فشلت مقارنة التواؤم.

القسم الرابع – استعمال الدليل لإطاري شهادة المفتاح العمومي وشهادة النعت

يستخدم الدليل إطار شهادة المفتاح العمومي كأساس لعدد من الخدمات الأمنية تشمل الاستيقان المعمّق وحماية عمليات الدليل وكذلك حماية المعطيات المخزونة. ويستخدم الدليل إطار شهادة النعت كأساس لتخطيطة التحكم في النفاذ المبنيّة على قواعد. وتعرّف هنا العلاقة بين عناصر إطاري شهادة المفتاح العمومي وشهادة النعت وبين مختلف الخدمات الأمنية في الدليل. والخدمات الأمنية الخاصة التي يقدمها الدليل محددة بكاملها في المجموعة الكاملة من مواصفات الدليل.

18 الاستيقان الدليلي

يتحمل الدليل استيقان المستعملين الذي ينفذون إليه عبر وكلاء مستعملي الدليل (DUA)، كما يتحمل استيقان وكلاء أنظمة الدليل (DSA) للمستعملين وللأنظمة الأخرى DSA. ويمكن استخدام الاستيقان البسيط أو الاستيقان المعمّق حسب طبيعة البيئة. وتشرح الفقرات التالية الإجراءات الواجب اتّباعها للاستيقان البسيط والاستيقان المعمّق في الدليل.

1.18 إجراءات الاستيقان البسيط

أعدّ الاستيقان البسيط لتقديم ترخيص محلي مبني على الاسم المميز للمستعمل، وكلمة سر (اختيارية) متفق عليها بين الجانبين، وعلى تفاهم ثنائي الجانب بشأن معاني استخدام كلمة السر هذه والتعامل بها في ميدان معين. وأعدّ الاستيقان البسيط لكي يستخدم بصورة أساسية للاستخدام المحلي فقط أي لاستيقان كيانات أنداد بين وكيل مستعمل الدليل (DUA) ووكيل نظام الدليل (DSA) أو بين وكيل نظام الدليل (DSA) ووكيل آخر لنظام الدليل (DSA). ويمكن إجراء الاستيقان البسيط بوسائل عدة:

أ) تحويل الاسم المميز للمستعمل وكلمة السر (اختيارياً) بلغة واضحة (غير محميّة) إلى المَقْصد لأغراض التقييم؛

ب) تحويل الاسم المميز للمستعمل وكلمة السر ورقم عشوائي و/أو ختم التاريخ، على أن تتم حماية المجموعة بدالّة وحيدة الاتجاه؛

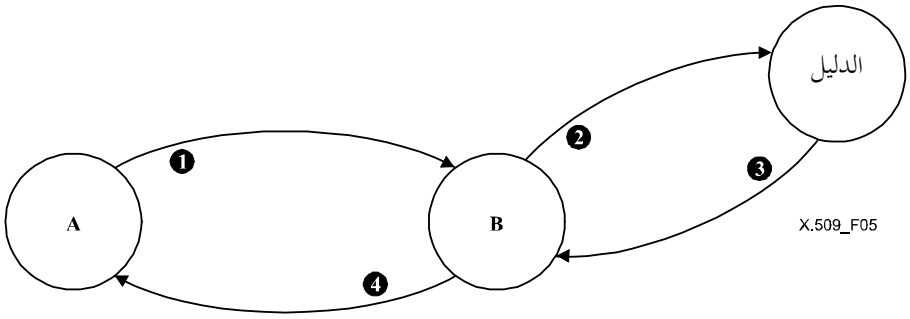
ج) تحويل المعلومات المحميّة المشروحة في الفقرة ب) مع رقم عشوائي و/أو ختم التاريخ، على أن تتم حماية المجموعة بدالّة وحيدة الاتجاه.

ملاحظة 1 – لا يوجد أي قيد يفرض أن تكون الدوالّ وحيدة الاتجاه مختلفة.

ملاحظة 2 – يمكن أن تتم الإشارة إلى إجراءات حماية كلمات السر في توسع خاص بالوثيقة.

يجب أن يتوفر حدّ أدنى من الأمان لاتقاء النفاذ غير المرخص به، عندما لا تكون كلمات السر محميّة. يجب ألا يعتبر هذا الأسلوب كأساس لخدمات موثوقة. وحماية الاسم المميز للمستعمل وكلمة السر كذلك تشكل سوية أمنية عالية. والخوارزميات التي تستعمل للحماية تكون بصورة عامة دوالّ وحيدة الاتجاه (غير عكوسة)، غير مجفّرة، سهلة التنفيذ كثيراً.

ويبين الشكل 5 الإجراء العام للقيام باستيقان بسيط.



الشكل 5 – إجراء استيقان بسيط غير محمي

والمراحل هي التالية:

1) مستعمل A مُصْدر، يرسل اسمه المميز وكلمة سرّه إلى مستعمل B مَقْصَد؛

2) يرسل المستعمل B الاسم المميز للمستعمل A وكلمة سره المزعومين إلى الدليل، لكي يتحقق من كلمة السر بمقارنتها بالكلمة المحفوظة في النعت **كلمة سر المستعمل (UserPassword)** من مدخل الدليل الخاص بالمستعمل A (باستخدام عملية المقارنة في الدليل)؛

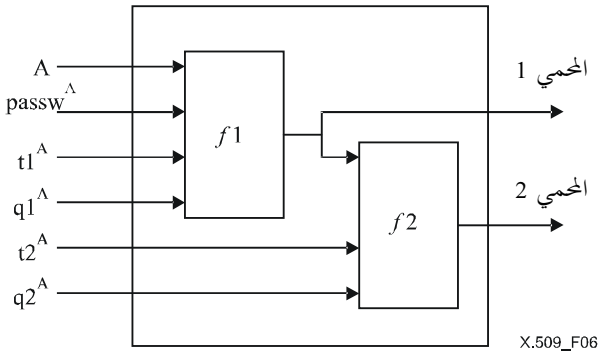
3) يؤكد الدليل (أو ينفي) للمستعمل B صلاحية الثبوتيات؛

4) يمكن إرسال نتيجة الاستيقان من حيث نجاحه أو فشله، إلى المستعمل A.

والشكل الأساسي للاستيقان البسيط يتضمن المرحلة 1) فقط، وبعد أن يتحقق المستعمل B من الاسم المميز وكلمة السر، فقد يتضمن المرحلة 4).

1.1.18 توليد معلومات محميّة للتعريف بالهوية

يوضح الشكل 6 نهجين، يمكن بها توليد معلومات محميّة للتعريف بالهوية. والدالّتان $f1$ و$f2$ هما الدالّتان وحيدتا الاتجاه (غير عكوستين) (متطابقتان أو مختلفتان)، وأختام التاريخ والأرقام العشوائية اختيارية، وخاضعة لاتفاقات ثنائية.

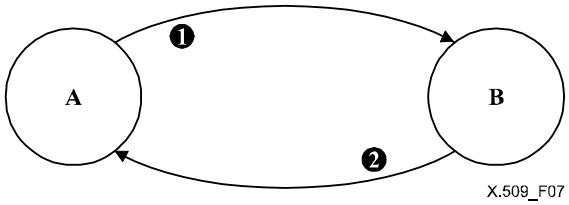


A الاسم المّيز للمستعمل
t^A أختام التاريخ
$passw^A$ كلمة السر للمستعملٍ A
q^A الأرقام العشوائية مع عدّاد مدمج (اختيارياً)

الشكل 6 – الاستيقان البسيط المحميّ

2.1.18 إجراء الاستيقان البسيط المحميّ

يوضح الشكل 7 إجراء الاستيقان البسيط المحميّ



الشكل 7 – إجراء الاستيقان البسيط المحميّ

المراحل المعنية هي التالية (باستخدام الدالّة $f1$ في البداية):

1) يرسل مستعمل A، مُصْدر، معلوماته المحمية للتعرف بالهوية (المستيقن1)، إلى مستعمل B. تتأمن الحماية بتطبيق الدالّة ($f1$) المبينة في الشكل 6، حيث يستعمل ختم التاريخ و/أو الرقم العشوائي (عندما يكون مستعملاً) للإقلال من التكرار إلى أقصى حدّ ولإخفاء كلمة السر.

وتكون حماية كلمة السر للمستعمل A من الشكل:

$$\text{Protected1} = f1\ (t1^A, q1^A, A, passw^A) \quad \text{(المحمي1)}$$

والمعلومات المرسلة إلى المستعمل B من الشكل:

Authenticator1 = $t1^A$, $q1^A$, A, Protected1 (المستيقن1)

2) يتحقق المستعمل B من المعلومات المحميّة للتعريف بالهوية التي أرسلها المستعمل A بتوليده (مستعملاً الاسم المميّز وختم التاريخ و/أو الرقم العشوائي التي قدمها المستعمل A، مع نسخة محلية من كلمة سر المستعمل A) نسخة محلية محميّة من كلمة سر المستعمل A (من الشكل المحميّ1). ويقارن المستعمل B من حيث التساوي المعلومات المزعومة للتعريف بالهوية (المحميّ1) بالقيمة المولّدة محلياً.

3) يؤكد المستعمل B أو ينفي للمستعمل A التحقق من المعلومات المحميّة للتعريف بالهوية.

ويمكن تعديل الإجراء لتقديم حماية أكبر باستخدام الدالتين *f*1 و*f*2. والفروقات الرئيسية هي التالية:

1) يرسل المستعمل A معلوماته الإضافية المحميّة للتعريف بالهوية (المستيقن2) إلى المستعمل B. وتتأمن حماية إضافية بتطبيق الدالّة الأخرى وحيدة الاتجاه *f*2، كما هو موضّح في الشكل 6. وتكون الحماية الإضافية من الشكل:

Protected2 = *f*2 ($t2^A$, $q2^A$, Protected1) (المحمي2)

والمعلومات المرسلة إلى المستعمل B من الشكل:

Authenticator2 = $t1^A$, $t2^A$, $q1^A$, $q2^A$, A, Protected2 (المستيقن2)

ولإجراء المقارنة، يولد المستعمل B قيمة محلية لكلمة سر المستعمل A الإضافية المحميّة، ويقارنها من حيث التساوي مع كلمة السر الواردة في المحميّ 2.

2) يؤكد المستعمل B أو ينفي للمستعمل A التحقق من المعلومات المحمية للتعريف بالهوية.

ملاحظة – الإجراءات المحددة في هذه الفقرات تدرج المستعملين A وB في مواصفتها. وعندما تطبق هذه الإجراءات على الدليل (المحددة في التوصية ITU-T X.511 | المعيار الدولي ISO/IEC 9594-3 وفي التوصية ITU-T X.518 | المعيار الدولي ISO/IEC 9594-4)، يمكن أن يكون المستعمل A وكيلاً لمستعمل الدليل (DUA) مرتبطاً بالمستعمل B الذي هو وكيل نظام الدليل (DSA)، أو كبديل يمكن أن يكون المستعمل B وكيلاً لنظام الدليل DSA مرتبطاً بالمستعمل B الذي هو وكيل آخر لنظام الدليل (DSA).

3.1.18 نمط النعت "كلمة سر المستعمل"

يحتوي نمط النعت *كلمة سر المستعمل* على كلمة السر الهدف. وقيمة النعت لكلمة سر المستعمل هي سلسلة يحددها الهدف.

```
userPassword ATTRIBUTE  ::= {
   WITH SYNTAX                OCTET STRING (SIZE (0..ub-user-password))
   EQUALITY MATCHING RULE     octetStringMatch
   ID                         id-at-userPassword }
```

2.18 الاستيقان المعمّق

الإجراءات المشروحة في هذه الفقرة تستعمل للاستيقان بين وكيل مستعمل الدليل (DUA) ووكيل نظام الدليل (DSA) وكذلك بين أزواج من وكلاء نظام الدليل. وتستخدم هذه الإجراءات إطار شهادة المفتاح العمومي المعرّف في هذه المواصفة. وفوق ذلك تستخدم هذه الإجراءات الدليل بالذات بصفته مستودعاً لمعلومات المفتاح العمومي المطلوبة للقيام بالاستيقان. وإدراج المعلمات ذات السلة في بروتوكولات الدليل محدّد في مواصفات البروتوكول بذاتها. ويمكن أيضاً استخدام الإجراءات المعرّفة هنا للاستيقان المعمّق في تطبيقات أخرى غير الدليل، تستعمل أيضاً مثل هذا المستودع. وعندما يستعمل الدليل هذه الإجراءات، يكون المصطلح "مستعمل" في هذه الإجراءات يحيل إلى وكيل مستعمل الدليل (DUA) أو إلى وكيل نظام الدليل (DSA).

وطريقة مقاربة الاستيقان المعمّق المعتمدة في مواصفة الدليل هذه، تستخدم صفات عائلة من أنظمة التجفير تدعى أنظمة التجفير بالمفتاح العمومي (PKCS). وأنظمة التجفير هذه التي توصف أيضاً بأنها غير متناظرة تشتمل على زوج من المفاتيح

أحدهما عمومي والآخر خاص، بدلاً من المفتاح الواحد الذي يستعمل في أنظمة التجفير التقليدية. ويعطي الملحق E مدخلاً موجزاً إلى أنظمة التجفير هذه وإلى الصفات التي تجعلها مفيدة في الاستيقان. ولكي يصبح نظام PKCS قابلاً للاستعمال في هذا الإطار من الاستيقان في الوقت الحاضر يجب أن يتوفر له كون المفتاحين المكوّنين لزوج المفاتيح، قابلين للاستعمال في التجفير، على أن يستعمل المفتاح الخاص للتجفير إن كان المفتاح العمومي مستعملاً، وأن يستعمل المفتاح العمومي للتجفير إن كان المفتاح الخاص مستعملاً. وبعبارة أخرى $X_p \bullet X_s = X_s \bullet X_p$, حيث X_p وX_s دالّتان للتجفير وفك التجفير تستخدمان المفتاحين العمومي والخاص للمستعمل X.

ملاحظة – هناك إمكانية لتوسع مستقبلي في مواصفة الدليل هذه، يتضمن أنماطاً بديلة من أنظمة التجفير بالمفتاح العمومي لا تحتاج إلى الصفة التبديلية، ولا إلى تعديل كبير في هذه المواصفة.

وإطار الاستيقان هذا لا يفرض استعمال نظام تجفير خاص، ومن المقرّر أن يكون الإطار قابلاً للتطبيق على أي نظام تجفير مناسب بالمفتاح العمومي، ويتقبل التغيرات التي تطرأ على الطرائق المستعملة نتيجة لأوجه التقدم التي تحصل في التجفير أو التقنيات الرياضياتية أو المقدرات الحاسوبية. وعلى كل حال، عندما يرغب مستعملان أن يستيقن كل منهما الآخر، فهما يتقبلان خوارزمية تجفير واحدة لكي يتم الاستيقان بشكل سليم. وهكذا فإن اختيار خوارزمية واحدة في سياق مجموعة من التطبيقات المتعلقة ببعضها، من شأنه أن يوسّع إلى أقصى حدّ جماعة المستعملين القادرين بكل أمان على استيقان بعضهم بعضاً والتواصل فيما بينهم.

يعتمد الاستيقان على امتلاك كل مستعمل اسماً مميزاً وحيداً. ويقع إسناد الأسماء المميزة على مسؤولية سلطات التسمية. ولذلك يجب أن يكون كل مستعمل واثقاً من أن سلطات التسمية لا تصدر أسماء مميزة مضاعفة.

ويتعرّف كل مستعمل بامتلاكه مفتاحه الخاص. ويكون في مقدور مستعمل آخر أن يحدد إن كان شريكه في الاتصال يمتلك المفتاح الخاص، وأن يستخدم هذه المعلومة ليؤكد أن شريكه في الاتصال هو المستعمل المقصود بالفعل. ويتوقف كون هذا التأكيد صالحاً على الاحتفاظ بسرّية المفتاح الخاص للمستعمل.

ولكي يتمكن مستعمل من تحديد كون شريكه في الاتصال يمتلك المفتاح الخاص لمستعمل آخر، يجب أن يكون هو نفسه يمتلك المفتاح العمومي من مدخل الدليل الخاص بالمستعمل، ولكن المتحقق من صحة هذا المفتاح أكثر إشكالاً. وهناك سبل مختلفة تتيح القيام بذلك: ويشرح البند الفرعي 1.2.18 عملية يمكن التحقق بها من المفتاح العمومي لمستعمل ما بالرجوع إلى الدليل. وتتطلب هذه العملية أن توجد بين المستعملين الراغبين في استيقان بعضهم بعضاً، سلسلة متصلة من نقاط الثقة في الدليل. ويمكن إنشاء مثل هذه السلسلة، بتحديد نقطة ثقة مشتركة. وتكون نقطة الثقة المشتركة هذه متعلقة بكل واحد من المستعملين بسلسلة متصلة من نقاط الثقة.

1.2.18 الحصول على شهادات المفتاح العمومي انطلاقاً من الدليل

يحتفظ بالشهادات في مداخل الدليل كنعوت من الأنماط: **شهادة المستعمل** و**شهادة سلطة إصدار الشهادة** و**زوج الشهادات المتقاطعة**. وهذه الأنماط من النعوت معروفة في الدليل. ويمكن تشغيل هذه النعوت باستعمال نفس عمليات البروتوكول المستعملة على النعوت الأخرى. وتجد تعريفات هذه الأنماط في البند الفرعي 3.3، ويعرّف البند الفرعي 2.11 مواصفة هذه الأنماط من النعوت.

وقبل أن يستيقن المستعملون بعضهم بعضاً، يجب أن يقدم الدليل في الحالة العامة مسيرات إصدار الشهادة الكاملة الذاهبة والعائدة. ومع ذلك يمكن عملياً خفض حجم المعلومات التي تستخرج من الدليل من أجل حالة معينة من الاستيقان بالطريقة التالية:

أ) إذا كان المستعملان الراغبان في استيقان بعضهما، تخدمها سلطة إصدار الشهادة نفسها، تصبح مسيرة إصدار الشهادة أمراً تافهاً، ويستطيع كل منهما فتح شهادة الآخر مباشرة؛

ب) وإذا كانت سلطتا إصدار الشهادة للمستعملَيْن مرّتبتين تراتبياً، يمكن للمستعمل اختزان المفاتيح العمومية والشهادات الذاهبة والشهادات العائدة لجميع سلطات إصدار الشهادة الموجودة بينه وبين جذر شجرة

معلومات الدليل (DIT). وهذا يقتضي أن يكون المستعمل بصورة عامة على معرفة بالمفاتيح العمومية وبشهادات ثلاث أو أربع فقط من سلطات إصدار الشهادة. ولا يعود المستعمل عندئذ بحاجة إلا للحصول على مسيرات إصدار الشهادة انطلاقاً من نقطة الثقة المشتركة؛

ج) إذا كان المستعمل يتصل كثيراً بمستعملين تصدّق عليهم سلطة معينة لإصدار الشهادة، يستطيع هذا المستعمل أن يتعرّف مسيرة إصدار الشهادة الذاهبة إلى هذه السلطة ومسيرة إصدار الشهادة المقابلة العائدة من هذه السلطة، ويصبح بذلك بحاجة إلى الحصول فقط على شهادة المستعمل الآخر من الدليل؛

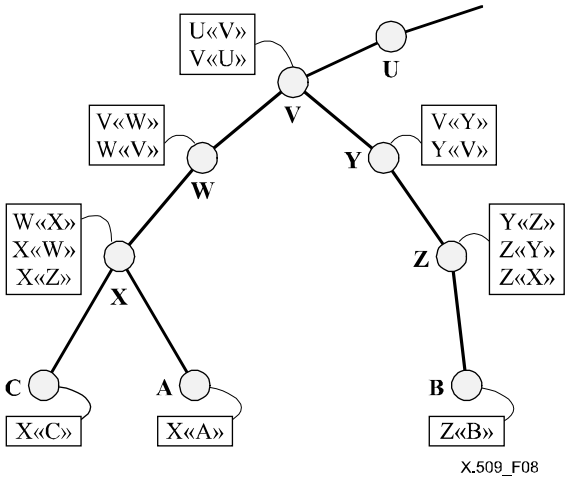
د) وتستطيع سلطتا إصدار الشهادة أن تصدّق كل منهما على الأخرى عبر اتفاق ثنائي، مما يؤدي إلى تقصير مسيرة إصدار الشهادة؛

هـ) إذا كان مستعملان قد اتصلا ببعضهما سابقاً، وتعرّف كل منهما شهادة الآخر، يصبحان قادرين على استيقان بعضهما دون اللجوء إلى الدليل.

وفي كل الأحوال يقوم المستعملان اللذان تعرّف كل منهما شهادة الآخر من مسيرة إصدار الشهادة، بالتحقق من صلاحية الشهادات.

1.1.2.18 مثال

يوضح الشكل 8 مثالاً افتراضياً لقطعة من شجرة معلومات الدليل (DIT)، تشكل فيها سلطات إصدار الشهادة تراتباً. ونفترض إلى جانب المعلومات المبيّنة على صعيد السلطات CA، أن كل مستعمل يعرف المفتاح العمومي لسلطة إصدار الشهادة التي تخصه، ويعرف كذلك مفتاحيه العمومي والخاص.



الشكل 8 – مثال افتراضي على تراتب سلطات إصدار الشهادة (CA)

فإذا كانت سلطات إصدار الشهادة للمستعملين مرتبة تراتبياً، يستطيع المستعمل A أن يحصل من الدليل على الشهادات التالية لكي يقيم مسيرة إصدار الشهادة إلى المستعمل B:

X<<W>>, W<<V>>, V<<Y>>, Y<<Z>>, Z<<B>>

وبمجرد أن يحصل A على هذه الشهادات، يمكنه أن يفتحها على التوالي في مسيرة إصدار الشهادة مما يتيح توفر محتوى شهادة المستعمل B، بما فيها مفتاحه العمومي Bp:

Bp = Xp • X<<W>> W<<V>> V<<Y>> Y<<Z>> Z<<B>>

ويجب على المستعمل A أن يحصل أيضاً من الدليل على الشهادات التالية، لكي يقيم مسيرة إصدار الشهادة للعودة من المستعمل B إلى المستعمل A:

Z<<Y>>, Y<<V>>, V<<W>>, W<<X>>, X<<A>>

وعندما يستلم المستعمل B هذه الشهادات من المستعمل A، يمكن للمستعمل B أن يفتحها على التوالي في مسيرة إصدار الشهادة للعودة، مما يتيح توفر محتوى شهادة المستعمل A، بما فيها مفتاحه العمومي Ap:

$$Ap = Zp \bullet Z\langle\langle Y\rangle\rangle\ Y\langle\langle V\rangle\rangle\ V\langle\langle W\rangle\rangle\ W\langle\langle X\rangle\rangle\ X\langle\langle A\rangle\rangle$$

تطبق الاستمثالات المشروحة في الفقرة 1.2.18 على النحو التالي:

أ) كل من المستعملين A وC يعرف مثلاً المفتاح Xp، بحيث يستطيع المستعمل A الحصول مباشرة على شهادة المستعمل C. فيختزل فتح شهادات مسيرة إصدار الشهادة إلى:

$$Cp = Xp \bullet X\langle\langle C\rangle\rangle$$

كما يختزل فتح شهادات مسيرة الإصدار للعودة إلى:

$$p = Xp \bullet X\langle\langle A\rangle\rangle$$

ب) إذا افترضنا أن المستعمل A يعلم من ذلك Up, U<<V>>, Vp, V<<W>>, Wp, W<<X>> إلخ، تختزل المعلومات التي يجب عليه استخراجها من الدليل لكي يقيم مسيرة إصدار الشهادة إلى:

$$\langle\langle Y\rangle\rangle, Y\langle\langle Z\rangle\rangle, Z\langle\langle B\rangle\rangle$$

كما تختزل المعلومات التي يجب على المستعمل A أن يستخرجها من الدليل لكي يقيم مسيرة إصدار الشهادة للعودة إلى:

$$\langle\langle Y\rangle\rangle, Y\langle\langle V\rangle\rangle$$

ج) وإذا افترضنا أن المستعمل A يتصل كثيراً بالمستعملين الذي تشهد لهم السلطة Z، يمكنه عندئذ أن يتعرف الشهادات <<Y>>, Y<<V>>, Y<<Z>>, Z<<Y>> (إضافة إلى المفاتيح العمومية المتعرّف إليها في الفقرة ب) أعلاه). ويكون عليه أن يستخرج فقط Z<<B>> من الدليل لكي يتصل بالمستعمل B.

د) إذا افترضنا أن المستعملين اللذين تشهد لهما السلطتان X وZ هما على تواصل متواتر، يمكن الاحتفاظ بالشهادة X<<Z>> في مدخل الدليل الخاص بالسلطة X، والعكس بالعكس (كما هو مبين في الشكل 8). فإذا أراد مستعمل A أن يتيقّن من B، لا يحتاج إلا للحصول على:

$$X\langle\langle Z\rangle\rangle, Z\langle\langle B\rangle\rangle$$

لكي يقيم مسيرة إصدار الشهادة، وإلى:

$$Z\langle\langle X\rangle\rangle$$

لكي يقيم مسيرة إصدار الشهادة للعودة.

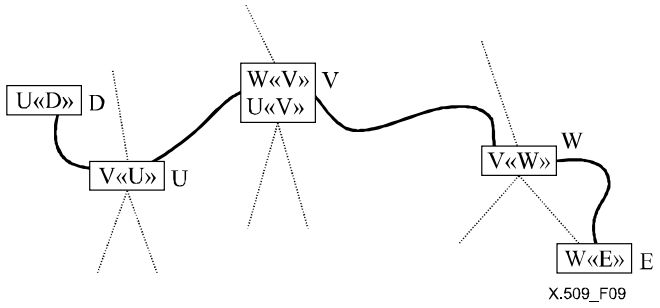
هـ) إذا افترضنا أن المستعملين A وC كانا قد اتصلا سابقاً، وتعرّف كل منهما شهادة الآخر يمكن لكل منهما أن يستعمل مباشرة مفتاح الآخر العمومي، أي:

$$Cp = Xp \bullet X\langle\langle C\rangle\rangle$$

و

$$Ap = Xp \bullet X\langle\langle A\rangle\rangle$$

وفي أغلب الحالات لا يكون بين سلطات إصدار الشهادة علاقات تراتبية. وفي المثال الافتراضي الوارد في الشكل 9، افترضنا مستعملاً D تصدق عليه السلطة U يودّ استيقان المستعمل E الذي تصدّق عليه السلطة W. فإن مدخل الدليل الخاص بالمستعمل D يحتوي على الشهادة U<<D>> والمدخل الخاص بالمستعمل E يحتوي على الشهادة W<<E>>.



الشكل 9 – مثال المسيرة غير التراتبية لإصدار الشهادة

لتكن V سلطة إصدار الشهادة التي سبق أن تبادلت معها سلطتا إصدار الشهادة U وW مفاتيح عمومية بطريقة موثوقة. وينتج عن ذلك أن الشهادات U<<V>>, V<<U>>, W<<V>>, V<<W>> كانت قد تولدت واختزنت في الدليل. ولنفترض أن الشهادتين U<<V>>, W<<V>> قد اختزنتا في مدخل السلطة V، وأن الشهادة V<<U>> قد اختزنت في مدخل السلطة U، وأن الشهادة V<<W>> قد اختزنت في مدخل السلطة W.

ويجب على المستعمل D أن يجد مسيرة إصدار الشهادة إلى المستعمل E. يمكنه أن ينفذ عدة استراتيجيات تكمن إحداها في اعتبار المستعملين والسلطات عُقَداً، والشهادات أقواساً في رسم بياني موجه. وفي ظل هذا الاعتبار، يجب على المستعمل D أن يقوم بالبحث في هذا الرسم البياني، ليجد مسيرة تذهب من U إلى E، على أن تكون إحدى هذه المسيرات U<<V>>, V<<W>>, W<<E>>. ويمكن إقامة مسيرة العودة أيضاً W<<V>>, V<<U>>, U<<D>>، بعد أن تكون المسيرة الأولى قد تمت إقامتها.

2.2.18 إجراءات الاستيقان المعمّق:

أبرزت أعلاه الخطوط العامة لطريقة الاستيقان الأساسية، وهي التأكيد على الهوية بإثبات امتلاك مفتاح خاص. وهناك عدة إجراءات ممكنة للاستيقان الذي يستعمل هذه الطريقة. وبصورة عامة، يعود إلى تطبيق معيّن أن يحدد الإجراءات المناسبة التي تلبي سياسته الأمنية. وتشرح هذه الفقرة ثلاثة إجراءات للاستيقان يمكن أن تكون مفيدة في مدى معيّن من التطبيقات.

ملاحظة – لا تشرح مواصفة الدليل هذه الإجراءات بالتفصيل اللازم لتنفيذها. ومع ذلك يمكن البحث في معايير أخرى يمكنها أن تفعل ذلك، سواء كانت لتطبيق خاص أو لتطبيق بصورة عامة.

وتتضمن هذه الإجراءات الثلاثة أعداداً مختلفة من تبادلات معلومات الاستيقان، وتوفر بالتالي أنماطاً مختلفة من الأمان للمشتركين فيها. وبصورة خاصة:

أ) الاستيقان وحيد الاتجاه المشروح في الفقرة 1.2.2.18 يقتضي نقلاً واحداً للمعلومات من مستعمل A معيّن إلى مستعمل آخر B، ويقوم بالأفعال التالية:

- هوية المستعمل A، وكون إذنة الاستيقان قد ولدها فعلاً هذا المستعمل A؛
- هوية المستعمل B، وكون إذنة الاستيقان قد أعدت بالفعل لكي ترسل إلى هذا المستعمل B؛
- تكاملية "وتفرّدية" (صفة الصدور مرة واحدة فقط) إذنة الاستيقان المنقولة حالياً.

والصفتان الأخيرتان يمكن توفيرهما أيضاً لمعطيات إضافية اعتباطية ترافق عملية النقل؛

ب) الاستيقان ثنائي الاتجاهات المشروح في الفقرة 2.2.2.18 يقتضي فوق ذلك جواباً من المستعمل B إلى المستعمل A، وهو يقوم بالأفعال التالية الإضافية:

- كون إذنة الاستيقان الموجودة في الجواب قد ولدها فعلاً المستعمل B وهي معدة للإرسال إلى المستعمل A؛
- صفتا التكافلية والتفردية لإذنة الاستيقان قد أرسلتا في الجواب؛

– (اختيارياً) السرّية المتبادلة بشأن أجزاء من الإذنات.

ج) الاستيقان ثلاثي الاتجاهات المشروح في الفقرة 3.2.2.18 يقتضي فوق ذلك نقلاً جديداً من المستعمل A إلى المستعمل B. إنه يقوم بنفس الأفعال التي يقوم بها الاستيقان ثنائي الاتجاهات ولكن دون الحاجة إلى تحقق من التصاحب بأختام التاريخ.

وفي كل مرة يجري فيها استيقان معمّق، يجب أن يحصل المستعمل A على المفتاح العمومي للمستعمل B وعلى مسيرة إصدار الشهادة للعودة من المستعمل B إلى المستعمل A، قبل القيام بأي تبادل للمعلومات. وقد يتطلب ذلك نفاذاً إلى الدليل كما هو مشروح في الفقرة 2.18. ولن يذكر ثانية أي نفاذ من هذا النوع في وصف الإجراءات لاحقاً.

والتحقق من أختام التاريخ المذكورة في الفقرات التالية لا ينطبق إلا إذا كانت تستعمل ميقاتيات متزامنة تستعمل في بيئة محلية أو كانت تستعمل ميقاتيات تمت مزامنتها باتفاقات ثنائية. ومع ذلك يوصى باستخدام التوقيت العالمي المنسق في الحالتين.

ويفترض في كل واحد من الإجراءات الثلاثة المشروحة أدناه، أن يكون الطرف A قد تحقق من صلاحية جميع الشهادات الموجودة في مسيرة إصدار الشهادة.

1.2.2.18 الاستيقان وحيد الاتجاه

تجري الخطوات التالية كما هو مبين في الشكل 10:

1) يولّد المستعمل A عدداً لا يتكرر هو r^A، يستعمل لكي يكشف الهجمات باستخدام تكرار الاستعمال ولكي يتّقي التزوير.

2) يرسل المستعمل A الرسالة التالية إلى المستعمل B:

$$BA, A\{t^A, r^A, B\}$$

حيث t^A هو ختم التاريخ. ويتكون t^A من واحد من تاريخين: وقت توليد الإذنة (اختياري) ووقت انتهاء الصلاحية. ويستعمل الشكل التالي كبديل، إذا كان الاستيقان الأصلي للمعطيات "sgnData" يجب أن يقدمه التوقيع الرقمي:

$$BA, A\{t^A, r^A, B, sgnData\}$$

ويستعمل الشكل التالي في الحالات التي تستعمل فيها لاحقاً المعطيات المنقولة كمفتاح خاص (وهذه المعلومات يمثلها "encData"):

$$BA, A\{t^A, r^A, B, sgnData, Bp[encData]\}$$

وينطوي استعمال المعطيات "encData" كمفتاح خاص، على أن اختيارها يجب أن يتم بكل عناية، لكي تكون مثلاً مفتاحاً قوياً حيث يستعمل نظام تجفير، كما هو مبين في الحقل "sgnData" من الإذنة.

3) ويقوم المستعمل B بالأعمال التالية:

أ) الحصول على المفتاح Ap من المسيرة BA، متحققاً من أن شهادة المستعمل A لم تنته صلاحيتها؛

ب) التحقق من التوقيع، وبالتالي من تكاملية المعلومات الموقّعة؛

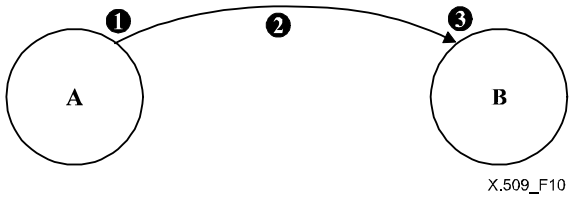
ج) التحقق من أن المستعمل B هو بالذات المَقْصد المقصود؛

د) التحقق من أن ختم التاريخ هو "الحالي"؛

ه) التحقق من أن العدد r^A لم يكرر استعماله، وهذا اختياري، ويمكن القيام بذلك بجعل العدد r^A يتضمن جزءاً تتابعياً، يمكن لتطبيق محلي أن يتحقق من وحدانية قيمته.

ويبقى العدد r^A صالحاً إلى تاريخ انتهاء صلاحيته الذي يبيّنه الختم t^A. ويترافق العدد r^A دائماً بجزء تتابعي يبين أن المستعمل A يجب ألا يكرر الإذنة أثناء الفترة الزمنية التي يحددها t^A، ولذلك لا لزوم للتحقق من قيمة العدد r^A نفسه.

ومن المعقول في كل الأحوال، أن يختزن الطرف B الجزء التتابعي مع ختم التاريخ t^A بشكل واضح ومعهما الجزء المفروم من الإذنة أثناء الفترة الزمنية التي يحددها t^A.



الشكل 10 – الاستيقان وحيد الاتجاه

2.2.2.18 الاستيقان ثنائي الاتجاهات

تجري الخطوات التالية كما هو مبين في الشكل 11:

1) كما هو مشروح في الفقرة 1.2.2.18؛

2) كما هو مشروح في الفقرة 1.2.2.18؛

3) كما هو مشروح في الفقرة 1.2.2.18؛

4) يولد المستعمل B عدداً لا يتكرر هو r^B، يستعمل لأغراض مماثلة لأغراض العدد r^A؛

5) يرسل المستعمل B إذنة الاستيقان التالية إلى المستعمل A:

$$B\{t^B, r^B, A, r^A\}$$

حيث t^B هو ختم تاريخ يعرّف مثل t^A.

ويستعمل الشكل التالي كبديل، إذا كان الاستيقان الأصلي للمعطيات "sgnData"، يجب أن يوفر التوقيع الرقمي:

$$B\{t^B, r^B, A, r^A, sgnData\}$$

ويستعمل الشكل التالي في الحالات التي تستعمل فيها لاحقاً المعطيات المنقولة كمفتاح خاص (هذه المعلومات يمثلها "encData"):

$$B\{t^B, r^B, A, r^A, sgnData, Ap[encData]\}$$

وينطوي استعمال المعطيات "encData" كمفتاح خاص، على أن اختيارها يجب أن يتم بكل عناية، لكي تكون مثلاً مفتاحاً قوياً حيث يستعمل نظام تجفير، كما هو مبين في الحقل "sgnData" من الإذنة.

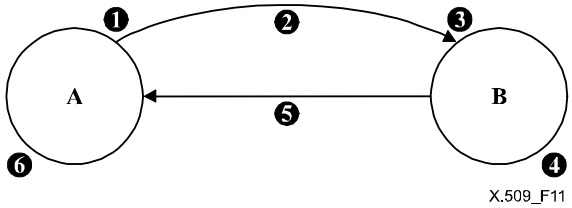
6) ويقوم المستعمل A بالأعمال التالية:

أ) التحقق من التوقيع، وبالتالي من تكاملية المعلومات الموقّعة؛

ب) التحقق من أن المستعمل A هو بالذات المَقْصد المقصود؛

ج) التحقق من أن ختم التاريخ t^B هو "الحالي"؛

د) التحقق من أن العدد r^B لم يكرر استعماله، وهذا اختياري (انظر الفقرة د) من الخطوة 3) في الفقرة 1.2.2.18).



الشكل 11 – الاستيقان ثنائي الاتجاهات

3.2.2.18 الاستيقان ثلاثي الاتجاهات

تجري الخطوات التالية كما هو مبين في الشكل 12:

1) كما هو مشروح في الفقرة 2.2.2.18؛

2) كما هو مشروح في الفقرة 2.2.2.18. يمكن أن يكون ختم التاريخ t^A يساوي الصفر؛

3) كما هو مشروح في الفقرة 2.2.2.18، ما عدا أن ختم التاريخ يحتاج إلى تحقق منه؛

4) كما هو مشروح في الفقرة 2.2.2.18؛

5) كما هو مشروح في الفقرة 2.2.2.18. يمكن أن يكون ختم التاريخ t^B يساوي الصفر؛

6) كما هو مشروح في الفقرة 2.2.2.18، ما عدا أن ختم التاريخ لا يحتاج إلى تحقق منه؛

7) يتحقق المستعمل A من أن r^A المستلم هو مطابق للعدل r^A الذي كان قد أرسل؛

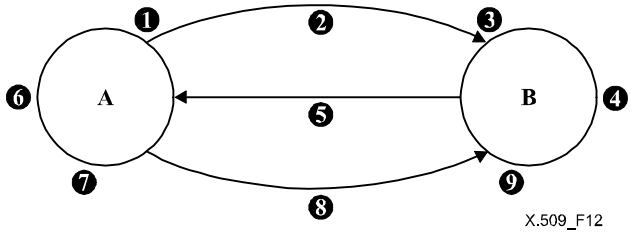
8) يرسل المستعمل A إذنة الاستيقان التالية إلى المستعمل B:

$$A\{r^B,B\}$$

9) يقوم المستعمل B بالأعمال التالي:

أ) التحقق من التوقيع، وبالتالي من تكاملية المعلومات الموقّعة؛

ب) التحقق من أن العدد r^B المستلم هو مطابق للعدل r^B الذي كان المستعمل B قد أرسله.



الشكل 12 – الاستيقان ثلاثي الاتجاهات

19 التحكم في النفاذ

الدليل موجود في بيئة تقوم فيها سلطات إدارية مختلفة بالتحكم في النفاذ إلى الجزء الخاص بكل منها من قاعدة معلومات الدليل (DIB). وتحديد تخطيطة التحكم في النفاذ يشمل الطرائق التي تقدم الوظائف التالية:

- تحديد معلومات التحكم في النفاذ؛
- التقيد بتنفيذ حقوق النفاذ التي تحددها هذه المعلومات للتحكم في النفاذ؛
- صيانة معلومات التحكم في النفاذ.

ينطبق التقيد بتنفيذ حقوق النفاذ التي تحددها هذه المعلومات للتحكم في النفاذ:

- معلومات الدليل المتعلقة بالأسماء؛
- معلومات مستعمل الدليل؛
- معلومات تشغيل الدليل التي تشمل معلومات التحكم في النفاذ.

تستطيع السلطات الإدارية أن تستعمل تخطيطة التحكم في النفاذ المقيّسة، كلها أو بعضها، أو أن تحدّد بكل حرية تخطيطتها الخاصة للتحكم في النفاذ حسب تقديرها.

التحكم الأساسي في النفاذ (BAC) المعرّف في التوصية ITU-T X.501 | المعيار الدولي ISO/IEC 9594-2 هو طريقة تقوم على قائمة تحكّم في النفاذ، تمكّن مديري الدليل من ربط الأذونات بسوية الاستيقان المحققة للربط بالدليل. ويستعمل إطار شهادة المفتاح العمومي المحدد في هذه المواصفة لتقديم تخطيطة الاستيقان المعمّق المستعمل لهذه الرابطة.

والتحكم في النفاذ المبني على قواعد (RBAC) المعرّف في التوصية ITU-T X.501 | المعيار الدولي ISO/IEC 9594-2، يستعمل إطار شهادة النعت المعرف في هذه المواصفة، لحمل نعوت التأهيل المستعملة في اتخاذ قرارات التحكم في النفاذ. ويمكن استعمال التحكم في النفاذ المبني على قواعد بالاشتراك مع التحكم الأساسي في النفاذ.

20 حماية عمليات الدليل

يستعمل إطار شهادة المفتاح العمومي المعرّف في هذه المواصفة في جميع بروتوكولات الدليل المحددة في سلسلة هذه التوصيات، من أجل حماية اختيارية للعمليات التي تشمل الطلبات والاستجابات والأخطاء. أما حماية التكاملية فيؤمنها التوقيع الرقمي للمرسل، والتحقق من هذا التوقيع الذي يقوم به المَقْصد مستخدماً شهادة المفتاح العمومي للمرسل. وتتأمن حماية السرّية باستخدام التجفير بالمفتاح العمومي الذي يجفّر المحتوى فيه باستخدام المفتاح العمومي الذي يتم الحصول عليه من شهادة المفتاح العمومي للمَقْصد المقصود، ويفك تجفيره المَقْصد لمقصود بواسطة المفتاح الخاص المقابل.

والطرائق وقواعد التركيب اللازمة لطلب عناصر الحماية وإدراجها في مبادلات البروتوكول، تكون محددة في كل واحد من بروتوكولات الدليل الموجودة في هذه السلسلة من المواصفات.

الملحق A

أُطُر شهادات النعت وشهادات المفتاح العمومي

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

يتضمن هذا الملحق بشكل ثلاث وحدات من الترميز ASN.1 جميع تعريفات النمط والقيمة وصنف موضوعات المعلومات المستعملة في مواصفة الدليل هذه من الترميز ASN.1. وهذه الوحدات هي **إطار الاستيقان (AuthenticationFramework)**، **وتوسعات الشهادة (CertificateExtensions)**، **وتعريفات شهادة النعت (AttributeCertificateDefinitions)**.

-- A.1 Authentication framework module *-- 1.A وحدة إطار الاستيقان*

```
AuthenticationFramework {joint-iso-itu-t ds(5) module(1) authenticationFramework(7) 5}
DEFINITIONS ::=
BEGIN

-- EXPORTS All --
-- The types and values defined in this module are exported for use in the other ASN.1 modules contained
-- within the Directory Specifications, and for the use of other applications which will use them to access
-- Directory services. Other applications may use them for their own purposes, but this will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
-- الأنماط والقيم المعرفة في هذه الوحدة تصدّر لاستعمالها في وحدات ASN.1 أخرى موجودة في الدليل، ولكي تستعملها
-- تطبيقات أخرى ترغب في النفاذ إلى خدمات الدليل. وقد تستعملها تطبيقات أخرى لأغراض خاصة بها، ولكن هذا
-- الاستعمال لن يفرض تقييدات على التوسعات والتعديلات اللازمة لصيانة خدمة الدليل وتحسينها.

IMPORTS
    id-at, id-nf, id-oc, informationFramework, upperBounds, selectedAttributeTypes, basicAccessControl,
    certificateExtensions
        FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 5}

    Name, ATTRIBUTE, OBJECT-CLASS, NAME-FORM, top
        FROM InformationFramework informationFramework

    ub-user-password, ub-content
        FROM UpperBounds upperBounds

    UniqueIdentifier, octetStringMatch, DirectoryString{}, commonName
        FROM SelectedAttributeTypes selectedAttributeTypes

    certificateExactMatch, certificatePairExactMatch, certificateListExactMatch, KeyUsage, GeneralNames,
       CertificatePoliciesSyntax, algorithmIdentifierMatch, CertPolicyId
        FROM CertificateExtensions certificateExtensions ;

-- public-key certificate definition --                    -- تعريف شهادة المفتاح العمومي --

Certificate                 ::=  SIGNED { SEQUENCE {
    version                 [0]  Version DEFAULT v1,
    serialNumber                 CertificateSerialNumber,
    signature                    AlgorithmIdentifier,
    issuer                       Name,
    validity                     Validity,
    subject                      Name,
    subjectPublicKeyInfo         SubjectPublicKeyInfo,
    issuerUniqueIdentifier  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                                 -- if present, version shall be v2 or v3    -- إن وجد تكون الصيغة v2 أو v3
    subjectUniqueIdentifier [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                                 -- if present, version shall be v2 or v3    -- إن وجد تكون الصيغة v2 أو v3
    extensions              [3]  Extensions OPTIONAL
                                 -- if present, version shall be be v3 -- } }    -- إن وجد تكون الصيغة v3 -- { {

Version                     ::=  INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber     ::=  INTEGER

AlgorithmIdentifier              ::=  SEQUENCE {
    algorithm               ALGORITHM.&id ({SupportedAlgorithms}),
    parameters              ALGORITHM.&Type ({SupportedAlgorithms}{ @algorithm}) OPTIONAL }
```

```
-- Definition of the following information object set is deferred, perhaps to standardized
-- profiles or to protocol implementation conformance statements. The set is required to
-- specify a table constraint on the parameters component of AlgorithmIdentifier.
-- تعريف موضوع المعلومات التالية مؤجل، بانتظار إعلانات محتملة عن جانبيات مقيّسة أو عن تطابق تنفيذ
-- بروتوكول. هذه المجموعة مطلوبة لمواصفة جدول مكوّنة المعلمات لمجال معرّف هوية الخوارزمية.
SupportedAlgorithms     ALGORITHM ::= { ... }

Validity                ::= SEQUENCE {
    notBefore       Time,
    notAfter        Time }

SubjectPublicKeyInfo    ::= SEQUENCE {
    algorithm           AlgorithmIdentifier,
    subjectPublicKey    BIT STRING }

Time ::= CHOICE {
    utcTime             UTCTime,
    generalizedTime     GeneralizedTime }

Extensions ::= SEQUENCE OF Extension
-- For those extensions where ordering of individual extensions within the SEQUENCE is significant, the
-- specification of those individual extensions shall include the rules for the significance of the order therein
-- عندما يكون ترتيب التوسعات داخل التتابع ذا معنى، فإن مواصفة هذه التوسعات الإفرادية ستشمل قواعد المعاني بالترتيب الذي وردت فيه.

Extension ::= SEQUENCE {
    extnId          EXTENSION.&id ({ExtensionSet}),
    critical        BOOLEAN DEFAULT FALSE,
    extnValue       OCTET STRING
                    -- contains a DER encoding of a value of type &ExtnType
                    -- for the extension object identified by extnId -- }
                    -- يحتوي تشفير DER (قواعد التشفير المميزة) لقيمة النمط ExtnType
                    -- من موضوع التوسع المحدّد بالمجال extnId -- {

ExtensionSet EXTENSION      ::= { ... }

EXTENSION ::= CLASS {
    &id         OBJECT IDENTIFIER UNIQUE,
    &ExtnType }
WITH SYNTAX {
    SYNTAX          &ExtnType
    IDENTIFIED BY   &id }

-- other PKI certificate constructs                    -- بنى أخرى لشهادة البنية PKI

Certificates                ::=     SEQUENCE {
    userCertificate                 Certificate,
    certificationPath               ForwardCertificationPath OPTIONAL}

ForwardCertificationPath    ::=     SEQUENCE OF CrossCertificates

CrossCertificates           ::=     SET OF Certificate

CertificationPath           ::=     SEQUENCE {
    userCertificate                 Certificate,
    theCACertificates               SEQUENCE OF CertificatePair OPTIONAL}

CertificatePair         ::=     SEQUENCE {
    forward         [0]         Certificate OPTIONAL,
    reverse         [1]         Certificate OPTIONAL
                    -- at least one of the pair shall be present -- }
                    -- يجب أن يكون واحد من فردي الزوج موجوداً -- {
    (WITH COMPONENTS { ..., forward PRESENT} |
    WITH COMPONENTS { ..., reverse PRESENT})

-- certificate revocation list (CRL)                   -- قائمة إبطال الشهادات (CRL)

CertificateList         ::=     SIGNED { SEQUENCE {
    version                         Version OPTIONAL,
                    -- if present, version shall be v2  -- إن وجد تكون الصيغة v2
    signature                       AlgorithmIdentifier,
    issuer                          Name,
    thisUpdate                      Time,
    nextUpdate                      Time OPTIONAL,
    revokedCertificates             SEQUENCE OF SEQUENCE {
        serialNumber                    CertificateSerialNumber,
        revocationDate                  Time,
```

```
        crlEntryExtensions              Extensions OPTIONAL } OPTIONAL,
    crlExtensions       [0]             Extensions OPTIONAL }}
-- information object classes --                                   -- أصناف موضوعات المعلومات --

ALGORITHM ::=   TYPE-IDENTIFIER

-- parameterized types --                                          -- أنماط ذات معلمات --

HASH {ToBeHashed}       ::=         SEQUENCE {
    algorithmIdentifier             AlgorithmIdentifier,
    hashValue                       BIT STRING ( CONSTRAINED BY {
        -- shall be the result of applying a hashing procedure to the DER-encoded octets --
                                    -- يجب أن يكون نتيجة تطبيق إجراء فرم على الأثمونات المشفرة بالتشفير DER --
    -- of a value of --ToBeHashed } ) }          { ( { يطلب فرمها } ) }  -- قيمته --


ENCRYPTED-HASH { ToBeSigned }       ::=         BIT STRING ( CONSTRAINED BY {
    -- shall be the result of applying a hashing procedure to the DER-encoded (see 6.1) octets --
    -- of a value of -- ToBeSigned -- and then applying an encipherment procedure to those octets -- })
                                    -- يجب أن يكون نتيجة تطبيق إجراء فرم على الأثمونات المشفرة بالتشفير DER (قواعد التشفير المميزة) (انظر 1.6) --
                                    -- قيمته -- يطلب توقيعها -- ثم تطبيق إجراء تشفير على هذه الأثمونات -- { )

ENCRYPTED { ToBeEnciphered }        ::=         BIT STRING ( CONSTRAINED BY {
    -- shall be the result of applying an encipherment procedure --
    -- to the BER-encoded octets of a value of -- ToBeEnciphered})
                                    -- يجب أن يكون نتيجة تطبيق إجراء تجفير --
                                    -- على الأثمونات المشفرة بالتشفير BER (قواعد التشفير الأساسية)

SIGNATURE { ToBeSigned }            ::=         SEQUENCE {
    algorithmIdentifier             AlgorithmIdentifier,
    encrypted                       ENCRYPTED-HASH { ToBeSigned }}


SIGNED { ToBeSigned }               ::=         SEQUENCE {
    toBeSigned                      ToBeSigned,
    COMPONENTS OF                   SIGNATURE { ToBeSigned }}

-- PKI object classes --                                          -- أصناف الموضوعات --

pkiUser  OBJECT-CLASS       ::= {
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {userCertificate}
    ID              id-oc-pkiUser }


pkiCA OBJECT-CLASS          ::= {
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {cACertificate |
                    certificateRevocationList |
                    authorityRevocationList |
                    crossCertificatePair }
    ID              id-oc-pkiCA }


cRLDistributionPoint            OBJECT-CLASS            ::= {
    SUBCLASS OF                 { top }
    KIND                        structural
    MUST CONTAIN                { commonName }
    MAY CONTAIN                 { certificateRevocationList |
                                authorityRevocationList |
                                deltaRevocationList }
    ID                          id-oc-cRLDistributionPoint }


cRLDistPtNameForm  NAME-FORM        ::= {
    NAMES                       cRLDistributionPoint
    WITH ATTRIBUTES             { commonName}
    ID                          id-nf-cRLDistPtNameForm }
```

```
deltaCRL      OBJECT-CLASS        ::= {
    SUBCLASS OF             {top}
    KIND                    auxiliary
    MAY CONTAIN             {deltaRevocationList}
    ID                      id-oc-deltaCRL }

cpCps    OBJECT-CLASS       ::= {
    SUBCLASS OF             {top}
    KIND                    auxiliary
    MAY CONTAIN             {certificatePolicy |
                            certificationPracticeStmt}
    ID                      id-oc-cpCps }


pkiCertPath         OBJECT-CLASS        ::= {
    SUBCLASS OF             {top}
    KIND                    auxiliary
    MAY CONTAIN             { pkiPath }
    ID                      id-oc-pkiCertPath }
```

-- PKI directory attributes -- *-- النعوت الدليلية للبنية PKI --*

```
userCertificate                 ATTRIBUTE  ::=           {
        WITH SYNTAX                                     Certificate
        EQUALITY MATCHING RULE              certificateExactMatch
        ID                                              id-at-userCertificate}

cACertificate                   ATTRIBUTE  ::=           {
        WITH SYNTAX                                     Certificate
        EQUALITY MATCHING RULE              certificateExactMatch
        ID                                              id-at-cAcertificate }

crossCertificatePair        ATTRIBUTE  ::=          {
        WITH SYNTAX                                     CertificatePair
        EQUALITY MATCHING RULE              certificatePairExactMatch
        ID                                              id-at-crossCertificatePair }

certificateRevocationList  ATTRIBUTE  ::=          {
        WITH SYNTAX                                     CertificateList
        EQUALITY MATCHING RULE              certificateListExactMatch
        ID                                              id-at-certificateRevocationList }

authorityRevocationList    ATTRIBUTE  ::=          {
        WITH SYNTAX                                     CertificateList
        EQUALITY MATCHING RULE              certificateListExactMatch
        ID                                              id-at-authorityRevocationList }

deltaRevocationList ATTRIBUTE ::= {
        WITH SYNTAX                                     CertificateList
        EQUALITY MATCHING RULE              certificateListExactMatch
        ID                                              id-at-deltaRevocationList }


supportedAlgorithms  ATTRIBUTE ::= {
    WITH SYNTAX                     SupportedAlgorithm
    EQUALITY MATCHING RULE          algorithmIdentifierMatch
    ID                              id-at-supportedAlgorithms }

SupportedAlgorithm ::= SEQUENCE {
    algorithmIdentifier                     AlgorithmIdentifier,
    intendedUsage                   [0]     KeyUsage OPTIONAL,
    intendedCertificatePolicies     [1]     CertificatePoliciesSyntax OPTIONAL }


certificationPracticeStmt    ATTRIBUTE  ::=  {
    WITH SYNTAX       InfoSyntax
    ID                      id-at-certificationPracticeStmt }
```

```
InfoSyntax    ::=  CHOICE {
   content          DirectoryString {ub-content},
   pointer          SEQUENCE {
      name                GeneralNames,
      hash                HASH { HashedPolicyInfo } OPTIONAL } }

POLICY  ::=  TYPE-IDENTIFIER

HashedPolicyInfo      ::=    POLICY.&Type( {Policies} )
Policies POLICY ::= {...} -- Defined by implementors --          -- يعرّفها المنفذون --


certificatePolicy   ATTRIBUTE   ::=  {
   WITH SYNTAX       PolicySyntax
   ID                id-at-certificatePolicy }


PolicySyntax ::=  SEQUENCE {
   policyIdentifier     PolicyID,
   policySyntax         InfoSyntax
   }


PolicyID       ::=  CertPolicyId


pkiPath        ATTRIBUTE   ::= {
   WITH SYNTAX       PkiPath
   ID                id-at-pkiPath }


PkiPath        ::=  SEQUENCE OF Certificate


userPassword     ATTRIBUTE   ::=  {
   WITH SYNTAX                      OCTET STRING (SIZE (0..ub-user-password))
   EQUALITY MATCHING RULE           octetStringMatch
   ID                               id-at-userPassword }

-- object identifier assignments --                    -- إسنادات معرف هوية الموضوع --
-- object classes --                                   -- أصناف الموضوعات --
id-oc-cRLDistributionPoint          OBJECT IDENTIFIER ::=          {id-oc 19}
id-oc-pkiUser                       OBJECT IDENTIFIER ::=          {id-oc 21}
id-oc-pkiCA                         OBJECT IDENTIFIER ::=          {id-oc 22}
id-oc-deltaCRL                      OBJECT IDENTIFIER ::=          {id-oc 23}
id-oc-cpCps                         OBJECT IDENTIFIER ::=          {id-oc 30}
id-oc-pkiCertPath                   OBJECT IDENTIFIER ::=          {id-oc 31}
-- name forms--                                        -- أشكال الاسم --
id-nf-cRLDistPtNameForm             OBJECT IDENTIFIER ::=          {id-nf 14}
-- directory attributes--                              -- النعوت الدليلية --
id-at-userPassword                  OBJECT IDENTIFIER ::=          {id-at 35}
id-at-userCertificate               OBJECT IDENTIFIER ::=          {id-at 36}
id-at-cAcertificate                 OBJECT IDENTIFIER ::=          {id-at 37}
id-at-authorityRevocationList       OBJECT IDENTIFIER ::=          {id-at 38}
id-at-certificateRevocationList     OBJECT IDENTIFIER ::=          {id-at 39}
id-at-crossCertificatePair          OBJECT IDENTIFIER ::=          {id-at 40}
id-at-supportedAlgorithms           OBJECT IDENTIFIER ::=          {id-at 52}
id-at-deltaRevocationList           OBJECT IDENTIFIER ::=          {id-at 53}
id-at-certificationPracticeStmt     OBJECT IDENTIFIER ::=          {id-at 68}
id-at-certificatePolicy             OBJECT IDENTIFIER ::=          {id-at 69}
id-at-pkiPath                       OBJECT IDENTIFIER ::=          {id-at 70}

END                                                        النهاية
```

-- A.2 Certificate extensions module *وحدة توسعات الشهادة 2.A --*

```
CertificateExtensions {joint-iso-itu-t ds(5) module(1) certificateExtensions(26) 5}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL --

IMPORTS
    id-at, id-ce, id-mr, informationFramework, authenticationFramework,
        selectedAttributeTypes, upperBounds
        FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
        usefulDefinitions(0) 5}

    Name, RelativeDistinguishedName, ATTRIBUTE, Attribute, MATCHING-RULE
        FROM InformationFramework informationFramework

    CertificateSerialNumber, CertificateList, AlgorithmIdentifier,
        EXTENSION, Time, PolicyID
        FROM AuthenticationFramework authenticationFramework

    DirectoryString {}
        FROM SelectedAttributeTypes selectedAttributeTypes

    ub-name
        FROM UpperBounds upperBounds

    ORAddress
        FROM MTSAbstractService {joint-iso-itu-t mhs(6) mts(3)
        modules(0) mts-abstract-service(1) version-1999 (1) } ;

-- Unless explicitly noted otherwise, there is no significance to the ordering   -- لا يوجد معنى لترتيب مكونات التتابع من الموجود
-- of components of a SEQUENCE OF construct in this Specification.               -- في هذه المواصفة، ما لم يشر إلى غير ذلك صراحة.

-- public-key certificate and CRL extensions --                                  -- توسعات شهادة المفتاح العمومي والقائمة CRL --

authorityKeyIdentifier EXTENSION ::= {
    SYNTAX              AuthorityKeyIdentifier
    IDENTIFIED BY       id-ce-authorityKeyIdentifier }

AuthorityKeyIdentifier ::= SEQUENCE {
    keyIdentifier               [0] KeyIdentifier               OPTIONAL,
    authorityCertIssuer         [1] GeneralNames                OPTIONAL,
    authorityCertSerialNumber   [2] CertificateSerialNumber     OPTIONAL }
    ( WITH COMPONENTS           {..., authorityCertIssuer PRESENT,
                    authorityCertSerialNumber PRESENT} |
    WITH COMPONENTS             {..., authorityCertIssuer ABSENT,
                    authorityCertSerialNumber ABSENT} )

KeyIdentifier ::= OCTET STRING

subjectKeyIdentifier EXTENSION ::= {
    SYNTAX              SubjectKeyIdentifier
    IDENTIFIED BY       id-ce-subjectKeyIdentifier }

SubjectKeyIdentifier ::= KeyIdentifier


keyUsage EXTENSION ::= {
        SYNTAX              KeyUsage
        IDENTIFIED BY       id-ce-keyUsage }

KeyUsage ::= BIT STRING {
    digitalSignature        (0),
    contentCommitment       (1),
    keyEncipherment         (2),
    dataEncipherment        (3),
    keyAgreement            (4),
    keyCertSign             (5),
    cRLSign                 (6),
    encipherOnly            (7),
    decipherOnly            (8) }
```

```
extKeyUsage EXTENSION ::= {
    SYNTAX              SEQUENCE SIZE (1..MAX) OF KeyPurposeId
    IDENTIFIED BY       id-ce-extKeyUsage }

KeyPurposeId ::= OBJECT IDENTIFIER

privateKeyUsagePeriod EXTENSION ::= {
    SYNTAX              PrivateKeyUsagePeriod
    IDENTIFIED BY       id-ce-privateKeyUsagePeriod }

PrivateKeyUsagePeriod ::= SEQUENCE {
    notBefore       [0]   GeneralizedTime OPTIONAL,
    notAfter        [1]   GeneralizedTime OPTIONAL }
    ( WITH COMPONENTS {..., notBefore PRESENT} |
    WITH COMPONENTS     {..., notAfter PRESENT} )

certificatePolicies EXTENSION ::= {
    SYNTAX              CertificatePoliciesSyntax
    IDENTIFIED BY       id-ce-certificatePolicies }

CertificatePoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
    policyIdentifier    CertPolicyId,
    policyQualifiers    SEQUENCE SIZE (1..MAX) OF
                            PolicyQualifierInfo OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId       CERT-POLICY-QUALIFIER.&id
                            ({SupportedPolicyQualifiers}),
    qualifier               CERT-POLICY-QUALIFIER.&Qualifier
                            ({SupportedPolicyQualifiers}{@policyQualifierId})
                            OPTIONAL }

SupportedPolicyQualifiers CERT-POLICY-QUALIFIER ::= { ... }

anyPolicy     OBJECT IDENTIFIER    ::=   { 2 5 29 32 0 }

CERT-POLICY-QUALIFIER ::= CLASS {
    &id             OBJECT IDENTIFIER UNIQUE,
    &Qualifier      OPTIONAL }
WITH SYNTAX {
    POLICY-QUALIFIER-ID   &id
    [QUALIFIER-TYPE   &Qualifier] }


policyMappings EXTENSION ::= {
    SYNTAX              PolicyMappingsSyntax
    IDENTIFIED BY       id-ce-policyMappings }

PolicyMappingsSyntax ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
    issuerDomainPolicy          CertPolicyId,
    subjectDomainPolicy         CertPolicyId }


subjectAltName EXTENSION ::= {
    SYNTAX              GeneralNames
    IDENTIFIED BY       id-ce-subjectAltName }

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
    otherName                   [0]   INSTANCE OF OTHER-NAME,
    rfc822Name                  [1]   IA5String,
    dNSName                     [2]   IA5String,
    x400Address                 [3]   ORAddress,
    directoryName               [4]   Name,
    ediPartyName                [5]   EDIPartyName,
    uniformResourceIdentifier   [6]   IA5String,
    iPAddress                   [7]   OCTET STRING,
    registeredID                [8]   OBJECT IDENTIFIER }
```

```
OTHER-NAME ::= TYPE-IDENTIFIER

EDIPartyName ::= SEQUENCE {
    nameAssigner        [0]   DirectoryString {ub-name} OPTIONAL,
    partyName           [1]   DirectoryString {ub-name} }


issuerAltName EXTENSION ::= {
    SYNTAX              GeneralNames
    IDENTIFIED BY       id-ce-issuerAltName }


subjectDirectoryAttributes EXTENSION ::= {
    SYNTAX              AttributesSyntax
    IDENTIFIED BY       id-ce-subjectDirectoryAttributes }

AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute


basicConstraints EXTENSION ::= {
    SYNTAX              BasicConstraintsSyntax
    IDENTIFIED BY       id-ce-basicConstraints }

BasicConstraintsSyntax ::= SEQUENCE {
    cA                      BOOLEAN DEFAULT FALSE,
    pathLenConstraint       INTEGER (0..MAX) OPTIONAL }


nameConstraints EXTENSION ::= {
    SYNTAX          NameConstraintsSyntax
    IDENTIFIED BY       id-ce-nameConstraint }

NameConstraintsSyntax ::= SEQUENCE {
    permittedSubtrees       [0]   GeneralSubtrees OPTIONAL,
    excludedSubtrees        [1]   GeneralSubtrees OPTIONAL,
    requiredNameForms       [2]   NameForms OPTIONAL  }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
    base                    GeneralName,
    minimum  [0]   BaseDistance DEFAULT 0,
    maximum  [1]   BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)


NameForms  ::= SEQUENCE {
   basicNameForms    [0]   BasicNameForms OPTIONAL,
   otherNameForms    [1]   SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER OPTIONAL }
(ALL EXCEPT ({ -- none; i.e., at least one component shall be present -- }))
                                        -- لا شيء؛ أي توجد مكوّنة واحدة على الأقل --

BasicNameForms  ::= BIT STRING {
    rfc822Name              (0),
    dNSName             (1),
    x400Address         (2),
    directoryName       (3),
    ediPartyName        (4),
    uniformResourceIdentifier    (5),
    iPAddress           (6),
    registeredID            (7) }  (SIZE (1..MAX))

policyConstraints EXTENSION ::= {
    SYNTAX              PolicyConstraintsSyntax
    IDENTIFIED BY       id-ce-policyConstraints }
PolicyConstraintsSyntax ::= SEQUENCE {
    requireExplicitPolicy     [0] SkipCerts OPTIONAL,
    inhibitPolicyMapping      [1] SkipCerts OPTIONAL }

SkipCerts ::= INTEGER (0..MAX)
```

```
cRLNumber EXTENSION ::= {
    SYNTAX                  CRLNumber
    IDENTIFIED BY       id-ce-cRLNumber }
CRLNumber ::= INTEGER (0..MAX)

reasonCode EXTENSION ::= {
    SYNTAX              CRLReason
    IDENTIFIED BY       id-ce-reasonCode }
CRLReason ::= ENUMERATED {
    unspecified                 (0),
    keyCompromise               (1),
    cACompromise                (2),
    affiliationChanged          (3),
    superseded                  (4),
    cessationOfOperation        (5),
    certificateHold             (6),
    removeFromCRL               (8),
    privilegeWithdrawn          (9),
    aaCompromise                (10) }

holdInstructionCode EXTENSION ::= {
    SYNTAX              HoldInstruction
    IDENTIFIED BY       id-ce-instructionCode }
HoldInstruction ::= OBJECT IDENTIFIER

invalidityDate EXTENSION ::= {
    SYNTAX              GeneralizedTime
    IDENTIFIED BY       id-ce-invalidityDate }

crlScope EXTENSION ::= {
    SYNTAX                  CRLScopeSyntax
    IDENTIFIED BY           id-ce-cRLScope }
CRLScopeSyntax ::=          SEQUENCE SIZE (1..MAX) OF PerAuthorityScope
PerAuthorityScope ::= SEQUENCE {
    authorityName               [0]   GeneralName OPTIONAL,
    distributionPoint           [1]   DistributionPointName OPTIONAL,
    onlyContains                [2]   OnlyCertificateTypes OPTIONAL,
    onlySomeReasons             [4]   ReasonFlags OPTIONAL,
    serialNumberRange           [5]   NumberRange OPTIONAL,
    subjectKeyIdRange           [6]   NumberRange OPTIONAL,
    nameSubtrees                [7]   GeneralNames OPTIONAL,
    baseRevocationInfo          [9]   BaseRevocationInfo OPTIONAL
    }
OnlyCertificateTypes ::= BIT STRING {
    user            (0),
    authority       (1),
    attribute       (2) }
NumberRange ::= SEQUENCE {
    startingNumber      [0]         INTEGER OPTIONAL,
    endingNumber        [1]         INTEGER OPTIONAL,
    modulus                         INTEGER OPTIONAL }
BaseRevocationInfo ::= SEQUENCE {
    cRLStreamIdentifier         [0]   CRLStreamIdentifier    OPTIONAL,
    cRLNumber                   [1]   CRLNumber,
    baseThisUpdate              [2]   GeneralizedTime }

statusReferrals EXTENSION  ::= {
    SYNTAX              StatusReferrals
    IDENTIFIED BY       id-ce-statusReferrals }
StatusReferrals ::= SEQUENCE SIZE (1..MAX) OF StatusReferral
StatusReferral  ::=  CHOICE {
    cRLReferral         [0]         CRLReferral,
    otherReferral       [1]         INSTANCE OF OTHER-REFERRAL}
CRLReferral ::= SEQUENCE  {
    issuer              [0]         GeneralName OPTIONAL,
    location            [1]         GeneralName OPTIONAL,
    deltaRefInfo        [2]         DeltaRefInfo OPTIONAL,
    cRLScope                        CRLScopeSyntax,
```

```
    lastUpdate          [3]     GeneralizedTime OPTIONAL,
    lastChangedCRL      [4]     GeneralizedTime OPTIONAL}
DeltaRefInfo ::= SEQUENCE {
    deltaLocation       GeneralName,
    lastDelta           GeneralizedTime OPTIONAL }
OTHER-REFERRAL ::= TYPE-IDENTIFIER

cRLStreamIdentifier EXTENSION    ::= {
    SYNTAX              CRLStreamIdentifier
    IDENTIFIED BY       id-ce-cRLStreamIdentifier }

CRLStreamIdentifier ::= INTEGER (0..MAX)

orderedList EXTENSION    ::= {
    SYNTAX              OrderedListSyntax
    IDENTIFIED BY       id-ce-orderedList }
OrderedListSyntax ::= ENUMERATED {
ascSerialNum      (0),
ascRevDate        (1) }

deltaInfo EXTENSION  ::=  {
    SYNTAX              DeltaInformation
    IDENTIFIED BY       id-ce-deltaInfo }
DeltaInformation  ::=  SEQUENCE {
    deltaLocation       GeneralName,
    nextDelta           GeneralizedTime OPTIONAL }

cRLDistributionPoints EXTENSION ::= {
    SYNTAX              CRLDistPointsSyntax
    IDENTIFIED BY       id-ce-cRLDistributionPoints }
CRLDistPointsSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
DistributionPoint ::= SEQUENCE {
    distributionPoint   [0]     DistributionPointName OPTIONAL,
    reasons             [1]     ReasonFlags OPTIONAL,
    cRLIssuer           [2]     GeneralNames OPTIONAL }
DistributionPointName ::= CHOICE {
    fullName                    [0]  GeneralNames,
    nameRelativeToCRLIssuer     [1]  RelativeDistinguishedName }
ReasonFlags ::= BIT STRING {
    unused                  (0),
    keyCompromise           (1),
    cACompromise            (2),
    affiliationChanged      (3),
    superseded              (4),
    cessationOfOperation    (5),
    certificateHold         (6),
    privilegeWithdrawn      (7),
    aACompromise            (8) }

issuingDistributionPoint EXTENSION  ::= {
    SYNTAX IssuingDistPointSyntax
    IDENTIFIED BY id-ce-issuingDistributionPoint }

IssuingDistPointSyntax ::= SEQUENCE {
    -- If onlyContainsUserPublicKeyCerts and onlyContainsCACerts are both FALSE,
    -- the CRL covers both certificate types
                                يحتوي فقط على شهادات المفتاح العمومي للمستعمل ويحتوي فقط على شهادات
                                إذا كانت المكونتان --
                                سلطة إصدار الشهادة موضوعتين كلتيهما على "خاطئة"، تكون القائمة CRL تغطي كلا النمطين --

    distributionPoint               [0] DistributionPointName OPTIONAL,
    onlyContainsUserPublicKeyCerts      [1] BOOLEAN DEFAULT FALSE,
    onlyContainsCACerts             [2] BOOLEAN DEFAULT FALSE,
    onlySomeReasons                 [3] ReasonFlags OPTIONAL,
    indirectCRL                     [4] BOOLEAN DEFAULT FALSE }
certificateIssuer EXTENSION ::= {
    SYNTAX              GeneralNames
    IDENTIFIED BY       id-ce-certificateIssuer }
```

```
deltaCRLIndicator EXTENSION ::= {
    SYNTAX              BaseCRLNumber
    IDENTIFIED BY       id-ce-deltaCRLIndicator }
BaseCRLNumber ::= CRLNumber

toBeRevoked  EXTENSION  ::= {
    SYNTAX          ToBeRevokedSyntax
    IDENTIFIED BYid-ce-toBeRevoked }

ToBeRevokedSyntax::=      SEQUENCE SIZE(1..MAX) OF ToBeRevokedGroup

ToBeRevokedGroup    ::=   SEQUENCE {
    certificateIssuer     [0]   GeneralName OPTIONAL,
    reasonInfo            [1]   ReasonInfo    OPTIONAL,
    revocationTime              GeneralizedTime,
    certificateGroup            CertificateGroup }

ReasonInfo                ::=   SEQUENCE {
    reasonCode                  CRLReason,
    holdInstructionCode         HoldInstruction OPTIONAL }

CertificateGroup   ::=   CHOICE {
    serialNumbers         [0]   CertificateSerialNumbers,
    serialNumberRange[1]   CertificateGroupNumberRange,
    nameSubtree           [2]   GeneralName }

CertificateGroupNumberRange ::= SEQUENCE {
    startingNumber        [0]   INTEGER,
    endingNumber          [1]   INTEGER }

CertificateSerialNumbers ::=      SEQUENCE SIZE(1..MAX) OF CertificateSerialNumber

revokedGroups  EXTENSION  ::= {
    SYNTAX          RevokedGroupsSyntax
    IDENTIFIED BYid-ce-RevokedGroups }

RevokedGroupsSyntax ::=  SEQUENCE SIZE (1..MAX) OF RevokedGroup

RevokedGroup ::=SEQUENCE {
    certificateIssuer           [0]   GeneralName OPTIONAL,
    reasonInfo                  [1]   ReasonInfo OPTIONAL,
    invalidityDate              [2]   GeneralizedTime OPTIONAL,
    revokedcertificateGroup[3]   RevokedCertificateGroup }

RevokedCertificateGroup ::=      CHOICE {
    serialNumberRangeNumberRange,
    nameSubtree         GeneralName }

expiredCertsOnCRL EXTENSION  ::= {
    SYNTAX   ExpiredCertsOnCRL
    IDENTIFIED BYid-ce-expiredCertsOnCRL }

ExpiredCertsOnCRL    ::= GeneralizedTime
baseUpdateTime EXTENSION    ::= {
    SYNTAX              GeneralizedTime
    IDENTIFIED BY       id-ce-baseUpdateTime }

freshestCRL EXTENSION    ::= {
    SYNTAX              CRLDistPointsSyntax
    IDENTIFIED BY       id-ce-freshestCRL }

aAissuingDistributionPoint EXTENSION ::= {
    SYNTAX AAIssuingDistPointSyntax
    IDENTIFIED BY id-ce-aAissuingDistributionPoint }

AAIssuingDistPointSyntax ::= SEQUENCE {
    distributionPoint                 [ 0 ] DistributionPointName OPTIONAL,
    onlySomeReasons                   [ 1 ] ReasonFlags OPTIONAL,
    indirectCRL                       [ 2 ] BOOLEAN DEFAULT FALSE,
    containsUserAttributeCerts        [ 3 ] BOOLEAN DEFAULT TRUE,
```

```
    containsAACerts                 [ 4 ] BOOLEAN DEFAULT TRUE,
    containsSOAPublicKeyCerts       [ 5 ] BOOLEAN DEFAULT TRUE }

inhibitAnyPolicy   EXTENSION   ::= {
    SYNTAX         SkipCerts
IDENTIFIED BY      id-ce-inhibitAnyPolicy }
```

-- PKI matching rules -- *-- قواعد مواءمة البنية PKI --*

```
certificateExactMatch MATCHING-RULE ::= {
    SYNTAX         CertificateExactAssertion
    ID             id-mr-certificateExactMatch }
CertificateExactAssertion ::= SEQUENCE {
    serialNumber       CertificateSerialNumber,
    issuer             Name }

certificateMatch MATCHING-RULE ::= {
    SYNTAX         CertificateAssertion
    ID             id-mr-certificateMatch }

CertificateAssertion ::= SEQUENCE {
    serialNumber           [0] CertificateSerialNumber      OPTIONAL,
    issuer                 [1] Name                         OPTIONAL,
    subjectKeyIdentifier   [2] SubjectKeyIdentifier         OPTIONAL,
    authorityKeyIdentifier [3] AuthorityKeyIdentifier       OPTIONAL,
    certificateValid       [4] Time                         OPTIONAL,
    privateKeyValid        [5] GeneralizedTime              OPTIONAL,
    subjectPublicKeyAlgID  [6] OBJECT IDENTIFIER            OPTIONAL,
    keyUsage               [7] KeyUsage                     OPTIONAL,
    subjectAltName         [8] AltNameType                  OPTIONAL,
    policy                 [9] CertPolicySet                OPTIONAL,
    pathToName             [10] Name                        OPTIONAL,
    subject                [11]  Name                       OPTIONAL,
    nameConstraints        [12]  NameConstraintsSyntax      OPTIONAL }

AltNameType ::= CHOICE {
    builtinNameForm    ENUMERATED {
          rfc822Name                (1),
          dNSName                   (2),
          x400Address               (3),
          directoryName             (4),
          ediPartyName              (5),
          uniformResourceIdentifier (6),
          iPAddress                 (7),
          registeredId              (8) },
    otherNameForm      OBJECT IDENTIFIER }

CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId

certificatePairExactMatch MATCHING-RULE    ::=   {
    SYNTAX         CertificatePairExactAssertion
    ID             id-mr-certificatePairExactMatch }

CertificatePairExactAssertion ::= SEQUENCE {
    issuedToThisCAAssertion       [0] CertificateExactAssertion OPTIONAL,
    issuedByThisCAAssertion       [1] CertificateExactAssertion OPTIONAL }
    ( WITH COMPONENTS             {..., issuedToThisCAAssertion PRESENT} |
      WITH COMPONENTS             {..., issuedByThisCAAssertion PRESENT} )

certificatePairMatch MATCHING-RULE ::={
    SYNTAX         CertificatePairAssertion
    ID             id-mr-certificatePairMatch }

CertificatePairAssertion ::= SEQUENCE {
    issuedToThisCAAssertion    [0] CertificateAssertion OPTIONAL,
    issuedByThisCAAssertion    [1] CertificateAssertion OPTIONAL }
    ( WITH COMPONENTS          {..., issuedToThisCAAssertion PRESENT} |
      WITH COMPONENTS          {..., issuedByThisCAAssertion PRESENT} )
```

```
certificateListExactMatch MATCHING-RULE    ::=   {
    SYNTAX          CertificateListExactAssertion
    ID              id-mr-certificateListExactMatch }

CertificateListExactAssertion ::= SEQUENCE {
    issuer                  Name,
    thisUpdate              Time,
    distributionPoint       DistributionPointName OPTIONAL }

certificateListMatch MATCHING-RULE ::= {
    SYNTAX          CertificateListAssertion
    ID              id-mr-certificateListMatch }

CertificateListAssertion ::= SEQUENCE {
    issuer                          Name            OPTIONAL,
    minCRLNumber            [0]     CRLNumber       OPTIONAL,
    maxCRLNumber            [1]     CRLNumber       OPTIONAL,
    reasonFlags                     ReasonFlags     OPTIONAL,
    dateAndTime                     Time            OPTIONAL,
    distributionPoint       [2]     DistributionPointName OPTIONAL,
    authorityKeyIdentifier  [3]     AuthorityKeyIdentifier OPTIONAL}

algorithmIdentifierMatch MATCHING-RULE     ::=   {
    SYNTAX          AlgorithmIdentifier
    ID              id-mr-algorithmIdentifierMatch }

policyMatch MATCHING-RULE   ::= {
    SYNTAX          PolicyID
    ID              id-mr-policyMatch }

pkiPathMatch MATCHING-RULE  ::= {
SYNTAX      PkiPathMatchSyntax
ID          id-mr-pkiPathMatch }

PkiPathMatchSyntax    ::= SEQUENCE {
firstIssuer         Name,
lastSubject         Name }

enhancedCertificateMatch MATCHING-RULE  ::= {
    SYNTAX  EnhancedCertificateAssertion
    ID      id-mr-enhancedCertificateMatch }

EnhancedCertificateAssertion  ::= SEQUENCE {
    serialNumber            [0]  CertificateSerialNumber    OPTIONAL,
    issuer                  [1]  Name                       OPTIONAL,
    subjectKeyIdentifier    [2]  SubjectKeyIdentifier       OPTIONAL,
    authorityKeyIdentifier  [3]  AuthorityKeyIdentifier     OPTIONAL,
    certificateValid        [4]  Time                       OPTIONAL,
    privateKeyValid         [5]  GeneralizedTime            OPTIONAL,
    subjectPublicKeyAlgID   [6]  OBJECT IDENTIFIER          OPTIONAL,
    keyUsage                [7]  KeyUsage                   OPTIONAL,
    subjectAltName          [8]  AltName                    OPTIONAL,
    policy                  [9]  CertPolicySet              OPTIONAL,
    pathToName              [10] GeneralNames               OPTIONAL,
    subject                 [11] Name                       OPTIONAL,
    nameConstraints         [12] NameConstraintsSyntax      OPTIONAL
}

(ALL EXCEPT ({-- none; at least one component shall be present --}))      -- لا شيء، توجد مكوّنة واحدة على الأقل --

AltName  ::= SEQUENCE {
        altnameType     AltNameType,
        altNameValue    GeneralName OPTIONAL }

-- Object identifier assignments --                                      -- إسنادات معرّف هوية الموضوع --

id-ce-subjectDirectoryAttributes        OBJECT IDENTIFIER   ::=  {id-ce 9}
id-ce-subjectKeyIdentifier              OBJECT IDENTIFIER   ::=  {id-ce 14}
id-ce-keyUsage                          OBJECT IDENTIFIER   ::=  {id-ce 15}
```

```
id-ce-privateKeyUsagePeriod          OBJECT IDENTIFIER  ::=  {id-ce 16}
id-ce-subjectAltName                 OBJECT IDENTIFIER  ::=  {id-ce 17}
id-ce-issuerAltName                  OBJECT IDENTIFIER  ::=  {id-ce 18}
id-ce-basicConstraints               OBJECT IDENTIFIER  ::=  {id-ce 19}
id-ce-cRLNumber                      OBJECT IDENTIFIER  ::=  {id-ce 20}
id-ce-reasonCode                     OBJECT IDENTIFIER  ::=  {id-ce 21}
id-ce-instructionCode                OBJECT IDENTIFIER  ::=  {id-ce 23}
id-ce-invalidityDate                 OBJECT IDENTIFIER  ::=  {id-ce 24}
id-ce-deltaCRLIndicator              OBJECT IDENTIFIER  ::=  {id-ce 27}
id-ce-issuingDistributionPoint       OBJECT IDENTIFIER  ::=  {id-ce 28}
id-ce-certificateIssuer              OBJECT IDENTIFIER  ::=  {id-ce 29}
id-ce-nameConstraint                 OBJECT IDENTIFIER  ::=  {id-ce 30 1}

id-ce-cRLDistributionPoints          OBJECT IDENTIFIER  ::=  {id-ce 31}
id-ce-certificatePolicies            OBJECT IDENTIFIER  ::=  {id-ce 32}
id-ce-policyMappings                 OBJECT IDENTIFIER  ::=  {id-ce 33}
-- deprecated                        OBJECT IDENTIFIER  ::=  {id-ce 34}
id-ce-authorityKeyIdentifier         OBJECT IDENTIFIER  ::=  {id-ce 35}
id-ce-policyConstraints              OBJECT IDENTIFIER  ::=  {id-ce 36}
id-ce-extKeyUsage                    OBJECT IDENTIFIER  ::=  {id-ce 37}
id-ce-cRLStreamIdentifier            OBJECT IDENTIFIER  ::=  {id-ce 40}
id-ce-cRLScope                       OBJECT IDENTIFIER  ::=  {id-ce 44}
id-ce-statusReferrals                OBJECT IDENTIFIER  ::=  {id-ce 45}
id-ce-freshestCRL                    OBJECT IDENTIFIER  ::=  {id-ce 46}
id-ce-orderedList                    OBJECT IDENTIFIER  ::=  {id-ce 47}
id-ce-baseUpdateTime                 OBJECT IDENTIFIER  ::=  {id-ce 51}
id-ce-deltaInfo                      OBJECT IDENTIFIER  ::=  {id-ce 53}
id-ce-inhibitAnyPolicy               OBJECT IDENTIFIER  ::=  {id-ce 54}
id-ce-toBeRevoked                    OBJECT IDENTIFIER  ::=  {id-ce 58}
id-ce-RevokedGroups                  OBJECT IDENTIFIER  ::=  {id-ce 59}
id-ce-expiredCertsOnCRL              OBJECT IDENTIFIER  ::=  {id-ce 60}
id-ce-aAissuingDistributionPoint     OBJECT IDENTIFIER  ::=  {id-ce 63}

-- matching rule OIDs --                                  -- قواعد مواءمة معرّفات هوية الموضوع --

id-mr-certificateExactMatch          OBJECT IDENTIFIER  ::=  {id-mr 34}
id-mr-certificateMatch               OBJECT IDENTIFIER  ::=  {id-mr 35}
id-mr-certificatePairExactMatch      OBJECT IDENTIFIER  ::=  {id-mr 36}
id-mr-certificatePairMatch           OBJECT IDENTIFIER  ::=  {id-mr 37}
id-mr-certificateListExactMatch      OBJECT IDENTIFIER  ::=  {id-mr 38}
id-mr-certificateListMatch           OBJECT IDENTIFIER  ::=  {id-mr 39}
id-mr-algorithmIdentifierMatch       OBJECT IDENTIFIER  ::=  {id-mr 40}
id-mr-policyMatch                    OBJECT IDENTIFIER  ::=  {id-mr 60}
id-mr-pkiPathMatch                   OBJECT IDENTIFIER  ::=  {id-mr 62}
id-mr-enhancedCertificateMatch       OBJECT IDENTIFIER  ::=  {id-mr 65}

-- The following OBJECT IDENTIFIERS are not used by this Specification:   -- لا تستعمل هذه المواصفة معرّفات هوية الموضوع التالية:
-- {id-ce 2}, {id-ce 3}, {id-ce 4}, {id-ce 5}, {id-ce 6}, {id-ce 7},
-- {id-ce 8}, {id-ce 10}, {id-ce 11}, {id-ce 12}, {id-ce 13},
-- {id-ce 22}, {id-ce 25}, {id-ce 26}, {id-ce 30}
END                                                          النهاية
```

-- A.3 Attribute Certificate Framework module -- 3.A وحدة إطار شهادة النعت

```
AttributeCertificateDefinitions {joint-iso-itu-t ds(5) module(1) attributeCertificateDefinitions(32) 5}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL --

IMPORTS
    id-at, id-ce, id-mr, informationFramework, authenticationFramework,
        selectedAttributeTypes, upperBounds, id-oc, certificateExtensions
        FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
        usefulDefinitions(0) 5}
```

```
    Name, RelativeDistinguishedName, ATTRIBUTE, Attribute,
        MATCHING-RULE, AttributeType, OBJECT-CLASS, top
        FROM InformationFramework informationFramework

    CertificateSerialNumber, CertificateList, AlgorithmIdentifier,
        EXTENSION, SIGNED{}, InfoSyntax, PolicySyntax, Extensions, Certificate
        FROM AuthenticationFramework authenticationFramework

    DirectoryString{}, TimeSpecification, UniqueIdentifier
        FROM SelectedAttributeTypes selectedAttributeTypes

    GeneralName, GeneralNames, NameConstraintsSyntax, certificateListExactMatch
        FROM CertificateExtensions certificateExtensions

    ub-name
        FROM UpperBounds upperBounds

    UserNotice
        FROM PKIX1Implicit93 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5)
pkix(7) id-mod(0) id-pkix1-implicit-93(4)}

    ORAddress
        FROM MTSAbstractService {joint-iso-itu-t mhs(6) mts(3)
        modules(0) mts-abstract-service(1) version-1999 (1) } ;

-- Unless explicitly noted otherwise, there is no significance to the ordering      -- لا يوجد معنى لترتيب مكونات التتابع من الموجود
-- of components of a SEQUENCE OF construct in this Specification.                  -- في هذه المواصفة، ما لم يشر إلى غير ذلك صراحة.

-- attribute certificate constructs --                                             -- بنى شهادة النعت --

AttributeCertificate ::= SIGNED {AttributeCertificateInfo}
AttributeCertificateInfo ::= SEQUENCE
    {
    version                 AttCertVersion, -- version is v2        -- الصيغة هي v2
    holder                  Holder,
    issuer                  AttCertIssuer,
    signature               AlgorithmIdentifier,
    serialNumber            CertificateSerialNumber,
    attrCertValidityPeriod  AttCertValidityPeriod,
    attributes              SEQUENCE OF Attribute,
    issuerUniqueID          UniqueIdentifier    OPTIONAL,
    extensions              Extensions          OPTIONAL
    }

AttCertVersion     ::= INTEGER { v2(1) }

Holder    ::=   SEQUENCE
          {
          baseCertificateID     [0] IssuerSerial            OPTIONAL,
               -- the issuer and serial number of  the holder's Public Key Certificate
                                                  -- مُصدر ورقم تسلسل شهادة المفتاح العمومي للحامل
          entityName            [1] GeneralNames            OPTIONAL,
               -- the name of the entity or role                -- اسم الكيان أو الدور
          objectDigestInfo      [2] ObjectDigestInfo        OPTIONAL
               -- used to directly authenticate the holder, e.g., an executable
-- at least one of baseCertificateID, entityName or objectDigestInfo shall be present --}
                    -- يستعمل لاستيقان الحامل مباشرة، أي يجب أن يكون موجوداً واحد على الأقل يمكن تنفيذه من: baseCertificateID أو entityName
                                                  {-- أو objectDigestInfo --

ObjectDigestInfo    ::= SEQUENCE {
    digestedObjectType  ENUMERATED {
        publicKey           (0),
        publicKeyCert       (1),
        otherObjectTypes    (2) },
    otherObjectTypeID       OBJECT IDENTIFIER  OPTIONAL,
    digestAlgorithm         AlgorithmIdentifier,
    objectDigest            BIT STRING }
```

```
AttCertIssuer ::=   [0]   SEQUENCE {
    issuerName              GeneralNames  OPTIONAL,
    baseCertificateID   [0]   IssuerSerial  OPTIONAL,
    objectDigestInfo    [1]   ObjectDigestInfo  OPTIONAL }

-- At least one component shall be present                    -- مكوّنة واحدة على الأقل يجب أن تكون موجودة
    ( WITH COMPONENTS { ..., issuerName  PRESENT } |
      WITH COMPONENTS { ..., baseCertificateID  PRESENT } |
      WITH COMPONENTS { ..., objectDigestInfo PRESENT } )

IssuerSerial  ::=  SEQUENCE {
    issuer          GeneralNames,
    serial          CertificateSerialNumber,
    issuerUID       UniqueIdentifier OPTIONAL }
AttCertValidityPeriod  ::= SEQUENCE {
    notBeforeTime       GeneralizedTime,
    notAfterTime        GeneralizedTime }
AttributeCertificationPath  ::=  SEQUENCE {
    attributeCertificate            AttributeCertificate,
    acPath                          SEQUENCE OF ACPathData OPTIONAL }
ACPathData  ::=  SEQUENCE {
    certificate           [0]  Certificate  OPTIONAL,
    attributeCertificate  [1]  AttributeCertificate  OPTIONAL }

PrivilegePolicy     ::=   OBJECT IDENTIFIER

-- privilege attributes --                                    -- نعوت الامتياز --

role    ATTRIBUTE::= {
        WITH SYNTAX         RoleSyntax
        ID                  id-at-role }

xmlPrivilegeInfo   ATTRIBUTE  ::= {
    WITH SYNTAX UTF8String --contains XML-encoded privilege information
    ID              id-at-xMLPrivilegeInfo }

RoleSyntax   ::=   SEQUENCE {
    roleAuthority       [0]       GeneralNames OPTIONAL,
    roleName            [1]       GeneralName }

-- PMI object classes --                                      --أصناف موضوعات البنية PMI--

pmiUser OBJECT-CLASS ::= {
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {attributeCertificateAttribute}
    ID              id-oc-pmiUser
    }

pmiAA OBJECT-CLASS ::= {
-- a PMI AA
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {aACertificate |
                     attributeCertificateRevocationList |
                     attributeAuthorityRevocationList}
    ID              id-oc-pmiAA
    }

pmiSOA OBJECT-CLASS ::= {  -- a PMI Source of Authority       -- مَصْدر السلطة للبنية PMI

    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {attributeCertificateRevocationList |
                     attributeAuthorityRevocationList |
                     attributeDescriptorCertificate}
```

```
    ID                  id-oc-pmiSOA
    }


attCertCRLDistributionPt    OBJECT-CLASS ::= {
    SUBCLASS OF             {top}
    KIND                    auxiliary
    MAY CONTAIN             { attributeCertificateRevocationList |
                            attributeAuthorityRevocationList }
    ID                      id-oc-attCertCRLDistributionPts
    }

pmiDelegationPath           OBJECT-CLASS   ::= {
    SUBCLASS OF             {top}
    KIND                    auxiliary
    MAY CONTAIN             { delegationPath }
    ID                      id-oc-pmiDelegationPath }

privilegePolicy             OBJECT-CLASS   ::= {
    SUBCLASS OF             {top}
    KIND                    auxiliary
    MAY CONTAIN             {privPolicy }
    ID                      id-oc-privilegePolicy }
protectedPrivilegePolicy    OBJECT-CLASS   ::= {
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {protPrivPolicy }
    ID              id-oc-protectedPrivilegePolicy }
```

-- PMI directory attributes -- *-- النعوت الدليلية للبنية PMI --*

```
attributeCertificateAttribute       ATTRIBUTE  ::= {
    WITH SYNTAX                     AttributeCertificate
    EQUALITY MATCHING RULE          attributeCertificateExactMatch
    ID                              id-at-attributeCertificate }

aACertificate                       ATTRIBUTE    ::=  {
    WITH SYNTAX                     AttributeCertificate
    EQUALITY MATCHING RULE          attributeCertificateExactMatch
    ID                              id-at-aACertificate }

attributeDescriptorCertificate      ATTRIBUTE  ::= {
    WITH SYNTAX                     AttributeCertificate
    EQUALITY MATCHING RULE          attributeCertificateExactMatch
    ID                              id-at-attributeDescriptorCertificate }

attributeCertificateRevocationList  ATTRIBUTE ::= {
    WITH SYNTAX                     CertificateList
    EQUALITY MATCHING RULE          certificateListExactMatch
    ID                              id-at-attributeCertificateRevocationList}

attributeAuthorityRevocationList    ATTRIBUTE    ::= {
    WITH SYNTAX                     CertificateList
    EQUALITY MATCHING RULE          certificateListExactMatch
    ID                              id-at-attributeAuthorityRevocationList }

delegationPath          ATTRIBUTE ::= {
    WITH SYNTAX         AttCertPath
    ID                  id-at-delegationPath }
AttCertPath   ::=  SEQUENCE OF AttributeCertificate
privPolicy              ATTRIBUTE ::= {
    WITH SYNTAX         PolicySyntax
    ID                  id-at-privPolicy }
protPrivPolicy     ATTRIBUTE   ::= {
    WITH SYNTAX                     AttributeCertificate
    EQUALITY MATCHING RULE          attributeCertificateExactMatch
    ID                              id-at-protPrivPolicy }
xmlPrivPolicyATTRIBUTE   ::= {
    WITH SYNTAX UTF8String --contains XML-encoded privilege policy information
```

```
    ID          id-at-xMLPprotPrivPolicy }          -- تحتوي على معلومات عن سياسة الامتياز المشفر XML
```

-- Attribute certificate extensions and matching rules -- -- التوسعات وقواعد المواءمة في شهادة النعت --

```
attributeCertificateExactMatch MATCHING-RULE ::= {
    SYNTAX          AttributeCertificateExactAssertion
    ID              id-mr-attributeCertificateExactMatch }

AttributeCertificateExactAssertion ::=    SEQUENCE {
    serialNumber        CertificateSerialNumber,
    issuer              AttCertIssuer
    }

attributeCertificateMatch MATCHING-RULE ::= {
    SYNTAX          AttributeCertificateAssertion
    ID              id-mr-attributeCertificateMatch }

AttributeCertificateAssertion ::= SEQUENCE {
    holder              [0]  CHOICE {
        baseCertificateID   [0]  IssuerSerial,
        holderName              [1]  GeneralNames} OPTIONAL,
    issuer              [1]  GeneralNames OPTIONAL,
    attCertValidity     [2]  GeneralizedTime OPTIONAL,
    attType             [3]  SET OF AttributeType OPTIONAL}
```

-- At least one component of the sequence shall be present -- مكوّنة واحدة من التتابع على الأقل يجب أن تكون موجودة

```
holderIssuerMatch MATCHING-RULE ::= {
    SYNTAX          HolderIssuerAssertion
    ID              id-mr-holderIssuerMatch }
HolderIssuerAssertion ::=  SEQUENCE {
    holder          [0]         Holder  OPTIONAL,
    issuer          [1]         AttCertIssuer OPTIONAL
    }

delegationPathMatch MATCHING-RULE ::= {
    SYNTAX          DelMatchSyntax
    ID              id-mr-delegationPathMatch }

DelMatchSyntax  ::=  SEQUENCE {
    firstIssuer     AttCertIssuer,
    lastHolder      Holder }

sOAIdentifier EXTENSION ::= {
    SYNTAX              NULL
    IDENTIFIED BY       id-ce-sOAIdentifier }

sOAIdentifierMatch MATCHING-RULE ::= {
    SYNTAX                  NULL
    ID                      id-mr-sOAIdentifierMatch }

authorityAttributeIdentifier EXTENSION ::=
    {
    SYNTAX              AuthorityAttributeIdentifierSyntax
    IDENTIFIED BY       { id-ce-authorityAttributeIdentifier } }

AuthorityAttributeIdentifierSyntax  ::=    SEQUENCE SIZE (1..MAX) OF AuthAttId

AuthAttId     ::=  IssuerSerial
authAttIdMatch MATCHING-RULE ::= {
    SYNTAX          AuthorityAttributeIdentifierSyntax
    ID              id-mr-authAttIdMatch }

roleSpecCertIdentifier EXTENSION ::=
    {
    SYNTAX              RoleSpecCertIdentifierSyntax
    IDENTIFIED BY       { id-ce-roleSpecCertIdentifier } }
RoleSpecCertIdentifierSyntax ::= SEQUENCE SIZE (1..MAX) OF RoleSpecCertIdentifier
```

```
RoleSpecCertIdentifier  ::= SEQUENCE {
    roleName                [0]  GeneralName,
    roleCertIssuer          [1]  GeneralName,
    roleCertSerialNumber    [2]  CertificateSerialNumber    OPTIONAL,
    roleCertLocator         [3]  GeneralNames               OPTIONAL }

roleSpecCertIdMatch MATCHING-RULE  ::= {
    SYNTAX        RoleSpecCertIdentifierSyntax
    ID            id-mr-roleSpecCertIdMatch }

basicAttConstraints EXTENSION ::=
    {
        SYNTAX              BasicAttConstraintsSyntax
        IDENTIFIED BY       { id-ce-basicAttConstraints }
    }
BasicAttConstraintsSyntax ::= SEQUENCE
    {
        authority           BOOLEAN DEFAULT FALSE,
        pathLenConstraint   INTEGER (0..MAX) OPTIONAL
    }

basicAttConstraintsMatch MATCHING-RULE  ::= {
    SYNTAX        BasicAttConstraintsSyntax
    ID            id-mr-basicAttConstraintsMatch }

delegatedNameConstraints EXTENSION ::= {
    SYNTAX              NameConstraintsSyntax
    IDENTIFIED BY       id-ce-delegatedNameConstraints }

delegatedNameConstraintsMatch MATCHING-RULE  ::= {
    SYNTAX        NameConstraintsSyntax
    ID            id-mr-delegatedNameConstraintsMatch}

timeSpecification EXTENSION  ::=  {
    SYNTAX              TimeSpecification
    IDENTIFIED BY       id-ce-timeSpecification }

timeSpecificationMatch MATCHING-RULE  ::= {
    SYNTAX        TimeSpecification
    ID            id-mr-timeSpecMatch }

acceptableCertPolicies EXTENSION ::= {
    SYNTAX              AcceptableCertPoliciesSyntax
    IDENTIFIED BY       id-ce-acceptableCertPolicies }
AcceptableCertPoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId
CertPolicyId ::= OBJECT IDENTIFIER

acceptableCertPoliciesMatch MATCHING-RULE  ::= {
    SYNTAX        AcceptableCertPoliciesSyntax
    ID            id-mr-acceptableCertPoliciesMatch }
attributeDescriptor EXTENSION  ::= {
    SYNTAX              AttributeDescriptorSyntax
    IDENTIFIED BY       {id-ce-attributeDescriptor } }

AttributeDescriptorSyntax  ::= SEQUENCE {
    identifier                  AttributeIdentifier,
    attributeSyntax             OCTET STRING (SIZE(1..MAX)),
    name                [0]     AttributeName   OPTIONAL,
    description         [1]     AttributeDescription    OPTIONAL,
    dominationRule              PrivilegePolicyIdentifier}

AttributeIdentifier  ::= ATTRIBUTE.&id({AttributeIDs})
AttributeIDs ATTRIBUTE  ::= {...}
AttributeName  ::= UTF8String(SIZE(1..MAX))
AttributeDescription  ::= UTF8String(SIZE(1..MAX))

PrivilegePolicyIdentifier     ::=  SEQUENCE {
    privilegePolicy             PrivilegePolicy,
    privPolSyntax               InfoSyntax }
```

```
attDescriptor MATCHING-RULE  ::= {
    SYNTAX          AttributeDescriptorSyntax
    ID              id-mr-attDescriptorMatch }
userNotice  EXTENSION  ::= {
    SYNTAX              SEQUENCE SIZE (1..MAX) OF UserNotice
    IDENTIFIED BY       id-ce-userNotice }

targetingInformation  EXTENSION  ::= {
    SYNTAX              SEQUENCE SIZE (1..MAX) OF Targets
    IDENTIFIED BY       id-ce-targetInformation }

Targets  ::=  SEQUENCE SIZE (1..MAX) OF Target

Target::=CHOICE {
    targetName          [0]     GeneralName,
    targetGroup         [1]     GeneralName,
    targetCert          [2]     TargetCert }

TargetCert    ::=  SEQUENCE {
    targetCertificate   IssuerSerial,
    targetName          GeneralName OPTIONAL,
    certDigestInfo      ObjectDigestInfo OPTIONAL }

noRevAvail EXTENSION ::=  {
    SYNTAX              NULL
    IDENTIFIED BY       id-ce-noRevAvail }

acceptablePrivilegePolicies EXTENSION ::= {
    SYNTAX              AcceptablePrivilegePoliciesSyntax
    IDENTIFIED BY       id-ce-acceptablePrivilegePolicies }

AcceptablePrivilegePoliciesSyntax  ::=    SEQUENCE SIZE (1..MAX) OF PrivilegePolicy

indirectIssuer EXTENSION ::= {
    SYNTAX          BOOLEAN
    IDENTIFIED BY       id-ce-indirectIssuer }

indirectIssuerMatch MATCHING-RULE  ::= {
    SYNTAX   BOOLEAN
    ID  id-mr-indirectIssuerMatch }

noAssertion EXTENSION ::= {
    SYNTAX NULL
    IDENTIFIED BY id-ce-noAssertion }

issuedOnBehalfOf EXTENSION ::= {
    SYNTAX GeneralName
    IDENTIFIED BY id-ce-issuedOnBehalfOf }
```

-- object identifier assignments -- *-- إسنادات معرّف هوية الموضوع --*

-- object classes -- *-- أصناف الموضوعات --*

```
id-oc-pmiUser                       OBJECT IDENTIFIER ::=   {id-oc 24}
id-oc-pmiAA                         OBJECT IDENTIFIER ::=   {id-oc 25}
id-oc-pmiSOA                        OBJECT IDENTIFIER ::=   {id-oc 26}
id-oc-attCertCRLDistributionPts     OBJECT IDENTIFIER ::=   {id-oc 27}
id-oc-privilegePolicy               OBJECT IDENTIFIER ::=   {id-oc 32}
id-oc-pmiDelegationPath             OBJECT IDENTIFIER ::=   {id-oc 33}
id-oc-protectedPrivilegePolicy      OBJECT IDENTIFIER ::=   {id-oc 34}
```

-- directory attributes -- *-- النعوت الدليلية --*

```
id-at-attributeCertificate              OBJECT IDENTIFIER ::=   {id-at 58}
id-at-attributeCertificateRevocationList OBJECT IDENTIFIER ::=  {id-at 59}
id-at-aACertificate                     OBJECT IDENTIFIER ::=   {id-at 61}
```

```
id-at-attributeDescriptorCertificate      OBJECT IDENTIFIER ::=  {id-at 62}
id-at-attributeAuthorityRevocationList    OBJECT IDENTIFIER ::=  {id-at 63}
id-at-privPolicy                          OBJECT IDENTIFIER ::=  {id-at 71}
id-at-role                                OBJECT IDENTIFIER ::=  {id-at 72}
id-at-delegationPath                      OBJECT IDENTIFIER ::=  {id-at 73}
id-at-protPrivPolicy                      OBJECT IDENTIFIER ::=  {id-at 74}
id-at-xMLPrivilegeInfo                    OBJECT IDENTIFIER ::=  {id-at 75}
id-at-xMLPprotPrivPolicy                  OBJECT IDENTIFIER ::=  {id-at 76}

-- attribute certificate extensions --                          -- توسعات شهادة النعت --

id-ce-authorityAttributeIdentifier        OBJECT IDENTIFIER ::=  {id-ce 38}
id-ce-roleSpecCertIdentifier              OBJECT IDENTIFIER ::=  {id-ce 39}
id-ce-basicAttConstraints                 OBJECT IDENTIFIER ::=  {id-ce 41}
id-ce-delegatedNameConstraints            OBJECT IDENTIFIER ::=  {id-ce 42}
id-ce-timeSpecification                   OBJECT IDENTIFIER ::=  {id-ce 43}
id-ce-attributeDescriptor                 OBJECT IDENTIFIER ::=  {id-ce 48}
id-ce-userNotice                          OBJECT IDENTIFIER ::=  {id-ce 49}
id-ce-sOAIdentifier                       OBJECT IDENTIFIER ::=  {id-ce 50}
id-ce-acceptableCertPolicies              OBJECT IDENTIFIER ::=  {id-ce 52}
id-ce-targetInformation                   OBJECT IDENTIFIER ::=  {id-ce 55}
id-ce-noRevAvail                          OBJECT IDENTIFIER ::=  {id-ce 56}
id-ce-acceptablePrivilegePolicies         OBJECT IDENTIFIER ::=  {id-ce 57}
id-ce-indirectIssuer                      OBJECT IDENTIFIER ::=  {id-ce 61}
id-ce-noAssertion                         OBJECT IDENTIFIER ::=  {id-ce 62}
id-ce-issuedOnBehalfOf                    OBJECT IDENTIFIER ::=  {id-ce 64}

-- PMI matching rules --                                        --PMI قواعد المواءمة للبنية --

id-mr-attributeCertificateMatch           OBJECT IDENTIFIER ::=  {id-mr 42}
id-mr-attributeCertificateExactMatch      OBJECT IDENTIFIER ::=  {id-mr 45}
id-mr-holderIssuerMatch                   OBJECT IDENTIFIER ::=  {id-mr 46}
id-mr-authAttIdMatch                      OBJECT IDENTIFIER ::=  {id-mr 53}
id-mr-roleSpecCertIdMatch                 OBJECT IDENTIFIER ::=  {id-mr 54}
id-mr-basicAttConstraintsMatch            OBJECT IDENTIFIER ::=  {id-mr 55}
id-mr-delegatedNameConstraintsMatch       OBJECT IDENTIFIER ::=  {id-mr 56}
id-mr-timeSpecMatch                       OBJECT IDENTIFIER ::=  {id-mr 57}
id-mr-attDescriptorMatch                  OBJECT IDENTIFIER ::=  {id-mr 58}
id-mr-acceptableCertPoliciesMatch         OBJECT IDENTIFIER ::=  {id-mr 59}
id-mr-delegationPathMatch                 OBJECT IDENTIFIER ::=  {id-mr 61}
id-mr-sOAIdentifierMatch                  OBJECT IDENTIFIER ::=  {id-mr 66}
id-mr-indirectIssuerMatch                 OBJECT IDENTIFIER ::=  {id-mr 67}

END                                                              النهاية
```

الملحق B

قواعد توليد ومعالجة قوائم إبطال الشهادات (CRL)

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

1.B المدخل

يحتاج الطرف الواثق (مستعمل الشهادة) أن يكون قادراً على التحقق من الوضع القانوني لإبطال شهادة، لكي يحدد إن كان يمكنه الثقة بهذه الشهادة أم لا. وقائمة إبطال الشهادة (CRL) هي إحدى الآليات التي تستطيع الأطراف الواثقة الحصول منها على معلومات الإبطال. ويمكن استخدام آليات أخرى لهذا الغرض، غير أنها تقع خارج نطاق هذه المواصفة.

ويتطرق هذا الملحق إلى استخدام الأطراف الواثقة قوائم إبطال الشهادات للتحقق من الوضع القانوني لإبطال شهادة. ويمكن للسلطات المختلفة أن تعتمد سياسات متباينة بشأن إصدارها قوائم الإبطال. ففي بعض الحالات مثلاً يمكن لسلطة إصدار الشهادة أن ترخص لسلطة أخرى أن تصدر قائمة إبطال شهادات، فيما يخص الشهادات التي تصدرها هي. وقد تدمج بعض السلطات إبطال شهادات الكيان النهائي مع شهادات سلطة إصدار الشهادة في قائمة واحدة، بينما قد تعمل سلطات أخرى على فصل هذه الشهادة في قوائم منفصلة. وقد تلجأ بعض الإدارات إلى تجزيء مجموعة شهاداتها إلى مجموعات فرعية من قوائم إبطال الشهادات، بينما قد تصدر سلطات أخرى قوائم دلتا لتحيين قائمة بين الفترات المنتظمة لإصدار القائمة CRL. ونتيجة لذلك، تحتاج الأطراف الواثقة أن تكون قادرة على تحديد مجال تطبيق الشهادات CRL التي تستخرجها، لكي تتأكد من أن المتوفر عندها هو المجموعة الكاملة من معلومات الإبطال التي تغطي مجال تطبيق الشهادة المدروسة الخاص بدواعي الإبطال ذات الصلة، مع مراعاة السياسة التي تعمل بموجبها. ويقدم هذا الملحق آلية إلى الأطراف الواثقة من أجل تحديد مجال تطبيق الشهادات المستخرجة.

كتب هذا الملحق للتحقق من الوضع القانوني لإبطال شهادات المفتاح العمومي باستخدام قوائم إبطال الشهادات (CRL)، وقوائم إبطال شهادات الكيان النهائي المملوءة والكاملة (EPRL)، وقوائم إبطال سلطات إصدار الشهادة (CARL). ومع ذلك يمكن تطبيق هذا الوصف للتحقق من الوضع القانوني لإبطال شهادات النعت باستخدام قوائم إبطال شهادات النعت (ACRL)، وقوائم إبطال سلطات النعت (AARL). ولأغراض هذا الملحق، يمكن اعتبار القوائم ACRL بدلاً من CRL، واعتبار EPRL هي قوائم ACRL مملوءة وكاملة للكيانات النهائية، واعتبار القوائم AARL بدلاً من القوائم CARL. وبطريقة مماثلة يمكن مقابلة نعوت الدليل المعددة في الفقرة 4.B بنعوت القوائم AARL وACRL، ومقابلة الحقول التي تحدد أنماط الشهادات في توسع نقطة التوزيع المُصدرة بالحقول التي تنطبق على البنية التحتية لإدارة الامتياز.

1.1.B أنماط قوائم إبطال الشهادات (CRL)

يمكن أن يتيسر للطرف الواثق نمط واحد أو أكثر من أنماط قوائم إبطال الشهادات (CRL) التالية، حسب ملامح الإبطال الواردة في سياسة سلطة إصدار الشهادة:

- قائمة CRL مملوءة وكاملة؛
- قائمة CRL لكيانات نهائية (EPRL) مملوءة وكاملة؛
- قائمة إبطال سلطات إصدار الشهادة (CARL) مملوءة وكاملة؛
- قائمة CRL أو EPRL أو CARL لنقطة التوزيع؛
- قائمة CRL أو EPRL أو CARL غير مباشرة (ICRL)؛
- قائمة دلتا CRL أو EPRL أو CARL؛
- قائمة دلتا CRL (dCRL) أو EPRL أو CARL غير مباشرة؛

فأما القائمة CRL المملوءة والكاملة فهي قائمة جميع شهادات الكيان النهائي وشهادات سلطة إصدار الشهادة الصادرة عن إحدى السلطات والمبطلة لأي واحد فقط من دواعي الإبطال أو للدواعي كلها.

وأما القائمة EPRL المملوءة والكاملة فهي قائمة جميع شهادات الكيان النهائي الصادرة عن إحدى السلطات والمبطلة لأي واحد فقط من دواعي الإبطال أو للدواعي كلها.

وأما القائمة CARL المملوءة والكاملة فهي قائمة شهادات سلطة إصدار الشهادة الصادرة عن إحدى السلطات والمبطلة لأي واحد فقط من دواعي الإبطال أو للدواعي كلها.

وأما القائمة CRL أو EPRL أو CARL لنقطة التوزيع فهي قائمة تغطي جميع الشهادات أو مجموعة فرعية من الشهادات الصادرة عن إحدى السلطات. وتختار المجموعة الفرعية استناداً إلى عدد من المعايير.

وأما القائمة CRL أو EPRL أو CARL غير المباشرة (ICRL) فهي قائمة CRL تحتوي على قائمة شهادات مبطلة، يكون بعضها أو كلها غير صادرة عن السلطة المصدرة للقائمة CRL والموقعة عليها.

وأما القائمة دلتا CRL أو EPRL أو CARL فهي قائمة CRL تحتوي على التعديلات على قائمة CRL كانت كاملة لمجال تطبيق معين في الوقت المعيّن في القائمة CRL التي يحال إليها في القائمة dCRL. ويلاحظ أن القائمة CRL التي يحال إليها يمكن أن تكون قائمة CRL كاملة لمجال التطبيق المعطى أو أن تكون قائمة dCRL مستعملة محلياً لإنشاء قائمة CRL كاملة للمجال المعطى.

جميع أنماط القوائم CRL المذكورة أعلاه (ما عدا القائمة dCRL) هي أنماط للقوائم CRL الكاملة لمجال تطبيقها المعيّن. ويجب أن تستعمل القائمة dCRL بالاشتراك مع قائمة CRL مصاحبة هي كاملة لنفس المجال، بغية رسم صورة كاملة للوضع القانوني لإبطال الشهادات.

وأما القائمة دلتا CRL أو EPRL أو CARL غير المباشرة فهي قائمة CRL لا تحتوي إلا على التعديلات على مجموعة مؤلفة من قائمة CRL واحدة أو أكثر من واحدة، هي كاملة لمجالات تطبيقها المعينة، وبعض هذه الشهادات أو كلها لم يكن قد صدر عن السلطة المُصْدرة لهذه الشهادة CRL والموقعة عليها.

وفي هذا السياق كما في سياق هذه المواصفة، يعرّف "مجال التطبيق لقائمة CRL" ببعدين مستقلين. أحدهما هو مجموعة الشهادات التي تغطيها القائمة CRL، والبعد الآخر هو مجموعة شفرات الدواعي التي تغطيها القائمة CRL. ويمكن تحديد مجال التطبيق لقائمة CRL بواحدة أو بأكثر من واحدة من الوسائل التالية:

- توسع نقطة التوزيع المُصْدرة (IDP) في القائمة CRL؛ أو
- وسائل أخرى تقع خارج نطاق هذه المواصفة.

2.1.B معالجة القائمة CRL

إذا كان طرف واثق يستخدم القوائم CRL كآلية لتحديد ما إذا كانت إحدى الشهادات مبطلة، يجب عليه أن يستخدم القائمة (أو القوائم) CRL الخاصة بهذه الشهادة. ويشرح هذا الملحق الإجراء اللازم للحصول على القوائم CRL المناسبة ومعالجتها، مروراً بعدد من المراحل المعينة. والتطبيق المكافئ وظيفياً للسلوك الخارجي الناتج عن هذا الإجراء، يجب أن يعتبر أيضاً مطابقاً لهذا الملحق وهذه المواصفة المصاحبة. ولم تُقيّس الخوارزمية التي يجب أن يستخدمها تطبيق خاص لكي يستنتج المُخْرج الصحيح (أي الوضع القانوني لإبطال شهادة) من مُدْخلات معينة (الشهادة ذاتها والمُدْخل من السياسة المحلية). فمثلاً على الرغم من أن الإجراء مشروح على أنه تتابع مرتّب من مراحل المعالجة، يمكن لتطبيق ما أن يستعمل قوائم CRL موجودة في مَخْبئة المحلي، بدلاً من أن يستخرج القوائم CRL في كل مرة يعالج فيها إحدى الشهادات، شريطة أن تكون هذه الشهادة CRL كاملة لمجال تطبيق الشهادة، ولا تنتهك أي واحدة من معلمات الشهادة أو السياسة.

والمراحل العامة التالية مشروحة في الفقرات من 2.B إلى 5.B أدناه:

1) تحديد معلمات القوائم CRL؛

2) تحديد القوائم CRL اللازمة؛

3) الحصول على القوائم CRL؛

4) معالجة القوائم CRL.

تحديد المرحلة 1) المعلمات التي تؤخذ من الشهادة أو من مصادر أخرى لاستعمالها في تحديد أنماط القوائم CRL اللازمة.

وتستخدم المرحلة 2) قيم المعلمات لتحديد القوائم CRL.

وتحدد المرحلة 3) نعوت الدليل التي تستخرج منها أنماط القوائم CRL.

وتشرح المرحلة 4) معالجة القوائم CRL المناسبة.

2.B تحديد معلمات القوائم CRL

إن المعلومات الكائنة في الشهادة ذاتها، وكذلك المعلومات المأخوذة من السياسة التي يعمل الطرف الواثق بموجبها، هي التي تقدم المعلمات اللازمة لتحديد القوائم المناسبة من القوائم CRL المرشحة. والمعلومات التالية هي اللازمة لتحديد الأنماط المناسبة من القوائم CRL:

- نمط الشهادة (هل هي شهادة كيان نهائي أم شهادة سلطة إصدار الشهادة)؛
- نقطة التوزيع الحرجة للقائمة CRL؛
- أحدث قائمة CRL حرجة؛
- شفرات الدواعي المعنية.

يمكن تحديد نمط الشهادة ضمن توسع التقييدات الأساسية في الشهادة. وعندما يكون التوسع موجوداً فهو يدل إن كانت الشهادة هي شهادة سلطة إصدار الشهادة أم هي شهادة كيان نهائي. أما إذا كان التوسع غائباً، فيعتبر نمط الشهادة هو شهادة كيان نهائي. وهذه المعلومة لازمة لتحديد ما إذا كانت القوائم CRL أو EPRL أو CARL يمكن استعمالها للتحقق من الشهادة من حيث إبطالها.

وإذا كانت الشهادة تحتوي على توسع نقطة التوزيع الحرجة للقائمة CRL، يكون على نظام معالجة شهادة الطرف الواثق أن يتفهم هذا التوسع، لكي يحصل ويستعمل الشهادات CRL التي يشير إليها توسع نقطة توزيع القائمة CRL من حيث شفرات الدواعي، بغية تحديد الوضع القانوني لإبطال الشهادة. فقد لا يكون كافياً مثلاً الاعتماد على قائمة CRL مملوءة.

وإذا كانت الشهادة تحتوي على توسع أحدث شهادة CRL حرجة، لا يستطيع الطرف الواثق استخدام الشهادة إن لم يكن قد سبق له أن استخرج أحدث قائمة CRL وتحقق منها.

وتحدد السياسة شفرات الواعي المعنيّة، ويقدمها التطبيق عادة. ويوصى بأن تحتوي هذه الشفرات على جميع شفرات الدواعي. وهذه المعلومات لازمة لتحديد أي القوائم CRL تكون كافية من حيث شفرات الدواعي.

ويلاحظ أن السياسة ربما تفرض إن كان يتوقع من الطرف الواثق أن يكون معتمداً أم لا للتحقق من الوضع القانوني لإبطال القوائم dCRL، عندما يكون التوسع **أحدث قائمة CRL** موسوماً بغير الحرج أو عندما لا يكون موجوداً في الشهادة. وتشرح المرحلة 4) معالجة هذه القوائم dCRL الاختيارية على الرغم من أن ذلك لا يدخل في نطاق هذه المرحلة.

3.B تحديد القوائم CRL اللازمة

تحدد قيم المعلمات المشروحة في الفقرة 2.B المعيار الذي تتحدد بموجبه أنماط القوائم CRL اللازمة للتحقق من الوضع القانوني لإبطال شهادة معينة. ويمكن القيام بتحديد أنماط القوائم CRL استناداً إلى مجموعات المعايير التالية المشروحة في الفقرات 1.3.B إلى 4.3.B أدناه.

- شهادة كيان نهائي مع تأكيد حرج لنقطة توزيع قائمة CRL؛
- شهادة كيان نهائي بدون تأكيد حرج لنقطة توزيع قائمة CRL؛
- شهادة سلطة إصدار الشهادة مع تأكيد حرج لنقطة توزيع قائمة CRL؛
- شهادة سلطة إصدار الشهادة بدون تأكيد حرج لنقطة توزيع قائمة CRL.

والتعامل مع المعلمات الباقية (التوسع الحرج لأحدث قائمة CRL ومجموعة شفرات الدواعي المعنيّة) مشروح في كل واحدة من الفقرات.

ويلاحظ أن أكثر من نمط واحد من القوائم CRL يمكنه تلبية المتطلبات في كل حالة. وعندما يكون اختيار أنماط القوائم CRL ممكناً، يقوم الطرف الواثق بانتقاء أي واحد من الأنماط المناسبة لكي يستعمله.

1.3.B شهادة كيان نهائي مع نقطة توزيع حرجة للقائمة CRL

إذا كانت الشهادة هي شهادة كيان نهائي، وكان التوسع **نقاط توزيع القوائم CRL (cRLDistributionPoints)** موجوداً في الشهادة وموسوماً بالحرج، يمكن الحصول على القوائم CRL التالية:

- قائمة CRL من واحدة من نقاط التوزيع المسمّاة للقوائم CRL، تغطي واحدة أو أكثر من واحدة من شفرات الدواعي المعنيّة؛
- إذا لم تكن هذه القائمة CRL تغطي جميع شفرات الدواعي المعنية، يمكن الحصول على الوضع القانوني للإبطال الخاص ببقية شفرات الدواعي عن طريق أي تجميعة من القوائم CRL التالية:
  - قوائم CRL أخرى من نقطة التوزيع؛
  - قوائم CRL أخرى كاملة؛
  - قوائم EPRL أخرى كاملة.

وإذا كان التوسع أحدث قائمة CRL موجوداً أيضاً في الشهادة وموسوماً بالحرج، يمكن الحصول أيضاً على قائمة CRL واحدة أو على أكثر من واحدة، من نقطة توزيع واحدة أو أكثر مسمّاة في هذا التوسع، للتأكد من التحقق من أحدث معلومات الإبطال لجميع شفرات الدواعي المعنية.

2.3.B شهادة كيان نهائي بدون نقطة توزيع حرجة للقائمة CRL

إذا كانت الشهادة هي شهادة كيان نهائي، وكان التوسع **نقاط توزيع القوائم CRL** ليس موجوداً في الشهادة أو كان موجوداً ولكنه غير موسوم بالحرج، يمكن الحصول على الوضع القانوني للإبطال الخاص بشفرات الدواعي عن طريق أي تجميعة من القوائم CRL التالية:

- قوائم CRL من نقطة التوزيع (إن وجدت)؛
- قوائم CRL كاملة؛
- قوائم EPRL كاملة.

وإذا كان التوسع أحدث قائمة CRL موجوداً أيضاً في الشهادة وموسوماً بالحرج، يمكن الحصول أيضاً على قائمة CRL واحدة أو على أكثر من واحدة، من نقطة توزيع واحدة أو أكثر مسمّاة في هذا التوسع، للتأكد من التحقق من أحدث معلومات الإبطال لجميع شفرات الدواعي المعنية.

3.3.B شهادة سلطة إصدار الشهادة مع نقطة توزيع حرجة للقائمة CRL

إذا كانت الشهادة هي شهادة سلطة إصدار الشهادة وكان التوسع **نقاط توزيع القوائم CRL** موجوداً في الشهادة وموسوماً بالحرج، يمكن الحصول على القوائم CRL/CARL التالية:

- قائمة CRL أو CARL من واحدة من نقاط التوزيع المسمّاة، تغطي واحدة أو أكثر من واحدة من شفرات الدواعي المعنيّة؛
- إذا لم تكن هذه القائمة CRL/CARL تغطي جميع شفرات الدواعي المعنية، يمكن الحصول على الوضع القانوني للإبطال الخاص ببقية شفرات الدواعي عن طريق أي تجميعة من القوائم CRL/CARL التالية:
  - قوائم CRL/CARL أخرى من نقطة التوزيع؛
  - قوائم CRL كاملة؛
  - قوائم CARL كاملة.

وإذا كان التوسع أحدث قائمة CRL موجوداً أيضاً في الشهادة وموسوماً بالحرج، يمكن الحصول أيضاً على قائمة CRL/CARL واحدة أو على أكثر من واحدة، من نقطة توزيع واحدة أو أكثر مسمّاة في هذا التوسع، للتأكد من التحقق من أحدث معلومات الإبطال لجميع شفرات الدواعي المعنية.

4.3.B شهادة سلطة إصدار الشهادة بدون نقطة توزيع حرجة للقائمة CRL

إذا كانت الشهادة هي شهادة سلطة إصدار الشهادة وكان التوسع **نقاط توزيع القوائم CRL** غير موجود في الشهادة أو كان موجوداً ولكنه غير موسوم بالحرج، يمكن الحصول على الوضع القانوني للإبطال الخاص بشفرات الدواعي عن طريق أي تجميعة من القوائم CRL التالية:

- قوائم CRL/CARL من نقطة التوزيع (إن وجدت)؛
- قوائم CRL كاملة؛
- قوائم CARL كاملة.

وإذا كان التوسع أحدث قائمة CRL موجوداً أيضاً في الشهادة وموسوماً بالحرج، يمكن الحصول أيضاً على قائمة CRL/CARL واحدة أو أكثر من واحدة، من نقطة توزيع واحدة أو أكثر مسمّاة في هذا التوسع، للتأكد من التحقق من أحدث معلومات الإبطال لجميع شفرات الدواعي المعنية.

4.B الحصول على القوائم CRL

إذا كان الطرف الواثق يستخرج قوائم CRL معنية من الدليل، يمكن الحصول على هذه القوائم CRL من نقاط توزيع القوائم CRL أو من مدخل الدليل الخاص بمُصدر الشهادة عن طريق استخراج النعوت المناسبة، وهي نعت واحد أو أكثر من النعوت التالية:

- قائمة إبطال الشهادات؛
- قائمة إبطال السلطات؛
- قائمة الإبطال دلتا.

5.B معالجة القوائم CRL

يصبح الطرف الواثق جاهزاً لمعالجة القوائم، بعد أن يكون قد درس المعلمات المشروحة في الفقرة 2.B، وحدّد أنماط القوائم CRL المناسبة المشروحة في الفقرة 3.B، واستخرج مجموعة مناسبة من القوائم CRL المشروحة في الفقرة 4.B. وستحتوي مجموعة القوائم CRL على قائمة CRL أساسية واحدة على الأقل، كما يمكنها أن تحتوي على قائمة dCRL واحدة أو أكثر. ويجب على الطرف الواثق أن يتأكد أثناء معالجة كل قائمة CRL، من أن هذه القائمة صحيحة من حيث مجال تطبيقها. ولكن الطرف الواثق يكون قد حدّد بالفعل أن القائمة CRL مناسبة لمجال تطبيق الشهادة المعنية، أثناء مرحلتي المعالجة السابقتين 2.B و3.B. وبالإضافة إلى ذلك يجب التحقق من صلاحية القوائم CRL، كما يجب التحقق من القوائم لتحديد ما إذا كانت الشهادة قد أبطلت أم لا وهذه التحققات مشروحة في الفقرات من 1.5.B إلى 4.5.B أدناه:

1.5.B إقرار صلاحية القائمة CRL الأساسية من حيث مجال تطبيقها

يوجد كما هو مشروح في الفقرة 3.B أكثر من نمط واحد من القوائم CRL يمكن استعماله كقائمة CRL أساسية، للتحقق من الوضع القانوني لإبطال شهادة. ويمكن للطرف الواثق أن يستخدم واحداً أو أكثر من واحد من أنماط القوائم CRL الأساسية، حسب سياسة إصدار القائمة CRL الصادرة عن سلطة إصدارها:

- قوائم CRL كاملة لجميع الكيانات؛
- قوائم EPRL كاملة؛
- قوائم CARL كاملة؛
- قوائم CRL/EPRL/CARL مستندة إلى نقطة توزيع.

ويجب أن تستوفى مجموعة الشروط الواردة في الفقرات من 1.1.5.B إلى 4.1.5.B لكي يتمكن طرف واثق من استعمال قائمة CRL أساسية يمكن اعتمادها للتحقق من الوضع القانوني لإبطال شهادة، من حيث شفرات الدواعي المعنية.

وتعالج في كل فقرة حالة القوائم CRL الأساسية غير المباشرة.

1.1.5.B القائمة CRL الكاملة

يجب أن تستوفى جميع الشروط التالية لكي يتحدد أن قائمة CRL هي قائمة CRL كاملة لشهادات الكيان النهائي وشهادات سلطة إصدار الشهادة المسؤول عنها مُصْدر القائمة CRL، ولجميع شفرات الدواعي المعنية:

- يجب أن يكون توسع مؤشر القائمة دلتا CRL غير موجود؛
- يمكن أن يكون موجوداً توسع نقطة التوزيع المُصْدرة؛
- إما ألا يحتوي توسع نقطة التوزيع المصدرة على حقل نقطة التوزيع، وإما أن يتواءم أحد الأسماء الواردة في حقل نقطة التوزيع مع حقل **المُصْدر** في القائمة CRL؛
- إما أن يكون توسع نقطة التوزيع المُصْدرة لا تحتوي على أي واحد من الحقول التالية وإما إذا احتوى على أي واحد من الحقول التالية، لا يوضع أي واحد من الحقول الموجودة على القيمة **"صائب"**: containsUserPublicKeyCerts و/أو containsCACerts و/أو containsUserAttributeCerts و/أو containsAACerts و/أو containsSOAPublicKeyCerts؛
- إذا كان الحقل **شفرات الدواعي (reasonCodes)** موجوداً في التوسع نقطة التوزيع المُصْدرة، يجب أن يحتوي حقل شفرات الدواعي على جميع الدواعي المعنية بالتطبيق؛
- يمكن لتوسع نقطة التوزيع المُصْدرة أن يحتوي أو لا يحتوي على الحق **القائمة CRL غير المباشرة (indirectCRL)** (وعليه لا يحتاج هذا الحقل إلى التحقق منه).

2.1.5.B القائمة EPRL الكاملة

يجب أن تستوفى جميع الشروط التالية لكي يتحد أن قائمة CRL هي قائمة EPRL كاملة لجميع شفرات الدواعي المعنية:

- يجب أن يكون توسع مؤشر القائمة دلتا CRL غير موجود؛
- يجب أن يكون توسع نقطة التوزيع المصدرة موجوداً؛
- إما ألا يحتوي توسع نقطة التوزيع المصدرة على حقل نقطة التوزيع، وإما أن يتواءم أحد الأسماء الواردة في حقل نقطة التوزيع مع حقل **المُصْدر** في القائمة CRL؛
- يجب أن يحتوي توسع نقطة التوزيع المصدرة على الحقل **يحتوي على شهادات المفتاح العمومي للمستعمل (containsUserPublicKeyCerts)**. ويجب أن يوضع هذا الحقل على القيمة "**صائب**"؛
- إذا كان الحقل **شفرات الدواعي (reasonCodes)** موجوداً في التوسع نقطة التوزيع المصدرة يجب أن يحتوي حقل شفرات الدواعي على جميع الدواعي المعنية بالتطبيق؛
- يمكن لتوسع نقطة التوزيع المُصْدرة أن يحتوي أو لا يحتوي على الحقل **القائمة CRL غير المباشرة (indirectCRL)** (وعليه لا يحتاج هذا الحقل إلى التحقق منه)؛

ولا يمكن استعمال القائمة CRL إلا إذا كان الطرف الواثق قد حدّد أن شهادة الصاحب هي شهادة كيان نهائي. وهكذا إذا احتوت شهادة الصاحب على توسع **التقييدات الأساسية** يجب أن تكون قيمة cA موضوعة على "**خاطئ**".

3.1.5.B القائمة CARL الكاملة

يجب أن تستوفى جميع الشروط التالية لكي يتحد أن قائمة CRL هي قائمة CARL كاملة لجميع شفرات الدواعي المعنية:

- يجب أن يكون توسع مؤشر القائمة دلتا CRL غير موجود؛
- يجب أن يكون توسع نقطة التوزيع المصدرة موجوداً؛
- إما ألا يحتوي توسع نقطة التوزيع المصدرة على حقل نقطة التوزيع، وإما أن يتواءم أحد الأسماء الواردة في حقل نقطة التوزيع مع حقل **المُصْدر** في القائمة CRL؛
- يجب أن يحتوي توسع نقطة التوزيع المصدرة على الحقل **يحتوي على شهادات سلطة إصدار الشهادة**. ويجب أن يوضع هذا الحقل على القيمة "**صائب**"؛
- إذا كان الحقل **شفرات الدواعي (reasonCodes)** موجوداً في التوسع نقطة التوزيع المصدرة، يجب أن يحتوي حقل شفرات الدواعي على جميع الدواعي المعنية بالتطبيق؛
- يمكن لتوسع نقطة التوزيع المُصْدرة أن يحتوي أو لا يحتوي على الحقل **القائمة CRL غير المباشرة (indirectCRL)** (وعليه لا يحتاج هذا الحقل إلى التحقق منه)؛

ولا يمكن استعمال القائمة CARL إلا إذا كانت شهادة الصاحب هي شهادة كيان نهائي. وهكذا يجب أن تحتوي شهادة الصاحب على توسع **التقييدات الأساسية**، على أن تكون قيمة cA موضوعة على "**خاطئ**".

4.1.5.B القوائم CRL/EPRL/CARL المستندة إلى نقطة توزيع

يجب أن تستوفى جميع الشروط التالية لكي يتحد أن قائمة CRL هي واحدة من القوائم CRL المبينة في توسع نقطة توزيع القوائم CRL أو في التوسع أحدث قائمة CRL في الشهادة:

- إما أن يكون حقل نقطة التوزيع من توسع نقطة التوزيع المصدرة للقوائم CRL غير موجود (فقط في الحالة التي لا يكون فيها توسع نقطة القوائم CRL حرجاً)، وإما أن يتواءم أحد الأسماء الواردة في حقل نقطة

التوزيع من توسع نقطة توزيع القوائم CRL أو الواردة في توسع أحدث قائمة CRL للشهادة مع واحد من الأسماء الواردة في حقل نقطة التوزيع من توسع نقطة التوزيع المُصْدرة للقائمة CRL. أو بدلاً من ذلك، يتواءم أحد الأسماء الواردة في حقل مُصْدر القائمة CRL من نقطة توزيع القوائم CRL في الشهادة أو الواردة في توسع أحدث قائمة CRL، مع أحد الأسماء الواردة في نقطة التوزيع من نقطة التوزيع المُصْدرة (IDP)؛

- وإما أن يكون توسع نقطة التوزيع المُصدرة لا يحتوي على أي واحد من الحقول التالية، وإما إذا احتوى على أي واحد من الحقول التالية، لا يوضع أي واحد من الحقول الموجودة على القيمة "**صائب**": containsUserPublicKeyCerts و/أو containsCACerts و/أو containsUserAttributeCerts و/أو containsAACerts و/أو containsSOAPublicKeyCerts، وإما أن يوضع الحقل الخاص بنمط الشهادة على القيمة "**صائب**" (انظر الجدول 1.B بخصوص نمط الحقل الموافق لكل نمط شهادة)؛

- إذا كان الحقل **شفرات الدواعي** موجوداً في توسع نقطة توزيع القوائم CRL أو في توسع أحدث قائمة CRL الخاص بالشهادة، يجب أن يكون هذا الحقل إما غير موجود في توسع نقطة التوسيع المصدرة للقائمة CRL وإما يجب أن يحتوي على واحدة على الأقل من شفرات الدواعي المؤكد عليها في توسع نقطة توزيع القائمة CRL الخاص بالشهادة؛

- إذا كان الحقل **مُصْدر القائمة CRL (cRLIssuer)** غير موجود في توسع نقطة التوزيع القائمة CRL الخاص بالشهادة، يجب أن تكون القائمة CRL موقّعة من نفس سلطة إصدار الشهادة التي وقعت على الشهادة.

- إذا كان الحقل **مصدر القائمة CRL** موجوداً في التوسع النسبي (توسع نقطة توزيع القوائم CRL أو توسع أحدث قائمة CRL) الخاص بالشهادة، يجب أن تكون القائمة CRL موقعة من نفس مصدر القائمة CRL المحدّد في توسع نقطة توزيع القوائم CRL أو توسع أحدث قائمة CRL خاص بالشهادة، ويجب أن تحتوي القائمة CRL على الحقل **القائمة CRL غير المباشرة (indirectCRL)** في توسع نقطة التوزيع المُصْدرة.

ملاحظة – عندما يختبر وجود الدواعي وحقل مُصْدر القائمة CRL، لا يكون الاختبار ناجحاً إلا إذا كان الحقل موجوداً في نفس حقل نقطة التوزيع الموجود في توسع نقطة توزيع القوائم CRL أو في توسع أحدث قائمة CRL الذي يوجد بشأنه اسم في حقل نقطة التوزيع متوافق مع توسع نقطة التوزيع المصدرة من القائمة CRL.

الجدول 1.B – نمط الشهادة الموافق لنمط الحقل نقطة التوسع المُصْدرة

نمط الشهادة	حقل نقطة التوزيع المُصْدرة
كيان نهائي (المفتاح العمومي)	containsUserPublicKeyCerts
سلطة إصدار الشهادة (CA)	containsCACerts
كيان نهائي (النعت)	containsUserAttributeCerts
سلطة النعت (AA)	containsAACerts
مَصْدر السلطة (SOA)	containsSOAPublicKeyCerts

2.5.B إقرار صلاحية القائمة دلتا CRL من حيث مجال تطبيقها

يمكن للطرف الواثق أن يتحقق أيضاً من القوائم دلتا CRL (dCRL)، إما لأن هذا التحقق مطلوب من توسع **أحدث قائمة CRL** حرج وارد في الشهادة أو في القائمة CRL، وإما لأن السياسة التي يعمل بموجبها الطرف الواثق تتطلب التحقق من القائمة dCRL.

ويمكن للطرف الواثق أن يكون متأكداً دوماً من صحة المعلومات التي يمتلكها من القائمة CRL عن شهادة، إن كانت جميع الشروط التالية مستوفاة:

- القائمة CRL الأساسية التي يستخدمها الطرف الواثق هي القائمة المناسبة للشهادة، من حيث مجال التطبيق؛
- القائمة دلتا CRL التي يستخدمها الطرف الواثق هي القائمة المناسبة للشهادة، من حيث مجال التطبيق؛
- القائمة CRL الأساسية كانت قد صدرت في وقت إصدار القائمة CRL الأساسية التي تحيل إليها القائمة dCRL، أو بعد هذا الوقت.

كما يجب أن تستوفى جميع الشروط التالية لتحديد كون القائمة dCRL مناسبة للشهادة:

- يجب أن يكون موجوداً توسع مبيّن القائمة دلتا CRL (dCRL)؛
- يجب إصدار القائمة dCRL بعد إصدار القائمة CRL الأساسية. وأحد الأساليب التي تضمن هذا الأمر هو التحقق من أن رقم القائمة CRL في التوسع **رقم القائمة CRL** للقائمة dCRL هو أكبر من رقم القائمة CRL في التوسع **رقم القائمة CRL** للقائمة CRL الأساسية التي يستعملها الطرف الواثق، وأن حقلي معرف **هوية تقاطر القوائم CRL** يتواءمان في القائمة CRL الأساسية وفي القائمة دلتا CRL. وقد يحتاج هذا الأسلوب إلى معالجة منطقية إضافية لاختتام الأرقام. وهناك أسلوب آخر يكمن في مقارنة الحقلين **هذا التحيين** الموجودين في القائمة الأساسية وفي القائمة dCRL المتوفرتين لدى الطرف الواثق؛
- يجب أن تكون القائمة CRL الأساسية التي يستعملها الطرف الواثق هي القائمة التي صدرت بشأنها القائمة دلتا CRL، أو هي قائمة صدرت بعدها. وأحد الأساليب التي تضمن هذا الأمر هو التحقق من أن رقم القائمة CRL في التوسع **مبين في القائمة دلتا CRL** الخاص بالقائمة dCRL هو يساوي أو أصغر من رقم القائمة CRL في التوسع **رقم القائمة CRL** الخاص بالقائمة CRL الأساسية التي يستعملها الطرف الواثق، وأن الحقلين **معرف هوية تقاطر القوائم CRL** في القائمة الأساسية وفي القائمة دلتا CRL متوائمان. وقد يحتاج هذا الأسلوب إلى معالجة منطقية إضافية لاختتام الأرقام. وهناك أسلوب آخر يكمن في مقارنة الحقلين **هذا التحيين** في القائمة CRL الأساسية المتوفرة لدى الطرف الواثق وفي القائمة CRL الأساسية التي تشير إليها القائمة دلتا CRL. وهناك أيضاً أسلوب آخر يكمن في مقارنة حقل **هذا التحيين** الموجود في القائمة CRL الأساسية المتوفرة لدى الطرف الواثق والتوسع **وقت التحيين الأساسي (baseUpdateTime)** الموجود في القائمة دلتا CRL المتوفرة لدى الطرف الواثق.

  ملاحظة – يستطيع الطرف الواثق أن ينشئ دائماً قائمة CRL أساسية، بتطبيقه قائمة دلتا CRL على قائمة CRL أساسية، طالما تم استيفاء القاعدتين السابقتين باستخدام التحققين من **رقم القائمة CRL** ومن **معرف هوية تقاطر القوائم CRL**. وفي هذه الحالة يكون التوسع **رقم القائمة CRL والحقل هذا التحيين** في القائمة CRL الأساسية الجديدة كما هما في القائمة دلتا CRL. والطرف الواثق لا يعرف حقل **التحيين التالي** للقائمة CRL الأساسية الجديدة وليس بحاجة إليه لكي يقيم تصاحباً مع قائمة dCRL أخرى.

- إذا كانت القائمة دلتا CRL تحتوي على التوسع نقطة التوزيع المُصْدرة، يكون مجال تطبيق نقطة التوزيع المصدرة متسقاً مع الشهادة، كما هو مشروح في الفقرة 4.1.5.B أعلاه؛
- إذا كانت القائمة dCRL لا تحتوي على واحد من التوسعين التاليين: **معرف هوية التقاطر (streamIdentifier)** و**نقطة التوزيع المُصْدرة (issuingDistributionPoint)**، يجب ألا تستعمل إلا بالاشتراك مع قائمة CRL أساسية مملوءة وكاملة.

3.5.B التحقق من صلاحية وتداول القائمة CRL الأساسية

يجب أن تستوفى جميع الشروط التالية للتحقق من أن قائمة CRL صحيحة وأنها لم تعدّل منذ صدورها:

- يكون الطرف الواثق قادراً على الحصول على المفتاح العمومي للمُصْدر، المعرفة هويته في القائمة CRL باستخدام وسائل الاستيقان؛

- يجري التحقق من التوقيع على القائمة CRL الأساسية باستخدام هذا المفتاح العمومي المستيقن؛
- إذا كان حقل **التحيين التالي** موجوداً، يجب أن يكون الوقت الحالي سابقاً لقيمة هذا الحقل؛
- يجب أن يكون اسم المُصْدر في القائمة CRL متوائماً مع اسم المُصْدر في الشهادة التي يجري التحقق من إبطالها، إلا إذا كانت القائمة CRL مستخرجة من نقطة توزيع القائمة CRL في الشهادة وكان التوسع نقطة توزيع القائمة CRL يحتوي على المكوّنة **مُصْدر القائمة** CRL. وفي هذه الحالة، يجب أن يكون أحد الأسماء الواردة في المكوّنة مُصْدر القائمة CRL من التوسع نقطة توزيع القائمة CRL، متوائماً مع اسم المُصْدر في القائمة CRL.

4.5.B صلاحية القائمة دلتا CRL والتحققات من القائمة

يجب أن تستوفى جميع الشروط التالية للتحقق من أن قائمة دلتا CRL صحيحة وأنها لم تعدّل منذ صدورها:

- يكون الطرف الواثق قادراً على الحصول على المفتاح العمومي للمُصْدر، المعرفة هويته في القائمة CRL باستخدام وسائل الاستيقان؛
- يجب التحقق من التوقيع على القائمة دلتا CRL الأساسية باستخدام هذا المفتاح العمومي المستيقن؛
- إذا كان حقل **التحيين التالي** موجوداً، يجب أن يكون الوقت الحالي سابقاً لقيمة هذا الحقل؛
- يجب أن يكون اسم المُصْدر في القائمة دلتا CRL متوائماً مع اسم المُصْدر في الشهادة التي يجري التحقق من إبطالها، إلا إذا كانت القائمة دلتا CRL مستخرجة من نقطة توزيع القائمة CRL في الشهادة، وكان التوسع نقطة توزيع القائمة CRL يحتوي على المكوّنة **مُصْدر القائمة** CRL. وفي هذه الحالة، يجب أن يكون أحد الأسماء الواردة في المكوّنة مُصْدر القائمة CRL من التوسع نقطة توزيع القائمة، متوائماً مع اسم المُصْدر الوارد في القائمة CRL.

الملحق C

أمثلة من إصدار قائمة دلتا CRL

(لا يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

يوجد نموذجان لإصدار القوائم CRL، يقتضيان استعمال قوائم dCRL لمجموعة معنية من الشهادات.

في النموذج الأول، تحيل كل قائمة dCRL إلى أحدث قائمة CRL كاملة لمجال التطبيق المعطي ويمكن إصدار عدة قوائم dCRL لمجال التطبيق نفسه، قبل أن تصدر قائمة CRL جديدة كاملة لهذا المجال المعطى. وتستعمل القائمة CRL الجديدة الكاملة لهذا المجال المعطى كأساس للتتابع الجديد من القوائم dCRL، وهي تشكل القائمة CRL المحال إليها في التوسع المعني للقائمة dCRL. وعند إصدار القائمة CRL الجديدة الكاملة الخاصة بمجال التطبيق، تصدر أيضاً قائمة dCRL نهائية بشأن القائمة CRL السابقة الكاملة خاصة بمجال التطبيق.

والنموذج الثاني شبيه جداً بالأول، لا يختلف عنه إلا بكون القائمة CRL التي تحيل إليها قائمة CRL ليست بالضرورة واحدة كاملة لمجال تطبيق معطى (أي، يمكن لقائمة CRL محال إليها أن تكون قد أصدرت بصفة قائمة دلتا CRL). وإذا كانت القائمة CRL المحال إليها هي قائمة كاملة لمجال التطبيق المعطى، يمكنها ألا تكون بالضرورة أحدث قائمة كاملة لهذا المجال.

ونظام استعمال الشهادات الذي يعالج قائمة dCRL، يجب عليه أن يمتلك قائمة CRL تكون كاملة لمجال التطبيق المعطى، وأن تكون حالية على الأقل بقدر ما هي حالية القائمة CRL المحال إليها في القائمة dCRL. وهذه القائمة CRL التي هي كاملة لمجال التطبيق المعطى يمكن أن تكون قائمة صادرة بهذه الصفة عن السلطة المسؤولة أو قائمة أنشأها محلياً نظام استعمال الشهادات. ويلاحظ أنه يقع ازدواج في المعلومات في بعض الحالات ما بين القائمة dCRL والقائمة CRL الكاملة بالنسبة لمجال التطبيق المعطى، إذا كان نظام استعمال الشهادات يمتلك مثلاً قائمة CRL كانت صادرة بعد قائمة محال إليها في القائمة dCRL.

ويعرض الجدول التالي ثلاثة أمثلة من استخدام القوائم dCRL. والمثال 1 هو التخطيطة التقليدية المشروحة في النموذج الأول أعلاه، والمثالان 2 و3 هما شكلان بديلان للنموذج الثاني أعلاه.

ففي المثال 2، تصدر السلطة قوائم CRL كاملة بالنسبة إلى مجال تطبيق معطى، كل يومين، وتحيل القوائم dCRL إلى القائمة CRL الكاملة ما قبل الأخيرة. وقد تكون هذه الطريقة مفيدة في البيئات التي يلزم فيها تخفيض عدد المستعملين الذين ينفذون بنفس الوقت إلى مستودع لسحب قائمة CRL كاملة بالنسبة إلى مجال تطبيق معطى. وفي المثال 2 يستطيع المستعملون الذين يمتلكون أحدث قائمة CRL كاملة بالنسبة إلى المجال، ومعهم أيضاً المستعملون الذين يمتلكون القائمة CRL ما قبل الأخيرة الكاملة بالنسبة إلى المجال، أن يستعملوا نفس القائمة dCRL. ويكون لدى مجموعتي المستعملين كلتيهما معلومات الإبطال الكاملة عن الشهادات الخاصة بهذا المجال المعطى وقت إصدار القائمة dCRL المتوفرة لهم.

وفي المثال 3 تصدر القوائم CRL الكاملة بالنسبة إلى مجال التطبيق المعطى، مرةً واحدةً كل أسبوع كما في المثال 1، غير أن كل قائمة dCRL تحيل إلى قاعدة معلومات عن الإبطال مؤرخة قبل سبعة أيام من هذه القائمة dCRL.

ولا يقدم هذا الملحق أي مثال من استعمال القوائم CRL غير المباشرة، غير أن هذه الحالة تمثل مجموعة فوقية لهذه الأمثلة.

وليست هذه الأشكال إلا أمثلة، ويمكن أن توجد أشكال أخرى مختلفة، تتوقف على السياسة المحلية. ومن العوامل التي يجب مراعاتها عند وضع هذه السياسة عدد المستعملين وتواتر نفاذهم إلى القوائم CRL، وتكرارية القوائم CRL، وتقاسم الحمولة بين أنظمة الدليل التي تمسك بالقوائم CRL، والأداءات، واشتراكات زمن الكمون وغيرها.

يوم	المثال 1 – القائمة دلتا تحيل إلى قائمة CRL كاملة لمجال التطبيق المعطى		المثال 2 – القائمة دلتا تحيل إلى قائمة CRL ما قبل الأخيرة الكاملة لمجال التطبيق		المثال 3 – القائمة دلتا تحيل إلى معلومات إبطال مؤرخة من 7 أيام	
	القائمة CRL الكاملة	القائمة دلتا CRL	القائمة CRL الكاملة	القائمة دلتا CRL	القائمة CRL الكاملة	القائمة دلتا CRL
8	thisUpdate=day 8 nextUpdate=day 15 crlNumber=8	thisUpdate=day 8 nextUpdate=day 9 crlNumber=8 BaseCRLNumber=1	thisUpdate=day 8 nextUpdate=day 10 crlNumber=8	thisUpdate=day 8 nextUpdate=day 9 crlNumber=8 BaseCRLNumber=6	thisUpdate=day 8 nextUpdate=day 15 cRLNumber=8	thisUpdate=day 8 nextUpdate=day 9 cRLNumber=8 BaseCRLNumber= 1
9	غير صادرة	thisUpdate=day 9 nextUpdate=day 10 crlNumber=9 BaseCRLNumber=8	غير صادرة	thisUpdate=day 9 nextUpdate=day 10 crlNumber=9 BaseCRLNumber=6	غير صادرة	thisUpdate=day 9 nextUpdate=day 10 cRLNumber=9 BaseCRLNumber= 2
10	غير صادرة	thisUpdate=day 10 nextUpdate=day 11 crlNumber=10 BaseCRLNumber=8	thisUpdate=day 10 nextUpdate=day 12 crlNumber=10	thisUpdate=day 10 nextUpdate=day 11 crlNumber=10 BaseCRLNumber=8	غير صادرة	thisUpdate=day 10 nextUpdate=day 11 cRLNumber=10 BaseCRLNumber= 3
11-14	نفس ملامح الأيام السابقة					
15	thisUpdate=day 15 nextUpdate=day 22 crlNumber=15	thisUpdate=day 15 nextUpdate=day 16 crlNumber=15 BaseCRLNumber=8	غير صادرة	thisUpdate=day 15 nextUpdate=day 16 crlNumber=15 BaseCRLNumber=12	thisUpdate=day 15 nextUpdate=day 22 cRLNumber=15	thisUpdate=day 15 nextUpdate=day 16 cRLNumber=15 BaseCRLNumber= 8
16	غير صادرة	thisUpdate=day 16 nextUpdate=day 17 crlNumber=16 BaseCRLNumber=15	thisUpdate=day 16 nextUpdate=day 18 crlNumber=16	thisUpdate=day 16 nextUpdate=day 17 crlNumber=16 BaseCRLNumber=14	غير صادرة	thisUpdate=day 16 nextUpdate=day 17 cRLNumber=16 BaseCRLNumber= 9

الملحق D

أمثلة من تعريفات سياسة الامتياز ونعت الامتياز

(لا يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

1.D المدخل

تعرّف سياسة الامتياز، من حيث إدارة الامتياز، بكل وضوح متى ينبغي للمتحقق من الامتياز أن يستنتج أن مجموعة من الامتيازات المقدمة هي كافية لكي يقرر منح النفاذ لمؤكد الامتياز (إلى طلب هدف أو مورد أو تطبيق). ويمكن أن تساعد المواصفة الرسمية سياسة الامتياز متحققاً من الامتياز لكي يجري تقييماً أوتوماتياً لامتيازات مؤكد امتياز، من حيث حساسية المورد المطلوب، بفعل كونها تتضمن القواعد التي تقرر نجاح أو فشل طلب مؤكد الامتياز، بعد مراعاة امتياز هذا الأخير وحساسية المورد.

لما كان من الضروري ضمان تكاملية سياسة الامتياز التي تستعمل في مثل هذا التحديد، يمكن لمعرّف هوية سياسة الامتياز، تحت شكل معرف هوية للهدف وفرم لسياسة الامتياز بالكامل أن يحمل في أهداف موقّعة ومخزونة في مداخل الدليل. ولا تقيّس هذه المواصفة أي نحو (قواعد تركيب) خاص يمكن استعماله لتعريف مرحلة من سياسة الامتياز.

2.D أمثلة من النَحْو (قواعد التركيب)

يمكن تعريف سياسة الامتياز باستعمال أي قواعد تركيب، بما فيها النص الواضح. ويقدم هذا الملحق مثالين من النَحْو، يمكن استعمالها لمساعدة الذين يعرّفون سياسات الامتياز، على تفهم مختلف الخيارات المطروحة لعملية التعريف، ويجب التشديد على أن هذين المثالين هما على سبيل المثال فقط، وأن تنفيذ إدارة الامتياز عبر استخدام شهادات النعت أو توسع **نعوت الدليل للصاحب (subjectDirectoryAttributes)** في شهادات المفتاح العمومي، **ليس لازماً** لاعتماد هذين النحوين أو أي نَحْو خاص آخر.

1.2.D المثال الأول

قواعد التركيب التالية من الترميز ASN.1 هي مثال لأداة مرنة شاملة تستعمل في تعريف سياسة الامتياز.

```
PrivilegePolicySyntax       ::= SEQUENCE {
    version         Version,
    ppe             PrivPolicyExpression }

PrivPolicyExpression        ::= CHOICE {
    ppPredicate     [0] PrivPolicyPredicate,
    and             [1] SET SIZE (2..MAX) OF PrivPolicyExpression,
    or              [2] SET SIZE (2..MAX) OF PrivPolicyExpression,
    not             [3] PrivPolicyExpression,
    orderedPPE      [4] SEQUENCE OF PrivPolicyExpression }
    -- Note: "sequence" defines the temporal order in which the
    -- privilege shall be examined
                                    -- ملاحظة: "التتابع" يحدد الترتيب الزمني الذي يجب
                                    -- أن يجري وفقه تفحص الامتياز

PrivPolicyPredicate         ::= CHOICE {
    present                 [0] PrivilegeIdentifier,
    equality                [1] PrivilegeComparison, -- single/set-valued priv.  -- امتياز بقيمة وحيدة أو مجموعة.
    greaterOrEqual          [2] PrivilegeComparison, -- single-valued priv.      -- امتياز بقيمة وحيدة.
    lessOrEqual             [3] PrivilegeComparison, -- single-valued priv.      -- امتياز بقيمة وحيدة.
    subordinate             [4] PrivilegeComparison, -- single-valued priv.      -- امتياز بقيمة وحيدة.
    substrings              [5] SEQUENCE {           -- single-valued priv.      -- امتياز بقيمة وحيدة.
        type                        PrivilegeType,
        initial                 [0] PrivilegeValue OPTIONAL,
        any                     [1] SEQUENCE OF PrivilegeValue,
        final                   [2] PrivilegeValue OPTIONAL },
```

```
    subsetOf            [6] PrivilegeComparison, -- set-valued priv. -- امتياز بقيمة وحيدة.
    supersetOf          [7] PrivilegeComparison, -- set-valued priv. -- امتياز بقيمة وحيدة.
    nonNullSetInter     [8] PrivilegeComparison, -- set-valued priv. -- امتياز بقيمة وحيدة.
    approxMatch         [9] PrivilegeComparison,
    -- single/set-valued priv. (approximation defined by application)  -- امتياز بقيمة وحيدة أو مجموعة (تقريب يحدده التطبيق)
extensibleMatch     [10] SEQUENCE {
        matchingRule        OBJECT IDENTIFIER,
        inputs              PrivilegeComparison } }


PrivilegeComparison   ::= CHOICE {

    explicit            [0] Privilege,
    -- the value(s) of an external privilege identified by  -- قيمة أو قيم امتياز خارجي يعرّفه التعبير Privilege.privilegeId،
    -- Privilege.privilegeId is(are) compared with the value(s)  -- تقارن بالقيمة أو القيم المقدمة صراحة في التعبير
    -- explicitly provided in Privilege.privilegeValueSet  -- Privilege.privilegeValueSet

    byReference     [1] PrivilegeIdPair }
    -- the value(s) of an external privilege identified by  -- قيمة أو قيم امتياز خارجي يعرّفه التعبير
    -- PrivilegeIdPair.firstPrivilege is(are) compared with  -- PrivilegeIdPair.firstPrivilege، تقارن بالقيمة أو القيم
    -- the value(s) of a second external privilege identified by  -- الخاصة بامتياز خارجي آخر يعرفه التعبير
    -- PrivilegeIdPair.secondPrivilege  PrivilegeIdPair.secondPrivilege

Privilege           ::= SEQUENCE {
    type                PRIVILEGE.&id ({SupportedPrivileges}),
    values              SET SIZE (0..MAX) OF
                        PRIVILEGE.&Type ({SupportedPrivileges} {@type})
    }

SupportedPrivileges PRIVILEGE     ::=  { ... }

PRIVILEGE   ::=  ATTRIBUTE
-- Privilege is analogous to Attribute  -- الامتياز مماثل للنعت

PrivilegeIdPair     ::=  SEQUENCE {
    firstPrivilege      PrivilegeIdentifier,
    secondPrivilege     PrivilegeIdentifier }

PrivilegeIdentifier ::=  CHOICE {
    privilegeType       [0] PRIVILEGE.&id ({SupportedPrivileges}),
    xmlTag              [1] OCTET STRING,
    edifactField        [2] OCTET STRING }\
-- PrivilegeIdentifier extends the concept of AttributeType to other  -- معرف هوية الامتياز يوسع مفهوم نعت الامتياز
-- (e.g., tagged) environments, such as XML and EDIFACT  -- إلى بيئات أخرى (مع واسمة مثلاً) مثل اللغة XML
                                                          -- أو التبادل EDIFACT

Version             ::= INTEGER { v1(0) }
```

ويمكن أن يساعد مثال محسوس على توضيح إحداث البنية **سياسة** الامتياز واستعمالها.

لنعتبر امتياز الموافقة على زيادة أجر. وللتبسيط نفترض أن السياسة المطلوب تنفيذها تنص على أن كبار المديرين التنفيذيين ومن فوقهم هم الذين يوافقون على الزيادات، وأن الموافقة تعطى فقط لمن دونهم مرتبة (أي يستطيع المدير أن يوافق على زيادة لكبير المديرين التنفيذيين، ولكنه لا يستطيع الموافقة لمدير عام مساعد). ولنفترض في هذا المثال أن هناك ستة مستويات تراتبية ("الموظف التقني" = 0، "والمدير التنفيذي = 1، "وكبير المديرين التنفيذيين" = 2، "والمدير" = 3، "والمدير العام المساعد" = 4، "والمدير العام" = 5).

ولنفترض فوق ذلك أن نمط النعت ("الامتياز") الذي يبين مستوى تراتبياً في شهادة نعت، له معرف هوية هدف هو *OID-C* وأن نمط النعت ("الحساسية) الذي يعرّف مستوى تراتبياً في سجل قاعدة المعطيات الذي يحتوي على حقل "الأجر" المطلوب

تعديله، له معرّف هوية هدف هو *OID-C* (الذي سيستعاض عنه بمعرفات هوية هدف حقيقية في تنفيذ محسوس). والتعبير البولاني التالي يحدد سياسة "الموافقة على الأجر" المطلوبة (تشفير هذه السياسة في تعبير **سياسة الامتياز** هو مهمة سهلة نسبياً:

AND (NOT (lessOrEqual (value corresponding to OID-C, value corresponding to OID-D))
subsetOf (value corresponding to OID-C, { 2, 3, 4, 5 }))

و (**لا** (أصغر أو يساوي (القيمة المقابلة للمعرّف OID-C، القيمة المقابلة للمعرّف OID-C))
مجموعة فرعية من (القيمة المقابلة للمعرّف OID-C، { 2, 3, 4, 5 }))

وتشفير السياسة هذا يعني أن الوضع التراتبي للموافق على الزيادة يجب أن يكون أعلى (المبين بالعبارة "**لا** أصغر – أو يساوي") من وضع الشخص الموافَق له، وأن الوضع التراتبي للموافق على الزيادة يجب أن ينتمي إلى المجال {كبير المديرين التنفيذيين، ...، المدير العام}، حتى تكون نتيجة تقييم هذا التعبير البولاني هي "صائبة". وأول مقارنة امتياز، تجري "بالإحالة" ما بين القيم المقابلة لنمط النعت "الوضع التراتبي" للكيانين المتدخلين. وثاني مقارنة امتياز هي "صريحة"، وفي هذه الحالة تقارن القيمة المقابلة للامتياز "الوضع التراتبي" للموافق على الزيادة لقائمة صريحة من القيم. ويكون المتحقق من الامتياز في هذه الحالة بحاجة إلى تعبير يشفّر هذه السياسة مع نعتين، يصاحب أحدهما الموافق على الزيادة ويصاحب الآخر الموافق له. ويمكن لنعت الموافق على الزيادة (الوارد في شهادة النعت) أن يأخذ القيمة {3 *OID-C*}، ويمكن لنعت الموافق له (الذي يمكن أن يكون مسجلاً في قاعدة معطيات النعت) أن يأخذ القيمة {3 *OID-D*}. ومقارنة قيمة نمط النعت للموافق على الزيادة (التي تساوي 3 في هذا المثال) بقيمة النعت المقابل لنمط نعت الموافق له (التي تساوي 3 أيضاً في هذا المثال) تعطي القيمة "خاطئ" للتعبير "**لا** أصغر – أو يساوي"، بحيث يجد أول مدير نفسه رافضاً إضافة الموافقة على زيادة أجر المدير الثاني أما إذا كان نعت الموافق له بالعكس يساوي {1 *OID-D*}، يكون الترخيص قد أعطي للمدير حتى يوافق على زيادة أجر المدير التنفيذي.

وليس صعباً تصور حصول إضافات إلى التعبير السابق. فيمكن أن تضاف مثلاً حجة ثالثة للتعبير "**و**" تقول بأن المتحول البيئي "الوقت الفعلي" الحاصل من الميقاتية المحلية، والمشفّر في نعت يعرف هويته معرّف من نمط الهدف *OID-E*، يجب أن ينتمي على مجال خاص محدد صراحة في نعت معرّف الهوية بنمط هدف هو *OID-F*. وبهذا الشكل يرخص بزيادة الأجر فقط إذا كانت الشروط السابقة مستوفاة وحصل تقديم الطلب أثناء ساعات الدوام.

2.2.D المثال الثاني

السياسة الأمنية في أبسط أشكالها هي مجموعة من المعايير اللازمة لتقديم خدمات أمنية. وفيما يخص التحكم في النفاذ، تشكل السياسة الأمنية مجموعة فرعية من سياسة أمنية أرفع مستوى، تحدد فيها الوسائل التي تنفذ سياسات التحكم في النفاذ ما بين المبادرين والدرئيات المستهدفة. ويجب أن تسمح وسائل التحكم في النفاذ بالاتصال حين تسمح به سياسة معينة، وأن ترفض الاتصال حين لا تسمح به صراحة سياسة معينة.

وتشكل السياسة الأمنية أساس القرارات التي تتخذها إجراءات التحكم في النفاذ. ويتم نقل معلومات السياسة الأمنية الخاصة بالمجال عن طريق ملف معلومات السياسية الأمنية (SPIF).

وملف معلومات السياسة الأمنية (SPIF) هو موضوع موقّع لتأمين الحماية من التعديلات غير المرخصة. ويحتوي الملف SPIF على المعلومات المستعملة لتفسير معلمات التحكم في النفاذ الواردة في الواسمة الأمنية وفي نعت الأهلية. ويجب أن يترافق معرف هوية السياسة الأمنية الوارد في نعت الأهلية بنحو (بقواعد تركيب) وعلم دلالات خاصين بالتنفيذ، كما تعرفهما السياسة الأمنية. ويدار هذا النَحْو الخاص بالتنفيذ المصاحب لسياسة أمنية خاصة، في ملف معلومات السياسة الأمنية (SPIF).

وينقل الملف SPIF تكافؤات ما بين التراخيص والحساسيات عن طريق ميادين السياسة الأمنية، ويقدم تمثيلاً للواسمات الأمنية بشكل مطبوع، ويقابل سلاسل سمات مرئية تحتوي على مستويات مع فئات أمنية لغرض عرضها على المستعملين النهائيين عند انتقاء النعوت الأمنية لموضوع من المعطيات. وتجري التقابلات بحيث يمكن لواسمة أمنية مولدة في أحد ميادين السياسة الأمنية أن تفسّر تفسيراً صحيحاً في ميدان آخر من ميادين السياسة الأمنية. ويمكن للملف SPIF أن يقابل نعت الأهلية بحقول

الرسالة الأمنية وواسمات العرض التي تعرض قاصدة المستعمل. وإذا كان هذا التقابل قابلاً للتطبيق، فإنه يحقق أن المقصد المقصود تتوفر له الترخيصات اللازمة لكي يقبل موضوع المعطيات.

ويحتوي ملف معلومات السياسة الأمنية (SPIF) على الحقول التالية:

- **حقل معلومات الصيغة (versionInformation)**: يبيّن صيغة النحو في الترميز ASN.1.
- **حقل معلومات التحيين (updateInformation)**: يبين صيغة النحو والدلالات لمواصفة الملف SPIF.
- **حقل معطيات تعرف هوية السياسة الأمنية (securityPolicyIdData)**: يحدّد السياسة الأمنية التي ينطبق عليها الملف SPIF.
- **حقل معرف هوية الامتياز (privilegeId)**: يبين معرف هوية الهدف الذي يميز النحو الموجود في فئة أمن نعت الأهلية.
- **حقل معرف هوية التحكم في النفاذ المبني على قواعد (rbac) (rbacId)**: معرف هوية هدف يميز نَحْو فئة الأمن المستعملة بالاشتراك مع الملف SPIF.
- **حقل تصنيفات أمنية (securityClassifications)**: يقابل تصنيف الواسمات الأمنية مع تصنيف نعوت الأهلية وتقدم أيضاً تقابلات للتكافؤات.
- **حقل مجموعات الواسمات للفئة الأمنية (securityCategoryTagSets)**: يقابل الفئات الأمنية للواسمات الأمنية مع الفئات الأمنية لنعوت الأهلية، وتقدم أيضاً تقابلات للتكافؤات.
- **حقل السياسات المتكافئة (equivalentPolicies)**: يدعم جميع السياسات المتكافئة في الملف SPIF.
- **حقل معطيات معرف الهوية للسياسة الأمنية بالتغيب (defaultSecurityPolicyIdData)**: يبيّن السياسة الأمنية التي تطبق عند استلام معطيات بدون واسمة أمنية.
- **حقل التوسعات (extensions)**: يقدم طريقة تسمح بإدراج وظائفيات إضافية عندما تتبين حاجات جديدة في المستقبل.

ويتم تعريف ملف معلومات السياسة الأمنية (SPIF) باستخدام النحو التالي:

```
SecurityPolicyInformationFile ::= SIGNED {SPIF}
SPIF ::= SEQUENCE    {
    versionInformation              VersionInformationData DEFAULT v1,
    updateInformation               UpdateInformationData,
    securityPolicyIdData                    ObjectIdData,
    privilegeId                             OBJECT IDENTIFIER,
    rbacId                                  OBJECT IDENTIFIER,
    securityClassifications         [0]     SEQUENCE OF SecurityClassification OPTIONAL,
    securityCategories              [1]     SEQUENCE OF SecurityCategory  OPTIONAL,
    equivalentPolicies              [2]     SEQUENCE OF EquivalentPolicy  OPTIONAL,
    defaultSecurityPolicyIdData     [3]     ObjectIdData OPTIONAL,
    extensions                      [4]     Extensions OPTIONAL }

VersionInformationData ::= INTEGER { v1(0) }


UpdateInformationData ::= SEQUENCE    {
    sPIFVersionNumber               INTEGER,
    creationDate                    GeneralizedTime,
    originatorDistinguishedName     Name,
    keyIdentifier                   OCTET STRING OPTIONAL }

ObjectIdData ::=   SEQUENCE {
    objectId            OBJECT IDENTIFIER,
    objectIdName        DirectoryString {ubObjectIdNameLength} }
```

```
SecurityClassification ::=  SEQUENCE  {
    labelAndCertValue                   INTEGER,
    classificationName                  DirectoryString {ubClassificationNameLength},
    equivalentClassifications   [0]     SEQUENCE OF EquivalentClassification OPTIONAL,
    hierarchyValue                      INTEGER,
    markingData                 [1]     SEQUENCE OF MarkingData OPTIONAL,
    requiredCategory            [2]     SEQUENCE OF OptionalCategoryGroup OPTIONAL,
    obsolete                            BOOLEAN DEFAULT FALSE           }

EquivalentClassification ::= SEQUENCE {
    securityPolicyId            OBJECT IDENTIFIER,
    labelAndCertValue           INTEGER,
    applied                     INTEGER {
                                    encrypt  (0),
                                    decrypt  (1),
                                    both     (2) } }

MarkingData ::= SEQUENCE {
    markingPhrase       DirectoryString {ubMarkingPhraseLength} OPTIONAL,
    markingCodes        SEQUENCE OF MarkingCode OPTIONAL }

MarkingCode ::= INTEGER {
    pageTop                 (1),
    pageBottom              (2),
    pageTopBottom           (3),
    documentEnd             (4),
    noNameDisplay           (5),
    noMarkingDisplay        (6),
    unused                  (7),
    documentStart           (8),
    suppressClassName       (9)}

OptionalCategoryGroup ::= SEQUENCE {
    operation               INTEGER {
                                onlyOne         (1),
                                oneOrMore       (2),
                                all             (3)},
    categoryGroup           SEQUENCE OF OptionalCategoryData }

OptionalCategoryData ::= SEQUENCE {
    optCatDataId            OC-DATA.&id({CatData}),
    categorydata            OC-DATA.&Type({CatData}{@optCatDataId }) }

OC-DATA ::= TYPE-IDENTIFIER

CatData OC-DATA ::= {  ... }

EquivalentPolicy   ::= SEQUENCE {
    securityPolicyId        OBJECT IDENTIFIER,
    securityPolicyName      DirectoryString {ubObjectIDNameLength}
    OPTIONAL}

Extensions ::= SEQUENCE OF Extension

Extension ::= SEQUENCE {
    extensionId             EXTENSION.&objId ({ExtensionSet}),
    critical                BOOLEAN DEFAULT FALSE,
    extensionValue              OCTET STRING  }
```

ويلاحظ أن النَحْو في مثال SPIF تطوري، وأن التعريف والواصف الكاملين لكل عنصر فيه موجودان في التوصية ITU-T X.841 | في المعيار الدولي ISO/IEC 15816.

3.D مثال نعت الامتياز

يقدم المثال التالي نعتاً يستعمل لنقل امتياز خاص، وهو مثال توضيحي فقط. ويوجد توصيف فعلي لهذا النحو والنعت المصاحب له في الفقرة 5.19 من التوصية ITU-T X.501 | في المعيار الدولي ISO/IEC 9594-2. ويحمل هذا النعت الخاص أهلية يمكن أن تصحب كياناً مسمّى، قد يكون وكيل مستعمل الدليل (DUA) لأغراض الاتصال بوكيل نظام الدليل (DSA).

ويمكن لنعت الأهلية أن يصحب أهلية لكيان مسمّى يشمل وكلاء DUA.

```
clearance  ATTRIBUTE ::= {
    WITH SYNTAX                 Clearance
    ID                          id-at-clearance }

Clearance  ::=  SEQUENCE {
    policyId                OBJECT IDENTIFIER,
    classList               ClassList DEFAULT {unclassified},
    securityCategories      SET SIZE (1MAX) OF SecurityCategory  OPTIONAL}

ClassList  ::=  BIT STRING {
    unmarked            (0),
    unclassified        (1),
    restricted          (2),
    confidential        (3),
    secret              (4),
    topSecret           (5) }
```

والمكوّنات الإفرادية مشروحة مع التوصيف الفعلي لهذا الامتياز في الوثيقة المشار إليها.

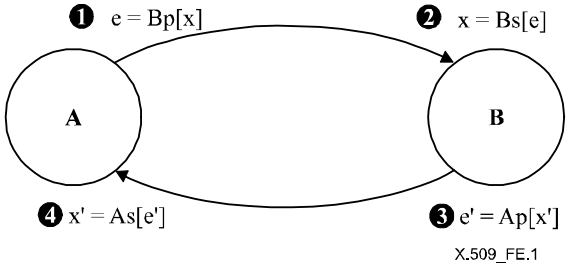
الملحق E

مدخل إلى التجفير بالمفتاح العمومي[3]

(لا يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

في أنظمة التجفير التقليدية، يكون المفتاح الذي يستخدمه مرسل الرسالة السرية لإجراء تجفيرها هو نفس المفتاح الذي يستخدمه مستلم الرسالة الشرعي للقيام بفك تجفيرها.

أما في أنظمة التجفير بالمفتاح العمومي (PKCS) فيستعمل زوج من المفاتيح، حيث يستخدم أحد مفتاحي الزوج للتجفير ويستعمل الآخر لفك التجفير. ويرتبط كل زوج من المفاتيح بمستعمل خاص X. ويكون أحد المفتاحين المعروف باسم المفتاح العمومي (Xp)، معروفاً من العموم، ويمكن أن يستخدمه أي مستعمل لتجفير المعطيات ولا يستطيع فك تجفير المعطيات إلا المستعمل X الذي يمتلك المفتاح الخاص المكمِّل (Xs)، (ويمثل ذلك الترميز [[D = Xs[Xp[D]). ويستحيل اكتشاف المفتاح الخاص حسابياً انطلاقاً من معرفة المفتاح العمومي. ويستطيع كل مستعمل إيصال عنصر من المعلومات، لا يستطيع اكتشافه إلا المستعمل X بتجفيره عن طريق المفتاح Xp. وبتوسيع الفكرة، يمكن لمستعملَيْن أن يتواصلا سراً بأن يستخدم كل منهما المفتاح العمومي لتجفير المعطيات كما هو مبين في الشكل 1.E.



الشكل 1.E – استخدام النظام PKCS لتبادل المعلومات السرية

يمتلك المستعمل A مفتاحاً عمومياً Ap ومفتاحاً خاصاً As. ويمتلك المستعمل B طقماً آخر من المفاتيح، هما Bp وBs. ويعرف كل من المستعملين A وB أن يتبادلا المعلومات السرية بتطبيقهما العمليات التالية (الممثلة في الشكل 1.E):

1) يرغب المستعمل A في إرسال معلوما سرية x إلى المستعمل B. يقوم A إذا بتجفير المعلومة x بمفتاح تجفير المستعمل B، ويرسل المعلومة المجفرة e إلى المستعمل B. ويمثل هذا بالتالي:

$$e = Bp[x]$$

2) يستطيع المستعمل B فك تجفير هذه المعلومة المجفّرة e لكي يحصل منها على المعلومة e، عن طريق مفتاحه الخاص لفك التجفير Bs. وتجدر الملاحظة أن المستعمل B هو المالك الوحيد للمفتاح Bs، ولما كان هذا المفتاح لا يمكن اكتشافه أو إرساله أبداً، فإن من المستحيل لطرف ثالث أن يحصل على المعلومة x. وامتلاك المفتاح الخاص Bs هو الذي يعيّن هوية المستعمل B. وتمثل عملية فك التجفير بالتالي:

$$x = Bs[e], \text{ or } x = Bs[Bp[x]]$$

---

[3] لمزيد من المعلومات انظر: DIFFIE (W.) and HELLMAN (M.E.): New Directions in Cryptography, *IEEE Transactions on Information Theory*, IT-22, No. 6, November 1976.

3) يستطيع المستعمل B أن يرسل الآن معلومة سرية 'x إلى المستعمل A بواسطة مفتاح التجفير Ap للمستعمل A:

$$e' = Ap[x']$$

4) يستطيع المستعمل A الحصول على المعلومة السرية 'x عن طريق فك تجفير المعلومة المجفرة 'x:

$$x' = As[e'], \text{ or } x' = As[Ap[x']]$$

وبهذه الوسيلة، تمكن المستعملان A وB من تبادل المعلومتين السريتين x و'x. ولا يمكن لأحد أن يحصل على هاتين المعلومتين إلا المستعملان A وB ، بفعل أن مفتاحيهما الخاصين لا يمكن اكتشافهما.

ويمكن لمثل هذا التبادل الذي يسهل نقل المعلومات السرية ما بين طرفين، أن يتحقق من هويتهما. فالمستعملان A وB معروفا الهوية بامتلاكهما مفتاحي التجفير الخاصين As وBs. إذاً يستطيع المستعمل A أن يحدد إن كان المستعمل B يمتلك مفتاح التجفير الخاص Bs، بحصوله على الجزء x من رسالته التي أرسلها في الرسالة 'x العائدة من المستعمل B. وهذا يبين للمستعمل A أن الاتصال قد جرى مع مالك المفتاح الخاص Bs. ويستطيع المستعمل B كذلك أن يتحقق من هوية المستعمل A.

وتمتلك بعض الأنظمة PKCS صفة تمكنها من عكس عمليتي فك التجفير والتجفير بحيث يمكن الحصول على D = Xp[Xs[D]]. وهكذا يصبح عنصر المعلومات الذي لا يمكن أن يرسله إلا المستعمل X، مقروءاً من كل مستعمل آخر (يمتلك المفتاح Xp). ويمكن الاستفادة من ذلك للتأكد من أصل المعلومة، كما يصلح أساساً للتوقيعات الرقمية. ولا يمكن أن تستعمل في إطار الاستيقان هذا إلا الأنظمة PKCS التي تمتلك صفة التبادلية هذه. ويشرح الملحق D خوارزمية من هذا النمط.

الملحق F

تعريف مرجعي لمعرّفات هوية موضوع الخوارزميات

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

يعرف هذا الملحق معرّفات هوية الموضوع المسندة إلى خوارزميات الاستيقان والتجفير، في غياب سجل رسمي للإسناد. ومن المزمع أن يستعمل مثل هذا السجل عندما يصبح متيسراً. وتأخذ التعريفات شكل وحدة الترميز ANS.1 المسماة **معرفات هوية موضوع الخوارزميات (AlgorithmObjectIdentifiers)**.

```
AlgorithmObjectIdentifiers {joint-iso-itu-t ds(5) module(1) algorithmObjectIdentifiers(8) 5}
DEFINITIONS ::=
BEGIN

-- EXPORTS All --

-- The types and values defined in this module are exported for use in the other ASN.1 modules contained
-- within the Directory Specifications, and for the use of other applications which will use them to access
-- Directory services. Other applications may use them for their own purposes, but this will not constrain
-- extensions and modifications needed to maintain or improve the Directory service.
-- الأنماط والقيم المعرّفة في هذه الوحدة يتم تصديرها، لكي تستعمل في الوحدات الأخرى من الترميز ASN.1 الموجودة
-- في مواصفات الدليل، وفي غيرها من التطبيقات التي سوف تستخدمها للنفاذ إلى خدمات الدليل. وقد تستعملها تطبيقات
-- أخرى لأغراض خاصة بها، ولكن ذلك لن يقيّد التوسعات والتعديلات الواجب إدخالها لتحيين أو تحسين خدمة الدليل.

IMPORTS
    algorithm, authenticationFramework
        FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 5}
    ALGORITHM
        FROM AuthenticationFramework authenticationFramework     ;

-- categories of object identifier --

encryptionAlgorithm   OBJECT IDENTIFIER  ::=  {algorithm 1}
hashAlgorithm         OBJECT IDENTIFIER  ::=  {algorithm 2}
signatureAlgorithm    OBJECT IDENTIFIER  ::=  {algorithm 3}

-- synonyms --   -- مترادفات --

id-ea          OBJECT IDENTIFIER  ::=  encryptionAlgorithm
id-ha          OBJECT IDENTIFIER  ::=  hashAlgorithm
id-sa          OBJECT IDENTIFIER  ::=  signatureAlgorithm

-- algorithms --   -- خوارزميات --

rsaALGORITHM  ::=  {
    KeySize
    IDENTIFIED BYid-ea-rsa }

KeySize       ::=  INTEGER

-- the following object identifier assignments reserve values assigned to deprecated functions
-- إسناد معرفات هوية الموضوع التالية يحفظ القيم المسندة إلى الدول المتروكة

id-ea-rsa                 OBJECT IDENTIFIER  ::=  {id-ea 1}

id-ha-sqMod-n             OBJECT IDENTIFIER  ::=  {id-ha 1}
id-sa-sqMod-nWithRSA      OBJECT IDENTIFIER  ::=  {id-sa 1}

END
```

الملحق G

أمثلة من استعمال تقييدات مسيرة إصدار الشهادة

(لا يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

1.G المثال 1: استعمال تقييدات أساسية

لنفترض أن الشركة Widget ترغب في تصديق متبادل على سلطة إصدار الشهادة المركزية من مجموعة Acme الصناعية، غير أنها ترغب أيضاً من أوساط الشركة Widget ألا تستعمل إلا شهادات الكيان النهائي الصادرة عن سلطة إصدار الشهادة هذه، وليس الشهادات الصادرة عن سلطة أخرى لإصدار الشهادة، تصدّق عليها هذه السلطة لإصدار الشهادة.

تستطيع الشركة Widget أن تلبي هذا الشرط، بإصدارها شهادة إلى السلطة المركزية لإصدار الشهادة في المجموعة Acme تشتمل على قيمة حقل التوسع التالية:

قيمة حقل التقييدات الأساسية:

{ cA TRUE, pathLenConstraint 0 }

2.G المثال 2: استعمال تقابل السياسات وتقييدات السياسات

لنفترض أن سيناريو التصديق المتبادل التالي مطلوب بين حكومتي كندا والولايات المتحدة الأمريكية:

أ) ترغب سلطة إصدار شهادة تابعة للحكومة الكندية في أن تصدّق على استعمال توقيعات حكومة الولايات المتحدة بالنسبة إلى سياسة كندية تدعى *Can/US-Trade*؛

ب) وحكومة الولايات المتحدة عندها سياسة تدعى *US/Can-Trade*، والحكومة الكندية مستعدة أن تعتبر هذه السياسة مكافئة لسياستها *Can/US-Trade*؛

ج) والحكومة الكندية ترغب في تطبيق تدابير سلامة، تتطلب من جميع شهادات الولايات المتحدة أن تعلن صراحة تأييدها للسياسة، وحظرها مطابقة سياسات أخرى في نطاق الولايات المتحدة.

تستطيع سلطة إصدار الشهادة التابعة للحكومة الكندية إصدار شهادة لصالح سلطة إصدار شهادة تابعة لحكومة الولايات المتحدة، تكون فيها قيم حقل التوسع التالية:

قيمة حقل سياسات الشهادة:

{{ policyIdentifier -- *object identifier for Can/US-Trade* -- **}}** *-- معرف هوية الموضوع للسياسة Can/US-Trade*

قيمة حقل تقابلات السياسات:

{{ issuerDomainPolicy *-- object identifier for Can/US-Trade --* **,** *-- معرف هوية الموضوع للسياسة Can/US-Trade*

subjectDomainPolicy *-- object identifier for US/Can-Trade --* **}}**

قيمة حقل تقييدات السياسات:

{{ policySet { *-- object identifier for Can/US-Trade --* **}, requireExplicitPolicy (0),**

-- معرف هوية الموضوع للسياسة Can/US-Trade

inhibitPolicyMapping (0)}}

3.G استعمال توسع تقييدات الاسم

1.3.G أمثلة من أنساق الشهادة تحتوي على توسع تقييدات الاسم

تستطيع سلطة إصدار الشهادة أن تضع تقييدات متنوعة على أسماء الصاحب (في حقل **الصاحب** أو في التوسع **الاسم البديل للصاحب**) في الشهادات التي تصدرها، وفي الشهادات اللاحقة في مسيرة إصدار الشهادة، بإدراجها توسع **تقييدات الاسم** في شهاداتها الصادرة عن سلطة إصدارها الشهادة. وتشرح هذه الفقرة أمثلة من أنساق الشهادات تحتوي على توسع **تقييدات الاسم**.

وفي سبيل تبسيط هذه الأمثلة، فإن أشكال **الأسماء المطلوبة (requiredNameForms)** في توسع تقييدات الاسم في هذه الأمثلة تدل فقط على **الاسم rfc822 (rfc822Name)** وعلى **الاسم المميز DN (directoryName)**.

1.1.3.G أمثلة الأشجار الفرعية المسموحة (*permittedSubtrees*)

(1-1) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN إن وجد، يكون مساوياً أو تابعاً مباشرة للشركة Acme Inc في الولايات المتحدة (أي {C=US, O=Acme Inc} ,.(U.S. (i.e.

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	(فارغ)	(فارغ)

(2-1) إذا كانت شهادة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، يكون مساوياً أو تابعاً مباشرة للشركة Acme Inc في الولايات المتحدة (أي {C=US, O=Acme Inc}).

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **maximum 1**}}	(فارغ)	(فارغ)

(3-1) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، يكون تابعاً للشركة Acme Inc في الولايات المتحدة (أي {C=US, O=Acme Inc}).

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **minimum 1**}}	(فارغ)	(فارغ)

(4-1) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، يكون مساوياً أو تابعاً للشركة Acme Inc في الولايات المتحدة (أي {C=US, O=Acme Inc})، أو يكون مساوياً أو تابعاً للشركة Acme Ltd في المملكة المتحدة (أي {C=UK, O=Acme Ltd}).

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=UK, O=Acme Ltd}}}	(فارغ)	(فارغ)

2.1.3.G أمثلة الأشجار الفرعية المستبعدة *(excludedSubtrees)*

(1-2) إذا كانت شهادة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، لا يكون مساوياً ولا تابعاً مباشرة للشركة Acme Corp في كندا (أي {C=CA, O=Acme Corp}).

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
(فارغ)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}}}	(فارغ)

(2-2) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، لا يكون تابعاً لأي تابع مباشر للشركة Acme Corp في كندا (أي {C=CA, O=Acme Corp}).

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
(فارغ)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}, **minimum 2**}}	(فارغ)

(3-2) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، لا يكون مساوياً للشركة Acme Corp في كندا (أي {C=CA, O=Acme Corp}).

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
(فارغ)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}, **maximum 0**}}	(فارغ)

(4-2) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، لا يكون مساوياً ولا تابعاً للشركة Acme Corp في كندا (أي {C=CA, O=Acme Corp})، ولا يكون مساوياً ولا تابعاً لشركة Asia Acme في اليابان (أي {C=JP, O=Asia Acme}).

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
(فارغ)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}}, {**base**(**directoryName**) {C=JP, O=Asia Acme}}}	(فارغ)

3.1.3.G أمثلة الأشجار الفرعية المسموحة والمستبعدة

(1-3) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، يكون مساوياً أو تابعاً للشركة Acme Inc في الولايات المتحدة (أي {C=US, O=Acme Inc})، ما عدا الوحدات التنظيمية للبحث والتطوير (R&D) في الشركة Acme Ltd، والكيانات التابعة لهذه الوحدات.

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	{{**base**(**directoryName**) {C=US, O=Acme Inc, OU=R&D}}}	(فارغ)

(2-3) إذا كانت شهادة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، يكون مساوياً لواحد من التوابع المباشرة للشركة Acme Inc في الولايات المتحدة (أي {C=US, O=Acme Inc})، ما عدا وحدة المشتريات التنظيمية (أي {C=US, O=Acme Inc, OU=مشتريات}).

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **minimum 1**, **maximum 1**}}	{{**base**(**directoryName**) {C=US, O=Acme Inc, OU=Purchasing}}}	(فارغ)

4.1.3.G أمثلة الأشجار الفرعية المسموحة والمستبعدة مع أشكال الأسماء المطلوبة

(1-4) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، يكون واحد على الأقل من أسماء صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) الواردة في الشهادة هو في شكل الاسم المميز DN. مع ذلك لا يكون أي اسم صاحب مقيداً بأي مكان أسماء.

توسع **nameConstraints**			
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**	
		الاسم rfc822	DN
(فارغ)	(فارغ)	لا	نعم

(2-4) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، يكون واحد على الأقل من أسماء الصاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) هو في شكل الاسم المميز DN. وفوق ذلك كل اسم صاحب هو في شكل الاسم المميز DN، يكون مستوفياً تقييدات أمكنة الأسماء المحددة **بالأشجار الفرعية المسموحة وبالأشجار الفرعية المستبعدة**.

توسع **nameConstraints**			
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**	
		الاسم rfc822	DN
{{**base**(**directoryName**) {C=JP, O=Asia Acme}}}	{{**base**(**directoryName**) {C=JP, O=Asia Acme, OU=Marketing}}}	لا	نعم

(3-4) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، يكون مستوفياً تقييدات أمكنة الأسماء المحددة **بالأشجار الفرعية المسموحة وبالأشجار الفرعية المستبعدة**.

توسع **nameConstraints**			
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**	
		الاسم rfc822	DN
{{**base**(**directoryName**) {C=JP, O=Asia Acme}}}	{{**base**(**directoryName**) {C=JP, O=Asia Acme, OU=Marketing}}}	لا	لا

ملاحظة – هذا المثال العلوي من شهادة السلطة CA يتواءم مع شهدة السلطة CA التالية التي تحتوي على توسع **تقييدات الاسم** بدون العنصر **أشكال الأسماء المطلوبة (requiredNameForms)**.

توسع **nameConstraints**		
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**
{{**base**(**directoryName**) {C=JP, O=Asia Acme}}}	{{**base**(**directoryName**) {C=JP, O=Asia Acme, OU=Marketing}}}	(فارغ)

(4-4) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، فكل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم المميز DN، إن وجد، يكون واحد على الأقل من **الاسم البديل للصاحب** موجوداً بشكل الاسم **rfc822**، وإن كان اسمه ليس مقيداً بأي مكان أسماء.

توسع **nameConstraints**			
permittedSubtrees	**excludedSubtrees**	**requiredNameForms**	
		الاسم rfc822	DN
{{**base**(**directoryName**) {C=JP, O=Asia Acme}}}	{{**base**(**directoryName**) {C=JP, O=Asia Acme, OU=Marketing}}}	نعم	لا

(5-4) إذا كانت شهادة السلطة CA تحتوي على توسع **تقييدات الاسم** التالي، لجميع الشهادات اللاحقة الموجودة في مسيرة إصدار الشهادة، يكون واحد على الأقل من أسماء الصاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) في الشهادة، موجوداً في شكل الاسم المميز أو في شكل الاسم rfc822. وكل اسم صاحب موجود في شكل الاسم المميز DN، إن وجد، يكون مستوفياً تقييدات أمكنة الأسماء المحددة بالأشجار الفرعية المسموحة وبالأشجار الفرعية المستبعدة. بينما لا يكون اسم الصاحب الموجود في شكل الاسم rfc822 مقيداً بأي مكان أسماء.

توسع **nameConstraints**			
permittedSubtrees	**ExcludedSubtrees**	**requiredNameForms**	
		الاسم rfc822	DN
{{**base**(**directoryName**) {C=JP, O=Asia Acme}}}	{{**base**(**directoryName**) {C=JP, O=Asia Acme, OU=Marketing}}}	نعم	نعم

2.3.G أمثلة عن معالجة الشهادات التي فيها توسع تقييدات الاسم

تشرح هذه الفقرة كيف يتم إقرار صلاحية اسم الصاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) أثناء معالجة الشهادة بالنسبة إلى متحولات الحالة في معالجة المسيرة، وهذه المتحولات هي: *الأشجار الفرعية المسموحة والأشجار الفرعية المستبعدة وأشكال الأسماء المطلوبة*.

وللتبسيط، لا يأخذ متحول الحالة في معالجة المسيرة الذي هو *أشكال الأسماء المطلوبة*، سوى القيم التالية في هذه الأمثلة وهي الاسم rfc822 **(rfc822Name)**، والاسم المميز الدليلي (DN) **(directoryName)**، ومعرف هوية المورد المنتظم URI **(uniformResourceIdentifier)**.

1.2.3.G تقييدا أمكنة الأسماء التي تحددها *الأشجار الفرعية المسموحة* في شكل الاسم DN

في هذه الحالة، كل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم DN وظاهر في الشهادة المدروسة، يستوفي التقييد الذي يحدده متحول الحالة في معالجة المسيرة *الأشجار الفرعية المسموحة*.

(1-1) توجد شجرة فرعية مسموحة واحدة لشكل الاسم DN، وشكل الاسم DN إلزامي في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	لا يوجد	لا	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Ltd*,OU=Purchasing}
2	**subject** = {} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com NOTE – *DN missing*
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=*Acme Ltd*, OU=Purchasing}
4	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
5	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=*Acme Ltd*, OU=Accounting}

(2-1) توجد شجرتان فرعيتان مسموحتان لشكل الاسم DN إلزامي في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=US, O=Acme Ltd}}}	لا يوجد	لا	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing}
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU= Accounting}

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme International*, OU=Accounting}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com NOTE – *DN missing*
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme International*, OU=Accounting}
4	**subject** = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
5	**subject** = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Corp*, OU=Accounting}
6	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com

(3-1) توجد شجرة فرعية مسموحة واحدة لشكل الاسم DN، والمكوّنة *أشكال الأسماء المطلوبة* خالية.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	لا يوجد	خالٍ		

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}
6	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Ltd*,OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Ltd*, OU=Accounting}
3	**subject** = {C=US, O=*Acme Ltd*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
4	**subject** = {C=US, O=*Acme Ltd*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Ltd*, OU=Purchasing}

2.2.3.G تقييدات أمكنة الأسماء التي تحددها *الأشجار الفرعية المستبعدة* في شكل الاسم DN

في هذه الحالة، كل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم DN وظاهر في الشهادة المدروسة، يستوفي التقييد الذي يحدده متحول الحالة في معالجة المسيرة *الأشجار الفرعية المستبعدة*.

(1-2) توجد شجرة فرعية مستبعدة واحدة لشكل الاسم DN، وشكل الاسم DN إلزامي في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
لا يوجد	{{**base**(**directoryName**) {C=US, O=Acme Ltd}}}	لا	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com NOTE – *DN missing*
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Ltd*, OU=Accounting}

(2-2) توجد شجرتان فرعيتان مستبعدتان لشكل الاسم DN، وشكل الاسم DN إلزامي في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
لا يوجد	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=US, O=Acme Ltd}}}	لا	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme International, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing}
3	**subject** = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme N.Y, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
3	**subject** = {} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com NOTE – *DN missing*
4	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Accounting}
5	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com

(3-2) توجد شجرة فرعية مستبعدة واحدة لشكل الاسم DN والمكوّنة *أشكال الأسماء المطلوبة* خالية.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
لا يوجد	{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	خالية		

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing}
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Accounting}
6	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Accounting}

3.2.3.G تقييدات أمكنة الأسماء المحددة فقط من *أشكال الأسماء المطلوبة*

(1-3) وجود شكل الاسم DN إلزامي في *أشكال الأسماء المطلوبة*

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
لا يوجد	لا يوجد	لا	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=JP, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=JP, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
5	**subject** = {C=JP, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Accounting}

أمثلة من الشهادات غير المقبولة

1	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com NOTE – *DN missing*
2	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-ltd.com NOTE – *DN missing*

(2-3) وجود شكل الاسم DN أو الاسم **rfc822name** إلزامي في *أشكال الأسماء المطلوبة*

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
لا يوجد	لا يوجد	نعم	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=JP, O=Acme Inc, OU=Purchasing}
3	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
5	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com **subjectAltName**(**rfc822Name**) = purchasing@acme-ltd.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-ltd.com NOTE – *DN and rfc822 missing*
2	**subject** = {} **subjectAltName**(**dNSName**) = www.acme-ltd.com NOTE – *DN and rfc822 missing*

4.2.3.G تقييدات أمكنة الأسماء المحددة في *الأشجار الفرعية المستبعدة* في أشكال الأسماء المتعددة

في هذه الحالة، كل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم DN أو الاسم rfc822 وظاهر في الشهادة المدروسة، يستوفي التقييد الذي يحدده متحول الحالة في معالجة المسيرة *الأشجار الفرعية المسموحة*.

(1-4) توجد شجرة فرعية مسموحة واحدة لشكل الاسم DN، وشجرة فرعية مسموحة أخرى لشكل الاسم **rfc822Name**. وفوق ذلك فإن وجود شكل الاسم DN إلزامي في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) .acme.com}}	لا يوجد	لا	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}
4	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com NOTE – *DN missing*
3	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*
5	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-ltd.com*
6	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com NOTE – *DN missing*

(2-4) توجد شجرة فرعية مسموحة واحدة لشكل الاسم DN، وشجرة فرعية مسموحة أخرى لشكل الاسم **rfc822Name**. وفوق ذلك يكون واحد على الأقل من شكل الاسم DN أو الاسم **rfc822Name** إلزامياً في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) .acme.com}}	لا يوجد	نعم	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = { C=US, O=Acme Inc, OU=Accounting}
5	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*
3	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*
5	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-ltd.com*
6	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com NOTE – *DN and rfc822 missing*

(3-4) توجد شجرة فرعية مسموحة واحدة لشكل الاسم DN، وشجرة فرعية مسموحة أخرى لشكل الاسم **rfc822Name**. لا توجد أشكال اسم إلزامية في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) .acme.com}}	لا يوجد	خالٍ		

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme.com
5	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*
3	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*
5	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*

5.2.3.G تقييدات أمكنة الأسماء المحددة *بالأشجار الفرعية المستبعدة* في أشكال الأسماء المتعددة

في هذه الحالة، كل اسم صاحب (في حقل الصاحب **"subject"** أو في توسع الاسم البديل للصاحب **"subjectAltName"**) موجود في شكل الاسم DN أو الاسم rfc822 وظاهر في الشهادة المدروسة، يستوفي التقييد الذي يحدده متحول الحالة في معالجة المسيرة *الأشجار الفرعية المستبعدة*.

(1-5) توجد شجرة فرعية مستبعدة واحدة لشكل الاسم DN، وشجرة فرعية مسموحة أخرى لشكل الاسم **rfc822Name**. وفوق ذلك فإن وجود شكل الاسم DN إلزامي في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
لا يوجد	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) .acme.com}}	لا	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Accounting}
4	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-ltd.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com NOTE – *DN missing*
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
4	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-inc.com
5	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
6	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Accounting}
7	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com **ملاحظة** – *ينقص الاسم DN*

(2-5) توجد شجرة فرعية مستبعدة واحدة لشكل الاسم DN، وشجرة فرعية مستبعدة أخرى لشكل الاسم **rfc822Name**. وفوق ذلك فإن واحداً على الأقل من شكل الاسم DN أو الاسم **rfc822Name** يكون إلزامياً *في أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
لا يوجد	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) .acme.com}}	نعم	نعم	لا

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.org
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Accounting}
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-ltd.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
4	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-inc.com
5	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
6	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Accounting}
7	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com **ملاحظة** – *ينقص الاسم DN والاسم rfc822*

(3-5) توجد شجرة فرعية مستبعدة واحدة لشكل الاسم DN، وشجرة فرعية مستبعدة أخرى لشكل الاسم **rfc822Name**. ولا توجد أشكال اسم إلزامية في *أشكال الأسماء المطلوبة*.

متحولات الحالة في معالجة المسيرة				
permitted-subtrees	*excluded-subtrees*	*required-name-forms*		
		rfc822	DN	URI
لا يوجد	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) .acme.com}}	خالٍ		

أمثلة من الشهادات المقبولة

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-ltd.com

أمثلة من الشهادات غير المقبولة

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
4	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-inc.com
5	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
6	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Accounting}

الملحق H

خطوط توجيهية تحدد السياسات التي تصلح لها مسيرة إصدار شهادة

(لا يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

يهدف هذا الملحق إلى تقديم خطوط توجيهية بشأن التطبيقات الصالحة للبنية التحتية PKI بالنسبة إلى معالجة إقرار الصلاحية لمسيرة إصدار الشهادة من حيث علاقتها بالسياسات. ويشرح البند 10 (إجراءات معالجة مسيرة إصدار الشهادة) في هذه المواصفة التحكم في المعالجة الخاصة بسياسات الشهادة بواسطة البنية التحتية PKI عبر محتويات الشهادات.

يتطرق هذا الملحق إلى تدميث مُدْخلين متعلقين بالسياسة في إجراءات معالجة المسيرة هما *مجموعة سياسات أولية وسياسة صريحة أولية*. وإضافة إلى هذين المُدْخلين، فإن المُدْخلين إلى الإجراءات: *حظر أولي لتقابل السياسات وحظر أولي لأي سياسة*، اللذين يمكن أن يبادر إليهما المستعمل، يؤثران في معالجة المعلومات المتعلقة بالسياسة أثناء المسيرة، ومع ذلك فإنهما يقعان خارج نطاق هذا الملحق. وعندما يوضع المُدخل *حظر أولي لتقابل السياسات* على القيمة **"صائب"**، فهو يمنع استخدام تقابلات السياسات في عمليات ناجحة لإقرار صلاحية المسيرة. بينما يمنع وضع المُدْخل *حظر أولي لأي سياسة* على القيمة **"صائب"** معرف الهوية الخاص **لأي سياسة**، إن وجد في إحدى الشهادات، من تكوين تواؤم مقبول مع معرف الهوية الخاص لسياسة ما.

ويعني المصطلح "المستعمل" في هذا الملحق "إنساناً مستعملاً"، أو "تطبيقاً" أقرت صلاحيته البنية التحتية PKI.

والسيناريوهات التالية متوقعة:

1) يتطلب المستعمل إقرار صلاحية مسيرة إصدار الشهادة، من أجل إحدى السياسات التي تهم المستعمل.

2) يتطلب المستعمل إقرار صلاحية مسيرة إصدار الشهادة، من أجل سياسة واحدى على الأقل، مهما تكن هذه السياسة. ويجب (يمكن) استعمال هذا السيناريو عندما يكون المستعمل ينوي القيام بمعالجة إضافية للسياسة تستخدم معطيات نصية أخرى ومحتويات معلومات أخرى، لكي تساعد كلها على قبول وجهة نظره بشأن المعاملة الخاصة لإحدى السياسات التي تكون مسيرة إصدار الشهادة صالحة لها.

3) ليس للمستعمل أي متطلبات بشأن مسيرة إصدار الشهادة. أو بعبارة أخرى إنه مستعد أن يقبل مسيرة إصدار شهادة تكون صالحة بصورة عامة، من دون أن يكون مستعداً بالضرورة لقبول أي سياسة.

4) يود المستعمل أن تكون مسيرة إصدار الشهغادة صالحة من أجل واحدة من السياسات التي تهمه، وإلا فإنه يرغب أن يتمكن من إعادة النظر في المسيرات غير الصالحة للسياسات التي تهم المستعمل. ويجب (يمكن) استعمال هذا السيناريو عندما يتطلب المستعمل بصورة عامة أن تكون مسيرة إصدار الشهادة صالحة من أجل سياسة مقبولة من المستعمل، ولكنها تستند إلى معطيات نصية أخرى ومحتويات معلومات أخرى، ربما تسمح له بتخطي فشل لاحق بإحدى السياسات.

وتشرح الفقرات التالية كيف يستطيع المستعمل أن يعمل لكي يحصل على المعلومات اللازمة من محرّك مناسب لإقرار صلاحية إحدى المسيرات.

1.H مسيرة إصدار الشهادة صالحة لسياسة مطلوبة يحددها المستعمل

يتطلب المستعمل في هذا السيناريو أن تكون مسيرة إصدار الشهادة صالحة من أجل إحدى السياسات التي تهم المستعمل. وفي سبيل الحصول على المعلومات المطلوبة، ينبغي للمستعمل أن يضع كما يلي مُدْخلات إقرار الصلاحية لمسيرة إصدار الشهادة المتعلقة بمعالجة السياسة:

مجموعة السياسات الأولية = {مجموعة السياسات التي تهم المستعمل}

سياسة صريحة أولية = **صائب**

وإذا نجح إقرار صلاحية المسيرة، تكون مسيرة إصدار الشهادة صالحة لواحدة على الأقل من السياسات التي تهم المستعمل. وتكون مسيرة إصدار الشهادة صالحة للسياسات المعددة في متحول الخرج *مجموعة السياسات المفروضة من المستعمل*.

وينبغي في هذا السيناريو ألا تستعمل التطبيقات مسيرة إصدار شهادة، إذا كان قد رفضها محرك إقرار صلاحية المسيرة بسبب فشل مرتبط بسياسة الشهادة.[4]

2.H مسيرة إصدار شهادة صالحة لأي سياسة مطلوبة

يتطلب المستعمل في هذا السيناريو أن تكون مسيرة إصدار الشهادة صالحة لسياسة واحدة على الأقل، غير أن المستعمل لا يهتم بأي سياسة هي. وفي سبيل الحصول على المعلومات المطلوبة، ينبغي للمستعمل أن يضع كما يلي مُدْخلات إقرار الصلاحية لمسيرة إصدار الشهادة المتعلقة بمعالجة السياسة:

مجموعة السياسات الأولية = **{أي سياسة}**

سياسة صريحة أولية = **صائب**

وإذا نجح إقرار صلاحية المسيرة، تكون مسيرة إصدار الشهادة صالحة لسياسة واحدة على الأقل. وتكون مسيرة إصدار الشهادة صالحة للسياسات المعددة في متحول الخرج *مجموعة السياسات المفروضة من المستعمل*.

وينبغي في هذا السيناريو ألا تستعمل التطبيقات مسيرة إصدار شهادة، إذا كان قد رفضها محرك إقرار صلاحية المسيرة بسبب فشل مرتبط بسياسة الشهادة.

3.H مسيرة إصدار شهادة صالحة بصرف النظر عن الشهادة

ليس للمستعمل في هذا السيناريو أي متطلبات خاصة بالسياسة بشأن مسيرة إصدار الشهادة. وفي سبيل الحصول على المعلومات المطلوبة، ينبغي للمستعمل أن يضع كما يلي مُدْخلات إقرار الصلاحية لمسيرة إصدار الشهادة المتعلقة بمعالجة السياسة:

مجموعة السياسات الأولية = **{أي سياسة}**

سياسة صريحة أولية = **خاطئ**

وإذا نجح إقرار صلاحية المسيرة، تكون مسيرة إصدار الشهادة صالحة من أجل السياسات المعددة في متحول الخرج *مجموعة السياسات المفروضة من المستعمل*.

وينبغي في هذا السيناريو ألا تستعمل التطبيقات مسيرة إصدار شهادة، إذا كان قد رفضها محرك إقرار صلاحية المسيرة بسبب فشل مرتبط بسياسة الشهادة.

وتجدر الملاحظة أن مسيرة إصدار الشهادة يمكن أن يصيبها في هذا السيناريو فشل مرتبط بالسياسة ومثال ذلك إذا كانت البنية التحتية (أي شهادة سلطة CA موجودة في مسيرة إصدار الشهادة) تستدعي وضع *مبين سياسة صريحة*. وفي هذه الحالة، يقوم محرك مناسب لإقرار صلاحية المسيرة بترجيع فشل. وينبغي للتطبيقات أن ترفض مسيرة إصدار الشهادة بسبب فشل من هذا النوع.

---

[4] فشل إقرار الصلاحية لمسيرة هو فشل مرتبط بسياسة الشهادة، عندما يتسبب في الفشل توسع (توسعات) ترتبط بسياسة الشهادة أو يتسبب فيه متحول (متحولات) حالة يرتبط بسياسة الشهادة. أما التوسعات المرتبطة بسياسة الشهادة فهي: **سياسات الشهادة (certificatePolicies)**، **وتقابلات السياسات (policyMappings)**، **وتقييدات السياسة (policyConstraints)**، **وحظر أي سياسة (inhibitAnyPolicy)**. وأما متحولات الحالة المرتبطة بسياسة الشهادة فهي: *مجموعة السياسات المفروضة من السلطة، ومبين سياسة صريحة، ومبين حظر تقابل السياسات، ومبين حظر أي سياسة*.

4.H مسيرة إصدار شهادة صالحة لسياسة خاصة بالمستعمل مرغوبة ولكنها ليست مطلوبة

يرغب المستعمل في هذا السيناريو أن تكون مسيرة إصدار الشهادة صالحة لواحدة من السياسات التي تهم المستعمل، ولكنه لا يريد أن يرفض المسيرات غير الصالحة لأي واحدة من السياسات التي تهم المستعمل. وفي سبيل الحصول على المعلومات المطلوبة، ينبغي للمستعمل أن يضع كما يلي مُدْخلات إقرار الصلاحية لمسيرة إصدار الشهادة المتعلقة بمعالجة السياسة:

مجموعة السياسات الأولية = {مجموعة السياسات التي تهم المستعمل}

سياسة صريحة أولية = **خاطئ**

وإذا نجح إقرار صلاحية المسيرة، تكون مسيرة إصدار الشهادة صالحة من أجل السياسات المعددة في متحول الخرج *مجموعة السياسات المفروضة من المستعمل*. ويلاحظ بأن المتحول *مجموعة السياسات المفروضة من المستعمل* ربما يكون *معدوماً* في هذه الحالة، عندما لا يكون *مبين سياسة صريحة* موضوعاً. وينبغي للتطبيق أن يتفحص المتحول *مجموعة السياسات المفروضة من المستعمل* العائد، لكي يحدد إن كانت المسيرة مقبولة من المستعمل.

وينبغي للتطبيق أن يرفض مسيرة إصدار الشهادة بسبب الفشل المرتبط بالسياسة الذي تسببه البنية التحتية في هذا السيناريو (أي عندما تكون *مجموعة السياسات المفروضة من السلطة* خالية، ويكون مبين سياسة صريحة موضوعاً).

وتجدر الملاحظة أن مسيرة إصدار الشهادة يمكن أن يصيبها في هذا السيناريو فشل مرتبط بالسياسة. ومثال ذلك إذا كانت البنية التحتية (أي شهادة سلطة CA موجودة في مسيرة إصدار الشهادة) تستدعي وضع *مبين سياسة صريحة*. وفي هذه الحالة، إذا كانت المسيرة غير صالحة لأي سياسة، أي *مجموعة السياسات المفروضة من السلطة* خالية، يقوم محرك مناسب لإقرار صلاحية المسيرة بترجيع فشل. وينبغي للتطبيقات أن ترفض مسيرة إصدار الشهادة بسبب فشل من هذا النوع.

وهناك مثال آخر من فشل مرتبط بالسياسة هو اجتماع مُدْخل المستعمل مع البنية التحتية. وهذا يحدث عندما تتسبب شهادة السلطة CA الموجودة في مسيرة إصدار الشهادة في وضع *مبين سياسة صريحة* و*مجموعة السياسات المفروضة من السلطة* غير خالية بينما *مجموعة السياسات المفروضة من المستعمل* خالية. ويقوم محرك مناسب لإقرار صلاحية المسيرة بترجيع فشل. وفي هذه الحالة إذا كان الداعي الوحيد الذي يجعل محرك إقرار صلاحية المسيرة يعيد "الفشل"، هو أن *مجموعة السياسات المفروضة من المستعمل* خالية، تستطيع التطبيقات أن تختار تخطّي هذا الفشل وقبول مسيرة إصدار الشهادة. وتبقى التقييدات المفروضة من السلطة مستوفاة، بفعل كون مجموعة *السياسات المفروضة من السلطة* غير خالية. وقبول أحد التطبيقات لهذه المسيرة يكافئ إعادة تقديم التطبيق للمسيرة إلى محرك إقرار الصلاحية مع كون *مجموعة السياسات الأولية* تساوي *أي سياسة*، و*سياسة صريحة أولية* تساوي "**خاطئ**" كما يكافئ تفحص *مجموعة السياسات المفروضة من المستعمل* المعادة، بغية تحديد ما إذا كانت المسيرة مقبولة.

الملحق I

مسائل توسع شهادة استعمال المفتاح

(لا يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

إن دمج بتة الالتزام بالمحتوى (contentCommitment) في توسع شهادة استعمال المفتاح مع غيرها من بتات استعمال المفتاح، قد يحتاج إلى مقتضيات أمنية تتوقف على البيئة الأمنية المتوقع استعمال الشهادة فيها. وإذا أمكن التحكم الكامل في بيئة الصاحب والوثوق بها تماماً، لن تكون هناك أي مقتضيات أمنية خاصة. وهذه هي الحال مثلاً عندما يكون الصاحب واثقاً تماماً بالمعطيات الموقّعة فعلاً أو واثقاً تماماً بالخصائص الأمنية لبروتوكول الاستيقان المستعمل. وإذا لم يمكن التحكم الكامل في بيئة الصاحب والوثوق بها تماماً، يمكن عندئذ توقيع الالتزامات توقيعاً غير مقصود. ويمكن أن نذكر على سبيل المثال تبادلات الاستيقان التي تحدث بصورة سيئة واستعمال مكوّنة برامجيات غير شرعية. وعندما يستعمل صاحبٌ بيئاتٍ غير موثوق بها، يمكن الحدّ من المقتضيات الأمنية باعتمادالتدبيرين التاليين:

- عدم الجمع في الشهادات بين قيم استعمال مفتاح "الالتزام بالمحتوى" وبين قيم أخرى لاستعمال المفتاح، واستعمال المفتاح الخاص المقابل فقط مع هذه الشهادة؛
- الحدّ من استعمال المفاتيح الخاصة المصاحبة للشهادات التي تكون فيها بتة استعمال المفتاح العمومي "الالتزام بالمحتوى" موضوعة، وقَصْر هذا الاستعمال على البيئات التي تعتبر موثوقة وقابلة للتحكم فيها بالقدر الكافي.

الملحق J

قائمة هجائية بتعريفات بنود المعلومات

(لا يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

يقدم هذا الملحق قائمة هجائية بتعريفات أنساق الشهادات والوقائم CRL، وتوسعات الشهادات، وأصناف الموضوعات، وأشكال الاسم، وأنماط النعت، وقواعد المواءمة المعرّفة في مواصفة الدليل هذه.

البند		رقم الفقرة
Certificate and CRL formats	***أنساق الشهادات والقوائم CRL***	
Certificate revocation list	قائمة إبطال الشهادات	3.7
Public-key certificate format	نسق شهادة المفتاح العمومي	7
Attribute certificate format	نسق شهادة النعت	1.12
Certificate, CRL & CRL entry extensions	***توسعات الشهادة والقائمة CRL ومدخل القائمة CRL***	
Freshest CRL extension	توسع أحدث قائمة CRL	6.2.6.8
Key usage extension	توسع استعمال المفتاح	3.2.2.8
Extended key usage extension	توسع استعمال المفتاح الموسع	4.2.2.8
Subject alternative name extension	توسع الاسم البديل للصاحب	1.2.3.8
Issuer alternative name extension	توسع الاسم البديل للمُصْدر	2.2.3.8
Base update extension	توسع التحيين الأساسي	5.2.6.8
Basic constraints extension	توسع التقييدات الساسية	1.2.4.8
Expired certificates on CRL extension	توسع الشهادات المنتهية صلاحيتها في القائمة CRL	12.2.5.8
To be revoked extension	توسع الشهادات الواجب إبطالها	10.2.5.8
Ordered list extension	توسع القائمة المرتبة	8.2.5.8
Indirect issuer extension	توسع المُصْدر غير المباشر	5.2.1.15
Targeting information extension	توسع المعلومات المستهدفة	2.2.1.15
Delta information extension	توسع المعلومات دلتا	9.2.5.8
Invalidity date extension	توسع تاريخ عدم الصلاحية	4.2.5.8
User notice extension	توسع تبليغ المستعمل	3.2.1.15
Policy mappings extension	توسع تقابلات السياسات	7.2.2.8
Delegated name constraints extension	توسع تقييدات الاسم المفوّض به	2.2.5.15
Name constraints extension	توسع تقييدات الأسماء	2.2.4.8
Policy constraints extension	توسع تقييدات السياسة	3.2.4.8
Basic attribute constraints extension	توسع تقييدات النعت الأساسية	1.2.5.15
Time specification extension	توسع توصيف المدة	1.2.1.15
Inhibit any policy extension	توسع حظر أي سياسة	4.2.4.8
CRL number extension	توسع رقم القائمة CRL	1.2.5.8
Acceptable privilege policies extension	توسع سياسات الامتياز المقبولة	4.2.1.15
Certificate policies extension	توسع سياسات الشهادة	6.2.2.8
Acceptable certificate policies extension	توسع سياسات الشهادة المقبولة	3.2.5.15

البند		رقم الفقرة
Reason code extension	توسع شفرة الداعي	2.2.5.8
Hold instruction code extension	توسع شفرة تعليمات الوضع في الانتظار	3.2.5.8
Issued on Behalf Of extension	توسع صادر نيبة عن (باسم ...)	6.2.5.15
No assertion extension	توسع غياب التأكيد	6.2.1.15
No revocation information extension	توسع غياب معلومات الإبطال	2.2.2.15
Private key usage period extension	توسع فترة استعمال المفتاح الخاص	5.2.2.8
Delta CRL indicator extension	توسع مبين القائمة دلتا CRL	4.2.6.8
CRL scope extension	توسع مجال تطبيق القائمة CRL	5.2.5.8
Revoked group of certificates extension	توسع مجموعة الشهادات المبطلة	11.2.5.8
Status referral extension	توسع مرجع الوضع القانوني	6.2.5.8
Certificate issuer extension	توسع مصدر الشهادة	3.2.6.8
Role specification certificate identifier extension	توسع معرف الهوية لشهادة توصيف الدور	1.2.4.15
SOA identifier extension	توسع معرف الهوية لَمصْدر السلطة	1.2.3.15
Authority attribute identifier extension	توسع معرف الهوية لنعت السلطة	4.2.5.15
CRL stream identifier extension	توسع معرف هوية تقاطر القوائم CRL	7.2.5.8
Authority key identifier extension	توسع معرف هوية مفتاح السلطة	1.2.2.8
Subject key identifier extension	توسع معرف هوية مفتاح الصاحب	2.2.2.8
Subject directory attributes extension	توسع نعوت الدليل للصاحب	3.2.3.8
CRL distribution points extension	توسع نقاط توزيع القوائم CRL	1.2.6.8
Issuing distribution point extension	توسع نقطة التوزيع المُصْدرة	2.2.6.8
Attribute descriptor extension	توسع واصف النعت	2.2.3.15
Object classes and name forms	***أصناف الموضوعات وأشكال الاسم***	
Delta CRL object class	صنف الموضوعات "القائمة دلتا CRL"	4.1.11
PKI CA object class	صنف الموضوعات "سلطة إصدار الشهادة في البنية PKI"	2.1.11
PMI AA object class	صنف الموضوعات "سلطة النعت في البنية PKI"	2.1.17
Protected privilege policy object class	صنف الموضوعات "سياسة الامتياز المحمية"	7.1.17
Privilege policy object class	صنف الموضوعات "سياسة الامتياز"	6.1.17
Certificate policy and CPS object class	صنف الموضوعات "سياسة الشهادة وإعلان الممارسات في إصدار الشهادة"	5.1.11
Attribute certificate CRL distribution point object class	صنف الموضوعات "شهادة نعت لنقطة توزيع القائمة CRL"	4.1.17
PKI user object class	صنف الموضوعات "مستعمل البنية التحتية PKI"	1.1.11
PMI user object class	صنف الموضوعات "مستعمل البنية التحتية PKI"	1.1.71
PMI delegation path	صنف الموضوعات "مسيرة التفويض في البنية PKI"	5.1.17
PKI certificate path object class	صنف الموضوعات "مسيرة الشهادة في البنية PKI"	6.1.11
PMI SOA object class	صنف الموضوعات "مَصدر السلطة في البنية PKI"	3.1.17
CRL distribution points object class and name form	صنف الموضوعات وشكل الاسم لنقاط توزيع القائمة CRL	3.1.11
Directory attributes	***نعوت الدليل***	
Certification practice statement attribute	نعت "إعلان الممارسات في إصدار الشهادة"	8.2.11
Supported algorithms attribute	نعت "الخوارزميات المدعومة"	7.2.11
Cross-certificate pair attribute	نعت "زوج الشهادات المتقاطعة"	3.2.11
Protected privilege policy attribute	نعت "سياسة الامتياز المحميّة"	8.2.17

البند		رقم الفقرة
Privilege policy attribute	نعت "سياسة الامتياز"	7.2.17
Certificate policy attribute	نعت "سياسة الشهادة"	9.2.11
User certificate attribute	نعت "شهادة المستعمل"	1.2.11
Attribute certificate attribute	نعت "شهادة النعت"	1.2.17
CA certificate attribute	نعت "شهادة سلطة إصدار الشهادة"	2.2.11
AA certificate attribute	نعت "شهادة سلطة النعت"	2.2.17
Attribute descriptor certificate attribute	نعت "شهادة واصف النعت"	3.2.17
Authority revocation list attribute	نعت "قائمة إبطال السلطات"	5.2.11
Certificate revocation list attribute	نعت "قائمة إبطال الشهادات"	4.2.11
Delta revocation list attribute	نعت "قائمة إبطال دلتا"	6.2.11
Attribute certificate revocation list attribute	نعت "قائمة إبطال شهادات النعت"	4.2.17
AA certificate revocation list attribute	نعت "قائمة إبطال شهادات سلطة النعت"	5.2.17
PKI path attribute	نعت "مسيرة البنية التحتية PKI"	10.2.11
Delegation path attribute	نعت "مسيرة التفويض"	6.2.17
XML Protected privilege policy attribute	نعت سياسة الامتياز المحميّة في اللغة XML	9.2.17
XML privilege information attribute	نعت معلومات عن الامتياز في اللغة XML	5.15
Matching rules	***قواعد المواءمة***	
Indirect issuer match	توسع المُصْدر غير المباشر (مواءمة)	5.2.1.15
Enhanced certificate match	قاعدة محسّنة لمواءمة الشهادة	10.3.11
Policy match	مواءمة السياسة	8.3.11
Certificate match	مواءمة الشهادة	2.3.11
Holder issuer match	مواءمة المُصْدر/الحامل	3.3.17
Delegated name constraints match	مواءمة تقييدات الاسم المفوض به	1.2.2.5.15
Basic attribute constraints match	مواءمة تقييدات النعت الأساسية	1.1.2.5.15
Time specification match	مواءمة توصيف المدة	1.1.2.1.15
Certificate pair match	مواءمة زوج الشهادات	4.3.11
Acceptable certificate policies match	مواءمة سياسات الشهادة المقبولة	1.3.2.5.15
Attribute certificate match	مواءمة شهادة النعت	2.3.17
Certificate list match	مواءمة قائمة الشهادات	6.3.11
PKI Path match	مواءمة مسيرة البنية التحتية PKI	9.3.11
Delegation path match	مواءمة مسيرة التفويض	4.3.17
Certificate pair exact match	مواءمة مضبوطة لزوج الشهادات	3.3.11
Certificate list exact match	مواءمة مضبوطة لقائمة الشهادات	5.3.11
Certificate exact match	مواءمة مضبوطة للشهادة	1.3.11
Attribute certificate exact match	مواءمة مضبوطة لشهادة النعت	1.3.17
Role specification certificate ID match	مواءمة معرف الهوية لشهادة توصيف الدور	1.1.2.4.15
Algorithm identifier match	مواءمة معرف هوية الخوارزمية	7.3.11
AA identifier match	مواءمة معرف هوية سلطة النعت	1.4.2.5.15
SOA identifier match	مواءمة معرف هوية مَصْدر السلطة	1.1.2.3.15
Attribute descriptor match	مواءمة واصف النعت	1.2.2.3.15

الملحق K

التعديلات والتصويبات

(لا يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

تتضمن هذه الطبعة من المواصفة للدليل مشروع التعديل التالي الذي صوّتت ووافقت ووافقت عليه المنظمتان ISO/UEC:

- التعديل 4 بشأن التوسعات في شهادات النعت والمفتاح العمومي.

وتتضمن هذه الطبعة من هذه المواصفة للدليل التصويبات التقنية التالية التي تخص الأخطاء المشار إليها في كشوف الأخطاء التالية الخاصة بالطبعة الرابعة من هذه المواصفة:

- التصويب التقني رقم 1 (الذي يعني كشوف الأخطاء 272، 273، 274، 275، 276، 277، 278، 279)؛
- التصويب التقني رقم 2 (الذي يعني كشوف الأخطاء 284، 285، 286)؛
- التصويب التقني رقم 3 (الذي يعني كشوف الأخطاء 281، 282، 289، 291، 296، 298، 299، 300، 301، 304، 305).

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 وتعدد الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات البرامج الإذاعية الصوتية والتلفزيونية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	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	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات المعطيات على الشبكة الهاتفية
السلسلة X	**شبكات المعطيات والاتصالات بين الأنظمة المفتوحة والأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا
جنيف، 2006